

eForensics

Magazine

Computer

VOL. 1 NO. 1

INTERVIEW WITH KRISTINN GUÐJONSSON – THE CREATOR OF THE TOOL log2timeline

- **DAVID SCHIPPERS SERIES:
HOW TO - THE BLACKBAG
ACQUISITION I & II**
- **REGISTRY FORENSICS**
- **LAWTECH EUROPEAN CON-
GRESS IN PRAGUE**
- **DNSCHANGER MALWARE:
A NIGHTMARE FOR INTERNET**

Nevada PI Lic#1948 Expert Data Forensics is a d/b/a ICS of Nevada LLC.
2675 S. Jones St. Suite 207A, Las Vegas NV 89146
PO Box 35006 Las Vegas, NV 89133
T: 702-435-8885 O: 888-355-3888 F: 702-453-8887
[Lic#1498] [Tax ID: 20-4239533]

ExpertDataForensics.com



**EXPERT DATA
FORENSICS**

**INVESTIGATORS OF
ELECTRONIC EVIDENCE**

Digital Forensic & Investigative Services

- First response
- Extraction & preservation of digital contents
- Electronic investigations (Lic#1498)
- Chain of custody
- Expert witness for court/depositions
- Digital data & electronic analysis
- Seizure of digital evidence for forensic purposes
- Investigation of digital evidence
- Recovery of deleted digital content
- Consultation & preventative strategy
- Corporate systems & security analysis
- Data analysis & recovery
- Cell phones & mobile devices data extraction, preservation & analysis
- Retrieve & analyse text messages, emails, images etc.
- Corporate digital crime reconstruction
- Web surfing pattern analysis
- Online hacking, Email investigation
- Authentication of digital data (certificate)
- Password recovery
- Cyber hacking, stalking and activity patterns
- Electronic fraud detection
- Digital corporate sabotage
- Corporate/private infringement
- Employee misuse

Forensic Data Recovery Services

- We specialize in forensic data recovery from computers, cell phones, PDA's
- Data recovery of hard disk
- Data recovery of deleted files
- Digital imaging from electronic device
- Password recovery
- Digital recovery of deleted data contents (emails, txt messages, web chats)

Who Uses Our Services

- Attorneys in litigation criminal, defence, civil and general
- Government/state & federal
- Domestic disputes & child custody
- Employers with employee issues
- CPA's & Accountants in accounting disputes
- Private Investigators
- Insurance Agencies
- Corporations/individuals with fraud issues

Who Do We Service?

- Private Individuals; who hire us in matters of domestic affairs such as; divorce, custody, mistrust, family disputes.
- Corporations; who hire us to assist in; partnership disputes/mistrust, employee/management/mistrust, verifications in mergers and acquisition transactions, sexual harassment, corporate espionage, data authentication, corporate sabotage, embezzlement, fraud.
- Private Investigators; we provide specialized support services to investigators with electronic, digital data and eDiscovery involving password retrievals, eSecurity, data recovery and electronic authentication.
- Legal Professionals; attorneys from all fields, court appointed council, receivers, legal support services and paralegals in civil and criminal matters
- Government; matters involving public defense and private consulting, matters involving child exploitation and cybercrimes.



TEAM

Editor: Joanna Derehajło
joanna.derehajlo@software.com.pl

Betatesters/Proofreaders: Sean E., Vaman Amarjeet, Nicolas Villatte, Loren O'Brien, Mindy Rockwell, Gabriele Biondo, Jan-Tilo Kirchhoff, Salvatore Fiorillo, Danilo Massa, Scott Taylor, Olivier Caleff

Senior Consultant/Publisher: Paweł Marciniak

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

Art Director: Mateusz Jagielski
mateuszjagielski@gmail.com
DTP: Mateusz Jagielski

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

Marketing Director: Ewa Dudzic

Publisher: Software Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokszerska 1
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.

THERE IS A CLEAR NEED FOR BETTER DATA REDUCTION TECHNIQUES THAN WE CURRENTLY HAVE.

Dear Readers!

We would love to think over the future of the digital forensics which is definitely evolving. More and more different tools and techniques come into being. We are so happy about that Kristinn Guðjónsson – the inventor of the tools and specialist who works on the incident response team at Google – shares his opinions and knowledge with you. He also describes the usage of tool log-2timeline which was awarded for being The Best Digital Forensics Tool in 2011! We have asked Kristinn Guðjónsson about the future of digital forensics and he admitted that there is a clear need for better data reduction techniques than we currently have. Do you agree with his opinion? Take a look at the interview via [page 6](#). Remember about the security while using the network tools, programs or even an iPhone! You get more info from an article: “Registry Forensics” – Arshdeep Chaggar shows how to use the registry editor which helps to secure the system. Praveen Parihar via “DNSChanger Malware: A Nightmare For Internet” describes DNSChanger, DNS and how to check if DNSChanger has infected our system.

David Shippers, our new author, prepare for you very interesting two-part article series called: “How to – The Black Bag Acquisition” describing the planning, onsite operations and field/offsite/lab acquisition steps to complete the acquisition process. Very useful knowledge!

Beware of the attackers! They can crack password and get the access to the computer... Can we protect our data nowadays? Can we feel safe? Read the “Sam File Forensics: Windows Password audit” by Praveen Parihar via [page 24](#).

At the end, you learn about the encryption - process which enables to protect our privacy – and encrypting the packets. If you use an iPhone, you should read the last text by Donovan Farrow.

Big thanks to our authors who did their best and prepared texts for you. I hope you like them. I cannot imagine work without our beta-testers and proofreaders... They are so helpful and have a lot of patience! I know that I can always count on you,

Enjoy reading,
Joanna Derehajło
& eForensics Team,

Thank you for your great support and invaluable help!

6. INTERVIEW OF THE ISSUE

by Vaman Amarjeet, Sean E. and eForensics Editor

Kristinn Guðjónsson – the expert works on the incident response team at Google – is answering the questions concerning digital forensic and himself. He also describes the usage of tool log2timeline which he has created. The log2timeline was awarded for being The Best Digital Forensics Tool in 2011.

NETWORK FORENSICS

10. REGISTRY FORENSICS

by Arshdeep Chaggar

In this article, Arshdeep Chaggar, shows how to use the registry editor which helps to secure the system.

12. DNSChanger MALWARE: A NIGHTMARE FOR INTERNET

by Praveen Parihar

The article describes DNSChanger, DNS and how to check if DNSChanger has infected our system.

16. HOW TO – THE BLACK BAG ACQUISITION PART I

by Dave Shippers

The first part of a two-part article series, covering the planning, onsite operations and field acquisition steps

20. HOW TO – THE BLACK BAG ACQUISITION PART II

by Dave Shippers

The second part of two-part article series which covers the offsite/lab acquisition steps to complete the acquisition process.

24. SAM FILE FORENSICS: Windows Password audit

by Praveen Parihar

The article warns before attackers. Author explains the truth inside password hashing and how an attacker can crack windows password and get the access to the windows computer.

NETWORK FORENSICS

28. ENCRYPTING YOUR PACKETS

by Donald Cinco

Donald Cinco describes what the Encryption is and explains how to secure our privacy. The author describes installing a software to encrypt our data and presents how to encrypting the packets. He also mention why we should use it.

MOBILE FORENSICS

34. A STEP BY STEP: DIGITAL FORENSICS PROCESS OF COLLECTING EVIDENCE FROM AN iPhone

by Donovan Farrow

In this article, Donovan Farrow take you through a step by step digital forensic process of collecting evidence from an iPhone. These steps will help you build a defensible process in order to present your data in court.

INTERVIEW WITH KRISTINN GUÐJÓNSSON

Kristinn Guðjónsson works on the incident response team at Google, where his daily responsibilities include incident response, computer forensics and tool development. Before joining Google, he worked as a technical security manager at ArionBanki and, before that, as a team leader of information security at Skyggvir.

Kristinn holds a Master of Science degree in Computer Engineering from INT (Institute National des Telecommunications) in Paris as well as a Bachelor of Science degree in Electrical and Computer Engineering from the University of Iceland. Kristinn, also, holds several GIAC certifications such as GCIA, GCIH and GCFA Gold.

Kristinn has given talks at various security conferences, taught courses in both University of Reykjavík and University of Iceland on information security as well as regularly giving seminars to increase security awareness among employees of various companies in Iceland. Kristinn occasionally writes blogs about computer forensics and incident response, which can be read at <http://blog.kiddaland.net> and on the SANS forensic blog <https://blogs.sans.org/computer-forensics>. He is also the author and creator of the tool log2timeline, an artifact timeline creation and analysis tool.

1. When and how did you get involved in digital forensics?

"My story is neither heartbreaking nor filled with super exciting stories that 'wow' people, more a very plain story of a simple engineer. After first hearing about what an engineer does at the age of 12, I knew that I wanted to become one, even though I really had no idea what that meant. And, despite my initial aspirations to become an electrical engineer, I ended up on the darker side of computer engineering. When it came time to register for university, it was of no surprise that I chose electrical and computer engineering. However, as

soon as I entered the computer science classes, I realized that I wanted to shift gears and focus on the computer engineering aspect, and more specifically, security – a field that somehow bewitched me. I've always had the need to know how things work, and I quickly realized that those skills fit well in the security arena. Despite little emphasis on security at my university, I tried to pick courses that were somewhat related to security – whenever I had the chance – as well as study the field on my own.

I had been working for a local hosting provider in my home country, while in school, and continued to do so after graduation.

There I led the information security team, which meant getting involved in incident response (IR). Though it covered only a small percentage of my time, I really enjoyed it. I started taking SANS courses to further strengthen my knowledge in the field and finally took the 508 (forensics) class in 2008. There was no turning back after that; I knew that forensics was the field in which I wanted to specialize. Afterwards, I moved from doing part-time incident response to spending most of my time on IR and forensics as a consultant, ending up working full-time in the field."

2. What does your tool log2timeline do? Would you describe its specific usage?

"Essentially, what you are trying to accomplish with any forensics or incident response investigation is to convey a story. In the incident response world, that story usually revolves around how a system was compromised and what the attackers managed to accomplish while having access to the compromised system. In the more traditional forensics investigations, the story often revolves around user action, that is, what a particular user did or did not do on the computer.

In order for us to be able to tell this story, we need to gather digital evidence from various data sources and correlate them. And, the best way to correlate different data sources is to find some commonality that can be used to join it. As it happens, there are quite a few artifacts on any given computer system that contain timestamps. Besides the traditional timestamps that are stored for every file on the system, there are, also, many log files or other files that contain timestamps, associated with entries within them. This makes it perfect to correlate all these different data sources by their common denominator: timestamps. It, also, makes it even easier for us to tell the story. When we correlate all these different data points, we have them in the correct time order. So, then, we know the sequence of events.

In essence, log2timeline is a tool that extracts all those time-stamped events, which are spread throughout the entire file system, and combines them into a single data source that can be analyzed by the investigator. The tool is built as a modular framework with plugins that can either define an output or a parser, making it easy to extend its capabilities. It, also, deals with presenting all the timestamps that are collected in the same manner, independent of how they are stored in the system.

The tool's main focus is to make it easier for the investigator to correlate these different data sources in a simple manner and, by doing so, potentially pointing them to additional evidence or artifacts that may need further attention. It is often the case that you only know part of the story when the initial analysis starts, and seeing events that occur in temporal proximity to those data points can quickly lead you to additional source that can help you paint the complete picture."

3. It seems like the trend in forensics is to emphasize malware and breach investigations over more traditional, conventional abuse and misuse investigations. How do you feel that this trend affects our profession?

"I don't think this is a trend at all. These are just different types of investigations, depending on your job role. Corporate investigations often revolve more around breach or malware investigations, while law enforcement deals more with the traditional ones. These are just two different types of investigations that share some common methodologies and artifacts and, also,

differ in many ways to how the investigations are approached."

4. What is the importance of timestamp analysis in digital forensics?

"As I answered previously, timestamps serve a very important factor in digital forensics. They both indicate when a certain event occurred, and, therefore, in which order, as well as being key to correlating different data sources. That makes timeline analysis a very powerful technique for investigators, since it can quickly identify sequence of events and find events that are in temporal proximity to one another.

Collecting timestamps from different data sources, also, provides a great way for investigators to spot anomalies in their data set. It is often very difficult or impossible for attackers or malicious users to change all timestamps that they touch through their actions. They may be able to change some of them. However, it may be either impossible or at least very hard to change all of them. Analyzing timestamps from several different data sources can, therefore, serve as a means to confirm or deny that a malicious user or attacker has purposely modified timestamps. Even though other methods – like analyzing data that should be stored in sequence – can be used to detect time stamping or other methods of timestamp changes, super-timeline analysis provides the investigator with a quick and reliable method of doing so."

5. Which certifications do you feel one must attain, so as to prove one's skills and have a better chance for a job opportunity?

"This is a tough question to ask, since there are a plethora of certifications out there that you can take. I haven't gone through all of them myself, so it's difficult for me to compare them.

Personally, I've always leaned toward the more technical and less vendor-related certifications, which, in my case, have been SANS certifications. However, there are other certifications than SANS out there that have that focus, too. I feel that certifications that focus more on techniques and methodologies over explicit tool usage are more useful for the investigator in the end; that is, certifications that train you as an investigator as opposed to teach you how to use a specific tool. However, knowing your tools is also very important. Sometimes, it can help, taking these tool certifications in addition to the broader technique-based ones.

And, again, this all depends. Some jobs require you to have certain certifications, whether that is because they depend on a certain tool or for some other reasons. Then it might make sense to get that particular certification to increase your chances, before applying. Overall, I think all these certifications have a place, for no other reason than to show that you have the minimum skills to pass that particular certificate. But, they should not be the sole factor in any hiring decision, whether that is to deny or hire someone. That is, they may help you, but, in the end, it is not enough just to get some certification and think that will be your golden ticket."

6. What, according to you, are the most important characteristics of good Digital Investigator?

"This is also a tough question, since this field is filled with pe-

ople with very diverse backgrounds. The field of digital forensics involves people that have either a strong computer science or technical background or those that came into the field from the military or law enforcement side and really know how to conduct investigations but may lack deep technical skills or even those that have both (some people just have it all).

I think that both of these skill sets are important to have, or, at least, some exposure to both. Despite the fact that you can be a very successful forensic investigator without knowing anything about programming, I do believe that some exposure to software development is important. Knowing how to read code and understand software development helps you understand some of the artifacts you need to analyze.

In addition, there are various aspects of each examination that may be repetitive or involve looking for the same things over and over, again. Knowing, at least, how to write simple scripts really helps with automating these tasks and can save you a lot of valuable time.

There are, also, so many great open-source forensics tools out there that may lack some plugins or functionality that you really need during an investigation. Knowing some basic scripting is sometimes enough to create a plugin that can be used in these tools and benefit the community as a whole and make your life easier."

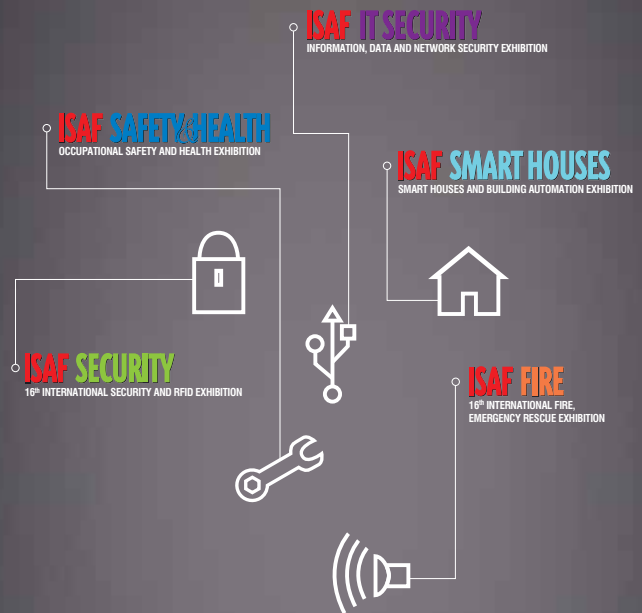
7. What, according to you, is the future of Digital Forensics?

"We have been seeing the sheer volume of data increasing over the past few years, and I think we will continue to see that. Also, with new tools and techniques, we manage to extract more features or data sources into our investigations, all of which contribute to one thing: more data that we need to analyze.

This often leads to overwhelming data presented to investigators. So, I think that there is a clear need for better data reduction techniques than we currently have. I like to believe that we will see new tools coming out that try to fix that gap and help us reduce the ever-increasing data set into a manageable one. This may, also, require us to rethink some of the procedures and approaches that we take, since we cannot examine everything anymore."



The **Most Comprehensive** Exhibition
of the Fastest Growing Sectors of recent years
in the **Center of Eurasia**



www.isaffuari.com

SEPTEMBER 20th - 23rd, 2012
IFM ISTANBUL EXPO CENTER (IDTM)



MARMARA
TANITIM FUARCILIK
T. +90 212 503 32 32 | marmara@marmarafuar.com.tr
www.marmarafuar.com.tr

THIS EXHIBITION IS ORGANIZED WITH THE PERMISSIONS OF T.O.B.B.
IN ACCORDANCE WITH THE LAW NUMBER 5174.

LTEC

LAWTECH EUROPE CONGRESS

2012

Buy **SUBSCRIPTION** to our magazine for 1 year and
get a free ticket (worth EUR 199) to
LawTech Europe Congress!

During the LTEC, you will have the chance to win an
iPad, a **Blackberry**, and an **Amazon Kindle** - See prizes



REGISTRY FORENSICS

The world is moving at a very rapid pace and so is the technology. Everyone around us is some how related to the digital world. We use laptops Smartphone etc to communicate with are friends and family. There are Wi-Fi networks all over the places like hospital, school, colleges, and offices etc which help us to stay connected. The network setup is done so that each one in the network is connected to it.

ARSHDEEP CHAGGAR

There are different users who use the network be it in office or in a college. Every system that is connected to the network be in LAN, MAN, WAN etc has important information in it. There are official file of high security which may have the financial statics of the company. An attacker can breach or compromise with network security to access the systems. To safe guard the systems there is a need to monitor the intrusion detection systems i.e. IDS. To under stand the network better we need to know how the attacker can attack the system, what are the recovery options available to us to eliminate the attacker. The security of the system can be breached thru the registry file i.e. by opening the registry editor. To open it we have to go to run and type regedit.

key's value is similar to a file within a folder. In the right-hand pane of the Windows Registry - a value's name is similar to a file's name, its type is similar to a file's extension, and its data is similar to the actual contents of a file.

The classification of the different keys is as follows:

1.HKEY_CLASSES_ROOT (HKCR)

Information stored here ensures that the correct program opens when it is executed in Windows Explorer. It also contains further details on drag-and-drop rules, shortcuts, and information on the user interface. Alias for: HKLM\Software\Classes

2.HKEY_CURRENT_USER (HKCU)

Contains configuration information for the user who is currently logged into the system, including user's folders, screen colors, and Control Panel settings. Alias for a user specific branch in HKEY_USERS. The generic information usually applies to all users and is HKU\DEFAULT.

3.HKEY_LOCAL_MACHINE (HKLM)

Contains machine hardware-specific information that the operating system runs on. It includes a list of drives mounted on the system and generic configurations of installed hardware and applications.

4.HKEY_USERS (HKU)

Contains configuration information of all user profiles on the system, which concerns application configurations, and visual settings.

5.HKEY_CURRENT_CONFIG (HCU)

Stores information about the systems current configuration. Alias for: HKLM\Config\profile

Till date, there are many different tools available to forensic examiners for extracting evidentiary information from the Registry. Registry Editor is free and available on any installation of Microsoft Windows XP with administrator privileges.

To examine the registry

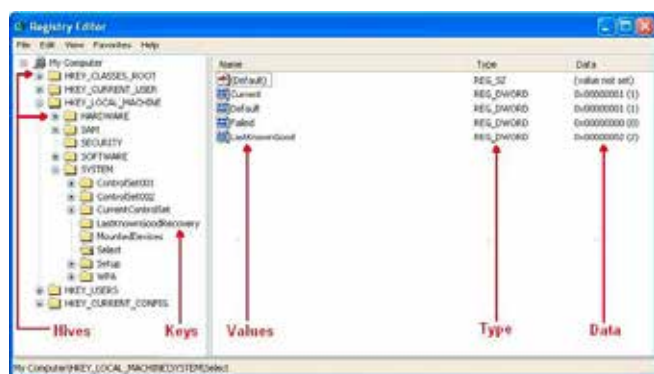


Figure The opening of the registry editor

The left side pane is having the organized listing of the folders. There are 5 hives which begin with HKEY. HKEY is an abbreviation for Handled to a Key. Among the 5 hive there are only two which are real HKEY_USERS and HKEY_LOCAL_MACHINE while the rest of the 3 are the sub hive or the branches of them. The entire 5 hive consist of the values and sub keys. Values are the names of certain items within a key, which uniquely identify specific values pertaining to the operating system, or to applications that depend upon that value. The keys and sub keys located within the five main hives are similar to folders and subfolders of Windows Explorer, and a

The value associated with all the registry keys is called the 'LastWrite' time, which is very similar to the last modification time of a file. FILETIME structure stores a value and indicates when the Registry Key was last modified. The LastWrite time is updated when a registry key has been created, modified, accessed, or deleted. Unfortunately, only the LastWrite time of a registry key can be obtained, where as a LastWrite time for the registry value cannot. Knowing the LastWrite time of a key can allow a forensic analyst to infer the approximate date or time an event occurred. And although one may know the last time a Registry key was modified, it still remains difficult to determine what value was actually changed. Using the Registry as a log is most helpful in the correlation between the LastWrite time of a Registry key and other sources of information, such as MAC (modified, accessed, or created) times found within the file system.

MRU lists

MRU, or 'most recently used' lists contain entries made due to specific actions performed by the user. There are numerous MRU lists located throughout various Registry keys. The Registry maintains these lists of items in case the user returns to them in the future. It is basically similar to how the history and cookies act to a web browser.

UserAssist

The UserAssist key, HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, contains two or more subkeys which have long hexadecimal names that appear as globally unique identifiers (GUIDs). Each subkey records values that pertain to specific objects the user has accessed on the system, such as Control Panel applets, shortcut files, programs, etc. These values however, are encoded using a ROT-13 encryption algorithm, sometimes known as a Caesar cipher.



Figure HKEY_CURRENT_USER shows configuration information for the user who is currently logged into the system

Wireless Networks

Wireless networks today are popular and are only becoming more popular. A wireless ethernet card picks up wireless access points within its range, which are identified by their SSID or service set identifier. When an individual connects to a network or hotspot the SSID is logged within Windows XP as a preferred network connection. Unsurprisingly, this can be found in the Registry in the HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces key. When opening this Registry key there may be subkeys beneath it, like UserAssist, that look like GUIDs. The contents of these should contain the values 'ActiveSettings' and 'Static#0000'. There may be additional values that begin with 'Static#' and are sequentially

numbered. In the binary data of these 'Static#' values are the network SSIDs of all the wireless access points that system has connected to. This can be seen by right clicking the value and selecting 'modify'. Windows also logs the network settings of that particular connection - such as the IP address, DHCP domain, subnet mask, etc. The Registry key in which this can be found is HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\.

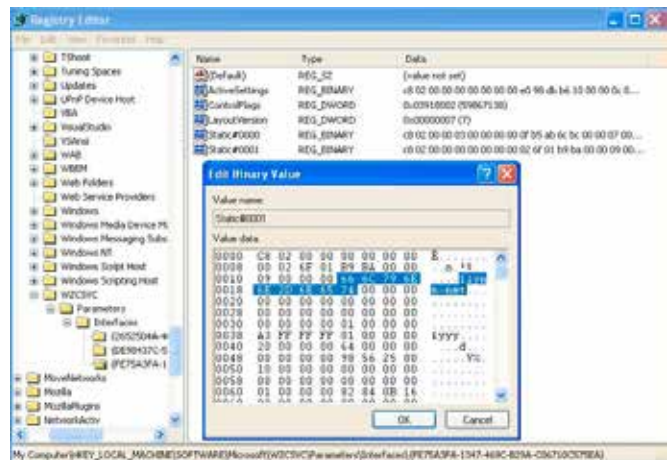


Figure HKEY_LOCAL_MACHINE (HKLM)

It is important for the computer forensics experts to understand complex structure of the Windows Registry of the Windows OS in homes and businesses. The Registry holds the potential evidence and also the information which can help in the uncovering the data in an investigation of the system related issues. An examiner can develop a more precise account on what actions occurred on the given machine by understanding the fundamentals of the Registry from a forensics standpoint. For as long as operating systems are dependent upon the Registry as a configuration database, and for as long as applications continue to use that database for storage, there will always be different locations to discover that provide evidential support in an investigation.

References:

NirSoft (<http://www.nirsoft.net>)

SysInternals/Microsoft tools (<http://technet.microsoft.com/en-us/sysinternals/bb896653> | <http://technet.microsoft.com/en-us/sysinternals/>)

By Arshdeep Chaggar
INFIZEAL TECHNOLOGIES, New Delhi
Senior Technical Consultant

DNSChanger malware: A NIGHTMARE FOR INTERNET

PRAVEEN PARIHAR

DNSChanger a malware or Trojan which brought a nightmare to all internet users and this is the only Trojan or malware which has sustained for such a long time i.e. 5 years, as it was started in may 2005 and recently it infected lot of servers and created a havoc among internet users and service provider as well, Before going into the depth of DNSChanger we would describe a little bit about DNS.

DNS (Domain Name System) is an Internet service that converts domain names into the numerical Internet protocol (IP) addresses that computers use to talk to each other. One cannot remember thousands of IP Addresses therefore DNS converts respective domain name into IP addresses. When a User access a particular website such as google.com (domain name) which is first converted into respective IP Addresses. This domain name is converted using Domain name server. DNS server is operated by an Internet service provider (ISP) and It is included in one's computer as well. DNS is a critical component of computer operating environment, we would not be able to access websites, send e-mail, or use any other Internet services without DNS.

Criminals have learned that if they can control a user's DNS server, they can control what sites the user connects to on the Internet. By controlling DNS, a criminal can get an unsuspecting user to connect to a fraudulent website or to interfere with user's web browsing. One way criminals do this is by infecting computers with a class of malicious software (malware) called DNSChanger. In this scenario, the criminal uses the malware to change the user's DNS server settings to replace the ISP's original DNS servers with malicious DNS servers operated by the criminal. A DNS server operated by a criminal is referred to as a rogue DNS server. These rogue DNS servers could

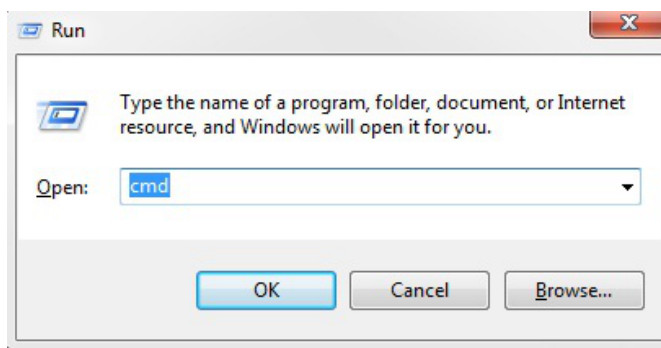
bring some more malicious contents on the network and further network can be compromised based on the vulnerabilities present on the operating system. Recently The FBI has uncovered a network of rogue DNS servers and has taken steps to disable it. The FBI is also undertaking an effort to identify and notify victims who have been impacted by the DNSChanger malware. One consequence of disabling the rogue DNS network is that victims who rely on the rogue DNS network for DNS service could lose access to DNS services. FBI is working with private sectors to clean rogue DNS server and fix the infected computers. Although the establishment of the clean

DNS servers does not guarantee that the computers are safe from other malware but it ensures that users are free from rogue DNS servers and they are not infected with DNSChanger.

DNSChanger malware causes a computer to use rogue DNS servers and compromise the small office and home office which is running on DHCP network. The malware attempts to access these devices using common default usernames and passwords and, if successful, changes the DNS servers these devices use from the ISP's original DNS servers to rogue DNS servers. When DNSChanger infects a victim computer then it is redirected to an advertisement website which makes money and this malware could be installed in the form of email attachment, phishing and malicious website .The malware targets small and office network and targets to exploit default username and password vulnerabilities and exploit the network further which makes the malware contagious in nature.

How to check If DNSChanger has infected you:

The best way to evaluate your computer against DNSChanger Trojan is just to check the DNS settings of local computer first because it might be possible that only a specific computer is infected with the malware and Internet service provider is not infected which can be checked using the following steps:-



A user needs to check the IP Address of DNS server which could be found under this:

Ipconfig /all which gives the detail of Domain name server which is related to your ISP (Internet service provider)



As it is shown in figure 1(a), DNS and DHCP server have been shown and some of the information is hidden because of security issues.

This DNS server obtained with this observation needs to be checked against the black-listed rogue DNS server so that one can make sure that DNSChanger malware has not affected user and a forensics investigator can analyze the registry entry to ensure the presence of DNSChanger on victim's computer.

The DNSChanger working group has also established a website to check if a user is infected with DNSChanger or not. This website fetches the DNS server to which the victim is connected and checks it against the rogue DNS server list which is stored in the database.

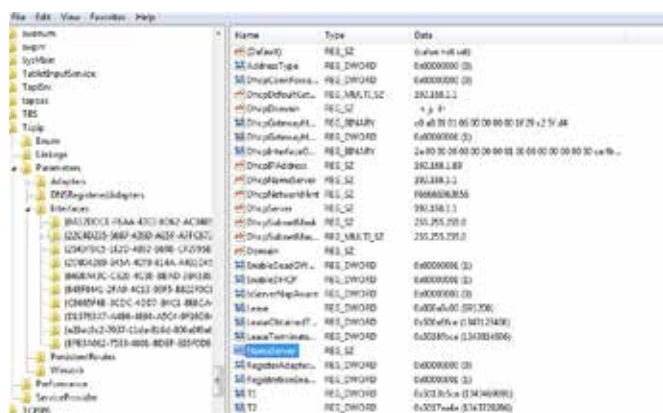
(Website: www.dns-ok.us)

Identify DNSChanger Trojan artifacts:

When a DNSChanger malware is installed on victim's computer then it will change the infected system's Domain Name Server (DNS) settings and diverts the traffic to Unsolicited, and potentially illegal sites or advertisement website which is established to make money. Trojan is only 15KB in size and It changes the registry entry so that victim can be redirected to rogue Domain Name Server.

Trojan.Win32.DNSChanger.AI

A forensic investigator analyzed one of the infected computer in which PayPal-2.5.200-MSWin32-x86-2005.Exe was installed on the computer because a user opened an email attachment without checking the integrity and md5 hashes of software which he wanted to install and the moment software got installed, a Trojan called DNSChanger was installed in the backdoor and it was programmed to change the DNS server of victim computer which was a rogue DNS server. Investigation reveals the registry entry which got infected and changed because of this Trojan.



The registry entry gets modified when DNSChanger Trojan gets installed in backdoor and essentially it affects "Name-Server" registry key which is responsible for searching domain name server and a user gets redirected to rogue DNS if a Trojan changes the entries into malicious and rogue Domain Name Server IP Address.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\Name of Interface (random)

Local machine registry consists of TCP/IP parameters which shows all interfaces present on the victim's computer and network adapters which are installed on the system.

Registry location which is affected because of DNSChanger.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{22C4D235-5687-435D-AE5F-AFFC6733BFDE} details:

DHCP name: dynamic host configuration protocol which has been assigned by Internet service provider DHCP server.

DHCP IP Address: DHCP IP address which has been assigned by DHCP server.

Name Server: This is the core key which plays an important role while infecting victim's computer at the time of DNSChanger Trojan attack.

According to the Microsoft comprehensive case study on DNSChanger it was observed that:

1. If br.exe file is present then victim has been infected with DNSChanger.
2. DNS settings have been changed then you are infected with DNSChanger.
3. BAT/DNSChanger can be bonded with an application and once installed it produces two files in the temp folder, which you can check it by:
Start->run.>%temp%

If these two files are present then you are infected with this Trojan.

1. Blackr~1.exe - the accompanying application
2. br.exe - detected as Trojan: BAT/DNSChanger.

At the time of DNSChanger attack NameServer key would be replaced with a rogue DNS server IP address and this IP address would be encrypted so that victim won't be able to understand once he tries to examine the registry as well but this encrypted IP address can be easily decrypted and rogue IP address can be determined

This malware has a negative impact such as If a rogue DNS server would be turned off then victims which are infected with this malware, would not be able to access internet as well and once you are infected with DNSChanger, it infects the hard-disk sector as well therefore it might be the case where you need to install the operating system again although some of companies have released anti-malware tool-kit to clean DNSChanger malware. Some of DNSChanger malware have even stolen the keystrokes and redirected the users to advertisement based websites to make money but if you are infected with this malware, lot of anti-virus companies like trend-micro, Norton, McAfee, Microsoft have released their anti-malware toolkit which would check the registry entry and remove the unexpected entry and DNSChanger malware as well and McAfee stinger anti-malware toolkit which removes the DNSChanger Trojan tries to identify infected files and if found, it removes them:

1. FakeAlert-KS.gen.aw
2. FakeAlert-KS.gen.ax
3. FakeAlert-PJ.gen.bs
4. FakeAlert-SecurityTool.ex
5. FakeAlert-SecurityTool.ey
6. Generic BackDoor.abh
7. Generic BackDoor.abi
8. Generic BackDoor.abj
9. Generic BackDoor.abk
10. Generic BackDoor.abl

Similarly trend micro has released the advanced tool to remove Trojan DNSChanger files which are generated at the time of attack.

It was suggested by top most vendors (Norton, Microsoft, McAfee, Trend micro,) that a user can avoid BAT/DNSChanger Trojan if he has taken proper measures to defend this Trojan.

1. Enable a firewall on your computer.
2. Get the latest computer updates for all your installed software.
3. Use up-to-date antivirus software.
4. Limit user privileges on the computer.
5. Avoid downloading pirated software.
6. Protect yourself against social engineering attacks.
8. Do not open unsolicited emails.
9. Perform the necessary steps and identify if DNSChanger is installed and remove the temporary files and run the anti-malware toolkit if required.

References:

<http://guides.yoosecurity.com/how-to-remove-trojanw32dn-schanger-without-affecting-network-traffic/> <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan:BAT/Dnschanger.B>

Author Bio

Praveen Parihar is an information security enthusiast, having 2 years of experience in this field. The author is an RHCE, CEH, CCNA certified professional along with having a rich experience in vulnerability assessment. At present Praveen is working as an Information Security Auditor at Aneja Associates, Mumbai (India).

A person is holding a large, solid blue rectangular sign in front of their face. The sign features the text "cyber gates" in a white, stylized, serif font. The person is wearing a black long-sleeved shirt and dark blue jeans. Their hands are visible at the top and bottom edges of the sign, holding it in place. The background is plain white.

cyber
gates

HOW TO - THE BLACK BAG ACQUISITION Part 1

DAVID SCHIPPERS, EnCE, Network+, A+

<https://twitter.com/DASchippers>

This is the first part of a two-part article series, covering the planning, onsite operations, and field acquisition steps. The second part of this two-part article will cover the offsite/lab acquisition steps to complete the acquisition process.

In the field of digital forensics, there are different types of investigations. Many people think of police or government investigations when digital forensics is mentioned. A large number of situations in the private sector require digital forensics investigations. Divorce cases, fraud, misuse of company resources, and pornography in the workplace are some examples of reasons in which a digital forensics examiner may be called in to perform an investigation.

Some investigations are conducted during the business day. In other cases, the business owner or a spouse may require an investigator to operate covertly. Covert acquisition of human intelligence is commonly referred to as a “Black Bag” operation. Black Bag operations offer some of the most challenging and difficult situations for evidence acquisitions. Securing evidence in a covert and secretive manner can be very dangerous and challenging for the unprepared investigator.

To be successful at Black Bag investigations/acquisitions, investigators should:

- Plan out the operation carefully
- Maintain appropriate security
- Follow a specific set of steps
- Have a well-designed and tested kit(s)
- Conduct onsite forensic acquisition steps
- Conduct offsite forensic acquisitions steps

One of the first things that the examiner should do is plan out the operation. Pre-planning is where one will begin a successful evidence acquisition. The examiner should gather as much information as possible, concerning the environment and acquisition source(s) (e.g. the type of equipment; sizes of hard drives; normal state of the equipment –running or turned off at the expected time of acquisition; expected quantity of equipment to be acquired). With this information, the

investigator can customize his or her field kit to contain any additional equipment needed for the specific job. Most of this discussion will presume a computer or equipment must be left. But, if one is seizing equipment, onsite acquisition timeframes are obviously different from that which is discussed, below. It will, also, predicate the ability to transport the quantity of seized equipment.



Figure 1- Field Kit Sample 1 - Tools

There are plenty of digital forensics field kit descriptions. Instead of duplicating them here, this author would recommend finding a solid forensics book. An examiner's field kit contains some very important items, categories of which are, but not limited to, all possible connectors for drive duplication; extensive tool sets; and non-cell encrypted walkie-talkie sets. Forensic duplicators and write-blockers are more examples of absolute necessities for acquisitions. For redundancy, it is wise to have duplicates of each type of equipment (Failure of high-demand equipment is extremely problematic in Black Bag acquisitions). Another critical, pre-acquisition decision point is determining the amount of forensic duplicators and write-blockers that will be needed, based off of the acquisition request. If one needs to create forensic copies of multiple-terabyte drives, a simple forensic duplicator will probably not suffice. Forensic duplicators publish their copy speeds. The examiner should utilize these in calculations to determine the amount of time the duplicator will need to create a copy. Similarly, write-blockers utilized for acquisitions on a host computer will run at USB version speeds. One should calculate the anticipated time to acquire the suspect machines. If the examiner's equipment does not provide the ability to perform acquisitions in the timeframe required, he or she might need faster or more equipment to copy multiple suspect machines simultaneously.



Figure 2 - Field Kit Sample 2 – Connectors & Miscellaneous

This author's recommendation would be to ensure all acquisition equipment has been tested and verified as forensically sound. Brand new equipment can fail, especially if one has never tested it to ensure it is working and operating in a forensically sound fashion. The last thing one needs on a Black Bag operation is to leave for more equipment. Time is of the essence. The purpose is to acquire evidence, as quickly as possible, in a forensically sound manner. Testing equipment on a Black Bag operation is a sure-fire way to entertain failure.

Another component of the planning process is to carefully review the acquisition request. There are many legal implications in digital forensics. It is imperative that the examiner completely understands the request and ensures legal compliance in performing the request. Some government agencies require special licensing and credentials to perform acquisitions and examinations. It is essential that one is operating within the legal requirements. In particular, the examiner needs to clearly understand the legal implications for the country, state or locality in which the operation will occur. Some requests are private requests that may not be focused on legal action, but are still governed by laws and governmental requirements. Many lawyers are unaware of specific conditions and requirements with which digital forensics investigators must comply. In every investigation that this author participates, he assumes every action will be scrutinized by a court of law. Many clients do not intend to enter into legal action, initially. Their intentions can quickly change, depending on the findings. It is best to assume one's work will always be submitted as evidence in a trial or court proceeding and is still subject to legal requirements.

One area that needs vigilance is security and safety during the Black Bag operation. Even if one is physically capable of stopping someone from impeding the investigation, one should not be providing security and conducting an acquisition simultaneously. If the need is anticipated, another safety and security-focused person should participate in the operation. They should operate as a lookout and provide security, while the examiner acquires evidence. Based off of planning, one should determine the best location to monitor personnel safety and prevent unwanted intruders from interfering in the acquisition. The last thing one needs is for the suspect to appear during the acquisition process. Suspects can destroy equipment, impede focus, disrupt the process and cost credibility in legal proceedings if they cause a break in the forensically sound process. More importantly, intruders can hurt or kill an examiner. If they are being investigated, people can go insane with rage. When this happens, things get serious very quickly. To assume any investigation is not capable of violence is a massive miscalculation. One must be prepared and safe at all times.

In addition to security, it might behoove one to contact local law enforcement. Black Bag operations happen at odd hours, which may be interpreted as theft or burglary by local law enforcement. Notification to law enforcement may preclude time delays or temporary imprisonment.

On the flip side, it is wise to provide as few details as possible to law enforcement. If one were investigating the friend of a local police officer, it would not be wise to provide that name to law enforcement. As much as law enforcement is supposed to be ethical and trustworthy, there are always bad apples in every bunch. It is best to provide the address of the acquisition and have a written request or email request available, if necessary. The exact name of an employee or person should not be necessary for law enforcement. If they are especially inquisitive about the operation, it might indicate a personal interest, which should raise red flags. If they have an undercover operation somewhere, they may inquire about the investigation more. Strange interest by law enforcement should prompt extreme caution while handling acquisitions.

With pre-planning addressed, one can move into the actual Black Bag operation. It is always wise to ensure the site of the acquisition appears to be in normal status. Someone wor-

king late, or other strange variances could indicate that the suspect of the investigation was somehow tipped off about the investigation. If things are normal, entry with a provided key or access method is best. The first course of action for the acquisition is safety. The facility should not hold any massive activity surprises. If things are proceeding in an acceptable manner, safety and security should be the number one priority. During this phase, non-cell network walkie-talkies on an encrypted channel should be utilized to communicate between the acquisition and security team members. This allows teams to communicate when and where cell networks are down or unavailable. It also allows privacy from prying ears.

Once safety and security are handled, location and identification of suspect equipment is the next concern. The scene should be photographed and observed. It is imperative to note any peculiarities and oddities in and around the suspect devices. These clues may later help provide possible passwords for encrypted files or volumes. Equipment connections and setup should be documented thoroughly as part of the acquisition process. Removable media, USB drives and CD/DVD drives, connected or inserted in the equipment should be documented and acquired, if necessary.

After gathering key data about the scene, one should take a moment and decide on a specific course of action. If it is a computer, how will one gain access to the drive to be copied? Is the computer on, and does one need to acquire the memory contents before acquiring the hard drive? Before acting, one should take notes on intended actions and in what logical order they will be performed. This will help ensure documentation of the process that one uses and actually follows, during this process (Remember, time is of essence, but so are accuracy and sound forensic practices).

The next steps depend upon the acquisition request. Some clients want the computer or device pulled from use. This is a seizure procedure and will not be addressed in this article. For this example, one assumes the client wants the device copied and left in use. This is very common in private Black Bag operations. It is imperative that the suspect remains unaware that an investigation has been started. This situation requires both speed and precision.

The examiner should open the computer and remove the hard drive, taking photographs of the inside of the case and connections, in order to reconnect everything back to working order. Before opening the case, one reviews it for oddities and potential traps. There have been situations where private computers have been booby-trapped to destroy components and drives. At the least, one should inspect the case to ensure it has not been altered with intent to harm the examiner during opening.

With the hard drive disconnected, one should power on the computer and verify the boot sequence and date/time of the BIOS. The examiner should document all CMOS settings by photographing all of the screens (This is assuming drive acquisition from a PC). Below is a sample photograph.



Figure 3 - CMOS Example From Suspect Computer

One must be sure to document and/or photograph configurations of hard drives and settings, remaining aware that, even if one is duplicating the drives, this is part of the acquisition. So, it is imperative that this be completed with the source computer(s). Sometimes, minutes or seconds are critical in an investigation. The only way to know exactly the time differentials is to obtain time and date information and configuration information on the actual source computers.

Once the hard drive is removed, the drive specifications and serial numbers should be photographed and recorded. The photographs should clearly show all drive information and pin configuration. If the drive is small and can be acquired in the time allotted, one can begin an acquisition with a write-blocker. If it is a large drive, a forensic duplicator is the best option. These provide a much quicker duplication than a write-blocker acquisition.

To duplicate a drive, one connects the drive to the forensic duplicator's source input, then, connects the target drive to the duplicator's output. Each forensic duplicator can operate a little differently. This is the importance of using and testing the equipment before field use. The examiner will be stressed during a Black Bag acquisition. It is best to know the process and follow a checklist to stay forensically sound. The photograph below illustrates a Tableau forensic duplicator, connected and ready.



Figure 4 - TABLEAU Forensic Duplicator

Another suggestion is to label drives upon removal from the suspect computer. This will help the examiner stay organized. The last thing needed on a black bag investigation is to confuse the suspect's source drive and the examiner's destination drive. (Note: One should log the destination drive in field notes before leaving to perform the Black Bag operation. This is another way to identify drives, if one gets confused.)

The examiner should gather MD5 & SHA1 hashes of each duplicated drive, ensuring that they are forensically sound duplicates. If the forensic duplicator displays source and destination drive hashes, photograph the display screen with the equipment connected. This is a great way to prove that an exact copy was created.

With the drive duplicated, one can then tag it and secure it in field storage cases. The forensic duplicator allows one to place the original drive back into the suspect's computer and leave. This is critical to leaving a Black Bag investigation quickly. One, also, needs a duplicate of the original drive left in a perfect forensic state. This allows acquisition and, if the acquisition file is corrupted or an error occurs, one can re-acquire the drive. This is absolutely critical from a recovery perspective.

With the duplication complete, the examiner can re-assemble the suspect computer(s), then, test the computers to ensure they boot and start up. If the computers are inoperable, it may tip off the suspect that an investigation is in progress. After completing final field checks and removing all traces of one's presence at the scene, one should, now, ensure all of the field acquisition steps have been completed and then return to the lab.



LTEC LAWTECH EUROPE CONGRESS 2012

Electronic Evidence Computer Forensics Legal Technology

November 12th, 2012
Clarion Congress Hotel, Prague
Czech Republic

HOW TO - THE BLACK BAG ACQUISITION Part 2

DAVID SCHIPPERS, EnCE, Network+, A+
<https://twitter.com/DASchippers>

In the first part of this two part series, this author introduced some key concepts for Black Bag acquisitions. Black Bag acquisitions offer some of the most challenging and difficult situations for evidence acquisitions. Securing evidence in a covert and secretive manner can be very dangerous and challenging for the unprepared investigator.

To be successful at Black Bag investigations/acquisitions, investigators should:

- Plan out the operation carefully
- Maintain appropriate security
- Follow a specific set of steps
- Have well a designed and tested kit
- Conduct onsite forensic acquisition steps
- Conduct offsite forensic acquisitions steps

In the first part of this series, this author covered the planning, security and field steps for acquisitions. This article will pick up from where the field operations completed. At this point, the examiner has a forensically duplicated hard drive, CMOS information, documented setup and diagrammed connections for the suspect computer(s) (For more detailed information, please, read the first part of this series: "How To - The Black Bag Acquisition Part 1.")

Before continuing with the acquisition steps, it is important to stress the legal requirements and implications of forensics work. As mentioned in the previous article, it is not uncommon for lawyers and private organizations that request digital forensics investigations to misunderstand or be unaware of the legal requirements for the country, state, or locality in which the

operation occurs. It is imperative that the examiner is versed and knowledgeable about all legal requirements and aspects on the digital forensics investigation being conducted.

Once in the lab, the duplicate drive should be tagged and inventoried. Once the acquisition is done, one needs to have a documented chain of custody and storage in combination safe or a secure, access-controlled area. It is advisable to have tightly restricted access with documentation on what date and time authorized personnel had access to the forensic copy of the suspect drive. If one stores evidence in a safe where with exclusive access to the drives, one tightly controls the access.

At this point, this author will cover the acquisition of the drive. First, the examiner connects the drive to a write-blocker and ensures the write-blocker is in a write-blocking status. The photograph in Figure 1 illustrates a drive connected to a Tableau write-blocker. The indicator lights are illustrating that the device is in write-block status.



Figure 1 – TABLEAU Write Blocker In Write Block Status

After the drive is connected to the host computer, the examiner will need to acquire the drive through forensic software. Guidance Software's EnCase version 6 will be used to illustrate this example.

After creating a new case, one selects Add Device (Figure 2).

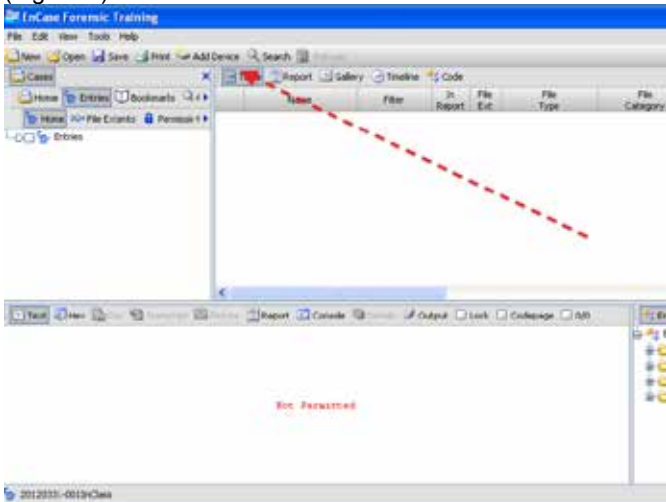


Figure 2 – EnCase – Main Screen

In this step, Local Drives option, then, Next are selected in that order (Figure 3).

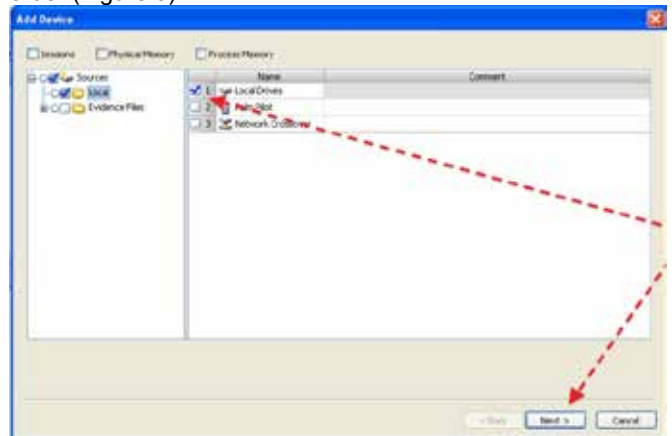


Figure 3 – EnCase – Add Device

In Figure 4, one verifies that the description and displayed sectors match the drive to be acquired, then, selects that drive. (Note: Some drives have Host Protected Areas (HPA) and other hidden areas. The examiner should have checked for the presence of an HPA and accounted for such in sectors calculation.)



Figure 4 – EnCase – Choose Devices

Selecting Next advances the process (Figure 5).

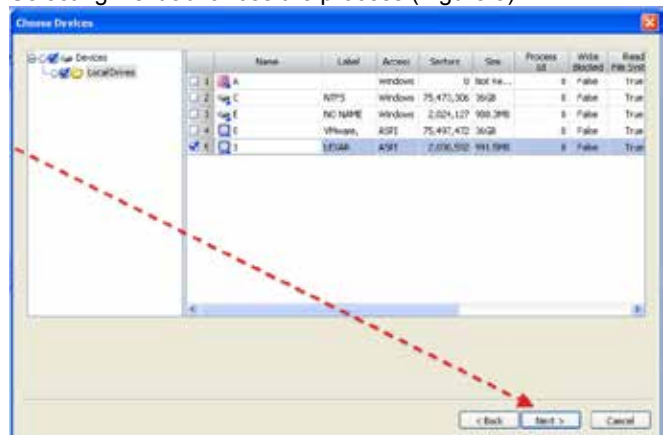


Figure 5 – EnCase – Choose Devices

Selecting Finish in the subsequent window completes this part of the process (Figure 6).



Figure 6 – EnCase – Preview Devices

At this point, Preview Mode is displayed. There is a small triangle in the bottom right of the drive symbol, indicating Preview Mode (Figure 7).

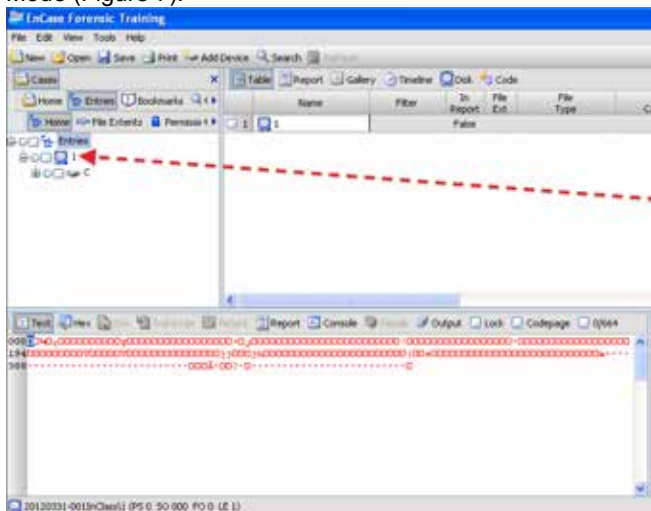


Figure 7 – EnCase – Source Drive in Preview

In this step, a Right Click on the drive icon brings up the context menu, and Acquire is selected (Figure 8).

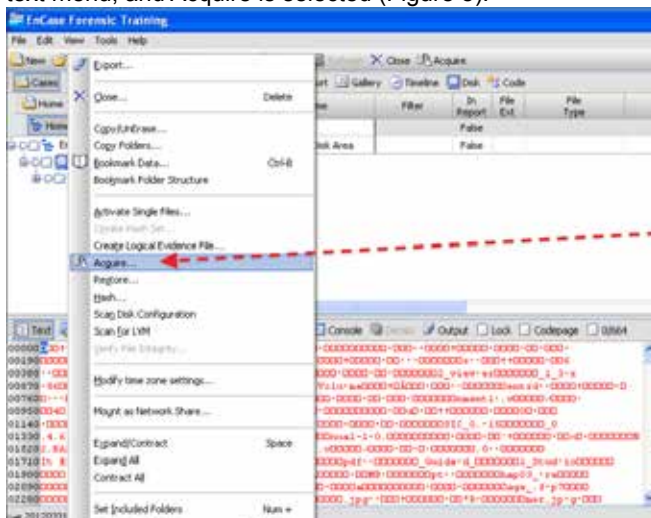


Figure 8 – EnCase – Begin Software Acquisition

One selects the Appropriate settings (most often Replace source drive and check Acquire another disk with more disks to acquire), then, selects Next (Figure 9).

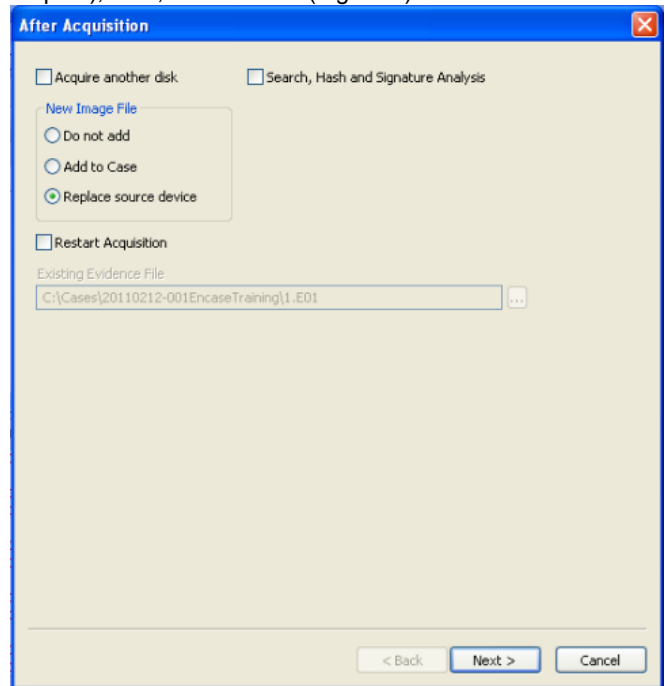


Figure 9 – EnCase – After Acquisition Options

On the following screen, one enters Name, Case Number, Notes, Compression Type (none, unless necessary) and Output Path, then, selects Next (Figure 10).

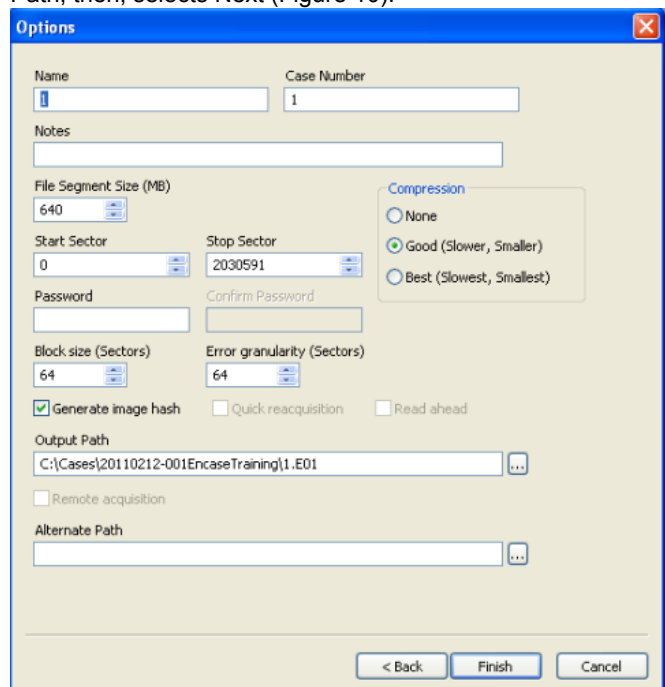


Figure 10 – EnCase – Case Options

As the drive is being acquired, time estimates will be displayed (Figure 11).

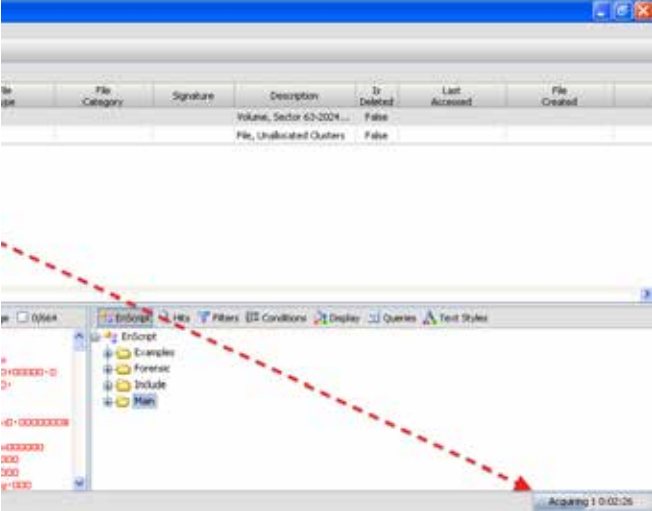


Figure 11 – EnCase – Acquisition Information

After the acquisition completes, an Acquire window is displayed. Then, the Acquisition Hash information should be compared to the hashes obtained during forensic duplication. If they do not match, there is a critical issue. The hashes should be exact matches, illustrating a forensically sound copy. One selects Note and then OK (Figure 12).

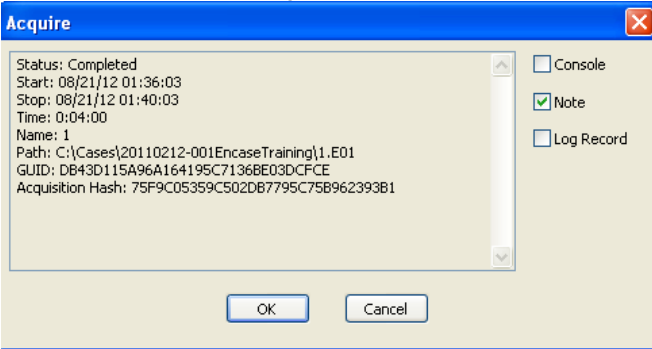


Figure 12

At this point, the examiner can begin searching the acquired drive based on client-provided parameters. If re-acquisition is required and selected, the software will prompt one through the process, again.

A digital forensic investigator will likely receive a request to perform a Black Bag operation/acquisition, at some point. The considerations and steps provided in these articles are intended as guidelines. Each specific situation can pose significant challenges and issues. The situation provided here was a simple straightforward Black Bag acquisition. Planning and information gathering before the actual acquisition are essential in a successful Black Bag operation. Planning helps ensure field kits are properly equipped and processes are correctly implemented.

Finally, the safety of the examiner and the rest of the team should be of the utmost importance. It cannot be stressed enough that even simple Black Bag operations can go sour quickly. If this happens, a security minded approach will pay off immensely.

Author bio —————
David Schippers is a Certified Forensic Examiner with EnCase (EnCE) from Guidance Software. David completed an associate's degree in Network Administration from Grand Rapids Community College and a bachelor's degree in Information Security and Intelligence with a specialization in digital forensics from Ferris State University. He is currently finishing a master's degree in Information Systems Management from Ferris State University and holds Network+ and A+ certifications. He has been involved in forensic and malware responses in educational and private environments. David, also, continues research and testing on the utilization of metadata associated with image file formats.



SAM File Forensics: Windows Password audit

PRAVEEN PARIHAR

Windows has become a most vulnerable platform for all the Technogeeks. Most of the tools are available online which can be used by an attacker to crack windows password and It's not a rocket science for an attacker to crack windows password Event if a person does not have a physical access on the system. When it comes to understand the logic behind windows password and encryption it becomes difficult to understand what exactly happened which made an attacker capable of cracking password.

Here we will explain the truth inside password hashing and how an attacker can get the access on a target windows computer.

When a windows user sets a particular password then it is converted into related hashes and then it is encrypted and stored in a file which is called **Security Account Manager (SAM)** which is located at following location:

C:\Windows\System32\config

It's a well known fact that SAM file is in use while an operating system is used and It is locked therefore One can never access it while running windows itself because when operating system is loaded then It is locked and made available to kernel.

Then you must be thinking how come an attacker gets access to SAM (Security Account Manager) file which consists of user account and passwords because these hashes are one way encryption which cannot be decrypted. In this case attacker converts the equivalent words into hashes and it's compared with the hashes stored in the SAM file and if the hash matches then Attacker is able to bypass windows password authentication similarly attacker can use different techniques by which he can even get a copy of SAM File or he can dump the SAM

file and passwords which are inside SAM file and later on It can be decrypted using different softwares like L0phtcrack & Cain & Abel etc. because windows is using LM hashes and NTLM hashes for password authentication and latest version of NTLM v2 has been launched for enhanced security and which can also be cracked using different softwares available in the market. As intent of writing such article is that whenever a windows system is compromised then it can use different methods to bypass security authentication, we will try to map these incidents with SAM file and try to make sure that SAM file is not dumped and difficult to bypass windows system.

Although we have different incidents in which we use different method of bypassing such as dictionary based attack, Brute force attack and which can be performed using Ophcrack, Windows NT password recovery, ERD Commander, Samdump, chntpw etc and these tools would be using rainbow tables to compare those hashes and converting them in plain text or these tool can dump a SAM file and later on they can dump the password using pwdump (version2 & 3) although these methods have become really popular and used by an attacker but if user creates additional encryption using Syskey which is

an additional feature of windows password authentication to provide an additional layer of security which can be enabled by an attacker using:

Start->run-> type Syskey update



It further provides an encryption for SAM file so that it cannot be accessed directly and even by using such tools which we have mentioned, would not be able to bypass this mechanism of Syskey encryption.

Here we will be showing you how we can dump a SAM file even if we cannot access this file while an operating system has been started and for that purpose we will be using pwdump and this tool would be able to dump LM hashes for respective account and later on these hashes can be cracked using L0phtcrack, Rainbow crack, Cain & Abel and lots of on-line tools which can break the LM Hashes and It can be obtained in a plain text and the information extracted from SAM file and pwdump usage have been shown:



No history available

Administrator: 500: NO PASSWORD***: NO PASSWORD*****.**

ASPNET: 1004: NO PASSWORD***:59829CF6815A3124E94D1D8E3D9FB292:**

Guest: 501: NO PASSWORD***: NO PASSWORD*****.**

Praveen: 1000: NO PASSWORD***:A5B-1C4398302B25C03F44AF7FEBEB7EC:::**

__vmware_user__:1002: NO PASSWORD***:FAA4DD37DBADA3DEA24BAF51FB-DE6DE6:::**

Completed. LM hashes extracted

This output has been extracted from SAM(Security Account Manager) which illustrates that there are three users including VMware user while extracting password:

Administrator: 500(UID) and password hashes could not be extracted.

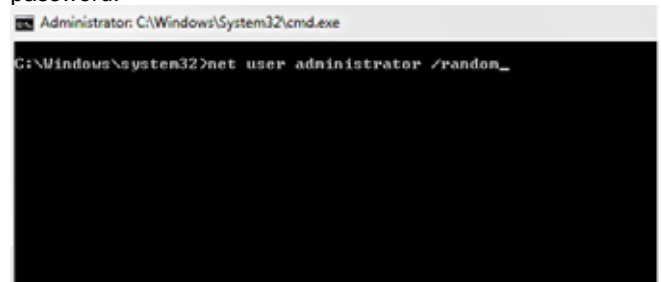
Praveen: 1000(Non-admin) and LM hashes could be extracted.

VMware User: 1002(Non-admin) LM hashes could be extracted.

Similarly one can use Samdump2 tool which is embedded in backtrack by default, can be used to crack windows hashes and later on it can be decrypted using John the ripper, L0pht-crack, Cain & Abel etc.

Intent of showing the entire demonstration from forensics perspective was to examine SAM file and Its hashes at the time of attack if investigator is not able to bypass the system and then only he can complete his forensic investigation.

Similarly If a Forensic investigator is able to get the administrative privilege but he is not aware of previous windows password then he can use this feature of command prompt which randomly generates a password without asking old password:



One more interesting thing can be analyzed by an Investigator was to find out hidden accounts in the system which could have created to launch a successful attack.

Net user gives all the users present on the system and once we get to know the user It can be enabled using following commands:

net user Praveen /active: yes

net user Praveen /active: no

It has become really easy for a forensics analyst to bypass these security measures and analyze the victim's computer and dump the SAM file and trace the footprints of an attacker.

Enhanced Security Used by Security Analyst to make sure that It is not cracked easily:

1. Enable power on password
2. Enable BIOS password
3. Enable Syskey password
4. Choose latest operating system windows 7 (updated)/Windows 8 If possible
5. Choose strong password more than 15 characters.

Latest operating system has been suggested because of NTLM V2 version which is using Salted encryption and while choosing passwords make sure that it should contain special characters and strength of password should be more than 15 which become difficult to crack and bypass the system.

Hey readers just keep reading eForensics Magazine there are lot of cool stuffs to come-up in the next versions such as Case study of Truecrypt decryption by FBI and lot of other stuffs as well.

Author bio

Praveen Parihar is an Information Security Enthusiastic and having 2 years of Experience in this field and author is RHCE,-CEH,CCNA certified professional along with this author has a rich experience in Vulnerability assessment and At present Praveen is working as Information Security Auditor at Aneja Associates, Mumbai (India)



Join

eForensics Magazine team!



eForensics Magazine is looking for regular contributors. If you want to be a part of the first magazine devoted to penetration testing, now's your chance to join us. We especially need:

- news contributors – send in a piece of news of an interest for a pentester and make your own comment on it.
- “point of view” section writers – short articles (800 words tops) with you discussing an issue you think should be discussed.
- “vulnerability check” writers – what a pentester can use in his work.
- reviewers – found an interesting tool? Review it for us.
- betatesters – read an article before it's published in the magazine and share your opinion on it with us.

Regular contributors are given free subscription to the magazine and – if they represent companies – free advertising in the mag. And, of course, an earned mention in the magazine.

Worth it? Ask for details:

maciej.kozuszek@software.com.pl

PANNONE

CYBER CRIME LAWYERS

Pannone are one of the first UK firms to recognise the need for specialist cyber crime advice. We can both defend and prosecute matters on behalf of private individuals and corporate bodies.

We are able to examine material or secure evidence in-situ and will then represent your needs at every step of the way.

Our team has a wealth of experience in this growing area and are able to give discrete, specialist advice.

Please contact David Cook on

0161 909 3000

for a discussion in confidence or email

david.cook@pannone.co.uk

www.pannone.com

ENCRYPTING YOUR PACKETS

DONALD CINCO

What is Encryption?

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

The result of the process is encrypted information (in cryptography, referred to as cipher text). The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption in many contexts, the word encryption may also implicitly refer to the reverse process, and decryption e.g. “software for encryption” can typically also perform decryption. Encryption has long been used by militaries and governments to facilitate secret communication.

Encrypting such files at rest helps protect them, should physical security measures fail. Nowadays it's being used all around us; in ATM cards, on ecommerce websites, in game consoles, for the distribution of copyrighted music and film and many more applications. This is all possible due to the rise of the computer and readily available gross amounts of computing-power (<https://en.wikipedia.org/wiki/Encryption>).

There are literally thousands of ways to intercept data. The Internet is probably the most dangerous place for your data when concerned with privacy. If you don't use an encrypted connection with the server, pretty much anybody can get their hands on your full communication. People in your local network, your Internet provider, the host of the web-site you're visiting, etc.

So, how can we be safe and secure our privacy from work, Internet cafe's, hotels, hotspots etc.? Simple! By using encryption readily available in the Internet and the best part, it is FREE!!!

Before we begin installing any software to encrypt our data we need to understand why we need to secure our data in our network and in the Internet. First, I am going to use a packet

monitoring software called Wireshark if you don't have it you can download it from their main site <http://www.wireshark.org/> it's free.

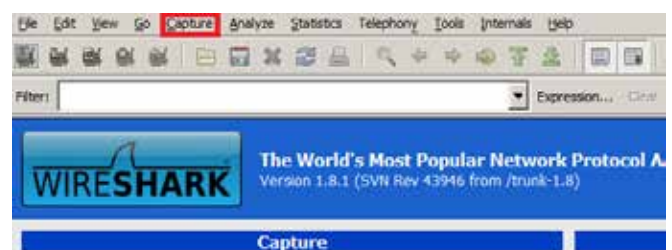


Figure 1

Once you open Wireshark click on the “Capture” then “Interface” then we will need to look for an interface to capture all of the packets coming in and out the network see fig-2

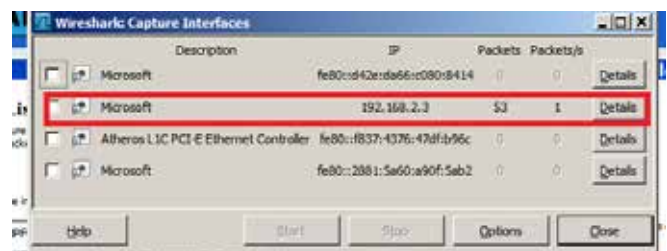


Figure 2

In this image (Fig. 2) I can see one interface has an IP address so I check this box. That's the interface we will use. After the box is checked the Start button will activate. Hit start.

Now I will open my Yahoo Messenger and Sign In. Great! My friend NDF4n6 is online I will send him a message; while I'm sending him a message my packet capture tool is capturing all the packets in my network.

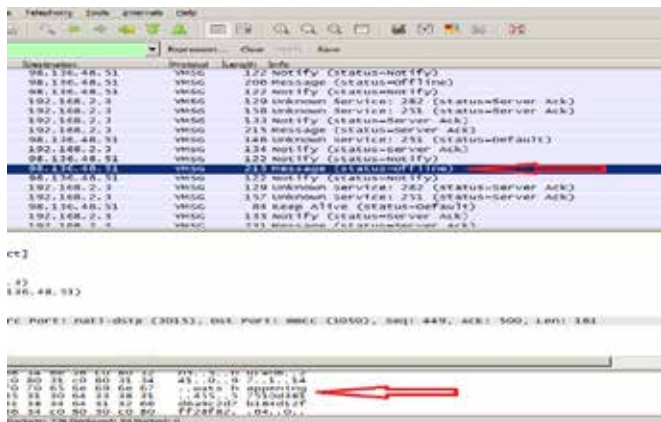


Figure 3

As you can see Wireshark is capturing all conversation in YM and yes Instant Messenger is sending all packets in text format so let's take a look at NDF4n6 reply in Fig. 4.

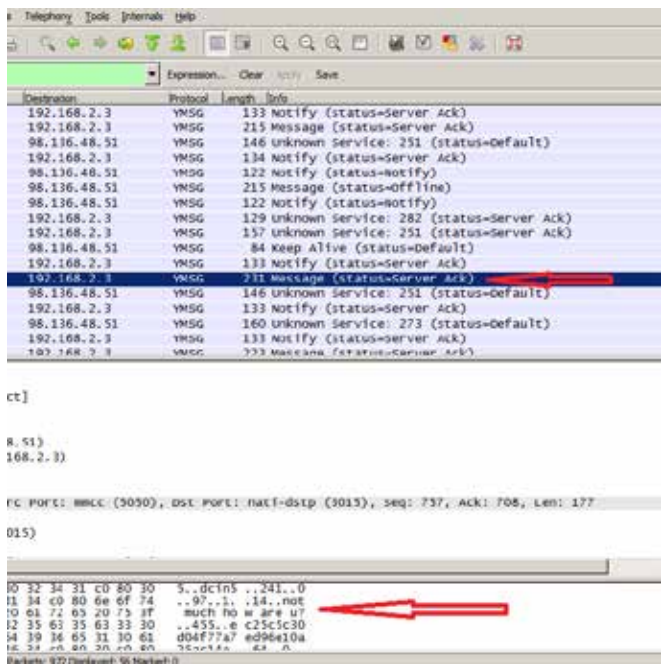


Figure 4



Now let's see if we can find some more important data. See fig. 5.

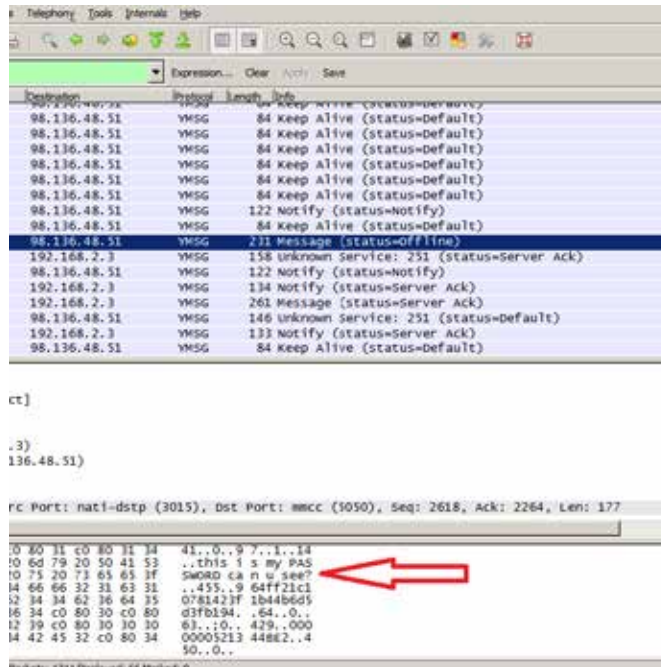


Figure 5

Now, since we see that Wireshark is able to capture the password you sent via YM, it's imperative to understand that using Instant Messenger does not encrypt your data in the network. Anyone who has knowledge of using any packet analyzer can easily capture your sensitive information.

So how can we protect our data in our network? We can protect our data in the network using various plug-ins and avoid using YM, IAM, Gtalk, MSN etc. There are other open source chatting software substitutes for instant messenger like Miranda, Torchat and Pidgin. In this case we will be using Pidgin you can download it here <http://pidgin.im> Pidgin is a universal chat client so you can always stay in touch with your friends and family even if they are using other chat clients. Ok, I assume you would like to be more secure and you just downloaded and installed pidgin. Now we need a plug-in called **Off-the-Record Messaging** (OTR) what is OTR? <http://www.cypherpunks.ca/otr/>

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

Encryption

No one else can read your instant messages.

Authentication

You are assured the correspondent is who you think it is.

Deniability

The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

Perfect forward secrecy

If you lose control of your private keys, no previous conversation is compromised.

So, now we have installed both the Pidgin and OTR now let's configure it.

Open Pidgin

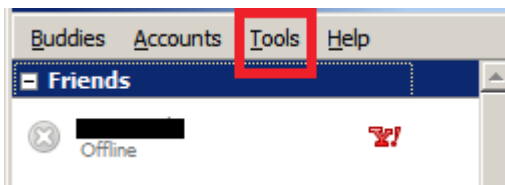


Figure 6

Click on **Tools** and then **Plugins** and look for the **Off The Record Messaging** and check inside the box. And you're done. **Remember both parties must have the same chat client or else it will only be secure one direction.** Now let's see what this baby can do. Let's run Pidgin and hopefully you have already checked the OTR plug-in. I will be communicating again with NDF4n6 but this time we will be using Pidgin. Let's see! I will run my Wireshark and we will see if we can capture both parties' messages in the network.

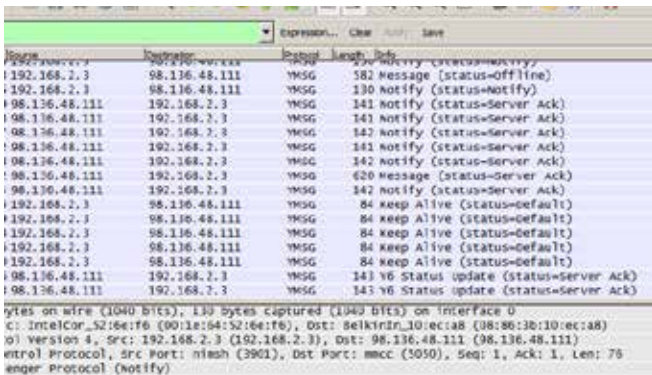


Figure 7

Ok we see NDF4n6 and Dcin5 are online in Fig. 7 we will test and send a message through PIDGIN Universal Messenger with OTR enabled. Let's see if we can send a message securely.

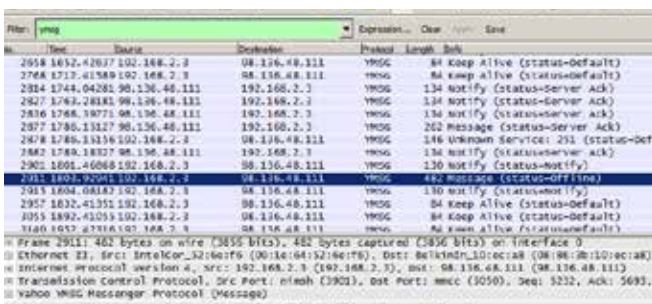


Figure 8

Look Fig. 8 You can see we accomplished sending messages securely without compromising our data in the network. Now if one person is using Pidgin and the other is YM this is what it will look like. One will be compromise while the person who's using Pidgin will stay secure. See Fig. 9

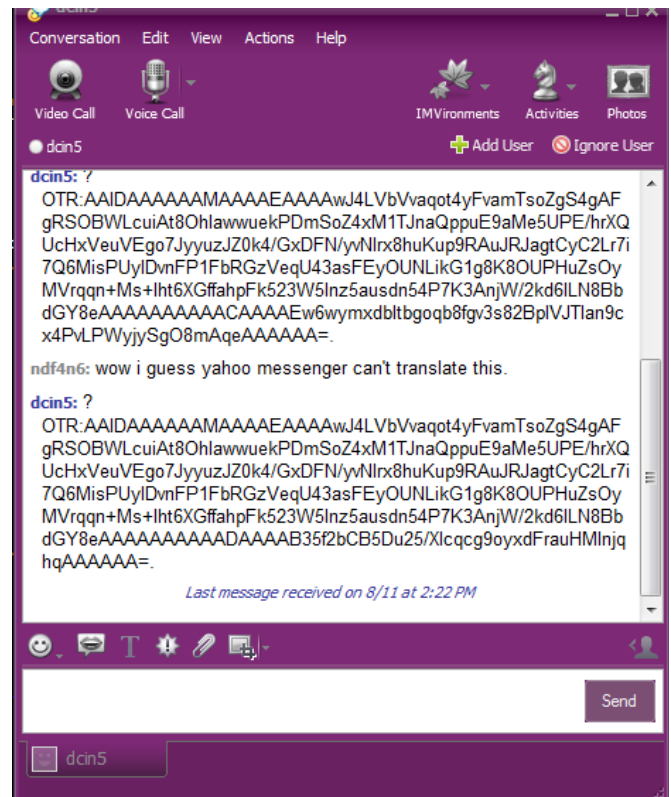


Figure 9

Ok now we accomplished how we secure our I.M. messages but what about securing in the Internet?

Yes, it's definitely very important to secure our password especially if we are logged into a website that doesn't have SSL / https. Many Packet analyzers can capture your login info by going to these websites, let's see how this is done.

Ok, first we need to turn on our Wireshark once again. I hope you already know how to set up your Wireshark packet capturing software, if not go back to fig. 1 and refresh your memory.

Now Wireshark is on and ready to capture everything in our network. Now we will open our browser and go to <http://www.somesite.com>. As you can see we are going to login in a non-secure site, and our password can be compromise. Let's look at fig. 10



Figure 10

I typed my username and passwords in a non-secure site not using https. Now let's see if our packet analyzer can capture our packets.

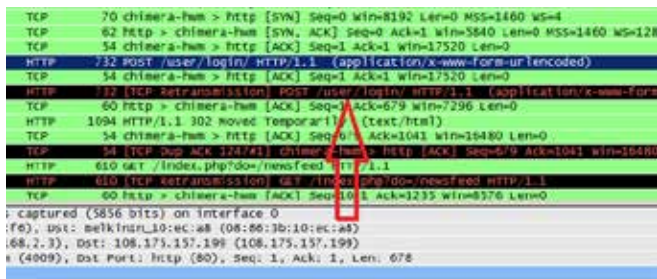


Figure 11

Ok this is what my packet analyzer gave me so what I am looking for is a HTTP filter and then look for the word **POST**. Highlight it and click the **Analyze** tab. Then click **Follow TCP Stream** because it's easier to find what we are looking for in the TCP stream. Let's look at fig. 12 and see what we can find.



Figure 12

There as you can see in Fig. 12 we managed to capture the data and we got the password and username including the cookie session ID. Now, how can we avoid this and make our connection more secure in the network?

It's is simple: using a portable app like **Ultrasurf** for IE (<http://ultrasurf.us>). Because it is portable, there is no need to install this app and you can put it in your USB flash drive if ever you want to carry it with you. For Firefox and Chrome you can use - HTTPS Everywhere - <https://www.eff.org/https-everywhere>). HTTPS Everywhere act differently, remember to look at the product web site.

To check how Ultrasurf product works, go to www.whatsmyip.org and record your IP Address. Now let's run it and your IE browser should open up. Now that your browser is up lets go back to www.whatsmyip.org and check to see if your IP has changed. If it has changed that means you are good to go and ready to surf, below is not my true IP. Ultrasurf works creating a local proxy that FORWARD all the traffic to an Ultrasurf server encrypting it, the Ultrasurf server acts like another proxy forwarding the requests and the responses to/from the target web site. Remember to be careful while using solutions like Ultrasurr because the company that own the product can be able to get all the traffic in the clear text.

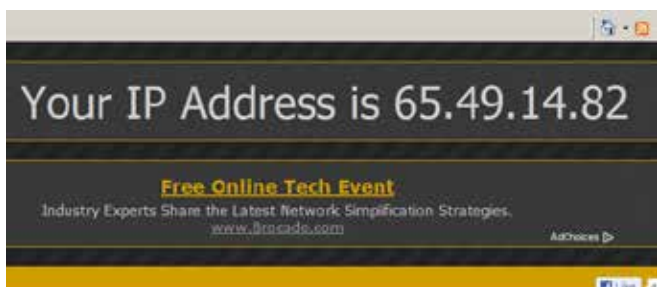


Figure 13

Ok, now I will go back to the same site where I just went earlier and we will fire up the Wireshark for the last time and we will see if we can secure our connection by using Ultrasurf.



Figure 14

Ok I am now in the same site and I will login once again and we will see if our connection is secure even if we are connecting to a non encrypted website (https). After logging in I went to my analyzer and checked to see if I managed to sniff my password in the network.

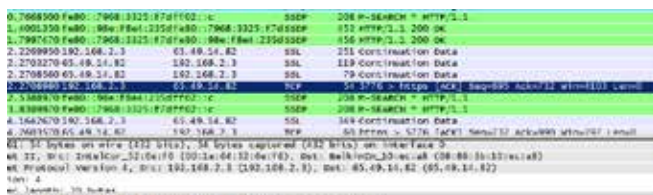


Figure 15

As you can see above in Fig. 15 using Ultrasurf and IE browser the packet analyzer is showing us that we are connected to SSL. Now lets see if we can see anything from the TCP Stream View.

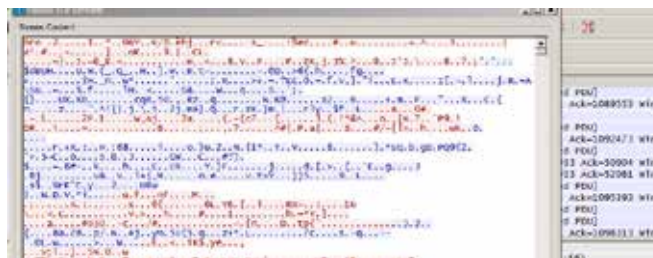


Figure 16

In our Stream content what we can see is that our packets are encrypted and we have a secure connection.

Conclusion

We abide to improve in technology, we made progress in security though we will continually find flaws, and because of humans are the weakest links. In this article it does not mean you are 100% secure, there are many tools out there than can perform SSL stripping technique, but it's also a good practice to secure your communication than nothing at all.

EOF

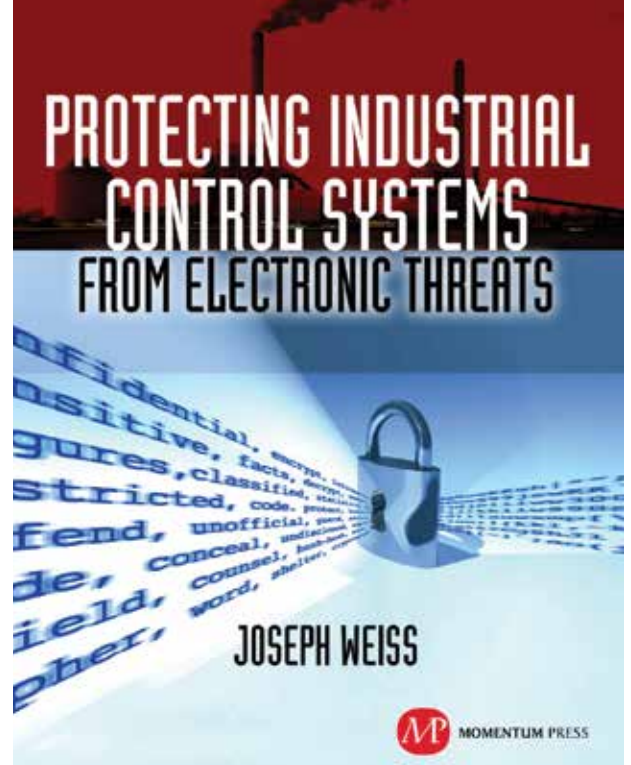
DISCLAIMER: This information is for educational and secure communication practices purposes only. It is illegal in many countries to use sniffing tools on networks you do not own, so be warned, IT IS ENTIRELY YOUR OWN RESPONSIBILITY IF YOU ACT AGAINST THE LAW.

Authors Bio

Donald Cinco is the research and development director for Nevada Digital Forensics and is a licensed pen tester, and holds certifications in Certified Ethical Hacker, Certified Computer Security Analyst, Computer Hacking Forensic Investigator and CompTIA +.

Donald joined NDF with 13 years experience in variety of expertise from computer forensics, malware analysis, website vulnerability assessment and exploit exploration.

His passion and dedication in the I.T and Digital Forensics brings competitiveness in a challenging digital world. <http://www.nvdigitalforensics.com>



For many years, Joe Weiss has been sounding the alarm regarding the potential adverse impact of the ‘law of unintended consequences’ on the evolving convergence between industrial control systems technology and information technology. In this informative book, he makes a strong case regarding the need for situational awareness, analytical thinking, dedicated personnel resources with appropriate training, and technical excellence when attempting to protect industrial process controls and SCADA systems from potential malicious or inadvertent cyber incidents.”

—**DAVE RAHN**, *Registered Professional Engineer, with 35 years experience.*



MOMENTUM PRESS

FOR US ORDERS:

www.momentumpress.net

PHONE 800.689.2432

FOR INTERNATIONAL ORDERS:

McGraw-Hill Professional

www.mcgraw-hill.co.uk

PHONE: 44 (0)1628 502700



ACUMIN

Global Information Risk Management Recruitment

Information Security & Risk Management | Governance & Compliance
Penetration Testing, Forensics & Intrusion Analysis | Technical Security | Business Continuity Management
Sales Engineering | Sales & Marketing | Public Sector Security | Executive Management

Network and/or Application Penetration Tester

Ref: 14951 **Location:** UK wide **Salary:** £25k-£75k base + bonus + package
Job Type: Permanent

Multiple opportunities for Penetration Testers. Varying levels of experience will be considered. You will be offered first rate project exposure as well as on-going training, culminating in superb earning potential.

Key competencies and experience required:

- Use of a variety of network security testing tools and exploits to identify vulnerabilities and recommend corrective action
- Manual penetration testing and a deep understanding of IP networking in a security context
- Deep knowledge of IP networking protocols
- Experience with security testing of Web-based applications
- Intimate knowledge of at least one enterprise development framework
- Proven ability to explain verbally the output of a penetration test to a non-technical client
- Strong inter-personal and communication skills
- Report-writing and presentation skills
- Must be prepared to travel

Desirables:

- Code review skills
- CHECK, CREST or TIGER qualification
- Current UK driving licence

Please email your CV to careers@acumin.co.uk quoting the reference above

Web Application Penetration Tester and Security Specialist

Ref: RF14803 **Location:** South East **Salary package:** £400-£600 per day
Job Type: Contract

This blue chip finance organisation is currently developing its internal information security function, and as such has identified a need for a lead security specialist with a particular focus on web application security.

Responsibilities

- Conduct technical security assessments against strategic initiatives prior to final release in to an operating environment.
- Carry out such tests and assessments against internal standards as well as industry standards such as SAS70 and PCI-DSS.
- Define and execute penetration tests as part of the review lifecycle for infrastructure, applications, and web applications.
- Perform regular vulnerability assessments using scanning tools to ensure the on going security of systems to emerging and known threats.
- Provide expertise in to forensics investigations and incident management as required.
- Identify and manage required resources, creating reusable documentation, processes, and toolsets.

Requirements:

- Strong understanding of technical security principles around penetration testing, vulnerability management, and forensics.
- Knowledge of current assessment techniques and toolsets such as OWASP guidelines, WebInspect and Fortify.
- Prior working experience of industry standards and processes - PCI, ITIL, Prince, COBIT, COSO.
- Demonstrable track record of security design, review, and implementation.

Please email your CV to careers@acumin.co.uk quoting the reference above

A STEP BY STEP DIGITAL FORENSICS PROCESS OF COLLECTING EVIDENCE FROM AN iPHONE


DONOVAN FARROW

Living in today's society, where everyone is using the latest and greatest cell phone. It has become difficult for digital examiners to keep up with the latest technology. Everyday we wake up in the morning, log on to our favorite mobile site to find the birth of a new phone (or maybe that is just me). Not only does this phone have a new shinny design but it also has a new operation system (OS). This is great news for all the techies that lust to have that new phone smell, and enjoy waiting in line for the new phone on a Friday night. However, a digital forensic examiner who's gets such new phones could face some problems. Here are the questions that you will be asking yourself before receiving the phone from client. Does my software support this phone? If not, I wonder if they have an update for it? How am I going to afford ANOTHER mobile seizure kit? I cannot solve all of these questions but I will do my best to help one of the most popular items. In this article I will take you through a step by step digital forensic process of collecting evidence from an iPhone. These steps will help you build a defensible process in order to present your data in court. I have also found a tool that will help you achieve this on a very limited budget.

First thing you should address as a forensics examiner is the chain of custody (COC). A chain of custody is like the biography of the data's you examining. It has a record of the data's birth (Creation of pristine copy). It has the record date if it was cloned by an individual (Creation of a Working Copy). This would also include anytime the data moved from one place to another place (Moved by forensic tech from Evidence Vault). The COC would also include a MD5 Hash value (or a SHA-1) of the data that has been preserved. Another item the COC would contain is the time that an action occurred with the data. An example of this would be someone taking the data from the evidence vault to be analyzed. The COC should be stored in a secure location and only authorized personal should have access to it. Below is an example of a CoC that is used by my company.

Description/Case:			
Manufacture:	Model#	Serial#	

CHAIN OF CUSTODY



Date/Time:	FROM:	TO:	REASON:
	Signature:	Signature:	

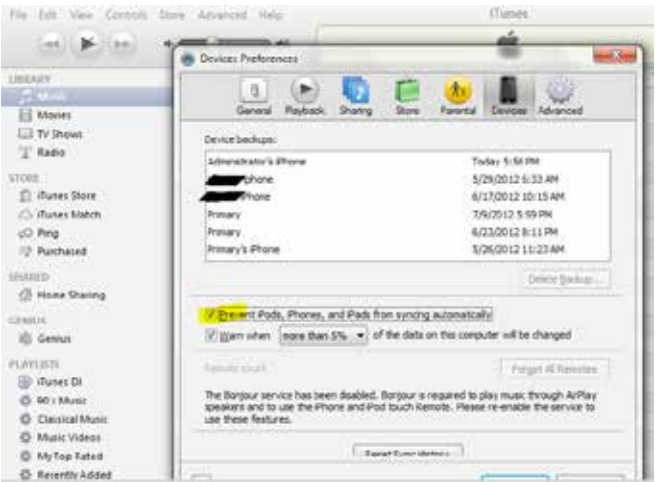
You could always go out, spend some money and have someone build you a customized CoC to fit the specific device in acquisition. However, the example shown above is pretty basic and is very easy for attorneys to understand. It contains a description box for you to indicate case names and a place to sign over digital contents to the new custodian of data. An example of this would be if a client handed an examiner a hard drive the client would record the date and sign contents over to the examiner. This also works the other way. When the examiner hands the hard drive back to the client they must sign it back to client. It is important to note that the COC moves with the digital data. I personally keep a copy for my own records but the original COC stays with the original hard drive. You could always have more details about the product being collected in the CoC but the ones listed in the CoC are attributes you should be able to see just by looking at the phone. The bottom part of the CoC example is the transfer of hands portion. In my opinion it is always important to have the person you are giving an item to sign the CoC during transfer. Remember this data might be presented in court at a later time and this is the last thing you want is counsel picking on you about the CoC. After the CoC is updated let's get to the digital acquisition of the phone.

As stated before we are going to analyze some basic features that are commonly required to be done from an iPhone, but on a very tight budget. Upon retrieval of the phone I would recommend you put the mobile device in a Faraday bag - it is an item that will shield the phone from all telecommunication towers, Wi-Fi, and Bluetooth connections.

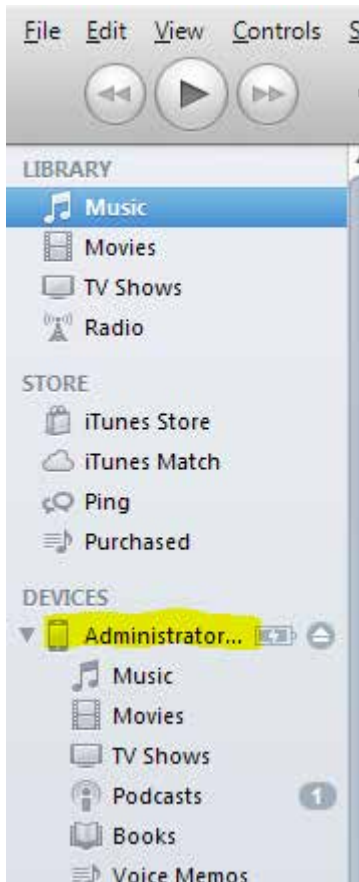
Another way you can perform a seizure of the phone (if it is not password protected) and not allow cellular data to manipulate the phone would be going into settings of the phone. Once in you need to disable Wi-Fi, Bluetooth, and put the phone in Airplane Mode. This will then stop cellular communication, Wi-Fi, and Bluetooth connections with the mobile device. Make sure that if you change these settings you document this in your report.

When phone is back at your lab you have been requested to pull off any text messages, calendar items, pictures, and voicemails. I choose these items because they are the most common ones to be requested from an iPhone.

Before hooking the phone into your examination computer make sure that you have iTunes installed on the machine. This will allow the computer to apply the correct drivers to the device. Once you have installed iTunes on your machine open it up and go to Edit at the top. Once the drop down menu is available, select "preferences" at the bottom of the list. When the window pops up click on the picture of the iPhone called "Devices". This will take you to a screen as show below. It is very important that you have the checkbox below checked. This will allow that phone not to be written over by an older backup that is located on your forensic machine. This is highly important and could ruin your data if you are not careful. I would recommend you get a test phone and see if your machine functions to our desire before plugging in the acquisitioned phone. Also note that performing a backup of the phone will change particular attributes of the phone. This would result in a different MD5 Hash set on the original collection. During this exercise we are examining the backup file from the phone and NOT the phone itself. Make sure you always update your documentation when working through forensic process.

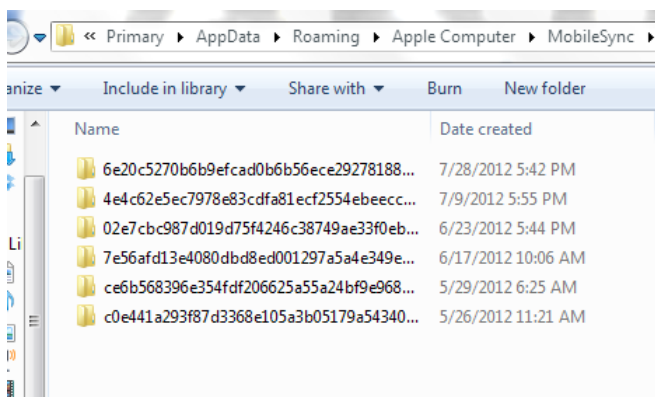


Once you have verified that iPhones are not automatically syncing, you can plug in your acquisitioned iPhone. When you plug in your iPhone you will probably notice that owner of the name appears on the left column under devices.



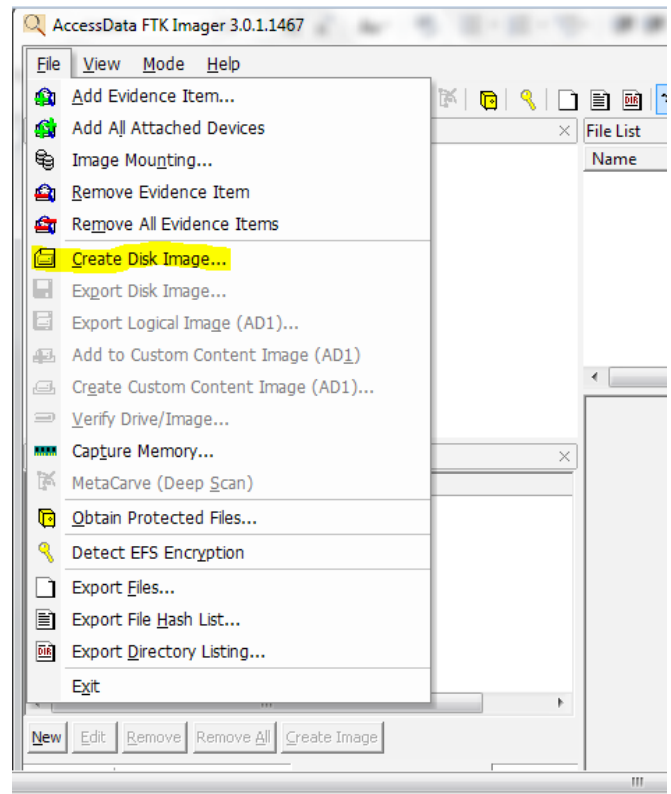
This "owner" of the phone is named Administrator. This naming convention is setup during the first time the phone is plugged into iTunes or if a user restores phone to factory defaults and then attempts to connect to iTunes. Now that you have verified connection of phone right click on the owners name and select "Backup" from the list. A backup will commonly take about 10 to 15 minutes depending on the size of the phone and amount of information on it. Once the phone has backed up successfully you can start your analysis.

Once your mobile device is finished backing up to your computer go to the backup directory. The default directory for back is C:\Users*Username\AppData\Roaming\Apple Computer\MobileSync\Backup. In this directory you may notice multiple folders.

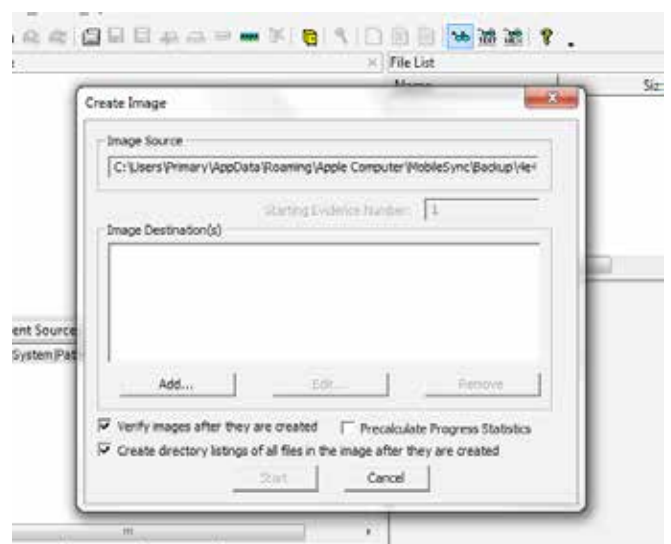


If you look at the created Date attribute you can find out which folder was just recently created before your backup was performed. Once you have determined your backup location you

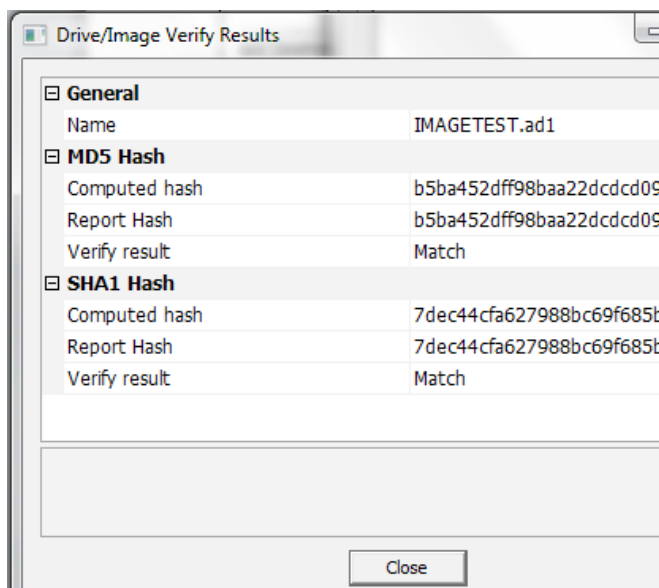
can now create a forensic image of the folder. For this part I use a tool called FTK Imager. This tool is free and is available at AccessData's website. Once you have the tool launched click "File" in the top left of the screen and select "Create Disk Image" (Shown below).



Once you have selected "Create Disk Image" select "Contents of a folder" and then browse to the location of the backup. Once the backup is selected and click finish. You should now be prompted on the export destination of the forensic image file.

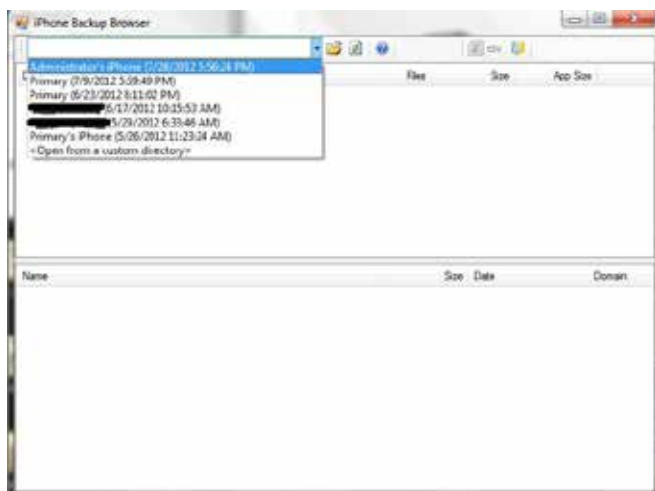


I would recommend you place this backup on a USB stick or hard drive for preservation location. Once you have added the Image Destination, desired settings, and name of image select Start. This will then export a forensic image file along with a MD5 Hash of the image file that was created.

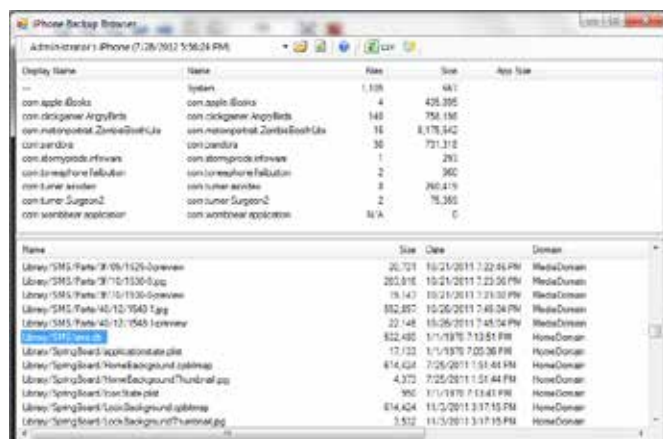


Now that this image file is created ensure that you create a new CoC with the proper information.

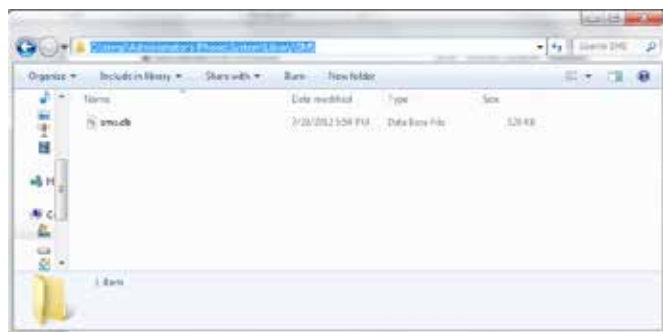
Since you now have a forensic copy of the iPhone backup you can now perform your analysis on the working copy. First thing to do is download a tool called iPhone backup browser. This is an open source project provided and supported by many charitable developers across the world. Once you have installed your program go ahead and launch it and click on the drop down box. Once you see the owners name of the recent backup select it from the list.



Once you have your backup item selected you can see a list of applications installed and system database files on the iPhone. I have selected the sms.db database file, highlighted below, this contains all text message activity utilized on the iPhone. This includes all incoming, outgoing, draft and templates text message items. Once you have the items selected click the Export button on the far right on the tool bar at the top of your program.



Once you have selected the item you would like and click the export button your data is then exported the following directory C:\temp*Owners's iPhone\System/Library\SMS. The temp directory is a place that was setup by the designer of the program and cannot be changed from the front end interface.



Now that you have your data exported from the backup you can now start your analysis of the database. For this part of the analysis I use a tool called Epilog (<http://www.ccl-forensics.com/Software/epilog-from-ccl-forensics.html>). This program is available to purchase for around 400.00USD "on one nominated computer". Epilog allows the digital examiner to look inside the database by converting database tables into readable text. Epilog has many different "Signature Files". These signature files allow for many different type of database analysis. A few examples that you could use would be the SMS, call log, and the Email signature. Below is an example from the administrator iPhone with SMS signature file being ran on the backup SMS database file.



As you can see from the screenshot this tool allows you to see many different metadata attributes of the text message. This tool also allows you to determine the status of the text message. This would mean if the items was read, to, from, and if the items was deleted (in some cases).

After are you finished with your analysis you can use the export feature created in the tool. I personally like to use the XML file. This file type makes it much easier to format the data to your client's preference.

Below is an example of what the exported items look like in a XML format have presented similar data in multiple cases:

[illegible]

My clients have been happy with the quick turn around and report format that was possible due to this tool. I hope this information is helpful to you and will be a good contribution to your forensic lab. The tools used in this article cost around 407.00USD. When comparing these tools to other forensic tools that provided the same results you save around 3,000GBP! Imagine what you could do if had an extra 3,000GBP lying around your lab. Please continue to do your part and support the open source community. Thank you for reading and hope you have learnt something new today.

Comments

Even that might work, depending on the scope of the Forensics that you are doing. But then, you should at least mention that there is logical and physical evidence acquiring and this one is logical

And, forensics has to be repeatable and for that documentation is important, I suggest you had a few words on documenting the process whilst its being done.

I do not agree fully with the concept of using iTunes to do forensics as there is a chance that I tunes mite write into the phone and thereby rendering the evidence unusable in the court of law.

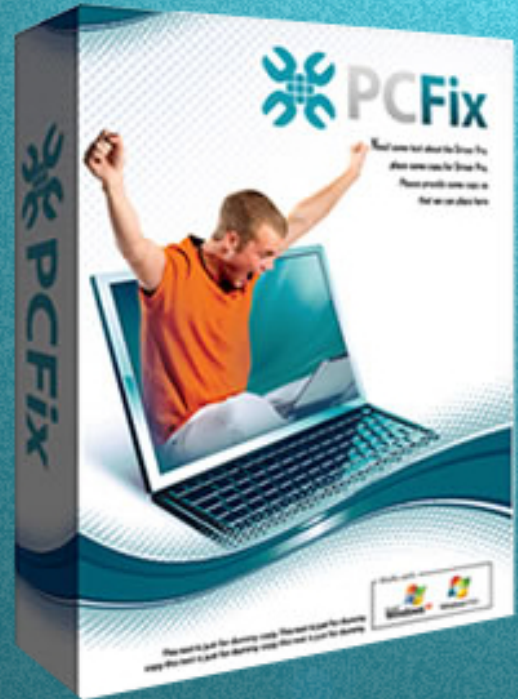
Agreed with most of your comment and addressed them by creating a forensic image of the backup folder. Then storing that to a USB or hard drive and starting another CoC.

Author bio

Donovan Farrow is the Founder/Owner of Alias Forensics. He currently holds multiple certifications relating to the computer forensic field including the Computer Certified Examiner (CCE) along with a GIAC Certified Forensic Analyst (GCFA). He has worked well over 200 litigation cases and has served as an expert witness in court. He is also a publish author and has been a presenter to many BAR associations and legal events. Donovan has assisted in the development of forensic program for local colleges in Oklahoma. He is a current member of the following organizations; International Society of Computer Forensic Examiners, EDRM, InfraGard- Oklahoma, and the OCCC Advisor Board



PC Fix



Fix Windows Registry & Repair PC Errors!



Before you continue:

- ✓ Free scan your Computer now!
- ✓ Improve PC Stability and performances
- ✓ Clean you registry from Windows errors

Instant Scan



For instant registration visit <http://bit.ly/XDEFR>

Digital Evidence First Responder

Instructor-led Online Training

Certification Program: XCySS Certified Digital Evidence First Responder (XDEFR)
(Accredited by Internet And Mobile Association of India)

Duration: 8 Hours (2Hours X 4Days)

Schedule: 1100 - 1300 (EST) / 2130 - 2330(IST), 16th, 23rd, 30th Sept. 2012 & 7th Oct. 2012 (Sundays Only)
1900 - 2100 (EST) / 0530 - 0730 (IST) 1st, 2nd, 3rd & 4th Oct. 2012, (Mon to Thu)

Objective: The purpose of this training program is to prepare professionals in identifying, seizing, preserving and transportation of digital evidence in accordance with the legal requirements. Digital evidences are volatile and can be easily tampered, therefore it may provide an alibi to the culprits if the digital evidence is not handled and managed from the very start in accordance procedure established by the relevant statutory and regulatory mechanism. While the training is not being overwhelmingly technical in delivery, this program provides a sufficient overview of techno-legal aspect in order to prepare digital evidence first responder. On successful completion of training and certification the management can confidently authorized such person to handle/manage digital/ electronic evidence that it can stand the scrutiny of law for admissibility, authenticity and verifiability in corporate disciplinary action, civil suits or criminal proceedings. *(Training is product neutral and does not recommend any specific product)*

➡ Course Outline:

- ❖ **Primer of Cyber Forensics**
- ❖ **Roles and Responsibilities of DEFR**
- ❖ **Integration with Incidence Response Team**
- ❖ **Identification and Collection of Electronic Evidence**
- ❖ **Forensic Copying and Acquisition of Electronic Evidence**
- ❖ **Preservation and Transportation of Electronic Evidence**
- ❖ **Relevant Laws and Regulation**
 - ➡ **For International trainee**
 - ➡ **For Indian Trainee**
- ❖ **International Best Practices**

Level: Introductory

Pre-requisite: Basic Computer Knowledge, No advanced preparation required.

Who should attend: IT professionals, CERT/CSIRT members, Incident handlers, Para-legals, Advocates, Investigators, E-discovery professionals, Information Security Analyst, Risk Analyst

Fee: \$349 USD for foreign trainee (Rs.9,999 INR for Indian trainee)

About Chief Instructor

The Course designer and Chief Instructor is Commander Mukesh Saini (Retd). Some of his former appointments include Naval Officer with specialization in telecommunication and electronic warfare, National Coordinator of Information Security (Govt. of India), Convener of sectorial cyber security officers (GOI), Interlocutor with international bodies and foreign governments on information security on behalf of GOI and Chief (Information) Security Advisor to Microsoft. He has vast experience of more than 25 years in the field of information security, cyber security, cyber warfare, cyber counter terrorism and policy formulation at national and international level including drafting UN resolution on the subject. He is author of several books, research papers and articles on the subject of information security. He holds three masters degrees viz. MBA, MCA and MSc. He also holds several professional certifications including CISSP and ISO 27001 Lead Auditor.

ISSE

INTEGRATED SAFETY & SECURITY EXHIBITION
LEADING NATIONAL SAFETY & SECURITY
EXHIBITION IN RUSSIA

INTEGRATED SAFETY AND SECURITY EXHIBITION 2013 May 21-24

Moscow,
All-Russia Exhibition Center, Hall 75

Protection
& Defence



Technical Facilities
for Border and Customs Control



Security Technical Systems
and Equipment



Fire
Protection



Rescue
Equipment



Disaster
Medicine



Environmental
Safety



Industrial
Safety



Equipment for Nuclear, Chemical
and Biological Safety



Information and Communication
Security



Transport
Safety



           www.isse-russia.ru

Organizers:



Ministry of the Russian Federation for Civil
Defence, Emergencies and Elimination
of Consequences of Natural Disasters
(EMERCOM of Russia)



Ministry of the Interior
of Russia



Federal Service
of Military-Technical
Cooperation

ISSE-2013: open space for the Exhibitors

In spite of the fact that there are still 8 months to go before the ISSE-2013 grand opening, the exhibition space on the outdoor area in front of the pavilion #75 is almost fully booked by the ISSE Exhibitors. The annual event that consists of the exhibition, congress and demonstration program by tradition will be held during 21 — 24 May 2013.

At the moment more than 80% of outdoor exhibition space has been reserved by the leading companies that will demonstrate their new products in action to the visitors of the ISSE-2013. Over 5000 sq.m. of the outdoor exhibition area become every year a meeting point for the Exhibitors and the professionals of the sphere. As it is already known, the largest space on the outdoor area will be taken by Iveco which «appetite» grows year in year out. Iveco AMT LLC is a Russian manufacturer of heavy-load trucks under license from Iveco. Iveco AMT trucks are made to individual orders adjusted to the peculiarity of their operation in Russia. Also the visitors will be able to see here trucks manufactured by GAZ Group. Next to them Vargashi Plant of Firefighting & Special Equipment will present its unique products. Several large areas will be taken by the well-known company «Pozhtechnika» and their Ukrainian colleagues - «Pozhspetsmash» company. On the exposition «side» will be located the exhibits of the BEREK Company. The new products of such manufacturers as CPS, Chetra-Forest, Peleng, Scania Rus, Omnimed and other companies will be presented here as well. May is not only a time of clear sky, bright sun and good weather but also a perfect time for business communication. Here you can see beautiful, powerful and vitally important means of transport and special equipment which is used in case of emergency. With the years functional capabilities and capacity of represented means of transport broaden. Outdoor area now displays armored cars, as well as unmanned vehicles. As practice shows this very format of exhibition organizing helps the exhibitors to establish direct business contacts with suppliers and consumers. Outdoor exhibition area gives the exhibitors an opportunity to demonstrate full potential of large-size exhibits. This makes positive influence on quality of negotiations and leads subsequently to signing contracts. Comparing outdoor exhibition area of previous years one may see that its quality grows permanently which will certainly attract more print and electronic media journalists especially TV journalists. Among the exhibits you will see in action the powerful lifting cranes, telescopic towers, and other special equipment, as well as get acquainted with their tactical and technical characteristics. This is where the exhibitors will be able to demonstrate unique capabilities of their products to potential customers. Advanced engineering solutions attract customers and experts - the Visitors of the Integrated Safety & Security Exhibition by its novelty. The exclusive feature of ISSE-2013 is that it is held as a large scale integrated event of the security, defense and law enforcement bodies of Russia.

The business program and other aspects of the Exhibition are available at www.isse-russia.ru/en. We are looking forward to new Exhibitors and Visitors of the International Integrated Safety and Security Exhibition. Подробнее: <http://www.isse-russia.ru/en/site.xp/052052050124055053051050.html>

CYBER THREATS REACHING NEW HEIGHTS

Cyber attacks reaching new heights of sophistication. High profile of cyberespionage occurring in last years.

1 2 3



CYBER AND SCADA SECURITY

[CLICK HERE](#)



DENIAL OF SERVICE SIMULATOR

[CLICK HERE](#)



CYBERDIN INTRUSION DETECTION

[CLICK HERE](#)



WEB APPLICATION PENETRATION

[CLICK HERE](#)



STATION HARDENING BYPASS

[CLICK HERE](#)



PRODUCT PENETRATION TESTS

[CLICK HERE](#)

ABOUT US

01

Cyberdin - Your Cyber Domain Inspector, is a leading cyber security and penetration services provider.

02

Specializes in cybercrime, application & network security and security products bypass.

03

Led by a senior team, former IDF intelligence and information security units (8200 unit).

OUR SERVICES

Cyberdin provides wide range of service in the Cyber security and the Penetration testing area.

- Cyber & SCADA Security
- Denial of Service Simulator
- Web Application Penetration
- Station Hardening Bypass
- Product Penetration Tests
- Mobile Applications Penetration
- Cyberdin Intrusion Detection
- Wireless Penetration Test
- Biometric Systems Penetration

DENIAL OF SERVICE (DOS) SIMULATOR



Denial of Service Simulator

CyberDin developed unique and advanced Denial of Service (DOS) simulators and DDOS network architecture that allows simulate current and future DDOS and Application Layer DOS attacks...

Teamwork

Innovation

Quality

Integrity

Passion



Sense of Security Compliance, Protection and Business Confidence

Sense of Security is an Australian based information security and risk management consulting practice. From our offices in Sydney and Melbourne we deliver industry leading services and research to our clients locally, nationally and internationally.

Since our inception in 2002, our company has performed tremendously well. We thrive on team work, service excellence and leadership through research and innovation. We are seeking talented people to join our team. If you are an experienced security consultant with a thorough understanding of Networking, Operation Systems and Application Security, please apply with a resume to careers@senseofsecurity.com.au and quote reference PTM-TS-12.

info@senseofsecurity.com.au
www.senseofsecurity.com.au



secureninja.com

Forging IT Security Experts

- Security+
- CISSP®
- CEH (Professional Hacking) v7.1
- CAP (Certified Authorization Professional)
- CISA
- CISM
- CCNA Security
- CWNA
- CWSP
- DIACAP
- ECSA / LPT Dual Certification
- ECSP (Certified Secure Programmer)
- EDRP (Disaster Recovery Professional)
- CCE (Computer Forensics)
- CCNA Security
- CHFI
- ISSEP
- Cloud Security
- Digital Mobile Forensics
- SSCP
- Security+
- Security Awareness Training
- ... And more



**Expert IT
Security
Training &
Services**

Free Hotel Offer on Select Boot Camps

Offers ends on Jan 31, 2012 – Call 703-535-8600 and mention code: **PentestNinja** to secure your special rate.

Welcome Military – Veterans Benefits & GI Bill Post 9/11 Approved
WIA (Workforce Investment Act) Approved



www.secureninja.com



703 535 8600



Sign Up & Get Free
Quiz Engine
From ccure.org