eForensics Magazine

Computer

VOL.2NO.9

# Computer Forensics JumpStart Vol. 2

100+ PAGES

TWELVE OPEN-SOURCE LINUX FORENSIC TOOLS

A BEGINNER'S GUIDE TO FORENSIC IMAGING

DIGITAL FORENSICS ON CLOUD STORAGE

FOUR WINDOWS XP FORENSIC ANALYSIS TIPS & TRICKS

DETECT AND PREVENT FILE TAMPERING IN MULTIMEDIA FILES

Issue 09/2013 (12) August

FEDERAL AGENCY
CYBER STRATEGY

eForensics Magazine
TEAM

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

**Betatesters/Proofreaders:**
Johan Scholtz, M1ndl3ss, Massa Danilo, Nicolas Villatte, James Fleit, Simohammed Serrhini, Andrew J. Levandoski, Owain Williams, Alex Rams, Leighton Johnson, Richard C. Leitz Jr., Gabriele Biondo, Akash Rosen, Olivier Caleff, Brett Shavers, Dave Nash, Pardhasaradhi C.H., Kishore P.V., Henrik Becker, Dr D.B. Karron.

**Senior Consultant/Publisher:**
Paweł Marciniak

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

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

**DTP:** Ireneusz Pogroszewski

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

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

**Publisher:** Hakin9 Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 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.*

# Dear Readers!

**We're happy to see you again!**

**As promised in my previous issue, here is Computer Forensics JumpStart Volume #2. This time, I tried to keep the focus on different operating systems like Windows, Linux and iOS, some open source tools, tips and tricks. It's a perfect continuation of my previous edition, and I would suggest you read Computer Forensics JumpStart Volume #1 first!**
**What is this Volume all about? This time you'll learn even more about different operating systems. Also, I decided to add an article about a very important part of computer forensics science – eDiscovery. It's not a secret that Mozilla became very popular (especially after Firefox OS was presented), and that's why you'll also find an article about this web browser. You will also find an article dedicated to a progressive developing area; cloud storage, and a life case study in forensic investigation "The Golden Nugget".**
**By the way, your interest in foundational forensics is so overwhelming, that I decided to prepare a special series with more specific topics. For example, in the end of August you'll be able to find on our website special issue titled "Computer Forensics: Preparation Stage", where you'll find all that one should know, and what one should remember about, before an investigation process will start.**
**I would like to say thanks to all authors and proofreaders who helped me to gather all these articles in one issue and publish it for eForensics readers. Also, thanks to my team which supports and helps me.**

**Peace, love, unity.**
**Artur Inderike**
**eForensics Team**

# FORENSICS ON LINUX

by Barry Kokotailo

The majority of forensics examinations conducted today comprise Windows machines. Considering that the vast majority of desktops in use today are Windows based, this should not be of a surprise. However a good majority of servers and workstations are Linux based and running interesting services such as databases, web and file services. During the career span of a forensics professional you will need to perform a forensic examination of a Linux machine. This article will give you the step by step procedure in order to acquire an image, analysis, and report on the findings.

**What you will learn:**

- Image Linux based media and memory.
- Analyze data from a Linux image.
- Present reports to non technical staff.

**What you should know:**

Ideally you should be an experienced Linux systems administrator with at least a couple of years of experience in a Linux data center. A minimum would be basic UNIX command skills with knowledge in networking and programming.

How do you know when you have been hacked? How do you know when malware has been planted? Strange as it may seem, it could come down to a feeling of "something is not right". When systems are brought into production they behave in a certain fashion. Then one day they start exhibiting abnormal behavior. The bandwidth usage increases. The CPU spends a lot more time doing something in the wee hours of the morning. Users complaining of slow service. This would all be indicators of an intrusion. Hopefully you would have been using some type of performance monitor such as Nagios (*http://www.nagios.org/*) for your infrastructure in order to baseline your systems and generate alerts when abnormal behavior exists.

## THE IMAGING PROCESS

The imaging process depends on the target machine. If the target machine is a standalone desktop server managed by a single user, you have total control over when this machine comes off line and when the various drive partitions are imaged. If the machine is a development server, you need to make sure the developers, database analysts and administrators are off the machine before you can bring the server down. The worst case scenario is the Linux server is a production server. At that time you have to schedule downtime for the machine and try to acquire the images in as short a period of time possible. Would help if the server was part of a pool of servers, so that pulling the suspect server would not interrupt business operations. Worst case situation is the target machine comes down the business is down until you complete the image. Business owners do not like this one. A final resort is to take an image while the machine is running. Not recommended. Calls in to question the integrity of your image. On any of the scenarios described, document, document, document.

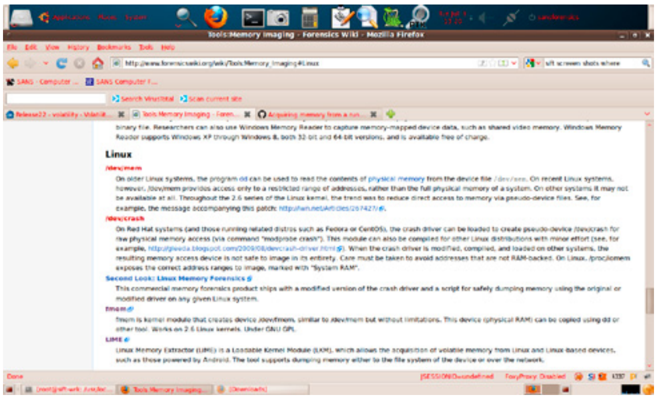
## IMAGE THE MEMORY FIRST

Once the above decisions have been made, we need to acquire the memory image from the system. The utility I will use is fmem (*http://www.forensicswiki.org/wiki/Tools:Memory_Imaging#Linux*) (Figure 1).

Make a directory called `/usr/local/src/fmem` on the target machine. Download the fmem source into this directory. Uncompress the source and change into the source tree. Build the new device `/dev/fmem` by issuing the commands "make" and. `/run .sh`. Then I can dump the memory.

Ignore the error messages. So the commands in summary are:

```
# mkdir  /usr/local/src/fmem
# mv  fmem-current.tgz  /usr/local/src/fmem
# cd  /usr/local/src/fmem
# tar  zxvf   *gz
# cd  fmem_1.6-0
# make
# ./run.sh
```



Tools:Memory Imaging - Forensics Wiki - Mozilla Firefox

http://www.forensicswiki.org/wiki/Tools:Memory_Imaging#Linux

binary file. Researchers can also use Windows Memory Reader to capture memory-mapped device data, such as shared video memory. Windows Memory Reader supports Windows XP through Windows 8, both 32 bit and 64 bit versions, and is available free of charge.

**Linux**

**/dev/mem**

On older Linux systems, the program dd can be used to read the contents of physical memory from the device file /dev/mem. On recent Linux systems, however, /dev/mem provides access only to a restricted range of addresses, rather than the full physical memory of a system. On other systems it may not be available at all. Throughout the 2.6 series of the Linux kernel, the trend was to reduce direct access to memory via pseudo-device files. See, for example, the message accompanying this patch: http://lwn.net/Articles/267427/.

**/dev/crash**

On Red Hat systems (and those running related distros such as Fedora or CentOS), the crash driver can be loaded to create pseudo-device /dev/crash for raw physical memory access (via command "modprobe crash"). This module can also be compiled for other Linux distributions with minor effort (see, for example, http://gleeda.blogspot.com/2009/08/devcrash-driver.html). When the crash driver is modified, compiled, and loaded on other systems, the resulting memory access device is not safe to image in its entirety. Care must be taken to avoid addresses that are not RAM-backed. On Linux, /proc/iomem exposes the correct address ranges to image, marked with "System RAM".

**Second Look: Linux Memory Forensics**

This commercial memory forensics product ships with a modified version of the crash driver and a script for safely dumping memory using the original or modified driver on any given Linux system.

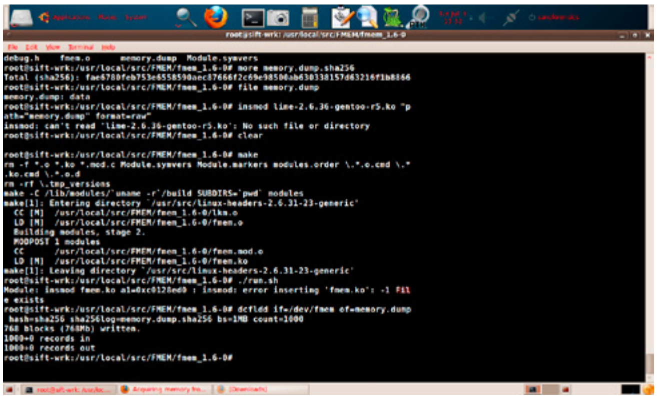
**fmem**

fmem is kernel module that creates device /dev/fmem, similar to /dev/mem but without limitations. This device (physical RAM) can be copied using dd or other tool. Works on 2.6 Linux kernels. Under GNU GPL.

**LiME**

Linux Memory Extractor (LiME) is a Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices, such as those powered by Android. The tool supports dumping memory either to the file system of the device or over the network.

**Figure 1.** *Location where you find fmem*



root@sift-wrk: /usr/local/src/FMEM/fmem_1.6-0

```
debug.h    fmem.o      memory.dump  Module.symvers
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# more memory.dump.sha256
Total (sha256): fae6780feb753e6558590aec87666f2c69e98500ab630338157d63216f1b8866
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# file memory.dump
memory.dump: data
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# insmod lime-2.6.36-gentoo-r5.ko "p
ath="memory.dump" format=raw"
insmod: can't read 'lime-2.6.36-gentoo-r5.ko': No such file or directory
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# clear

root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# make
rm -f *.o *.ko *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*
.ko.cmd \.*.o.d
rm -rf \.tmp_versions
make -C /lib/modules/`uname -r`/build SUBDIRS=`pwd` modules
make[1]: Entering directory `/usr/src/linux-headers-2.6.31-23-generic'
  CC [M]  /usr/local/src/FMEM/fmem_1.6-0/lkm.o
  LD [M]  /usr/local/src/FMEM/fmem_1.6-0/fmem.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /usr/local/src/FMEM/fmem_1.6-0/fmem.mod.o
  LD [M]  /usr/local/src/FMEM/fmem_1.6-0/fmem.ko
make[1]: Leaving directory `/usr/src/linux-headers-2.6.31-23-generic'
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# ./run.sh
Module: insmod fmem.ko a1=0xc0128ed0 : insmod: error inserting 'fmem.ko': -1 Fil
e exists
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0# dcfldd if=/dev/fmem of=memory.dump
 hash=sha256 sha256log=memory.dump.sha256 bs=1MB count=1000
768 blocks (768Mb) written.
1000+0 records in
1000+0 records out
root@sift-wrk:/usr/local/src/FMEM/fmem_1.6-0#
```

**Figure 2.** *The installation of /dev/fmem and the generation of the memory image*

```
# dcfldd  if=/dev/fmem of=memory.dump  hash=sha256
sha256log=memory-dump-sha256-hash.log bs=1MB
count=1000
```

The `dcfldd` command is used to generate a memory dump file called memory.dump. The hash file is created called `memory-dump-sha256-hash.log` with a file size of 1 gig of memory. Size according to your memory size.

I save the memory.dump file onto a USB stick for removal to the lab (Figure 2).

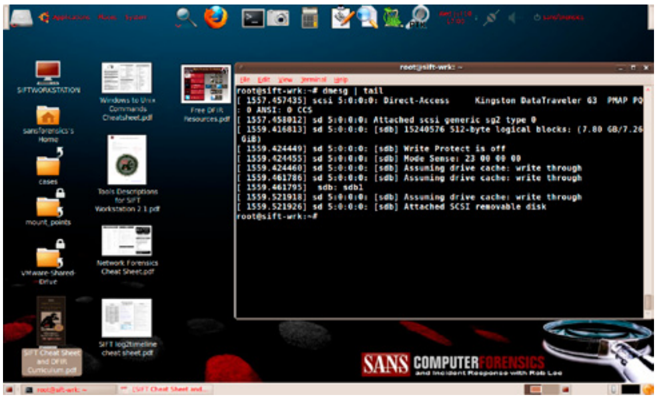
Once I have the memory dump file, I will run it across volatility to determine if the image is recognized by volatility for future processing:

```
# python vol.py -f /memory/memory.dump imageinfo
```

If you get a valid profile, you feed the profile using `--profile="Something"` to the vol.py script to dump various items of interest. For example, I can use the following command to try an examine the arp tables from the memory dump:

```
# python vol.py  -f  /memory/memory.dump
--profile=LinuxUbuntu1204x64  linux_pslist
```

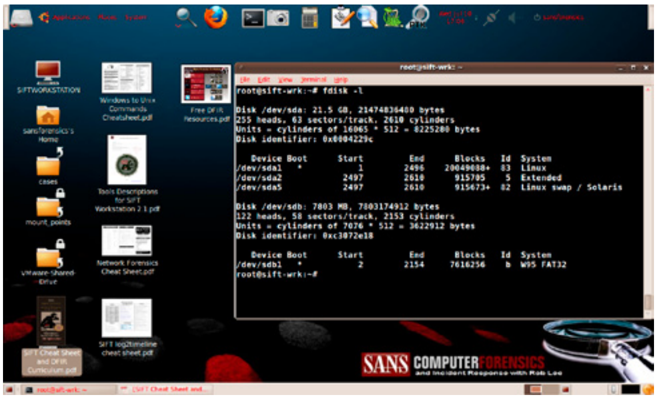
A list of other items of interest can be located at this url *http://code.google.com/p/volatility/wiki/LinuxCommandReference22#linux_pslist.*



root@sift-wrk: ~

```
root@sift-wrk:~# dmesg | tail
[ 1557.457435] scsi 5:0:0:0: Direct-Access     Kingston DataTraveler G3  PMAP PQ
: 0 ANSI: 0 CCS
[ 1557.458012] sd 5:0:0:0: Attached scsi generic sg2 type 0
[ 1559.416813] sd 5:0:0:0: [sdb] 15240576 512-byte logical blocks: (7.80 GB/7.26
 GiB)
[ 1559.424449] sd 5:0:0:0: [sdb] Write Protect is off
[ 1559.424455] sd 5:0:0:0: [sdb] Mode Sense: 23 00 00 00
[ 1559.424460] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[ 1559.461786] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[ 1559.461795]  sdb: sdb1
[ 1559.521918] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[ 1559.521926] sd 5:0:0:0: [sdb] Attached SCSI removable disk
root@sift-wrk:~#
```

**Figure 3.** *Output of dmesg indicating the suspect KIngston drive is called /dev/sdb*



root@sift-wrk: ~

```
root@sift-wrk:~# fdisk -l

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x0004229c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1        2496    20049088+  83  Linux
/dev/sda2            2497        2610      915705    5  Extended
/dev/sda5            2497        2610      915673+  82  Linux swap / Solaris

Disk /dev/sdb: 7803 MB, 7803174912 bytes
122 heads, 58 sectors/track, 2153 cylinders
Units = cylinders of 7076 * 512 = 3622912 bytes
Disk identifier: 0xc3072e18

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *           2        2154     7616256    b  W95 FAT32
root@sift-wrk:~#
```

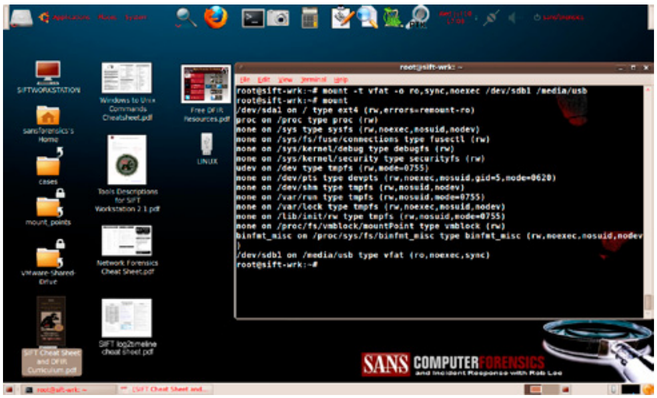
**Figure 4.** *The output of "fdisk -l" to verify the name of the suspect media and the file system type*

The list of image profiles for Linux are limited. Can build it for some systems at the present time. Check this web page for pre-built (*http://code.google.com/p/volatility/wiki/LinuxProfiles*) or this web page on how to build your own profiles (*http://code.google.com/p/volatility/wiki/LinuxMemoryForensics*).

The release of Volatility 2.3 in June 2013 should introduce additional features and profiles for Linux memory acquisitions.

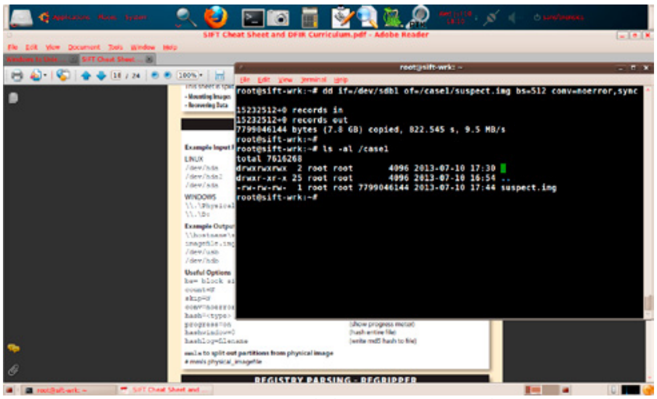
I can run simple commands such as strings to filter strings out from the memory dump:

```
# strings /memory/memory.dump > mem-results.txt
```



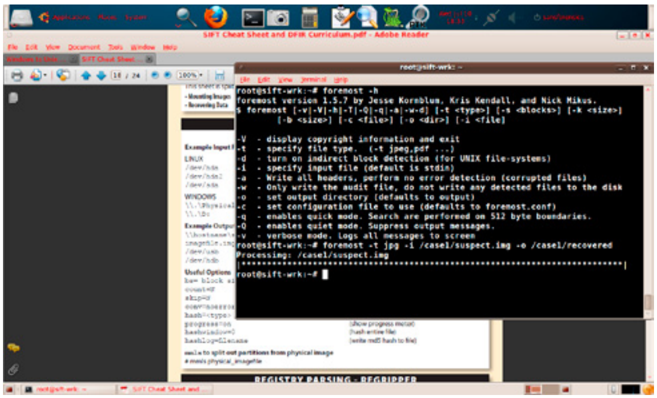
```
root@sift-wrk:~# mount -t vfat -o ro,sync,noexec /dev/sdb1 /media/usb
root@sift-wrk:~# mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw)
none on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type tmpfs (rw,mode=0755)
none on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
none on /dev/shm type tmpfs (rw,nosuid,nodev)
none on /var/run type tmpfs (rw,nosuid,mode=0755)
none on /var/lock type tmpfs (rw,noexec,nosuid,nodev)
none on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
none on /proc/fs/vmblock/mountPoint type vmblock (rw)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev
)
/dev/sdb1 on /media/usb type vfat (ro,noexec,sync)
root@sift-wrk:~#
```

**Figure 5.** *I mount the suspect device and verify the mount worked and the options are in effect*



```
root@sift-wrk:~# dd if=/dev/sdb1 of=/case1/suspect.img bs=512 conv=noerror,sync

15232512+0 records in
15232512+0 records out
7799046144 bytes (7.8 GB) copied, 822.545 s, 9.5 MB/s
root@sift-wrk:~#
root@sift-wrk:~# ls -al /case1
total 7616268
drwxrwxrwx  2 root root       4096 2013-07-10 17:30 .
drwxr-xr-x 25 root root       4096 2013-07-10 16:54 ..
-rw-rw-rw-  1 root root 7799046144 2013-07-10 17:44 suspect.img
root@sift-wrk:~#
```

**Figure 6.** *Here I have imaged the suspect media. Notice the size of the partition is about 8 Gigs*



```
root@sift-wrk:~# foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
root@sift-wrk:~# foremost -t jpg -i /case1/suspect.img -o /case1/recovered
Processing: /case1/suspect.img
|*****************************************************************************|
root@sift-wrk:~#
```

**Figure 7.** *Help with foremost. Here I am recovering jpg files from the image and storing any recovered files into the /case1/recovered folder*

From here, I can search for keywords in the strings file:

```
# grep -i badguy mem-results.txt
```

**NOTE**

Any time you are working on a live suspect system, every action alters the state of the suspect system. You must document and possibly defend in court all actions related to what you did on the suspect system.

## IMAGE THE DRIVES

I will use the dd command to create an image of the suspect media. First I will insert the device into a USB write blocker that is connected to my SIFT Kit. I will check the system with dmesg to determine if the device was recognized (Figure 3).

I will also run `fdisk -l` to verify the device name and to also find out what file system type it is (Figure 4).

```
# dmesg | grep  sd
# fdisk -l
```

Once I have identified the name of the suspect media and the file system type, I can then mount it in read only mode on the loopback interface with no possibility of any code executing (Figure 5).

```
# mount -t vfat -o ro,sync,noexec  /dev/sdb1 /
                  media/usb
```

Once mounted I can create a dd image of the media.

```
# dd if=/dev/sdb1 of=/case1/suspect.img
                  conv=noerror,sync
```

You will notice that there is only one partition on the `/dev/sdb` device. If there were more, I would re-execute the `dd` command on each one of the partitions and save them as a separate image with a unique and distinctive name. For example if there were three partitions to image called `/dev/sb1`, `/dev/sdb2`, and `/dev/sdb3`:

```
# dd if=/dev/sdb1 of=/case1/root.img bs=512
conv=noerror,sync
# dd if=/dev/sdb2 of=/case1/usr.img bs=512
conv=noerror,sync
# dd if=/dev/sdb3 of=/case1/home.img bs=512
conv=noerror,sync
```

The imaging can take a substantial period of time, depending on the size of the partition (Figure 6).

## THE ANALYZE PHASE

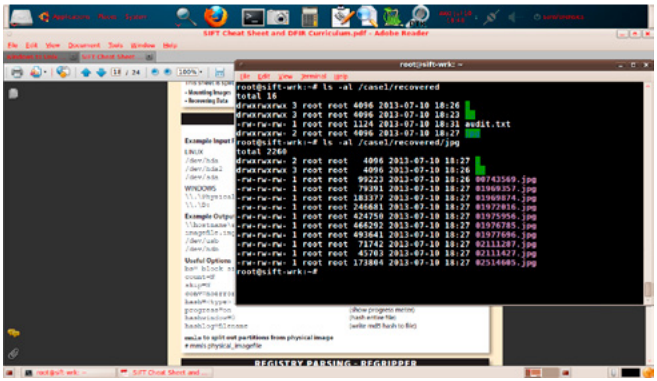
The first thing I perform on the suspect image is to recover any deleted files. The SIFT Toolkit has a tool called foremost that be used for this purpose. The tool works by examining the headers and footers of any deleted file and making a determination of what file type it is. This overcomes the act of the bad guy renaming all his pictures with a pdf extension. I can specify the extension to look for on the command line or I can edit the `/etc/foremost.conf` file. This file indicates all files you can recover and if you have additional file types, you can add the header and footer definitions here (Figure 7 and Figure 8).

```
# foremost -t jpg -i /case1/suspect.img -o /case1/
                  recovered
```

## STRING SEARCHS

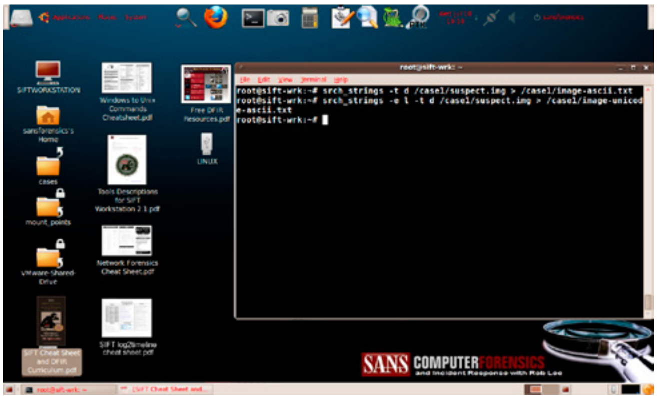
A method used to extract information of value is performing both ascii and unicode string searches on the image. I compile a list of keywords that are related to the case. Names, address, phones numbers, emails, anything unique related to this case. Of course we avoid words like "the" or "of" which would generate a huge amount of false positives. I would place these words inside a file and use grep to parse the results of the string searches for those keywords saving the results in separate and uniquely identifiable files.

```
# srch_strings -t d /case1/suspect.img > /case1/
image.ascii.txt
# srch_strings  -e l -t d /case1/suspect.img > /
case1/image.unciode.ascii.txt
```



```
root@sift-wrk:~# ls -al /case1/recovered
total 16
drwxrwxrwx 3 root root 4096 2013-07-10 18:26 .
drwxrwxrwx 3 root root 4096 2013-07-10 18:23 ..
-rw-rw-rw- 1 root root 1124 2013-07-10 18:31 audit.txt
drwxrwxrw- 2 root root 4096 2013-07-10 18:27 jpg
root@sift-wrk:~# ls -al /case1/recovered/jpg
total 2260
drwxrwxrw- 2 root root   4096 2013-07-10 18:27 .
drwxrwxrwx 3 root root   4096 2013-07-10 18:26 ..
-rw-rw-rw- 1 root root  99223 2013-07-10 18:26 00743569.jpg
-rw-rw-rw- 1 root root  79391 2013-07-10 18:27 01969357.jpg
-rw-rw-rw- 1 root root 183377 2013-07-10 18:27 01969874.jpg
-rw-rw-rw- 1 root root 246681 2013-07-10 18:27 01972016.jpg
-rw-rw-rw- 1 root root 424750 2013-07-10 18:27 01975956.jpg
-rw-rw-rw- 1 root root 466292 2013-07-10 18:27 01976785.jpg
-rw-rw-rw- 1 root root 493641 2013-07-10 18:27 01977696.jpg
-rw-rw-rw- 1 root root  71742 2013-07-10 18:27 02111287.jpg
-rw-rw-rw- 1 root root  45703 2013-07-10 18:27 02111427.jpg
-rw-rw-rw- 1 root root 173804 2013-07-10 18:27 02514605.jpg
root@sift-wrk:~#
```

**Figure 8.** *Listing of /case1/recovered directory. An audit file and another directory with recovered jpgs*



```
root@sift-wrk:~# srch_strings -t d /case1/suspect.img > /case1/image-ascii.txt
root@sift-wrk:~# srch_strings -e l -t d /case1/suspect.img > /case1/image-unicod
e-ascii.txt
root@sift-wrk:~# 
```

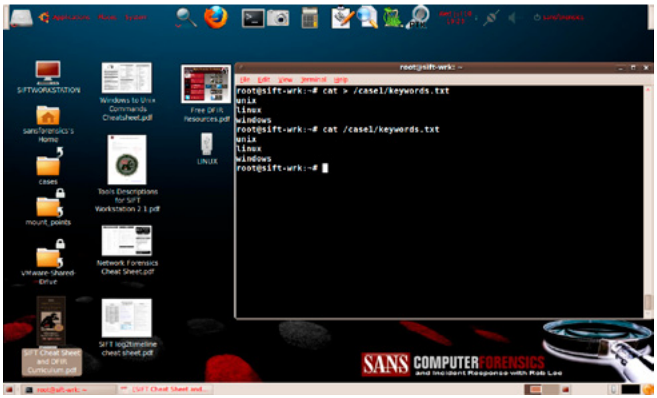
**Figure 9.** *String searches for ascii and unicode strings. The "-t d" specifies decimal offset on match. "-e l" specifies use small character size and endianess*

The l in lowercase l, not the digit 1 (Figure 9 and Figure 10).

```
#cat > /case1/keywords.txt
unix
linux
windows
#
```

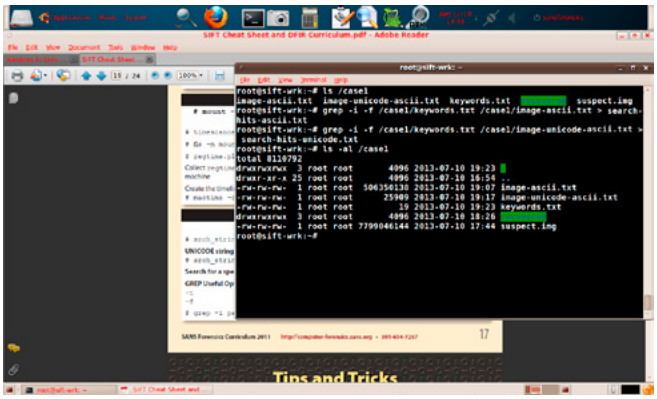
See Figure 11 and Figure 12.

```
# grep -i -f /case1/keywords.txt  /case1/image-
ascii.txt > search-hits.ascii.txt
```



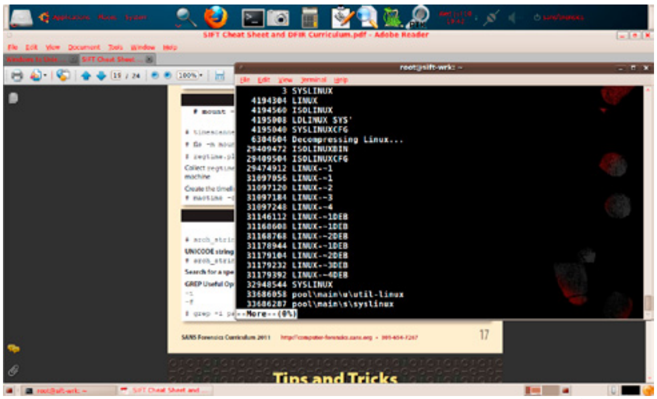
```
root@sift-wrk:~# cat > /case1/keywords.txt
unix
linux
windows
root@sift-wrk:~# cat /case1/keywords.txt
unix
linux
windows
root@sift-wrk:~# 
```

**Figure 10.** *Create a small file called keywords.txt that has the necessary keywords for the case*



```
root@sift-wrk:~# ls /case1
image-ascii.txt  image-unicode-ascii.txt  keywords.txt  recovered  suspect.img
root@sift-wrk:~# grep -i -f /case1/keywords.txt /case1/image-ascii.txt > search-
hits-ascii.txt
root@sift-wrk:~# grep -i -f /case1/keywords.txt /case1/image-unicode-ascii.txt >
 search-hits-unicode.txt
root@sift-wrk:~# ls -al /case1
total 8110792
drwxrwxrwx  3 root root       4096 2013-07-10 19:23 .
drwxr-xr-x 25 root root       4096 2013-07-10 16:54 ..
-rw-rw-rw-  1 root root  506350130 2013-07-10 19:07 image-ascii.txt
-rw-rw-rw-  1 root root      25909 2013-07-10 19:17 image-unicode-ascii.txt
-rw-rw-rw-  1 root root         19 2013-07-10 19:23 keywords.txt
drwxrwxrwx  3 root root       4096 2013-07-10 18:26 recovered
-rw-rw-rw-  1 root root 7799046144 2013-07-10 17:44 suspect.img
root@sift-wrk:~#
```

**Figure 11.** *Search results on ascii and unicode character sets*



```
       3 SYSLINUX
 4194304 LINUX
 4194560 ISOLINUX
 4195008 LDLINUX SYS'
 4195040 SYSLINUXCFG
 6304604 Decompressing Linux...
29409472 ISOLINUXBIN
29409504 ISOLINUXCFG
29474912 LINUX--1
31097056 LINUX--1
31097120 LINUX--2
31097184 LINUX--3
31097248 LINUX--4
31146112 LINUX--1DEB
31168608 LINUX--1DEB
31168768 LINUX--2DEB
31178944 LINUX--1DEB
31179104 LINUX--2DEB
31179232 LINUX--3DEB
31179392 LINUX--4DEB
32948544 SYSLINUX
33686058 pool\main\u\util-linux
33686287 pool\main\s\syslinux
--More--(0%)
```

**Figure 12.** *The ascii search results. The number in the first column is the decimal offset from the beginning of the image where the match occurred. Can be used with other tools to examine that part of the image*

```
# grep -i -f /case1/keywords.txt  /case1/image.
unicode-ascii.txt > search-hits-unicode.txt
# more search-hits-ascii.txt
```

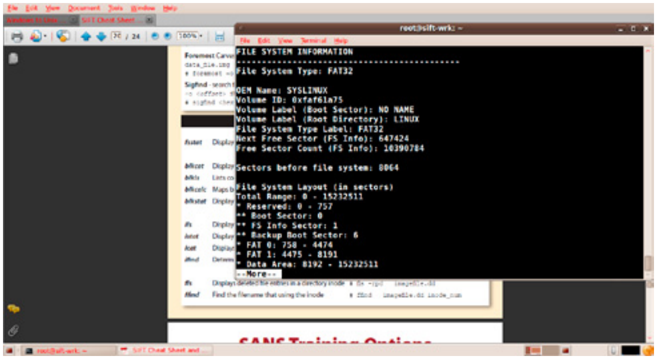
## SLEUTHKIT TOOLS OF INTEREST

Several tools from the Sleuth Toolkit can be used to further analyze the image for evidence.

- fsstat – Displays the file system details. Looking for data and inode size. The range of data and inodes.
- blkcat – Displays the contents of a disk block
- blkstat – Stats on blocks.
- ils – Displays details on file inodes.
- istat – Displays information on specific inode.
- ffind – Finds filename associated with an inode (Figure 13 and 14).

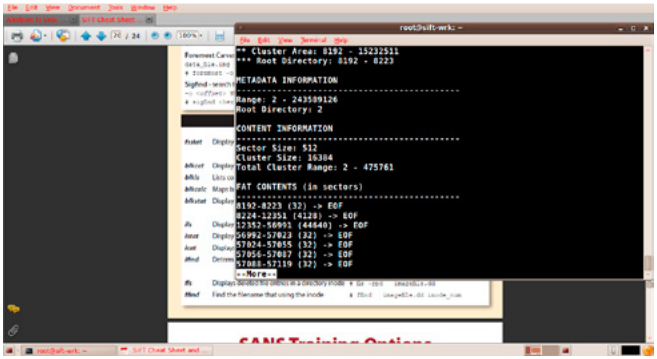
## THE TIMELINE

The SIFT Toolkit has this three commands to generate a timeline. With a timeline, it allows you to see what files have been added, changed, or deleted from the system. From this you can gain some knowledge as to what the bad guy was up to (Figure 15).



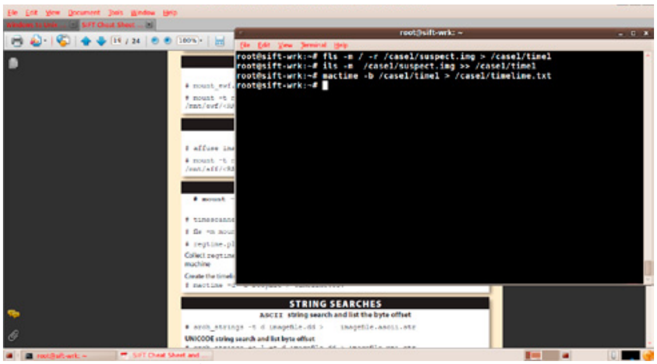
```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: SYSLINUX
Volume ID: 0xfaf61a75
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): LINUX
File System Type Label: FAT32
Next Free Sector (FS Info): 647424
Free Sector Count (FS Info): 10390784

Sectors before file system: 8064

File System Layout (in sectors)
Total Range: 0 - 15232511
* Reserved: 0 - 757
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 758 - 4474
* FAT 1: 4475 - 8191
* Data Area: 8192 - 15232511
--More--
```

**Figure 13.** *The start of fsstat....*



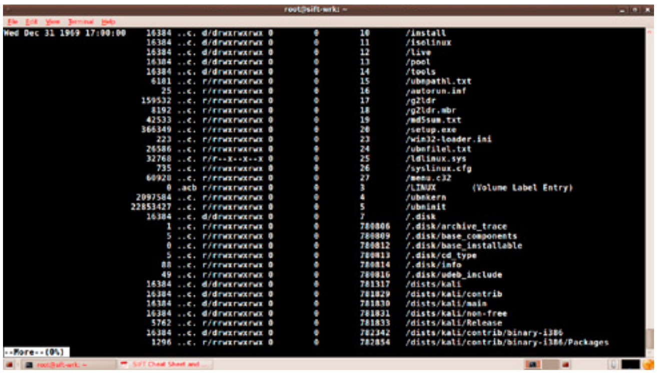
```
** Cluster Area: 8192 - 15232511
*** Root Directory: 8192 - 8223

METADATA INFORMATION
--------------------------------------------
Range: 2 - 243589126
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 16384
Total Cluster Range: 2 - 475761

FAT CONTENTS (in sectors)
--------------------------------------------
8192-8223 (32) -> EOF
8224-12351 (4128) -> EOF
12352-56991 (44640) -> EOF
56992-57023 (32) -> EOF
57024-57055 (32) -> EOF
57056-57087 (32) -> EOF
57088-57119 (32) -> EOF
--More--
```

**Figure 14.** *The end of fsstat*



```
root@sift-wrk:~# fls -m / -r /case1/suspect.img > /case1/time1
root@sift-wrk:~# ils -m  /case1/suspect.img >> /case1/time1
root@sift-wrk:~# mactime -b /case1/time1 > /case1/timeline.txt
root@sift-wrk:~# 
```

**Figure 15.** *Using fls, ils and mactime to generate the timeline*



```
Wed Dec 31 1969 17:00:00    16384 ..c. d/drwxrwxrwx 0      0       10       /install
                            16384 ..c. d/drwxrwxrwx 0      0       11       /isolinux
                            16384 ..c. d/drwxrwxrwx 0      0       12       /live
                            16384 ..c. d/drwxrwxrwx 0      0       13       /pool
                            16384 ..c. d/drwxrwxrwx 0      0       14       /tools
                             6181 ..c. r/rrwxrwxrwx 0      0       15       /ubnpathl.txt
                               25 ..c. r/rrwxrwxrwx 0      0       16       /autorun.inf
                           159532 ..c. r/rrwxrwxrwx 0      0       17       /g2ldr
                             8192 ..c. r/rrwxrwxrwx 0      0       18       /g2ldr.mbr
                            42533 ..c. r/rrwxrwxrwx 0      0       19       /md5sum.txt
                           366349 ..c. r/rrwxrwxrwx 0      0       20       /setup.exe
                              223 ..c. r/rrwxrwxrwx 0      0       23       /win32-loader.ini
                            26586 ..c. r/rrwxrwxrwx 0      0       24       /ubnfilel.txt
                            32768 ..c. r/r--x--x--x 0      0       25       /ldlinux.sys
                              735 ..c. r/rrwxrwxrwx 0      0       26       /syslinux.cfg
                            60920 ..c. r/rrwxrwxrwx 0      0       27       /menu.c32
                                0 .acb r/rrwxrwxrwx 0      0       3        /LINUX       (Volume Label Entry)
                          2097584 ..c. r/rrwxrwxrwx 0      0       4        /ubnkern
                         22853427 ..c. r/rrwxrwxrwx 0      0       5        /ubninit
                            16384 ..c. d/drwxrwxrwx 0      0       7        /.disk
                                1 ..c. r/rrwxrwxrwx 0      0       780806   /.disk/archive_trace
                                5 ..c. r/rrwxrwxrwx 0      0       780809   /.disk/base_components
                                0 ..c. r/rrwxrwxrwx 0      0       780812   /.disk/base_installable
                                5 ..c. r/rrwxrwxrwx 0      0       780813   /.disk/cd_type
                               88 ..c. r/rrwxrwxrwx 0      0       780814   /.disk/info
                               49 ..c. r/rrwxrwxrwx 0      0       780816   /.disk/udeb_include
                            16384 ..c. d/drwxrwxrwx 0      0       781317   /dists/kali
                            16384 ..c. d/drwxrwxrwx 0      0       781829   /dists/kali/contrib
                            16384 ..c. d/drwxrwxrwx 0      0       781830   /dists/kali/main
                            16384 ..c. d/drwxrwxrwx 0      0       781831   /dists/kali/non-free
                             5762 ..c. r/rrwxrwxrwx 0      0       781833   /dists/kali/Release
                            16384 ..c. d/drwxrwxrwx 0      0       782342   /dists/kali/contrib/binary-i386
                             1296 ..c. r/rrwxrwxrwx 0      0       782854   /dists/kali/contrib/binary-i386/Packages
--More--(0%)
```

**Figure 16.** *The timeline file. Here you can see what files have changed their modification, access, or creation times giving you a clear indication of what has changed on this disk*

```
# fls -m / -r /case1/susepct.ing > /case1/time1
# ils -m /case1/susepct.img >> /case1/time1
# mactime -b /case1/time1 > /case1/timeline.txt
# more /case1/timeline.txt
```

## THE FINAL REPORT

Of course at the end of all this, a generated report would be in order. Have an executive summary listing the key findings. Have a detailed breakdown of all the relevant findings of the case. One method to use is Camtasia to record the entire investigation and have that as the details section of the report. The standard SIFT Toolkit has OpenOffice and Okular to assist in documenting the case. Either way, the final report should be able to be understood by non-technical staff.

## CONCLUSION

Although I have used the SIFT Toolkit for this article, there are a number of open source forensics tools that can be used either in a Windows or Linux environment to solve forensics cases. With additional contributions from the forensics community, the list of open source tools should grow exponentially as the science of digital forensics continues to mature.

### About the Author

*I have been working in the IT field since 1986. In that time I acquired knowledge and experience in Windows, Macintosh, UNIX, networking, programming, pen-testing, forensics and incident response. I have acquired several certifications: CISA, CISSP, EnCE, ACE, CSA, CSNA, RET, CEH. I currently work for the Edmonton Public School Board in Edmonton, Alberta, Canada and operate my own company Cerberus Security Integrators Inc. http://www.forensics-canada.com in my spare time. I teach classes at a local post-secondary institute in forensics and UNIX operating systems. When I have some free time I golf and fly fish. A more complete profile of me can be accessed over at http://www.linkedin.com/pub/barry-kokotailo/28/565/405*

KPMG
*cutting through complexity*

# Are you prepared?

kpmg.ca/forensic

SECURITY
ROL • COMPLEXITY • RISK
CTRONIC
ITY • THREAT • CONTRO
• FORENSICS
CONTROL • RISK • DATABASE
HNOLOGY
MPLEXITY • THREAT • ATTACK
VESTIGATIONS
OMPLEXITY • ELECTRONIC • CYBER SECURITY • RISK • THREAT
ORPORATE • INTELLIGENCE
YBER SECURITY • ATTACK • THREAT • CYBER SECURITY
TECHNOLOGY • eDISCOVERY
OMPLEXITY • ELECTRONIC • INFORMATION • THREAT • CONTROL
DATA ANALYTICS • INFORMATION
SK • INFORMATION • TECHNOLOGY • ATTACK • RISK
NTELLIGENCE • DATA RECOVERY
OMPLEXITY • ELECTRONIC • INFORMATION • THREAT • CONTROL
ROTECTION • INFORMATION
TELLIGENCE • ELECTRONIC • CONTROL • RISK • COMPLEXITY
ISK • COMPLEXITY • INTRUSION
FORMATION • RISK • TECHNOLOGY • ATTACK • RISK

# HOW TO PERFORM FORENSIC ANALYSIS

## ON IOS OPERATING AND FILE SYSTEMS

**by Deivison Pinheiro Franco and Nágila Magalhães Cardoso**

With Apple Operation System (iOS) design and the large amount of storage space available, records of emails, text messages, browsing history, chat, map searching, and more are all being kept. With the amount of information available to forensic analysts on iOS, this article will cover the basics to accurately retrieve evidence from this platform and build forensically analysis when applicable. Once the image logically, via backup or physically has been obtained, files of interest will be highlighted for a forensic examiner to review.

**What you will learn:**

- The changes in the Apple Operating System (iOS) and the addition of the App Store to the iOS environment;
- Features that iOS offers and its limitations;
- The iOS Operating and File Systems evolution;
- What iOS Operating and File Systems are and how it can have evidences for forensic analysis;
- Delve into the details of the iDevice file system in order to provide context for investigations.

**What you should know:**

- A basic understanding of Apple Operating System (iOS);
- A basic understanding of Apple File Systems (HFS, HFS+ and HFSX);
- A basic understanding of mobile forensics analysis.

In this article, we'll look at changes in the operating system (OS) and the addition of the App Store to the iOS environment, and then we'll delve into the details of the iDevice file system in order to provide context for investigations.

iOS, the operating system for the iPhone, iPod, and iPad, was first released with the first-generation iPhone in June 2008. This revolutionized the way cell phones would be created in the future. HTC, Motorola, and Google have since jumped into the smartphone market with their Android phones, as has Research in Motion with its Blackberry phones.

Beginning with iOS 2, Apple allowed the development of application for its App Store. The iPhone SDK gave application developers the access they needed to write applications for all devices. For a developer to release software to the App Store, the developer had to enroll into the iPhone Developer Program, the initial interface of which is shown in Figure 1. A standard program had a cost of $99 and an enterprise program had a cost of $299. The developer also had to sign an extensive agreement with Apple in order to develop and add applications to the App Store. Apple also had a strict and sometimes time-consuming approval process. Over time, Apple has loosened some of its rules, and has even accommodated apps such as Google Voice and applications developed with Adobe Flash.

One of the biggest challenges that Apple has faced is the army of hackers that descended onto the iPhone. The original hackers of the iPhone justified their actions by virtue of the fact that the iPhone and iOS didn't allow certain functions (e.g., MMS, tethering, customization) or third-party applications other than those available from the App Store. Some hackers also took the stance that the iPhone was insecure, and they wanted to show Apple the flaws that it had. Some of the more notorious groups were the iPhone Dev Team and the Chronic Dev Team. Some of their more maverick members have splintered to develop jailbreaks to further their own ambitions and fame.

The modus operandi of all these hackers was notoriety – becoming known to the masses – which became an intoxicating motivation. By late 2009, other hackers had developed viruses and exploits to jailbroken iPhones. These exploits invaded the provider's network to seek out and find jailbroken iPhones. This was a concern that Apple addressed in its counter to the Electronic Freedom Foundation's claim to allow jailbreaking as an exception to the DMCA (*Digital Media Copyright Act*).

The Library of Congress decided that jailbreaking your phone was an exception. However, the deciders of this policy didn't take into account the increase of threats that would invade AT&T and Apple. So Apple and AT&T would have to protect their networks and OS. Since the release of the first Apple mobile device, Apple and the hackers have played a cat-and-mouse game. The first jailbreaks were crude and were prone to crashing the phone and making the iPhone nonfunctional, otherwise known as "bricking" the phone. Some of the jailbreaks and unlocks had the following monikers: Pwnage, Qwkpwn, RedSn0w, Yellowsn0w, iLiberty, Purplera1n, Blackra1n and Greenpois0n.

All circumvented the security measures of the iPhone by either replacing the OS with one engineered on user-created firmware, or just patching the kernel and/or bootrom, which allowed the device to run unsigned code.

## THE IOS FILE SYSTEM

### HFS+ FILE SYSTEM

In 1996, Apple developed a new file system that would accommodate storing large data sets. As physical disk size was increasing at breakneck speed, a file system had to be developed to support the growing need for storage. Hence, Apple developed the *Hierarchical File System* (HFS). The structure of HFS can be complicated to understand. At the physical level, the disks formatted with HFS are in 512 – byte blocks. These are similar to Windows-based sectors. There are two types of blocks on an HFS system: logical blocks and allocation blocks. The logical blocks are numbered from the first to the last on a given volume. They are static and are the same size as the physical blocks, 512 bytes. Allocation blocks are groups of logical blocks used by the HFS system to track data in a more efficient way. To reduce fragmentation on an HFS volume, groups of allocation blocks are tied together as clumps. This organization is shown in Figure 2.

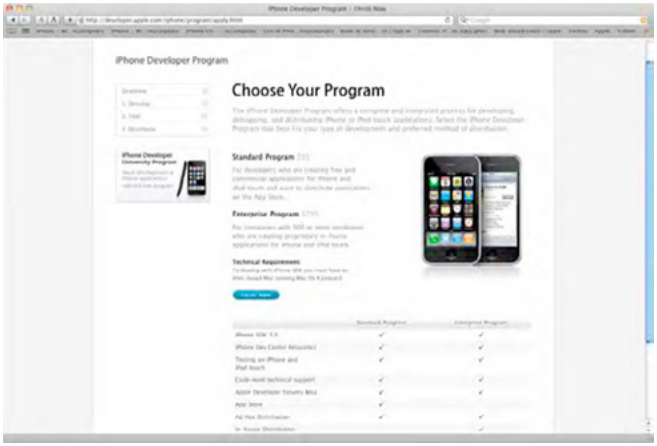


**Figure 1.** *iPhone developer program*

- The first 1024 bytes: Reserved for boot blocks;
- Volume header: The next 1024 bytes are for the volume header, which contains information in regards to the structure of the HFS volume. There is a backup volume header at the last 1024 bytes of the HFS volume. There are also volume header signatures. HFS plus the volume header signature is seen as "H+." For HFSX it is "HX";
- Allocation file: The allocation file simply tracks which allocation blocks are is use by the file system;
- Extents overflow file: This tracks all the allocation blocks that belong to a file's data forks. The contains a list of all extents used by a file and the associated blocks in the appropriate order;
- Catalog file: The HFS+ file system uses a catalog file system to maintain all the information in regards to files and folders within a volume. These are in a hierarchical system of nodes:

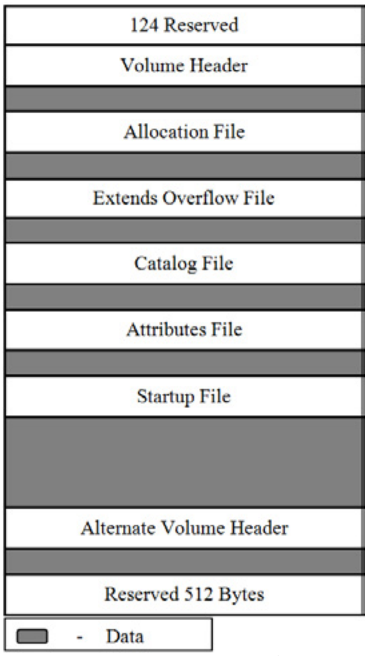
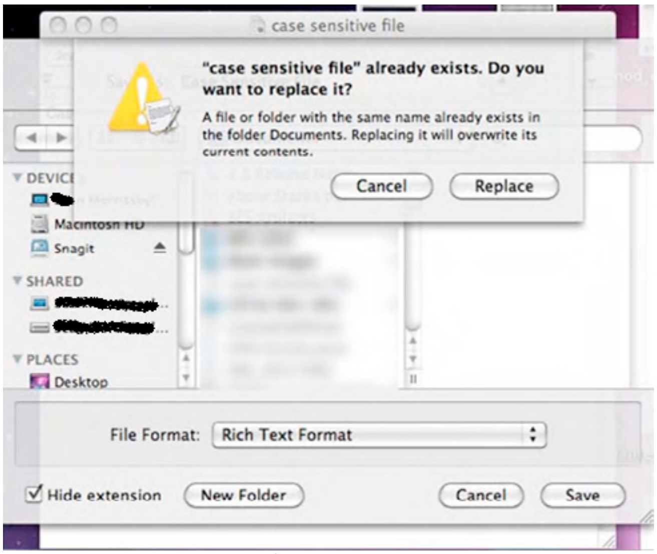

124 Reserved
Volume Header
Allocation File
Extends Overflow File
Catalog File
Attributes File
Startup File
Alternate Volume Header
Reserved 512 Bytes
▨ - Data

**Figure 2.** *The structure of an HFS+ file system*

Header node (The location of the Header node is tracked in the volume header. Within that, the catalog ID number is stored as well. This number is assigned by the catalog file, which gets the next number from the volume header that tracks the last number assigned. The catalog file will increment that number by one and assign it to that file, and is in turn store in the Header node. Attributes file: This file is reserved for future use of data forks; Startup file: This file was designed to assist in booting a system that did not have built-in ROM support; After the startup file: Where all the data in a volume is stored and tracked by the file system; Alternate volume header: A backup of the volume header and is primarily used for disk repair; The last 512 bytes: Reserved.), Index node, Leaf nodes and Map nodes.

In terms of date and time, Apple has used absolute time, otherwise known as local time. UNIX time is used as well. The iOS system utilizes both of these time schemes. Since absolute time does not take into account the differences in time zones, one must be cognizant to identify the location of the system to understand actual the data and time of artifacts.



case sensitive file

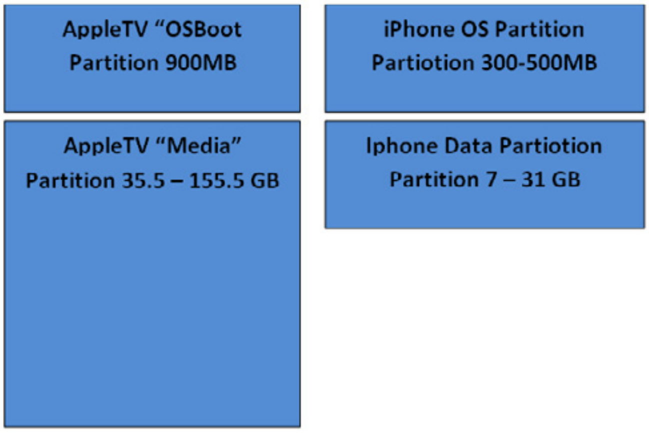
"case sensitive file" already exists. Do you want to replace it?

A file or folder with the same name already exists in the folder Documents. Replacing it will overwrite its current contents.

File Format: Rich Text Format

☑ Hide extension

**Figure 3.** *Error message from saving on an HFS+ system*



AppleTV "OSBoot Partition 900MB

iPhone OS Partition Partiotion 300-500MB

AppleTV "Media" Partition 35.5 – 155.5 GB

Iphone Data Partiotion Partition 7 – 31 GB

**Figure 4.** *The similarities between the iPhone and Apple TV*

Data within the HFS file system utilizes a catalog file system or B*tree (balanced tree) to organize files. This balanced tree uses a catalog file and extents overflows in its organization scheme. B*trees are comprised of nodes. These nodes are grouped together in linear fashion, which makes data access faster. When data is added or deleted, the extents are constantly balanced to keep its efficiency. Each file that is created on an HFS file system is given a unique number – a catalog ID number. The HFS volume header tracks the numbering of the catalog ID and will increment by one each file added. These numbers can be reused, but this is tracked by the HFS volume header.

Typically, the reuse of catalog ID numbers is mainly seen in server environments, where large numbers of files are created. This number is consistently used to bind each node together in a file.

## THE HFSX FILE SYSTEM

All Apple mobile devices use HFSX as the file system. HFSX is a variation of HFS+ with one major difference. HFSX is case sensitive. This means that two files on the file system can have the exact same name – but the case sensitivity is what allows the file system to differentiate between the two. For example: Case sensitive.doc / Case Sensitive.doc

Both of these files can exist on a HFSX file system. On OS X on a desktop or laptop, the following error occurs when the two file names with different cases are attempted to be saved. If the same were attempted on an HFS+ system, the following error will be seen, as shown in Figure 3.

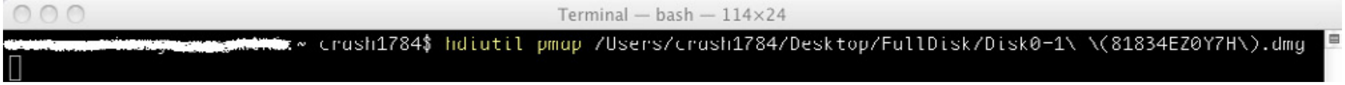
## IPHONE PARTITION AND VOLUME INFORMATION

The partition and volumes of the iPhone also have some history to them. Apple TV, another product of Apple, also came out with a scaled-down version of OS X. It had only one user and two partitions – an OS and data partition. Like the iPhone, Apple TV was designed to hold multimedia and access the Internet and iTunes. AppleTV appears to be a project test bed for HFSX for Apple and the use of a jailed system. Today the new AppleTV now utilizes the HFSX and jailed system of iOS 4. Figure 4 demonstrates the similarities between the iPhone and Apple TV.

## IPHONE PARTITION INFORMATION ACQUISITION

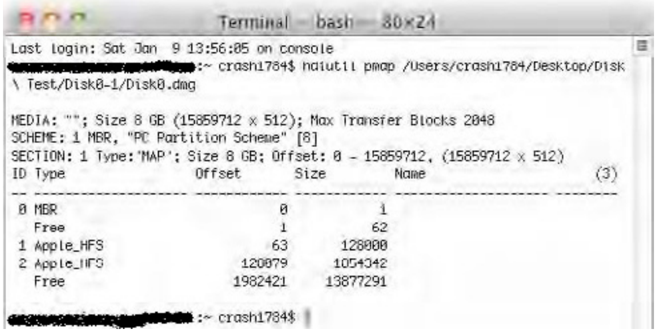
Using two tools on the Mac from the command line, we can see the partition structure of the iPhone. Hdiutil is a command-line binary that is already on the Mac, and there are h the following switches, pmap and imageinfo, which can give the picture of the iPhone.

Hdiutil is a great program for looking at the structure of an iOS system. HDiutil with the option pmap gives an overall view of the partitioning scheme on a device. Hdiutil with the option imageinfo gives a gran-



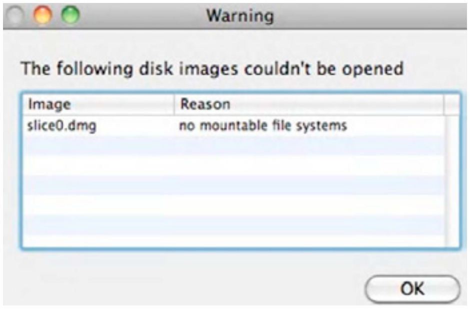
```
[redacted]:~ crash1784$ hdiutil pmap /Users/crash1784/Desktop/FullDisk/Disk0-1\ \(81834EZ0Y7H\).dmg
```

**Figure 5.** *Steps to acquire partition information on the iPhone*



```
Last login: Sat Jan  9 13:56:05 on console
[redacted]:~ crash1784$ hdiutil pmap /Users/crash1784/Desktop/Disk
\ Test/Disk0-1/Disk0.dmg

MEDIA: ""; Size 8 GB (15859712 x 512); Max Transfer Blocks 2048
SCHEME: 1 MBR, "PC Partition Scheme" [8]
SECTION: 1 Type:'MAP'; Size 8 GB; Offset: 0 - 15859712, (15859712 x 512)
ID Type                 Offset       Size         Name                      (3)
-- -------------------- ------------ ------------ -------------------- --------
 0 MBR                             0            1
   Free                            1           62
 1 Apple_HFS                      63       128000
 2 Apple_HFS                  128079      1054342
   Free                      1982421     13877291

[redacted]:~ crash1784$
```

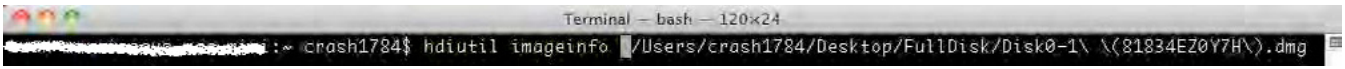
**Figure 6.** *Output of the partition acquisition*



The following disk images couldn't be opened

| Image | Reason |
|---|---|
| slice0.dmg | no mountable file systems |

**Figure 10.** *Error produced when a RAW image of Disk0 is in the mounting process*

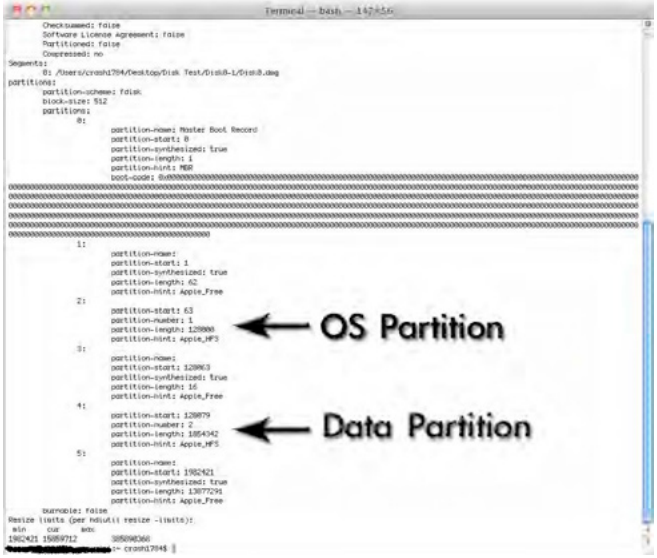


```
[redacted]:~ crash1784$ hdiutil imageinfo /Users/crash1784/Desktop/FullDisk/Disk0-1\ \(81834EZ0Y7H\).dmg
```

**Figure 7.** *Command hdiutil imageinfo*

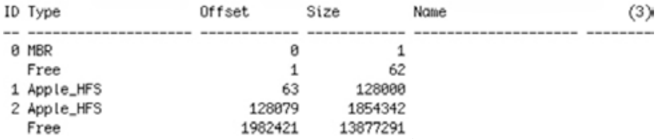
ular look at each partition and information in regards to each. To acquire iPhone partition information:

- Open the Terminal application;
- Navigate to /Applications/Utilities/Terminal. From the command line, type: hdiutil pmap, and then drag and drop an image of the iPhone from the finder to the terminal and press Enter, as depicted in Figure 5. You'll see the output shown in Figure 6.
- Next, from the terminal, type the command: hdiutil imageinfo, and then drag and drop a raw disk image or .dmg and press Enter, as shown in Figure 7. You'll see the output shown in Figure 8.



```
        Checksummed: false
        Software License Agreement: false
        Partitioned: false
        Compressed: no
Segments:
        0: /Users/crash1784/Desktop/Disk Test/Disk0-1/Disk0.dmg
partitions:
        partition-scheme: fdisk
        block-size: 512
        partitions:
                0:
                        partition-name: Master Boot Record
                        partition-start: 0
                        partition-synthesized: true
                        partition-length: 1
                        partition-hint: MBR
                        boot-code: 0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000
                1:
                        partition-name:
                        partition-start: 1
                        partition-synthesized: true
                        partition-length: 62
                        partition-hint: Apple_Free
                2:
                        partition-start: 63
                        partition-number: 1
                        partition-length: 128000
                        partition-hint: Apple_HFS
                3:
                        partition-name:
                        partition-start: 128063
                        partition-synthesized: true
                        partition-length: 16
                        partition-hint: Apple_Free
                4:
                        partition-start: 128079
                        partition-number: 2
                        partition-length: 1854342
                        partition-hint: Apple_HFS
                5:
                        partition-name:
                        partition-start: 1982421
                        partition-synthesized: true
                        partition-length: 13877291
                        partition-hint: Apple_Free
        burnable: false
Resize limits (per hdiutil resize -limits):
 min      cur       max
1982421 15859712        385898368
[redacted]:~ crash1784$
```

**Figure 8.** *Output of the command hdiutil imageinfo*



```
ID Type                 Offset       Size         Name                      (3)
-- -------------------- ------------ ------------ -------------------- --------
 0 MBR                             0            1
   Free                            1           62
 1 Apple_HFS                      63       128000
 2 Apple_HFS                  128079      1854342
   Free                      1982421     13877291
```

**Figure 9.** *Hdiutil reports as the start of each partition*

The previous two images show the partition scheme of the Apple iPhone OS. However, the information from hdiutil is incorrect. If the image were correct, Mac OS would be able to mount the iPhone image. If we look at what hduitil reports as the start of each partition, as shown in Figure 9, the answer becomes clear.

When OS X attempts to mount this volume it sees the first HFS volume at sector 63 and the second HFS volume at 128079. The actual starting sector is as follows: the OS volume header is at sector 504 and the data volume header is at sector 1024632. It is because of the offsets of these volumes that even a Mac cannot mount a Disk0 (the complete raw image of the physical disk) image properly. The disk utility can mount images of either the OS partition (Disk0s1) or data partition (Disk0s2) themselves, without any errors. When a raw image of Disk0 is in the process of mounting, the following error shown in Figure 10 occurs.

However, if the gathered .dmg of the whole raw disk was copied, the offsets can be corrected and the image can be mounted properly. Creating a plug-in for MacFUSE can assist in allowing the Mac OS to properly mount the complete Disk0. Information in regards to creating a plug-in can be found at *http://code.google.com/p/macfuse.*

## OS PARTITION

The OS partition is a read-only volume. This can be seen by following the path located at private/etc/fstab. Open the fstab file with TextEdit, and the following information is then shown in Figure 11.

As on all Macs, the partitions are divided in into disks and slices. The RAW disk is "Disk0." There is only one disk on the iPhone, hence you see Disk0. The OS partition is "Disk0s1" and the Data partition is "Disk0s2." Next you see both partitions from Figure 11, and the `/dev/disk0s1` and then `/hfs` denoting an HFS volume after that. Next to hfs is ro. This means that the volume is read-only. The data partition `/dev/Disk0s2` is a read/write HFS volume. Due to the fact that the system partition is read-only, all the data that is on this volume is usually non-evidentiary unless the phone has been jailbroken.

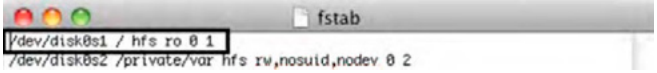
The relevance of this file is that if you see `/dev/disk0s1 /hfs` rw, the system has been jailbroken. This is a good artifact to use to validate if an imaging process has tampered with the UNIX jail of the iDevice system.

## IOS SYSTEM PARTITION

The system partition shown in Figure 12 is of the iOS device described in Table 1. The contents of this partition are usually non-evidentiary; however, sometimes an examination could be necessary.

The path `private/etc/passwd` is the password file of the OS. Tools like John the Ripper, which can be downloaded at *www.openwall.com/john/*, allow for cracking the root and mobile passwords. The root and mobile passwords are encrypted using a DES algorithm that requires a 2 character salt key and an 8 character text password, which yields an 11 character value. With jailbroken iPhones, a more advanced user can change these passwords. A password for root that has never changed since the first iPhone is "Alpine," as shown in Figure 13.

Due to the design of the iPhone, there are procedures that can break the phone or use copyrighted software to bypass the security measures in order to image an iPhone. As will be discussed in this article, there are numerous areas of investigation that will maintain the integrity of the evidence and still locate valuable artifacts and secure convictions. For each firmware version, the OS partition



```
/dev/disk0s1 / hfs ro 0 1
/dev/disk0s2 /private/var hfs rw,nosuid,nodev 0 2
```

**Figure 11.** *Opening the fstab file in TextEdit*

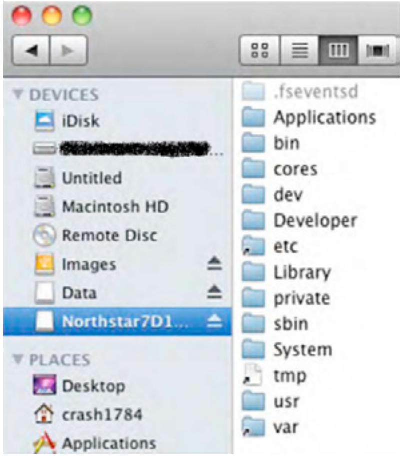
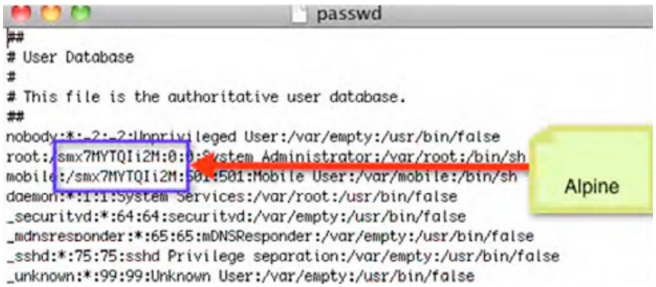


**Figure 12.** *iOS system partition*



```
##
# User Database
#
# This file is the authoritative user database.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:/smx7MYTQIi2M:0:0:System Administrator:/var/root:/bin/sh
mobile:/smx7MYTQIi2M:501:501:Mobile User:/var/mobile:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_securityd:*:64:64:securityd:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false
_sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
_unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false
```

**Figure 13.** *The password Alpine*

**Table 1.** *System partition of the iOS device*

| Directory | Description |
|---|---|
| `Application` | Has symbolic links that point to the `/var/stacsh` directory |
| `Etc` | Has a symbolic link to `/private/etc` |
| `Tmp` | Has a symbolic link to |
| `User` | Has a symbolic link |
| `Var` | Has a symbolic link to `/private/var` |
| `Damaged files` | Can contain artifacts of a previous jailbreak |
| `Bin` | Contains one command-line binary, launchctl |
| `Cores` | Empty |
| `Dev` | Empty |
| `Developer` | Empty |
| `Library` | As with any OS X system, contains system plug-ins and settings:<br>`Application support`: Bluetooth models and PIN codes<br>`Audio`: Contains the audio plug-in<br>`Cashes`: Empty<br>`File systems`: Empty<br>`Internet Plug`: Empty<br>`LaunchAgents`: Empty<br>`LaunchDaemons`: Empty<br>`Manager Preferences`: Contains a symbolic link to Mobile<br>`Printers`: Empty<br>`Ringtones`: Contains system-installed ringtones<br>`Updates`: Empty<br>`Wallpaper`: Contains numerous PNG files and thumbnails (non-evidentiaty) |
| `private` | Contains the `Etc` and `Var` folders:<br>`Etc`: Contains fstab.master.passwd, passwd files (both master and passwd: same)<br>`Var`: Empty |
| `sbin` | Contains command-line binaries |
| `System` | Library folder that contains system preferences and settings; includes `/System/Library/CoreService/SystemVersion.plist`: Firmware Version |
| `Usr` | Contains more command-line binaries and time zone data |

has volume names that correspond to the iOS version. Table 2 shows the iOS version (from 1.00 to 4.1) and the corresponding volume name of the OS system partitions.

## IOS DATA PARTITION

Over the years, there has been little change in the makeup of this data partition. You can see some of the changes in the file system from logical acquisitions. The bulk of the evidence that can be acquired from this device comes from the read/write partition, also known the data partition, as shown in Figure 14 and the Table 3 shows the directories and accompanying items of interest.

**Table 2.** *iOS version and corresponding volume name*

| iOS Version | Volume Name | iOS Version | Volume Name |
|---|---|---|---|
| 1.00 | Alpine 1A420 | 3.1.2 | Northstar 7D11 |
| 1.0.0 | Heavenly 1A543a | 3.1.3 | SUNorthstarTwo 7E18 |
| 1.0.1 | Heavenly 1C25 | 2.00 | Big Bear 5A345 |
| 1.0.2 | Heavenly 1C28 | 2.00 | Big Bear 5A347 |
| 1.1.1 | Snowbird 3A109a | 2.0.1 | Beg Bear 5B108 |
| 1.1.2 | Oktoberfest 3B48b | 2.0.2 | Big Bear 5C1 |
| 1.1.3 | Little Bear 4A93 | 2.1 | Sugar Bowl 5F136 |
| 1.1.4 | Little Bear 4A102 | 2.2 | Timberline 5G77 |
| 2 | Big Bear 5A347 | 2.2.1 | SUTimberline 5H11 |
| 2.0.1 | Big Bear 5B108 | 3.00 | Kirkwood 7A341 |
| 2.0.2 | Big bear 5C1 | 3.0.1 | Kirkwood 7A400 |
| 2.1 | Sugar Bowl 5F136 | 3.1 | Northstar 7C144 |
| 2.2 | Timberline 5G77 | 3.1.2 | Northstar 7D11 |
| 2.2.1 | SYTimberline 5H11 | 3.1.3 | SUNorthstarTwo 7E18 |
| 3 | Kirkwood 7A341 | 3.2 | Wildcat7B367 |
| 3.0.1 | Kirkwood 7A400 | 4.0 | Apex8A306 |
| 3.1 | Northstar 7C144 | 4.1 | Baker8B177 |

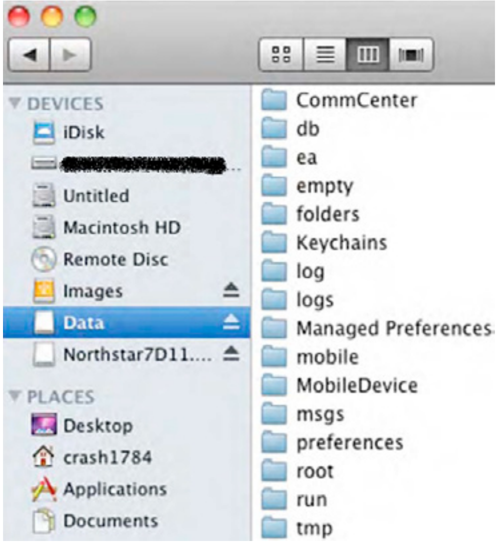


**Figure 14.** *Data partition directory structure*

The data partition is riddled with a lot of information that will assist in any investigation. When an Apple device gets backed up from iTunes, it gathers information from the Mobile directory. Table 4 shows all the artifacts that are acquired logically and items that are also stored as backups on a Mac or PC.

## SQLITE DATABASES

The iDevice OS uses the SQLite database format to store information on the phone. An examination

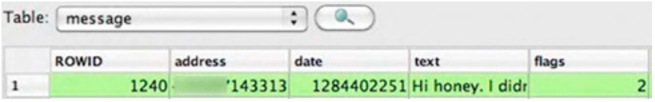


Table: message

|  | ROWID | address | date | text | flags |
|---|---|---|---|---|---|
| 1 | 1240 | [redacted]'143313 | 1284402251 | Hi honey. I didr | 2 |

**Figure 15.** *The ROWID, address, date, text and flags*

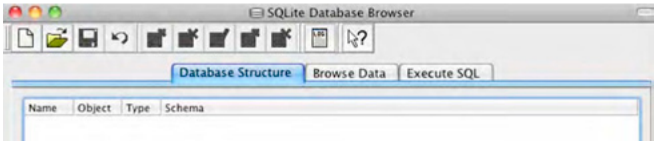


**Figure 16.** *The Interface of the SQLite Database Browser Application*

**Table 3.** *Directories and corresponding items of interest*

| Directory | Items of Interest |
|---|---|
| `CommCenter` | No artifacts |
| `Dhcpclient` | One plist that contains the last IP address and router information for that device |
| `db` | No artifacts |
| `Ea` | Empty |
| `Folders` | Empty |
| `Keychains` | `Keychain.db`, which contains user passwords from various applications |
| `Log` | Empty |
| `Logs` | `General.log`: The OS version and serial number<br>`Lockdown.log`: Lockdown deamon log |
| `Manager Preferences` | Empty |
| `Mobile` | Bulk of the user data |
| `MobileDevice` | Empty |
| `Preferebces` | `System configuration`: Network artifacts backed up |
| `Root` | `Caches`: GPS location information<br>`Lockdown`: Pairing certificates<br>`Preferences`: No artifacts |
| `Run` | System log |
| `tmp` | `Manifest.plist`: plist backup |
| `Vm` | Empty |

of the logical extraction shows numerous SQLite databases for the operation of the phone and by developers of applications. The iPhone also uses these databases to cross-reference information

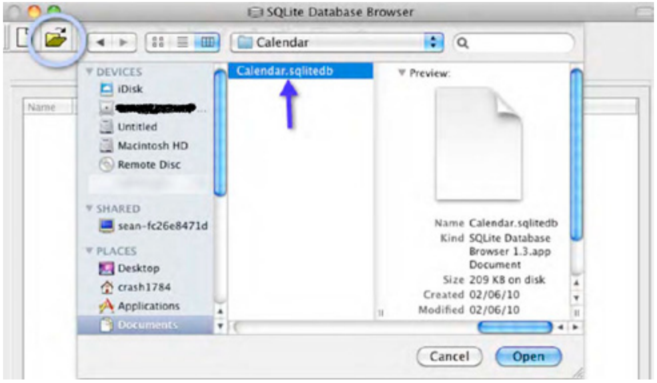


**Figure 17.** *Adding SQLite database browser*

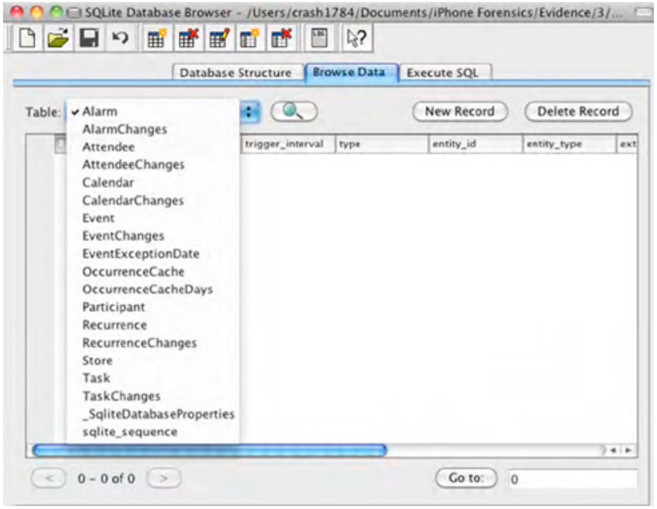


**Figure 18.** *Moving to the browse data tab and picking the table to review*

**Table 4.** *Artifacts organized by directory and whether they are in backup*

| Directory | In Backup | Artifact |
|---|---|---|
| `Mobile/Application` | + | Plists, SQLite databases |
| `Library/AddressBook` | + | Contacts and images |
| `Library/Caches` | | SQLite database: MapTiles |
| `Library/Calendar` | + | SQLite database: Events |
| `Library/CallHistory` | + | SQLite database: Call logs |
| `Library/Carrier Bundles` | | Carrier information |
| `Library/Caches/Com.apple.itunesstored` | | iTunes purchase information |
| `Library/ConfigurationProfiles` | + | Plist password history |
| `Library/Cookies` | + | Plist: Internet cookies |
| `Library/DataAccess` | + | E-mail account information |
| `Library/Keyboard` | + | .dat file: Dynamic text |
| `Library/Logs` | + | Log files |
| `Library/Mail` | + | In Logical Data, no artifacts |
| `Library/Maps` | + | Plist: Bookmarks, directions, history |
| `Library/Mobileinstallation` | + | Applications that use Locations |
| `Library/Notes` | + | SQLite database: Notes |
| `Library/Preferences` | + | Plist System and user settings |
| `Library/RemoteNotification` | + | Plist: Apps that have push notification |
| `Library/Safari` | + | Plist: Bookmarks, history |
| `Library/SafeHarbour` | | Location of where app data is stored |
| `Library/SMS` | + | SMS and MMS data |
| `Library/Voicemail` | + | .arm files: Voice messages |
| `Library/Webclips` | | |
| `Library/Webkit` | + | SQLite databases: Gmail account info, caches e-mail messages |
| `Media/DCIM` | + | iPhone camera photos |
| `Media/PhotoData` | + | Additional photo information and thumbnails |
| `Media /iTunes _ Control` | | Music and video from iTunes |
| `Media/Books` | | Books from the iBookstore and synced PDFs |

from one database to the other, which gets displayed on the UI. These databases interact with each other to give the user an informative experience. The big three databases are the Address Book, SMS, and Call History databases.

## ADDRESS BOOK DATABASE

This database has 18 tables. Table 5 provides the information that would be relevant in an investigation.

## SMS DATABASE

The SMS database is the container that keeps records of text messages sent and received by the Messages application. Table 6 shows the tables that make up this database.

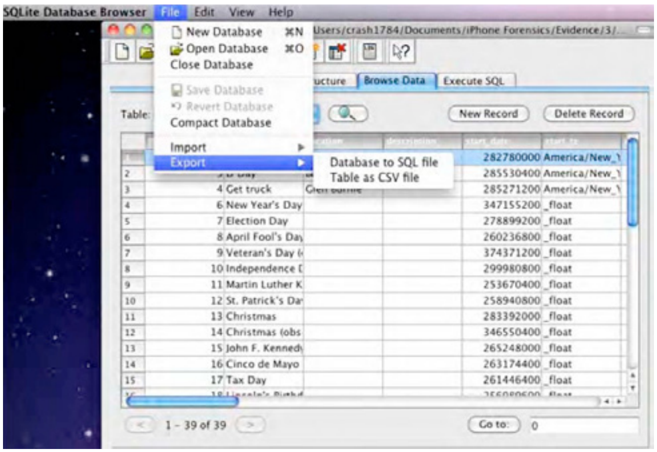
In Figure 15, you can see the ROWID (row identification), which is a number for the message, the address (the phone number that the text came from), and the date and time of the text. The date and time values are in Unix time and can be converted using several free tools. The flags are for sent and received text messages.

**Table 5.** *The address book database*

| Table | Relevant Data |
|---|---|
| `AB Group` | Group information |
| `ABGroupChanges` | Non-evidentiary |
| `ABGroupMembers` | Contacts associated each group |
| `ABMultiValue` | When a contact has multiple values, phone numbers, e-mail address books, company URLs, etc. |
| `ABMultiValueEntry` | Street addresses for contacts |
| `ABMultiValueEntryKey` | Non-evidentiary |
| `ABMultiValueLabel` | Non-evidentiary |
| `ABPerson` | Name, organization, department, notes, etc. |
| `ABPersonChanges` | Non-evidentiary |
| `ABPersonMulti ValueDeletes` | Non-evidentiary |
| `ABPersonSearchKey` | Non-evidentiary |
| `ABPersonSearchKey` | Non-evidentiary |
| `ABPhoneLastFour` | Non-evidentiary |
| `ABRecent` | Recently used e-mail addresses |
| `ABStore` | Non-evidentiary |
| `RirstSortSectionCount` | Non-evidentiary |
| `FirstSortSectionCount` | Non-evidentiary |
| `_ SqliteDatabase Properties` | Non-evidentiary |
| `Sqlite _ sequence` | Non-evidentiary (but contains good information on the structure of the database) |

**Table 6.** *The tables and relevant data of the SMS database*

| Table | Relevant Data |
|---|---|
| `_ SqliteDataBase Properties` | Contains database properties (non-evidentiary) |
| `Group _ member` | Assigns an incoming text a group ID that then will pull all the text messages from the iPhone owner ans the party having the conversation |
| `Message` | Contains the content of the message, date and time, and whether the message was sent or received; also lists the associated group ID |
| `Msg _ group` | Gives the group ID and ID of the last message in that group |
| `Msg _ Pieces` | Tracks all MMS messages |
| `Sqlite _ sequence` | Provides a sequestial list of all tables in the database |



| | | | |
|---|---|---|---|
| 1 | | 282780000 | America/New_Y |
| 2 | | 285530400 | America/New_Y |
| 3 | 4 Get truck | 285271200 | America/New_Y |
| 4 | 6 New Year's Day | 347155200 | _float |
| 5 | 7 Election Day | 278899200 | _float |
| 6 | 8 April Fool's Day | 260236800 | _float |
| 7 | 9 Veteran's Day ( | 374371200 | _float |
| 8 | 10 Independence [ | 299980800 | _float |
| 9 | 11 Martin Luther K | 253670400 | _float |
| 10 | 12 St. Patrick's Da | 258940800 | _float |
| 11 | 13 Christmas | 283392000 | _float |
| 12 | 14 Christmas (obs | 346550400 | _float |
| 13 | 15 John F. Kenned | 265248000 | _float |
| 14 | 16 Cinco de Mayo | 263174400 | _float |
| 15 | 17 Tax Day | 261446400 | _float |

**Figure 19.** *The CSV format can be opened in other Applications*

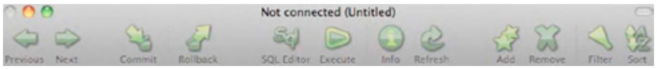
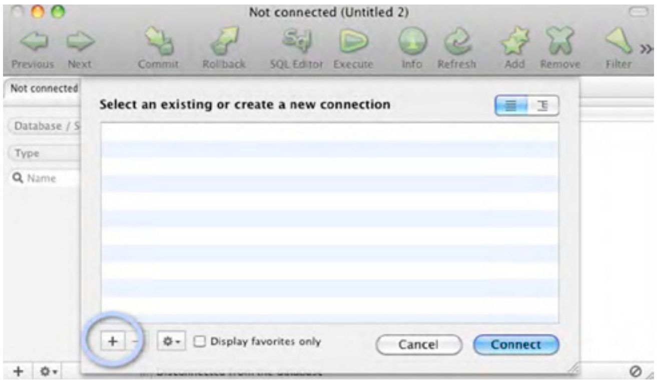


**Figure 20.** *The Froq interface*



Select an existing or create a new connection

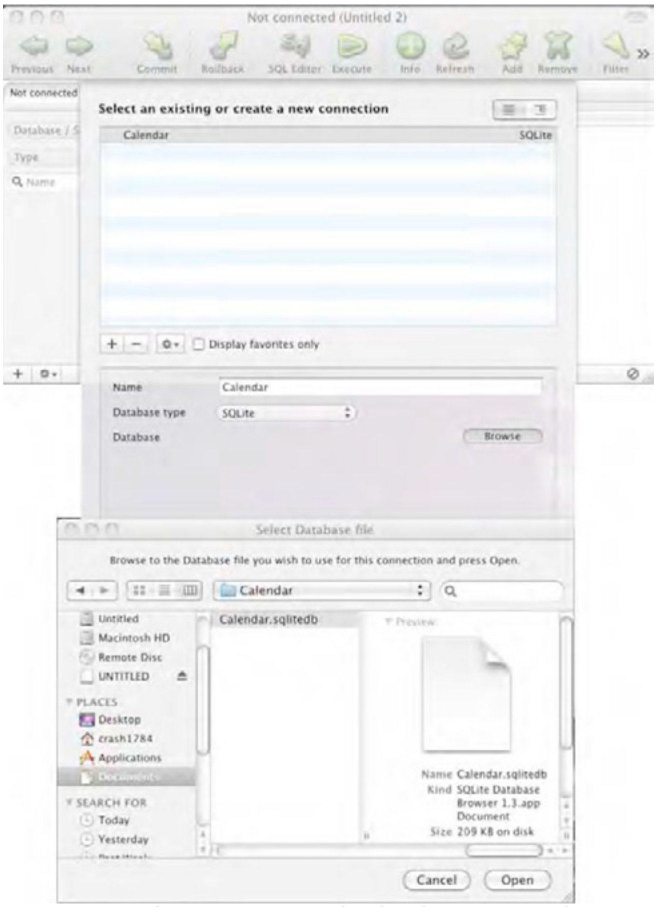
**Figure 21.** *Creating a new connection*

## CALL HISTORY DATABASE

The Call History database is a simpler database, and the only one that has restrictions – it will only hold 100 calls. The Address Book database is the hub of a lot of other applications on the iDevice. A lot of data correlation occurs between this database and others. For example, the Call History database correlates the numbers from the sent and/or received call with the names associated with those numbers in the Address Book database. Table 7 describes the tables and artifacts of relevance.

**Table 7.** *Tables and relevant data artifacts*

| Table | Relevant Data |
|---|---|
| `SqliteDatabaseProperties` | |
| `Call` | Contains phone numbers, date and time info, and the duration of the call; also flags incoming, outgoing, and missed calls, and calls that have voicemails |
| `Data` | Tracks the number of bytes the iPhone has sent and received |
| `Sqlite _ sequence` | Contains a sequential list of tabled in the database |



Not connected (Untitled 2)

Select an existing or create a new connection

| Calendar | SQLite |
|---|---|

☐ Display favorites only

Name: Calendar
Database type: SQLite
Database

Select Database file

Browse to the Database file you wish to use for this connection and press Open.

Calendar.sqlitedb

Name Calendar.sqlitedb
Kind SQLite Database Browser 1.3.app Document
Size 209 KB on disk

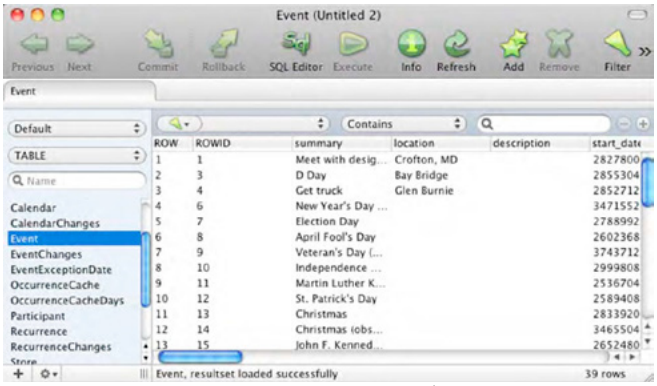
**Figure 22.** *Selecting SQLite as the database type and browsing to the relevant one*

## RETRIEVING DATA FROM SQLITE DATABASES

There are applications that can assist in extracting data from SQLite databases that can be used in other applications or tools. One of these SQLite database applications is SQLite Database Browser. The interface of this application is shown in Figure 16.

To add SQLite Database Browser, click the Open icon and navigate to the relevant database, as shown in Figure 17.

After the relevant database is brought into SQLite Database Browser, one can browse through the tables in the database. First move to the Browse

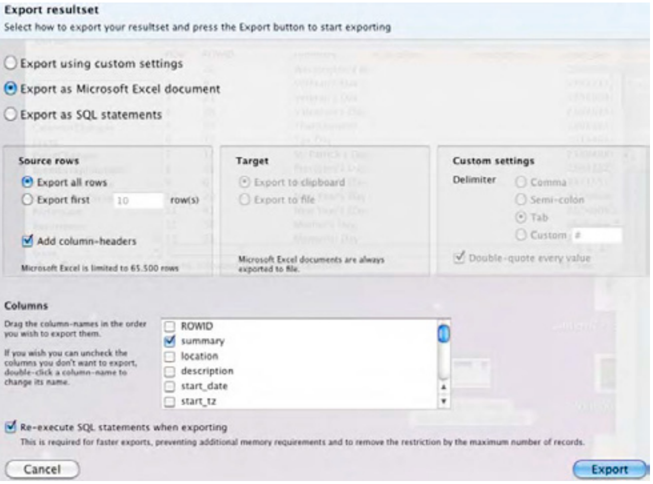


Event (Untitled 2)

| ROW | ROWID | summary | location | description | start_date |
|---|---|---|---|---|---|
| 1 | 1 | Meet with desig... | Crofton, MD | | 2827800 |
| 2 | 3 | D Day | Bay Bridge | | 2855304 |
| 3 | 4 | Get truck | Glen Burnie | | 2852712 |
| 4 | 6 | New Year's Day ... | | | 3471552 |
| 5 | 7 | Election Day | | | 2788992 |
| 6 | 8 | April Fool's Day | | | 2602368 |
| 7 | 9 | Veteran's Day (... | | | 3743712 |
| 8 | 10 | Independence ... | | | 2999808 |
| 9 | 11 | Martin Luther K... | | | 2536704 |
| 10 | 12 | St. Patrick's Day | | | 2589408 |
| 11 | 13 | Christmas | | | 2833920 |
| 12 | 14 | Christmas (obs... | | | 3465504 |
| 13 | 15 | John F. Kenned... | | | 2652480 |

Event, resultset loaded successfully — 39 rows

**Figure 23.** *Database brought into Froq for analysis*



Export resultset

Select how to export your resultset and press the Export button to start exporting

○ Export using custom settings
● Export as Microsoft Excel document
○ Export as SQL statements

Source rows
● Export all rows
○ Export first 10 row(s)
☑ Add column-headers
Microsoft Excel is limited to 65.500 rows

Target
● Export to clipboard
○ Export to file
Microsoft Excel documents are always exported to file.

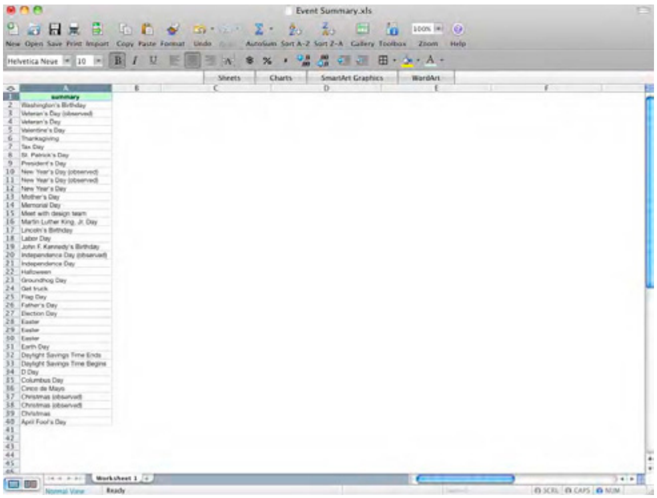
Custom settings
Delimiter ○ Comma ○ Semi-colon ● Tab ○ Custom #
☑ Double-quote every value

Columns
Drag the column-names in the order you wish to export them.
If you wish you can uncheck the columns you don't want to export, double-click a column-name to change its name.

☐ ROWID
☑ summary
☐ location
☐ description
☐ start_date
☐ start_tz

☑ Re-execute SQL statements when exporting
This is required for faster exports, preventing additional memory requirements and to remove the restriction by the maximum number of records.

**Figure 24.** *"Export Resultset" screen*



Event Summary.xls

| | A |
|---|---|
| 1 | summary |
| 2 | Washington's Birthday |
| 3 | Veteran's Day (observed) |
| 4 | Veteran's Day |
| 5 | Valentine's Day |
| 6 | Thanksgiving |
| 7 | Tax Day |
| 8 | St. Patrick's Day |
| 9 | President's Day |
| 10 | New Year's Day (observed) |
| 11 | New Year's Day (observed) |
| 12 | New Year's Day |
| 13 | Mother's Day |
| 14 | Memorial Day |
| 15 | Meet with design team |
| 16 | Martin Luther King, Jr. Day |
| 17 | Lincoln's Birthday |
| 18 | Labor Day |
| 19 | John F. Kennedy's Birthday |
| 20 | Independence Day (observed) |
| 21 | Independence Day |
| 22 | Halloween |
| 23 | Groundhog Day |
| 24 | Get truck |
| 25 | Flag Day |
| 26 | Father's Day |
| 27 | Election Day |
| 28 | Easter |
| 29 | Easter |
| 30 | Easter |
| 31 | Earth Day |
| 32 | Daylight Savings Time Ends |
| 33 | Daylight Savings Time Begins |
| 34 | D Day |
| 35 | Columbus Day |
| 36 | Cinco de Mayo |
| 37 | Christmas (observed) |
| 38 | Christmas (observed) |
| 39 | Christmas |
| 40 | April Fool's Day |

**Figure 25.** *Exported data viewed in Excel*

Data tab and then pick the table to review from the Table drop-down list. This is shown in Figure 18.

The data can be exported from SQLite Database Browser to a CSV (Comma Separated Value) format, which in turn can be opened with applications such as Microsoft Excel, as shown in Figure 19.

Another application worth mentioning is Froq, developed by Alwin Troost. This application is proprietary and can be purchased at *www.alwintroost.nl/?id=82*. This application has a lot of functionality and is an excellent tool for viewing the tables of a database and exporting the portions of the database needed for a given investigation. The interface of Froq is shown in Figure 20. To view a database of interest, perform the following steps:

- Go to the Froq menu bar and select connect | connect;
- The next box will ask you to select an existing connection or create a new one. Select a new connection by clicking the +, as shown in Figure 21;
- In the expanded window, give the connection a name – for example, Calendar;
- For the database type, select SQLite;
- From the Browse tab, navigate to the relevant database. (Steps 4 and 5 are shown in Figure 22);
- Then the database will be brought into Froq for analysis. The tables can be selected from the left pane, and the data can be seen in the right pane, as shown in Figure 23. To export data from this application, return to the top toolbar;
- Select Resultset | Export;
- There are three types of settings: Custom, export as an excel spreadsheet, or as SQL statements;
- Under the columns, you can be as granular as necessary for the data that is required. For example, select "Export as Microsoft Excel document." Then select the "Export all rows" radio button from the "Source rows" section, and select the columns needed;
- Then select "Export." The resulting screen is shown in Figure 24;
- After the data is exported, it can be viewed in Excel, as shown in Figure 25.

## PROPERTY LISTS

Property lists are XML files that are commonly seen in standard OS X systems. Since iOs is a modified

**Table 8.** *Property lists and relevant data directory property lists and artifacts*

| Directory | Property Lists and Artifacts |
|---|---|
| Db | |
| Keychain | |
| Managed preferences | Com.apple.sprongboard.plist: Add artifact |
| Mobile/library/Cookies | Cookies.plist: Web-related artifacts |
| Mobile/Library/Mail | Accounts.plists: E-mail accounts<br>Metadata.plist: Dates and times of e-mail puuls |
| Mobile/Library.Maps | Bookmarks.plist: Map bookmarks created by the user<br>History.plist: All routes and searches |
| Mobile/Library/Preferences | Com, apple.BTserver,airplane.plist: Shows that airplane mode was initiated on the device for Bluetooth<br>Com.apple.commcenter,plist: Stores ICCID and IMSI numbers<br>Com.apple.maps.plist: Recent map searches and last latitude and longitude of last map tile seen<br>Com.apple.mobilephone.settings.plist: Call-forwarding numbers<br>Com.apple.mobilephone.speeddial.plist: All favorite contacts for speed dial<br>Com.apple.mobilesafari.plist: Recent Safari searches<br>Com.apple.MobileSMS.plist: Any unset SMS messages<br>Com.apple.mobiletimer.plist: List of world clocks used<br>Com.apple.preference.plist: Keyboard language last used<br>Com.apple.springboard.plist: Lists of apps that are shown in the interface, password protection flag, wipe enable settings, last system version<br>Com.apple.weather.plist: Cities for weather reports, date and time of last update<br>Com.apple.youtube.plist: URLs of all videos bookmarked, history of all video watched, videos searched by user |
| Library/Safari | Bookmarks.plist: all Internet bookmarks – created and standard<br>History.plist: Web browsing history<br>Suspendedstate.plist: Web page title ans URL of all suspended web paged that are held in the background so that users can jump from one page to another easily (a maximum of eight pages can be saved at one time) |

OS X system, it stands to reason that we will also see property lists within the directory structure. The iOS data partition is riddled with property lists that can contain valuable information. Table 8 shows the property lists that contain data of relevance.

## VIEWING PROPERTY LISTS

Apple has given examiners a free tool to view property lists, the Property List Editor (also known as the plist) The Property List Editor is part of the developer tools, and is an optional install on the OS X installation disk. The newest versions can be downloaded from the Apple Developers web site, at *http://developer.apple.com/technologies/tools*. The Property List Editor can display these XML-formatted files in a readable manner, similar to how they are viewed on a Windows system (i.e., not in their raw form). Once the Property List Editor has either been installed from the OS X disk or downloaded from the Internet, the following steps can be followed to view a given property list:

- Navigate to /Developer/Applications/Utilities/Property List Editor;
- Double-click the application;
- From the Property list file menu, select Open;
- Next, navigate to the location of the plist you wish to view;
- Select the plist;
- Press the Open button;
- View the artifacts from the plist editor interface.

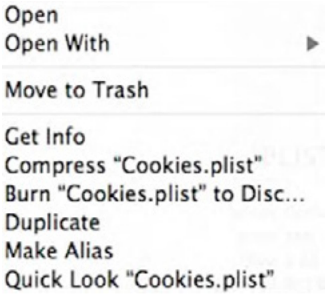
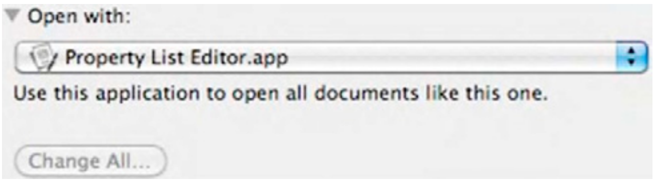


**Figure 26.** *Select "Get Info" from this drop-down menu*


Open with:

Property List Editor.app

Use this application to open all documents like this one.

**Figure 27.** *Expand the "Open with" portion of the window*

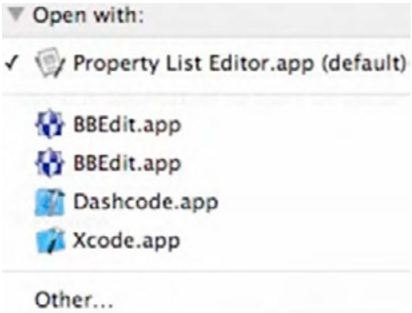


**Figure 28.** *Select other*

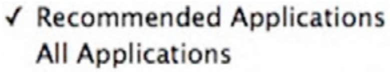
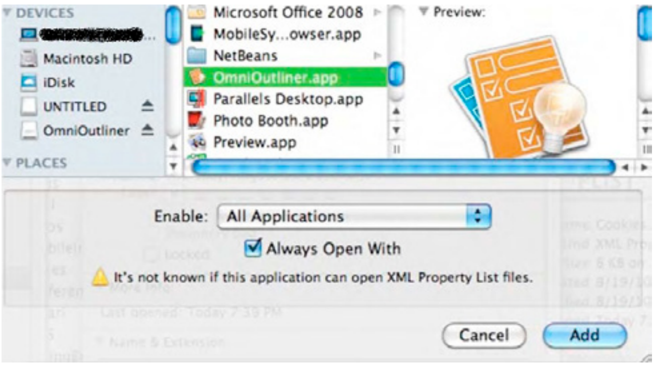


**Figure 29.** *Change "Recommended Applications" to "All Applications"*

The one thing that detracts from this free tool is the way it reports the artifacts. One can grab screenshots of the relevant data and add those images to a report. There is another application, OmniOutliner 3, an app bundled with OS X 1.4 (Tiger). It is a for-pay app, and it's available at *www.omnigroup.com/products/omnioutliner*. You can use this tool to view plists easily bring them into an existing report. The following describes how to view and report plists with OmniOutliner 3.

First you have to set up your Mac so that you can automatically open all plists with OmniOutliner.

- From Finder, find any plist on your volume (Library/Preferences is a good choice);
- Right-click the plist;
- Select Get Info, as shown in Figure 26;
- From the Get Info dialog box, expand the "Open with" portion of the window (shown in Figure 27);
- Now click the drop-down list and select Other, as shown in Figure 28;
- The next window will be another finder window in the application directory. You will have to change Recommended Applications to All Applications, as shown in Figure 29;



Enable: All Applications

☑ Always Open With

It's not known if this application can open XML Property List files.

**Figure 30.** *Select "Always Open With"*

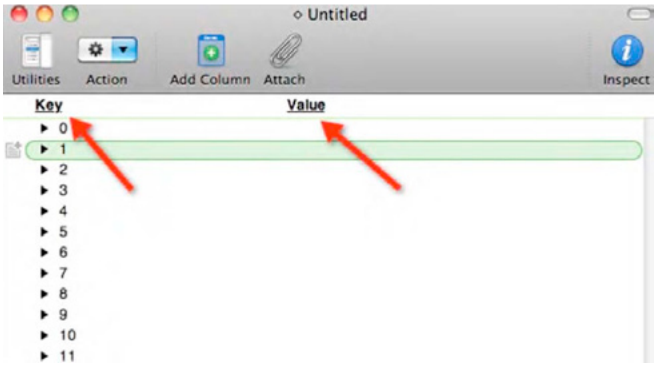
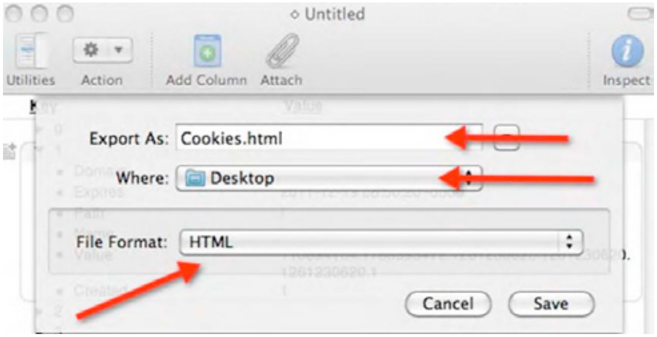


**Figure 31.** *Separate key and value columns*



Export As: Cookies.html
Where: Desktop
File Format: HTML

**Figure 32.** *Choose a file name, where to save the file and the file format*

- Then locate OmniOutliner and highlight the application;
- Then select the Always Open With box, and click the Add button, as shown in Figure 30 (all property lists will automatically open with OmniOutliner instead of the Property List Editor. If you wish to switch back to the Property List Editor, repeat the same steps, but select Property List Editor instead. Now that you have switched to OmniOutliner, the next steps will go through using OmniOutliner);
- Select a property list to examine and double-click the file. OmniOutliner will automatically open the plist.
- The values are separated into Key and Value columns, as shown in Figure 31.
- To expand all the keys, go to the menu bar and select View | Expand All. Now you'll be able to view all the keys and values.
- To report data from Omni Outliner
  - Either expand all or just the items of relevance;
  - Then go to the menu bar and select File | Export;
  - Enter a file name, where you want the file saved, and what format to export it in, as shown in Figure 32.

## CONCLUSIONS

The iOS operating and file systems have changed since its introduction in 2007. Since then the Apple device family has expanded and changed the way we communicate and now how we compute, it is important to understand the inner workings of the devices to intelligently articulate some of the processes that are accomplished to facilitate artifact extraction.

As shown in this article, there can be a mountain of data that can be captured from the devices. In this article, we reviewed the history of the iOS operating and file system, and artifacts that reside in the system and data partitions. We also looked at tools that can examine many of the artifacts that are on any iDevice. As we saw, most of the evidence on the iDevice is stored in SQLite databases and property lists.

### About the Author

*Deivison Pinheiro Franco is Graduated in Data Processing. Specialist in Computer Networks, in Computer Networks Support and in Forensic Sciences (Emphasis in Forensic Computing). Security Analyst of Bank of Amazônia. Professor at various colleges and universities of disciplines like: Computer Forensics, Information Security, Systems Audit, Computer Networks, Computer Architecture and Operating Systems. Computer Forensic Expert, IT Auditor and Pentester with the following certifications: CEH – Certified Ethical Hacker, CHFI – Certified Hacking Forensic Investigator, DSEH – Data Security Ethical Hacker, DSFE – Data Security Forensics Examiner, DSO – Data Security Officer and ISO/IEC 27002 Foundation.*

### About the Author

*Nágila Magalhães Cardoso is graduated in Computer Networks Technology and Specialist in Computer Security. Certified in network administration and technical in computer installation, maintenance and installation of computer networks. Panelist and professor of free computer courses in the areas of information technology and computer networks, with special knowledge in computer security and forensics.*

## REFERENCES

- Elmer-Dewitt, P. (2008, May, 16). iPhone Rollout: 42 Countries, 575 million potential customers. Fortune. Retrieved March 30, 2009 from *http://apple20.blogs.fortune.cnn.com/2008/05/16/iphone-rollout-42-countries-575-million-potential-customers/*
- Farley, T. (2007). The Cell-Phone Revolution. American Heritage of Invention and Technology. Retrieved March 24, 2009, from *www.americanheritage.com/events/articles/web/20070110-cell-phone-att-mobile-phone-motorola-federal-communications-commission-cdma-tdmagsm.shtml*.
- Fletcher, F. E., & Mow, L. C. (2002). What's happening with E-911? The Voice of Technology. Retrieved April 2, 2009, from *www.drinkerbiddle.com/files/Publication/d6e48706-e421-411c-ab6f-b4fa132be026/Presentation/PublicationAttachment/fdb0980a-7abf-40bf-a9cd-1b7f9c64f3c7/WhatHappeningWithE911.pdf*
- Hafner, K. (2007, July 6). iPhone futures turn out to be a risky investment. The New York Times, p. C3.
- Henderson, S. (2006). Learning from all fifty states: how to apply the fourth amendment and its state analogs to protect third party information from unreasonable search. The Catholic University Law Review, 55, 373.
- Kerr, O. (2004). The fourth amendment and new technologies: constitutional myths and the case for caution. Michigan Law Review, 102, 801.
- Krazit, T. (2009). Apple ready for third generation iPhone. Retrieved March 30, 2009, from *http://news.cent.com/apple-ready-for-third-generation-of-iphone/*
- Morrissey, Sean. (2010) iOS Forensic Analysis: for iPhone, iPad and iPod Touch. New York, NY: Apress.
- Roberts, M. (2007, July 25). AT&T profit soars: iPhone gives cell provider a boost. Augusta Chronicle, p. B11.
- Stillwagon, B. (2008). Bringing an end to warrantless cell phone searches. Georgia Law Review, 42, 1165.
- Walsh, D., & Finz, S. (2004, August 26). The Peterson trial: defendant lied often, recorded calls show, supporters mislead about whereabouts. San Francisco Chronicle, p. B1.

# PLACING THE SUSPECT BEHIND THE KEYBOARD

## CAN YOU PLACE THE SUSPECT AT A KEYBOARD WITH ONLY A DIGITAL FORENSICS ANALYSIS?

**by Brett Shavers**

Perhaps the most important and nearly impossible task in digital forensics is placing the suspect behind the keyboard. Digital evidence alone doesn't do it. Assumptions and preconceived beliefs don't do it. Luckily, most cases involving digital forensics are solved without having to physically place the suspect at the machine. Unfortunately, there are those cases in which the suspect does not admit to using the device or there is no other evidence proving it.

**What you will learn:**

- How to consider all types of evidence in your forensic analysis
- How to think beyond the data found on the hard drive
- Avoiding mistakes of chasing wrong leads
- Putting a complete case together, more than just a forensics analysis report

**What you should know:**

- Digital forensics processes and methodology
- Investigative (inquisitive) techniques or mindset
- Putting a case together is not just zeros and ones, but telling a complete story

Besides anonymous cyber-intrusions, in many criminal and civil cases where electronic media is involved, the suspect may have already been identified. In addition, the suspect may have admitted to using the specific evidence computer system, reducing the need to prove the admission with additional investigative efforts. Those are the easier investigations in placing someone at a keyboard; the suspect does all the work by admission!

This article addresses the more difficult cases where the suspect denies using the evidence computer (or other electronic device in question) or perhaps there was more than one person that may have accessed the electronic evidence. Even in cases were a suspect freely admits to being at the keyboard, it behooves an investigator to corroborate admissions with other evidence, because if the suspect recants or the admission not allowed as evidence, the case will have problems. Internet protocol (IP) addresses are not addressed in this article, for the main reason that an IP address is not a person. Like any piece of evidence, an IP address is a clue. It is one clue to a possible address, which may lead to a subscriber of an Internet service, which may lead to a person. Or, it may lead nowhere. Regardless, this article goes beyond chasing IP addresses.

I also use the terms "suspect" and "custodian" interchangeably, as well as referring to both criminal and civil cases. The processes and procedures work similarly in principle and concept and the tips are intended to give analysts incentive to think a little beyond the forensic examination to build a good case.

## FIRST THINGS FIRST

To conduct a digital forensics analysis, you need electronic media. With that, during a search and seizure of evidence, be sure to seize all items you are authorized to seize, because it most likely will be your only opportunity to seize relevant evidence. This applies to evidence seized pursuant to a search warrant just as much as it applies to collecting evidence from a compliant custodian in a civil litigation case. Once you leave the scene, consider that any items you leave behind will be gone. Should you realize that the external drive left on the desk should have been seized or imaged, you may not have the legal authority at the later time to retrieve it, the data likely will have changed, or perhaps the items are no longer accessible (they may be at the bottom of a lake).

One important aspect of seizing evidence related to the suspect will be documenting where the evidence was found in relation to the suspect or possible access by the suspect. Surely, seeing a suspect sitting in front of computer to be seized shows access to the computer and implies the suspect may have had control of the computer. Similarly, a tablet discovered in a dresser drawer in the suspect's bedroom shows accessibility to the tablet by the suspect (possibly others as well). These are important tidbits to consider to show accessibility and control of the items by the suspect.

### TRY THE EASY WAY

Although I do not like asking for directions when I drive around lost, I always ask questions of the suspect/custodian, even when I know the answers. Actually, I ask questions especially when I know the answers. For evidence, nothing beats statements made by a suspect against their penal interest. I recommend always asking questions until the suspect refuses to answer. Then, go do the hard work. Consider fingerprinting storage media and computer systems for irrefutable evidence of the identification of a person that has touched the evidence.

I would compare this strategy to turning the doorknob of a closed door to see if it is unlocked. If the door is locked, then you kick it down. Don't start kicking first…there may be an easier way. Turn the knob first…

## NOW THE HARDER STUFF – FORENSICS!

Digital forensics is not easy. No matter how much training and experience you have, there is always something that does not work right, such as a theory that doesn't pan out, system crashes, software failures, dozens of storage devices to examine, tons of data, encrypted files, and ever-changing operating systems to deal with on a constant basis. When looking for a piece of information to tie the suspect to a location or the computer, you are not just looking for the proverbial needle in a haystack; you are looking for a specific needle in a haystack of needles.

Some examinations may yield no evidence at all. Nothing. No illegal pictures, no stolen intellectual property, no harassing emails, nothing of value to your case. Other examinations may yield hundreds of thousands of illegal pictures or a stolen client list; yet, both situations are the same, as you still need to place the suspect at the keyboard. Merely finding electronic evidence on a hard drive is just that – evidence on a hard drive. Without creating a nexus between the suspect and evidence, your job is not complete.

There are aspects of a forensic analysis that can be beneficial as circumstantial evidence to help place the suspect at the keyboard. Evidence of logging into a computer is a start. Given a password protected operating system where only the suspect knows the credentials, the odds of a different person accessing that system is low. This theory does not work if the credentials are known to others or written on a notepad next to the computer.

This theory also applies to accessing applications that require credentials, such as an email client, or even webmail. Again, if only the suspect knows the credentials, the odds of another person using the system are low, but not impossible. Don't forget, sometimes the best person who knows if others have credentials for logging into a system is the suspect, so ask.

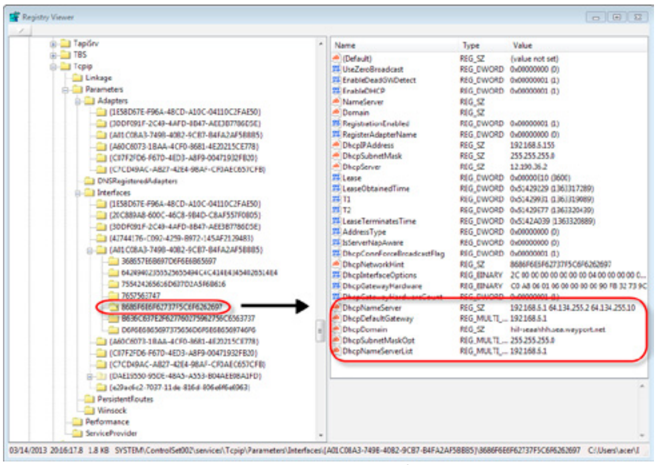
The forensic analysis of a computer system, or smart phone, can give a tremendous amount of information to be displayed in spreadsheets, timelines, and charts. In fact, a historical listing of computer activity can be recovered and detailed, showing any criminal acts or policy violations that occurred on the system. This is great evidence, but does not place a suspect at the keyboard. The work is necessary, but as in any incident involving electronic media, this work is only part of the totality of effort needed for a case. Yes, you need the evidence of the crime, but you also need to tie it to a suspect.

With electronic data that is clearly evidence, such as logs showing illegal access to a network or an illegal picture, you automatically want to tie that item with the suspect in some manner. At times, this may be easy, but other times, you may not be able to find enough circumstantial evidence to prove it. To help you tie evidence to a suspect, consider that non-evidential electronic data might do it. In one case where I examined a computer hard drive, the suspect denied ever using that specific computer. A quick check of previously attached devices showed an iPod connected over a period of time, which happened to be the same iPod belonging to the alleged suspect. This information makes questioning suspects easier in gaining more information to your goal of placing the suspect at the computer.

As an example, perhaps you have a location of an incident and your suspect denies ever being at that location, and if he was, it definitely was not during the time of the incident. The location could be a workplace or coffee shop. During your forensics analysis, you may find evidence of your suspect's locations based on IP addresses stored in the Windows registry. As an example, the registry maintains wireless connections related to network interface cards (NICs) located at:

```
\SYSTEM\ControlSet\services\Tcpip\Parameters\
                  Interfaces
```

It would be reasonable to assume that finding wireless access connections in the registry of a laptop means the laptop was at that particular physical location. Figure 1 shows an example of wireless connections where an IP address can be obtained, as a clue to follow and further investigate, not as an absolute physical location.

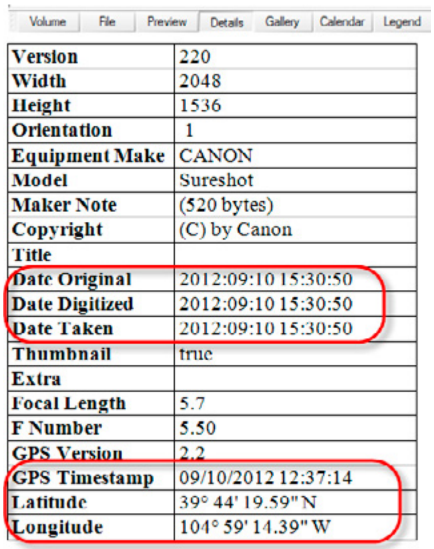


```
TapiSrv
TBS
Tcpip
  Linkage
  Parameters
    Adapters
      {1E58D67E-F96A-48CD-A10C-04110C2FAE50}
      {30DF091F-2C49-4AFD-8B47-AEE3B7786D5E}
      {A01C08A3-749B-4082-9CB7-B4FA2AF5B885}
      {A60C6073-1BAA-4CF0-8681-4E20215CE778}
      {C87F2FD6-F670-4ED3-A8F9-00471932FB20}
      {C7CD49AC-A827-42E4-98AF-CF0AEC657CFB}
    DNSRegisteredAdapters
    Interfaces
      {1E58D67E-F96A-48CD-A10C-04110C2FAE50}
      {20C889A8-600C-46C8-9B4D-C8AF557F0805}
      {30DF091F-2C49-4AFD-8B47-AEE3B7786D5E}
      {42744176-C092-4259-8972-145AF2129483}
      {A01C08A3-749B-4082-9CB7-B4FA2AF5B885}
        368657E6B697D6F6E6B65697
        6420696023555256554944C4C414E4345402651484
        755424265616D637D2A5F68616
        7657563747
        8686F6E6F62737F5C6F6262697
        8636C697E2F627760275962756C6563737
        D6F6E6865697375656D6F6E686569746F6
      {A60C6073-1BAA-4CF0-8681-4E20215CE778}
      {C87F2FD6-F670-4ED3-A8F9-00471932FB20}
      {C7CD49AC-A827-42E4-98AF-CF0AEC657CFB}
      {DAE15550-95DE-48A5-A553-B04AEE8BA1FD}
      {a20ac6c2-7037-11de-816d-806e6f6e6963}
    PersistentRoutes
    Winsock
  Performance
  ServiceProvider
```

| Name | Type | Value |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| UseZeroBroadcast | REG_DWORD | 0x00000000 (0) |
| EnableDeadGWDetect | REG_DWORD | 0x00000001 (1) |
| EnableDHCP | REG_DWORD | 0x00000001 (1) |
| NameServer | REG_SZ | |
| Domain | REG_SZ | |
| RegistrationEnabled | REG_DWORD | 0x00000001 (1) |
| RegisterAdapterName | REG_DWORD | 0x00000000 (0) |
| DhcpIPAddress | REG_SZ | 192.168.5.155 |
| DhcpSubnetMask | REG_SZ | 255.255.255.0 |
| DhcpServer | REG_SZ | 12.190.36.2 |
| Lease | REG_DWORD | 0x00000e10 (3600) |
| LeaseObtainedTime | REG_DWORD | 0x51429229 (1363317289) |
| T1 | REG_DWORD | 0x51429931 (1363319089) |
| T2 | REG_DWORD | 0x51429F77 (1363320439) |
| LeaseTerminatesTime | REG_DWORD | 0x5142A039 (1363320889) |
| AddressType | REG_DWORD | 0x00000000 (0) |
| IsServerNapAware | REG_DWORD | 0x00000000 (0) |
| DhcpConnForceBroadcastFlag | REG_DWORD | 0x00000001 (1) |
| DhcpNetworkHint | REG_SZ | 8686F6E6F62737F5C6F6262697 |
| DhcpInterfaceOptions | REG_BINARY | 2C 00 00 00 00 00 00 00 04 00 00 00 00 0... |
| DhcpGatewayHardware | REG_BINARY | C0 A8 05 01 06 00 00 00 00 90 FB 32 73 9C |
| DhcpGatewayHardwareCount | REG_DWORD | 0x00000001 (1) |
| DhcpNameServer | REG_SZ | 192.168.5.1 64.134.255.2 64.134.255.10 |
| DhcpDefaultGateway | REG_MULTI_... | 192.168.5.1 |
| DhcpDomain | REG_SZ | hil-seaahhh.sea.wayport.net |
| DhcpSubnetMaskOpt | REG_MULTI_... | 255.255.255.0 |
| DhcpNameServerList | REG_MULTI_... | 192.168.5.1 |

```
03/14/2013 20:16:17.8   1.8 KB   SYSTEM\ControlSet002\services\Tcpip\Parameters\Interfaces\{A01C08A3-749B-4082-9CB7-B4FA2AF5B885}\8686F6E6F62737F5C6F6262697   C:\Users\acer\
```

**Figure 1.** *Wireless access connection found in the registry*



| | |
|---|---|
| Version | 220 |
| Width | 2048 |
| Height | 1536 |
| Orientation | 1 |
| Equipment Make | CANON |
| Model | Sureshot |
| Maker Note | (520 bytes) |
| Copyright | (C) by Canon |
| Title | |
| Date Original | 2012:09:10 15:30:50 |
| Date Digitized | 2012:09:10 15:30:50 |
| Date Taken | 2012:09:10 15:30:50 |
| Thumbnail | true |
| Extra | |
| Focal Length | 5.7 |
| F Number | 5.50 |
| GPS Version | 2.2 |
| GPS Timestamp | 09/10/2012 12:37:14 |
| Latitude | 39° 44' 19.59" N |
| Longitude | 104° 59' 14.39" W |

**Figure 2.** *Metadata of a picture (.jpg file) using X-Ways Forensics*

One of the great things about metadata and electronic information is that metadata (information about data) is created and stored with most users knowing this is happening. If during your analysis you find pictures, be sure to check the metadata. You may find evidence tying your suspect to a specific place at a specific time as a picture's metadata (Exchangeable image format, or EXIF), may contain geolocation information.

Figure 2 is a screenshot of the metadata (EXIF) of a picture using X-Ways Forensics. From the EXIF data in this example, there is geotagging information showing the location where the picture was taken. If the picture was taken with the suspect's camera or smart phone, potentially, the suspect took the photo. If the suspect is actually seen in the photo, all the better.

The takeaway in this example is to look beyond the obvious evidence. Through the accumulation of geolocation data taken from smart phones, IP addresses, tablets, laptops, social networking posts, and surveillance videos, a timeline of your suspect's activity and locations can be made.

## SOMETIMES, YOU HAVE TO LEAVE THE OFFICE

As a forensic analyst, it is easy to be caught up with the multiple computer monitors attached to a high-end workstation on your desk that has various colored software dongles plugged in every USB port. Besides, what could be more exciting than discovering a hidden partition containing encrypted files that you were able to access using a password-bypassing program? How awesome is that!

I will admit that forensics is neat, but I also have to admit that tying a suspect to a computer sometimes requires actual footwork outside the office. At this point, if the suspect has denied using the evidence computer, or maybe admits using the computer on other occasions that were not related to criminal activity (or policy violations), you may need to go out of the office to gather more evidence.

The type of evidence you may want to consider looking for may exist along routes the suspect regularly takes to work or school. Video cameras, both government and private, are everywhere in larger cities. Almost every gas station has a video camera no matter the size of the city. Coffee shops, shopping malls, and hotel lobbies will usually have some sort of surveillance system. To prove or disprove your suspect's claims, you may have to obtain and view many video recordings in hopes of finding your suspect at a certain place and time. Although this may seem like a trivial task, cases have been made and broken by affirmatively placing a suspect at a specific location, even if it was just buying a cup of coffee at the local coffee stand.

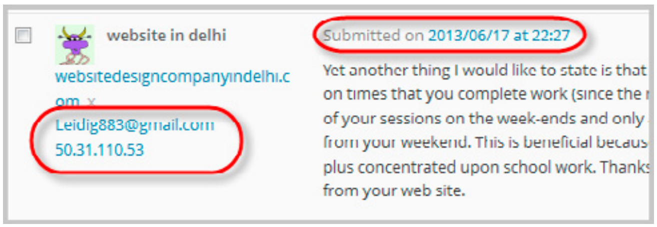
The location to which you try to pin your suspect could be a city, a house, or even a specific location in a building at a specific time. For example, if a file was deleted from the suspect's computer at his work, yet the suspect denies deleting this file, you may need to find where the suspect was at the time the file was deleted. Depending upon the number of employees and the methods used to track employees, this may be an easy task. Keycard controlled access points may show the suspect was actually in the lunchroom while at the same time keycard logs show a coworker in the where the suspect's computer was situated.

## BACK TO IP ADDRESSES

Ok, I said we would not get into IP addresses, but I meant that in the meaning that an IP address should not be thought of as a person. It is just a numerical designation of a device that uses the Internet Protocol. Obtaining a search warrant for a person, based solely on IP addresses and subscriber information could be considered negligent investigative work unless some other information exists to corroborate the information. There have been more than a few wrongfully served search warrants and arrest warrants based on an IP address. Technology allows for many avenues to hide a computer user's true IP address or to illegally access an open wireless access point, in effect, placing an innocent computer user at risk of being suspected of criminal activity.

However, IP addresses are still great clues. Today's cellular phones are now smart phones, logging our GPS locations, embedding GPS into our photos, and logging into WiFi hotspots. A forensic analysis of a smart phone not only extracts GPS locations, but also IP addresses used to access the Internet. Since most people do not loan their cell phone to others, when the suspect's phone connects to an open WiFi and logs that IP address, most likely, the phone's owner (the suspect) was at that location.

Third party service providers also log IP addresses to their customers. An example would be most social networking websites. Given an identified user account on a social networking site, any access by the suspect is likely logged by IP address. These logged IP addresses may be the suspect's home, work, or other location where the suspect accessed the service. Figure 3 shows the information obtained by a third party where the commenter's IP address along with date and time were captured. These are clues, circumstantial evidence, which when placed in context with other information can help place your suspect at a location (Figure 3).



□ website in delhi

websitedesigncompanyindelhi.com x

Leidig883@gmail.com

50.31.110.53

Submitted on 2013/06/17 at 22:27

Yet another thing I would like to state is that
on times that you complete work (since the
of your sessions on the week-ends and only
from your weekend. This is beneficial becaus
plus concentrated upon school work. Thanks
from your web site.

**Figure 3.** *IP address captured in an online comment*

Potentially, every IP address found in your forensic analysis or through third party service provider logs places the suspect at physical locations. Exceptions exist, but as with anything else, IP addresses are clues for you to follow.

## SO WHAT'S THE POINT?

My intention in this brief article is only to give the digital forensics analyst options to consider using other investigative methods to place the suspect at a keyboard. Some forensic analysts have the luxury of solely working the forensics end of a case while others (investigators) may work the entirety of an investigation, and must be able to manage all aspects in a focused manner as well as a being able to understand the entire case.

By ensuring a suspect has been accurately identified and placed at the keyboard (or smart phone), the digital forensics work will have been worthwhile. The best forensic exam without a suspect is just the best forensic exam. You already have a victim. You already have electronic evidence. The last part of the puzzle is finding and placing the suspect at the keyboard. Otherwise, what's the point?

## SUMMARY

I have given a high-level view of tips to place a suspect at a computer; however, there are many more methods to consider which go beyond a short article. The forensic analyst needs to be aware that no case is just a hard drive exam. Every criminal or civil case has victims, witnesses, suspects, and evidence to examine. Clues are everywhere, but if not taken in context with the rest of the case, clues can be overlooked or misinterpreted. Good forensic examiners can find everything on a hard drive. Great forensic examiners not only find everything on a hard drive, but they can put together a great case based on the totality of all evidence, thinking both in and out of the hard drive.

### About the Author

*Brett Shavers is a digital forensics expert and author. As both a former law enforcement officer and detective, Brett has investigated most types of crimes. As a private consultant, he has been retained by law firms for digital forensics analysis in civil litigation cases ranging from personal disputes to class action litigation. Brett's first book, on which this article is based, Placing the Suspect Behind the Keyboard, was published by Syngress in 2013.*

# EDISCOVERY 101: AN INTRODUCTION TO EDISCOVERY

**by Dauda Sule**

Volonino and Redpath (2010) quoted Judge Shira A. Scheindlin as follow: "We used to say there's e-discovery as if it was a subset of all discovery. But now there's no other discovery." The Law has been taking its course, technology has been developing; the result is the evolution of Law to keep up with technological advancements.

**What you will learn:**

- What discovery means
- What eDiscovery means
- The eDiscovery process

**What you should know:**

- Basic understanding of digital forensics
- Basic understanding of Law

Discovery (referred to as disclosure in the UK) is the process whereby each party in a legal dispute reviews evidential documents in their opponent's control, which are considered to be relevant to the case at hand. This usually takes place before full legal proceedings begin (as the outcome might result in a withdrawal of the case or an out of court settlement). Each party in the case (plaintiff or defendant) has the right to request any information deemed to be relevant to the case, in any format, from the opposing party; the opposing party must respond to the request either by providing the information or giving a very good reason why such information cannot be provided (Volonino and Redpath, 2010). According to Sommers (2012), disclosure (discovery) ensures that each party and the court in a case are fully aware of all the circumstances and to support the over-riding objective of ensuring the parties are on an equal footing, saving time and money, dealing with the case in a proportionate way while ensuring it is dealt with in an expeditious and fair manner.

## WHAT IS EDISCOVERY?

eDiscovery refers to electronic discovery (also called eDisclosure). eDiscovery involves parties in a legal dispute requesting and reviewing electronically stored information (ESI) that is relevant to the case. Rouse (2010) defined eDiscovery as any process in which ESI is sought, located, secured, and searched in order for it to be used as evidence in a civil or criminal case. In the US, the Federal Rules of Civil Procedure (FRCP) was amended in 2006, codifying the need for provision of ESI, which could be considered as the origin of eDiscovery. The UK's version was Practice direction 31B of 2010.

ESI refers to any form of document containing information or data that is electronic in nature, like disks, audio and/or video files, emails, network logs, image files, office documents, metadata, and computer programs (including malware). ESI can be used as evidence (e-evidence or digital evidence) in legal proceedings. Documents for discovery used to be in paper format before electronic data became the norm, and could be physically voluminous and tedious to handle. ESI, although more voluminous, could be handled, stored and transported in a much easier manner; what would have been printed on thousands of pages could be stored on something as small as a mini SD card. That notwithstanding, ESI needs to be handled with care, as it can be quite volatile, and some aspects like metadata could be modified by merely accessing the data.

eDiscovery requires ESI; but the ESI might be voluminous leading to unnecessary waste of time and resources in analyzing it. There has to be some sort of data mining to sift through the ESI and select only those relevant to the case. There may also be some information, which a party may have good reason to keep confidential, and not disclose to the opposing party. Such information is called privileged information, and the party having such has to declare it to the court or the other party. Such privileged information could include trade secrets or correspondence with a lawyer or doctor or the like. The court will have the final decision as to whether such information should be withheld or not.

## THE EDISCOVERY PROCESS

LWG Consulting (2009) stated that the *Electronic Discovery Reference Model* (EDRM) was developed in 2005 to help create best practices and guidelines for those working in the field of eDiscovery (lawyers, eDiscovery vendors, organizations preparing for litigation, and so on); and that it has become a standard of going through the eDiscovery process and aiding adherence to the *US Federal Rules of Civil Procedure* (FRCP). The model depicted in Figure 1 has nine phases as follow:

- Information Management
- Identification
- Preservation
- Collection
- Processing
- Review
- Analysis
- Production
- Presentation

## INFORMATION MANAGEMENT

The way an organization manages its data and information is very crucial for eDiscovery when the need for eDiscovery arises. A good information management policy ensures that whenever discovery becomes necessary, data and information can be readily and easily made available in a forensically sound manner without unnecessary delay. Laws pertaining to eDiscovery (like the US FRCP) *require digital evidence* (ESI) to be prepared and presented quickly when request for and in an acceptable manner. Good information management policies, like documenting retention policies and forensic readiness policies, go a long way in

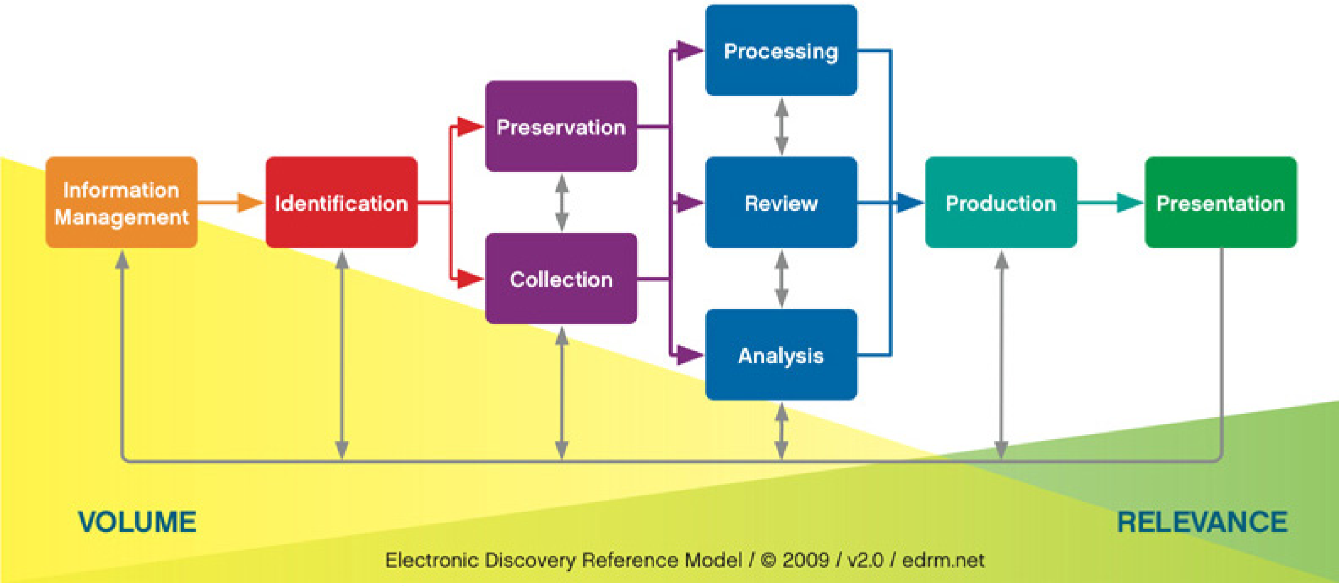


**Figure 1.** *The Electronic Discovery Reference Model (Source: EDRM – www.edrm.net)*

ensuring ESI is available in a timely and forensically sounding manner.

Poor information management policies can have a negative impact on an organization in the event of litigation and where eDiscovery becomes required. In the case of *AMD vs. Intel* in 2005, Intel failed to produce requested electronic documents in good time due to its faulty email retention policy, leading to severe sanctions against the company (McLaughlin, 2013). At the end of the day (in 2009), Intel had to settle AMD $1.25 billion (Shankland and Skillings, 2009); the cost of poor information management policy.

## IDENTIFICATION

In this phase, ESI that will be relevant to a case and its location are determined. The location could be email, hard drives, backup tapes, and so on. Identification of relevant ESI begins once litigation is reasonably anticipated. Prior to discovery, lawyers of the parties usually have a meet-and-confer session or a schedule conference to discuss, where they agree on what ESI would be relevant, and the methods of identifying such ESI (Volonino and Redpath, 2010). The location of identified ESI is assessed to determine what needs to be preserved.

The defendant, Delmar Gardens, in *Chura vs. Delmar Gardens of Lenexa, Inc. (2012)* failed to produce any ESI at all. This lead the court to raise concerns that the defendant either failed to preserve relevant ESI or failed to conduct a reasonable search in response to the plaintiff's request; and thus the defendant was ordered to prepare to present evidence of preservation of and search for ESI (K&L Gates, 2013). The defendant apparently failed to make an attempt at identifying relevant ESI or preserving it.

## PRESERVATION

Preservation begins immediately relevant ESI is identified. Once there is a reasonable anticipation of litigation, identified ESI have to be preserved by the organization. The duty to preserve evidence is responsibility of which the organization may be held accountable for. Employees who have relevant information in their custody (custodians) and IT departments need to be informed that their ESI has become subject to discovery; hence they have to be issued a litigation hold. The litigation hold is to ensure that custodians do not tamper with the ESI that has become relevant evidence from then on, avoiding risk of modification or loss; the IT department is to ensure that such ESI are isolated from access by the custodians and properly safeguarded. Maintaining a proper chain of custody ensures proper documentation of how the digital evidence was collected, stored, handled and analyzed – this can prove that ESI was properly preserved. In the *AMD vs. Intel* case, part of Intel's errors was a failure to properly communicate litigation hold to employees (relevant custodians of ESI). The Chura case mentioned under identification also shows the importance of preserving identified ESI. Another case where failure to preserve ESI cost a party is *Apple, Inc. vs. Samsung Elecs. Co. Ltd (2012)* in which Samsung was sanctioned for not halting an auto-delete feature on its email system (emails were part of requested ESI) and also failure to properly follow up on employees regarding litigation hold (K&L Gates, 2013). Sanctions were also considered to be appropriate against Apple for failure to issue litigation hold to its employees in a timely manner.

## COLLECTION

This phase involves acquiring ESI that had been identified and preserved. Often times, preservation and collection may take place simultaneously. The ESI is required to be collected in a forensically sound manner, should be proportionate, efficient and targeted. The ESI could be collected by self-collection or forensic imaging (LWG Consulting, 2009).

Self-collection of ESI involves manual copying of files and/or forwarding emails by information custodians, the ESI having been identified as relevant to the case at hand and notice of litigation hold having been sent to the custodians and IT department. This method is risky in that employees may intentionally or unintentionally modify ESI during the collection process.

Forensic imaging involves making bit-by-bit copies of information storage media in a bid to preserve the ESI from alteration or contamination. This can also capture deleted items; hence there might be a need to review such images to ensure privileged information is not included (in the review process).

In an extreme case (*Taylor vs. Mitre Corp., 2012*), Taylor – the plaintiff – use a sledge hammer and evidence wiping software to destroy his computer and erase some relevant ESI that should have been collected from his laptop (K&L Gates, 2013). That resulted in the court recommending the plaintiff to bear much of the legal expenses incurred by the defendant in the case.

## PROCESSING

Collected ESI needs to be processed before moving it to the review stage. Processing involves indexing, searching and de-duplicating the collected ESI to reduce non-relevant material, while fulfilling the requirements of the requesting party as well as the court. Some ESI may have to be extracted from files like compressed folders (for example, zip files); there may also be need to convert some files form native format where such format is outdated and no longer in use, or the software required to view it is not available to the requesting party and the court. The files, in such cases may be converted to formats that can be easily accessed by the other party.

The filtering involved in processing goes a long way in saving time for the parties and the court; it also reduces costs the organization processing the ESI. Volonino and Redpath (2010) stated that Gartner estimated the cost of reviewing one gigabyte of data for eDiscovery to be $18,750. It is quite clear that processing ESI to reduce irrelevant data is a cost-saver.

## REVIEW

ESI is reviewed after processing. The review tries to determine if there is any privileged information contained in the ESI, and to ensure the ESI is relevant and meets the necessary requirements of the case. The review can be done using a native file review or using a TIFF/PDF based review (LWG consulting, 2009).

In native file review, the files are reviewed in their native (original) format, usually in read only mode so as to prevent contamination of the ESI arising from unintentional modification. Even so, this does not eliminate the risk of modification. Emails are, however, normally converted to HTML format for native file review (LWG Consulting, 2009).

Files are reviewed in an image format (like PDF or TIFF) in a TIFF/PDF review. Here, the files are converted or saved in such image format to prevent alteration or contamination. The downside is some data cannot be viewed; for example, if the native format were Excel, formulas would not be available for review; only the output would be available in the image format.

A non-responsive document review may also be carried out. In this case, a sample of documents that have been considered not relevant to the litigation (based on keyword searches for example) are reviewed which may reveal if they contain relevant data, despite not having the keywords used for the search in them (LWG Consulting, 2009).

In the case of *Bro-Tech Corp vs. Thermax, Inc. (2008)*, quoted by K&L Gates (2013), the district court sustained the defendant's (Thermax) objection to a prior ruling by a magistrate court compelling the defendant produce entire servers to the plaintiff for review; the ruling was considered contrary to the law, and the defendant was allowed to do a pre-production review and make a more limited production. K&L Gates (2013) also stated the case of *Ciba-Geigy Corp. vs. Sandoz, Ltd (1995)* in which it was ruled that production of documents without first carrying out a review for privileged information was considered an inexcusable act of negligence and attorney-client privilege was waived. The Ciba-Geigy Corp. case should serve as a guide for parties in an eDiscovery case to ensure they carry out proper privilege reviews before production of ESI.

## ANALYSIS

Analysis is the next phase in the eDiscovery process, although in reality it normally takes place along with review. The ESI is further examined to ensure it is in line with the requirements of the requesting party and the litigation as a whole. Content of ESI are analyzed and the review could be enhanced using tools like concept searching tools. Concept searching tools extract content from ESI by using key concepts and subject matter to examine the ESI based on meaning of phrases and subject matter, as opposed to using keywords (LWG Consulting 2009). This kind of technique used in combination with others goes a long way to create ease in the eDiscovery process.

## PRODUCTION

In this phase, how, what, where and when ESI is produced to an opposing party is covered. The US FRCP Rule 34(b) gives the party requesting for ESI the right to determine what ESI should be produced, in what form and when. ESI could be produced on paper, in native form or image form. Paper production requires printing out the ESI on paper, which could be cumbersome and expensive (print-outs could end up being stacked several meters high). Native form production requires the ESI be produced in its original state, while image form requires production of the ESI in a duplicated form, which could be in the form of TIFF/PDF or forensic images. Image form production is easier to handle without altering the ESI, and is more commonly requested. In the event the requesting party fails to specify the format ESI should be produced, the court may accept a common format presented by the producing party. In the case of *Adams vs. Allianceone, Inc. (2011),* the court denied the plaintiff's motion to sanction the defendant for producing ESI in PDF format rather than native format, since the plaintiff did not specify any format in the request and moreover the PDF format was considered reasonably usable (K&L Gates, 2013).

The produced data could be delivered to the requesting party either as a final production or a rolling production. The final production involves delivery of data at once after all previous phases have been carried out. A rolling production involves delivery of the data to the requesting party in phases.

In the event privileged information is contained in what is produced – that is inadvertent disclosure – the producing party can request for its return using a clawback agreement (Volonino and Redpath, 2010). The clawback agreement would normally be agreed upon during the meet-and-confer session. A party will have to prove inadvertent disclosure for a clawback to be effected. In the case of *Callan vs. Christian Audigier (2009),* defendants sought to compel the plaintiff to comply with a clawback provision for the return of some inadvertently disclosed privileged information, but failed to prove the nature of privilege, nor any steps taken to avoid the disclosure. Hence, based on the failure, the court denied the defendants motion for clawback (K&L Gates, 2013).

Privileged information may be withdrawn or aspects of ESI in documents considered to be privileged may be redacted. Proper redaction software should be used for redaction, as methods available in formats like MS Word or Adobe reader can easily be uncovered. Redax, Redactionware and Redact-it are some examples of redaction software that are available.

## PRESENTATION

The final stage in the eDiscovery process is presentation of ESI at a trial or in settlement negotiations (Fayle, 2008). ESI has to be presented in a way that non-technical people (usually lawyers, judges and jury members tend not to be tech savvy) can easily comprehend and appreciate the e-evidence. The e-evidence also has to be presented in a way that is professional and convincing in a bid to prove or disprove a claim. The chain of custody may also need to be confirmed during the presentation to support the fact that ESI is authentic and forensically sound. A presentation should look appealing, not too flashy and should not be too techy such as to lose the judge or jury.

## POINT OF NOTE FOR THE REQUESTING PARTY

The party making a request for eDiscovery needs to be sure it knows what it wants, and also be sure that what it is requesting actually exists. In the 2008 case of *Autotech Techs Ltd. P'ship vs. Automationdirect.com* (taken from Volonino and Redpath, 2010), the defendant (Automationdirect.com) requested for ESI from the plaintiff (Autotech), but did not include metadata in the request. Autotech provided the ESI as requested, but after some time the defendant decided they wanted to have metadata as well. The judge ruled that the defendant had to be satisfied with what it requested for, which was provided by the plaintiff.

## MISCELLANEOUS

There are still many countries that are still trying to bring their laws up-to-date with advancements in technology. In Nigeria, for example, the Evidence Act of 2011 paved the way for admission of electronic evidence in courts. In such countries, eDiscovery might not yet even be an issue as their laws continue to be amended, evolve and adapt. Data protection and privacy laws also vary from country to country both in content and level of development, which can lead to complexities when ESI cuts across international borders. There is also the issue of some countries that consider giving evidence that is within their countries to another country as a kind of breach to their sovereignty, and hence it would be considered unheard of for ESI within such countries and especially as pertains to their citizens to be made available for discovery to a foreign country.

## SUMMARY

The process of eDiscovery has to be followed with due care by any organization that has reasonably anticipated litigation. Failure to comply with the steps can result in a very negative impact for an organization as was seen in the case of Intel in *AMD vs. Intel*, where the company ended up

## REFERENCES

- EDRM LLC (2009) EDRM Stages [Online]. Available from: *http://www.edrm.net/resources/edrm-stages-explained* (Accessed: 30 June 2013).
- Fayle, K. (2008) Introduction to the New World of eDiscovery [Online]. Available from: *http://technology.findlaw.com/electronic-discovery/introduction-to-the-new-world-of-ediscovery.html* (Accessed: 30 June 2013).
- K&L Gates (2013) Electronic Discovery Case Database [Online]. Available from: *http://ediscovery.klgates.com/search.aspx* (Accessed: 13 July 2013).
- Legal Information Institute (nd) Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and other Purposes [Online]. Available from: *http://www.law.cornell.edu/rules/frcp/rule_34* (Accessed: 30 June 2013).
- LWG Consulting (2009) An Introduction to the eDiscovery Process [Online]. Available from: *http://www.lwgconsulting.com/news/default.aspx?ArticleId=55* (Accessed: 30 June 2013).
- McLaughlin, D. (2013) Lessons of AMD v. Intel [Online]. Available from: *http://www.youtube.com/watch?v=jQ_9uLkw_Uo* (Accessed: 30 June 2013).
- Rouse, M. (2010) Electronic Discover (E-Discovery or eDiscovery) [Online]. Available from: *http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery* (Accessed: 29 June 2013).
- Shankland, S. and Skillings, J. (2009) Intel to Pay AMD $1.25 billion in Antitrust Settlement [Online]. Available from: *http://news.cnet.com/8301-1001_3-10396188-92.html* (Accessed: 30 June 2013).
- Sommer, P. (2012) Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers. 3rd Edition, Version 3.0. Information Assurance and Advisory Council.
- Volonino, L. and Redpath, I. (2010) e-Discovery for Dummies. Indiana: Wiley Publishing, Inc.

bearing huge costs due to inability to provide e-evidence as requested in good time resulting from poor email retention policies and ineffective litigation hold communication. An organization need not wait for a litigation to be anticipated to start preparing for eDiscovery; having a good information management system in place, like proper document retention policies, forensic readiness policies, backup and incident response policies, help the organization to be on its toes and be able to respond appropriately to eDiscovery requests and in good time.

The requesting party also has to be clear on and sure of what they request to be disclosed, as courts will not tolerate time wastage due to making unnecessary additional requests after they have been provided with what they requested for in the format request and within the timeframe requested. The case of Autotech Techs Ltd is an example of what happens when a party does not make an adequate request in the first instance.

## About the Author

*Dauda Sule, CISA. He is currently the Marketing Manager of Audit Associates Limited which is a consultancy firm that specializes in designing and organizing training programs pertaining to auditing, fraud detection and prevention, information security and assurance, and anti-money laundering. He is a CISA and has an M.Sc. in Computer Security from the University of Liverpool. Dauda also has a first degree black belt in Taekwondo. He has previous experience of over five years in the Nigerian Banking industry, and also did some time in Gtech Computers (a computer and allied services company) as a systems security and assurance supervisor.*

# HARD DRIVE FORENSIC PROCEDURES

**by Krystina Horvath and Thomas J. Bray**

Would hard drives obtained with digital forensics standards, require alternative methods of investigation? In this article, the forensic collection and preservation of data off of hard drives using AccessData's FTK Imager and Forensic Toolkit, will be presented. Metadata will also be considered during the forensic collection procedure.

**What you will learn:**

- Hard drive forensic procedures
- Uses of AccessData's FTK Imager and Forensic Toolkit during hard drive forensic collection and analysis
- Metadata considerations of forensic hard drive data

**What you should know:**

- Basic understanding of Windows operating systems
- Architecture of hard drives
- Installation of Windows-based forensic programs

What significance does a hard drive have in computer forensic investigation? The function of a hard drive is to store data and retrieve digital information. Information such as e-mail messages, instant messages, multimedia files, games, programs, images and other documents are saved and stored to a computer's hard drive. Basically, any activity or function a user carries out on their machine will be backed up onto the hard drive. When a hard drive is forensically processed, there will most likely be vast amounts of undiscovered or hidden data that could be unlocked through forensic processes and forensic analysis (Figure 1).

**Figure 1.** *Hard Drive*

This article will focus on three crucial computer forensic aspects: procedures and preservation, forensic tools and their uses, and metadata considerations after a hard drive has been forensically processed. If any of these aspects are compromised during investigation, the integrity of the forensic analysis will not stand up to court rulings.

## FORENSIC PROCEDURES

Implementing the correct forensic procedures in a hard drive investigation will help avoid compromising the evidence and solidify the integrity of harvested data presented in court. Computer forensics involves four steps: preservation of data, identification of evidence, extraction of data and documentation of findings. In this guide, we will focus on the first three steps of this process.

## PRESERVATION AND IDENTIFICATION OF DATA

Assuming that this is a live response analysis of a hard drive, law enforcement and the computer forensics investigator should secure the crime scene. The investigator should also perform documentation of the crime scene.  Written documentation along with photographs of all evidence should be compiled at this point. Particular attention to the power status of the computer and its monitor(s), and network and peripheral connections should be noted and well-documented for future reference.

Then, the scene must be processed for the identification of evidence. In this scenario, the hard drive will be our key piece of evidence. We will assume that the computer containing the hard drive has been left powered on. Extraction of data, or forensically processing the hard drive, may occur after proper preservation of the scene has been implemented and evidence has been documented in detail (Figure 2).

## EXTRACTION OF DATA

The preservation of data still exists when extracting data. In fact, preserving the data during an investigation is necessary in maintaining the integrity of the evidence.

**Figure 2.** *Crime Scene*

Working with a live machine is a tedious task that requires a plan to extract forensic evidence. It is highly recommended that the original evidence is preserved, while two copies of the data are made (an evidence copy and a working copy).

It is recommended that gloves are worn by the examiner to avoid leaving fingerprints on any evidence or in the suspect's workspace. In addition, the following supplies should be used to preserve the evidence while in transportation from the crime scene to the forensic laboratory:

- Additional gloves
- evidence tags and markers – to label evidence
- anti-static bags – to protect the hard drive during transportation.

## IMAGING THE HARD DRIVE USING FTK IMAGER LITE

In order to create these copies, our example will use AccessData's FTK Imager Lite v3.1.1 to image the powered on hard drive. Choosing the correct forensic tools for the extraction of data is critical to the preservation of the original evidence and data. Rather than using the full FTK Imager program, FTK Imager Lite is a more appropriate choice for live acquisition because no installation is required. It is an executable file that may be placed on a USB flash drive and inserted into the machine being investigated. In comparison, FTK Imager standard requires full installation of the program, which leaves a larger forensic footprint (activity that is logged onto the hard drive). FTK Imager Lite also uses the minimum number of files necessary to run the program and image a hard drive. The standard FTK Imager uses several more files during installation and investigation, leaving a dramatically larger forensic footprint on the hard drive.

FTK Imager Lite also allows an investigator to image a hard drive as a physical image as an AFF, DD, RAW, 001, E01 or S01 form or as a logical image with a drive letter assigned to it. A physical image of the hard drive should be used instead of a logical image. A physical image refers to the actual organization of data on a device. This imaging retrieves all of the binary coding possible from the device. In contrast, a logical image refers to how the information appears to a program or user as seen through an operating system. Logical imaging does not retrieve all binary coding from the machine. Therefore, this imaging process might miss retrieving data. The more data that is picked up by imaging a hard drive, the more evidence there is for the examiner to analyze and use in the analysis.

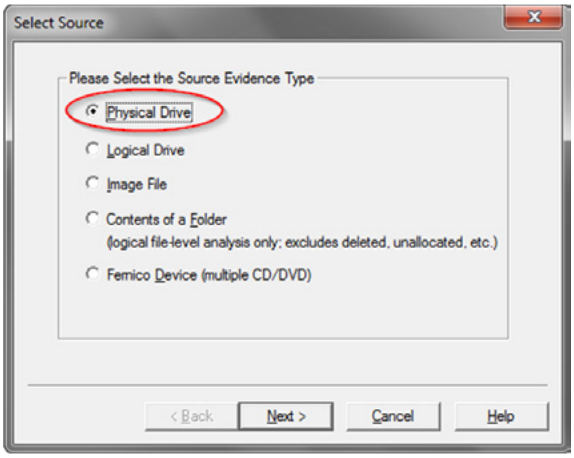
During the data extraction process, a forensic examiner will insert a USB flash drive (noting the date and time of insertion – as this action will be logged on the hard drive) containing FTK Imager Lite. From here, the examiner will want to avoid clicking any unnecessary icons, programs or documents so the forensic footprint stays small on the hard drive. Once the machine detects the USB flash drive and FTK Imager Lite is opened, the computer forensic examiner should begin creating a physical image of the hard drive.

To begin this process, the examiner will open up the FTK Imager Lite program and select the following options:

- Go to File and select *Create Disk Image*,

A box will pop up allowing the examiner to select the source evidence type, the examiner should choose physical drive (based on our earlier analysis of physical vs. logical imaging) (Figure 3),

- Then, the examiner will be asked to select the source drive. The examiner will choose the hard drive of the local machine (FIgure 4),
- Next, the investigator will select image options with a Create Image pop-up box. There will be an image source line that displays the evidence source drive that had been selected previously. The examiner will click on the *Add* button under Image Destination(s) to specify the destination image type (Raw-dd, SMART, E01 and AFF are the choices). In this case, an E01 image will be created. An E01 file is an executable image file that is compatible with several forensic tools and can easily be converted to another file format.
- Once the image type is selected, the examiner will assign a case number, evidence number, a unique description, the examiner's name and any notes to the evidence item information,
- Then, the destination folder for the created disk image must be selected along with assigning a filename to the imaged hard drive. In this case, the examiner will be working on a suspicious computer so the destination folder should be one located on an external hard drive of about the same size as the investigated computer's hard drive (a 500gb hard drive on the suspect's computer should require a 500gb external hard drive as a destination folder). The default imaged fragment size of 1500 MB and compression size of 6 may remain as these settings,
- After selecting, the destination information is complete, the examiner will be returned to the Create Image pop-up box. Check that the option to "Verify images after they are created" is selected to ensure that the imaged hard drive is verified. Lastly, the examiner will begin the imaging process by clicking *Start*.



Select Source

Please Select the Source Evidence Type

● Physical Drive

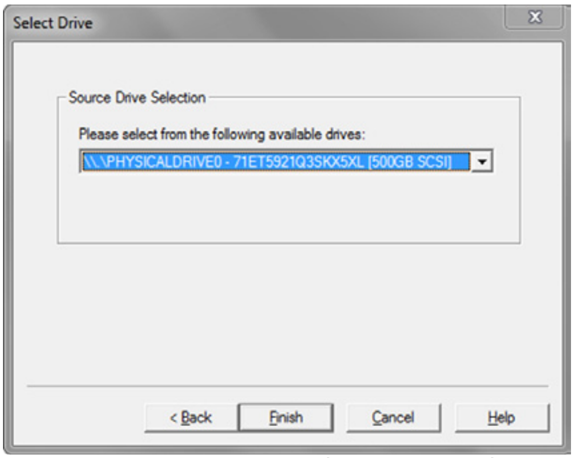
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

**Figure 3.** *FTK Imager Lite – Creating Disk Image*



Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - 71ET5921Q3SKX5XL [500GB SCSI]

**Figure 4.** *FTK Imager Lite – Selecting Drive to be Imaged*

Depending on how much data is stored on the hard drive, the image creation time will vary. Once the hard drive is imaged successfully, FTK Imager Lite provides an MD5 hash value verification of the image, maintaining the integrity of the original piece of evidence (this corresponds to the "Verify images after they are created" option). An MD5 hash value is a cryptographic hash function that is utilized to verify data (such as files and folders) integrity. If an MD5 hash value does not match the original MD5 hash value, this usually means that the data was tampered with and should be investigated further. After FTK Imager Lite has created an image of the hard drive in question, this version is now an evidence copy of the imaged hard drive.

After the evidence copy is created and all other evidence documentation and collection is completed, the examiner should label all evidence and pack it up in anti-static bags to prevent any devices from coming in contact with static electricity.

Once the examiner returns to the forensic laboratory, a copy of the imaged hard drive should be created as a working copy for the investigation. It is critical that the evidence copy is stored on a USB flash drive and kept in a secure spot to avoid tampering or loss. The working copy may be stored on the examiner's investigation machine. After a working copy has been created, the investigation of data using AccessData's Forensic Toolkit may commence.

## ANALYZING THE IMAGED HARD DRIVE USING FORENSIC TOOLKIT

AccessData's Forensic Toolkit is data analysis software. This freeware is a court-accepted forensic program that allows an examiner to drop files and imaged drives into it and analyze using a wide range of options.

When opening this program, the examiner will be asked to either: start a new case, open an existing case, preview evidence or go directly to working in Forensic Toolkit. In this instance, the examiner will *Start a New Case* and input their name, case number, case name and choose a file path and folder to store this analysis. In addition, a case description can be entered into this new case wizard to identify any key facts of the case. Next, forensic examiner information can be filled out with data identifying who employs the examiner, the examiner's name and contact information. This may be helpful during testimonial during the case or several years after the case has been closed and re-opened.

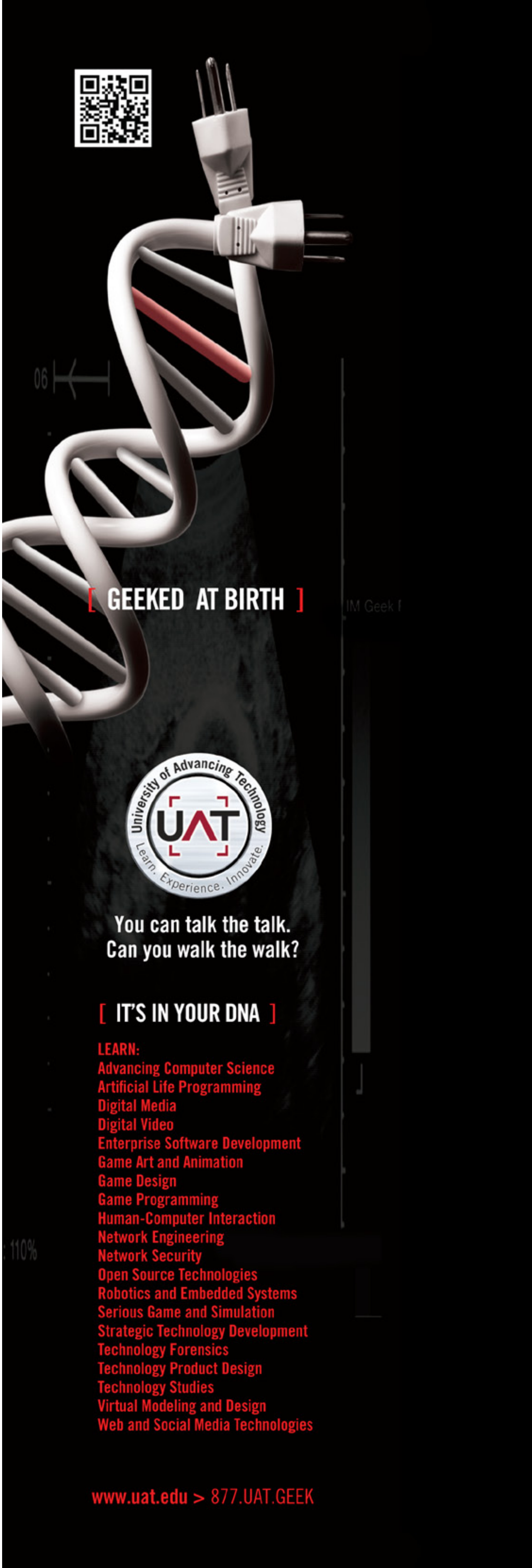
Next, the examiner will select case log options pertaining to the text file that Forensic Toolkit generates with the events that occur during the investigation. Forensic Toolkit defaults to all events (case and evidence events, error messages, bookmarking events, searching events, data carving/Internet searches and other events). When investigating an imaged hard drive, the default options are appropriate logs because much information is stored on hard drives.

Then, the examiner will be asked to choose processes to perform during the extraction of data. The default processes selected; MD5 hash, SHA1 hash, KFF lookup, entropy test, full test index, store thumbnails, decrypt EFS files and file listing database are all useful processes. These processes may remain selected.

Next, the investigator will select items to refine the case results. If the examiner has been requested to search e-mail messages or documents for certain information, then these options can be selected. However, if an investigator is not focusing on a certain piece of digital information, then the default options will include all data within the imaged hard drive.

Once these options are selected, the examiner may add the physical imaged hard drive as evidence into Forensic Toolkit by selecting the following:

- *Add Evidence* button on the Add Evidence box, a pop-up will allow the investigator to choose what type of evidence they would like to add to the program.


[ GEEKED AT BIRTH ]
University of Advancing Technology
UAT
Learn. Experience. Innovate.
You can talk the talk.
Can you walk the walk?
[ IT'S IN YOUR DNA ]
LEARN:
Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering
Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies
www.uat.edu > 877.UAT.GEEK

- A type of evidence list including; acquired image of a drive, local drive, contents of a folder and individual file are displayed. In the case of a physical imaged hard drive, an examiner would choose to add an acquired image of a drive.
- Once that option is selected, the examiner will locate where he/she saved the imaged hard drive and add to the case.
- From here, the examiner will assign an evidence identification name or number. This completes the case options and evidence addition.

Similar to FTK Imager Lite, when Forensic Toolkit processes evidence, the time elapsed depends on the size of the imaged hard drive. The more data the hard drive holds, the longer it will take to process and add the evidence.

After the evidence has been added to Forensic Toolkit, there are a number of features that may be used to analyze this imaged hard drive. Forensic Toolkit arranges the data pulled from the imaged hard drive into a cohesive overview tab that categorizes the types of files and data found into file statuses and file categories. For example, encrypted files that are located within the hard drive are displayed in an Encrypted Files button under File Status. This makes it easy for examiners to pinpoint, which files are encrypted and may be primary focus of the investigation.

There are other tabs in which the data pulled from the imaged hard drive is separated and can be searched individually. In Figure 5, the results of

A graphics tab and an e-mail tab allow the investigator to search these key pieces of information in depth.

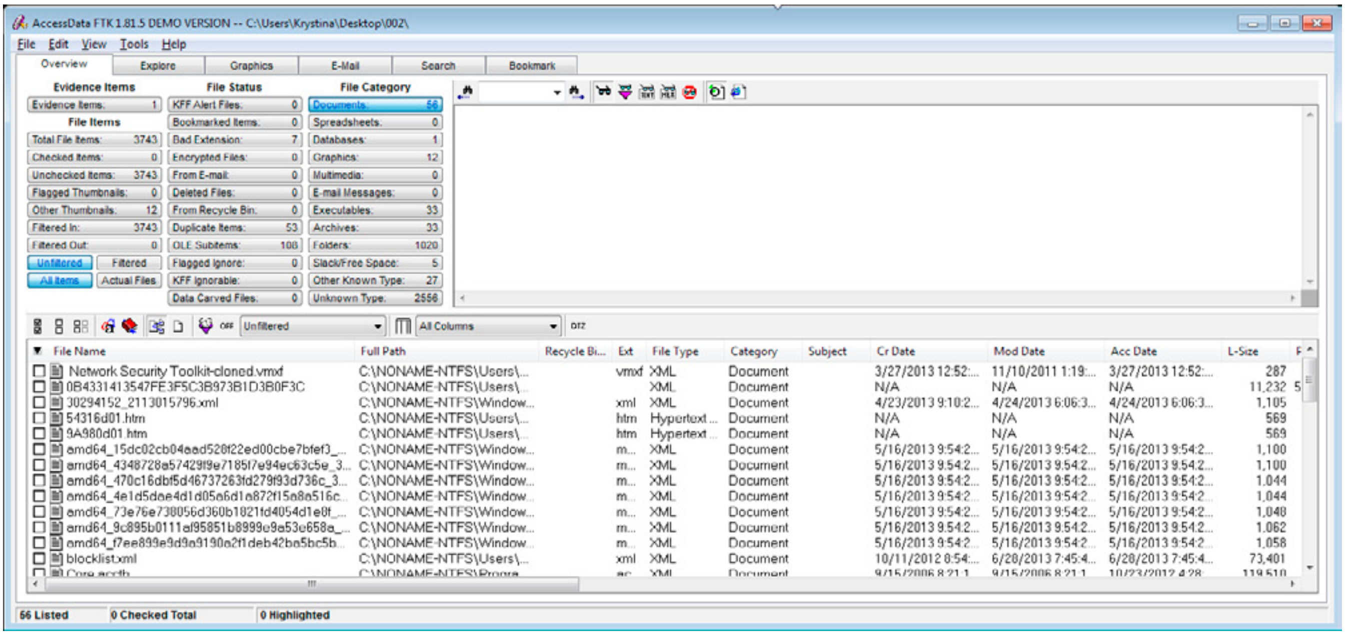
The graphics tab displays the evidence files in the middle of the Forensic Toolkit screen. The examiner will use this feature by navigating through the evidence files and searching for graphics. This tab does not pull any other information besides graphics. Therefore, when navigating through the evidence, only graphics will be shown if they are uncovered within a location. If a graphic is found and the examiner selects to view it, the graphic will appear next to the evidence file path in the middle of the screen and information about the graphic will appear on the bottom of the screen. This information can be helpful if there is a suspicious graphic found. The file name, file path, if it was moved into the Recycle Bin and other creation and modification data of the graphic are shown within the graphics tab. An investigator may feel that a graphic file holds interest in the investigation by information such as being moved to the Recycle Bin.

## E-MAIL INVESTIGATION

Another highly useful feature of Forensic Toolkit is the e-mail tab. Forensic Toolkit pulls all web e-mail messages and any other e-mail message found on the evidence and places it into this tab. The examiner can navigate through the e-mail tree located in the top, left-hand corner of the Forensic Toolkit screen to browse through e-mail messages on the imaged hard drive. The e-mail messages will be shown on the bottom of the screen with all metadata about the message shown on the top, right-hand side of the screen. Nefarious e-mail messages can be easily detected through this feature.

## SEARCH FUNCTION IN FTK

In addition, there is a search tab, which allows an examiner to search for any terms relevant to the case. For example, if the hard drive we are investigating is suspected to being used to send intellectual property documents to a foreign country (like



AccessData FTK 1.81.5 DEMO VERSION -- C:\Users\Krystina\Desktop\002\

| Evidence Items | | File Status | | File Category | |
|---|---|---|---|---|---|
| Evidence Items: | 1 | KFF Alert Files: | 0 | Documents: | 56 |
| File Items | | Bookmarked Items: | 0 | Spreadsheets: | 0 |
| Total File Items: | 3743 | Bad Extension: | 7 | Databases: | 1 |
| Checked Items: | 0 | Encrypted Files: | 0 | Graphics: | 12 |
| Unchecked Items: | 3743 | From E-mail: | 0 | Multimedia: | 0 |
| Flagged Thumbnails: | 0 | Deleted Files: | 0 | E-mail Messages: | 0 |
| Other Thumbnails: | 12 | From Recycle Bin: | 0 | Executables: | 33 |
| Filtered In: | 3743 | Duplicate Items: | 53 | Archives: | 33 |
| Filtered Out: | 0 | OLE Subitems: | 108 | Folders: | 1020 |
| Unfiltered | Filtered | Flagged Ignore: | 0 | Slack/Free Space: | 5 |
| All Items | Actual Files | KFF Ignorable: | 0 | Other Known Type: | 27 |
| | | Data Carved Files: | 0 | Unknown Type: | 2556 |

| File Name | Full Path | Recycle Bi... | Ext | File Type | Category | Subject | Cr Date | Mod Date | Acc Date | L-Size | F |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ Network Security Toolkit-cloned.vmxf | C:\NONAME-NTFS\Users\... | | vmxf | XML | Document | | 3/27/2013 12:52:... | 11/10/2011 1:19:... | 3/27/2013 12:52:... | 287 | |
| □ 0B4331413547FE3F5C3B973B1D3B0F3C | C:\NONAME-NTFS\Users\... | | | XML | Document | | N/A | N/A | N/A | 11,232 | 5 |
| □ 30294152_2113015796.xml | C:\NONAME-NTFS\Window... | | xml | XML | Document | | 4/23/2013 9:10:2... | 4/24/2013 6:06:3... | 4/24/2013 6:06:3... | 1,105 | |
| □ 54316d01.htm | C:\NONAME-NTFS\Users\... | | htm | Hypertext ... | Document | | N/A | N/A | N/A | 569 | |
| □ 9A980d01.htm | C:\NONAME-NTFS\Users\... | | htm | Hypertext ... | Document | | N/A | N/A | N/A | 569 | |
| □ amd64_15dc02cb04aad528f22ed00cbe7bfef3_... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,100 | |
| □ amd64_4348728a57429f9e7185f7e94ec63c5e_3... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,100 | |
| □ amd64_470c16dbf5d46737263fd279f93d736c_3... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,044 | |
| □ amd64_4e1d5dae4d1d05a6d1a872f15a8a516c... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,044 | |
| □ amd64_73e76e738056d360b1821fd4054d1e8f_... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,048 | |
| □ amd64_9c895b0111af95851b8999e9a53e658a_... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,062 | |
| □ amd64_f7ee899e9d9a9190a2f1deb42ba5bc5b... | C:\NONAME-NTFS\Window... | | m... | XML | Document | | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 5/16/2013 9:54:2... | 1,058 | |
| □ blocklist.xml | C:\NONAME-NTFS\Users\... | | xml | XML | Document | | 10/11/2012 8:54:... | 6/28/2013 7:45:4... | 6/28/2013 7:45:4... | 73,401 | |
| □ Core.accdb | C:\NONAME-NTFS\Progra... | | ac | XML | Document | | 9/15/2006 8:21:1 | 9/15/2006 8:21:1 | 10/23/2012 4:28: | 119,510 | |

56 Listed | 0 Checked Total | 0 Highlighted

**Figure 5.** *Extracted Document Metadata*

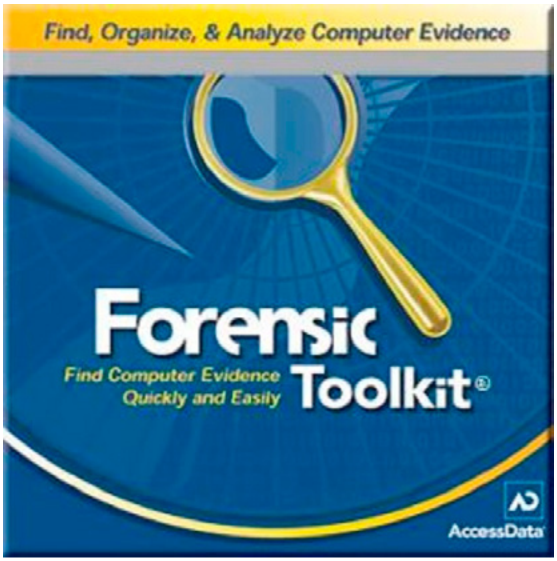

Find, Organize, & Analyze Computer Evidence
Forensic Toolkit®
Find Computer Evidence Quickly and Easily
AccessData

**Figure 6.** *AccessData's Forensic Toolkit*

China), an examiner may search for terms such as "China" or "Beijing", or Internet Protocol (IP) addresses corresponding to Beijing (these IP addresses will begin with 115.121.0.0 and end with 115.121.255.255). These searches are helpful when searching for programs such as Timestomp, which alters the creation and modification times of documents to lead computer forensic investigators in the wrong direction.

Another very useful Forensic Toolkit feature is a data carving option, which allows the examiner to carve out several types of image files found on the imaged hard drive. BMP, JPEG, PNG, PDF and even AOL/AIM buddy list images can be carved out of the evidence and displayed without using search terms or navigating through the graphics tab. Child pornography cases benefit greatly from this data carving feature. Instead of searching through text, this option pulls the image files and allows the examiner to view them.

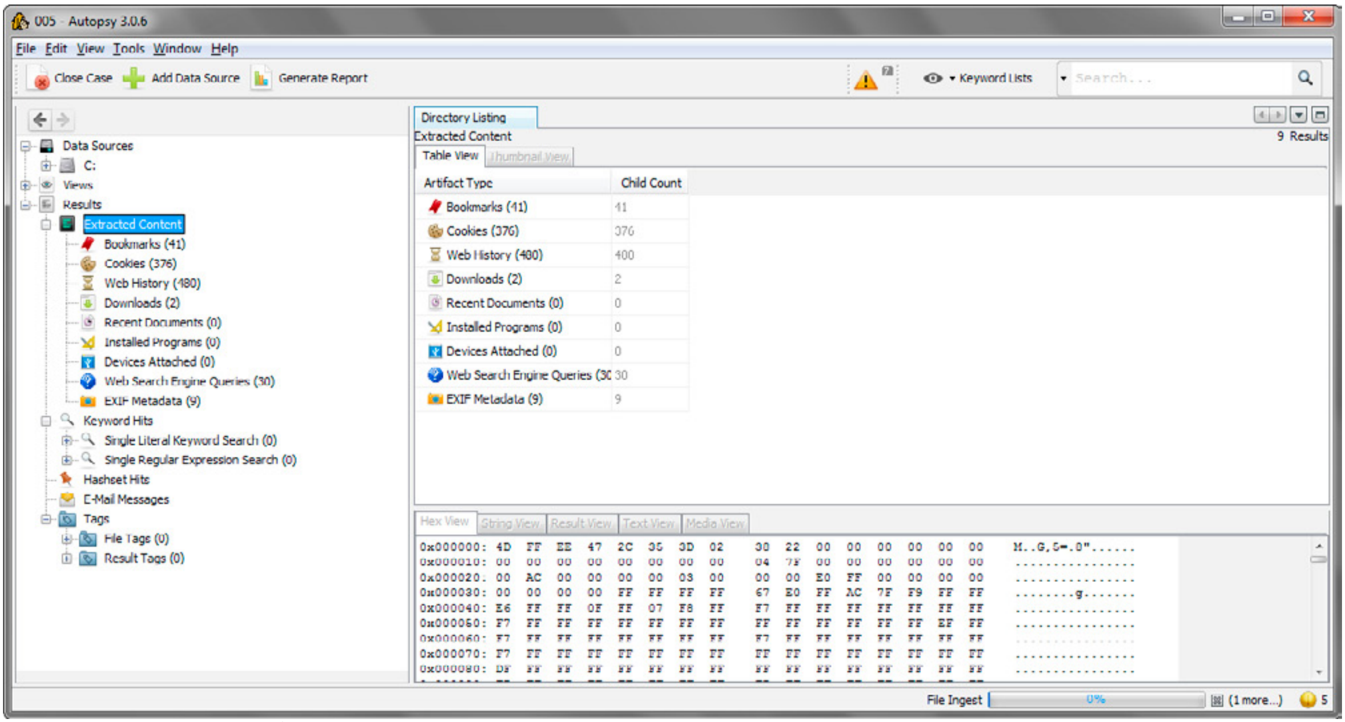
Lastly, any information that an examiner deems suspicious or nefarious can be bookmarked for court use. If an investigator finds a document that they feel is a critical piece of a case, they can right click on the document's file name and choose *Create New Bookmark*. The examiner can name the bookmark and add commentary, if the examiner feels necessary. There is also an option to include the bookmark in the Forensic Toolkit generated report. This is helpful when testifying in court. These pieces of information can be produced quickly and shown to the jury and judge.

## ANALYZING THE IMAGED HARD DRIVE USING THE SLEUTH KIT'S AUTOPSY

The Sleuth Kit's Autopsy v3.0.6 performs in a similar manner to Forensic Toolkit. After the imaged hard drive is loaded to the program via the *Add Data Source* option, Autopsy displays the extracted data in a single evidence tree. This allows the examiner to view all extracted content in one spot.

Figure 7 depicts results of an imaged hard drive after loading to Autopsy.

As you see, the extracted data is clearly broken out into specific artifact categories along with the number of hits displayed for each category. Autopsy will extract bookmarks, cookies, web history, downloads, recent documents, installed programs, devices attached, web search engine queries, e-mail messages, keyword hits, a listing of existing



| Artifact Type | Child Count |
|---|---|
| Bookmarks (41) | 41 |
| Cookies (376) | 376 |
| Web History (480) | 400 |
| Downloads (2) | 2 |
| Recent Documents (0) | 0 |
| Installed Programs (0) | 0 |
| Devices Attached (0) | 0 |
| Web Search Engine Queries (3C | 30 |
| EXIF Metadata (9) | 9 |

```
0x000000: 4D  FF  EE  47  2C  35  3D  02    30  22  00  00  00  00  00  00    M..G,5=.0"......
0x000010: 00  00  00  00  00  00  00  00    04  7F  00  00  00  00  00  00    ................
0x000020: 00  AC  00  00  00  00  03  00    00  00  E0  FF  00  00  00  00    ................
0x000030: 00  00  00  00  FF  FF  FF  FF    67  E0  FF  AC  7F  F9  FF  FF    ........g.......
0x000040: E6  FF  FF  0F  FF  07  F8  FF    F7  FF  FF  FF  FF  FF  FF  FF    ................
0x000050: F7  FF  FF  FF  FF  FF  FF  FF    FF  FF  FF  FF  FF  FF  EF  FF    ................
0x000060: F7  FF  FF  FF  FF  FF  FF  FF    F7  FF  FF  FF  FF  FF  FF  FF    ................
0x000070: F7  FF  FF  FF  FF  FF  FF  FF    FF  FF  FF  FF  FF  FF  FF  FF    ................
0x000080: DF  FF  FF  FF  FF  FF  FF  FF    FF  FF  FF  FF  FF  FF  FF  FF    ................
```

**Figure 7.** *Extracted Data from Autopsy*

and deleted files and executables, and EXIF (Exchangeable Image File) metadata.

Autopsy offers a *Search* option for examiners who have keywords they need to search. Perhaps one of the most useful features with Autopsy is the EXIF metadata that can be pulled. Any pictures that were uploaded onto the hard drive will appear in this data extraction and information about the geographical location, camera used to take the picture, date and time and the source file and file path of the picture is exposed. EXIF data cannot be extracted with Forensic Toolkit.

In addition, Autopsy provides a hash set filtering extraction. This will filter and flag files and folders using custom hash sets such as MD5Sum, HashKeeper and EnCase. The examiner can identify tampered files easily with this feature. Media, such as images and video, can be viewed easily with Autopsy. Extracted video files can be viewed within Autopsy rather than an external media viewer. Images can also be viewed through the program.

Lastly, Unicode strings extraction of unallocated space and unknown file types in multiple languages is offered through Autopsy. This will pull strings out of unallocated space (where nefarious files may reside).

## COMPILING AND ANALYZING THE DATA

After compiling all of this information, an examiner must analyze all of the metadata attached to each piece of pulled data. Metadata is known as data about data. Creation and modification times, file size, file name and file path, owner, keywords, etc. are all considered metadata. This metadata is a crucial means of creating a timeline of events that occurred within a computer. However, what if this metadata has been compromised?

## METADATA CONSIDERATIONS

Unfortunately, users may tamper with metadata of files or programs in an effort to throw examiners off track during an investigation. As previously mentioned, Timestomp is a program that allows a user to modify times when a machine was powered on or off, or when a document was modified or viewed.

How does tampering with metadata affect the integrity of an investigation? A user tampering with their metadata does not affect the integrity of the investigation itself. Instead, the metadata itself loses its integrity and the investigation suffers from false evidence.

Altered timestamps on files and other actions on a suspect's machine do not allow an examiner to create an accurate timeline of events. For example, if a computer is used by multiple users and the creation or viewing time of a document is compromised, there is no way to identify the responsible party. Therefore, the integrity of the metadata is compromised and part of the investigation cannot be solidified.

## ERROR OF RECOVERED DATA

Will an imaged hard drive provide completely recovered data from a suspect's machine? Before the hard drive is imaged, data loss may occur due to hardware failure, software corruption, viruses, theft, and hardware destruction. About 68% of data loss is in direct correlation with these causes.

While working on a live response acquisition, human error is to blame for data loss, especially volatile memory (RAM). It is not only critical to lessen the forensic footprint that an examiner leaves on a machine but the examiner must also proceed with caution so file information is not altered. When creating a disk image, it is recommended that a write blocker is used to ensure that no data is written back onto the hard drive during the information collection process.

While the data on a hard drive cannot be recovered completely, the examiner can increase the correctness of this data by using a write blocker during the imaging process.

## SUMMARY

In conclusion, it is critical to maintain the integrity of evidence when working in a live response acquisition atmosphere. Specific procedures and proper documentation are very important when investigating and ultimately, testifying in court. However, all data should be analyzed thoroughly for accurate metadata to ensure that the correct suspect is indicted.

### About the Author

*Krystina Horvath, MBA is currently in the midst of a career change from finance to computer forensics. Krystina is working on her capstone project for Utica College's Master of Science in Cybersecurity program. The topic for this paper focuses on proving the success of malware used in corporate and governmental cyber espionage attacks. Krystina also offers recommendations for security measures to help prevent malware attacks against these entities.*

### About the Co-author

*Thomas Bray is an Information Security and eDiscovery professional with more than twenty-five years experience in healthcare, financial services, information technology and consulting organizations. Throughout his career, he has successfully managed numerous large scale and technically complex eDiscovery projects. Mr. Bray is a Certified Information Security manager (CISM), an active member of the Information System Security Association (ISSA), and a published author of information security and eDiscovery articles.*

### THE INTERVIEW WITH

# TERRY TANG

### FOUNDER OF WISECLEANER

**by Aby Rao**

Terry Tang, founder of Wisecleaner.com and a programmer with rich development experience, has developed Wise Care 365, Wise Registry Cleaner, Wise Disk Cleaner and many other popular PC utilities software.

### Terry, you come from a programmer background. How and when did you decide to develop software that deals with windows security?

The internet environment in 2005 was kinda turmoil. I simply could not stay still seeing those different kinds of plug-ins, viruses and trojans wreaking havoc and the anti-virus software could do nothing but watching. Finally, I decided to develop my own software to deal with Windows security.

### Where are your products developed and what kind of quality assurance do they go through?

The first few products were developed at home, there was no special quality assurance process. I tested and kept the quality guaranteed only with my years of experience. Later on, we formed a professional team in our company and we now have professional quality control team members to maintain the high standard of every product.

### Tell us little bit about how WiseCleaner came into existence.

In the very first, I developed the first version of the software just because I needed it. Then I shared it on the internet to benefit more people, in which way I also gathered more needs and feedbacks to improve the software.

### Why did you decide to focus on windows registry?

Registry is the core data base of Windows. Most trojans and plug-ins make damage through modifying registry. To a great extent, the purity of Registry can decide whether Windows can run smoothly and determine its running speed.

### Are your products compatible with all very version of windows?

Our products keep pace with the times. The early versions supported Win98 and Win2000. From version 5, the Windows prior to WinXP were not supported. Currently, all Windows versions started from WinXP can be supported.

### Which is your most popular product and how often do you come out with new version?

Our most popular products are Wise Registry Cleaner and Wise Disk Cleaner. They keep updated every half month.

### WHAT ROLE DOES THE REGISTRY PLAY IN CONDUCTING VARIOUS FORENSICS ON THE SYSTEM?

Registry is the core data base of Windows, which customizes all kinds of running rules and behaviours. It's more like the configuration file of Windows. Amounts of Windows behaviours were recorded in Registry and Windows works according to the defines in Registry. Meanwhile, amounts of users' operation traces and behaviours are recorded in Registry, eg. Files list used to be opened with specific software, the location of these files and keywords used to type when surfing internet. All these made the examination of users' behaviours possible. Therefore, having these traces deleted can be beneficial in protecting users' privacy.

### What is WiseCare 365 and what does it accomplish.

Wise Care 365 is a comprehensive system optimization utilities, which combines many common optimization functions and useful tools. The optimization functions are as follows:

- Clean trash files in system: It saves disk space and makes Windows running more smoothly.
- Clean traces, including internet viewing traces, files visit traces, network visit traces, common software using traces, etc. It's effective to avoid leak of personal using habits and private information.
- Clean Registry: Delete unnecessary Registry keys to make Windows run more smoothly, reduce errors and run more stably.
- Defrag Disk to reduce fragments of Disk. It makes faster the saving and reading of files and the pages exchange of visual memory.
- Defrag Registry: It effectively cuts the size of Registry, accelerates the loading speed of startup registry and therefore accelerates bootup speed.
- Clean privacy: One of our original and exclusive functions to clean personal traces recorded by Windows, including URLs, pics, cookies viewed online and local files viewed, to avoid leak of privacy.
- System Slimming: One of our original and exclusive functions to effectively reduce disk space occupied by Windows system. It increases spaces available but not affects the normal running performance of Windows.
- Disk Eraser: It permanently deletes remaining files information to avoid anti-deletion.

### Do you have any products that will help perform or assist windows forensics analysis?

Yes. Wise Registry Cleaner and some functions in Wise Care 365.

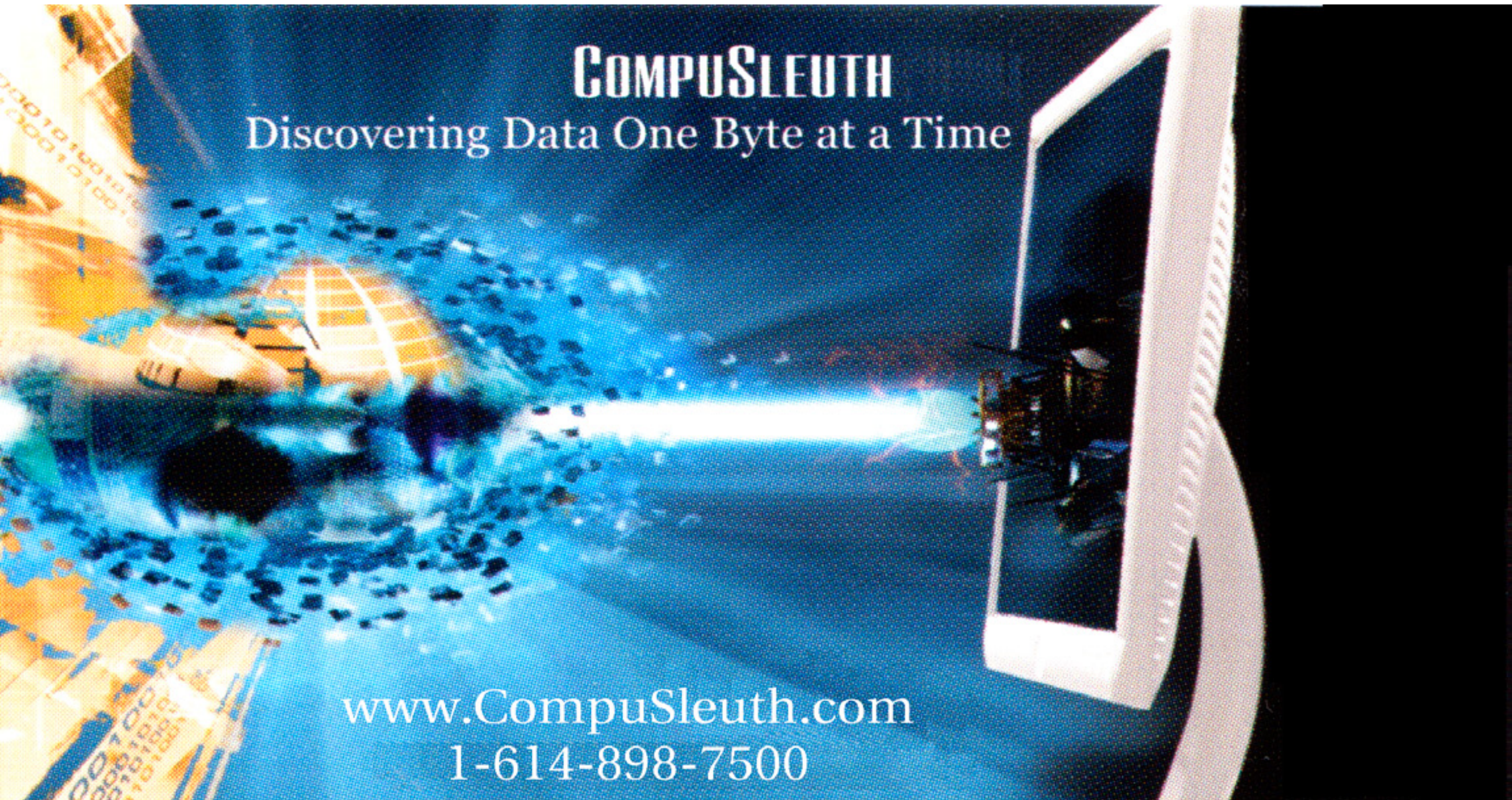
### What kind of support do you offer with your products?

We provide free and professional tech support via Email for all the users including freeware users. We promise to get back to our users within 48 hours.

### Any knowledge you can share with our e-forensics readers about windows forensics analysis?

It's a good habit to keep the registry and system clean. Experiments have proved that a PC regularly maintained with cleaning software remains stable and effective performance, while the performance of a PC without cleaning software will obviously be deteriorated and need to reinstall the OS to maintain efficiency within only one year. Meanwhile, keeping this habit can not only maintain system running speed, but also protect user's behaviour, habit and traces not to be stolen by organizations or persons with purposes.

**Thanks for your time.**



# DIGGING INTO MOZILLA FIREFOX ARTEFACTS

**by Gabriele Biondo**

Mozilla Firefox has been the most widespread web browser for years, and nowadays is the second most popular browser. From a computer forensics point of view, understanding how the caching mechanism works, is a key aspect. Although Mozilla Firefox is Open Source, auditing over 30 MB of source code is not viable. A quick'n'dirty, but effective approach, could be regarded as a type of gray box test.

**What you will learn:**

- How Mozilla caching works
- The structure of the .mozilla folder
- What does really happen while 'private browsing'
- A simple methodology for gray box testing

**What you should know:**

- This article is thought as a gray box software test, and the author tried to explain all the technical tools used to gather the results. No prior knowledge should be required.

The idea for this article comes from another article, by Jessica Riccio, published in the eForensics Magazine, in which an overview of how the most widespread web browsers implement the so-called 'incognito browsing' method was presented.

This article focuses only on the Linux version of the browser, in order not to overwhelm the reader with too much information. In detail, the `.mozilla` folder will be analyzed: this folder contains the artifacts created by Mozilla Firefox. Actually, it is impressive to notice how little we know about the browsers, which are one of the most used applications nowadays. This article is basically a step stone, a starting point for further investigation.

Another aspect pertains on Open Source software. De facto, Mozilla Firefox is Open Source software, so should be completely auditable, but, seriously, who has audited 36 Mb of bz2 archives of code? Moreover, several pieces of information are not well described online – one needs to dig and understand by testing.

## THE ENVIRONMENT

The environment that has been set up for this analysis is as follows: Table 1.

Mozilla, on Linux-based systems, creates a hidden directory in each user's folder, named `.mozilla`. This is shown in Figure 1 below. This directory will be the main place of this analysis, as it contains Mozilla profile information (Listing 1).

The profiles.ini file contains information used to keep track of profiles in Firefox. More info on this file could be found, for instance, in [1]. The `Crash`

Reports directory is not important for the purpose of this analysis. The mwad0hks (This is a random identifier. Reader's system could be different from this one.).default directory contains more interesting data, described in the next chapters.

## THE DATABASES

This set of databases already supplies the analyst with plenty of relevant information. Except for settings, contained in the databases: addons.sqlite and extensions.sqlite, the other databases give enough information to backtrack users' activities (Table 2).

## OTHER FILES

These files are mostly related to specific browser settings. Very important the sessionstore files, which may have a huge relevance, in terms of forensics analysis.

**Listing 1.** *The .Mozilla directory structure*

```
gbiondo@linuxMint ~ $ tree -d .mozilla
.mozilla
├── extensions
└── firefox
    ├── Crash Reports
    └── mwad0hks.default
        ├── bookmarkbackups
        ├── Cache
        │   ├── 0
        │   │   ├── 0D
        │   │   ├── 28
---8< ---8< --- SNIP---8< ---8< ---
        │   │   ├── F4
        │   │   └── FA
        │   ├── 1
---8< ---8< --- SNIP---8< ---8< ---
        │   ├── 2
---8< ---8< --- SNIP---8< ---8< ---
        │   ├── 3
---8< ---8< --- SNIP---8< ---8< ---
...................................
---8< ---8< --- SNIP---8< ---8< ---
        │   ├── D
---8< ---8< --- SNIP---8< ---8< ---
        │   ├── E
---8< ---8< --- SNIP---8< ---8< ---
        │   └── F
        │       ├── 03
---8< ---8< --- SNIP---8< ---8< ---
        │       └── F0
        ├── extensions
        ├── minidumps
        ├── safebrowsing
        ├── startupCache
        ├── thumbnails
        └── webapps
```

**Table 1.** *Environment*

| Entity | Versions |
|---|---|
| OS | linuxMint Downloads # cat /etc/*release*<br>DISTRIB_ID=LinuxMint<br>DISTRIB_RELEASE=15<br>DISTRIB_CODENAME=olivia<br>DISTRIB_DESCRIPTION="Linux Mint 15 Olivia"<br>NAME="Ubuntu"<br>VERSION="13.04, Raring Ringtail"<br>ID=ubuntu<br>ID_LIKE=debian<br>PRETTY_NAME="Ubuntu 13.04"<br>VERSION_ID="13.04"<br>HOME_URL="http://www.ubuntu.com/"<br>SUPPORT_URL="http://help.ubuntu.com/"<br>BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"<br>linuxMint Downloads # uname –a<br>Linux linuxMint 3.8.0-19-generic #29-Ubuntu SMP Wed Apr 17 18:16:28 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux |
| Firefox | linuxMint Downloads # which firefox<br>/usr/bin/firefox<br>linuxMint Downloads # `which firefox` --version<br><br>(process:4130): GLib-CRITICAL **: g_slice_set_config: assertion `sys_page_size == 0' failed<br>Mozilla Firefox 20.0 |

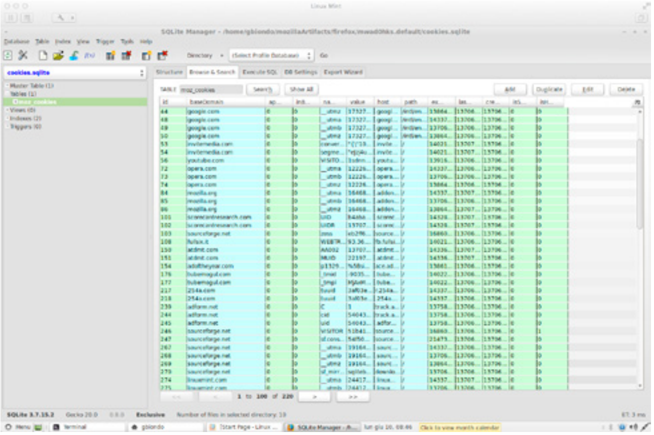


**Figure 1.** *Contents of cookies.sqlite database*

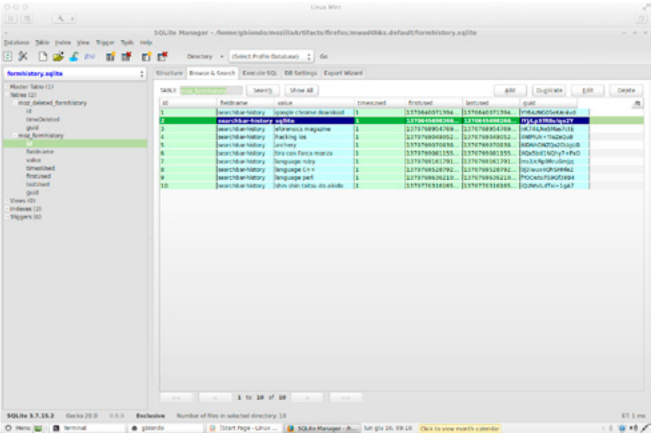


**Figure 3.** *Contents of the formhistory.sqlite database*

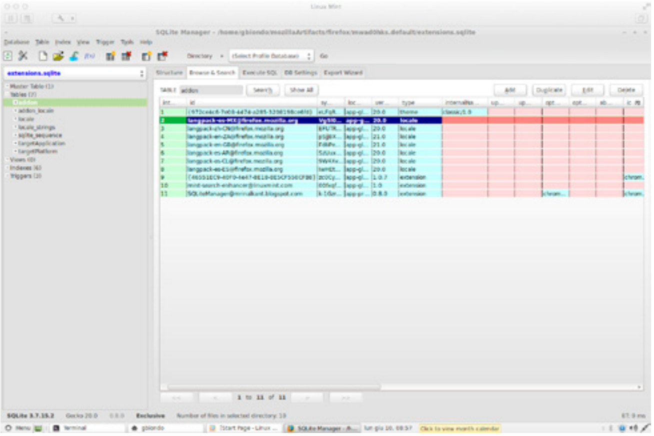


**Figure 2.** *Contents of the extensions.sqlite database*

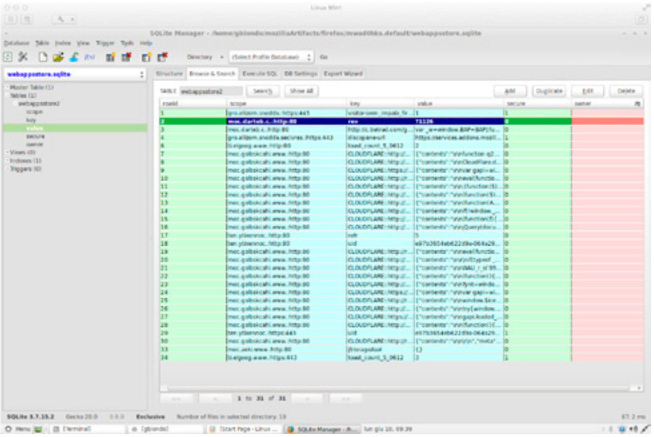


**Figure 4.** *Contents of the webapsstore.sqlite database*

**Table 2.** *Mozilla Firefox's databases*

| Database | Contents |
|---|---|
| addons.sqlite | stores the information that appears in the Addons tab > Extensions. It is a fairly complex database, containing information on all the addons (extensions) installed in the browser. |
| content-prefs.sqlite | contains site specific preferences. More info on this could be found on [2]. In the specific case, there is no content – no web-app has been browsed using this installation, yet. |
| cookies.sql | described in [3], holds all the cookies gathered by the browser. Figure 1 shows some contents of the installation under analysis. |
| downloads.sqlite | part of the Mozilla Download Manager, more information on this could be found on [4] and [5]. |
| extensions.sqlite | contains data about the extensions installed in the browser. More information on this could be found on [6]. Table 2 shows some contents of the installation under analysis. |
| formhistory.sqlite | remembers what the user has searched for in the Firefox search bar and what information the user has entered into forms on websites. Some contents are shown in Figure 3. |
| permissions.sqlite | [7] gives some information about it. Contains permissions given to the websites, on a punctual basis. |
| places.sqlite | stores the annotations, bookmarks, favorite icons, input history, keywords, and browsing history (a record of visited pages). |
| signons.sqlite | is the password manager of Mozilla firefox, basically. See [9] for further information |
| webappstore.sqlite | [10] does not report lots of information pertaining on this file, and also Figure 4 does not contain, yet, many information. |
| cert8.db | Is the certificate database tool for Firefox – certificates are stored in this database. Further information can be found in [14]. |
| key3.db | Contains the key used to encrypt the stored passwords. See [15] for further information |

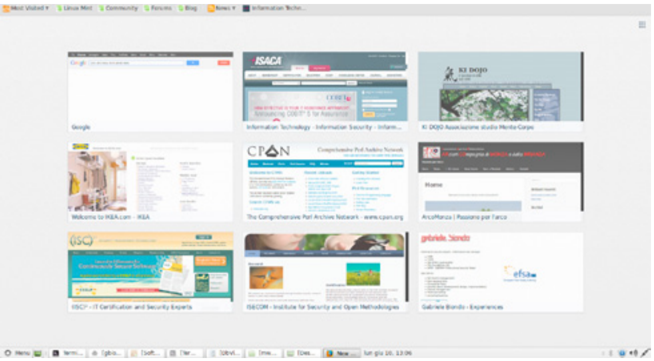


**Figure 5.** *New Firefox window opened*

## THE THUMBNAILS DIRECTORY

This directory contains all the thumbnails appearing when opening a new browser windows (see Figure 1), plus some historical contents. Those are all PNG images, 480x300 pixels wide. Some of them are reported in Figure 6 below. Obviously, also these files have sound forensics relevance in case of analysis.

## THE EXTENSIONS FOLDER

This folder actually contains all the extensions installed in Firefox. From a forensic standpoint, the interesting aspects are related to malware.

**Table 3.** *Other Mozilla Firefox's files*

| File | Contents |
|---|---|
| blocklist.xml | list of add-ons that Mozilla considers to be harmful to the user. See [11] for further information |
| urlclassifierkey3.txt | Key database for phishing protection [12] |
| compatibility.ini | Contains installation-specific information such as path, version, OS, and similar ones |
| extensions.ini | Contains the list of the installed extensions |
| search.json | Specifies the installed search engines in the search bar, along with their default settings |
| prefs.js | Contains some local preferences, accessible with about:url |
| sessionstore.js<br>sessionstore.bak | Contain all data needed to restore the previous sessions – see [13] |
| pluginreg.dat | Registration of all MIME types. See [12] |
| localstore.rdf | stores customized data on the interface, such as toolbar customizations, window positions and sizes, and tree sort orders. See [16] |
| mimeTypes.rdf | stores information about which action is to be performed when downloading certain types of files. More information on this in [17] |

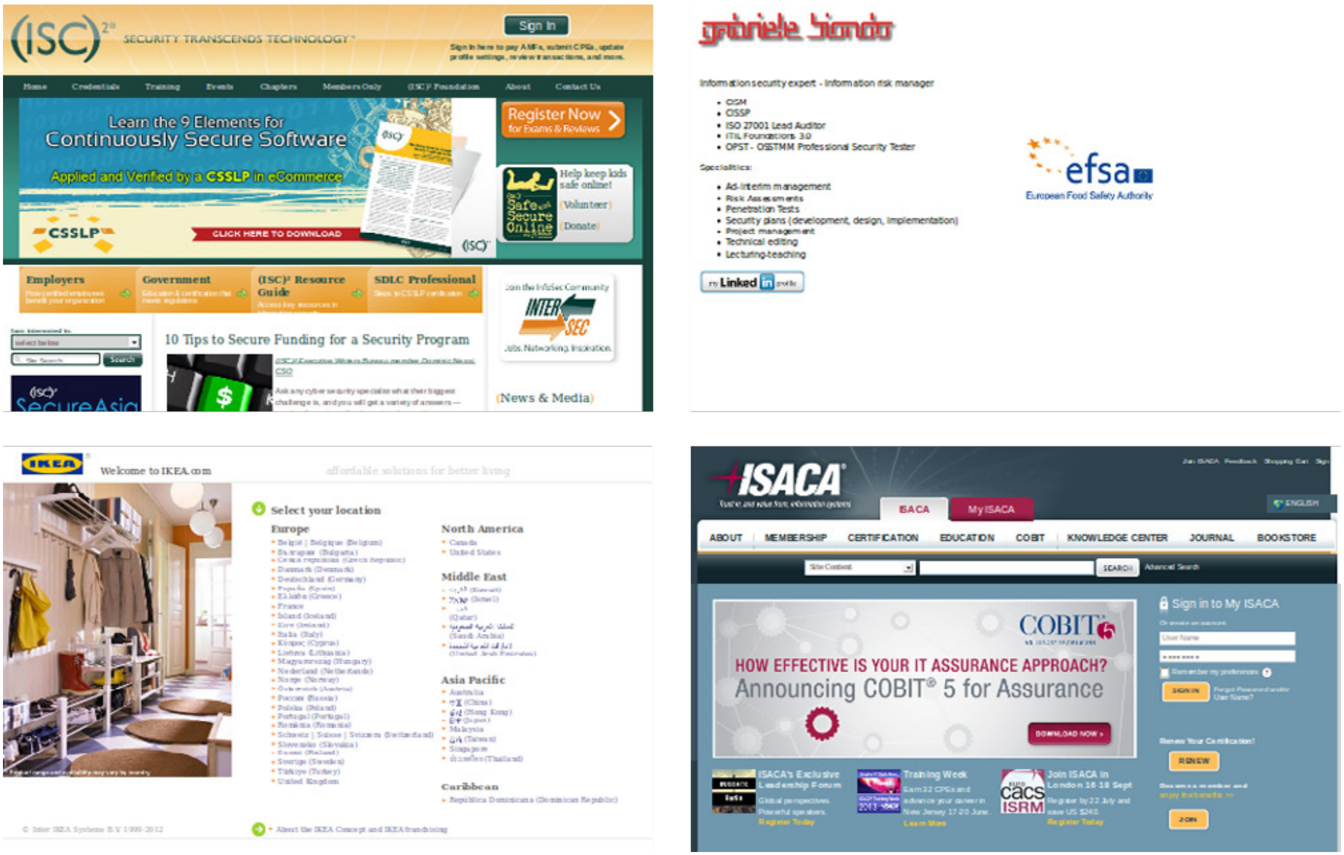

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY
Sign In
Learn the 9 Elements for Continuously Secure Software
Applied and Verified by a CSSLP in eCommerce
CLICK HERE TO DOWNLOAD
Register Now
Help keep kids safe online!
Employers
Government
(ISC)² Resource Guide
SDLC Professional
10 Tips to Secure Funding for a Security Program
News & Media
gabriele biondo
Information security expert - Information risk manager
efsa
European Food Safety Authority
IKEA
Welcome to IKEA.com
Select your location
Europe
North America
Middle East
Asia Pacific
Caribbean
ISACA
COBIT 5
HOW EFFECTIVE IS YOUR IT ASSURANCE APPROACH?
Announcing COBIT® 5 for Assurance
DOWNLOAD NOW
Sign in to My ISACA

**Figure 6.** *Some thumbnail files*

### THE SAFEBROWSING AND WEBAPPS FOLDERS

These folders are not relevant, from the perspective of this analysis.

### THE MINIDUMP FOLDER

This folder is meant to contain data generated from crashes. It may have relevance, but it depends on what has really happened: in general, no conclusion can be drawn. See [17] for further information.

### THE BOOKMARKBACKUP FOLDER

This folder contains the list of bookmarked website, in `.json` format.

### THE CACHE AND STARTUPCACHE FOLDERS

These folders contain the cache of Mozilla Firefox. They are obviously important, for forensics analyses-related purposes.

## ANALYSIS

Manually analyzing every single entry of the cache directory is error prone and time consuming. In order to speed up the process, a MySQL database and a couple of Ruby scripts have been written. These will not be shown nor discussed here: the interested reader can download them from [18] and get in touch with the author. The MySQL database stores the "extractions", being the contents of the `/home/<USERNAME>/.mozilla` folder at a given time. Each extraction is a collection of "entries", being the full paths (hence – the files' references) and their SHA 256 hash. The first of the two scripts (`mozillaExtract.rb`) populates the Database. The second script (`mozillaExtract.rb`) creates an HTML file comparing the last two extractions. A file can then:

- exist in both the two extractions. Two cases:
  - the two instances have the same hash: the file did not change
  - the two instances have different hashes: the file has changed
- appear in the last extraction, but not in the first: this is the case in which the user has visited a new site during the last session
- appear in the first extraction, but not in the last: the file has expired, very likely.

### THE ANALYSIS PROCESS

The analysis has followed quite a simple process:

- create a baseline of the files currently stored in the `.mozilla` folder of the user;
- create a tarball of the `.mozilla` directory, for deeper analysis purposes
- clear mozilla's cache
- create a new baseline (extraction)
- compare the last two baselines
- create a tarball of the `.mozilla` directory, for deeper analysis purposes
- surfing the web (in other words: re-populating the cache folder)
- create a new baseline (extraction)
- compare the last two baselines
- create a tarball of the `.mozilla` directory, for deeper analysis purposes
- by mistake, a link has been hit after "freezing" the cache. Once again, the following steps needed to be performed:
  - create a new baseline (extraction)
  - compare the last two baselines
  - create a tarball of the `.mozilla` directory, for deeper analysis purposes
- open a new private browsing window
- browsed some web content
- a new baseline (extraction)
- compare the last two baselines
- create a tarball of the `.mozilla` directory, for deeper analysis purposes

The process seems more complicated than what it is, actually. The key action, besides browsing, is summarized in the following commands: Listing 2.

As a side note: yes, a `find` could have been used instead. The reasons why the author spent some time writing scripts are that these scripts are only a portion of a bigger project requiring test.Moreover, writing in Ruby is a good fun :)

## RESULTS

The analysis process encompasses analyzing the differences between two adjacent extractions. Here only the first and the last extraction will be discussed, since these are the ones forensically relevant.

### EXTRACTION #1 VS. EXTRACTION #2

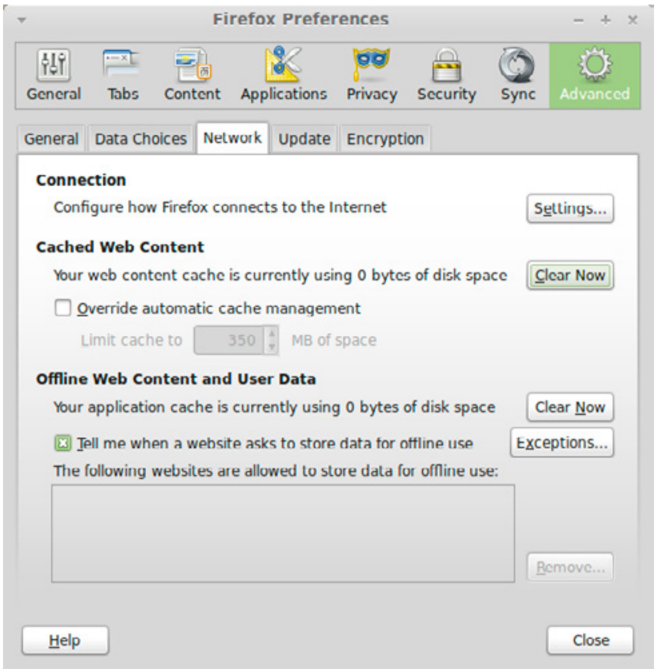
This is the situation where the pre-existent cache was removed with the Mozilla's functionality (see Figure 2). The hypothesis is finding all the cache deleted.

The directory structure is left unchanged: there are still all the directories whose name is like: `/home/gbiondo/.mozilla/firefox/mwad0hks.default/Cache/<NUMBER>`.

As expected: the cache is still *managed* in the same way, so no need to reinvent the wheel here.

**Listing 2.** *Scripts ran to extract Firefox information*

```
gbiondo@linuxMint ~/work $ ./mozillaExtract.rb
gbiondo@linuxMint ~/work $ ./extractionDiff.rb > thirdExtraction.html
gbiondo@linuxMint ~/work $ tar cvzf dotMozilla3.tgz .mozilla/
```



**Connection**

Configure how Firefox connects to the Internet

**Cached Web Content**

Your web content cache is currently using 0 bytes of disk space

□ Override automatic cache management

Limit cache to 350 MB of space

**Offline Web Content and User Data**

Your application cache is currently using 0 bytes of disk space

☒ Tell me when a website asks to store data for offline use

The following websites are allowed to store data for offline use:

**Figure 7.** *The 'clear cache' option*

However, their previous content is expired and a more in-depth look shows that the files haven't been replaced in any way. On the other hand, the following files have been changed: Listing 3.

Files 1 to 4 are obviously involved, since they contain the browser's cache.

File `cookies.sqlite` was not flushed, which is meaningful, since we asked only to get rid of the cache. The contents of both files have been exported, and a `diff --suppress-common-lines` command has been issued. The result is *not reported* on this article, since it is not easily readable on printed paper. The author has checked the results, determining that only mozilla.com and optimizely.com domain related cookies have changed.

Listing 4 illustrates that File 6 reports automatically updated preferences which have no relevance, in this case.

### EXTRACTION #3.1 VS. EXTRACTION #4

[19] shows how to set up the browser in order not to leave tracks. In this test case the setting 'always start Firefox in Private Browsing', described in [20] has been chosen: this reduces background noise and false positives. Finally, to analyze the responses from the remote websites, the connection from Firefox to the Internet is filtered with the Burp Suite, a web proxy used for penetration testing that, in this case, is only used as a passive pass-through.

Changes happened on this directory while surfing the web are reported below: Listing 5.

Four other files have been changed: Listing 6.

The files 4, 5, 6 and 7 are Google's anti-phishing and anti-malware APIs. More info on this technology can be found, for instance, in [21].

**Listing 3.** *Files changed between the two extractions*

```
1. /home/gbiondo/.mozilla/firefox/mwad0hks.default/Cache/_CACHE_001_
2. /home/gbiondo/.mozilla/firefox/mwad0hks.default/Cache/_CACHE_002_
3. /home/gbiondo/.mozilla/firefox/mwad0hks.default/Cache/_CACHE_003_
4. /home/gbiondo/.mozilla/firefox/mwad0hks.default/Cache/_CACHE_MAP_
5. /home/gbiondo/.mozilla/firefox/mwad0hks.default/cookies.sqlite
6. /home/gbiondo/.mozilla/firefox/mwad0hks.default/prefs.js
```

**Listing 4.** *Preferences updated*

```
< user_pref("app.update.lastUpdateTime.browser-cleanup-thumbnails", 1373371780);
---
> user_pref("app.update.lastUpdateTime.browser-cleanup-thumbnails", 1373453395);
25a26
> user_pref("browser.preferences.advanced.selectedTabIndex", 2);
33c34
< user_pref("datareporting.healthreport.lastDataSubmissionRequestedTime", "1373372038107");
---
> user_pref("datareporting.healthreport.lastDataSubmissionRequestedTime", "1373453337939");
41c42
< user_pref("datareporting.sessions.current.activeTicks", 6);
---
> user_pref("datareporting.sessions.current.activeTicks", 12);
46c47
< user_pref("datareporting.sessions.current.totalTime", 28804);
---
> user_pref("datareporting.sessions.current.totalTime", 138221);
```

File 1 shows that some cookies are changed, despite the ‘Private Browsing’ option. Analyzing the difference between the two cookie database, it is shown that Mozilla domain issued new instances of `__utma` and `__utmz`. These are both Google Analytic cookies; `__utma` counts the number of times a visitor has been to a given website (in this case, the Mozilla website) and `__utmz` keeps track of where the user came from. In this case, however, the cookies were requested by a Mozilla add-on. The format of these cookies is sufficiently described in [22], for instance. In both cases, a portion of the second parameter has changed. For `__utma`, this is totally logical, since the second parameter is a random user ID. In the `__utmz` case, the second parameter keeps track of when the related site was last visited. In both cases, this behavior is perfectly acceptable, since the traffic has been generated by an add-on. Three other cookies changed, namely `optimizelyEndUserId`, `optimizelySegments` and `optimizelyBuckets`, the customer is the Mozilla domain. Finally, the google.com’s “PREF” and “NID” cookies changed. This is meaningful, since the ubi.com site has connected to the youtube domain which “touches” those cookies – more info on this can be found in [23]. In principle, this should not have happened, and deserves a deeper analysis.

File 2 shows (`localstore.rdf`) stores toolbar and window size/position settings, and it is not influent on this analysis.

Changes in file 3 are self-explanatory. Listing 7 shows the differences between those two files; values are from the last version.

As a point of interest, all the preferences changed pertain on time-related factors, or on incremental numbers (for instance, the `pingCountTotal` variable). Unless the analyst has access to previous versions of this file, it supplies no help at all.

**Listing 5.** *Interesting files changed between the two extractions*

```
1. /home/gbiondo/.mozilla/firefox/mwad0hks.default/cookies.sqlite
2. /home/gbiondo/.mozilla/firefox/mwad0hks.default/localstore.rdf
3. /home/gbiondo/.mozilla/firefox/mwad0hks.default/prefs.js
```

**Listing 6.** *Other files changed between the two extractions*

```
4. /home/gbiondo/.mozilla/firefox/mwad0hks.default/safebrowsing/goog-malware-shavar.pset
5. /home/gbiondo/.mozilla/firefox/mwad0hks.default/safebrowsing/goog-malware-shavar.sbstore
6. /home/gbiondo/.mozilla/firefox/mwad0hks.default/safebrowsing/goog-phish-shavar.pset
7. /home/gbiondo/.mozilla/firefox/mwad0hks.default/safebrowsing/goog-phish-shavar.sbstore
```

**Listing 7.** *Changes in prefs.js file (final version)*

```
user_pref(“app.update.lastUpdateTime.addon-background-update-timer”, 1373784044);
user_pref(“app.update.lastUpdateTime.blocklist-background-update-timer”, 1373784164);
user_pref(“app.update.lastUpdateTime.browser-cleanup-thumbnails”, 1373783099);
user_pref(“app.update.lastUpdateTime.search-engine-update-timer”, 1373783924);

user_pref(“datareporting.healthreport.lastDataSubmissionRequestedTime”, “1373783864772”);

user_pref(“datareporting.sessions.current.activeTicks”, 29);

user_pref(“datareporting.sessions.current.firstPaint”, 661);
user_pref(“datareporting.sessions.current.main”, 24);
user_pref(“datareporting.sessions.current.sessionRestored”, 694);
user_pref(“datareporting.sessions.current.startTime”, “1373783803368”);
user_pref(“datareporting.sessions.current.totalTime”, 521871);
user_pref(“datareporting.sessions.currentIndex”, 14);

user_pref(“datareporting.sessions.previous.13”, “{\”s\”:1373782979199,\”a\”:22,\”t\”:167239,\”c\”:t
rue,\”m\”:44,\”fp\”:699,\”sr\”:750}”);

user_pref(“extensions.blocklist.pingCountTotal”, 11);
user_pref(“extensions.blocklist.pingCountVersion”, 11);

user_pref(“toolkit.startup.last_success”, 1373783803);
```

## REFERENCES

[1] *http://kb.mozillazine.org/Profiles.ini_file*
[2] *https://developer.mozilla.org/en/docs/Using_content_preferences*
[3] *http://kb.mozillazine.org/Cookies*
[4] *http://kb.mozillazine.org/Downloads_not_visible_in_Download_Manager*
[5] *https://support.mozilla.org/en-US/questions/956373*
[6] *http://support.mozilla.org/en-US/questions/794548*
[7] *http://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data*
[8] *http://kb.mozillazine.org/Places.sqlite*
[9] *http://kb.mozillazine.org/Password_Manager*
[10] *http://kb.mozillazine.org/Webappsstore.sqlite*
[11] *http://kb.mozillazine.org/Blocklist.xml*
[12] *http://kb.mozillazine.org/Profile_folder_-_Firefox*
[13] *http://kb.mozillazine.org/Session_Restore*
[14] *https://developer.mozilla.org/en-US/docs/NSS*
[15] *http://kb.mozillazine.org/Key3.db*
[16] *http://kb.mozillazine.org/Localstore.rdf*
[17] *http://kb.mozillazine.org/Breakpad#Mozilla_Crash_Reporter*
[18] *http://www.gbiondo.org/eforensicsMag*
[19] *http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info*
[20] *http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info#w_how-do-i-always-start-firefox-in-private-browsing*
[21] *https://developers.google.com/safe-browsing/developers_guide_v2*
[22] *http://blog.vkistudios.com/index.cfm/2010/8/31/GA-Basics-The-Structure-of-Cookie-Values*
[23] *http://www.google.com/intl/en_it/policies/technologies/types/*

As expected, the files `_CACHE_00x_` did not change. In a further article, the format of those files will be discussed in a further article.

## CONCLUSIONS

This analysis was superficial, but not shallow: trying to understand Mozilla's Caching is not so trivial as it may seem. Actually, the overall caching mechanism of Mozilla is complex and fascinating, from a coding perspective.

Next steps are repeating the same kind of analysis for other web browsers. In the next article, Google Chrome will be under analysis.

### About the Author

*Gabriele Biondo is a freelance Security Expert and Information Risk Manager, specialized in penetration testing and risk models. Through the years, he achieved several security related certifications, such as CISM, CISSP, ISO 27001 Lead Auditor, OPST. He cooperated with ISECOM, in the past, and now he is supporting eForensics Magazine as proofreader and beta-tester. Outside work, he's interested in photography, maths and his cats :). He can be contacted at gbiondo@gbiondo.org. Gabriele is also interested in developing projects together – shall you have something in mind, just feel free to drop a line or two in the mailbox.*

# THE GOLDEN NUGGET

by Paul Gwinnett

In writing an article about computer forensics for beginners I had to consider my 'Hi Tech/e forensics' introduction, which couldn't really be classed an 'exact science', more a case of various "digital journeys", stepping into the unknown and seeking reassurance by way of experiments and 'sound boarding' with my old mentor. In this article, I have tried to be as candid and practical as possible in the hope that those in the early stages of their e-forensics' career can have an insight into some of the issues I faced in my early years and how I dealt with them.

### What you will learn:

- The early years of an e-forensics' investigator and some of the practical issues.
- Why an initial 'forensic strategy' should be geared towards finding the 'Golden Nugget'
- The importance of asking the right questions
- Finding the evidence can sometimes be the easy part.
- How decisions by a manager/supervisor are critical when proportional time management is required.
- Playing 'Devil's Advocate' and why you should make the Devil your friend
- Corroborating Internet History and the system clock with externally derived artefacts

### What you should know:

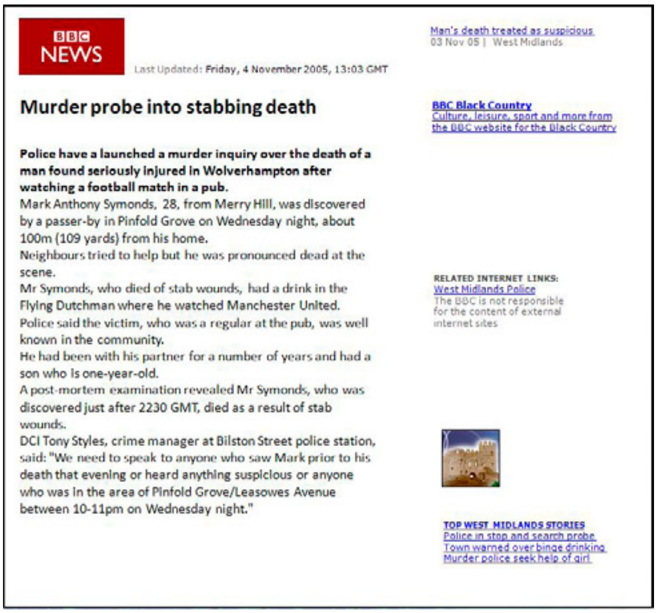
- How Encase works
- How Internet Explorer works
- What is a 'Live' file
- What is 'Unallocated Space'

This 'Digital journey' started on the November 2nd 2005 when unbeknown to me a man by the name of Mark Symons was brutally murdered while walking home from a pub in Wolverhampton. By all accounts it appears to be a preplanned attack whereby, he was approached from the rear and stabbed about 10 times; there was also a suggestion he may have been strangled too.

The usual 'Holmes' incident room was set up and a murder investigation commenced under the operational name 'Mintell'.

My understanding is, that in the May/June of 2006, after approximately 6 months of no credible leads as to who committed the stabbing, an external SIO (Senior Investigation Officer) was bought in to review the case prior to it being 'boxed off' and scaled down.

Having reviewed the case, the reviewing SIO set an action to swab all the family members for DNA. Apparently, there had been a small partial trace of DNA found on the victim's neck, not the normal amount required for court purposes, but maybe enough to identify any potential suspects. I am only guessing, but I imagine it was the statistic showing that the vast majority of murders are 'domestic' related, which led to this extra course of action. Either way, it proved a vital step in the investigation. In the summer of 2006 police visited the victim's sister's address and



BBC NEWS Last Updated: Friday, 4 November 2005, 13:03 GMT

Murder probe into stabbing death

**Police have a launched a murder inquiry over the death of a man found seriously injured in Wolverhampton after watching a football match in a pub.**
Mark Anthony Symonds, 28, from Merry Hill, was discovered by a passer-by in Pinfold Grove on Wednesday night, about 100m (109 yards) from his home.
Neighbours tried to help but he was pronounced dead at the scene.
Mr Symonds, who died of stab wounds, had a drink in the Flying Dutchman where he watched Manchester United.
Police said the victim, who was a regular at the pub, was well known in the community.
He had been with his partner for a number of years and had a son who is one-year-old.
A post-mortem examination revealed Mr Symonds, who was discovered just after 2230 GMT, died as a result of stab wounds.
DCI Tony Styles, crime manager at Bilston Street police station, said: "We need to speak to anyone who saw Mark prior to his death that evening or heard anything suspicious or anyone who was in the area of Pinfold Grove/Leasowes Avenue between 10-11pm on Wednesday night."

Man's death treated as suspicious
03 Nov 05 | West Midlands

**BBC Black Country**
Culture, leisure, sport and more from the BBC website for the Black Country

**RELATED INTERNET LINKS:**
West Midlands Police
The BBC is not responsible for the content of external internet sites

**TOP WEST MIDLANDS STORIES**
Police in stop and search probe
Town warned over binge drinking
Murder police seek help of girl

**Figure 1.** *BBC report*

asked for DNA samples. Also at the address at the time was the sister's husband a man by the name of Peter Britten.

Surprisingly, Britten initially refused to give his DNA and so officers returned a few days later when this time they were successful in obtaining consent and a DNA sample.

The sample of DNA given by Britten, matched the partial sample recovered from the victims neck and so police once again visited Britten's address but this time arrested him on suspicion of murder. Also at the address they found and seized Britten's computer tower.

As was customary in the West Midlands at the time, the initial (triage) analysis was undertaken by the local 'Hi Tech Rep'. The 40GB hard drive was acquired using Encase and the acquired product was then subjected to many key words, which had been supplied by the Incident Room. In this instance, officers from the incident room were invited down to the office and over a few days trawled through all the' search hits'. They found nothing of interest and so the case was delivered to the Central Hi Tech team to review prior to 'filing'.

**Figure 2.** *Exhibit SJS4 contained a 40GB hard drive*

During this period, I was still relatively new to computer forensics having only joined the Hi Tech Crime Unit in 2004. I have been relatively fortunate to have had quite a diverse career in policing; Surveillance, CID and intelligence but starting out in the Hi Tech world was different, there were so many 'unknowns' that learning as you go and treading carefully, seemed to be the only way to go – for me anyway.

In August 2006, I received the case and commenced BIOS checks on the motherboard, only to find the BIOS clock had reset due to a weak battery. "That's a good start!"

| | | | | |
|---|---|---|---|---|
| Exhibit SJS4 | System Time | 00:00 | System Date | 01/01/02 |
| | Actual Time | 15:24 | Actual Date | 15/08/06 |

**Figure 3.** *Checking the BIOS clock*

## THE FORENSIC STRATEGY

On reviewing the submitted paperwork, I noted the 'terms of reference' for the digital investigation related to whether Britten had used his computer to research DNA on the Internet. Despite this clear focus I am a great believer that before commencing any investigation a digital investigator has a duty to find out as much information as possible, as they can often be best placed to consider where evidence may be found.

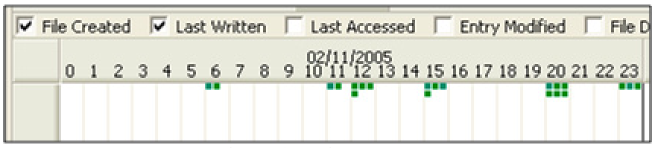
I telephoned the officer submitting the paperwork and discussed the case in detail. If I can get a good understanding of a case – the 'why', 'when', 'how', 'where' and 'who', I can formulate various 'hypothesis' and consider their impact and resulting residue on the digital environment. This helps me to tailor an initial 'digital forensic strategy' towards finding the ideal evidence or what I like to call 'The Golden Nugget'.

My strategy in this instance centred around the hypothesis that Britten may have, at some point snapped, and in the process of snapping may have dropped his guard. So I was going to initially focus my analysis around the 2nd November 2005 – the day of the murder. It was estimated that Mark Symonds had been murdered at 22:45hrs on the night of the 2nd.

## 'LIVE' V 'UNALLOCATED' ARTEFACTS

Using Encase I used the' time line' facility to identify any remaining live files for the 2nd: Figure 4.

Bearing in mind Britten was a heavy user of 40GB machine and the machine had been used regularly for 7-8 months since the 2nd (prior to its seizure), it was no surprise to see very few 'live' files remaining. As can be seen from the above snapshot, there appeared pockets of activity, start-



☑ File Created ☑ Last Written □ Last Accessed □ Entry Modified □ File D

**Figure 4.** *Timeline of live files for 2nd November*

ing at 0600hrs and finishing at midnight. I browsed the live files and noticed a cookie called *www.guntrader.co.uk*: Figure 5.

I thought this was a bit odd; the murder had taken place using a knife. Nevertheless, I decided to run 'guntrader' as a keyword across the whole case including 'Unallocated Space'.

I started trawling through the live 'search hits' and then had a look at the hits in 'Unallocated Space'.

I came across a 'guntrader' hit that was contained in the following string within unallocated space:

```
p-.
p-.
p-.URL.....uu._E...uu._E....etc...etc
p-.Visited:Administrator@http://www.guntrader.
co.uk....etc...etc
p-.
p-.
```

As this appeared to be fragments of an 'index.dat' (Internet Explorer History file) I decided to scroll up and down to see what other entries were apparent and nearby. At the time I recall being surprised that all the entries were not chronological but completely random within what was left of the index.dat.

## THE GOLDEN NUGGETT

I scrolled up and came across this entry:

```
p-.
p-.
p-.URL.....uu._E...uu._E....etc...etc
p-. Visited: Administrator@http://search.msn.com/
results.aspx?q=how+to+kill+a+man&first=11&FORM=PORE
p-.
p-.
```

I recall seeing this and thinking: "Is this really what I think it is?" I selected the date and time string within the entry – then – Encase – bookmark – 'Windows date and time' and converted it

```
p-.
p-.
p-.URL.....uu._E...uu._E....etc...etc
p-. Visited: Administrator@http://search.msn.com/
results.aspx?q=how+to+kill+a+man&first=11&FORM=PORE
p-.
p-.
```

The date and time converted to: *02/11/2005 15:43:22.*

"So someone has typed 'How to kill a man' into an MSN search engine 7 hours before the murder took place?" ............................BINGO!

I couldn't resist it – picked up the phone to share the information with the officer in the case: "Hi, Paul here, you'll never guess what I've found"........ you can guess the rest.

## PLAYING DEVIL'S ADVOCATE

The initial euphoria was short-lived as I slowly came to terms with the sobering thought that what I had found could be worthless unless I can show that this unallocated remnant of internet history was once the live and active 'index.dat' file that was being written to by Internet Explorer, at the time of the murder. Did I say 'time' Oh no....the BIOS clock!

By now 'Devil's advocate' was running riot:

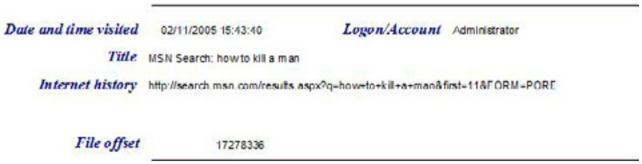
"How else can I prove the clock was accurate at the time?"

"Where are the original web pages, could they still be on the drive?"

"Perhaps some of the original pages will have a date and time stamp?"

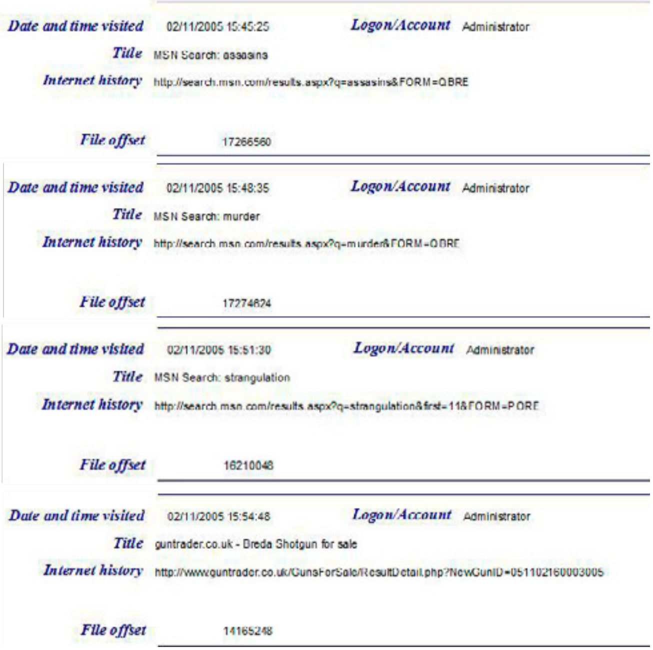
"Could I corroborate the BIOS clock with any logons or logs of remote sites visited?"

"Could the fragments of 'Index.dat' be from a different machine?"



Date and time visited 02/11/2005 15:43:40 Logon/Account Administrator
Title MSN Search: how to kill a man
Internet history http://search.msn.com/results.aspx?q=how+to+kill+a+man&first=11&FORM=PORE
File offset 17278336

**Figure 6.** *Record of 'Internet History' recovered from unallocated fragments*



Date and time visited 02/11/2005 15:45:25 Logon/Account Administrator
Title MSN Search: assasins
Internet history http://search.msn.com/results.aspx?q=assasins&FORM=QBRE
File offset 17266560

Date and time visited 02/11/2005 15:48:35 Logon/Account Administrator
Title MSN Search: murder
Internet history http://search.msn.com/results.aspx?q=murder&FORM=QBRE
File offset 17274624

Date and time visited 02/11/2005 15:51:30 Logon/Account Administrator
Title MSN Search: strangulation
Internet history http://search.msn.com/results.aspx?q=strangulation&first=11&FORM=PORE
File offset 16210048

Date and time visited 02/11/2005 15:54:48 Logon/Account Administrator
Title guntrader.co.uk - Breda Shotgun for sale
Internet history http://www.guntrader.co.uk/GunsForSale/ResultDetail.php?NewGunID=051102160003005
File offset 14165248

**Figure 7.** *Four further records of 'Internet History' recovered from unallocated fragments*

Who had access to the 'Administrator' account?

How can I authenticate this fragment as the original live index.dat file?

etc. etc.

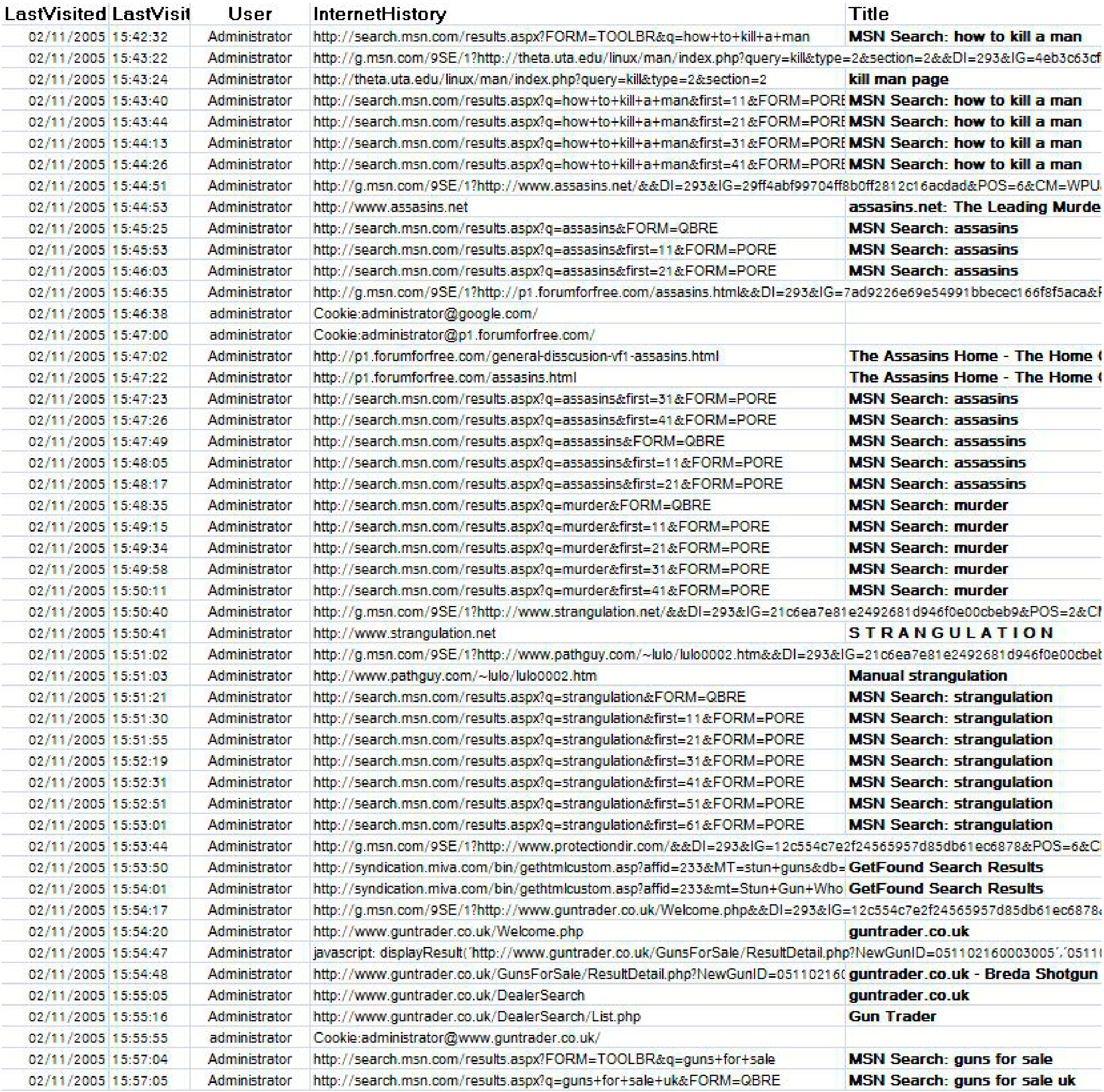
## PROPORTIONALITY

Fortunately for me, I had an excellent Detective Sergeant who understood the importance of investigation and proportionality. There was no pressure or rush, and in my opinion rightly so. If an organisation (Police Force) are willing to pay for a full blown incident room with 8 – 12 detectives, FLO's, SIO's and inputters for over 6 months then surely a single Hi Tech investigator developing an evidential 'golden nugget' is money well spent?

The first thing I did was to run Net-analysis across the entire machine to pull out any live or unallocated fragments of Internet history. In total there were 3 x fragments of Internet history found within 'Unallocated space', which contained date and time references to early November 2005

I then exported via net-analysis into Microsoft Access. Access was always my tool of choice when analysing Internet history as it gave me complete control over building queries and generating reports for presentations at court.

I used Access to convert an index.dat entry from its native appearance of:



| LastVisited | LastVisit | User | InternetHistory | Title |
|---|---|---|---|---|
| 02/11/2005 | 15:42:32 | Administrator | http://search.msn.com/results.aspx?FORM=TOOLBR&q=how+to+kill+a+man | **MSN Search: how to kill a man** |
| 02/11/2005 | 15:43:22 | Administrator | http://g.msn.com/9SE/1?http://theta.uta.edu/linux/man/index.php?query=kill&type=2&section=2&&DI=293&IG=4eb3c63cf | |
| 02/11/2005 | 15:43:24 | Administrator | http://theta.uta.edu/linux/man/index.php?query=kill&type=2&section=2 | **kill man page** |
| 02/11/2005 | 15:43:40 | Administrator | http://search.msn.com/results.aspx?q=how+to+kill+a+man&first=11&FORM=PORE | **MSN Search: how to kill a man** |
| 02/11/2005 | 15:43:44 | Administrator | http://search.msn.com/results.aspx?q=how+to+kill+a+man&first=21&FORM=PORE | **MSN Search: how to kill a man** |
| 02/11/2005 | 15:44:13 | Administrator | http://search.msn.com/results.aspx?q=how+to+kill+a+man&first=31&FORM=PORE | **MSN Search: how to kill a man** |
| 02/11/2005 | 15:44:26 | Administrator | http://search.msn.com/results.aspx?q=how+to+kill+a+man&first=41&FORM=PORE | **MSN Search: how to kill a man** |
| 02/11/2005 | 15:44:51 | Administrator | http://g.msn.com/9SE/1?http://www.assasins.net/&&DI=293&IG=29ff4abf99704ff8b0ff2812c16acdad&POS=6&CM=WPU | |
| 02/11/2005 | 15:44:53 | Administrator | http://www.assasins.net | **assasins.net: The Leading Murde** |
| 02/11/2005 | 15:45:25 | Administrator | http://search.msn.com/results.aspx?q=assasins&FORM=QBRE | **MSN Search: assasins** |
| 02/11/2005 | 15:45:53 | Administrator | http://search.msn.com/results.aspx?q=assasins&first=11&FORM=PORE | **MSN Search: assasins** |
| 02/11/2005 | 15:46:03 | Administrator | http://search.msn.com/results.aspx?q=assasins&first=21&FORM=PORE | **MSN Search: assasins** |
| 02/11/2005 | 15:46:35 | Administrator | http://g.msn.com/9SE/1?http://p1.forumforfree.com/assasins.html&&DI=293&IG=7ad9226e69e54991bbecec166f8f5aca&P | |
| 02/11/2005 | 15:46:38 | administrator | Cookie:administrator@google.com/ | |
| 02/11/2005 | 15:47:00 | administrator | Cookie:administrator@p1.forumforfree.com/ | |
| 02/11/2005 | 15:47:02 | Administrator | http://p1.forumforfree.com/general-disscusion-vf1-assasins.html | **The Assasins Home - The Home (** |
| 02/11/2005 | 15:47:22 | Administrator | http://p1.forumforfree.com/assasins.html | **The Assasins Home - The Home (** |
| 02/11/2005 | 15:47:23 | Administrator | http://search.msn.com/results.aspx?q=assasins&first=31&FORM=PORE | **MSN Search: assasins** |
| 02/11/2005 | 15:47:26 | Administrator | http://search.msn.com/results.aspx?q=assasins&first=41&FORM=PORE | **MSN Search: assasins** |
| 02/11/2005 | 15:47:49 | Administrator | http://search.msn.com/results.aspx?q=assassins&FORM=QBRE | **MSN Search: assassins** |
| 02/11/2005 | 15:48:05 | Administrator | http://search.msn.com/results.aspx?q=assassins&first=11&FORM=PORE | **MSN Search: assassins** |
| 02/11/2005 | 15:48:17 | Administrator | http://search.msn.com/results.aspx?q=assassins&first=21&FORM=PORE | **MSN Search: assassins** |
| 02/11/2005 | 15:48:35 | Administrator | http://search.msn.com/results.aspx?q=murder&FORM=QBRE | **MSN Search: murder** |
| 02/11/2005 | 15:49:15 | Administrator | http://search.msn.com/results.aspx?q=murder&first=11&FORM=PORE | **MSN Search: murder** |
| 02/11/2005 | 15:49:34 | Administrator | http://search.msn.com/results.aspx?q=murder&first=21&FORM=PORE | **MSN Search: murder** |
| 02/11/2005 | 15:49:58 | Administrator | http://search.msn.com/results.aspx?q=murder&first=31&FORM=PORE | **MSN Search: murder** |
| 02/11/2005 | 15:50:11 | Administrator | http://search.msn.com/results.aspx?q=murder&first=41&FORM=PORE | **MSN Search: murder** |
| 02/11/2005 | 15:50:40 | Administrator | http://g.msn.com/9SE/1?http://www.strangulation.net/&&DI=293&IG=21c6ea7e81e2492681d946f0e00cbeb9&POS=2&C | |
| 02/11/2005 | 15:50:41 | Administrator | http://www.strangulation.net | **STRANGULATION** |
| 02/11/2005 | 15:51:02 | Administrator | http://g.msn.com/9SE/1?http://www.pathguy.com/~lulo/lulo0002.htm&&DI=293&IG=21c6ea7e81e2492681d946f0e00cbet | |
| 02/11/2005 | 15:51:03 | Administrator | http://www.pathguy.com/~lulo/lulo0002.htm | **Manual strangulation** |
| 02/11/2005 | 15:51:21 | Administrator | http://search.msn.com/results.aspx?q=strangulation&FORM=QBRE | **MSN Search: strangulation** |
| 02/11/2005 | 15:51:30 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=11&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:51:55 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=21&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:52:19 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=31&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:52:31 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=41&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:52:51 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=51&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:53:01 | Administrator | http://search.msn.com/results.aspx?q=strangulation&first=61&FORM=PORE | **MSN Search: strangulation** |
| 02/11/2005 | 15:53:44 | Administrator | http://g.msn.com/9SE/1?http://www.protectiondir.com/&&DI=293&IG=12c554c7e2f24565957d85db61ec6878&POS=6&C | |
| 02/11/2005 | 15:53:50 | Administrator | http://syndication.miva.com/bin/gethtmlcustom.asp?affid=233&MT=stun+guns&db= | **GetFound Search Results** |
| 02/11/2005 | 15:54:01 | Administrator | http://syndication.miva.com/bin/gethtmlcustom.asp?affid=233&mt=Stun+Gun+Who | **GetFound Search Results** |
| 02/11/2005 | 15:54:17 | Administrator | http://g.msn.com/9SE/1?http://www.guntrader.co.uk/Welcome.php&&DI=293&IG=12c554c7e2f24565957d85db61ec6878 | |
| 02/11/2005 | 15:54:20 | Administrator | http://www.guntrader.co.uk/Welcome.php | **guntrader.co.uk** |
| 02/11/2005 | 15:54:47 | Administrator | javascript: displayResult('http://www.guntrader.co.uk/GunsForSale/ResultDetail.php?NewGunID=051102160003005','0511 | |
| 02/11/2005 | 15:54:48 | Administrator | http://www.guntrader.co.uk/GunsForSale/ResultDetail.php?NewGunID=05110216 | **guntrader.co.uk - Breda Shotgun** |
| 02/11/2005 | 15:55:05 | Administrator | http://www.guntrader.co.uk/DealerSearch | **guntrader.co.uk** |
| 02/11/2005 | 15:55:16 | Administrator | http://www.guntrader.co.uk/DealerSearch/List.php | **Gun Trader** |
| 02/11/2005 | 15:55:55 | administrator | Cookie:administrator@www.guntrader.co.uk/ | |
| 02/11/2005 | 15:57:04 | Administrator | http://search.msn.com/results.aspx?FORM=TOOLBR&q=guns+for+sale | **MSN Search: guns for sale** |
| 02/11/2005 | 15:57:05 | Administrator | http://search.msn.com/results.aspx?q=guns+for+sale+uk&FORM=QBRE | **MSN Search: guns for sale uk** |

**Figure 8.** *'Notable' afternoon sessio*

```
p-.
p-.
p-.URL.....uu._E...uu._E....etc...etc
p-. Visited: Administrator@http://search.msn.com/
results.aspx?q=how+to+kill+a+man&first=11&FORM=PORE
```

In to something more presentable for court, like this: Figure 6. Also within the same 25 minute afternoon session were the following examples of recorded internet history: Figure 7.

The notable afternoon session involving researching 'How to kill a man' was registered in the fragments as commencing at 15:42hrs and finishing at 15:57hrs. This 'notable' session with duplicates removed looked like this: Figure 8.

To the trained eye, it seems fairly obvious what has occurred on the afternoon of the 2nd November; however bearing in mind this is the crown court of a murder trial, was I really in a position to say it *had* occurred? Ultimately, I knew what I wanted to state in my 'Findings' and I used this objective to evaluate which areas needed substantiating. Once I had identified the weaker areas which were open to challenge, I could then explore steps to counter any arguments.

This process resulted in various weaker areas, the two major ones being:

- Authenticating the 3 x fragments of 'internet history' found in 'unallocated space' as being the original live index.dat files in use on the day
- Verifying that the computer's clock was accurate on or around the day of the murder

When the entries for the whole day were processed using net-analysis and access, activity for the whole day looked like this: Figure 9.

This was useful stuff for the 'incident room' as it gave a good picture of the activity throughout the whole day which the Detectives from the incident room could check against the accounts given by witnesses.

With verifying the clock in mind, I set about locating the original web pages; however, despite searching long and hard using keywords, I had no success. On reflection, it is understandable when you consider the drive is only 40GB and has been used regularly for a period of 7 months since the day in question. So I temporarily switched my attention to authenticating the fragments found.

To achieve this, I decided to review the live artefacts which were left on the drive and compare these with the fragments of 'internet history' to see if there was any correlation between the two (Figure 10).

Two cookies were still current/live and on the drive, one called 'guntrader' the other 'forumforfree'

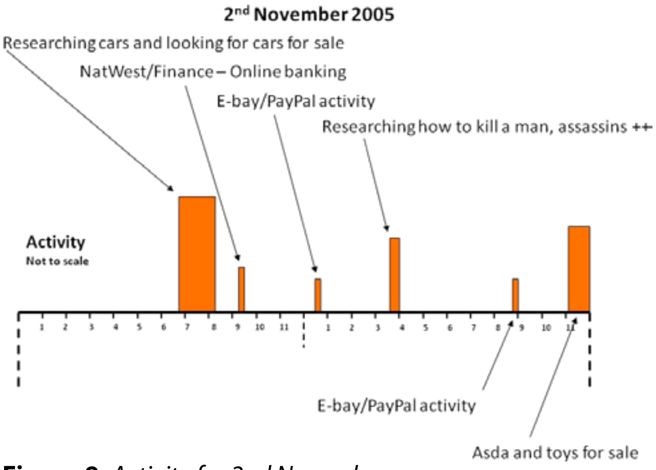
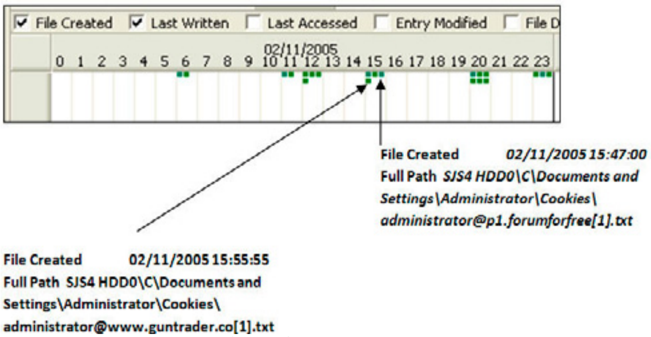


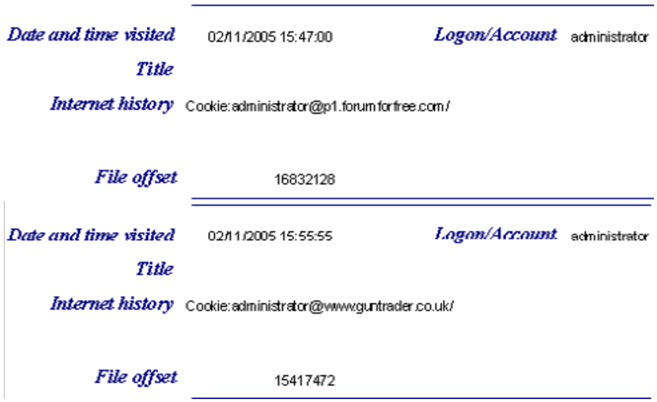
**Figure 9.** *Activity for 2nd November*



File Created 02/11/2005 15:47:00
Full Path *SJS4 HDD0\C\Documents and Settings\Administrator\Cookies\administrator@p1.forumforfree[1].txt*

File Created 02/11/2005 15:55:55
Full Path SJS4 HDD0\C\Documents and Settings\Administrator\Cookies\administrator@www.guntrader.co[1].txt

**Figure 10.** *'Live' artefacts for 2nd November*



| | |
|---|---|
| Date and time visited | 02/11/2005 15:47:00 |
| Logon/Account | administrator |
| Title | |
| Internet history | Cookie:administrator@p1.forumforfree.com/ |
| File offset | 16832128 |

| | |
|---|---|
| Date and time visited | 02/11/2005 15:55:55 |
| Logon/Account | administrator |
| Title | |
| Internet history | Cookie:administrator@www.guntrader.co.uk/ |
| File offset | 15417472 |

**Figure 11.** *Two records of 'Internet History' from unallocated fragments*

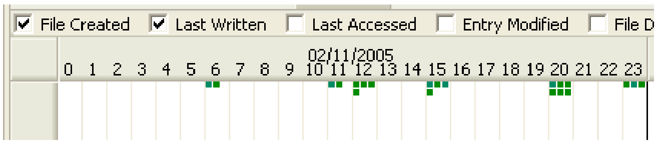
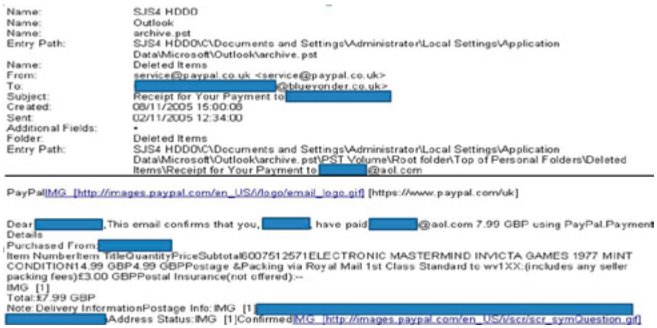


**Figure 12.** *Timeline of live files for 2nd November*



```
Name:               SJS4 HDD0
Name:               Outlook
Name:               archive.pst
Entry Path:         SJS4 HDD0\C\Documents and Settings\Administrator\Local Settings\Application
                    Data\Microsoft\Outlook\archive.pst
Name:               Deleted Items
From:               service@paypal.co.uk <service@paypal.co.uk>
To:                 [redacted]@blueyonder.co.uk>
Subject:            Receipt for Your Payment to [redacted]
Created:            08/11/2005 15:00:08
Sent:               02/11/2005 12:34:00
Additional Fields:  -
Folder:             Deleted Items
Entry Path:         SJS4 HDD0\C\Documents and Settings\Administrator\Local Settings\Application
                    Data\Microsoft\Outlook\archive.pst\PST Volume\Root folder\Top of Personal Folders\Deleted
                    Items\Receipt for Your Payment to [redacted]@aol.com

PayPalIMG [http://images.paypal.com/en_US/i/logo/email_logo.gif] [https://www.paypal.com/uk]

Dear [redacted],This email confirms that you, [redacted], have paid [redacted]@aol.com 7.99 GBP using PayPal.Payment
Details
Purchased From: [redacted]
Item NumberItem TitleQuantityPriceSubtotal600751 2571ELECTRONIC MASTERMIND INVICTA GAMES 1977 MINT
CONDITION14.99 GBP4.99 GBPPostage &Packing via Royal Mail 1st Class Standard to wv1XX:(includes any seller
packing fees)£3.00 GBPPostal Insurance(not offered):--
IMG [1]
Total:£7.99 GBP
Note: Delivery InformationPostage Info: IMG [1 [redacted]
[redacted]Address Status:IMG [1]ConfirmedIMG [http://images.paypal.com/en_US/i/scr/scr_symQuestion.gif]
```

**Figure 13.** *Deleted email found on SJS4*

A search across the fragments of 'internet history' produced the following records: Figure 11.

Once I had found that the 'internet history' (fragments) had registered the arrival of two 'Live' cookie files which were still live and current on the machine, it gave me the reassurance I sought and the corroboration necessary to authenticate the remnants found as the original live index.dat files in use on the day; Well...........not quite!

I still hadn't been able to verify the accuracy of the computer's clock. If the computer clock was a week or month out it could have been anytime within a 14 or 60 day period. I still needed to verify the computer clock on or around the day in question. I once again turned to the live artefacts and ran through the files (Figure 12). I came across the below deleted email: Figure 13. This email together with a second email proved very useful in confirming the accuracy of the clock on the 2nd November. The reason the emails proved so useful, was because, I also found within the fragments of 'internet history' the following record: Figure 14. When you compare the email: Figure 15.

You can see the 'item ID' for the 'Paypal – Send Money'' registered in fragment of 'internet history' is the same as the 'Item Number' in the email, and that this e-mail is a direct automated response from PayPal, in response to the purchase of an electronic mastermind game (ID 6007512571).

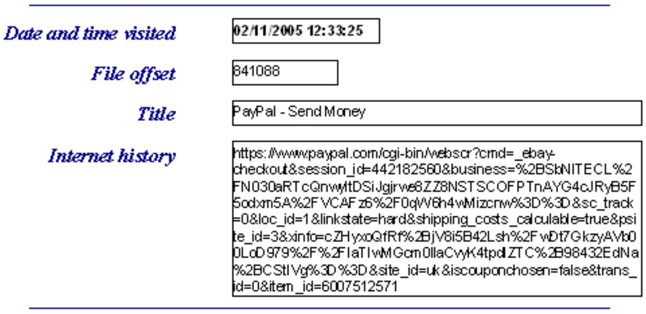
The 'Sent' time and date of the e-mail (02/11/2005 12:34:00) would have been derived from PayPals systems or servers, which are expected to be accurate. On this basis, the PayPal transaction recorded in the index.dat file and the corresponding e-bay response clarifies that, during this period, the clocks were relatively synchronised and accurate.

In addition, a second very similar 'internet history' record and corresponding email was also found, this time at 20:56hrs on 2nd November (Figure 16).

When you compare the email: Figure 17.

I was now comfortable that the clock on the machine was accurate at both 12:34hrs and 20:56hrs on the 2nd November either side of the 'Notable' afternoon session. Furthermore, the 3 separate fragments of the index.dat files found in 'Unallocated Space' had been authenticated and corroborated by the externally derived artefacts namely:

```
1 x e-mail sent by PayPal at - 02/11/2005 12:34:00
1 x Cookie received from p1.forumforfree.com -
02/11/2005 15:47:00
1 x Cookie received from guntrader.co.uk at -
02/11/2005 15:55:55
1 x e-mail sent by PayPal at - 02/11/2005 20:56:50
```

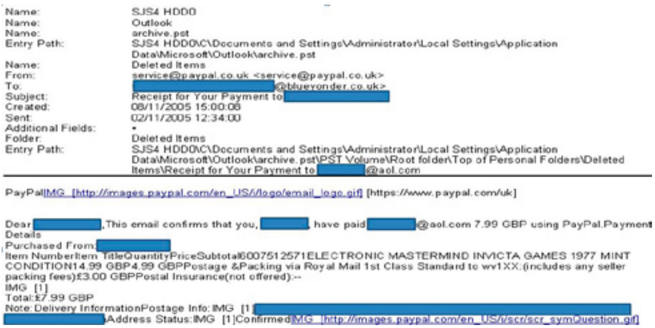

Date and time visited 02/11/2005 12:33:25

File offset 841088

Title PayPal - Send Money

Internet history https://www.paypal.com/cgi-bin/webscr?cmd=_ebay-checkout&session_id=442182560&business=%2BSbNITECL%2FN030aRTcQnwyltDSiJgjrwe8ZZ8NSTSCOFPTnAYG4cJRyB5F5odxm5A%2FVCAFz6%2F0qVV6h4wMizcrw%3D%3D&sc_track=0&loc_id=1&linkstate=hard&shipping_costs_calculable=true&psite_id=3&xinfo=cZHyxoQfRf%2BjV8i5B42Lsh%2FwDt7GkzyAVb00LoD979%2F%2FIaTIwMGcm0llaCvyK4tpdlZTC%2B98432EdNa%2BCStIVg%3D%3D&site_id=uk&iscouponchosen=false&trans_id=0&item_id=6007512571

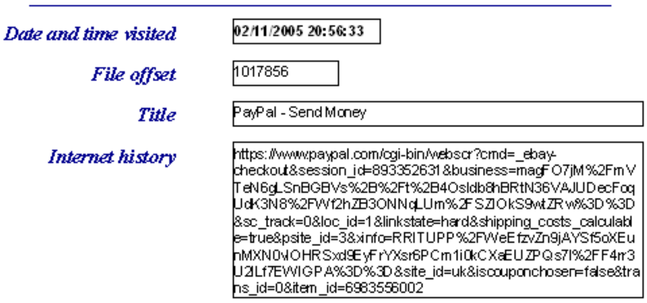
**Figure 14.** *'Internet History' record recovered from fragments*


Name: SJS4 HDD0
Name: Outlook
Name: archive.pst
Entry Path: SJS4 HDD0\C\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\archive.pst
Name: Deleted Items
From: service@paypal.co.uk <service@paypal.co.uk>
To: [redacted]@blueyonder.co.uk>
Subject: Receipt for Your Payment to [redacted]
Created: 08/11/2005 15:00:08
Sent: 02/11/2005 12:34:00
Additional Fields: •
Folder: Deleted Items
Entry Path: SJS4 HDD0\C\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\archive.pst\PST Volume\Root folder\Top of Personal Folders\Deleted Items\Receipt for Your Payment to [redacted]@aol.com

PayPalIMG [http://images.paypal.com/en_US/i/logo/email_logo.gif] [https://www.paypal.com/uk]

Dear [redacted],This email confirms that you, [redacted], have paid [redacted]@aol.com 7.99 GBP using PayPal.Payment Details
Purchased From:[redacted]
Item NumberItem TitleQuantityPriceSubtotal6007512571ELECTRONIC MASTERMIND INVICTA GAMES 1977 MINT CONDITION14.99 GBP4.99 GBPPostage &Packing via Royal Mail 1st Class Standard to wv1XX:(includes any seller packing fees)£3.00 GBPPostal Insurance(not offered):--
IMG [1]
Total:£7.99 GBP
Note: Delivery InformationPostage Info: IMG [1[redacted]
[redacted]Address Status:IMG [1]ConfirmedIMG [http://images.paypal.com/en_US/i/scr/scr_symQuestion.gif]

**Figure 15.** *Deleted email with 'Item ID' highlighted*

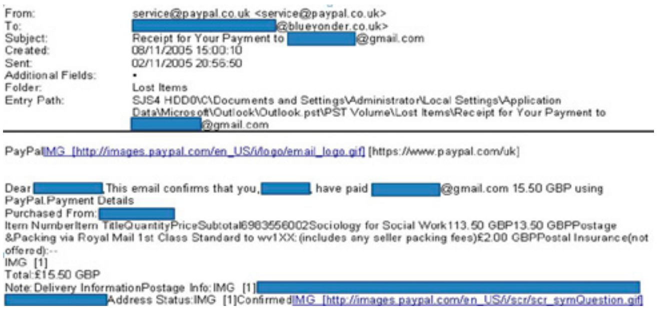

Date and time visited 02/11/2005 20:56:33

File offset 1017856

Title PayPal - Send Money

Internet history https://www.paypal.com/cgi-bin/webscr?cmd=_ebay-checkout&session_id=893352631&business=magFO7jM%2FmVTeN6gLSnBGBVs%2B%2Ft%2B4Osldb8hBRtN36VAJUDecFoqUdK3N8%2FWf2hZB3ONNqLUm%2FSZIOkS9wtZRw%3D%3D&sc_track=0&loc_id=1&linkstate=hard&shipping_costs_calculable=true&psite_id=3&xinfo=RRITUPP%2FWeEfzvZn9jAYSf5oXEunMXN0vIOHRSxd9EyFrYXsr6PCm1i0kCXaEUZPQs7I%2FF4rr3U2ILf7EWIGPA%3D%3D&site_id=uk&iscouponchosen=false&trans_id=0&item_id=6983556002

**Figure 16.** *'Internet History' record recovered from fragments*


From: service@paypal.co.uk <service@paypal.co.uk>
To: [redacted]@blueyonder.co.uk>
Subject: Receipt for Your Payment to [redacted]@gmail.com
Created: 08/11/2005 15:00:10
Sent: 02/11/2005 20:56:50
Additional Fields: •
Folder: Lost Items
Entry Path: SJS4 HDD0\C\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook\Outlook.pst\PST Volume\Lost Items\Receipt for Your Payment to [redacted]@gmail.com

PayPalIMG [http://images.paypal.com/en_US/i/logo/email_logo.gif] [https://www.paypal.com/uk]

Dear [redacted],This email confirms that you, [redacted], have paid [redacted]@gmail.com 15.50 GBP using PayPal.Payment Details
Purchased From:[redacted]
Item NumberItem TitleQuantityPriceSubtotal6983556002Sociology for Social Work113.50 GBP13.50 GBPPostage &Packing via Royal Mail 1st Class Standard to wv1XX:(includes any seller packing fees)£2.00 GBPPostal Insurance(not offered):--
IMG [1]
Total:£15.50 GBP
Note: Delivery InformationPostage Info: IMG [1][redacted]
[redacted]Address Status:IMG [1]ConfirmedIMG [http://images.paypal.com/en_US/i/scr/scr_symQuestion.gif]

**Figure 17.** *A second deleted email found on SJS4*

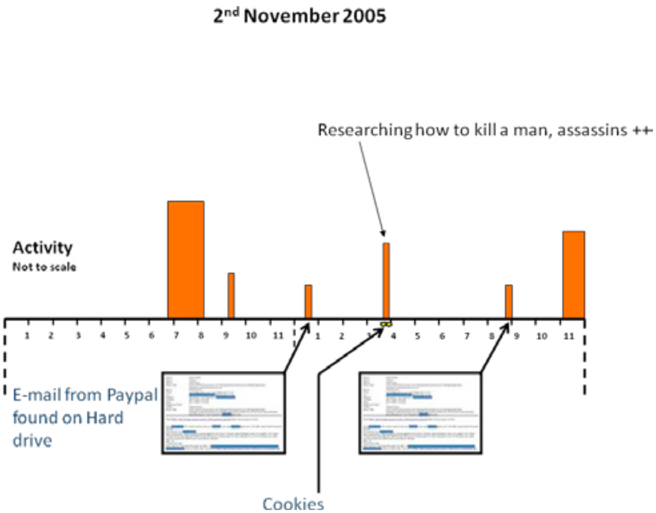
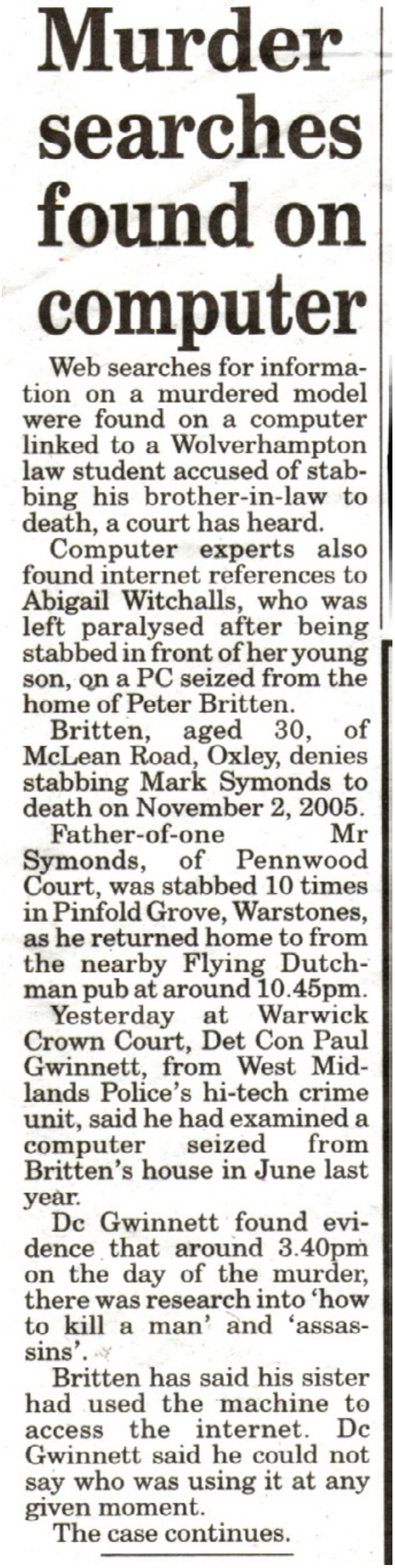


**Figure 18.** *Internet activity from 'Unallocated space' compared to externally derived 'Live/Deleted' artefacts*



Murder searches found on computer

Web searches for information on a murdered model were found on a computer linked to a Wolverhampton law student accused of stabbing his brother-in-law to death, a court has heard.

Computer experts also found internet references to Abigail Witchalls, who was left paralysed after being stabbed in front of her young son, on a PC seized from the home of Peter Britten.

Britten, aged 30, of McLean Road, Oxley, denies stabbing Mark Symonds to death on November 2, 2005.

Father-of-one Mr Symonds, of Pennwood Court, was stabbed 10 times in Pinfold Grove, Warstones, as he returned home to from the nearby Flying Dutchman pub at around 10.45pm.

Yesterday at Warwick Crown Court, Det Con Paul Gwinnett, from West Midlands Police's hi-tech crime unit, said he had examined a computer seized from Britten's house in June last year.

Dc Gwinnett found evidence that around 3.40pm on the day of the murder, there was research into 'how to kill a man' and 'assassins'.

Britten has said his sister had used the machine to access the internet. Dc Gwinnett said he could not say who was using it at any given moment.

The case continues.

**Figure 19.** *Newspaper reports from the Express and Star*

Despite this satisfying outcome, and without wishing to create too much bedtime reading, there was still a considerable amount of work to be undertaken including:

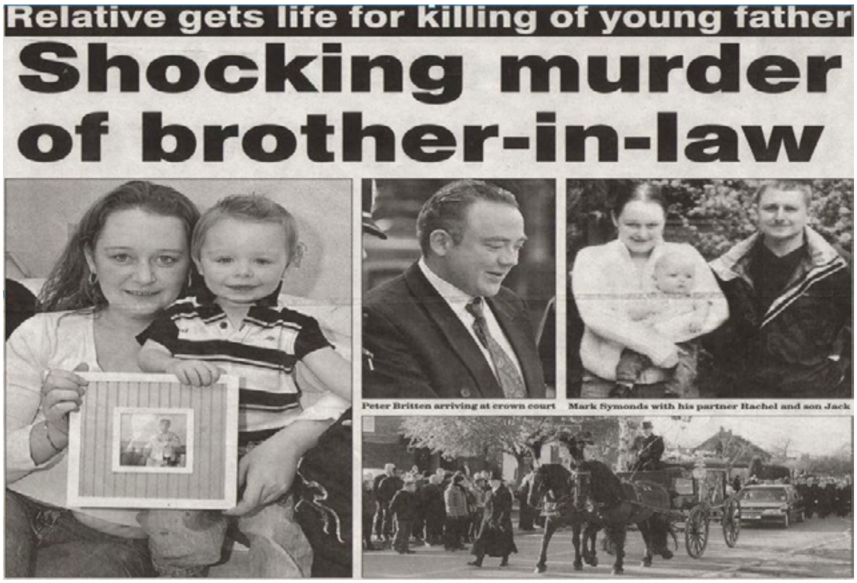
- Cloning the original drive and viewing 'operation' in its native environment
- Checking the 'logon on' of user account 'Administrator' and whether it was password protected. (in this instance – not password protected)
- Re producing the entire notable afternoon session
- Producing 500 pages of internet activity for the 1st and 2nd November
- Producing further notable 'internet activity' of research into DNA techniques and the attack on Abigail Witchall
- Producing a 50 slide PowerPoint presentation to introduce the 8 separate exhibits

However, once I had verified my work with my colleagues within the department and subjected myself to a further dose of 'Devil's Advocate' I felt as reassured as I could be that I had covered as many eventualities as possible.

I chose to use 'PowerPoint' to present my evidence as I was acutely aware that some of the jury may have never used a computer before let alone a web browser. Fortunately, the prosecuting QC (Queen's Counsel) agreed to give me control over the delivery of my presentation. This allowed me to don my 'Teacher Trainer' hat and focus the initial part of the presentation towards training the Jury in how an IE web browser works and what gets recorded in the 'Index.dat' files when a search has taken place.

During the trial, I gave my evidence using a 50 slide PowerPoint presentation which included

- Explaining to the jury how a web browser works
- How 'Internet activity' using an IE browser is registered within 'Index.dat' files
- Introduction to computer SJS4 and how it operates/boots
- The 3 x fragments of 'internet history' found on SJS4
- 'Internet activity' for the 1st and 2nd November
- 'Internet activity' for the 'notable' afternoon session



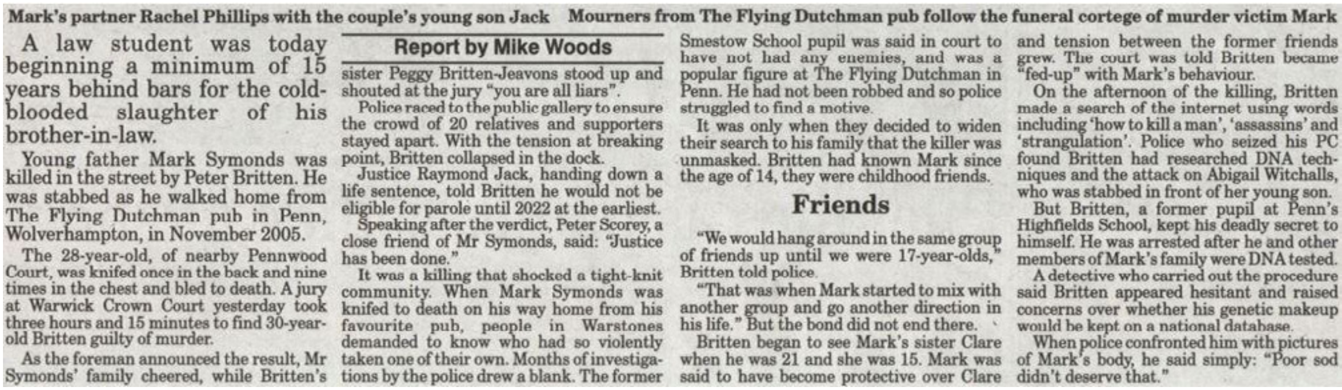
Relative gets life for killing of young father

Shocking murder of brother-in-law

Peter Britten arriving at crown court

Mark Symonds with his partner Rachel and son Jack

**Figure 20.** *Newspaper reports from the Express and Star*



Mark's partner Rachel Phillips with the couple's young son Jack Mourners from The Flying Dutchman pub follow the funeral cortege of murder victim Mark

A law student was today beginning a minimum of 15 years behind bars for the cold-blooded slaughter of his brother-in-law.

Young father Mark Symonds was killed in the street by Peter Britten. He was stabbed as he walked home from The Flying Dutchman pub in Penn, Wolverhampton, in November 2005.

The 28-year-old, of nearby Pennwood Court, was knifed once in the back and nine times in the chest and bled to death. A jury at Warwick Crown Court yesterday took three hours and 15 minutes to find 30-year-old Britten guilty of murder.

As the foreman announced the result, Mr Symonds' family cheered, while Britten's

**Report by Mike Woods**

sister Peggy Britten-Jeavons stood up and shouted at the jury "you are all liars".

Police raced to the public gallery to ensure the crowd of 20 relatives and supporters stayed apart. With the tension at breaking point, Britten collapsed in the dock.

Justice Raymond Jack, handing down a life sentence, told Britten he would not be eligible for parole until 2022 at the earliest.

Speaking after the verdict, Peter Scorey, a close friend of Mr Symonds, said: "Justice has been done."

It was a killing that shocked a tight-knit community. When Mark Symonds was knifed to death on his way home from his favourite pub, people in Warstones demanded to know who had so violently taken one of their own. Months of investigations by the police drew a blank. The former Smestow School pupil was said in court to have not had any enemies, and was a popular figure at The Flying Dutchman in Penn. He had not been robbed and so police struggled to find a motive.

It was only when they decided to widen their search to his family that the killer was unmasked. Britten had known Mark since the age of 14, they were childhood friends.

**Friends**

"We would hang around in the same group of friends up until we were 17-year-olds," Britten told police.

"That was when Mark started to mix with another group and go another direction in his life." But the bond did not end there.

Britten began to see Mark's sister Clare when he was 21 and she was 15. Mark was said to have become protective over Clare and tension between the former friends grew. The court was told Britten became "fed-up" with Mark's behaviour.

On the afternoon of the killing, Britten made a search of the internet using words including 'how to kill a man', 'assassins' and 'strangulation'. Police who seized his PC found Britten had researched DNA techniques and the attack on Abigail Witchalls, who was stabbed in front of her young son.

But Britten, a former pupil at Penn's Highfields School, kept his deadly secret to himself. He was arrested after he and other members of Mark's family were DNA tested.

A detective who carried out the procedure said Britten appeared hesitant and raised concerns over whether his genetic makeup would be kept on a national database.

When police confronted him with pictures of Mark's body, he said simply: "Poor sod didn't deserve that."

**Figure 21.** *Newspaper reports from the Express and Star*

- Authentication of the fragments from 'Unallocated space'
- Verification of the system clock on the 2nd November

Having done all this 'ground work' I could <u>finally</u> present my 'Findings'

## FINDINGS

These artefacts (*cookies and emails from previous court slide*), coupled with the evidence within the fragments of index.dat files indicate and are consistent with, exhibit SJS4 and the logon/account 'Administrator', being used to access the Web between 15:40 and 16:00hrs on the afternoon of 2nd November 2005, using Internet Explorer as the 'browser', and entering the following 'search terms' into web pages/search engines:

"How to kill a man"
"Assassins"
"Murder"
"Strangulation"
"Guns for sale UK"

My final few slides demonstrated:

- That there was no record of these 'search terms' being used before or since the 2nd November 2005.
- Recovered 'Internet activity' consistent with researching DNA and the attack on Abigail Witchall

The evidence was such that not only was it accepted but shortly before the trial a family member of the accused announced that they had actually conducted the searches. Whilst not able to prove or disprove this late revelation it seems likely, from the outcome of the trial, that this account was not accepted by the Jury.

## CONCLUSION

This 'Digital Journey' ended with Britten being convicted at Warwick Crown Court and sentenced to a minimum of 15 years.

I am writing this article with some 7 years more digital forensic experience under my belt and on reflection Operation 'Mintell' was probably one of the most interesting and challenging of cases I have ever had to work on especially when you take into account the dynamics of the family involved, the significance of the evidence found and the fact that I was relatively new to computer forensics at the time. Thanks to plenty of self-evaluation and verification work, I was able to approach each potential challenge in turn. In addition I learnt that with regards to proportionality and the legal system, to prevent a counterproductive outcome of more questions than answers (extra work/cost/confusion) it is also important to invest the right amount of time at the most appropriate stage of the judicial process. I am convinced that had I not done or been allowed the time to cover the various eventualities, the experience would have been quite different; As this 'Digital Journey' demonstrates, finding an evidential 'golden nugget' is the easy part, making it withstand expert scrutiny is the real challenge.

**About the Author**

*I joined the Metropolitan Police in 1984 at the tender age of 18, before transferring to the West Midlands in 1990. Prior to joining the Hi-Tech Crime Unit in 2004, I built on my CID and intelligence background by studying various forms of digital technologies and applications. In 2000 I gained a distinction in advanced systems/database design, and in 2003 passed the Cisco Certified Network Academy Program (CCNA). Over the past few years I have been focusing my digital forensic skills on investigating cases of fraud. Recently I have acquired Certification as a Certified Fraud Examiner (CFE) and am looking forward to new challenges in the private sector. LinkedIn profile: http://www.linkedin.com/pub/paul-gwinnett-cfe/20/b35/b02*

# TWELVE OPEN-SOURCE LINUX FORENSIC TOOLS

by Priscilla Lopez

There are several open-source Linux forensic tool suites and tools such as Kali Linux, DEFT, HELIX, Backtrack, CAINE, Knoppix STD, FCCU, The Penguin Sleuth Kit, ADIA, DFF, SMART, and SIFT. This article will give you a brief overview of the available tool suites. Afterwards, I will show you step-by-step how to install one of the tool suites and run a practice case sample.

**What you will learn:**

- about several Linux open-source tools,
- how to install and use one of the suites

**What you should know:**

- basic Linux commands

There are many open-source tools for Linux that are available for forensic use. There is no specific preference or sort order of the tools listed. The goal of this article is for you to familiarize yourself with them, pick a few, download, install and try them out with sample case evidence. It will be up to you to find the one you like the best. Some tools listed are deprecated. I included them only because they are still easily available. Sleuthkit and Autopsy are included in almost every tool suite so they are not listed. I included DFF as a standalone program because it doesn't seem as common and it was a bit of a challenge to install. Towards the end of this article there is a step-by-step on how to download, install and run a practice case sample. Many of the tools suites can be burned or mounted to CD/DVD, then installed or ran live. There are only a few that can be downloaded as a virtual machine file. Most tool suites include an installation and/or tool manual either in the ISO file, virtual machine file or website itself. Some of the tools require a username and/or password. Please refer to the manual to find out what it is. This list is not an all-inclusive comprehensive list. Enjoy!

## KALI LINUX

**Version:** N/A
**Developer(s):** Offensive Security
**Release Date:** April 26, 2013
**Website:** *http://www.kali.org/downloads/*

Kali Linux is pretty new and created by the same guys as Backtrack as its successor. Figure 1 shows the forensic tool menu and desktop. It looks and feel like Backtrack but there are more devices Kali Linux is available on. Samsung Note, Samsung Chromebook and Raspberry Pi just to mention a few. It was simple to install and simple to use. There are some good resources available from their website too.

## DEFT

**Version:** 7.2, 8 Beta
**Developer(s):** Stefano Fratepietro
**Release Date:** Jul 1, 2013
**Website:** *http://www.deftlinux.net/*

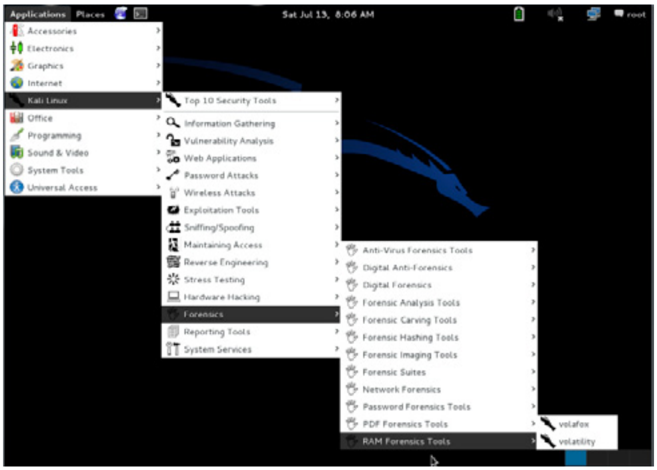


**Figure 1.** *The Kali Linux desktop and menu tool list*

**Figure 2.** *The Deft desktop*

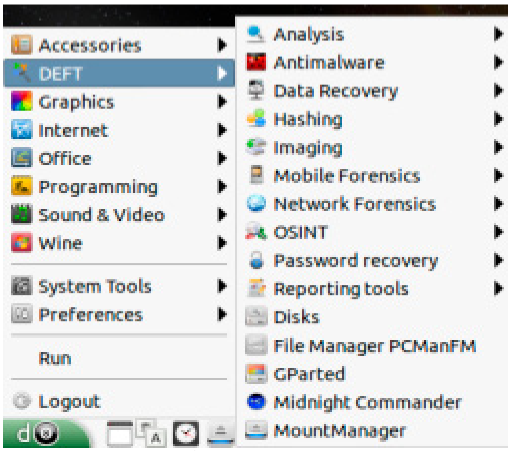


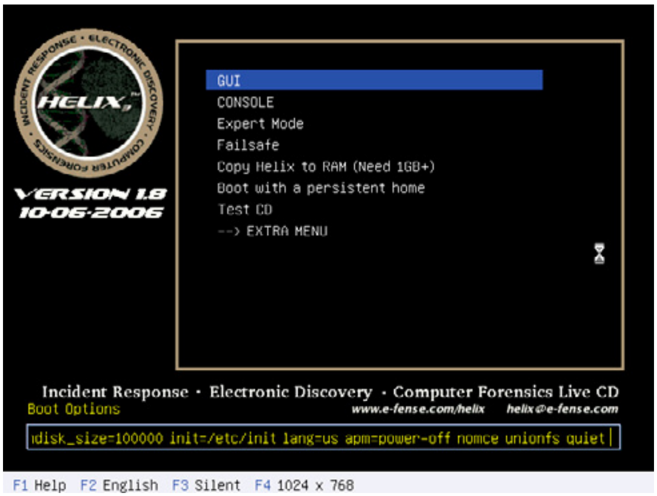
**Figure 3.** *The Deft tool list menu*

The new Deft 8 beta version includes Digital Forensic Framework which is listed below. I wouldn't recommend using the beta version for real-world due to all the bugs. According to their site, they will be releasing a virtual machine version soon. They do not have a beta manual yet but the 7.2 stable version is available on their site. The 7.2 manual is a must for the installation which is a little tricky. It can be ran as a live or as a virtual appliance. Figures 2 and 3 are screenshots of the desktop and menu. They also have listed on their website Dart 2, which is for Windows.

## HELIX3

**Version:** 2009R1
**Developer(s):** e-fense Inc
**Release Date:** June 23, 2009
**Website:** *https://www.e-fense.com/store/index.php?_a=viewProd&productId=11*

The newer versions of Helix are not free but the unsupported older version is still available for free. The manual is only available to forum members and there are no updates. There is only an ISO version available and it runs on Ubuntu very eas-


INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
HELIX
VERSION 1.8
10-06-2006
GUI
CONSOLE
Expert Mode
Failsafe
Copy Helix to RAM (Need 1GB+)
Boot with a persistent home
Test CD
--> EXTRA MENU
Incident Response • Electronic Discovery • Computer Forensics Live CD
www.e-fense.com/helix
helix@e-fense.com
Boot Options
F1 Help F2 English F3 Silent F4 1024 x 768

```
idisk_size=100000 init=/etc/init lang=us apm=power-off nomce unionfs quiet
```

**Figure 4.** *The HELIX3 version 1.8 boot menu*

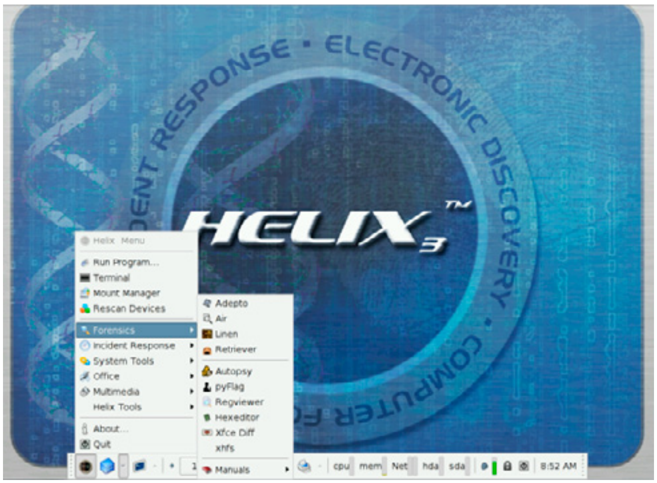


**Figure 5.** *The HELIX3 version 1.8 tool menu*

ily. The boot menu seen in Figure 4 give you many options and Figure 5 gives you a screenshot of the tool list menu. There is a good installation demo here: *http://computersecuritystudent.com/FORENSICS/HELIX/lesson2/.*

## BACKTRACK

**Version:** 5 R3
**Developer(s):** Offensive Security
**Release Date:** August 13, 2012
**Website:** *http://www.backtrack-linux.org/downloads/*

Backtrack is a very simple to use precursor of Kali Linux previously listed. It is just as easy to use and run. Just like Kali Linux the suite includes penetration testing tools. The menu is very simple to navigate and flows methodically from section to section. It is can be downloaded as an ISO that can be ran as a live CD/USB. The website also includes great tutorials (Figure 6).

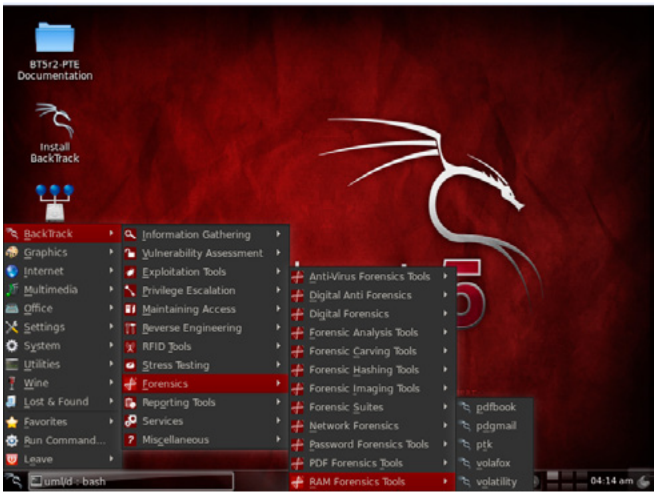


**Figure 6.** Backtrack 5r2 tool list menu

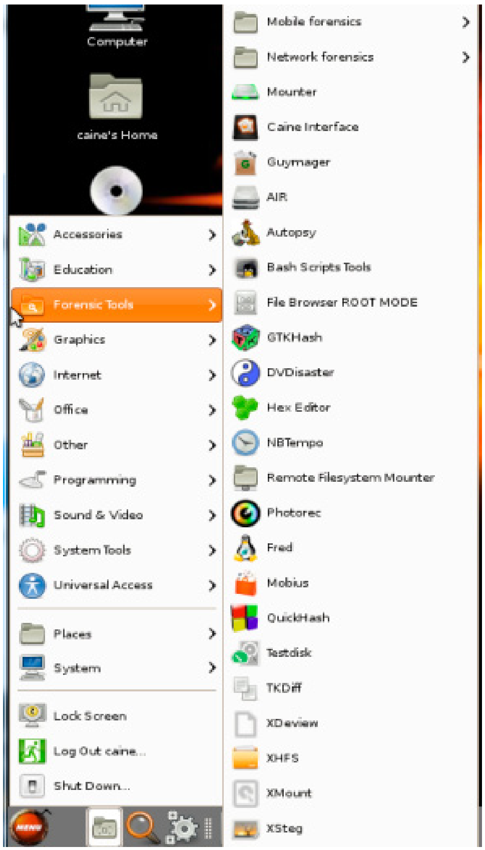


**Figure 7.** *The CAINE tool list menu*

## COMPUTER AIDED INVESTIGATIVE ENVIRONMENT (CAINE)

**Version:** 4.0
**Developer(s):** Nanni Bassetti
**Release Date:** March 18, 2013
**Website:** *http://www.caine-live.net/page5/page5.html*

CAINE is an Italian made forensic tools suite that can only be installed. NBCAINE is used for running a live CD/USB and both are available in ISO format. The website includes really good manuals and mounting policies. As you can see in Figure 7 it installs in English and there are a moderate amount of tools to work with. In Figure 8 you can see the pre-setup desktop and manual.

## KNOPPIX STD (SECURITY TOOLS DISTRIBUTION)

**Version:** 0.1
**Project Owner:** Mark Cumming
**Release Date:** January 24, 2004
**Website:** *http://s-t-d.org/download.html*

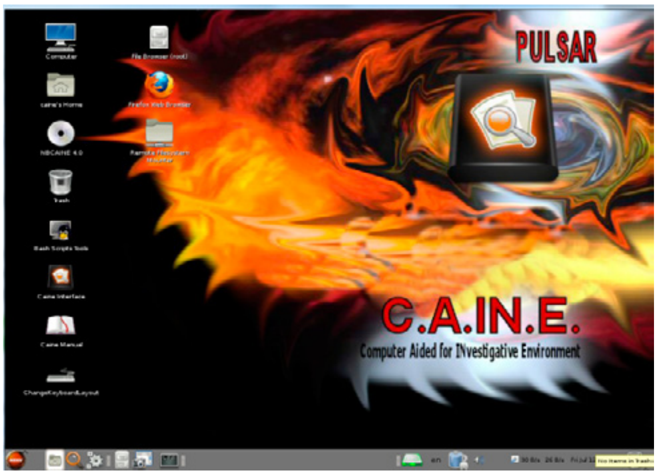


**Figure 8.** *The CAINE desktop*

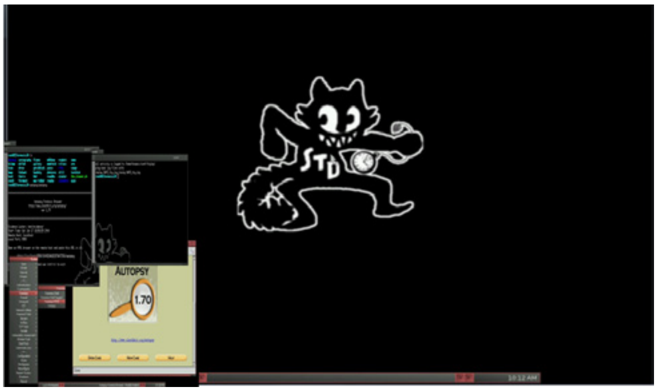


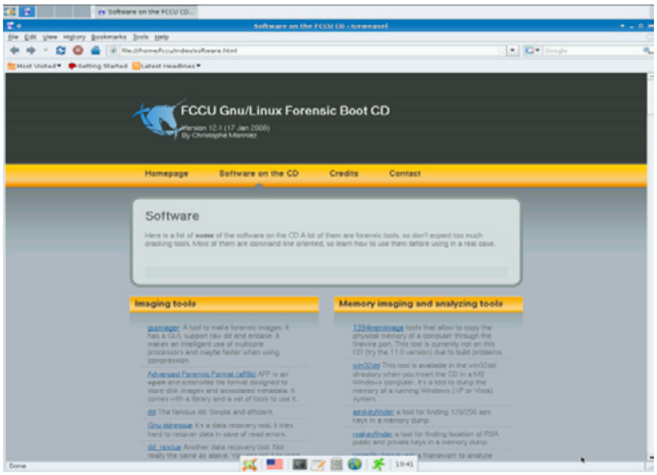
**Figure 9.** *The Knoppix STD desktop and tool list menu*

Knoppix STD is a deprecated tool suite that can be used for forensic practicing purposes. This tool is available as an ISO file. The website has a really great forum that is still gets posts! This tool is mostly based off a Linux distro called Knoppix. The website states that this tool is only available for live purposes. In Figure 9 you can also see that the suite includes honeypot and IDS tools.

## FEDERAL COMPUTER CRIME UNITE (FCCU)

**Version:** 12.1
**Developer(s):** Christophe Monniez, Geert Van Acker
**Release Date:** October 7, 2008
**Website:** *http://www.lnx4n6.be/index.php?sec=Downloads&page=bootCD*

FCCU is a Belgian forensic tools suite. The presentation pdf file found on their website has much has useful information. In Figure 10 you see a list of tools available in FCCU. They are almost all command line based. Figure 11 lets you know you have successfully arrived at the FCCU desktop.


Software on the FCCU CD...
Software on the FCCU CD - Iceweasel
File Edit View History Bookmarks Tools Help
file:///home/fccu/index/software.html
Google
Most Visited Getting Started Latest Headlines
FCCU Gnu/Linux Forensic Boot CD
Version 12.1 (17 Jan 2008)
By Christophe Monniez
Homepage
Software on the CD
Credits
Contact
Done
10:41

Software

Here is a list of **some** of the software on the CD A lot of them are forensic tools, so don't expect too much cracking tools. Most of them are command line oriented, so learn how to use them before using in a real case.

Imaging tools

- guymager A tool to make forensic images. It has a GUI, support raw dd and endase. It makes an intelligent use of multicore processors and maybe faster when using compression.
- Advanced Forensic Format (afflib) AFF is an **open** and extensible file format designed to store disk images and associated metadata. It comes with a library and a set of tools to use it.
- dd The famous dd. Simple and efficient.
- Gnu ddrescue It's a data recovery tool. It tries hard to recover data in case of read errors.
- dd_rescue Another data recovery tool. Not really the same as above. Yo

Memory imaging and analyzing tools

- 1394memimage tools that allow to copy the physical memory of a computer through the firewire port. This tool is currently not on this CD (try the 11.0 version) due to build problems.
- win32dd This tool is available in the win32dd directory when you insert the CD in a MS Windows computer. It's a tool to dump the memory of a running Windows (XP or Vista) system.
- aeskeyfinder a tool for finding 128/256 aes keys in a memory dump.
- rsakeyfinder a tool for finding location of RSA public and private keys in a memory dump.
- a framework to analyze

**Figure 10.** *The FCCU list of tools that pops up in the internet browser upon boot*

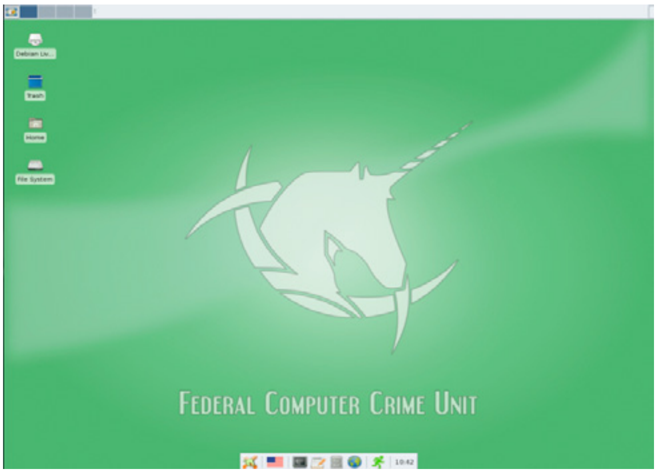
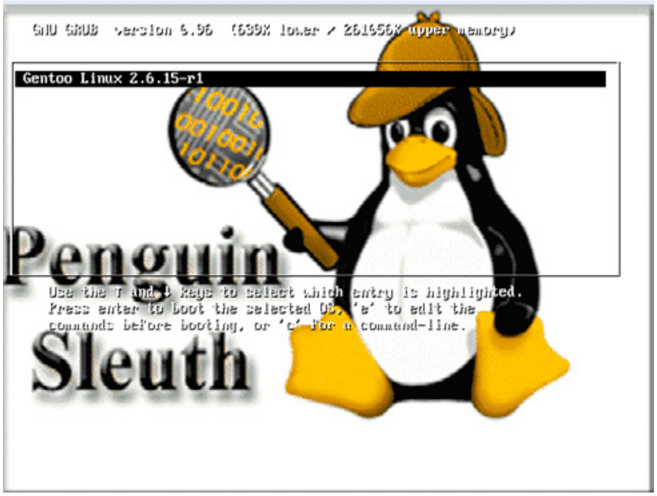


**Figure 11.** *The FCCU desktop*

## THE PENGUIN SLEUTH KIT

***Version:*** 0.96
***Creator:*** Ernest Baca
***Release Date:*** July 5, 2003, June 2006
***Website:*** *http://sourceforge.net/projects/psk/files/Penguin%20Sleuth/*, *http://www.linux-forensics.com*, *http://penguinsleuth.org*

The Penguin Sleuth Kit is another deprecated tool suite that can still be used for practice. It is also based off of the Linux distro. There are also a few network security tools included in the suite. The files is live USB/ISO and virtual appliance only. There is a manual available and the tool is also based off Knoppix (Figure 12).



```
GNU GRUB  version 0.96  (639K lower / 261656K upper memory)

 Gentoo Linux 2.6.15-r1

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, or 'c' for a command-line.
```

**Figure 12.** *Penguin Sleuth boot menu*

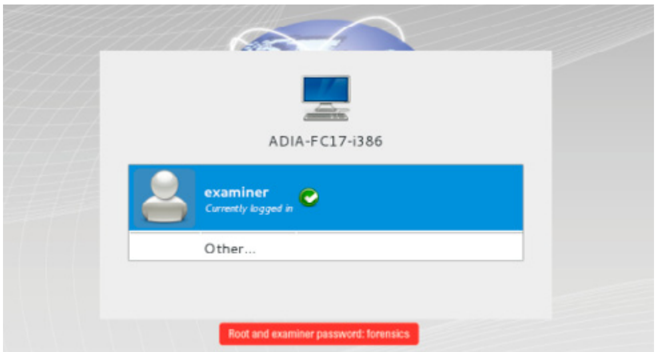


**Figure 13.** *The AIDA login screen*

ADIA
APPLIANCE FOR DIGITAL INVESTIGATION & ANALYSIS
Software Engineering Institute
Carnegie Mellon

**Figure 14.** *The AIDA desktop*

## APPLIANCE FOR DIGITAL INVESTIGATION AND ANALYSIS (ADIA)

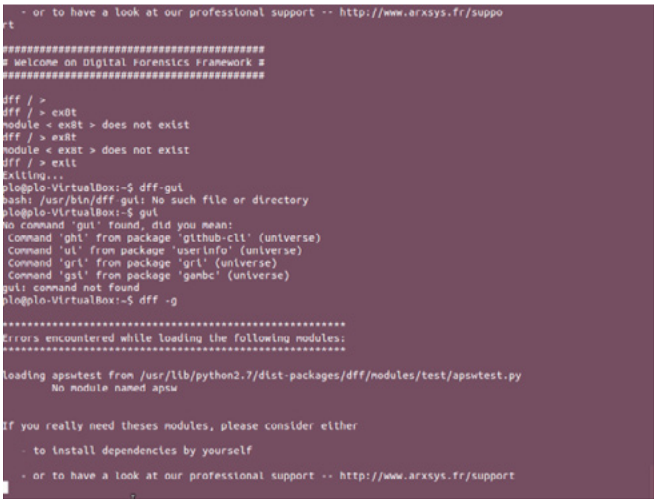
**Version:** Unknown
**Developer(s):** CERT
**Release Date:** March 2012
**Website:** *http://www.cert.org/forensics/tools.htm*

ADIA is only available as a virtual appliance. It was very easy to install. Figure 13 is a screenshot of the login. Figure 14 you can see that there are many pre-installed shortcuts and a manual on the desktop. The website has many other free forensic tools and resources.

## DIGITAL FORENSICS FRAMEWORK (DFF)

**Version:** 1.3.0
**Developer(s):** ArxSys
**Release Date:** February 12, 2013
**Website:** *http://www.digital-forensic.org/download/*

DFF is downloadable as a .deb file. It is only a program tool and not a suite of tools. When I installed the tool on my Ubuntu 13.04, I used `sudo apt -get -f install` to install the dependencies need to run the program. Afterwards I used `sudo apt-get install dff` to install the package. I attempted the instructions on the site but soon realized the code above worked best for me. To start the program use `dff -g`. This application was a bit of a challenge to install. This package can also be found on some other suites but not as much as Autopsy and The Sleuth Kit. The website states that there are different modules that can be added to the program to increase productivity. See Figure 15 for a command line screen shot and Figure 16 for a GUI screenshot.



```
   - or to have a look at our professional support -- http://www.arxsys.fr/suppo
rt

##########################################
# Welcome on Digital Forensics Framework #
##########################################

dff / >
dff / > ex8t
module < ex8t > does not exist
dff / > exRt
module < ex8t > does not exist
dff / > exit
Exiting...
plo@plo-VirtualBox:~$ dff-gui
bash: /usr/bin/dff-gui: No such file or directory
plo@plo-VirtualBox:~$ gui
No command 'gui' found, did you mean:
 Command 'ghi' from package 'github-cli' (universe)
 Command 'ui' from package 'userinfo' (universe)
 Command 'gri' from package 'gri' (universe)
 Command 'gsi' from package 'gambc' (universe)
gui: command not found
plo@plo-VirtualBox:~$ dff -g

*******************************************************
Errors encountered while loading the following modules:
*******************************************************

loading apswtest from /usr/lib/python2.7/dist-packages/dff/modules/test/apswtest.py
        No module named apsw


If you really need theses modules, please consider either

   - to install dependencies by yourself

   - or to have a look at our professional support -- http://www.arxsys.fr/support
```

**Figure 15.** *The DFF command line tool*

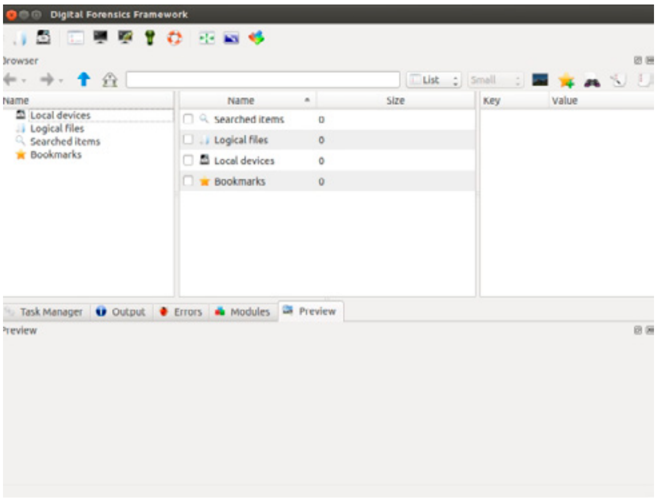


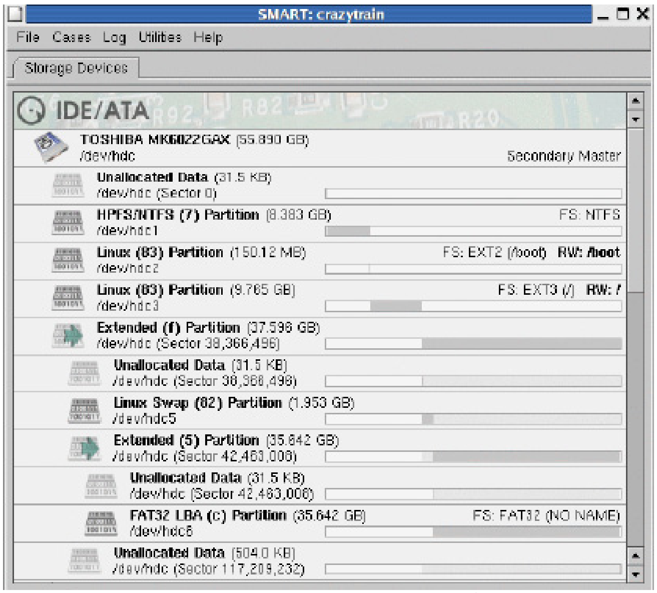
**Figure 16.** *The DFF GUI interface*

## STORAGE MEDIA ANALYSIS RECOVERY TOOLKIT (SMART)

**Version:** Unknown
**Developer(s):** ASR Data
**Release Date:** May 3, 2013
**Website:** *http://www.asrdata.com/forensic-software/smart-for-linux/*, *http://www.asrdata.com/forensic-software/smart-linux/*, *http://smartlinux.sourceforge.net/*

*Smart Linux* is the live CD/USB and *Smart for Linux* is for installation on Linux. The website says that in can be used for:

**Figure 17.** *The SMART Linux login screen (from the manual)*



TOSHIBA MK6022GAX (55.890 GB)
/dev/hdc — Secondary Master

Unallocated Data (31.5 KB)
/dev/hdc (Sector 0)

HPFS/NTFS (7) Partition (8.383 GB) — FS: NTFS
/dev/hdc1

Linux (83) Partition (150.12 MB) — FS: EXT2 (/boot) RW: /boot
/dev/hdc2

Linux (83) Partition (9.765 GB) — FS: EXT3 (/) RW: /
/dev/hdc3

Extended (f) Partition (37.596 GB)
/dev/hdc (Sector 38,366,496)

Unallocated Data (31.5 KB)
/dev/hdc (Sector 38,366,496)

Linux Swap (82) Partition (1.953 GB)
/dev/hdc5

Extended (5) Partition (35.642 GB)
/dev/hdc (Sector 42,463,006)

Unallocated Data (31.5 KB)
/dev/hdc (Sector 42,463,006)

FAT32 LBA (c) Partition (35.642 GB) — FS: FAT32 (NO NAME)
/dev/hdc6

Unallocated Data (504.0 KB)
/dev/hdc (Sector 117,209,232)

**Figure 18.** *The SMART Linux tool list menu (from the manual)*

- Knock-and-talk inquiries and investigations
- on-site or remote preview of a target system
- post mortem analysis of a dead system
- testing and verification of other forensic programs
- conversion of proprietary evidence file formats
- baselining of a system

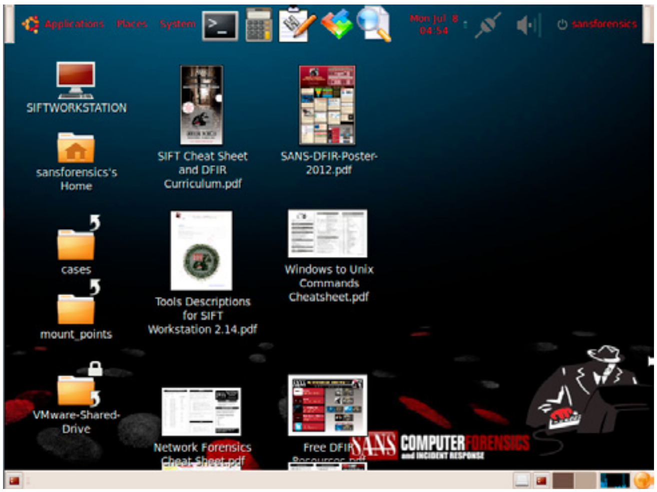

Applications
Places
System
Mon Jul 8 04:54
sansforensics
SIFTWORKSTATION
sansforensics's Home
cases
mount_points
VMware-Shared-Drive
SIFT Cheat Sheet and DFIR Curriculum.pdf
Tools Descriptions for SIFT Workstation 2.14.pdf
Network Forensics Cheat Sheet.pdf
SANS-DFIR-Poster-2012.pdf
Windows to Unix Commands Cheatsheet.pdf
Free DFIR Resources.pdf
SANS COMPUTER FORENSICS and INCIDENT RESPONSE

**Figure 19.** *The SANS Sift desktop*

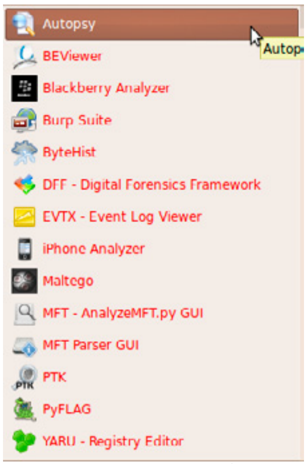
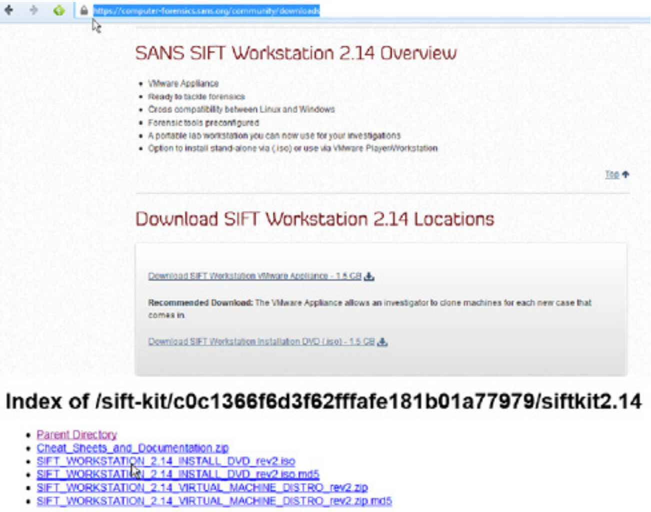


**Figure 20.** *The SANS Sift tool list menu*



https://computer-forensics.sans.org/community/downloads

SANS SIFT Workstation 2.14 Overview

- VMware Appliance
- Ready to tackle forensics
- Cross compatibility between Linux and Windows
- Forensic tools preconfigured
- A portable lab workstation you can now use for your investigations
- Option to install stand-alone via (.iso) or use via VMware Player/Workstation

Top

Download SIFT Workstation 2.14 Locations

Download SIFT Workstation VMware Appliance - 1.5 GB

**Recommended Download:** The VMware Appliance allows an investigator to clone machines for each new case that comes in.

Download SIFT Workstation Installation DVD (.iso) - 1.5 GB

Index of /sift-kit/c0c1366f6d3f62fffafe181b01a77979/siftkit2.14

- Parent Directory
- Cheat_Sheets_and_Documentation.zip
- SIFT_WORKSTATION_2.14_INSTALL_DVD_rev2.iso
- SIFT_WORKSTATION_2.14_INSTALL_DVD_rev2.iso.md5
- SIFT_WORKSTATION_2.14_VIRTUAL_MACHINE_DISTRO_rev2.zip
- SIFT_WORKSTATION_2.14_VIRTUAL_MACHINE_DISTRO_rev2.zip.md5

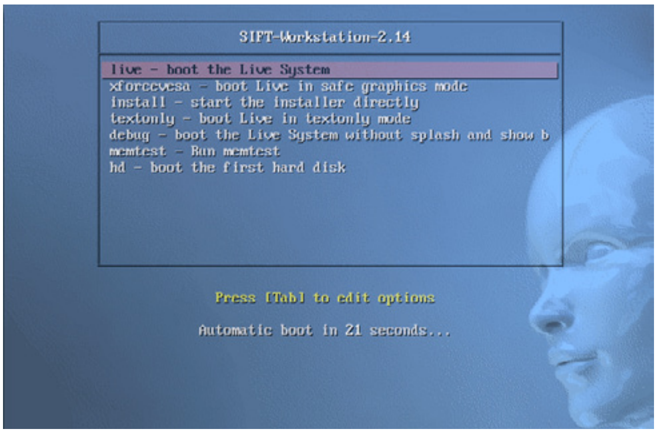
**Figure 21.** *The website for tool suite download*

The manual for installation is included in the download. The website also has other tools available for download. See Figure 17 and 18 for screenshots.

## SANS INVESTIGATIVE FORENSIC TOOLKIT (SIFT)

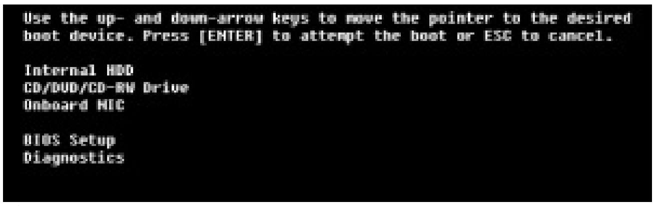
**Version:** 2.14
**Company/Creator:** SANS, Rob Lee
**Release Date:** December 2011
**Website:** *http://computer-forensics.sans.org/community/downloads*

SIFT is a virtual machine created by SANS for training purposes. It includes many resources and tools for forensic investigations. The website is loaded with resources. The desktop is loaded with resources and the menu tool list is easy to navigate as seen in Figure 19 and 20.



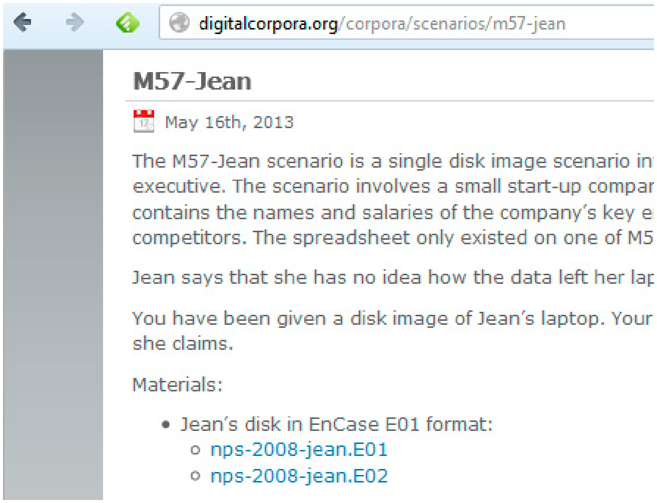
```
SIFT-Workstation-2.14

live - boot the Live System
xforcevesa - boot Live in safe graphics mode
install - start the installer directly
textonly - boot Live in textonly mode
debug - boot the Live System without splash and show b
memtest - Run memtest
hd - boot the first hard disk

Press [Tab] to edit options

Automatic boot in 21 seconds...
```

**Figure 22.** *The two .E01 files from http://digitalcorpora.org/corpora/scenarios/m57-jean*



```
Use the up- and down-arrow keys to move the pointer to the desired
boot device. Press [ENTER] to attempt the boot or ESC to cancel.

Internal HDD
CD/DVD/CD-RW Drive
Onboard NIC

BIOS Setup
Diagnostics
```

**Figure 23.** *Boot Menu*



digitalcorpora.org/corpora/scenarios/m57-jean

M57-Jean

May 16th, 2013

The M57-Jean scenario is a single disk image scenario in
executive. The scenario involves a small start-up compar
contains the names and salaries of the company's key e
competitors. The spreadsheet only existed on one of M5

Jean says that she has no idea how the data left her lap

You have been given a disk image of Jean's laptop. Your
she claims.

Materials:

- Jean's disk in EnCase E01 format:
  - nps-2008-jean.E01
  - nps-2008-jean.E02

**Figure 24.** *Sift CD boot menu*

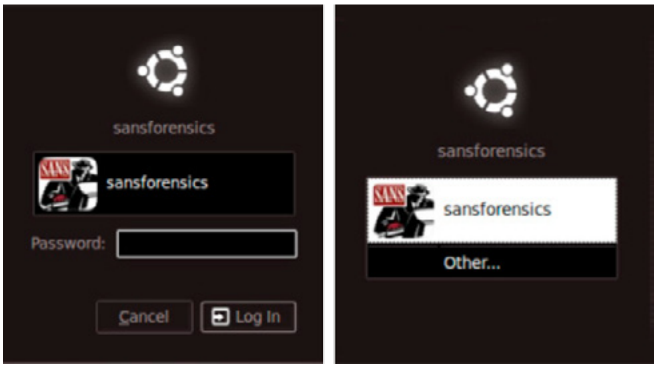


**Figure 25.** *Sift CD login screen*

## HOW TO INSTALL AND USE AN OPEN-SOURCE FORENSIC TOOL SUITE

This how-to guide does not follow the proper methodology for a real-case scenario. This is simply a guide for you to practice using one of the open-source tools provided in this article. Before trying beginning please go to from *https://computer-forensics.sans.org/community/downloads* and register for a SANS account.

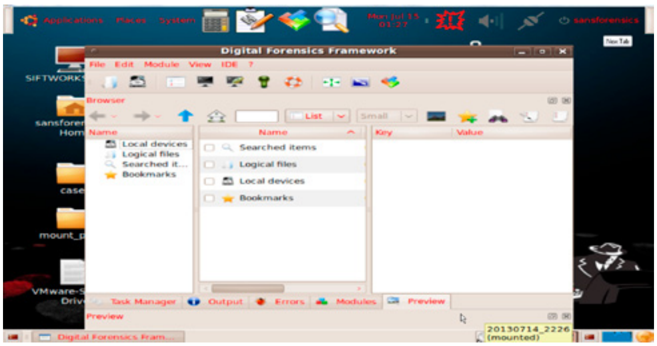
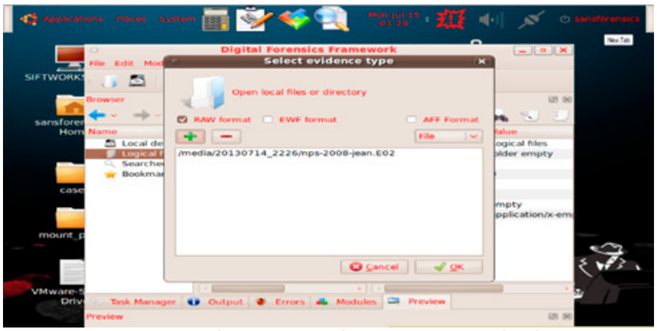
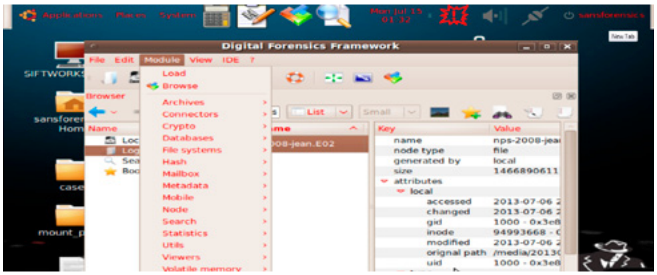


**Figure 26.** *SIFT workstation with DFF open*



/media/20130714_2226/nps-2008-jean.E02

**Figure 27.** *SIFT workstation with DFF open and selecting practice image*



| Key | Value |
|---|---|
| name | nps-2008-jea |
| node type | file |
| generated by | local |
| size | 1466890611 |
| attributes | |
| local | |
| accessed | 2013-07-06 |
| changed | 2013-07-06 |
| gid | 1000 - 0x3e8 |
| inode | 94993668 |
| modified | 2013-07-06 |
| orignal path | /media/2013 |
| uid | 1000 - 0x3e8 |

**Figure 28.** *SIFT workstation Module menu*

### ON THE WEB

List of Sites for practice evidence and challenges: http://www.forensicfocus.com/images-and-challenges

### STEP 1

Download *SANS SIFT Workstation 2.14 ISO from https://computer-forensics.sans.org/community/downloads* as seen in Figure 21. NOTE: You need registered to download this file.

### STEP 2

Download and save the two .E01 files, `nps-2008-jean.e01` and `nps-2008-jean-e01`, from *http://digitalcorpora.org/corpora/scenarios/m57-jean*. Figure 22.

### STEP 3

After downloading burn to DVD. Insert DVD into computer.

### STEP 4

Reboot your computer. During startup hit F12 or F10 (depends on your manufacturer) for you boot selection menu. Boot from DVD. Figure 23.

### STEP 5

Highlight and select the "live –boot the Live System". Figure 24.

### STEP 6

Click on sanforensics and type the password: forensics. Figure 25.

### STEP 7

Pick a tool of choice, add your files `nps-2008-jean.e01` and `nps-2008-jean-e01` and begin looking for data for the case. Figure 26-28

## SUMMARY

I hope that by glancing over these tools and the brief overview of them you can pick a few you would like to download, install and practice with the more sample case evidence. Many of the tools may be old but some of the tools included in the suites are still in use. These tools may not be as simple and souped up as the paid programs but it's a great place to start.

### About the Author

*Priscilla Lopez has earned M.S. in Information Security Assurance from WGU and B.S. in Computer Information and Technology with Minor in Business from UMUC. She holds five active computer certifications: CCNA, GIAC ISO Specialist, CEH, CHFI and CompTIA Network +. For over ten years she has been working with technology in her community, workplace, family and church. She is continuously expanding her knowledge and experience in the computer industry and enjoys sharing with students and those around her.*

# FOUR WINDOWS XP FORENSIC ANALYSIS TIPS & TRICKS

by Davide Barbato

When conducting forensics analysis of a Windows XP system, it must be taken into account some particular behaviors that can lead to misleading conclusions if not properly handled.

**What you will learn:**

- Specific Windows XP behaviors
- A basic knowledge of Windows LNK file structure

**What you should know:**

- A basic understanding of NTFS structure
- A basic understanding of Windows XP registry
- How to create and read timeline

Even if most of Windows based PCs and notebooks are shipped with Windows 7 or Windows 8, you could happen to deal with an old Windows XP operating system.

To an untrained eye, it could appear that Windows XP is just another Windows operating system family: It behaves completely different, and could lead to misleading conclusions if you are not familiar with XP. Think about a case in which you need to know if a user views a document or a folder, or opened a document and trashed them: Windows XP has different behavior in respect to Windows 7 and this need to be addressed.

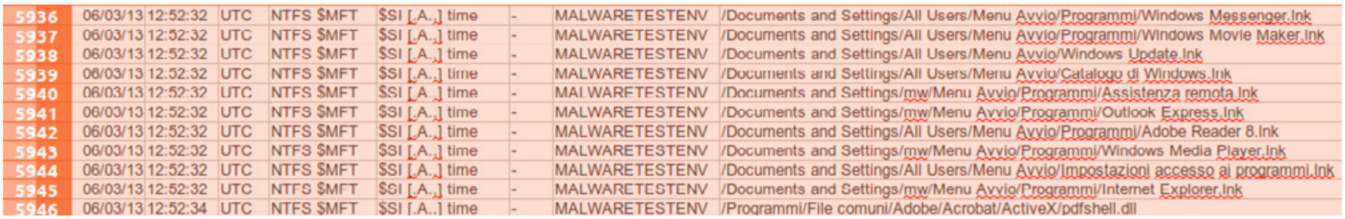
## NTFS DISABLE LAST ACCESS UPDATE

First of all, let's talk about the file system: even if Windows XP is really old, it's not so old to be shipped with FAT32 file system, so in this article we can assume that we are dealing with NTFS file system.

Based on that assumption, it is important and critical to remember that Windows XP, every time it reads a file or a directory, it changes the access time of `$SI` object, updating on the time the system is accessing the object. This means that even listing the content of a directory will update the *$SI* access time, losing the previous last access time.

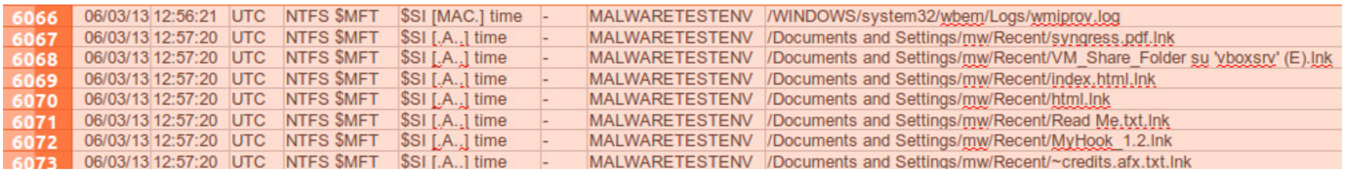
This behavior can be avoided adding a Registry key, under *HKLM\SYSTEM\CurrentControlSet\Control\FileSystem*, named *NtfsDisableLastAccessUpdate* and setting its value to 1.

Some scenarios presented in this article will deal with that behavior, trying to show how and when the access timestamp is updated.



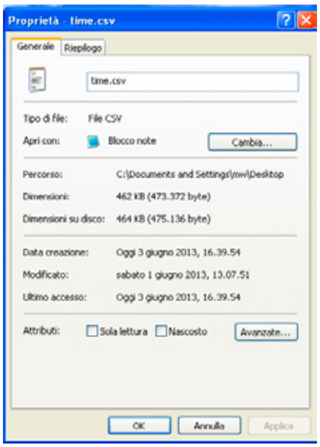
```
5936  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Programmi/Windows Messenger.lnk
5937  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Programmi/Windows Movie Maker.lnk
5938  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Windows Update.lnk
5939  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Catalogo di Windows.lnk
5940  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Menu Avvio/Programmi/Assistenza remota.lnk
5941  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Menu Avvio/Programmi/Outlook Express.lnk
5942  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Programmi/Adobe Reader 8.lnk
5943  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Menu Avvio/Programmi/Windows Media Player.lnk
5944  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/All Users/Menu Avvio/Impostazioni accesso ai programmi.lnk
5945  06/03/13 12:52:32  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Menu Avvio/Programmi/Internet Explorer.lnk
5946  06/03/13 12:52:34  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Programmi/File comuni/Adobe/Acrobat/ActiveX/pdfshell.dll
```

**Figure 1.** *User clicks the Start icon*



```
6066  06/03/13 12:56:21  UTC  NTFS $MFT  $SI [MAC.] time  -  MALWARETESTENV  /WINDOWS/system32/wbem/Logs/wmiprov.log
6067  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/syngress.pdf.lnk
6068  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/VM_Share_Folder su 'vboxsrv' (E).lnk
6069  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/index.html.lnk
6070  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/html.lnk
6071  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/Read Me.txt.lnk
6072  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/MyHook_1.2.lnk
6073  06/03/13 12:57:20  UTC  NTFS $MFT  $SI [.A..] time  -  MALWARETESTENV  /Documents and Settings/mw/Recent/~credits.afx.txt.lnk
```

**Figure 2.** *Recent menu folder*



time.csv

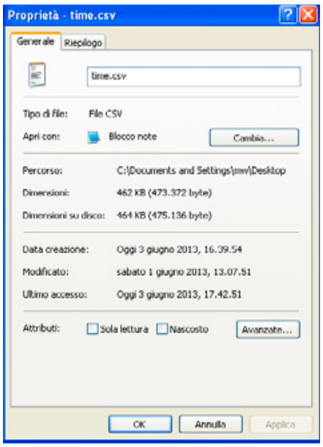
Tipo di file: File CSV
Apri con: Blocco note

Percorso: C:\Documents and Settings\mw\Desktop
Dimensioni: 462 KB (473.372 byte)
Dimensioni su disco: 464 KB (475.136 byte)

Data creazione: Oggi 3 giugno 2013, 16.39.54
Modificato: sabato 1 giugno 2013, 13.07.51
Ultimo accesso: Oggi 3 giugno 2013, 16.39.54

Attributi: □ Sola lettura □ Nascosto

**Figure 3.** *time.cvs property*



time.csv

Tipo di file: File CSV
Apri con: Blocco note

Percorso: C:\Documents and Settings\mw\Desktop
Dimensioni: 462 KB (473.372 byte)
Dimensioni su disco: 464 KB (475.136 byte)

Data creazione: Oggi 3 giugno 2013, 16.39.54
Modificato: sabato 1 giugno 2013, 13.07.51
Ultimo accesso: Oggi 3 giugno 2013, 17.42.51

Attributi: □ Sola lettura □ Nascosto

**Figure 4.** *time.csv last access updated*

## 01 OPENING WINDOWS MENU

What happen when a user clicks on the Start icon? What filesystem changes occurred? Here an excerpt of a timeline, presenting only the lines in which the user clicks the Start menu icon: Figure 1.

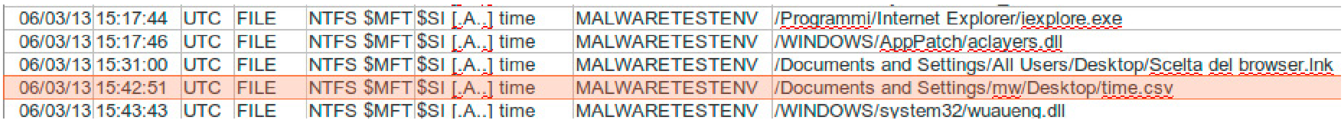
As you can see, Windows opens the menu directories (named “Menu Avvio”) and reads its content, updating the `$SI` access timestamp.

Let’s take a look at the Recent folder, under the start menu: when showing its content, Windows updates the `$SI` access timestamp, the same way as the menu items, listed above (Figure 2).

If you show the metadata information about the lnk files, you will see the access timestamp changed to 3 June 2013 at 12:57 UTC.

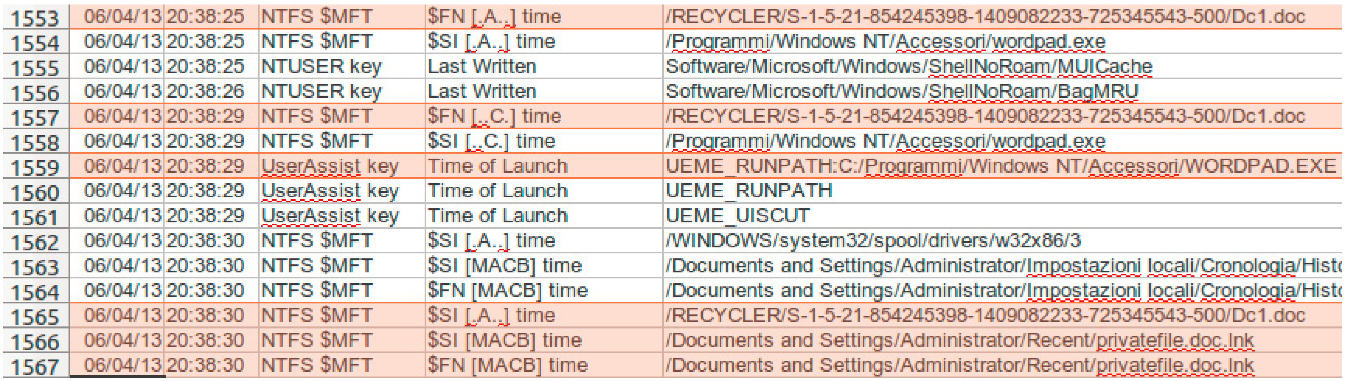
## 02 SHOWING FILE PROPERTY

Let's have a look at the file property below. The file was copied on 3 June 2013 at 16:39 CET, but cre-



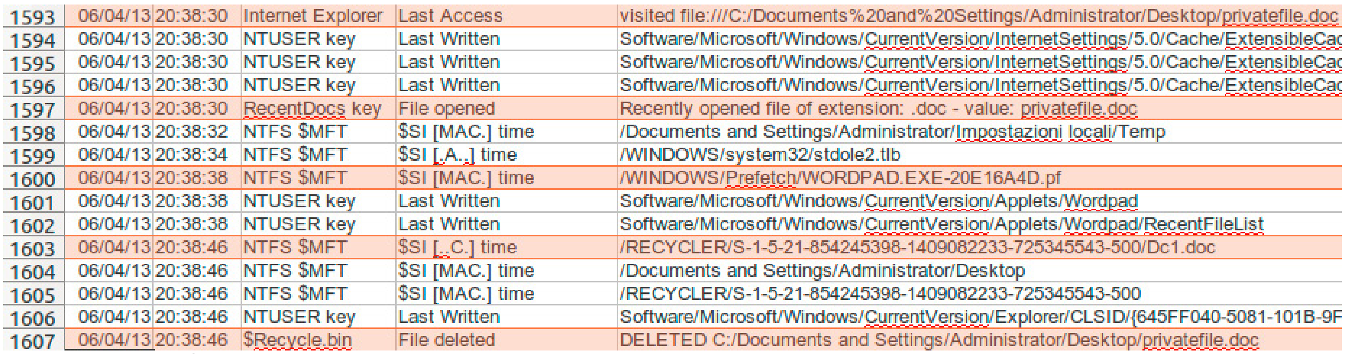
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 06/03/13 | 15:17:44 | UTC | FILE | NTFS $MFT | $SI [.A..] time | MALWARETESTENV | /Programmi/Internet Explorer/iexplore.exe |
| 06/03/13 | 15:17:46 | UTC | FILE | NTFS $MFT | $SI [.A..] time | MALWARETESTENV | /WINDOWS/AppPatch/aclayers.dll |
| 06/03/13 | 15:31:00 | UTC | FILE | NTFS $MFT | $SI [.A..] time | MALWARETESTENV | /Documents and Settings/All Users/Desktop/Scelta del browser.lnk |
| 06/03/13 | 15:42:51 | UTC | FILE | NTFS $MFT | $SI [.A..] time | MALWARETESTENV | /Documents and Settings/mw/Desktop/time.csv |
| 06/03/13 | 15:43:43 | UTC | FILE | NTFS $MFT | $SI [.A..] time | MALWARETESTENV | /WINDOWS/system32/wuaueng.dll |

**Figure 5.** *time.csv timeline*



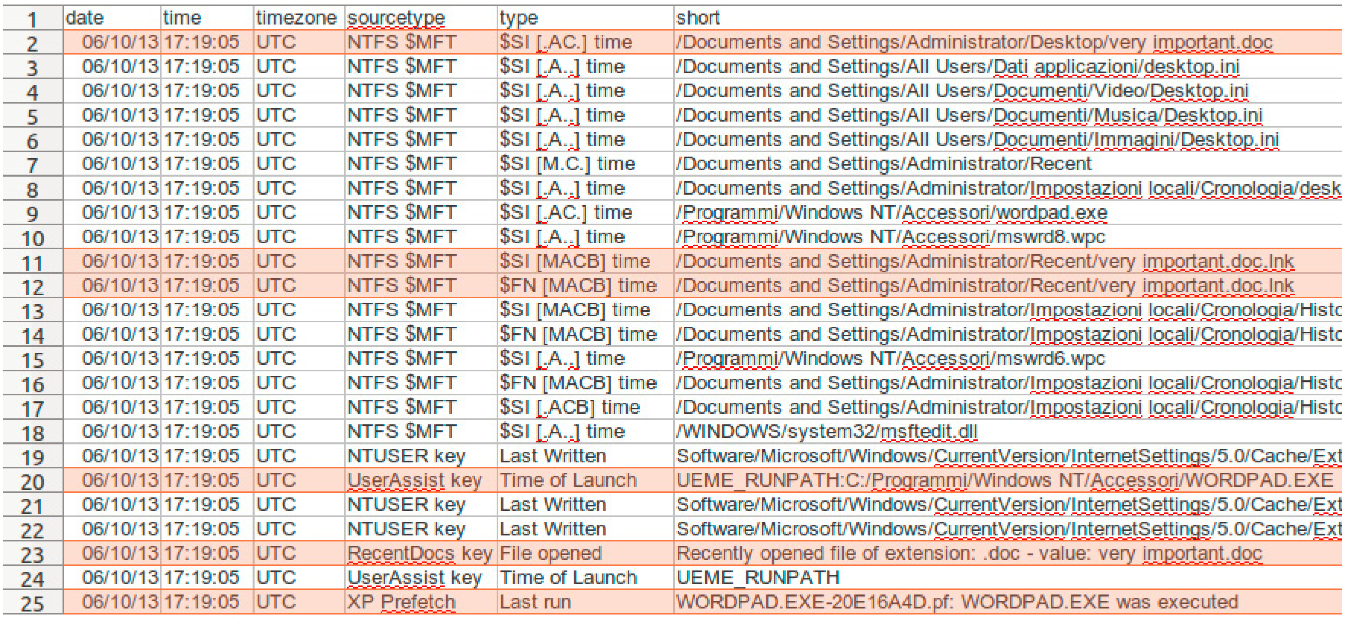
| | | | | | |
|---|---|---|---|---|---|
| 1553 | 06/04/13 | 20:38:25 | NTFS $MFT | $FN [.A..] time | /RECYCLER/S-1-5-21-854245398-1409082233-725345543-500/Dc1.doc |
| 1554 | 06/04/13 | 20:38:25 | NTFS $MFT | $SI [.A..] time | /Programmi/Windows NT/Accessori/wordpad.exe |
| 1555 | 06/04/13 | 20:38:25 | NTUSER key | Last Written | Software/Microsoft/Windows/ShellNoRoam/MUICache |
| 1556 | 06/04/13 | 20:38:26 | NTUSER key | Last Written | Software/Microsoft/Windows/ShellNoRoam/BagMRU |
| 1557 | 06/04/13 | 20:38:29 | NTFS $MFT | $FN [..C.] time | /RECYCLER/S-1-5-21-854245398-1409082233-725345543-500/Dc1.doc |
| 1558 | 06/04/13 | 20:38:29 | NTFS $MFT | $SI [..C.] time | /Programmi/Windows NT/Accessori/wordpad.exe |
| 1559 | 06/04/13 | 20:38:29 | UserAssist key | Time of Launch | UEME_RUNPATH:C:/Programmi/Windows NT/Accessori/WORDPAD.EXE |
| 1560 | 06/04/13 | 20:38:29 | UserAssist key | Time of Launch | UEME_RUNPATH |
| 1561 | 06/04/13 | 20:38:29 | UserAssist key | Time of Launch | UEME_UISCUT |
| 1562 | 06/04/13 | 20:38:30 | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/spool/drivers/w32x86/3 |
| 1563 | 06/04/13 | 20:38:30 | NTFS $MFT | $SI [MACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 1564 | 06/04/13 | 20:38:30 | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 1565 | 06/04/13 | 20:38:30 | NTFS $MFT | $SI [.A..] time | /RECYCLER/S-1-5-21-854245398-1409082233-725345543-500/Dc1.doc |
| 1566 | 06/04/13 | 20:38:30 | NTFS $MFT | $SI [MACB] time | /Documents and Settings/Administrator/Recent/privatefile.doc.lnk |
| 1567 | 06/04/13 | 20:38:30 | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Recent/privatefile.doc.lnk |

**Figure 6.** *privatefile.doc opening*



| | | | | | |
|---|---|---|---|---|---|
| 1593 | 06/04/13 | 20:38:30 | Internet Explorer | Last Access | visited file:///C:/Documents%20and%20Settings/Administrator/Desktop/privatefile.doc |
| 1594 | 06/04/13 | 20:38:30 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/ExtensibleCac |
| 1595 | 06/04/13 | 20:38:30 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/ExtensibleCac |
| 1596 | 06/04/13 | 20:38:30 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/ExtensibleCac |
| 1597 | 06/04/13 | 20:38:30 | RecentDocs key | File opened | Recently opened file of extension: .doc - value: privatefile.doc |
| 1598 | 06/04/13 | 20:38:32 | NTFS $MFT | $SI [MAC.] time | /Documents and Settings/Administrator/Impostazioni locali/Temp |
| 1599 | 06/04/13 | 20:38:34 | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/stdole2.tlb |
| 1600 | 06/04/13 | 20:38:38 | NTFS $MFT | $SI [MAC.] time | /WINDOWS/Prefetch/WORDPAD.EXE-20E16A4D.pf |
| 1601 | 06/04/13 | 20:38:38 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/Applets/Wordpad |
| 1602 | 06/04/13 | 20:38:38 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/Applets/Wordpad/RecentFileList |
| 1603 | 06/04/13 | 20:38:46 | NTFS $MFT | $SI [..C.] time | /RECYCLER/S-1-5-21-854245398-1409082233-725345543-500/Dc1.doc |
| 1604 | 06/04/13 | 20:38:46 | NTFS $MFT | $SI [MAC.] time | /Documents and Settings/Administrator/Desktop |
| 1605 | 06/04/13 | 20:38:46 | NTFS $MFT | $SI [MAC.] time | /RECYCLER/S-1-5-21-854245398-1409082233-725345543-500 |
| 1606 | 06/04/13 | 20:38:46 | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/Explorer/CLSID/{645FF040-5081-101B-9F |
| 1607 | 06/04/13 | 20:38:46 | $Recycle.bin | File deleted | DELETED C:/Documents and Settings/Administrator/Desktop/privatefile.doc |

**Figure 7.** *privatefile.doc opened and deleted*



| 1 | date | time | timezone | sourcetype | type | short |
|---|---|---|---|---|---|---|
| 2 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.AC.] time | /Documents and Settings/Administrator/Desktop/very important.doc |
| 3 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Documents and Settings/All Users/Dati applicazioni/desktop.ini |
| 4 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Documents and Settings/All Users/Documenti/Video/Desktop.ini |
| 5 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Documents and Settings/All Users/Documenti/Musica/Desktop.ini |
| 6 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Documents and Settings/All Users/Documenti/Immagini/Desktop.ini |
| 7 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [M.C.] time | /Documents and Settings/Administrator/Recent |
| 8 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/desk |
| 9 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.AC.] time | /Programmi/Windows NT/Accessori/wordpad.exe |
| 10 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Programmi/Windows NT/Accessori/mswrd8.wpc |
| 11 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [MACB] time | /Documents and Settings/Administrator/Recent/very important.doc.lnk |
| 12 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Recent/very important.doc.lnk |
| 13 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [MACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 14 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 15 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /Programmi/Windows NT/Accessori/mswrd6.wpc |
| 16 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 17 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.ACB] time | /Documents and Settings/Administrator/Impostazioni locali/Cronologia/Histo |
| 18 | 06/10/13 | 17:19:05 | UTC | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/msftedit.dll |
| 19 | 06/10/13 | 17:19:05 | UTC | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/Ext |
| 20 | 06/10/13 | 17:19:05 | UTC | UserAssist key | Time of Launch | UEME_RUNPATH:C:/Programmi/Windows NT/Accessori/WORDPAD.EXE |
| 21 | 06/10/13 | 17:19:05 | UTC | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/Ext |
| 22 | 06/10/13 | 17:19:05 | UTC | NTUSER key | Last Written | Software/Microsoft/Windows/CurrentVersion/InternetSettings/5.0/Cache/Ext |
| 23 | 06/10/13 | 17:19:05 | UTC | RecentDocs key | File opened | Recently opened file of extension: .doc - value: very important.doc |
| 24 | 06/10/13 | 17:19:05 | UTC | UserAssist key | Time of Launch | UEME_RUNPATH |
| 25 | 06/10/13 | 17:19:05 | UTC | XP Prefetch | Last run | WORDPAD.EXE-20E16A4D.pf: WORDPAD.EXE was executed |

**Figure 8.** *Opening of Desktop/very important.doc and file link creation*

ated on 1st June 2013, at 13:07 CET. If after 60 minutes we try to shows the file property again, we will see that: Figure 3 and Figure 4. The field “Ultimo accesso”, translated into “Last Access”, was updated to 3 June 2013 at 17:42 CET.

The timeline follows: you can see the updating of `$SI` access timestamp of *time.csv* (Figure 5).

So, at last, think about that: during an investigation, you find a powered on PC running Windows XP. You see a highly interesting file on the user desktop, and the law enforcement are looking for just that file. In that case, it is not uncommon to take a first look at the file, maybe just to know about the creation date and time, or know just the last access time.

So, you just right click on that file and see the property, getting the right values. But if the file was created at least 60 minutes before your right click action, then the second time you right click or analyze the file with your preferred tool, you will get the wrong date, that is, the time you right clicked the file. No more original last access time that you firstly saw.

## 03 OPENING DOCUMENT FILE

Let’s take a look on what happened when opening a document file on Figure 6.

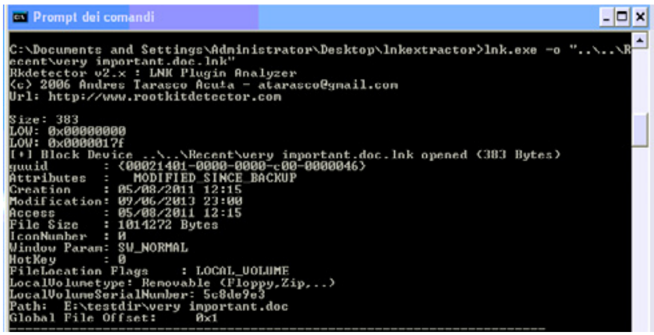
The really interesting part of that experiment is on rows 1553, 1557, 1565 and 1603: when you open a document file, in our case *privatefile.doc* (that was opened by *WordPad* program), a file was created under *RECYCLERS* folder.

It’s important to say that you will not find the `$SI` and `$FN` birth timestamp set because the file has the creation time set up as the original creation time, so you will find only the MFT change and file access timestamps set, as you can read on rows 1553 and 1557.

On rows 1566 and 1567 you can see the creation of a link file under the Recent folder, showed under the Start menu (Figure 6).

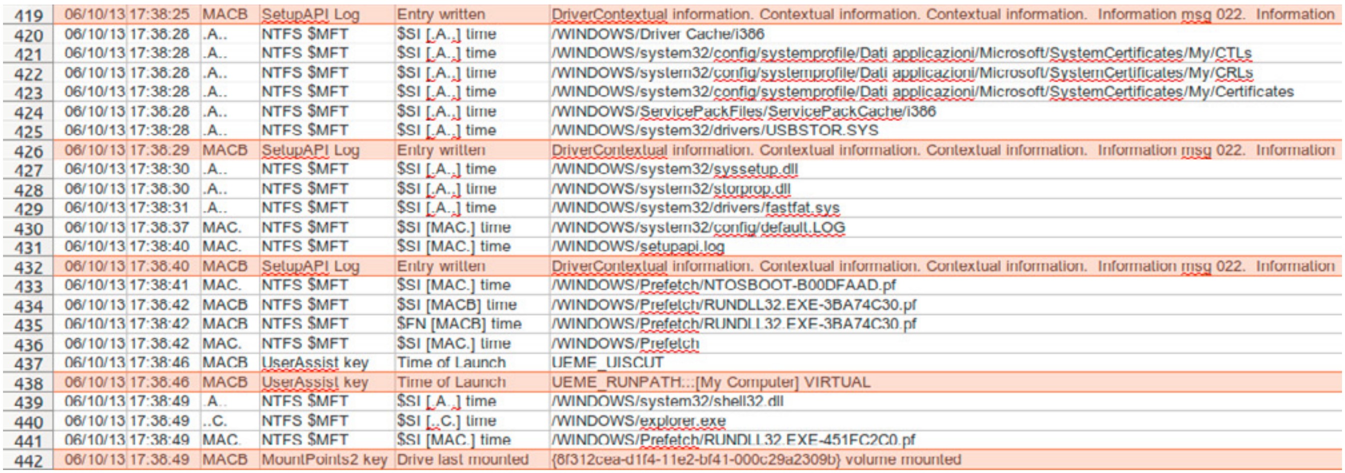
The file is named *Dc1.doc*: D stands for Deleted, c is the logical drive which the file belongs to, and 1 is a sequential number.

Figure 7 shows the start of *WORDPAD.EXE*, recorded by the Windows prefetch feature (row 1600), and then, on row 1603, the *Dc1.doc* metadata changed to reflect the action done on row 1607: the file was deleted, that is, moved into recycler bin (in this case, the DEL keystroke was typed) (Figure 7).



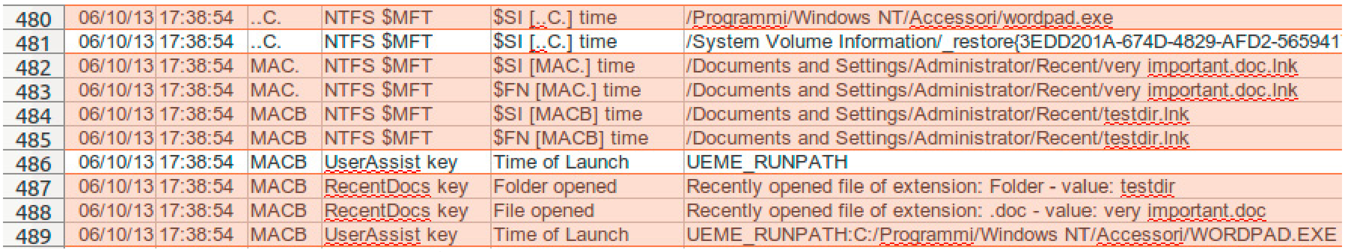
```
C:\Documents and Settings\Administrator\Desktop\lnkextractor>lnk.exe -o "..\..\R
ecent\very important.doc.lnk"
Rkdetector v2.x : LNK Plugin Analyzer
(c) 2006 Andres Tarasco Acuta - atarasco@gmail.com
Url: http://www.rootkitdetector.com

Size: 383
LOW: 0x00000000
LOW: 0x0000017f
[+] Block Device ..\..\Recent\very important.doc.lnk opened (383 Bytes)
guuid         : {00021401-0000-0000-c00-0000046}
Attributes    :   MODIFIED_SINCE_BACKUP
Creation      : 05/08/2011 12:15
Modification: 09/06/2013 23:00
Access        : 05/08/2011 12:15
File Size     : 1014272 Bytes
IconNumber    : 0
Window Param: SW_NORMAL
HotKey        : 0
FileLocation Flags     : LOCAL_VOLUME
LocalVolumetype: Removable (Floppy,Zip,...)
LocalVolumeSerialNumber: 5c8de9e3
Path:  E:\testdir\very important.doc
Global File Offset:      0x1
```

**Figure 11.** *lnkextractor in action*



| | | | | | | |
|---|---|---|---|---|---|---|
| 419 | 06/10/13 | 17:38:25 | MACB | SetupAPI Log | Entry written | DriverContextual information. Contextual information. Contextual information. Information msg 022. Information |
| 420 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/Driver Cache/i386 |
| 421 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/config/systemprofile/Dati applicazioni/Microsoft/SystemCertificates/My/CTLs |
| 422 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/config/systemprofile/Dati applicazioni/Microsoft/SystemCertificates/My/CRLs |
| 423 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/config/systemprofile/Dati applicazioni/Microsoft/SystemCertificates/My/Certificates |
| 424 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/ServicePackFiles/ServicePackCache/i386 |
| 425 | 06/10/13 | 17:38:28 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/drivers/USBSTOR.SYS |
| 426 | 06/10/13 | 17:38:29 | MACB | SetupAPI Log | Entry written | DriverContextual information. Contextual information. Contextual information. Information msg 022. Information |
| 427 | 06/10/13 | 17:38:30 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/syssetup.dll |
| 428 | 06/10/13 | 17:38:30 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/storprop.dll |
| 429 | 06/10/13 | 17:38:31 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/drivers/fastfat.sys |
| 430 | 06/10/13 | 17:38:37 | MAC. | NTFS $MFT | $SI [MAC.] time | /WINDOWS/system32/config/default.LOG |
| 431 | 06/10/13 | 17:38:40 | MAC. | NTFS $MFT | $SI [MAC.] time | /WINDOWS/setupapi.log |
| 432 | 06/10/13 | 17:38:40 | MACB | SetupAPI Log | Entry written | DriverContextual information. Contextual information. Contextual information. Information msg 022. Information |
| 433 | 06/10/13 | 17:38:41 | MAC. | NTFS $MFT | $SI [MAC.] time | /WINDOWS/Prefetch/NTOSBOOT-B00DFAAD.pf |
| 434 | 06/10/13 | 17:38:42 | MACB | NTFS $MFT | $SI [MACB] time | /WINDOWS/Prefetch/RUNDLL32.EXE-3BA74C30.pf |
| 435 | 06/10/13 | 17:38:42 | MACB | NTFS $MFT | $FN [MACB] time | /WINDOWS/Prefetch/RUNDLL32.EXE-3BA74C30.pf |
| 436 | 06/10/13 | 17:38:42 | MAC. | NTFS $MFT | $SI [MAC.] time | /WINDOWS/Prefetch |
| 437 | 06/10/13 | 17:38:46 | MACB | UserAssist key | Time of Launch | UEME_UISCUT |
| 438 | 06/10/13 | 17:38:46 | MACB | UserAssist key | Time of Launch | UEME_RUNPATH:::[My Computer] VIRTUAL |
| 439 | 06/10/13 | 17:38:49 | .A.. | NTFS $MFT | $SI [.A..] time | /WINDOWS/system32/shell32.dll |
| 440 | 06/10/13 | 17:38:49 | ..C. | NTFS $MFT | $SI [..C.] time | /WINDOWS/explorer.exe |
| 441 | 06/10/13 | 17:38:49 | MAC. | NTFS $MFT | $SI [MAC.] time | /WINDOWS/Prefetch/RUNDLL32.EXE-451FC2C0.pf |
| 442 | 06/10/13 | 17:38:49 | MACB | MountPoints2 key | Drive last mounted | {8f312cea-d1f4-11e2-bf41-000c29a2309b} volume mounted |

**Figure 9.** *USB plugging events*



| | | | | | | |
|---|---|---|---|---|---|---|
| 480 | 06/10/13 | 17:38:54 | ..C. | NTFS $MFT | $SI [..C.] time | /Programmi/Windows NT/Accessori/wordpad.exe |
| 481 | 06/10/13 | 17:38:54 | ..C. | NTFS $MFT | $SI [..C.] time | /System Volume Information/_restore{3EDD201A-674D-4829-AFD2-565941 |
| 482 | 06/10/13 | 17:38:54 | MAC. | NTFS $MFT | $SI [MAC.] time | /Documents and Settings/Administrator/Recent/very important.doc.lnk |
| 483 | 06/10/13 | 17:38:54 | MAC. | NTFS $MFT | $FN [MAC.] time | /Documents and Settings/Administrator/Recent/very important.doc.lnk |
| 484 | 06/10/13 | 17:38:54 | MACB | NTFS $MFT | $SI [MACB] time | /Documents and Settings/Administrator/Recent/testdir.lnk |
| 485 | 06/10/13 | 17:38:54 | MACB | NTFS $MFT | $FN [MACB] time | /Documents and Settings/Administrator/Recent/testdir.lnk |
| 486 | 06/10/13 | 17:38:54 | MACB | UserAssist key | Time of Launch | UEME_RUNPATH |
| 487 | 06/10/13 | 17:38:54 | MACB | RecentDocs key | Folder opened | Recently opened file of extension: Folder - value: testdir |
| 488 | 06/10/13 | 17:38:54 | MACB | RecentDocs key | File opened | Recently opened file of extension: .doc - value: very important.doc |
| 489 | 06/10/13 | 17:38:54 | MACB | UserAssist key | Time of Launch | UEME_RUNPATH:C:/Programmi/Windows NT/Accessori/WORDPAD.EXE |

**Figure 10.** *Opening very important.doc from a USB device*

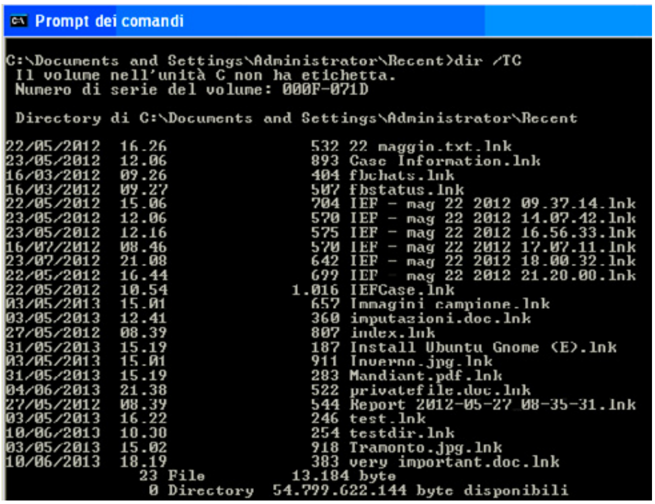
The key concept to keep in mind is: when you open a document file, with WordPad or Microsoft Office Word, a file is created under the *RECYCLERS* folder, so you can keep tracks of its changes and, if deleted, you can recover some basics information about it.

## 04 READING RECENTS FILE FOLDER

This is an interesting behavior of Windows XP, the scenario is: you view a file, say, on your Desktop folder. Windows creates a link file on the Recent folder, as saw on the previous paragraph.

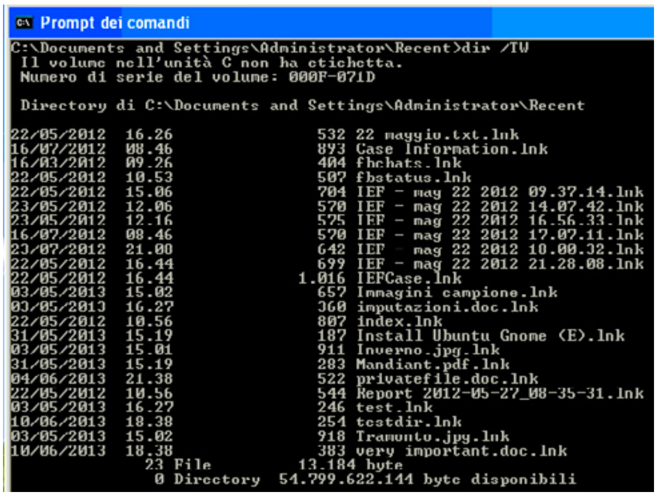
Later, you open a file with the same name but on a different location or folder: Windows XP does not create a new link file on the *Recent* folder, instead it updates the old one, so you lose the previous information.

Let's see how this happens. On Figure 8 you can see the opening of *very important.doc,* on row 2 you can see the click action on the file, resident on the user desktop, and at rows 11 and 12 you can see the creation of the link file in the *Recent* folder.



```
C:\Documents and Settings\Administrator\Recent>dir /TC
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 000F-071D

 Directory di C:\Documents and Settings\Administrator\Recent

22/05/2012  16.26                 532 22 maggio.txt.lnk
23/05/2012  12.06                 893 Case Information.lnk
16/03/2012  09.26                 404 fbchats.lnk
16/03/2012  09.27                 507 fbstatus.lnk
22/05/2012  15.06                 704 IEF - mag 22 2012 09.37.14.lnk
23/05/2012  12.06                 570 IEF - mag 22 2012 14.07.42.lnk
23/05/2012  12.16                 575 IEF - mag 22 2012 16.56.33.lnk
16/07/2012  08.46                 570 IEF - mag 22 2012 17.07.11.lnk
23/07/2012  21.08                 642 IEF - mag 22 2012 18.00.32.lnk
22/05/2012  16.44                 699 IEF - mag 22 2012 21.20.00.lnk
22/05/2012  10.54               1.016 IEFCase.lnk
03/05/2013  15.01                 657 Immagini campione.lnk
03/05/2013  12.41                 360 imputazioni.doc.lnk
27/05/2012  08.39                 807 index.lnk
31/05/2013  15.19                 187 Install Ubuntu Gnome (E).lnk
03/05/2013  15.01                 911 Inverno.jpg.lnk
31/05/2013  15.19                 283 Mandiant.pdf.lnk
04/06/2013  21.38                 522 privatefile.doc.lnk
27/05/2012  08.39                 544 Report 2012-05-27_08-35-31.lnk
03/05/2013  16.22                 246 test.lnk
10/06/2013  10.30                 254 testdir.lnk
03/05/2013  15.02                 918 Tramonto.jpg.lnk
10/06/2013  18.19                 383 very important.doc.lnk
              23 File         13.184 byte
               0 Directory  54.799.622.144 byte disponibili
```

**Figure 12.** *Link creation time*



```
C:\Documents and Settings\Administrator\Recent>dir /TW
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 000F-071D

 Directory di C:\Documents and Settings\Administrator\Recent

22/05/2012  16.26                 532 22 maggio.txt.lnk
16/07/2012  08.46                 893 Case Information.lnk
16/03/2012  09.26                 404 fbchats.lnk
22/05/2012  10.53                 507 fbstatus.lnk
22/05/2012  15.06                 704 IEF - mag 22 2012 09.37.14.lnk
23/05/2012  12.06                 570 IEF - mag 22 2012 14.07.42.lnk
23/05/2012  12.16                 575 IEF - mag 22 2012 16.56.33.lnk
16/07/2012  08.46                 570 IEF - mag 22 2012 17.07.11.lnk
23/07/2012  21.00                 642 IEF - mag 22 2012 10.00.32.lnk
22/05/2012  16.44                 699 IEF - mag 22 2012 21.28.08.lnk
22/05/2012  16.44               1.016 IEFCase.lnk
03/05/2013  15.02                 657 Immagini campione.lnk
03/05/2013  16.27                 360 imputazioni.doc.lnk
22/05/2012  10.56                 807 index.lnk
31/05/2013  15.19                 187 Install Ubuntu Gnome (E).lnk
03/05/2013  15.01                 911 Inverno.jpg.lnk
31/05/2013  15.19                 283 Mandiant.pdf.lnk
04/06/2013  21.38                 522 privatefile.doc.lnk
22/05/2012  10.56                 544 Report 2012-05-27_08-35-31.lnk
03/05/2013  16.27                 246 test.lnk
10/06/2013  18.38                 254 testdir.lnk
03/05/2013  15.02                 918 Tramonto.jpg.lnk
10/06/2013  18.38                 383 very important.doc.lnk
              23 File         13.184 byte
               0 Directory  54.799.622.144 byte disponibili
```

**Figure 13.** *lnk files modification timestamp*

The remaining highlighted rows shows the files involved in the file opening process.

Now, let's plug in a USB device (Figure 9) and click another file named *very important.doc*, the same name as the one on the user desktop.

Figure 10 shows this action: as you can see, on rows 482 and 483, the link file very *important.doc.lnk* is updated (MAC timestamp) to reflect our action, plus a new link created, *testdir.lnk*, newly created.

To better understand what happened, let try to parse the link file with *lnkextractor*: Figure 11 shows the v*ery important.doc.lnk* file information and metadata.

The timestamps shown refers to the object file, as is, *very important.doc*.

The important fields to take a look at are *LocalVolumetype*, telling us what kind of device the link refers to, *LocalVolumeSerialNumber*, as the name says, it's the logical volume serial number of the file location, *Path* is the folder where *very important.doc* resides.

To double check our test, have a look at the lnk timestamps.

Figure 12 shows *very important.doc.lnk* file creation: it is set to 18.19 (UTC+1), the time when *Desktop\very important.doc* was opened (see Figure 8, row 11).

The line "Numero di serie del volume", translated into Local Volume Serial Number, referring to the *C:* partition where *Desktop\very important.doc* resides, differs from the one recorded into very *important.doc.lnk*.

Figure 13 shows the modified timestamp of lnk files.

## CONCLUSIONS

In this article we have shown some Windows XP specific behavior that can must be taken into account when conducting forensics analysis of a Windows XP system.

We used often a timeline because it is an invaluable technique to know was happening and when on our system, but it is also important to cross-check the information and results gathered with timeline and other tools.

### About the Author

*Davide Barbato has 10 years of IT experience, the last three in Digital Forensics and Incident Response. He is currently employed in an important DFIR national firm, SSRI di Lorenzo Laurato S.a.s., in which his works as Chief Security Officer and DFIR analyst. He is also a teacher and speaker at national meetings and universities about Digital Forensics, IT Security and IT Privacy. davide.barbato@ssrilab.com*

# A BEGINNER'S GUIDE TO FORENSIC IMAGING

by Madeline Cheah

Are you starting on the road to a career in digital forensics? Or perhaps a student looking to get onto a course in this field? Maybe you just need a refresher after a little time away? This is a simple guide introducing you to one of the fundamentals of digital forensics, with a legislative narrative to set things in context.

**What you will learn:**

- perform a forensically safe imaging process, using either one of the Forensic Toolkit (FTK) tools (called FTK Imager) on Windows, or the dd command on Linux.
- highlight some of the current relevant issues surrounding dead analysis and
- will be aware of the implications of the ACPO Principles, particularly relevant if you're looking to start a course on digital forensics.

**What you should know:**

- be aware of the basics of hard drives,
- have a basic knowledge of Linux.
- have some understanding of the generic evidence handling processes (such as chain of custody) would also be beneficial in working through this guide.

This article deals with the art of forensic imaging, targeted specifically at students or those who have just started on the road to digital forensics. Imaging is one of the fundamentals of dead analysis (i.e. analysis of hard drives that does not involve investigation of live data) and is required to satisfy a number of laws and regulations including, in the UK, the ACPO Good Practice Guide for Handling Digital Evidence – also known as the ACPO Principles.

## THE ACPO GOOD PRACTICE GUIDE FOR HANDLING DIGITAL EVIDENCE

The ACPO Principles (as the above is also known as) is a crucial set of regulations dealing specifically with handling digital evidence and provides information on top of the normal handling of evidence expected as laid out by the Police and Criminal Evidence Act 1984 which also deals with arrest, detention, investigation and so forth.

The four principles are as follows:

### PRINCIPLE 1

No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

### PRINCIPLE 2

In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

### PRINCIPLE 3

An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

### PRINCIPLE 4

The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.
(ACPO, 2012)

The above forms the bedrock of the seizure and acquisition process, and is not only applicable to law enforcement. The principles should also be observed and considered when handling any sort of investigation, firstly because you never know if and when this data might be called upon in court, and secondly because it demonstrates your professionalism and competence as a digital forensics investigator. It is also worth noting that at every step during your seizure, your acquisition or your investigation, whether you are acting as first responder, investigator or analyst, you should create and maintain and audit trail in a way that enables a third party to follow and achieve the same result (which also complies with the concepts of universality and repeatability) and should be a mixture of contemporaneous notes (which are notes taken *at the time* of the activity, and is not the same as an account or summary), images, videos, case intake forms and all other forms of documentation which refers to the case.

Authority to perform any actions should also be present at every step of the way. The latter is usually the purview of the case officer or case manager, who will also ensure that other relevant legislation such as the Computer Misuse Act 1990, or the Data Protection Act 1998 is adhered to. Other considerations also come into play, such as dealing with issues to do with collateral intrusion, which relates to unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. In this case, wherever practicable, measures should be taken to avoid or minimize unnecessary intrusion, and where it is unavoidable to ensure that you have the authority to do so, and that the actions you take are *proportional* and *justified.* In other words, that all your actions are appropriate, and that there is adequate reason for doing as you have done or are about to do. Consideration should also be given to legally privileged data, such as legal records and information covered under the Data Protection Act 1998 – however, in many cases, an investigation would not proceed without a court order (such as a warrant of some kind) which supersedes any privilege.

Last but not least, live data should not be accessed unless you are aware of the repercussions and can justify your actions (as per principle 2). For example, if there was a screensaver on screen when you arrive as first responder you should not try to enter a password to log-on. Look for indications that on the display screen, such as whether there is an (active) webcam, or signs of active or ongoing communications. Generally, the safest option on finding a machine that is on is to take the power out by pulling out the kettle plug from a desktop computer, or removing the battery and power lead simultaneously from a laptop; however, it all depends on the circumstances. The machine(s) that you seize should then be transported back to the forensic lab for further study. It is important to note that taking such an action would mean that you would lose data held in memory as well as data regarding live connections.

So how then do we access the information held on a hard-drive or other storage media? This is where forensic imaging is important and comes into its own.

## WRITE-BLOCKERS

These are also known as "forensic disk controllers" and are used as a method of gaining read-only access to storage media without changing or altering data on the drives. This is a fundamental part of the imaging process, and the means of testing its veracity is shown later in this guide.

Write-blockers sit in between drive and operating system and intercept write commands, but allow read commands through, and can either report write commands as failures or cache these commands for the duration of the session. Hardware write-blockers can be divided into *native* (uses the same interface for in and out, for example IDE to IDE) or *tailgate* (which uses or adapts between different interfaces, for example SATA to IDE). Furthermore, there are both hardware write-blockers (Figure 1) and software write-blockers, which are usually operating system dependent, so a software write blocker that works on Windows may not work on Linux and vice versa.

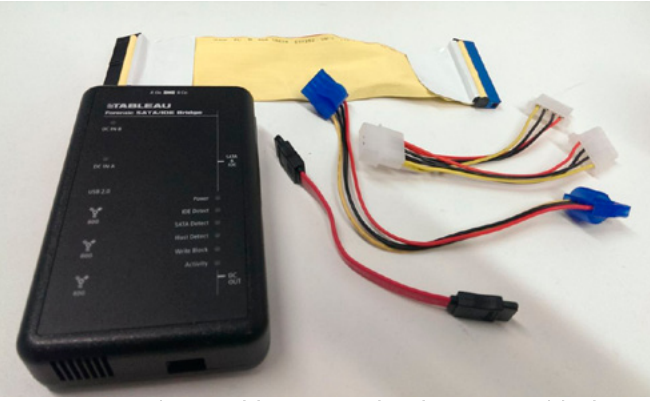


**Figure 1.** *A tailgate Tableau (T35e) hardware write-blocker with various leads*

It should be noted that for the particular model shown in Figure 1 that there is also a T35e RW (Figure 2) which is factory pre-set for both read *and* write, where-as the T35e model is set for permanent Read-Only.

As can be seen from Figure 3, there are lights to indicate that a hard drive is detected and that write-blocking is active. This can then be connected – depending on the write-blocking device used – to the forensic workstation, in this case using a micro-USB to USB cable.

Software write-blockers come in many flavours, but a good example is *SAFE Block XP*, designed for Windows XP, and is accepted by the National Institute of Standards and Technology. Other techniques such as disabling the write capabilities of USB ports in Windows registry could also be used, but these may not be forensically safe, as it has been reported that hex editing (using WinHex) can take place at the physical level (although it was blocked at the logical level).

You can test this out yourself by enabling USB write protection mode in registry (navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies` and switch WriteProtect from 0 to 1) and following the imaging processes outlined later on in this guide.

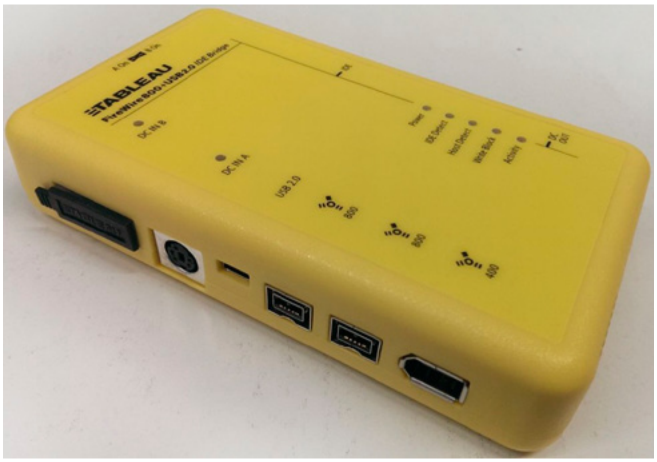


**Figure 2.** *A read-write capable write-blocker*

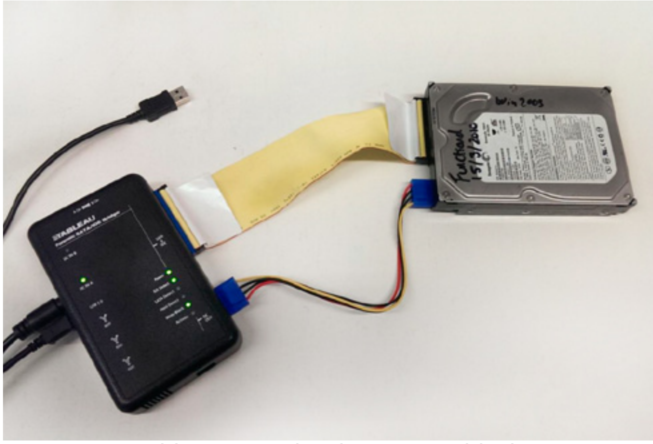


**Figure 3.** *A Tableau (T35e) hardware write-blocker connected to an 80Gb IDE hard drive*

## IMAGING

Imaging is the process of taking a *bit-by-bit* copy of storage media – it is not the same as copying. It is made by dumping data byte by byte or sector by sector, and will bring over everything on the drive, even unallocated space (which is extremely valuable to investigators in that "deleted" data is not the same as "erased data" and usually contains data that can be *carved*).

To ensure and prove that the data on the source drive (i.e. the disk you would like to image) is *identical* to the data on the destination drive (where you imaged your source disk to), a hash is taken before and after the imaging process. Because hash collisions are extremely rare, any change at all will change the checksum that results. The hashes verifying – where both image and source drive have identical hashes – is your proof that data on the source drive has not been altered and that the image held on the destination drive perfectly replicates your source data. As per ACPO principle 3, a note should be made of this.

There are several file formats used for disk images. The simplest of these is the raw image format, which can be created using the `dd` tool in Linux. It is functional and requires minimal resources; however it lacks some of the more useful features that modern image file formats contain, such as error correcting and compression. Other formats include AFF (*Advanced Forensics Format*), *E01* (an EnCase image file format and one of the de facto standards) and SMART (designed by the original authors of Expert Witness for Linux); these image formats are usually readable by many of digital forensic tools out there today.

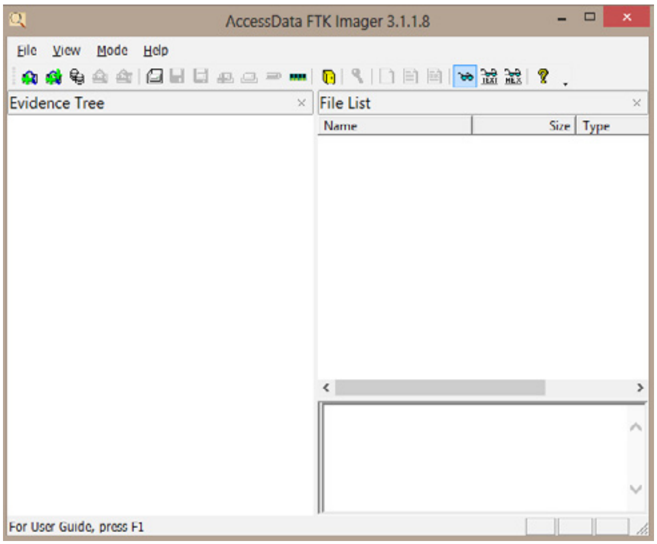


**Figure 4.** *FTK Imager main window*

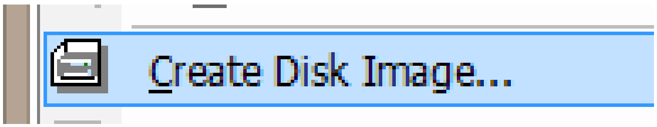


**Figure 5.** *Create Disk Image*

## THE IMAGING PROCESS USING FORENSIC TOOLKIT (FTK) IMAGER

*Forensic Toolkit (FTK)* is considered one of the industry standard suites in digital forensics, and this particular part of the process will lay out how to use the *Imager* tool, which is available for free from AccessData's website. Again, it cannot be emphasized enough that as part of this process, you should be keeping contemporaneous notes, both for your own records and to comply with the ACPO Principles.

After installing, run the program and you will see the Imager window appear (Figure 4).

Selecting "Create Disk Image" from the *File* menu (Figure 5) will bring up a dialog box allowing you to select from several options (Table 1)

**Table 1.** *FTK Imager options*

| | |
|---|---|
| Physical Drive | An actual drive connected to the workstation (such as where we've connected a drive via a write-blocker) |
| Logical Drive | A partition |
| Image File | Used to convert one kind of image file to another |
| Contents of a folder | Excludes deleted files and unallocated space, and is used for logical file-level analysis only |
| Ferrico Device | For multiple CD/DVDs |

In this case, the option to select is the "Physical Drive", at which point it will ask you to add a destination (to save your image file to) as seen in Figure 6, as well as other information, such as image format (Figure 7). Ensure that the option "Verify images after they are created" is checked as this verifies whether the hashes match at the end of your imaging process, thereby ensuring compliance with ACPO Principle 1.

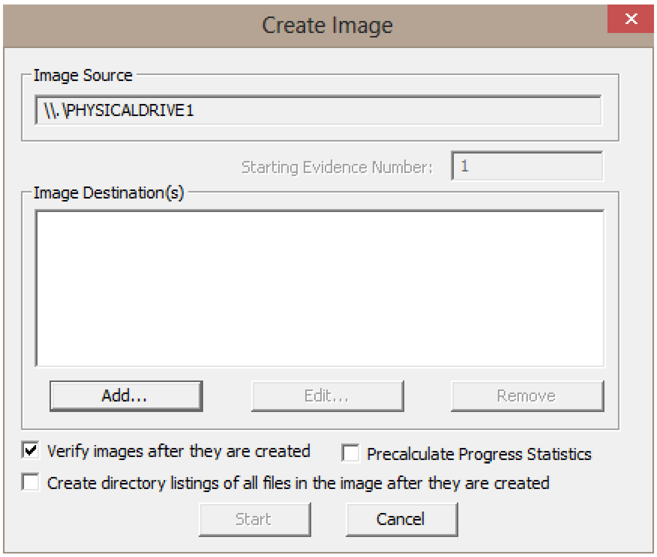

Create Image

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

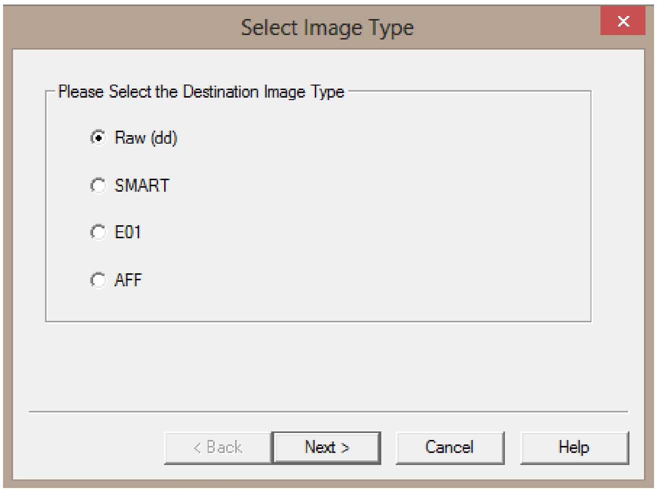
Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

**Figure 6.** *Creating an image*

Clicking *Next >* in the "Select Image Type" window will take you to a dialog box where you can input some case information (Figure 8) – again, this would form part of your audit trail. Remember that this case information is there for you to recall what the piece of evidence is – as a digital forensics investigator, you may do hundreds of these a year, and so it's vital that you include a descriptive label.


Select Image Type

Please Select the Destination Image Type

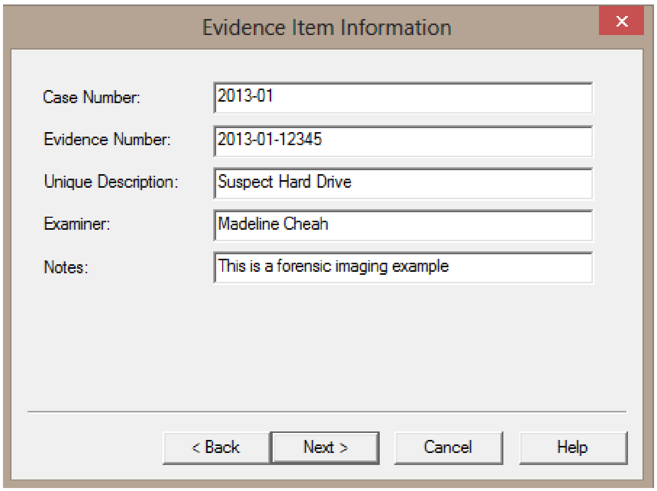
● Raw (dd)

○ SMART

○ E01

○ AFF

**Figure 7.** *Image file format options*


Evidence Item Information

Case Number: 2013-01

Evidence Number: 2013-01-12345

Unique Description: Suspect Hard Drive

Examiner: Madeline Cheah

Notes: This is a forensic imaging example

**Figure 8.** *Entering evidence information*

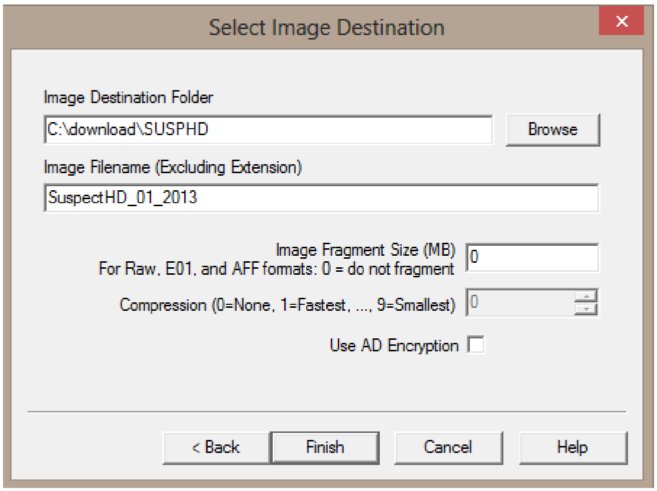

Select Image Destination

Image Destination Folder

C:\download\SUSPHD

Image Filename (Excluding Extension)

SuspectHD_01_2013

Image Fragment Size (MB) 0

For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

**Figure 9.** *Image destination and other options*

At the same time, all of these details are disclosable to defense, so ensure that you give nothing away that is sensitive, and keep it professional.

The program will then ask for image destination and filename (Figure 9) as well as asks you to enter a value for fragmentation (which allows for the breakup of a large image file into smaller files) compression and encryption. Note that in this case, there is no option to define compression, and that is because the format chosen did not support this (Figure 10).

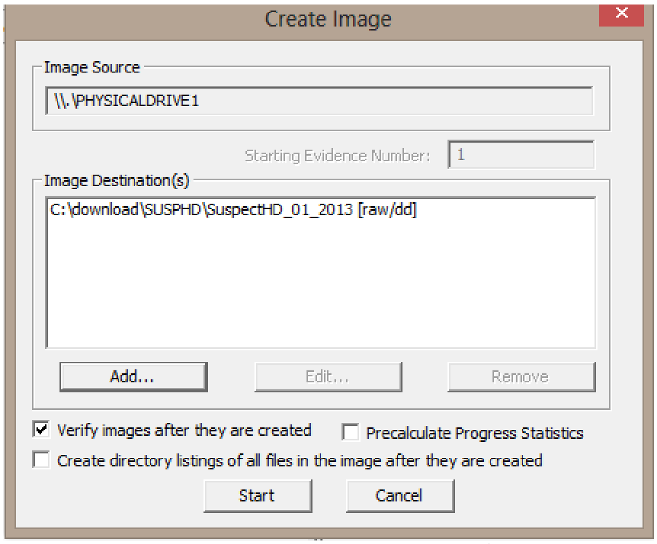

Create Image

Image Source
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)
C:\download\SUSPHD\SuspectHD_01_2013 [raw/dd]

☑ Verify images after they are created
☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created

**Figure 10.** *An image to be created in raw/dd format*

Clicking *Start* will result in the imaging starting (Figure 11), and depending on the size of the drive and the capabilities of your workstation could take a varying amount of time.

At the end of the process, hashes of source drive and image (Figure 12) are taken in order to verify that the data has not been altered in any way during transfer, that the image file contains an exact representation of the source drive, and since a write-blocker was used, no writes were made to the source drive, thereby complying with ACPO Principle 1.

As you can see, the process here is fairly simple, but the concepts themselves and how they fit within the digital forensics context should be one that you explore further as part of your study. For example, what happens if there is no authority but action was taken? What might you do to minimize collateral intrusion (defined as unnecessary invasion of privacy of an individual who is not under investigation)? What other legislation might come into play?

FTK Imager can also be used for triaging evidence. To *triage* is to prioritise and sort tasks or evidence based on need or urgency. This can be done by using the “Add Evidence” option under the *File* menu, rather than “Create Disk Image”, and it allows you to view a physical or logical drive or a file in a variety of ways.

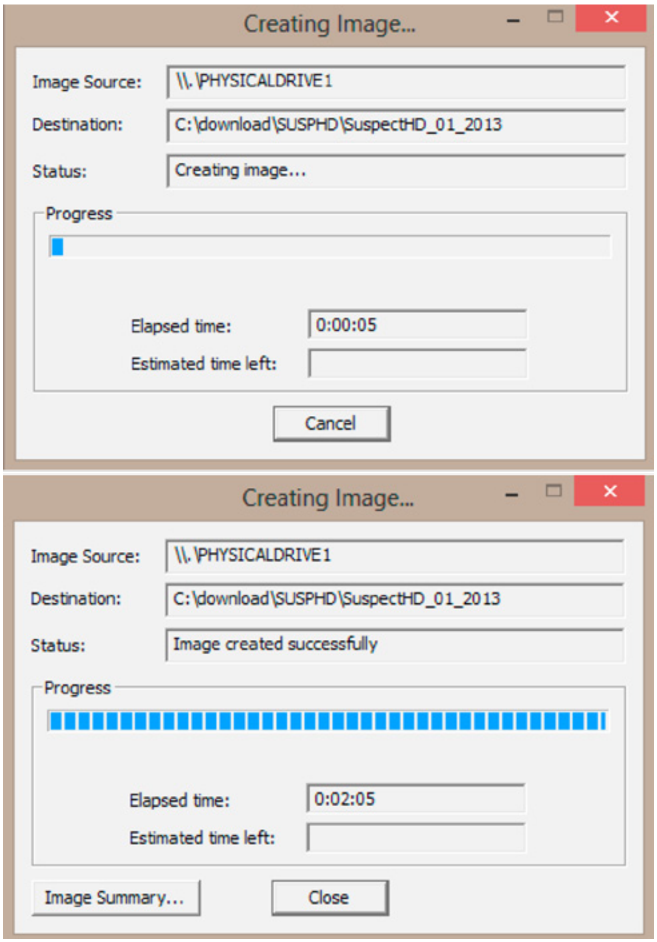

Creating Image...

Image Source: \\.\PHYSICALDRIVE1
Destination: C:\download\SUSPHD\SuspectHD_01_2013
Status: Creating image...

Progress

Elapsed time: 0:00:05
Estimated time left:

Creating Image...

Image Source: \\.\PHYSICALDRIVE1
Destination: C:\download\SUSPHD\SuspectHD_01_2013
Status: Image created successfully

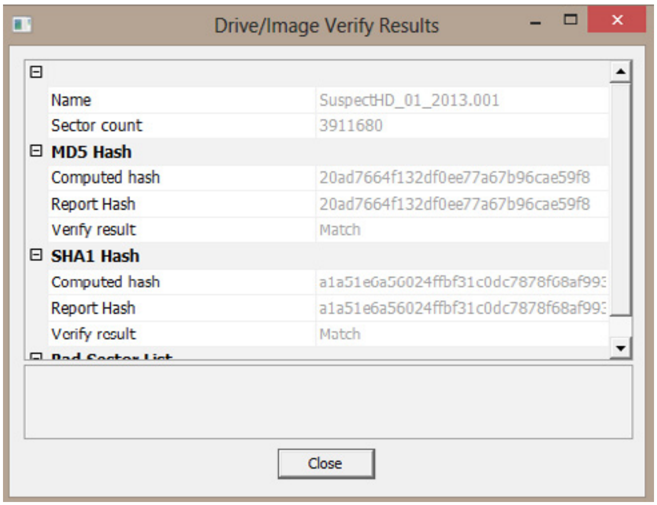
Progress

Elapsed time: 0:02:05
Estimated time left:

**Figure 11.** *Image being created*

## THE IMAGING PROCESS USING LINUX’S DD AND DCFLDD

As aforementioned, the *dd* command will result in a raw image file, but is a tool that is easy to use. The first step would be to mount the drive onto your Linux machine, if it isn’t already, and you can check this by using the command *mount* into the terminal. If you’re connecting a device via a hardware write-blocker (as you should be doing), you may need to mount the drive manually.


Drive/Image Verify Results

| | |
|---|---|
| Name | SuspectHD_01_2013.001 |
| Sector count | 3911680 |
| **MD5 Hash** | |
| Computed hash | 20ad7664f132df0ee77a67b96cae59f8 |
| Report Hash | 20ad7664f132df0ee77a67b96cae59f8 |
| Verify result | Match |
| **SHA1 Hash** | |
| Computed hash | a1a51e6a56024ffbf31c0dc7878f68af993 |
| Report Hash | a1a51e6a56024ffbf31c0dc7878f68af993 |
| Verify result | Match |
| **Bad Sector List** | |

**Figure 12.** *The hashes match*

Depending on the number of physical drives or logical drives you have already mounted, your mounted drive would be named along the lines of */dev/sdxy*, where x is a letter starting from "a" corresponding to physical drives, and y being a number depending on logical partitions on your physical drive. This is particularly important as reversing the source drive and target drive could result in data loss.

The basic command structure is as follows:

```
dd if=/dev/sdb1 of=/dev/test.image bs=xxxx
                       conv=noerror,notrunc
```

The breakdown of the command is given in Table 2.

**Table 2.** *Breakdown of the dd command*

| | |
|---|---|
| If | Input file/ source drive |
| Of | Output file / destination drive |
| Bs | Stands for "block size" with the default being (usually) 512. This setting may have an impact on performance. The value of this can be a decimal integer, or suffixes can be used to denote multiplications, for example w is multiplication of 2, and b is a multiplication of 512. |
| Notrunc | do not truncate the output file |
| Noerror | Keep going even if there is an error |

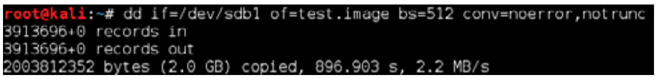
There are also several options you can use in order to make it easier to isolate the parts of the physical drive that you would like to image:

`count = n` where n is a number, and instructs dd to copy only n input blocks

`skip = n` where n is a number, and instructs dd to skip n input blocks before starting to copy

`conv=sync` If there is an error, null fill the rest of the block

This should result in the source drive being imaged (Figure 13) – the next step is to ensure that the image matches the source.



```
root@kali:~# dd if=/dev/sdb1 of=test.image bs=512 conv=noerror,notrunc
3913696+0 records in
3913696+0 records out
2003812352 bytes (2.0 GB) copied, 896.903 s, 2.2 MB/s
```

**Figure 13.** *dd command in action using Kali Linux*

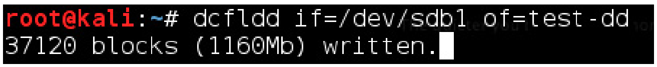
If you recall the guide for *FTK Imager,* the program verifies the hashes automatically at the end of the imaging process. Hashing (using the MD5 algorithm) can be performed using the *md5sum* command in Linux the structure of which is:

```
md5sum[OPTION][FILE] > hash.md5
```

This outputs the hash to a file called hash.md5; the hash of *test.image* as seen in Figure 13 can then be compared to the hash of the original drive that you imaged.

The *md5sum* in itself is a very useful command as it also allows you to verify programs that have known hashes in order to ensure that the program doesn't come with an unwelcome payload or has been tampered with. Alternatively, you can also use the SHA-1 algorithm, denoted by the command *sha1sum* – you'll notice that *FTK Imager* when verifying uses both hash types (Figure 12).

A good alternative is the *dcfldd* command (Figure 14), developed by the US Department of Defense specifically for forensics and security specialists – this should be available on all versions of Backtrack or Kali Linux. As with the *dd* command, be careful with the order of *if* and *of* as you can just as easily erase data if you get them mixed up.



```
root@kali:~# dcfldd if=/dev/sdb1 of=test-dd
37120 blocks (1160Mb) written.
```

**Figure 14.** *A demonstration of dcfldd in Kali Linux*

Notice that this is somewhat nicer, as it gives you a count of the blocks written as it is going. You can also add `hashlog=filename` to the end of the command in order to create a file containing the hash at the same time.

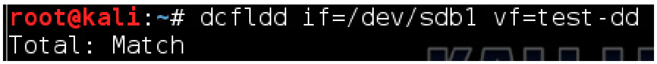
To view the MD5 hash calculated using *dcfldd*, type the following in:

```
Cat filename
```

The other nice thing about *dcfldd* is that you can verify the image you made against the original input with one simple command:

```
dcfldd if=filename vf=imagefilename
```

As you can see in Figure 15, there is a match between the drive that was imaged, and the image itself.



```
root@kali:~# dcfldd if=/dev/sdb1 vf=test-dd
Total: Match
```

**Figure 15.** *A demonstration of vf in Kali Linux*

## WARNING

If you are using VMWare as your tool of choice to run Linux on, the hashes may not match as VMWare adds quite a bit of extraneous information such as headers and rollback data when you use the *dd* tool.

The techniques described above can also be used for data recovery – whether it's recovering the whole disk, or recovering a single important file – or to back up data as well. You won't need to go through processing or documenting in the exact same way or to the same rigorous standards, especially if it's for personal use; however, it's always a good idea to have some sort of audit trail with these things.

## CONCLUSION

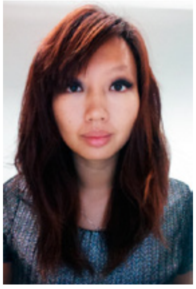
Although the above lays out the basic forensic imaging process, this is only really applicable to dead acquisition – live acquisition can be altogether more challenging, and is compounded by the fact that (amongst other things) there are issues surrounding convergent technology, and that everything is networked. Furthermore, legal precedent is still nascent (even for more established laws such as the Computer Misuse Act 1990) with many cases being settled out of court. There are also many ambiguities present, such as what constitutes a computer – the modern smartphone is more powerful than the computers in 1990 when the law was created.

To conclude, for those of you who wish to take it a step further, loading these images onto a digital forensics toolkit can be a good way to explore further – some suggestions are Passmark's OS Forensics, or some of the tools available on Kali Linux (these are free, or have a free trial version).

## SUMMARY

The aim of this guide was to provide beginners or those just starting digital forensics courses a flavor of the digital forensics process, starting from one of the fundamentals, imaging. Specialist tools and techniques are outlined, with some issues presented surrounding legislation as well as a step by step guide to creating a forensically safe image, in compliance with the ACPO Principles. The reader, from this, should then be able to explore and expand on other issues surrounding digital forensics investigation, not just directly but also peripherally related to this process, such as looking at first responders, addressing chain of custody or exploring live analysis.

### About the Author



*The author is an Assistant Lecturer in Digital Forensics and Ethical Hacking and a member of the Digital Security and Forensics (SaFe) Applied Research Group at Coventry University. Current research interests include browser forensics, the legal implications of digital forensic processes and cyber security education.*

## ON THE WEB

- *http://www.legislation.gov.uk/* – UK Legislation Archive
- *http://www.accessdata.com/support/product-downloads* – FTK Imager version 3.1.3 (MD5: fcf5196628e88608f779257a35ce5fd2)
- *http://www.tableau.com/index.php?pageid=products* – Tableau Write-Blockers
- *http://www.osforensics.com* – OS Forensics (Passmark)
- *http://www.kali.org* – Kali Linux (VMWare machines are also available here)

## GLOSSARY

ACPO – Association of Chief Police Officers, responsible for directing and leading the policing practices in England, Wales and Northern Ireland

Contemporaneous notes – Information that is recorded at the time or as soon afterwards as possible – it is not a past account or a summary.

EnCase – An industry standard digital forensics software created and maintained by Guidance Software.

Forensic Toolkit – An industry standard digital forensics package created and maintained by AccessData

MD5 – Message Digest 5; a cryptographic hash function used to create checksums in order to verify integrity

SHA-1 – Secure Hash Algorithm; also a cryptographic hash function used to create checksums in order to verify integrity

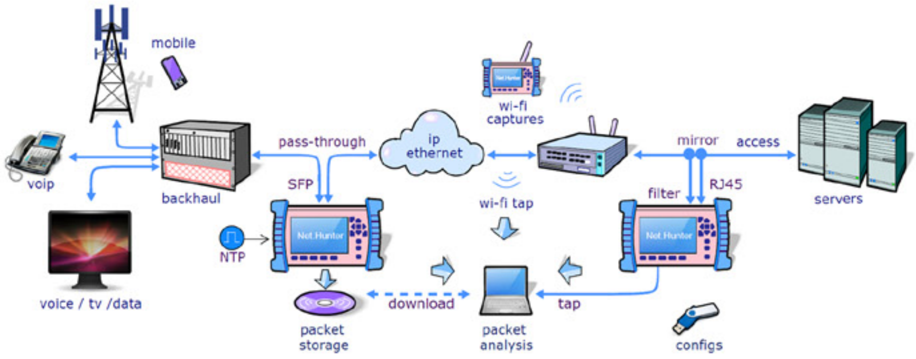
SSD – Solid state drive, a storage device that uses NAND-based flash memory rather than the traditional spinning disks

Write-blocker – A tool used to prevent writing to a disk, and can either be implemented using a hardware or a software tool

## REFERENCES

ACPO, 2012. ACPO Good Practice Guide for Digital Evidence [pdf] Available at: *http://www.datarecoveryspecialists.co.uk/cms/ckfinder/userfiles/files/digital-evidence-2012.pdf* [Accessed 17 June 2013]

# Net.Hunter a Tireless Packet Capture



- Stream-to-disk **packet capture tool**
- Full Duplex **wirespeed** performance
- **No delays**, jitter, or loss to live traffic
- User defined **filters**: MAC, IP, Port...
- Full **Traffic aggregation** (Rx+Tx)
- **Full Tap** to 1000BASE-T funtion
- IDEAL for **Security** and **Forensic**
- GOOD for **Lawful interception**
- **Hand-held,** self contained, batteries
- **Undetectable:** no IP no MAC

Critical Data
VoIP
IPTV capture
Data Loss
Denial of Service
Threats
Malware
Fatal Errors
Phishing
Protocol Analysis
Hackers
SPAM
Troubleshooting
Forensic Analysis

ALBEDO

www.albedotelecom.com
info.telecom@albedo.biz

# WINDOWS MEMORY FORENSICS & MEMORY ACQUISITION

**by Dr Craig S. Wright, GSE, GSM, LLM, MStat**

This article takes the reader through the process of imaging memory on a live Windows host. This is part one of a six part series and will introduce the reader to the topic before we go into the details of memory forensics. The first step in doing any memory forensics on a Windows host involves acquisition. If we do not have a sample of the memory image from a system we cannot analyze it. This sounds simple, but memory forensics is not like imaging an unmounted hard drive. Memory is powered and dynamic, and changes as we attempt to image it.

**What you will learn:**

- An introduction to Memory acquisition and imaging
- Memory analysis reasoning
- Why we image and analyse memory

**What you should know:**

- You should have a basic understanding of forensics and incident handling
- Understand system imaging
- Basic windows processes

This means it is not a repeatable process. Not that there is a requirement at all times for the results of a forensic process to provide the same output; in this it is not necessary to be able to repeat a process and obtain exactly the same results. It does not mean we cannot use a variable process in a forensic investigation. What it does mean is we have a set of steps that will allow us to image memory but that every time we do those the results will change.

## INTRODUCTION

Although the results obtained in a forensic analysis of memory will vary with no two memory images being able to display the same hash value, this does not mean the process does not follow with a scientific rigor. If the same investigator uses the same process to obtain and acquire an image of the system memory on the same computer twice in a row both images will vary significantly. The reason for this is that computer memory changes during the imaging process.

Parts of the physical memory are mapped to hardware devices. The majority of mapped and allocated hardware memory cannot be easily imaged and an attempt to do so will result in the image process crashing the system. So for all these differences and variations in the acquisition of a system's memory we have a process that can be followed but results that will vary each time it is used. Some forensic practitioners see this as a problem. That however is far from the truth. If we take medical forensics as an example, the practice of forensic autopsies has been followed for over 100 years. Yet in this practice it is not possible for another surgeon or coroner to return the organs to the body and repeat the process. What they can do is follow a set process that will gain similar results if they are not the same.

In this article we will discuss what you should know about imaging computer memory. You will learn the fundamentals of memory imaging on a Windows system. Further follow-up articles to this one we will look at using specific tools and imaging processes.

## WHERE DO WE START

Like any good forensic practice we need to follow repeatable processes. One of the best guidelines for doing this is the Internet engineering task force request for comment 3227 (*http://www.ietf.org/rfc/rfc3227.txt*) – RFC 3227, "Guidelines for Evidence Collection and Archiving".

Like all standards and checklists, this document is far from perfect and needs to be modified to suit many environments. It is however a starting guide that should be considered. Anytime you deviate from a well-known checklist such as this it is important to justify and document your reasons.

The first thing to note is that memory is volatile evidence. It changes rapidly and unlike a hard drive evidence can quickly disappear. For this reason it is necessary to acquire an image of the system memory whenever possible as early as possible into the acquisition process. Each time you run a command on the system we are changing evidence. In doing this we are potentially overwriting areas of memory that may contain valuable information necessary for a case. The quicker we gain access to the memory and image it the less likely it is we will lose that evidence.

The best forensic method is always the one that achieves the results we are seeking most economically, but more importantly with the fewest changes to the system. In this article we will not be discussing the more disruptive and potentially damaging methods (including the Cold Boot Method) that can be used in systems where access is not available to image memory.

### RFC3227

RFC 3227 provides us with some good guidelines on what we should image first. This is listed in order below:

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

Easy and Quick
Download of
YouTube
Videos!
WiseVideoSuite
Wise Video Downloader 1
✓ Access to HD Videos
✓ Search Without Browsers
✓ A-link-is-enough Download
✓ Easy and Fast
Official Website for More Information:
www.wisevideosuite.com/wisevideodownloader.html
Compatible with Windows 7
Windows 8 Compatible
Support system:
Windows XP, Vista, Win7/8
(both 32-bit and 64-bit)

In our case, the capture of non-hardware assigned memory will grab the majority of the system registers, cache routing tables etc. Though it is not possible to capture everything unaltered – it is highly unlikely that this will ever be achieved in any incident handling process.

## MEMORY IMAGING AND FORENSICS

Memory imaging differs markedly from many other forms of digital forensics. As we have already noted, memory imaging differs significantly from disk imaging. When we image a hard drive we generally do not have to skip areas and the same process can be run multiple times without altering any evidence. To that extent hard drives are not terribly volatile source of evidence

The process of running a memory imager requires that we load the process into memory. This process of course results in changes to the memory we are attempting to image. This is why the result is not repeatable in a way that will produce the same hash value each time we enact it. The worst part of all this is that we cannot even determine whether the program has correctly imaged the memory in all cases. Being that we can expect different results each time we run a memory imager we cannot accurately determine if a particular section of memory was missed or incorrectly copied.

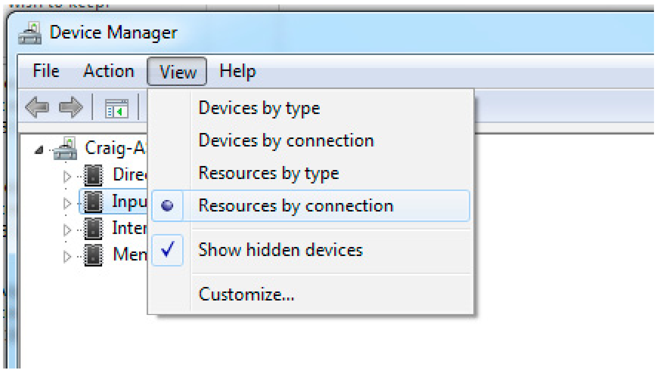
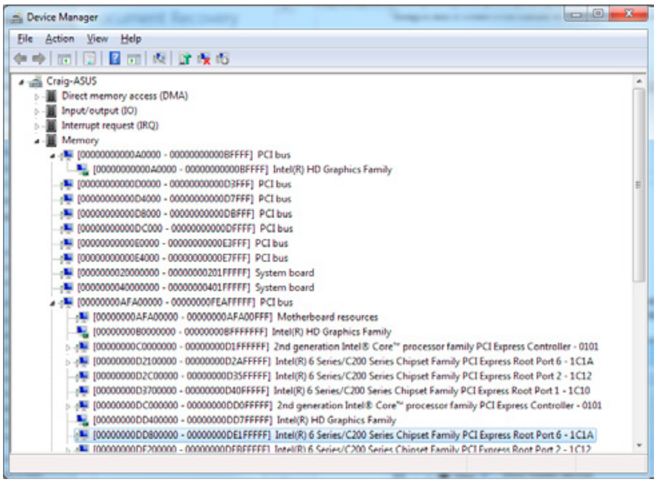


Figure 1. *Viewing Windows Memory*



```
Craig-ASUS
  Direct memory access (DMA)
  Input/output (IO)
  Interrupt request (IRQ)
  Memory
    [00000000000A0000 - 00000000000BFFFF]  PCI bus
      [00000000000A0000 - 00000000000BFFFF]  Intel(R) HD Graphics Family
    [00000000000D0000 - 00000000000D3FFF]  PCI bus
    [00000000000D4000 - 00000000000D7FFF]  PCI bus
    [00000000000D8000 - 00000000000DBFFF]  PCI bus
    [00000000000DC000 - 00000000000DFFFF]  PCI bus
    [00000000000E0000 - 00000000000E3FFF]  PCI bus
    [00000000000E4000 - 00000000000E7FFF]  PCI bus
    [0000000020000000 - 00000000201FFFFF]  System board
    [0000000040000000 - 00000000401FFFFF]  System board
    [00000000AFA00000 - 00000000FEAFFFFF]  PCI bus
      [00000000AFA00000 - 00000000AFA00FFF]  Motherboard resources
      [00000000B0000000 - 00000000BFFFFFFF]  Intel(R) HD Graphics Family
      [00000000C0000000 - 00000000D1FFFFFF]  2nd generation Intel® Core™ processor family PCI Express Controller - 0101
      [00000000D2100000 - 00000000D2AFFFFF]  Intel(R) 6 Series/C200 Series Chipset Family PCI Express Root Port 6 - 1C1A
      [00000000D2C00000 - 00000000D35FFFFF]  Intel(R) 6 Series/C200 Series Chipset Family PCI Express Root Port 2 - 1C12
      [00000000D3700000 - 00000000D40FFFFF]  Intel(R) 6 Series/C200 Series Chipset Family PCI Express Root Port 1 - 1C10
      [00000000DC000000 - 00000000DD0FFFFF]  2nd generation Intel® Core™ processor family PCI Express Controller - 0101
      [00000000DD400000 - 00000000DD7FFFFF]  Intel(R) HD Graphics Family
      [00000000DD800000 - 00000000DE1FFFFF]  Intel(R) 6 Series/C200 Series Chipset Family PCI Express Root Port 6 - 1C1A
      [00000000DF200000 - 00000000DFBFFFFF]  Intel(R) 6 Series/C200 Series Chipset Family PCI Express Root Port 2 - 1C12
```

Figure 2. *Windows Hardware Memory Locations*

Memory imaging is not an instantaneous process. The result of this is that a program or other data in memory can change from a portion of memory that has not been read to one that the imager has already copied as the process is run. Consequently, it is possible to miss copying selected areas of memory. This does not invalidate the forensic value of a memory image. What we need to understand is not that the collected evidence is invalid, but that we only have a subset of the entire memory from the machine we are seeking to image. What we do have is an accurate copy of what is on the machine. This is where the forensic value is gained. At the same time however, we may not have a complete copy of all of the evidence, and it could be further evidence that the evidence of an event or incident is missing from our investigation.

Cyber criminals are rational [1]. When they create malicious code they consider the economic constraints and opportunities [2] that are associated with producing and managing malicious code.

As a result, malicious code authors have created ways for their programs to bypass many memory capture processes. They specifically seek to evade memory imaging. There are reasons for this – if malicious code can evade detection, it can manage to remain undiscovered and hence active for longer periods of time. In doing this, the cybercriminals can maximize the economic returns that they gain from the creation of this malicious code.

I have discussed some of the methods used by malicious code authors and penetration testers (*Extending Control, API Hooking*) in penetration testing articles published in Hakin9 (*http://hakin9.org/buffer-overflow-exploiting-software-052012/*) amongst others. In some instances the attacker creates code that uses processes such as API hooking to link into system processes and kernel functions. Some of the more sophisticated Malware will recognize the name of an imaging program or the system calls that such a program makes and will intentionally alter its behavior. This could involve changing the location of the malicious code in memory as the system is imaged and it could even extend to feeding false data to the memory imager.

## DEVICE MEMORY

If we open up the Windows "Device Manager" and select "Resources by connection" (see Figure 1) we can have a look at the memory devices on a Windows system.

Under the Windows kernel object, `\Device\PhyiscalMemory` we have the means to obtain direct access to the memory on a Windows system.

We can see (Figure 2) that some of the physical memory is allocated to hardware devices. These areas are ones we need to avoid when imaging the memory as any request to these memory locations is written to the hardware device. This could crash the system. These are known as mapped memory locations.

These points are important to note when working on Windows systems. Each tool will have different specialties which require different privileges and have different advantages across different operating systems. Before we select which tool will be deployed in a particular imaging engagement, we need to consider the particular operating system we wish to image.

A particular problem comes from practicing with a tool on one operating system and then migrating the same processes to another. What works on Windows XP for instance may not work, or may even crash the system in Windows 7. In particular, it is important to practice on the various different systems you will engage with. If you are working in an environment with multiple operating systems it is important to practice on each of them. This means gaining an understanding of the following:

- the required system privilege levels
- the various system architecture (such as 32-bit versus 64-bit)
- the differences in operating systems including patching levels
- any difference where data is written or called from.

## CAPTURE TOOLS

In this article we will not address any of the commercial products. In later articles following this one we will continue with details on the use of particular tools that are available freely. It is wise to become familiar with a wide range of tools depending on the circumstances you work within.

Mandiant distributes two free tools for memory capture and analysis:

- Redline (*http://www.mandiant.com/resources/download/redline*)
- Memoryze (*https://www.mandiant.com/resources/download/memoryze*)

We will look at a free tool from MoonSol in this article.

## MOONSOLS DUMPIT

Moonsols provides a free Windows memory dump kit (*http://www.moonsols.com/ressources/*). As it states on its website you can do the following:

- This utility is used to generate a physical memory dump of Windows machines. It works with both x86 (32-bits) and x64 (64-bits) machines.
- The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting.
- Possible to deploy the executable on USB keys for quick incident response needs.

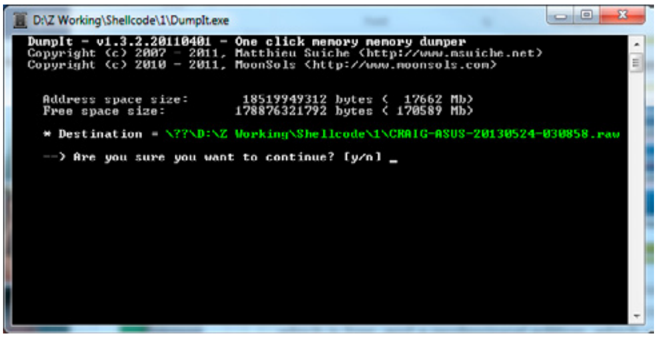
It is simple to run DumpIt. The program runs when you extract it from the file and it can be run from an external device such as a USB. In figure 3 we see it running with the default destination for a saved image. You do require Administrative privileges on the host. Running in default mode (such as double-clicking) saves the image which is named based on the time, the system ID and with the default extension of .raw.

The default location can be changed but happens to be the location where you run the program from. You will also note that the required size of the image is noted (Address space size) and that the available space on the destination drive is listed (Free space size). It is of course essential to ensure that there is sufficient free space on the drive to be able to complete the imaging process.

Starting a memory image capture is simple from the prompt noted in Figure 3 we just select “y” in order to image the drive or “n” to end the program.

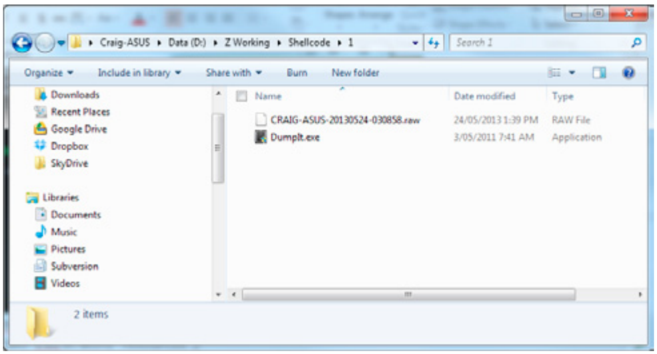
Once the image capture is completed, it will be stored in the destination directory as shown in Figure 4. At this point we have taken volatile memory and created a forensic image that we can analyze later without fearing further data loss. Always ensure that the image copy is made to an external device and not the primary hard drive (Figure 4).

There are no command line options built into DumpIt. You either need to change the location or hook data into the program to change its running



```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


  Address space size:        18519949312 bytes (  17662 Mb)
  Free space size:          178876321792 bytes ( 170589 Mb)

  * Destination = \??\D:\Z Working\Shellcode\1\CRAIG-ASUS-20130524-030858.raw

  --> Are you sure you want to continue? [y/n] _
```

**Figure 3.** *MoonSols DumpIt*



| Name | Date modified | Type |
|---|---|---|
| CRAIG-ASUS-20130524-030858.raw | 24/05/2013 1:39 PM | RAW File |
| DumpIt.exe | 3/05/2011 7:41 AM | Application |

**Figure 4.** *The memory image*

state. For this reason it can be considered a one step memory imaging program.

## PAGE FILE

The Windows page file is one of the simpler ways of analyzing memory. The location can vary but the file "pagefile.sys" is not too difficult to find even on an imaged hard drive. This creates a less volatile form of memory analysis. Another opportunity comes from analyzing the Windows hibernation file (Hiberfil.sys). One of the best ways of capturing memory is when a virtual machine is in use. System snapshots capture and save memory as well as hard drive-based information and evidence.

I will not list the general location of the page file as this does vary and more importantly a Windows system can have up to 16 different locations across different drives for storing page files. One of the most important reasons to capture a page file is that idle processes can be "paged" out of active memory when they are in the background. Simply imaging the systems memory could thus result in missing critical information.

Capturing a page file should be done separately to the complete imaging of the hard drive as the page file will change far more rapidly than the hard drive itself. It may be less volatile than system memory but it is still volatile evidence. To capture the page file will require access to the raw drive, as a direct copy cannot be made.

## VIRTUAL IMAGES

Another source of memory information that we can obtain comes from virtual images. Programs such as VMWare, Windows virtual PC and many others allow us to take a snapshot of the system. Sometimes we can run these directly, saving the captured virtual image and running it as a machine where we can interact and experiment. In addition files such as the ".vmem" file in VMWare contain information that we can extract with a tool such as Volatility.

When we take a virtualized machine image, the suspended file is not volatile at all. This file is a serialized memory image and Malware cannot hide in this environment. This gives an advantage to servers and workstations that run in a virtualized environment. These systems can be analyzed completely. In some instances they can be analyzed as the machine is still running.

## TO CONCLUDE...

In the next article, we will start analysing the image we have captured.

Memory is volatile evidence and as such needs to be acquired early in the process. Perhaps more critical is the difficulty associated with acquiring a memory image. As memory imaging is going to change in results every time we enact the procedure, but memory imaging is not robust. By its very nature, memory is fragile and if you attempt to access many areas of device memory you can crash the system. The results of this would be a complete destruction of all evidence. To ensure that this does not happen to you it is important to always practice using the tools you intend to image a live system with.

There are some ways to access system memory that are less volatile. These include hibernation files, page files and virtual machine images. When analyzing a system, always remember that you should collect as much evidence as you can in the time that is available. Also remember to document the process that you have followed and to practice this before imaging a live system.

If you walk into a forensic engagement and start by crashing the system very few people will take your evidence to be reliable. So remember...

Practice,
Practice,
Practice,

And when you're done doing that...

Practice some more…

## REFERENCES

[1] Wright, C. S. (2011). Criminal Specialization as a corollary of Rational Choice. Paper presented at the ICBIFE, HK, China.

[2] Wright, C. S. (2012). Territorial behaviour and the economics of botnets. Paper presented at the SECAU Perth, WA.

### About the Author

*Dr Craig Wright (Twitter: Dr_Craig_Wright) is a lecturer and researcher at Charles Sturt University and executive vice –president (strategy) of CSCSS (Centre for Strategic Cyberspace+ Security Science) with a focus on collaborating government bodies in securing cyber systems. With over 20 years of IT related experience, he is a sought-after public speaker both locally and internationally, training Australian and international government departments in Cyber Warfare and Cyber Defence, while also presenting his latest research findings at academic conferences. In addition to his security engagements Craig continues to author IT security related articles and books. Dr Wright holds the following industry certifications, GSE, CISSP, CISA, CISM, CCE, GCFA, GLEG, GREM and GSPA. He has numerous degrees in various fields including a Master's degree in Statistics, and a Master's Degree in Law specialising in International Commercial Law. Craig has just completed working on his second doctorate, a PhD on the Quantification of Information Systems Risk and is mad enough to be planning his third doctorate.*

# EXAMINING EXIF DATA IN DIGITAL PHOTOGRAPHS

**by Irv Schlanger MSIS, ACE, Security+ and Ruth Forese**

Digital photographs have become common as a source of evidence in forensic investigations. However, pixels alone do not tell the entire story – modern digital cameras also record Global Positioning Satellite (GPS) information as well as date and clock time into photographs using metadata known as EXIF tags. One of the main tasks of a forensic investigator is to extract useful evidence from a photograph and proving this information's authenticity. EXIF metadata in JPEG photographs can provide proof that a suspect was or was not at the scene of a crime. Because EXIF data can be altered by the very same software and techniques detailed below, law enforcement should take precautions and use established forensic practices when using metadata in investigations.

**What you will learn:**

- • How to extract EXIF data from JPEG photographs
- The basics of the EXIF standard and what kinds of information it stores
- The implications of using EXIF data in forensic investigations
- Invalidation or "Anti-forensics" of EXIF data

**What you should know:**

- Ability to transfer JPEG photographs from a camera to a computer
- Basic knowledge of image editing software
- Basic knowledge of how files are stored on a Windows System

Metadata is "data about data" and typically describes the data's contents such as its format or source. It can be used in both physical and electronic resources. In digital photography, it is the description of the millions of pixels the digital camera has captured. The time and location of the capture are a few elements of metadata. Investigators can take advantage of this valuable information to track down criminals. Historically, it has been successful in identifying and locating suspects in a number of investigations.

Metadata is hidden when a user views a photograph – it will only be displayed in a program that can extract it from the image file. We will examine four programs: *Opanda IEXIF*, *EXIFTool*, *GeoSetter,* and *EXIF PILOT,* which are powerful utilities capable of displaying and editing EXIF metadata in JPEG image files. These programs are useful as they allow the investigator to extract the hidden information from the photograph; however, these tools may be used by criminals with the intent of producing altered or misleading metadata evidence.

## THE EXIF STANDARD

Exchangeable image file format, or EXIF, is the current metadata standard for JPEG photographs and is used by almost every camera manufacturer. The standard defines how images are formatted and what kinds of information the file can store. The implementation of metadata standards such as EXIF allows software to more easily extract data from a photograph, since it is stored in a standardized way.

EXIF was first defined in 1995 by the Japan Electronic Industries Development Association. Version 2.3, the most recent version, was released in 2010 in a partnership with Camera & Imaging Products Association. The EXIF standard is most commonly associated with JPEG files but can also be used in other formats, such as TIFF (Tagged Image File Format) for uncompressed images and WAV (Waveform Audio Format) for audio.

EXIF data is located within the beginning segments of the JPEG image file. In a JPEG image, data not necessary to decode the picture itself is defined in sequences called Application Markers. The value that labels the beginning of EXIF data is placed into APP1, which is then followed by the EXIF data fields. A visual representation of the EXIF segment and their corresponding hex values is below, where the values are written in hexadecimal format. Marker 0xFFD8 defines the Start of Image Marker and is used to identify the image as a JPEG.

**Table 1.** *The basic layout of a JPEG file*

| SOI Marker | APP1 Marker | APP1 Data | Other Markers and Data |
|---|---|---|---|
| 0xFFD8 | 0xFFE1 | All EXIF data | Rest of image |

The EXIF tag structure uses the TIFF tag format, where each data field or descriptive tag is directly associated with a binary value. For example, EXIF tag number 0x0110 designates the camera model field while 0x0132 is used for date time. Tags are also defined by a data type. Some data types are:

- ASCII: ASCII character encoding, used for strings
- Rational: A fraction number
- Short: a smaller number, uses 2 bytes
- Long: a larger number, uses 4 bytes

The number of tags that a camera utilizes depends on its settings and capabilities. For instance, a camera without a GPS receiver, or with its location GPS setting disabled, will not enter GPS data. The EXIF standard also contains custom fields for camera manufactures to enter their own information. The following are just a few types of tags provided in the current EXIF standard:

- Camera settings such as focal length, exposure and aperture value
- Camera model, lens type and serial number
- The GPS coordinates and altitude
- Picture dimensions and orientation
- Thumbnail data
- Copyright information
- Author name and comments

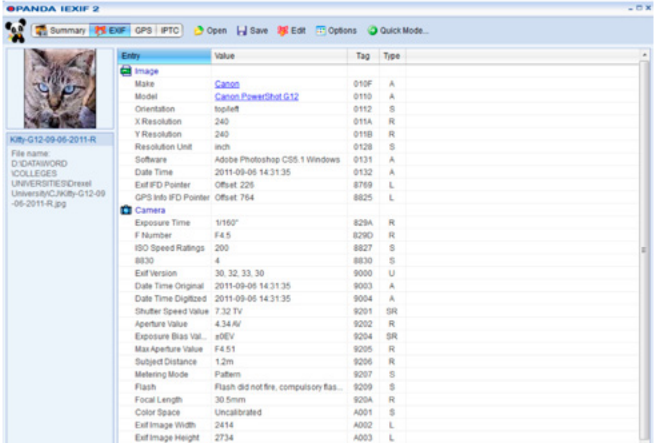
EXIF data fields share properties with other standards. EXIF data uses TIFF tag formatting in JPEG files to make it easier for data exchange between uncompressed and compressed formats. The IPTC (*International Press Telecommunications Council*) Information Interchange Model is another metadata standard, which shares some descriptive attributes with the EXIF standard such as GPS information. This standard can be implemented in JPEGs in addition to EXIF data.

## EXAMINING EXIF DATA USING SOFTWARE

EXIF data can be viewed by most modern image editing software. In the Windows operating system, Windows Explorer has its own EXIF viewer that runs when a user views an image's properties. Software editors may be able to erase or modify metadata. If the camera marked the wrong date and time, for instance, the photographer can correct the corresponding data value using these programs.

Some software is more specialized by having the sole purpose of managing EXIF data. These programs have more flexibility in editing the EXIF data and can analyze photographs that share common fields. A few programs also allow users to easily configure batch scripting to process many photographs once. Two of four programs evaluated: *EXIFTool*, and *GeoSetter* offer this kind of functionality.

Let's look at the features of; *Opanda IEXIF, EXIFTool*, *GeoSetter,* and *EXIF PILOT.*



Kitty-G12-09-06-2011-R
File name:
D:\DATA\WORD
\COLLEGES
UNIVERSITIES\Drexel
University\CJ\Kitty-G12-09
-06-2011-R.jpg

| Entry | Value | Tag | Type |
|---|---|---|---|
| Image | | | |
| Make | Canon | 010F | A |
| Model | Canon PowerShot G12 | 0110 | A |
| Orientation | top/left | 0112 | S |
| X Resolution | 240 | 011A | R |
| Y Resolution | 240 | 011B | R |
| Resolution Unit | inch | 0128 | S |
| Software | Adobe Photoshop CS5.1 Windows | 0131 | A |
| Date Time | 2011-09-06 14:31:35 | 0132 | A |
| Exif IFD Pointer | Offset: 226 | 8769 | L |
| GPS Info IFD Pointer | Offset: 764 | 8825 | L |
| Camera | | | |
| Exposure Time | 1/160" | 829A | R |
| F Number | F4.5 | 829D | R |
| ISO Speed Ratings | 200 | 8827 | S |
| 8830 | 4 | 8830 | S |
| Exif Version | 30, 32, 33, 30 | 9000 | U |
| Date Time Original | 2011-09-06 14:31:35 | 9003 | A |
| Date Time Digitized | 2011-09-06 14:31:35 | 9004 | A |
| Shutter Speed Value | 7.32 TV | 9201 | SR |
| Aperture Value | 4.34 AV | 9202 | R |
| Exposure Bias Val... | ±0EV | 9204 | SR |
| Max Aperture Value | F4.51 | 9205 | R |
| Subject Distance | 1.2m | 9206 | R |
| Metering Mode | Pattern | 9207 | S |
| Flash | Flash did not fire, compulsory flas... | 9209 | S |
| Focal Length | 30.5mm | 920A | R |
| Color Space | Uncalibrated | A001 | S |
| Exif Image Width | 2414 | A002 | L |
| Exif Image Height | 2734 | A003 | L |

**Figure 1A.** *An image's EXIF data displayed in Opanda IEXIF*

## PROGRAM 1: *OPANDA IEXIF*

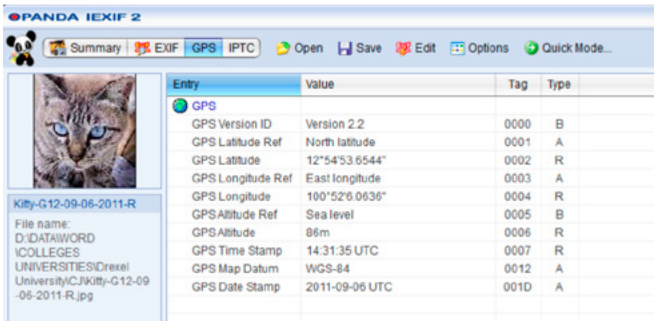
*Opanda IEXIF* is a free standalone utility that displays a picture's EXIF data in a user-friendly format. Its simple layout makes it suitable for both non-technical and technical users. Along with displaying EXIF data, it also provides convenient functions such as exporting metadata to XML format and an option to map GPS locations on Google Maps. The paid professional version, *Opanda PowerEXIF*, is more extensive and allows users to modify EXIF tags and implement batch processes for editing entire directories. Figure 1 below, is a screenshot of an image displayed in *Opanda IEXIF.*

Below is a description of the four columns;

- Entry: The data fields that contain entries
- Value: The value of each data field
- Tag: The hex value corresponding to each data field as defined in the standard
- Type: The type of data entered, such as ASCII (A), Long (L), Rational (R), and Short (S)

An image can be opened by clicking the "Open" icon or by dragging a file to the program window. The photo's metadata is then loaded and organized into four tabs. The "EXIF" category displays all of the EXIF information minus the GPS data, which has its own category. The "IPTC" category holds another set of metadata attributes defined by the International Press Telecommunications Council, and the "Summary" lists the more basic tags such as the date time and camera model.

Additional features are accessed by right clicking a data value. Metadata can be exported in multiple file formats for easy storage. Choosing "Locate Spot on Map by GPS" opens Google Maps within the user's default Web browser." The "Edit" button on the top toolbar is a professional version-only feature that enables the editing of data fields. Limited editing exists in the free version.

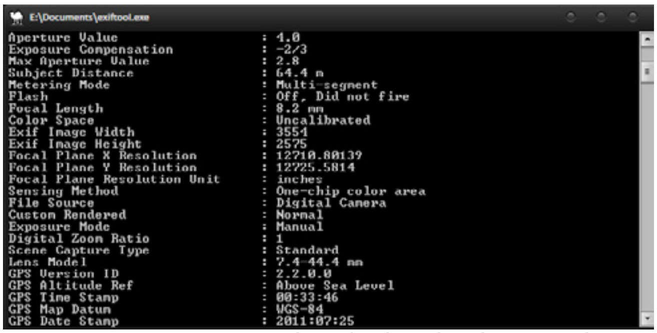


| Entry | Value | Tag | Type |
|---|---|---|---|
| GPS | | | |
| GPS Version ID | Version 2.2 | 0000 | B |
| GPS Latitude Ref | North latitude | 0001 | A |
| GPS Latitude | 12°54'53.6544" | 0002 | R |
| GPS Longitude Ref | East longitude | 0003 | A |
| GPS Longitude | 100°52'6.0636" | 0004 | R |
| GPS Altitude Ref | Sea level | 0005 | B |
| GPS Altitude | 86m | 0006 | R |
| GPS Time Stamp | 14:31:35 UTC | 0007 | R |
| GPS Map Datum | WGS-84 | 0012 | A |
| GPS Date Stamp | 2011-09-06 UTC | 001D | A |

Kitty-G12-09-06-2011-R

File name:
D:\DATA\WORD\COLLEGES UNIVERSITIES\Drexel University\CJ\Kitty-G12-09-06-2011-R.jpg

**Figure 1B.** *An image's EXIF GPS data displayed in Opanda IEXIF*



E:\Documents\exiftool.exe

```
Aperture Value                  : 4.0
Exposure Compensation           : -2/3
Max Aperture Value              : 2.8
Subject Distance                : 64.4 m
Metering Mode                   : Multi-segment
Flash                           : Off, Did not fire
Focal Length                    : 8.2 mm
Color Space                     : Uncalibrated
Exif Image Width                : 3554
Exif Image Height               : 2575
Focal Plane X Resolution        : 12710.80139
Focal Plane Y Resolution        : 12725.5814
Focal Plane Resolution Unit     : inches
Sensing Method                  : One-chip color area
File Source                     : Digital Camera
Custom Rendered                 : Normal
Exposure Mode                   : Manual
Digital Zoom Ratio              : 1
Scene Capture Type              : Standard
Lens Model                      : 7.4-44.4 mm
GPS Version ID                  : 2.2.0.0
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 00:33:46
GPS Map Datum                   : WGS-84
GPS Date Stamp                  : 2011:07:25
```

**Figure 2.** *An image's EXIF data displayed with EXIFTool using the Windows Command Prompt*

## PROGRAM 2: EXIFTOOL

*EXIFTool* is a command line application for viewing and modifying metadata. It provides a wide range of functionality, from editing, copying or extracting individual fields to processing tags for a folder containing numerous files, also referred to as batch processing. *EXIFToo*l is powerful compared to *Opanda IEXIF* but is better suited for technical users due to the complexity of the command line interface. However, user-friendly GUI programs that implement *EXIFTool's* interface are available online.

After downloading the executable, users can open a file by calling the *EXIFTool* command on an image or by dragging the file to the executable icon. If the latter is used, the `-k` parameter should be included to keep the command prompt open after execution. Below is a screenshot of an image's EXIF data in Windows Command Prompt. The original distribution was written in Perl, so it can also be installed on Linux systems for those familiar with the programming language (Figure 2).

To edit a tag, users must know the tag's name and format as defined in the EXIF standard. For example, "DateTimeOriginal" is the name of the photograph's original date and time tag listed in the format YYYY:MM:DD HH:MM:SS. A command to modify the date and time to arbitrary values would look something like the following example. The P argument is a helpful feature that preservers the file's modified date and time: `EXIFtool DateTimeOriginal="3000:02:20 12:13:14" -P fileName.jpg`.

**Table 2.** *Some sample EXIFTool Commands*

| Command | Function |
|---|---|
| `EXIFtool -b –DateTimeOriginal image.jpg > a.txt` | Extracts the date time of image.jpg in binary format and inserts it into a.txt |
| `EXIFtool -keyword= image.jpg` | Deletes all keywords from image.jpg |
| `EXIFtool -*GPS* image.jpg` | Output all fields with "GPS" in the name from image.jpg |

Users have complete control over an image's metadata with *EXIFTool*. Tags can be exported in different formats such as a PHP array and HTML for analysis, and sensitive files can be password protected. Relationships between files can also be displayed by using arguments like `-common`, which will list common information for a set of images in a directory. The simple `-r` argument recursively processes an associated command, allowing users to quickly modify hundreds of images at once. Additional examples of commands are listed: Table 2.

*EXIFTOOL* has the capability to work with a significantly greater number of file types when compared to other EXIF editing software.

## PROGRAM 3: *GEOSETTER*

*GeoSetter* takes advantage of *EXIFTool's* library by providing an interactive graphic user interface for setting GPS data. Like *Opanda IEXIF*, it uses Google Maps to track coordinates, displaying the map directly within the *GeoSetter* program window. As the name implies, *GeoSetter's* focus is on geo-tagging photographs, but it can also be used to view other EXIF data. Figure 3 and 4 below displays the main window with the Map and Image Info panels activated.

The Map panel provides a feature rich set of tools which are well suited for investigators looking to examine or compare multiple geo-tagged images. GPS data can be easily modified on a single file. Additionally, by dragging the existing purple marker on the map to a different location, or by setting a new marker and clicking the "Assign position marker to selected images" icon, *GeoSetter* will assign the new map marker coordinates to all of the selected images.

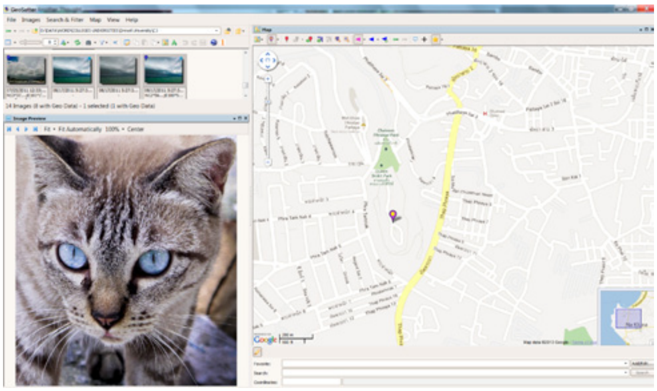


**Figure 3.** *A photograph with integrated map functionality displayed in GeoSetter*

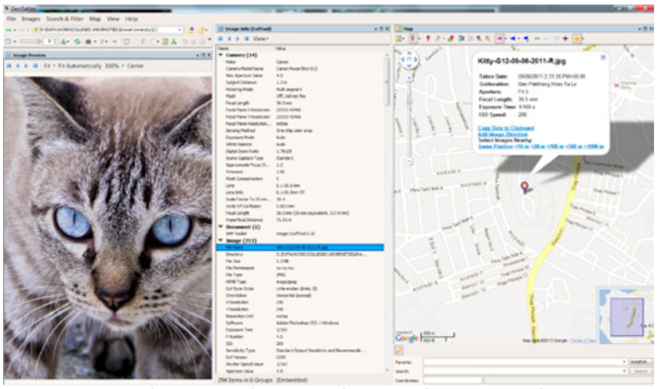


**Figure 4.** *A photograph's EXIF data and integrated map displayed in GeoSetter*

*GeoSetter's* panels can also be customized by dragging them, or removed entirely from the screen. For example, the user could disable the Map panel. This level of customization allows the program to be used as a simple EXIF viewer for those who do need all of the fields displayed.

An image's geographical data can also be modified by double clicking on its thumbnail in the explorer panel. A window appears that lets users manually input data or automatically find it online. Specifics such as time zones and contact information can also be added. These settings can then be used as a template for other images by clicking on "Save as Template" at the bottom of the window.

## PROGRAM 4: *EXIF PILOT*

*EXIF PILOT* utilizes an intuitive interface similar in design to Windows Explorer where the folder structure is on the left column, filenames and EXIF data is in the middle column, and a preview and edit options are in the rightmost column.

The four selectable categories of properties that can be edited are; File, EXIF, IPTC, and XMP, as shown in Figure 5.

*EXIF PILOT* allows the user to select one of the fields and click "Edit" at the bottom of the screen. This will open an edit dialog box specific to the field chosen where the user can change the value for the given field. See Figure 6.

Additionally, *EXIF PILOT* has robust import/export features. *EXIF PILOT* is capable of importing or exporting EXIF and IPTC data to or from the following file formats: XML, MS Excel, CSV, and the ability to create custom templates, see figure 7 below. The program's export features will save forensic investigators valuable time when generating reports that include information obtained during the forensic investigation. *EXIF PILOT* is a free program, and it has an available paid plugin which will enable batch processing of photographs.

*EXIF PILOT* also has the capability to work with a significantly greater number of file types when compared to other EXIF editing software.

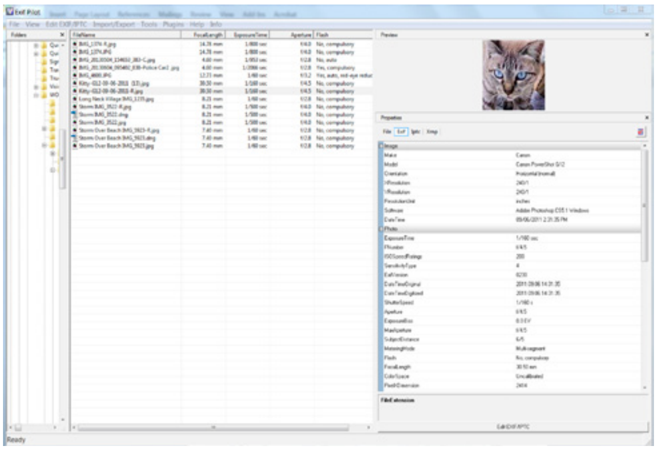


**Figure 5.** *EXIF PILOT's main screen*

## CASE STUDIES: USING EXIF DATA TO SOLVE CRIME

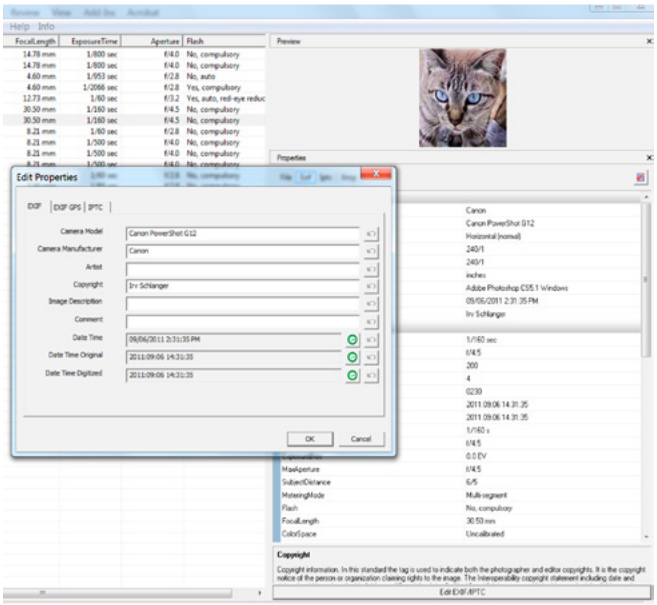
EXIF data can provide valuable information that might not be obtained by viewing a photograph by itself. Law enforcement could identify a person by examining metadata such as the author's name, GPS location or the camera's serial number. On a larger scale, analysts could process hundreds of images and discover relationships that reveal a criminal's entire lifestyle. The following cases are examples where law enforcement investigators have used EXIF data to their advantage:

### 2012, ARREST OF JOHN MCAFEE

EXIF data was used in the arrest of John McAfee, founder of computer security software company McAfee, Inc., when a journalist accidentally revealed his location by uploading a picture containing GPS coordinates to the Web (Cluley, 2012).

### 2012, ANONYMOUS HACKER CAUGHT BY FBI

Anonymous hacker Higinio Ochoa was detained shortly after uploading a picture of his girlfriend to the internet. The photograph's EXIF data exposed that he was using an iPhone in Melbourne, Australia, which helped the FBI to find his Facebook page and track him down (Schwartz, 2012).



Edit Properties

EXIF | EXIF GPS | IPTC

Camera Model: Canon PowerShot G12
Camera Manufacturer: Canon
Artist:
Copyright: Irv Schlanger
Image Description:
Comment:
Date Time: 09/06/2011 2:31:35 PM
Date Time Original: 2011:09:06 14:31:35
Date Time Digitized: 2011:09:06 14:31:35

**Figure 6.** *EXIF PILOT's "Edit Properties" dialog box for editing date and time*

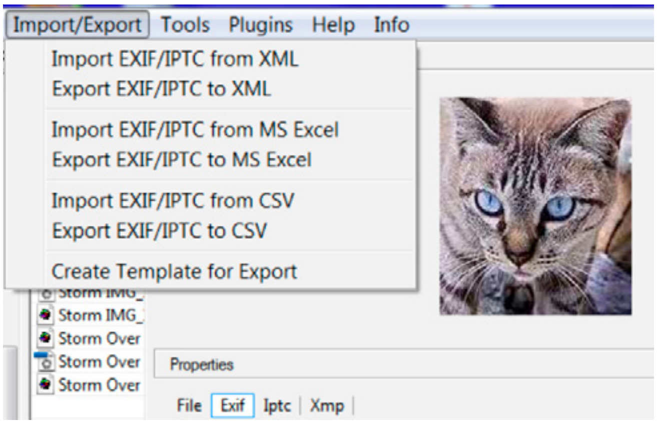


**Figure 7.** *EXIF PILOT's Import/Export drop-down menu*

### 2007, HARRY POTTER AND THE DEATHLY HALLOWS LEAK

The 7th book in the Harry Potter series was photographed and leaked online shortly before its release. Although the photograph's fate is uncertain, analysts were able to find the camera's serial number in the pictures' EXIF data. The serial number could potentially be used to identify the person who purchased the device (Schneier, 2007).

## EXIF DATA ANTI-FORENSICS

"Anti-forensics" refers to the countermeasures taken by an individual to thwart forensic analysis. Although EXIF data has been used successfully to arrest criminals, it could be rendered unreliable. Programs explored earlier: *Opanda EXIF*, *EXIFTool*, *GeoSetter*, and *EXIF PILOT* can replace the EXIF metadata with arbitrary information. A suspect could easily change the location and date time of an image in the hopes of misleading investigators. He or she can revert the modification date of the file, too, making it seem like the image was never edited. The `-P` preservation argument in *EXIFTool* is an example of such a method.

Metadata can also be removed by stripping it from the original JPEG or by saving a copy of the image in an editor. A function in Adobe Photoshop is the "Save for Web" option for saving photographs, which will automatically remove any EXIF data from the file. Another technique is adding a second photograph in a layer above the original, flattening the image and saving it, which associates the original EXIF data with the second image layered on top.

While the primary purpose of software programs such as Adobe Photoshop and *EXIFTool* is not metadata anti-forensics, scripts are available with that goal in mind. For example, a simple script written in the Python programming language randomizes data fields such as location, date, and time. A suspect would need to exercise caution when editing a photographs metadata. Time stamping a photograph, taken on a bright sunny beach, with a 1:00am value will certainly draw attention to the possibility of anti-forensics on the part of the suspect.

## OTHER PROBLEMS AFFECTING RELIABILITY

Metadata is not always accessible in photographs. Most social networking sites such as Facebook have recently begun to wipe EXIF data from their photographs for privacy and copyright reasons (Bailey, 2010). In this case, a forensic image containing the original photograph would have to be obtained from the suspect's computer using a valid chain of custody.

Problems concerning the reliability and availability of the EXIF metadata can occur before the photographs are transferred to a computer. EXIF data could be incorrect if the camera's clock is off, due to user error, travel, or clock drift. If the time zone is omitted, a correct time would be misleading. The camera may have been stolen or leant to a friend when the photograph in question was taken, EXIF metadata would not reveal these extenuating circumstances.

Additionally, problems may occur after photographs are transferred from the camera. Not all image editing programs are compatible with the latest EXIF standard, which may damage or corrupt the EXIF metadata upon saving.

Hashes are used by investigators to compare images and prove their authenticity. Hashing software, which creates a fixed-length string of characters for uniquely identifying a file, processes a file's data which includes its metadata. However, this does not include the date and time stamps which are properties on the disk, and not properties of the EXIF metadata. Hence, a file which was copied from a memory card to a computer disk drive would have the date and time that the file was copied, while the EXIF data within the file would remain the same. As such both the original file on the memory card and the copy on the computer's drive would produce the identical hash values despite looking as if they were created on two different dates. The identical hashes could create confusion during the investigation.

## INCREASING AN IMAGE'S RELIABILITY

To help ensure an image's authenticity, photographers can use digital signatures software directly on their cameras to mark their files as original. Digital signatures are a product of a mathematical function applied to a file and show that the file is in the expected format and from the expected sender. Higher end cameras from manufacturers like Nikon and Canon have their own processes for creating signatures. For instance, Canon's Original Data Security System uses a specialized smart card to verify a photograph's signature. The system confirms that it was taken with the camera and has not been altered. Researchers have discovered known vulnerabilities in the algorithms of several camera manufactures that reduce their dependability.

*Write Once Read Many* (WORM) SanDisk memory cards may be a more effective solution. As the name implies, stored data cannot be removed or altered but can be read multiple times. The cards can also only be written to with compatible firmware from companies such as Nikon and Fujifilm. The chance of altered metadata on a locked memory device such as a WORM card is very unlikely. WORM cards are usually no more expensive than a standard memory card, making them an affordable and easy option for securing photographs.

The proper chain of custody for handling evidence is also necessary to prevent the tampering or corruption of data under investigation. Utilizing well established guidelines for handling digital evidence, as well as maintaining the proper chain of custody, helps to ensure that the evidence will be admissible in court. Rules such as using NIST-certified or forensically-sound software, never working off of the original data, and recording actions taken during analysis are standard practices which will defend against the allegation of alteration.

It's important to maintain an established chain of custody for the evidence, as well as taking some extra precautions for sensitive digital media and equipment. For example, digital media is very sensitive to static-electric discharge and therefore needs to be placed in an antistatic bag. Additionally, digital media is sensitive to extreme temperatures – both hot and cold – which may occur when the media is transported or stored. For short durations, placing the media into a Styrofoam cooler is usually sufficient. However, if the media is going to be subject to extreme temperatures for an extended period of time, a temperature-controlled container will be necessary to prevent permanent damage to the evidence.

## CONCLUSION

If proper precautions and procedures are taken, EXIF data can be a valuable asset to forensic investigations. All metadata should be analyzed carefully and its authenticity should never be assumed. As the programs detailed above were able to illustrate, any part of an image's metadata can be altered to display whatever the user desires. These modifications require little technical knowledge and can be applied to any number of files using batch processes as well as other simple scripts.

For a photographer, implementing safeguards such as a WORM card or digital signature will increase an image's reliability. For an investigator, utilizing forensic best practices such as a write-blocking device will help prevent accidental data altering during an investigation. Digital evidence should always be processed on an image of the media, rather than on the original. A valid forensic chain of custody can establish the data's source back to a physical piece of evidence seized.

If a photograph appears to reveal crime, then EXIF data could be used as probable cause to obtain a search warrant or conducting further investigation such as the questioning of suspects. Each of the previously discussed investigations utilizing EXIF data employed these tactics. Image metadata – even though it is rarely seen – can play an essential role in an investigation when handled properly.

## WHAT EXIF DATA SOFTWARE IS BEST?

EXIF data software best suited for an investigator varies depending on his or her needs and resources. The four tools described above: *Opanda IEXIF, EXIFTool, GeoSetter* and *EXIF PILOT* can all process a photograph's metadata but possess slightly different features and capabilities:

- *Opanda IEXIF* is quick and easy-to-use; however, features such as processing of batch scripts are only available in the full version. *Opanda IEXIF* is well suited for the casual examination of a small number of files.
- *EXIFTool* is more technical and requires more time to learn but offers the largest variety of features. Tech-savvy professionals who need to analyze and compare many photographs will get the most use out of *EXIFTool*.
- *GeoSetter* is a free comprehensive EXIF viewer with a focus on geographical data. *GeoSetter* is an excellent tool. *GeoSetter's* capabilities match or exceed those found in other programs. *GeoSetter's* flexibility in configuration, ease of use, and built in map functions make it the clear choice for Law Enforcement Investigators. These features will help investigators quickly correlate the EXIF data present to a suspect or victim.
- *EXIF PILOT* is a simple program that gives investigators the ability to edit and export EXIF data with ease. *EXIF PILOT* is suitable for users who want to view EXIF data and edit fields on one or two photographs. However, like *Opanda IEXIF*, batch scripting is only available with the paid plugin. As mentioned earlier *EXIF PILOT* has the ability to process a larger number of file types compared to other software.

### About the Author

*Irv Schlanger is the President of Blackhole Cybersecurity LLC. His MSIS and BS degrees are from Drexel University in Philadelphia Pennsylvania. Additionally, he is an adjunct professor of Computer Crime and Information Warfare in the Criminal Justice Program at West Chester University located in West Chester Pennsylvania USA. His research interests are Information Warfare, Cyber Crime, Cyber Terrorism, and Computer Forensics. Ruth Forese is a Computer Science major and Technical Writing minor at West Chester University, she is currently part of the University's Information Assurance program. Outside of school she works as a web developer.*

## BIBLIOGRAPHY

- Bailey, J. (2010, April 22). Flickr and Facebook STILL Strip EXIF Data. Retrieved July 24, 2013, from Plagiarism Today: *http://www.plagiarismtoday.com/2010/04/22/flickr-and-facebook-still-strip-exif-data/*
- Cluley, G. (2012, December 3). Fugitive John McAfee's location revealed by photo meta-data screw-up. Retrieved July 9, 2013, from Naked Security: *http://nakedsecurity.sophos.com/2012/12/03/john-mcafee-location-exif/*
- ElcomSoft. (2010, November 30). CANON ORIGINAL DATA SECURITY SYSTEM VULNERABILITY. Retrieved July 6, 2013, from Elcomsoft: *http://www.elcomsoft.com/canon.html*
- Schneier, B. (2007, July 17). New Harry Potter Book Leaked on BitTorrent. Retrieved July 8, 2013, from Schneier on Security: *http://www.schneier.com/blog/archives/2007/07/new_harry_potte.html*
- Schwartz, M. J. (2012, April 16). Anonymous Hacker Girlfriend Pictures Revealed Much, Police Say. Retrieved July 8, 2013, from InformationWeek Security: *http://www.informationweek.com/security/government/anonymous-hacker-girlfriend-pictures-rev/232900329*
- Shah, A. (2010, June 23). SanDisk's SD card can store data for 100 years. Retrieved July 9, 2013, from Computerworld: *http://www.computerworld.com/s/article/9178428/SanDisk_s_SD_card_can_store_data_for_100_years*
- Tachibanaya, T. (1999, December 19). Description of Exif file format. Retrieved July 6, 2013, from Personal Information Architecture Research: *http://www.media.mit.edu/pia/Research/deepview/exif.html*

## REFERENCES

- EXIF standard version 2.3, *http://www.cipa.jp/english/hyoujunka/kikaku/pdf/DC-008-2010_E.pdf*
- Opanda IEXIF homepage, *http://opanda.com/en/iEXIF/*
- EXIFTool homepage, *http://www.sno.phy.queensu.ca/~phil/EXIFtool/*
- GeoSetter homepage, *http://www.geosetter.de/en/*
- EXIF Pilot homepage, *http://exifpilot.com*
- SpoofEXIF script blog post, *http://integriography.wordpress.com/2012/11/11/photograph-anti-forensics/*

# DIGITAL FORENSICS ON CLOUD STORAGE

**by Richard Leitz**

Digital Forensics experts in both law enforcement, and the corporate arena, have typically had either complete physical access to digital media, or live access to running servers, or the other computers that required examination. Due to the move from local storage of data and servers, to cloud based storage and services, the world of digital forensics has changed. This article will discuss how cloud based technology is making it more difficult for the digital forensics expert to gain access, and to examine digital media, that is stored on a cloud server in either the same country, or even worse, a different country.

**What you will learn:**

- Different Cloud Storage systems
- Problems with accessing forensic data in the cloud
- Problems with forensic software in the cloud
- Analysis of evidence

**What you should know:**

- Basics of Digital Forensics
- Basics of Cloud Storage

Forensics has been forced to evolve rapidly on a yearly basis, with new technology in the computer and network industry emerging rapidly. This article will review four different types of cloud computer resources, how these resources are used by the good and the bad, and how current digital forensic technology and techniques attempts to gain access to digital evidence that will withstand challenges in a court of law. Due to the diverse legal systems around the world, the basis of this article will rely on the US court system, with some references to investigations in the UK, Australia and South Korea. You should consider the four major types of cloud services available, to better understand the difficulties involved with accessing the digital data in the cloud.

## CLOUD SERVICE MODELS

Cloud computer services are currently broken into at least 10 types of services. However, the following four platform types, Iaas (infrastructure as a service), SaaS (software as a service) STaaS (Storage as a Service) and PaaS (platform as a Service) will be reviewed and discussed in this article. IaaS is a service where the “customer rents the hardware (processing time and speed, memory allocations, disk based storage, etc.) (Martini & Choo, p. 2), infrastructure on a subscription or pay-per-use model, and the services can be scaled upon demand (M. Taylor, Haggerty, Gresty, & Hegarty, 2010, p. 304). Using this feature in a Virtual environment allows IaaS to create a hardware platform based on any configuration the client requires. This type of environment is beneficial when trying to retrieve a forensic image. Examples of these would be Amazons Web Services, and Microsoft Windows Azure.

SaaS is "where the customers rents the software for use on a subscription or pay-per-use model (M. Taylor et al., 2010). Typical types of SaaS environments are email hosting, enterprise resource management, and human resource platforms. Examples of these would be Microsoft Office 365 and Google Docs. STaaS is probably one of most popular types of cloud based services that will be used for the perpetration of a computer crime. This is because of free or low cost access to file storage in the cloud. Examples of this are DropBox, Google Drive, Microsoft SkyDrive and Apple iCloud. The final service is PaaS where a "customer rents a development environment for application developers" (M. Taylor et al., 2010, p. 304). Force.com is a PaaS environment as well as "Wavemaker which is a visual development studio based on Java and hosted on Amazon EC2" (Keene, 2009, para. 6). The common theme amongst all of the cloud services is that they are not easily accessible, this is atypical from when a computer crime, or a corporate computer investigation is being performed. In the cloud environment the question now becomes how can current digital forensic technology be executed in a cloud platform, and what challenges the digital forensic investigator will have to resolve.

## CLOUD BASED DIGITAL EVIDENCE ACQUISITION

Current forensic work in the US is based on the National Institute of Standards and Technology (NIST) framework which consists of the following 4 phases:

- Identification of relevant data, collecting the data, and preserving its integrity.
- Use of automated or manual tools to extract data of interest while ensuring preservation.
- Analysis is concerned with deriving useful information from the examination.
- Creating a report to present the forensic analysis" (Martini & Choo, p. 3).

The problems with this 4 step process, in regards to a cloud environment, are that steps 1 and 2 are insufficient. This is based upon a quote in the journal "Digital Forensic Investigation of Cloud Storage Services" where the authors quote Barrett as saying that "conventional digital forensic methods are insufficient for investigating cloud storage services" (Chung, Park, Lee, & Kang, p. 2). Many of today's cloud based services are either browser based, or work from an application that can be run on a computer, smart phone – iPhone, Android, BB & Windows Phone- or even a tablet like the iPad or Android. This leaves the investigator with initially collecting data from the local device, and upon examination of the device, if it is found that a cloud based service was being used, then the preservation of evidence from the source should be gathered as soon as possible (Martini & Choo, p. 4). The 2nd part is how the digital data is stored in the cloud, is the cloud environment accessible in the same legal jurisdiction, and how the digital evidence can be retrieved in a way that will comply with jurisdictional legal standards for proper digital preservation. The first problems related to gaining access to cloud based data, is first trying to determine where in the world – literally – the data is located. A problem with the data center being located in another country is "where privacy laws are not readily enforced or non-existent. It could therefore potentially be difficult to establish a chain of custody for such data" (M. Taylor et al., 2010, p. 304). An additional problem with data being stored on a foreign server is that "the legal process to gain access to a public cloud computing system is more complex, and could delay investigations where the recovery of evidence is typically time critical" (M. Taylor et al., 2010, p. 305). A 3rd problem is "data in a cloud storage environment is often distributed physically within data centers" (Martini & Choo, p. 4). Upon finding that critical time sensitive data is being held in a cloud based data center, the next steps are how to properly gather the data.

Data acquisition can be performed in multiple ways based on the Cloud based service, and where the best access to the data is available. Dykstra and Sherman based their acquisition on a six layer cumulative trust system. The six layers are as follows: Table 1.

Current digital forensics investigations are performed by either a forensic image of a system, or a

**Table 1.** *Six layer cumulative trust system (Dykstra & Sherman, 2012, p. S93)*

| Layer | Cloud Layer | Acquisition method | Trust Required |
|---|---|---|---|
| 6 | Guess Application/data | Depends on data | Guest OS, hypervisor, host OS, hardware, network |
| 5 | Guest OS | Remote forensic app | Guest OS, hypervisor, host OS, hardware, network |
| 4 | Virtualization | Introspection | Hypervisor, host OS, hardware, network |
| 3 | Host OS | Access virtual disk | Host OS, Hardware, network |
| 2 | Physical Hardware | Access Physical disk | Hardware, network |
| 1 | Network | Packet Capture | Network |

live acquisition with tools like Encase or FTK Imager. In some cases, depending on where the data is stored, it is possible to "use EnCase servlets or FTK agents by remotely installing them in the cloud" (Dykstra & Sherman, 2012, p. s94). This process was tested by Dykstra and Sherman, in a test on a virtual machine (VM) residing on Amazons EC2. Their process consisted of creating a VM, and then using the Amazons management console to open up the necessary ports to deploy the EnCase servlets and FTK agent. Additionally, they tested three different programs to acquire images from the system memory of the VM. Their experiment was successful; however, I doubt if this process would have been so smooth if they were trying to acquire data in a typical digital forensic investigation, as opposed to controlled conditions. Even though their tests ran fine, when they compared the results with a local system that was a duplicate of what resided on Amazon, they found a potential legal problem. "Amazon does not provide checksums of volumes as they exist in their cloud, so it isn't possible to verify the integrity of the forensic disk image" (Dykstra & Sherman, 2012, p. S94). This leaves the legal authorities with a potential legal problem; this, based on the lack of validation for the disk images (Dykstra & Sherman, 2012, p. S97). An additional problem is the ability to trust that the Amazon management console was not accessed, and the VM image was not tampered with in any way. If there are no logs being recorded for access to the VM image, then there is no proof of when, or who accessed the image. While the remote access tests performed well for Dykstra and Sherman, they do not recommend using EnCase and FTK remote programs. This is because of the amount of trust that is required when used in the cloud environment. Additionally, these "remote programs will not work in other cloud environments like Microsoft Azure or Google AppEngine" (Dykstra & Sherman, 2012, p. S97).

Other ways to gather digital data from virtual machines for forensic examination is requesting the cloud provider export a copy of the VM in a snapshot; which will give access to the hard drive and memory. Some cloud services do not use a VM environment, so they may only be able to produce a "binary export of the data stored on the hosted software environment" (Martini & Choo, p. 5). There are potentially other problems for the cloud service providers' and their clients', when a forensic investigation is being performed.

"When digital evidence is required from a public cloud computing system, there is also the issue of continuity of service for the other users on the cloud. Ideally, a computer forensic investigation should not impact upon other cloud service users who are not the target of the investigation" (M. Taylor et al., 2010, p. 306). This exact problem occurred in January, 2012 when the owner of Megaupload, Kim Dotcom, was arrested and his file sharing site was taken down by authorities in the US. By taking down Megaupload, many legitimate paid users of the site, lost all access to their data, and the ability to download and move the data before it would be deleted. With all of the difficulties that the forensic investigator is dealing with in gaining legal access to the data, they still can have additional problems related to use of encryption.

Security researchers proposed using local encryption before uploading the data to the cloud, thereby securing the end-users data. (Mark Taylor, Haggerty, Gresty, & Lamb, 2011, p. 7). An additional concept proposed is to use digital secure authentication for access to the cloud data. This can actually be a benefit to the forensic investigator; by using public-private encryption certificates to authenticate the end user, it will provide more proof that they were accessing the data. The journal article "Digital Forensic Investigation of Cloud Storage Services" by Chung, Park, Lee and Kang, performed a very thorough forensic evaluation of four popular cloud based services (Amazon S3, Dropbox, Evernote and Google Docs).

Their examination looked for any artifacts that would have been left over when accessing the four services. They accessed all four services, from four of the most popular platforms (Windows, Macintosh, Iphone and Android phone). On the Windows system, they used either Internet Explorer, or an application supplied by the vendor. They found "traces of the application are left in the registry and log files & database files. The Mac had similar results except for the registry" (Chung et al., p. 5). When they investigated for artifacts on the Iphone and Android phone, a common theme was that Dropbox, Evernote, and Amazon S3, both phones and both the Mac and Windows systems, had files from SQLite database. This would make it easy for an investigator, who is familiar with SQLite, to gather important files from any of the devices for examination. This perhaps re-focuses on software vendors, who falls short of providing proper security. At the time of the article, the authors were able to copy data from a Windows system to another system, and gain access to the DropBox account. I believe the 2 factor authentication by DropBox, will make similar access impossible or very difficult.

Even in situations where a web browser was used, the authors were able to recover artifacts through the use of EnCase. After data collection, the analysis of the evidence is conducted.

## ANALYSIS OF EVIDENCE

Some of the concerns with retrieving data from the cloud vs. the "traditional media are that documents and files will typically have Meta data preserved from its original source. This may not be the case in cloud computing systems" (M. Taylor et al., 2010, p. 307). An investigator will have to hope that Meta data was in file before it was uploaded to the cloud, and will be available as evidence. Unlike a traditional media, which may have only one user, in a cloud environment, user identification can be questionable without a solid audit trail. Even if the data was retrieved and analyzed, there is always the possibility to show, without reasonable doubt, who had access and/or modified the digital evidence. An additional problem exists if the "evidence had any malicious software included in it then the ability to track down the effects from the malware upon data or programs stored in the cloud could be very complex" (M. Taylor et al., 2010, p. 307). Such a situation also makes it difficult to prove if the accused is guilty, due to the difficulty in obtaining digital evidence (M. Taylor et al., 2010, p. 307) to prove what they were, or were not, aware of. The analysis of the evidence may also require conversions from its current form; from which it was either downloaded, or given to the investigator by the cloud service provider. This can be a problem because some cloud environments, and mobile devices, may require the forensic application vendors to adapt, or create, new software that help extract the data into a common format for analysis. The many different scenarios that I have reviewed, have made it difficult to determine a solid conclusion on what needs to be done next in digital forensics industry.

## CONCLUSION

Concerns that I have for performing a digital forensic investigation in the cloud are based on the following. First, more logging and auditing for forensic discovery and analysis needs to be implemented by Cloud service providers. This is necessary to help reduce the "difficulty in analyzing the sequence of events in a particular transaction in a cloud system; this, since a variety of different machines might have been involved in the transaction" (Mark Taylor et al., 2011, p. 7). Second, there is a requirement for a standardization, and better forensic software written, to assist in extracting cloud data (Mark Taylor et al., 2011, p. 7). Third, because of the newer models of storing data in the cloud, there needs to be either a new creation, or an adaption of the current evidence based framework methodologies (Martini & Choo, p. 8). Adapted to one that is designed to work on the "various cloud platforms that would better enable forensic investigators to identify, preserve, collect, examine and analyze data in the cloud computing environment" (Martini & Choo, p. 8). Lastly, a forensic investigator must be well prepared to prove the integrity of their work; this, through the process of taking pictures, or video recording, of the equipment under investigation, the office environment, and output of the monitor screen (ChaeHo, Sung-Ho, & Kwang Sik, 2012, p. 86). This substantiates what processes were performed to both extract the digital evidence, as well as the process that was used, to capture the facts in the case.

My concerns are that law enforcement is at the disadvantage when it comes to performing digital forensics on the cloud environment. I say this because, it is so easy for a criminal to either commit a crime against a cloud based service or use a cloud service for storing of their data. A criminal only needs to encrypt their data on a local system that is using an encrypted hard drive, while using a browser in its secure or incognito mode, to reduce the evidence trail. Digital criminals can use a cloud service that is based in a country which isn't willing to deal with the legal system in their country. At this point and time, the advantage goes to the bad guys, while the good guys are playing catch up – *again!*

## REFERENCES

- ChaeHo, C., SungHo, C., & Kwang Sik, C. (2012). Cyber Forensic for Hadoop based Cloud System. International Journal of Security & Its Applications, 6(3), 83-89.
- Chung, H., Park, J., Lee, S., & Kang, C. Digital forensic investigation of cloud storage services. Digital Investigation(0). doi: 10.1016/j.diin.2012.05.015
- Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, Supplement(0), S90-S98. doi: 10.1016/j.diin.2012.05.001
- Keene, C. (2009, 3/26/2009). What Is Platform as a Service (PaaS)? Retrieved 11/11, 2012, from *http://cloud.dzone.com/articles/what-platform-service-paas*
- Martini, B., & Choo, K.-K. R. An integrated conceptual digital forensic framework for cloud computing. Digital Investigation(0). doi: 10.1016/j.diin.2012.07.001
- Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer Law &amp; Security Review, 26(3), 304-308. doi: 10.1016/j.clsr.2010.03.002
- Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. Network Security, 2011(3), 4-10. doi: 10.1016/s1353-4858(11)70024-1

### About the Author

*Richard Leitz is a security engineer with 20+ years of computer, network and security experience who works for the US Army. He has his Masters in Information Assurance and has acquired the GCSEC, MCSE, CCNA, Network+ and A+ certifications. He is currently finishing his MBA and studying for the CISSP and CEH certifications. He has previously taught computers classes in a local high school as well as managed a number of small businesses. He enjoys traveling and playing golf. He can be reached via Linked In @ http://www.linkedin.com/pub/richard-c-leitz-jr/1a/249/238/ or Rcleitz@gmail.com.*

# DETECT AND PREVENT FILE TAMPERING IN MULTIMEDIA FILES

## A STEP BY STEP GUIDE USING FREE AND OPEN-SOURCE SOFTWARE

**by Doug Carner, CPP/CHS-III**

Electronic files are vulnerable to tampering and corruption. Undetected, these changes can alter the meaning and value of critical evidence. By implementing a few simple steps, you can ensure that everyone is working from the exact same set of facts, and be able to prove if a file was altered prior to arriving into your care.

**What you will learn:**

- Version control through hash tag signatures
- How to access, interpret and alter video metadata
- Tamper detection using Video Error Level Analysis
- Using a hex editor to authenticate a file
- Using playback software to determine a file's origin
- Methods to embed or extract hidden parasite file data

**What you should know:**

- Familiarity with computer audio, video and image files
- Familiarity with installing PC based software from a website

In your professional career, you are called upon to sort through a wide array of electronic file evidence, including discovery material originating from external sources beyond your control. These files are typically shared by disc or download using the honor system. If any file becomes accidentally or willfully corrupted, the altered version could go unnoticed. From there, the incorrect version could be shared with attorneys, the courts, clients, and various experts.

If the modification creates a new perceived reality, or an attempted falsity, such unwitting modification could compromise the entire case. If the modification inserts illegal content, you could become an unwitting distributor. Even if the only change is an unintentional reduction in quality, it can leave evidence open to interpretation. Such changes can be difficult or impossible to detect through a visual inspection. Fortunately, even a single bit change within a large file can be detected through a few simple software tools.

## AUTHENTICATION

It can be challenging to trace changes to their source due to the number of people that have access to a given file. Achieving version control requires the ability to detect file modifications, even when they occur prior to your involvement. With this capability, recipients can determine if any files were altered prior to receipt. Although a full authentication analysis requires years of experience and sophisticated software, some basic tests can be quickly performed using free software and minimal guidance.

## HASH TAGS

Upon receipt or creation of a file, you can quantify the current file version in a manner that can be replicated by others, so as to ensure that they are working with a file indistinguishable in every way from the version that you have. This is accomplished by calculating a unique identifying value for each file, and then providing a means for all other file recipients to do the same, so these values can be matched as proof of file authenticity.

A Hash tag is an electronic identifier constructed solely from the file's contents and structure. The most common Hash tag is the 5th generation of the Message Digest algorithm, commonly known as MD5. There are dozens of free programs to calculate MD5 values and, regardless of the program used, the resulting MD5 value will always match for exact copies of the same file.

Two easy-to-use free MD5 programs are Digestit (*http://colonywest.us/digestit*) and Checksum (*http://corz.org/windows/software/checksum*). They support left click or drag-n-drop, and require less time to process than reading this paragraph. Other offerings, like Microsoft's™ File Checksum Integrity Verifier (*www.microsoft.com/en-us/download/details.aspx?id=11533*) are also free, but can be cumbersome to use.

As soon as you receive or generate an original electronic file or folder, use your preferred hash tag program to calculate its MD5 value (see Figure 1). You can then include a list of all the relevant MD5 values anytime you share those files. This list should be shared as read-only, and you can even create a hash tag for the file listing the other Hash tags.

At any time, a file recipient can generate their own list of MD5 values and, if they match, be reasonably confident that their file versions are identical and indistinguishable from the file versions under your control. Any changes, even the simple act of opening and resaving a file without any content changes, will alter the calculated MD5 value. Copying, downloading and sharing a file will not alter a files metadata or MD5 value. Best of all, MD5 values work on media files, presentations, documents, DVDs, ZIP files and anything else that can be shared electronically.

MD5 hash tagging is the easiest method to provide version control of all your electronic files. The MD5 Hash tag is so unique that you have significantly better odds of winning the Powerball lottery four times in a row, than altering a file to achieve the same MD5 value. However, because the MD5 algorithm is open-source, it has been reverse engineered and compromised under very controlled conditions. Although there are newer algorithms (example: MD6), MD5 remain the premiere balance of security and popular cross-platform support.

## AUDIO AUTHENTICATION

Audacity and Audition are extremely common audio editing programs. Each program allows the user to isolate a given frequency for deeper analysis. Editing may be detected as disruptions in the cyclical pulse of a given frequency, shifts in the bit rate (see Figure 2), or shifts in the DC component of that signal. All of these tests require specialized training to interpret the significance of such anomalies.

One solution is to open the file using any application that has a Spectrographic view, and then zoom in on areas of concern in search of data anomalies. If something looks suspicious, you will have cause for reaching out to a qualified expert.

## IMAGE AUTHENTICATION

Most image viewing programs include a "Properties" or "Info" menu option to display a picture's metadata. For images in the JPG format, additional metadata fields can be viewed using JpegSnoop (*http://sourceforge.net/projects/jpegsnoop*). JpegSnoop provides detailed information beyond the scope of this article (example: quantization tables) that requires training to interpret. However, JpegSnoop ends the report with summary information, including an interpretation if tampering is suspected (see Figure 3).

This is especially important since JPG images are quite prone to tampering. It should also be not-

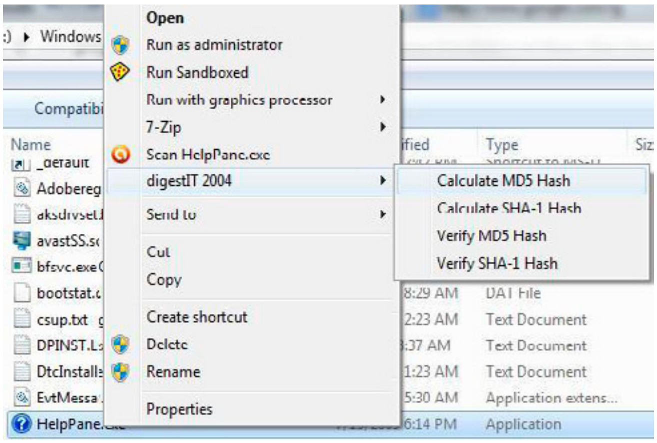


**Figure 1.** *Left click to calculate a file's MD5*

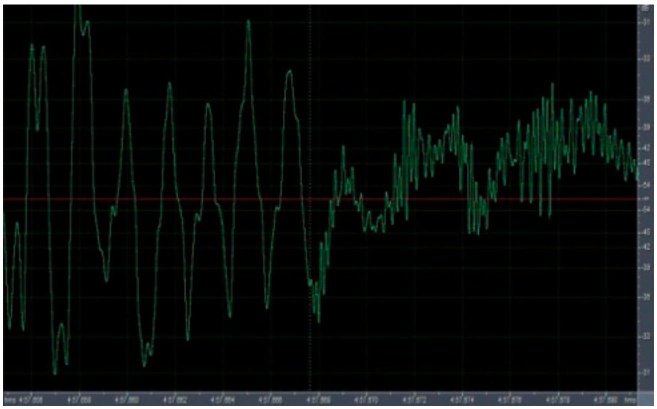


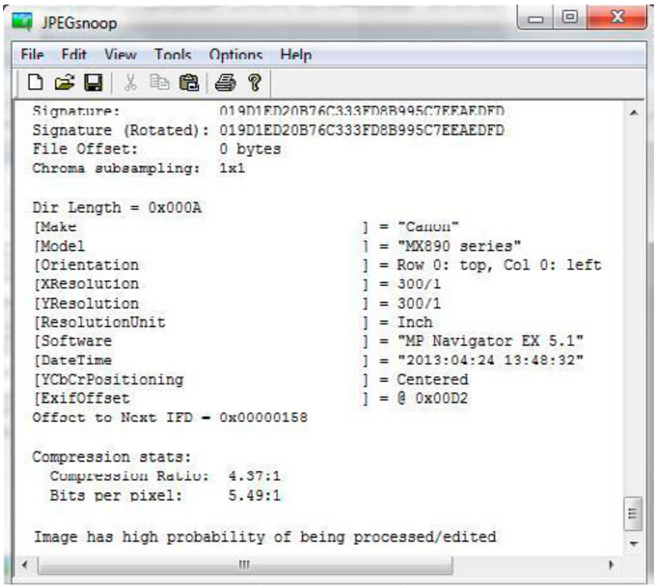
**Figure 2.** *Sudden increase in audio bit rate*

ed that free open-source software, like Analogexis (*http://analogexif.sourceforge.net*), can untraceably alter every metadata field of JPG and TIFF images (see Figure 4). Similar programs exist for other image formats, including a few raw and proprietary file types.

Often times you can compare a file's metadata and/or header values to published tables (example: a Google search) to determine if that information matches the expected information for that file type. By comparing the file's header and/or metadata to known facts, you can quickly separate fact from fiction.

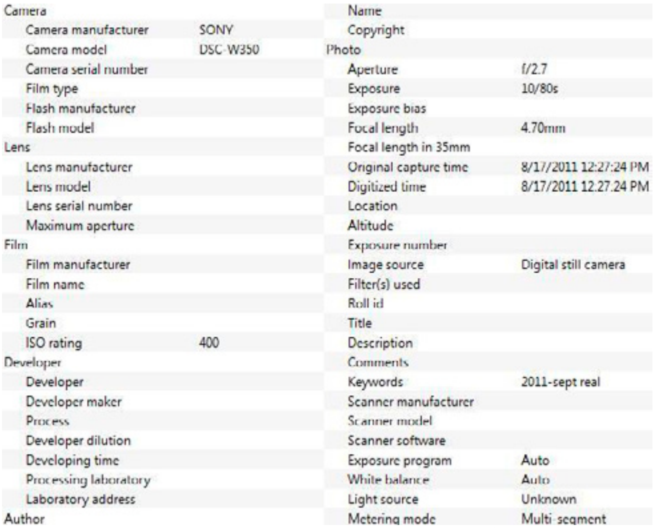
## VIDEO AUTHENTICATION

Compression and decompression (CoDec) instructions guide a computer on how to store and reconstruct a compacted video. Modern video CoDecs conserve considerable file space by suppressing high-frequency data and merging color details in ways that are designed to be minimally perceptive to the human eye. Because these changes are lossy, they result in quantization data errors.



```
Signature:              019D1ED20B76C333FD8B995C7EEAEDFD
Signature (Rotated):    019D1ED20B76C333FD8B995C7EEAEDFD
File Offset:            0 bytes
Chroma subsampling:     1x1

Dir Length = 0x000A
 [Make                             ] = "Canon"
 [Model                            ] = "MX890 series"
 [Orientation                      ] = Row 0: top, Col 0: left
 [XResolution                      ] = 300/1
 [YResolution                      ] = 300/1
 [ResolutionUnit                   ] = Inch
 [Software                         ] = "MP Navigator EX 5.1"
 [DateTime                         ] = "2013:04:24 13:48:32"
 [YCbCrPositioning                 ] = Centered
 [ExifOffset                       ] = @ 0x00D2
Offset to Next IFD = 0x00000158

Compression stats:
  Compression Ratio:  4.37:1
  Bits per pixel:     5.49:1

 Image has high probability of being processed/edited
```

**Figure 3.** *JpegSnoop's detection results report*



| | | | |
|---|---|---|---|
| Camera | | Name | |
| Camera manufacturer | SONY | Copyright | |
| Camera model | DSC-W350 | Photo | |
| Camera serial number | | Aperture | f/2.7 |
| Film type | | Exposure | 10/80s |
| Flash manufacturer | | Exposure bias | |
| Flash model | | Focal length | 4.70mm |
| Lens | | Focal length in 35mm | |
| Lens manufacturer | | Original capture time | 8/17/2011 12:27:24 PM |
| Lens model | | Digitized time | 8/17/2011 12.27.24 PM |
| Lens serial number | | Location | |
| Maximum aperture | | Altitude | |
| Film | | Exposure number | |
| Film manufacturer | | Image source | Digital still camera |
| Film name | | Filter(s) used | |
| Alias | | Roll id | |
| Grain | | Title | |
| ISO rating | 400 | Description | |
| Developer | | Comments | |
| Developer | | Keywords | 2011-sept real |
| Developer maker | | Scanner manufacturer | |
| Process | | Scanner model | |
| Developer dilution | | Scanner software | |
| Developing time | | Exposure program | Auto |
| Processing laboratory | | White balance | Auto |
| Laboratory address | | Light source | Unknown |
| Author | | Metering mode | Multi-segment |

**Figure 4.** *Analogexis can alter any Metadata field*

Each successive resave further deviates the video from the original version, but by decreasing amounts. If an object is added to, or relocated within, an already compressed video, it will be at the earlier stages of this process. When an altered video is resaved into a lossy format, the recent viewable manipulations will incur greater quantization changes than the remainder of the video content.

If you recompress a received video file, and then subtract that version from the file you received, the resulting video will only display the data errors between those versions. The resulting brightness directly relates the intensity of the data errors, with areas of greater contrast undergoing the greatest changes and resulting in greater brightness. If any pixels are disproportionally bright compared to other areas of comparable contrast, then those pixel locations denote suspected areas of tampering on the originally received video.

This test is called Video Error Level Analysis (VELA). VELA can be performed on any video using several video editing programs, including the popular open source VirtualDub program. VELA is based upon the concept of Error Level Analysis (*http://fotoforensics.com/*) which is used to authenticate single images. VELA's advantage is that it exploits the motion vectors that are absent in single images. Step-by-step instructions and a guide to interpreting the results can be found at the author's website (*http://ForensicProtection.com/VELA.html*).

## DUBBED VIDEO TEST

Open any video with software that allows the user to advance frame-by-frame, and advance through the first fifty continuous frames that show objects or people in motion. If the frame numbers advance, but the viewed scene ever remains unchanged, then that video includes duplicate identical frames.

VLC (*http://sourceforge.net/projects/vlc*) is a popular open-source video player that can decode most formats without requiring the installation of other software. Once a video has been opened and paused in VLC, the "e" button on the computer keyboard will advance the video one frame at a time, making it easy to perform the dubbed video test.

Duplicate frames are a strong indicator that the video was recorded from a slower playing version. This is common for video DVD files which play at 29.97 frames per second for countries following the NTSC standard, like the USA. Duplicate frames almost always indicate that you do not have an accurate copy of the original recording.

## REMOTE SCREEN CAPTURE VIDEO TEST

The more recent video CoDecs are based upon the h.264 standard which segments a video into a mosaic of small squares called “slices”, typically only eight pixels (screen dots) wide and eight pixels tall. It is common for DVRs to skip slices during remote playback when the internet connection cannot keep up with the video’s natural-speed playback data rate.

Using the software from the “Dubbed video test”, if frame-by-frame playback depicts any frames with slices that are abnormally bright or dark for just that one frame, then the file likely originated from remote viewing capture software.

### LOCAL SCREEN CAPTURE – CONVERSION VIDEO TEST

On-screen information is the last thing added to a video before it is saved onto, or played back by, a recording device. Use frame-by-frame playback to see if any video frame shows two different video frames or time stamps blended together. For example, a sequenced video is when one video input receives its signal from a cycling list of camera feeds.

If the video was converted at the incorrect speed (example: conversion software) or captured at a speed different than the video card’s refresh rate (example: screen capturing software) the resulting video can create blended frames (see Figure 5). The resulting video is an inaccurate and lower quality representation of the original recording.

## HIDDEN DATA

Every file has hidden data, even if the only purpose of the data is to denote the type of file it is or how it is to be played. Mining the hidden data can provide tremendous insight into the file’s true origin and authenticity.

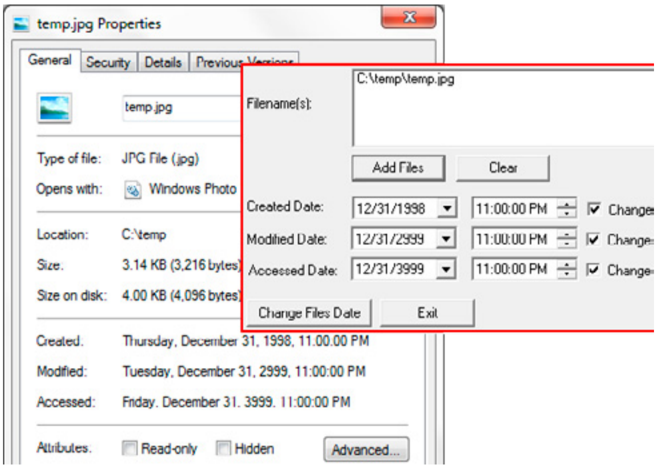
### METADATA

It is well known that a computer’s operating system can display a file’s last Modified, last Accessed and first Created dates, collectively known as the MAC dates. In Windows, this information is accessed by right clicking on a file, and then left clicking on the Properties option. However, MAC information is saved by the computer’s operating system and can become inaccurate from several causes including user error, virus, file transfer or free programs (see Figure 6) like FileDateCH (*http://www.nirsoft.net/utils/filedatech.html*). A more reliable date source is reading the metadata located within the target file.

Some metadata can be read with the tools you already have. For example, with Windows you can right click on the file, left click on Properties, and then left click on the Details tab. You may also be able to access certain metadata by simply choosing the Properties option located under the File menu of whatever software you are using to open the file.In the case of a media file, MediaInfo (*http://sourceforge.net/projects/mediainfo*) lets you review every metadata field of most audio and video files, even the hidden fields. If these details deviate from the known facts of the case, they become a strong indication of file tampering.

It is increasingly common for file metadata to include the *Global Positioning System* (GPS) coordinates denoting the actual location where the recording was created. You can enter these GPS values directly into a Google™ search box to translate them into an approximate street address. If the metadata includes a field labeled as “@xyz” these are the GPS coordinates in decimal format. The third GPS coordinate, the “z” value, is the above sea level altitude denoted in meters.

Depending on the GPS reception and capabilities of the recording unit, the GPS coordinates can pinpoint a specific room of a high-rise building. This accuracy results from advances in GPS technology that incorporates data from satellites and cell phone towers (aka Enhanced GPS). GPS data can make or break a case. For example, I recently had a case where a file’s GPS co-



temp.jpg Properties

General | Security | Details | Previous Versions

temp.jpg

Type of file: JPG File (.jpg)
Opens with: Windows Photo
Location: C:\temp
Size: 3.14 KB (3,216 bytes)
Size on disk: 4.00 KB (4,096 bytes)
Created: Thursday, December 31, 1998, 11.00.00 PM
Modified: Tuesday, December 31, 2999, 11:00:00 PM
Accessed: Friday, December 31, 3999, 11:00:00 PM
Attributes: □ Read-only □ Hidden [Advanced...]

Filename(s): C:\temp\temp.jpg
[Add Files] [Clear]
Created Date: 12/31/1998 11:00:00 PM ☑ Change
Modified Date: 12/31/2999 11:00:00 PM ☑ Change
Accessed Date: 12/31/3999 11:00:00 PM ☑ Change
[Change Files Date] [Exit]

**Figure 6.** *FileDateCH changing MAC dates*

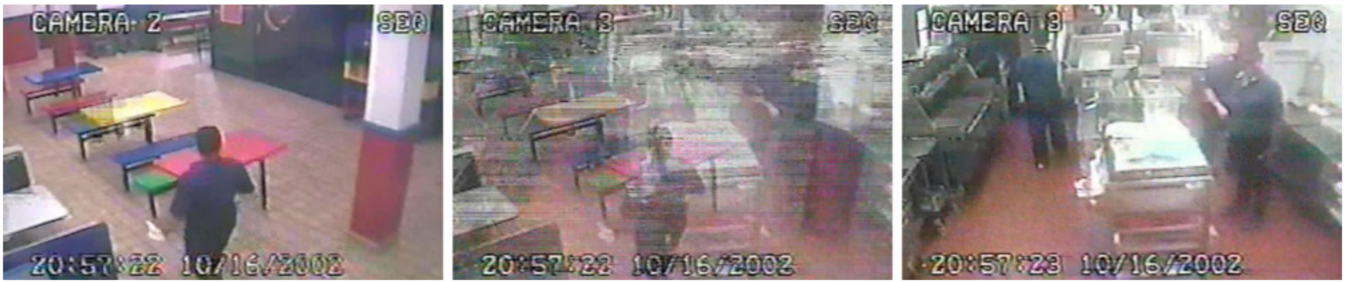


**Figure 5.** *Two sequenced frames on either side of a blended frame*

ordinates matched the address of someone with video editing skills, instead of the location depicted in the video.

The file's metadata may include the date-time of the file's creation and who was the last person to access it. Metadata may also include details about the software or equipment used to capture the recording, including the user settings in effect at the time of file saving. If these details do not match the case facts, then you may have strong evidence of after-the-fact file tampering. For example, if a video's metadata lists the file as being in a Windows format, but the event was captured on an iPhone, then you can be confident that you are not looking at the original recording as saved by that iPhone. Metadata inconsistencies should always initiate an extremely thorough series of authentication tests.

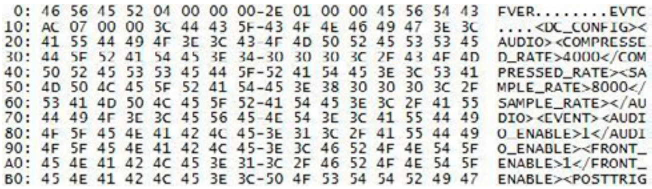
## HEX EDITORS

Hex editors allow the user to examine and modify any bit or byte of file data. Changing this inform will alter the file's Hash tag, but reading this data can provide deep insight into any programs that previously affected the underlying file data. Most of the identifying information is located at the beginning (header) and end (footer) of a file (see Figure 7). One of many free hex editors, and my personal favorite is BeHexEditor (*http://sourceforge.net/projects/hexbox*).

For example, the numeric value of each set of four characters (bytes), of the first 52 bytes of an AVI file, detail how the file is to be played (example: size, speed, audio type, offset, etc…). In this example, the value of bytes 32 through 35 denotes the videos width (in pixels) and the next four denote the height. The offset value allows the insertion of additional metadata which may include information about the creating software, creation time, geographic location, etc…

## STEGANOGRAPHY

Steganography is the art of hiding parasite data (example: messages, passwords, illegal information, etc…) within a host file, typically as a text inside an image file. The hidden data cannot be detected using a visual inspection, metadata tools or hex editors. There are several Steganography programs and data hidden with one program is nearly invisible to the others. The most popular is the open-source application OpenPuff (*http://embeddedSW.net*).



```
 0: 46 56 45 52 04 00 00 00-2E 01 00 00 45 56 54 43  FVER........EVTC
10: AC 07 00 00 3C 44 43 5F-43 4F 4E 46 49 47 3E 3C  ....<DC_CONFIG><
20: 41 55 44 49 4F 3E 3C 43-4F 4D 50 52 45 53 53 45  AUDIO><COMPRESSE
30: 44 5F 52 41 54 45 3E 34-30 30 30 3C 2F 43 4F 4D  D_RATE>4000</COM
40: 50 52 45 53 53 45 44 5F-52 41 54 45 3E 3C 53 41  PRESSED_RATE><SA
50: 4D 50 4C 45 5F 52 41 54-45 3E 38 30 30 30 3C 2F  MPLE_RATE>8000</
60: 53 41 4D 50 4C 45 5F 52-41 54 45 3E 3C 2F 41 55  SAMPLE_RATE></AU
70: 44 49 4F 3E 3C 45 56 45-4E 54 3E 3C 41 55 44 49  DIO><EVENT><AUDI
80: 4F 5F 45 4E 41 42 4C 45-3E 31 3C 2F 41 55 44 49  O_ENABLE>1</AUDI
90: 4F 5F 45 4E 41 42 4C 45-3E 3C 46 52 4F 4E 54 5F  O_ENABLE><FRONT_
A0: 45 4E 41 42 4C 45 3E 31-3C 2F 46 52 4F 4E 54 5F  ENABLE>1</FRONT_
B0: 45 4E 41 42 4C 45 3E 3C-50 4F 53 54 54 52 49 47  ENABLE><POSTTRIG
```

**Figure 7.** *File header as read by a hex editor*

## BIBLIOGRAPHY

- Video codecs and decompressors, retrieved 2013 from *http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3232547/*
- Dr. Neal Krawetz, "A Picture's Worth...", 2007 Black Hat conference, Caesars Palace – Las Vegas, retrieved 08/01/07, *http://blackhat.com/html/bh-usa-07/bh-usa-07-speakers.html#Krawetz*

## REFERENCES

- Photoshop CS3 for Forensic Professionals, George Reis, ISBN 978-0470114544
- Basic Television and Video Systems (6th edition), Bernard Grob, ISBN 978-0028004372
- How Video Works (2nd edition), Marcus Weise and Diana Weynand, ISBN 978-0240809335
- Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems, *http://www.rcfl.gov/webinar/Video_Evidence_From_CCTV_system_flipbook.pdf*
- CCTV Networking & Digital Technology (2nd edition), Vlado Damjanovski, ISBN 978-0750678001

Unless protected through Hash tag version control, Steganography would allow a file to contain illegal or personal information without the knowledge of the person distributing the file. As with any content change, adding or changing content with a Steganography program will change that file's MD5 Hash tag.

## IN SUMMARY

It is an unavoidable reality that electronic files are vulnerable to tampering and corruption. Undetected, these changes can alter the meaning and value of critical evidence. From version control to authentication, the above steps can help ensure that everyone is working from an authentic and identical set of facts.

**About the Author**

*I am an audio – video enhancement and authentication expert, and am board certified by the American College of Forensic Examiners and the American Society for Industrial Security. Over the last twenty years I have processed evidence in over a thousand cases worldwide including the George Zimmerman – Trayvon Martin shooting, and the Mathew Clark beating. I have pioneered industry innovations and routinely donate my time to innocence projects, indigent clients and as an industry educator. I am the founder and lead analyst of Forensic Protection, a world class lab that has received both prosecution and defense praise for detailed work leading to an exceptionally high rate of pretrial case dismissal or settlement. A complete CV is available at http://ForensicProtection.com.*

New Package Installer
Improved Technology for Protection against yet-unknown Threats
New Anti-Rootkit Module
Online Service Dr.Web Cloud
Improved Parental Control
Free Upgrade to New Version
Unified User Interface
Better than ever: Dr.Web Security Space version 8.0! 30-day trial available from https://download.drweb.com/?lng=en

XRY
COMPLETE