Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Detailed Forensic Procedure for Laptop computers

Forensic analysis is the process of accurately documenting and interpreting information for presentation to an authoritative group. In most situations that group would be a court of law, but management will often request forensic preservation of information as well. Due to the easily changeable nature of digital information, great care must be put into the handling of any forensic analysis. Evidence grade information must be unbiased, and complete before it can be relied upon. Not only must the data be collected, but a...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

Matt Pierce

Detailed Forensic Procedure for Laptop computers

06-11-2003

© SANS Institute 2003, Author retains full rights

GIAC Security Essentials Certificate
GSEC Practical Assignment V 1.4b - Option 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Forensic analysis is the process of accurately documenting and interpreting information for presentation to an authoritative group. In most situations that group would be a court of law, but management will often request forensic preservation of information as well. Due to the easily changeable nature of digital information, great care must be put into the handling of any forensic analysis. Evidence grade information must be unbiased, and complete before it can be relied upon. Not only must the data be collected, but also the original media must be preserved. Furthermore it is necessary to record the state of the computer that produced the data. Laptop computers present additional technical issues. The hardware in a laptop computer has typically been modified for energy preservation and size. These modifications can frustrate a forensic examiner's normal use of tools and procedures. This document will discuss what forensic analysis is and why it is important. Also discussed will be how laptop computers affect forensic analysis. Finally, this document will describe three procedures for developing forensic information from a laptop computer running a Microsoft operating system.

Forensics

The forensic process touches on all phases of the Confidentiality, Integrity, and Availability (CIA) security model. A forensic examiner must maintain a strict impartiality to protect the confidentiality of the parties involved in the data. This confidentiality can be crucial if these parties proceed with a court case. The reputation of the forensic examiner will reflect on the quality of the data preserved. Inappropriately presenting the data, or disclosing information to unnecessary parties can be construed as biasing the evidence. The integrity of the data must be diligently maintained. Electronic data is easy to repudiate due to its changeable nature. An analyst can show that data has been tampered with only if the party who did the tampering is less skilled than the technician who performed the analysis is. As such, you must take every precaution that the data not be modified at any time after the supposed event that brought about the challenge the data pertains to. The preserved data must be available to experts from both parties involved for independent analysis. Verifiably exact duplicates of the preserved data sets must be created for controlled distribution to the necessary parties. It is within this framework that a forensic examiner may work to provide the untarnished truth.

The legal process impacts the American society at all levels. Within this process the truth has an odd definition, the only truth is what you can proven. There are several high profile court cases where the evidence presented was challenged or dismissed due to mishandling of the data. Email has taken center stage in many such cases. People discuss all manners of subjects in email, including subjects that they would prefer remain private. Microsoft corporation faced evidence from internal emails during their Anti-Trust hearings with the Department of Justice(DOJ 65.3 II). The presentation of electronic evidence in the form of email provided a powerful argument in the government's case. The data provided by forensic analysis of the Microsoft email system highlighted the power of electronic data in legal cases. During the proceedings, the court ordered Microsoft to produce any information concerning the broad scope of the case. Failure to provide all relevant data would have left Microsoft in contempt of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

court. The scope of such an order against a defendant has many companies reevaluating their data retention policies. The capacity of forensic analysis to recover data that the owners themselves have forgotten has created quite a stir in the corporate world.

Electronic data is a fragile sledgehammer. It has the ability to provide a lot of information about the goings on in a particular case. But it has a high burden of proof do to its volatile nature. For example, the United States of America has accused Zacarias Moussaoui of conspiring to commit a terrorist act. A key piece of evidence in this case is Mr. Moussaoui's personal laptop computer. The standby counsel for Mr. Moussaoui sought to exclude the laptop data from evidence based on questions raised about the forensic process used by the FBI. The FBI in return provided a detailed description of procedures, and tools used in the preservation of that laptop computer. If the FBI had not been able to authoritatively prove each step of the forensic analysis, they could have lost the ability to use that data in the court case. By following a meticulous forensics process, they were able to provide a firm rebuttal to the stand by counsel's challenge.

Forensics Process

The process of forensic analysis begins the moment a question is raised about the activities that occur on a computer. The first most critical task of a forensic analyst is to create an evidence log that accurately and completely documents the forensic process. Every access to the machine in question should be recorded with date and time, as well as exactly what tasks were performed. This document is to become legal evidence and as such should be kept secured without perjury.

Data is contained in two separate systems in most computers. First there is short-term volatile memory, typically the random access memory. (RAM) RAM is the working area in which programs, and data are manipulated by the operating system. Most operating systems keep data about the machine's state in short-term memory areas. This machine state data can provide an analyst with insight into recent network activity, processor usage levels, recent commands, and a host of other computer activities. Much of the most critical information about a computer is lost the moment it is turned off. To often this is the first reaction of a first responder when a computer is called into question. To retain this information it is necessary the analyst have access to the computer as soon as it is determined forensics is to be performed. Response time is critical, some of this data expires after as little as 2 minutes. The examiner must then run programs to extract the data and save the results off system. The results of this data extraction should be burned onto write once optical media in order to prevent tampering. Special care must be taken to avoid making any changes to the system during the forensic process.

Long term memory allows the computer to store data that is not immediately needed by the operating system. There are many forms of long term storage: hard disk, floppies, optical disk, tapes, and many other formats. The most common device is the hard disk. A hard disk is basically a flat plate coated with rust that a magnet arranges into a logical order. Magnetic media is very easy to manipulate or damage. It is necessary for a forensic examiner to preserve the long term storage medium without change. Typically the examiner will make an exact copy of the data on the computer to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

another storage medium. Special programs are then used to create a mathematically derived hash of the source data. Any changes to the source data will result in a different hash sum. The copy of the data then has a hash created. The results from both data sets are compared to verify that the copy is an exact duplication. It is further suggested to create at least one verified copy of the data set on a write once optical medium to prevent tampering or decay. At this point the original is sealed in an anti-static airtight bag. The source data should then be turned over to a company officer, law enforcement official or other appropriate responsible party. This source copy should be retained in a locked container with limited access. Any copies made for distribution should be made from the verified data copy, and should be likewise verified. Following these steps with extreme diligence will allow the original media to be examined with extensive data extraction tools if it is necessary to do so.

Typically, analysis of the data should only be made on a verified copy of the original data set. It is highly recommended to retain a control copy separate from the copy used during content analysis. Content analysis is the act of extracting useable information from the preserved media. This information could consist of e-mails, or data files, or the time stamps on certain files. What information is needed will depend on the details of a particular case. By paying close attention to the method used to extract that data, the forensic examiner can make a strong argument as to the reliability of the information provided.

Laptop Particulars

Laptop computers are designed to be light, and conserve battery power. Because of this a laptop is probably the most inbred of all computing systems. The hardware in a laptop is typically custom built for that particular model. Very few components follow any given industry standard. This complicates the process of forensic analysis. For example, the interface for a laptop's IDE hard drive is smaller than the typical 40-pin ATA ribbon connector. Most laptops do not allow for the use of more than one hard disk at any given time. Many laptops do not allow for the use of a CD-ROM and a Floppy disk at the same time, complicating the use of some recovery tools. Furthermore laptops may require special drivers or software modules in order to function properly. This creates a situation where the tools and methods used to extract data from a common desktop computer need to be modified to adapt to the laptops proprietary hardware.

Regardless of what means the analyst uses to copy the data on the long-term storage device, it is essential that the original OS not be booted. Most operating systems modify file access dates, and clear cache files on boot. Instead, boot the machine from either the CD-ROM or the floppy. The examples in this document use the Gentoo Linux Live CD 1.4_rc4 and the windows 98se boot disk to provide access to the appropriate devices and tools (Gentoo). Other operating systems may be available but are not detailed here.

A laptop hard disk uses a 50pin interface that integrates data, power, and provisioning into one connector. Many vendors implement a 44pin connector that leaves the provisioning apart to be configured separately with jumpers. Electrically these connectors follow the ATA specifications, and this makes it an easy job to convert one interface to the other. Converter kits are sold that will adapt the two connector

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

types. Someone with a basic understanding of electronics can construct such a converter (ATA). Knowing about the connector types allows a forensic analyst to be prepared before he/she is faced with copying data from a laptop hard disk. This method will typically be used when the original disk has been removed from the computer and the analysis is being performed elsewhere. There is a potential difficulty in that not all computers handle Logical Block Addressing (LBA) in the same manner.

Another option is to install a PCMCIA ATA controller card. Such a device allows for the addition of a second laptop hard disk. This assures the analyst that both drives were written using the same bios, thus using the same LBA translation scheme. This is a fast method of creating an image of the original disk. Additionally it is a good method to use when the analyst has limited access to the suspect computer. The machine does not have to be removed to a lab environment nor is a trusted network needed. The trouble in this approach is that your PCMCIA device must be supported by the media bootable OS. This can limit the range of tools available, as most MS dos based boot disks do not support PCMCIA devices.

The final connection option is to use a network adapter and transfer the disk image across a network connection. This can be a convenient option if there is a network available. Transferring across the network allows you to avoid issues involving LBA translation errors, as the copy is an exact binary image. Such a transfer though can get you in trouble with your network administrator. Sending gigabytes of data across the network can cause noticeable performance problems. It is a good practice to protect the data connection during transport to ensure that the information is not tampered with in transit. Finally this is the slowest available option, the bandwidth available to a network connection is trivial compared to that available to the hard drive IO bus's bandwidth.

Live Forensic Process

There are two states a computer can be in when it is time to perform forensic analysis. The computer can be live, where the computer is running and the operating system is available. Or the system can be powered down, in which case the only procedure available is to perform a disk image. Whether or not the forensic analyst should work with a live system is a bit of a judgment call. It is possible that the forensic process will alert an intruder, or trigger an automated self-destruct program. Conversely the operating system of most computers contain a wealth of information about the recent activities of a computer system. The process that follows is targeted for a Microsoft Windows 2000 operating system. There are too many specific OS environment variables to cover even the common Microsoft platforms, much less a comprehensive view of all platforms. This is intended to be an application of the concepts described above as an illustration of the process. Much of the command usage was modeled on the ResponseKit CD for Win2k/XP/NT (Jones). It is recommended that the commands be consolidated into a batch file to speed the collection of information. Such a batch file is included in Appendix A.

! Analyst receives the initial notification of event requiring forensic preservation !

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Create Event Log

The first thing an analyst needs to do is to document the initial contact and the events leading up to the forensic analysis. This should include any known contact with the machine in question and a description of its operating state. This document should be protected by all means possible. Access to this document should be strictly limited to the analyst. Remember to record each task as it is being performed and note the time of performance in the event log.

Establish Trusted Network Repository

In order to minimize the impact of the forensic process on the computer being analyzed it is recommended that a Cryptcat server be setup to accept the log files from the analysis tools (Cryptcat). The server should be a trusted machine that is thoroughly secured. The –l places cryptcat in the listen mode. The –p assigns the service to port 2505. This can be any port not in use, 2505 is simply a free port chosen from the IANA common port assignment list (IANA).

cryptcat –l –p 2505 > date-case-logfiles.txt

Record the System Time and Date

PC operating systems keep track of time in a fairly inaccurate manner. As such the time on a computer is liable to drift. It is necessary to know the margin of this drift in order to interpret file access times. Record the time and date reported by the operating system, and compare that with the time from a reliable source such as a time sync server. Document what timeserver was used.

Record ARP cache

The ARP cache stores the MAC address to IP address translations for the last 2 minutes. The –a switch pulls the active ARP cache entries. The xxx.xxx.xxx.xxx denotes the IP address of the cryptcat server.

arp –a | cryptcat xxx.xxx.xxx.xxx 2505

Record NetBEUI cache

NetBEUI is the Microsoft protocol for local area networks. The names of any NetBEUI capable systems that the machine has accessed recently will be stored in memory.

nbtstat –c | cryptcat xxx.xxx.xxx.xxx 2505

Record IP configuration

The IP configuration establishes the network address configuration of the computer being analyzed.

i*pconfig /all | cryptcat xxx.xxx.xxx.xxx 2505*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Record Network connections

Netstat is a tool that will list all network connections, protocols, and port numbers.

netstat –an | cryptcat xxx.xxx.xxx.xxx 2505

Fport network process enumeration

Fport is a very useful tool from Foundstone that lists active network ports and shows what file has them open (Foundstone).

fport –a | cryptcat xxx.xxx.xxx.xxx 2505

Psinfo Process enumeration

Psinfo is a part of the pstools application suite from Sysinternals that lists the running processes (Sysinternals).

psinfo | cryptcat xxx.xxx.xxx.xxx 2505

Psloggedon user logged on enumeration

Psloggedon is a part of the pstools application suite from Sysinternals that lists what users are logged on to the system (Sysinternals).

psloggedon | cryptcat xxx.xxx.xxx.xxx 2505

Psfile remote file access enumeration

Psfile is a part of the pstools application suite from Sysinternals that lists files that are being accessed remotely (Sysinternals).

psfile | cryptcat xxx.xxx.xxx.xxx 2505

Psservice running services enumeration

Psservice is a part of the pstools application suite from Sysinternals that lists services that are currently running on a system (Sysinternals).

psservice | cryptcat xxx.xxx.xxx.xxx 2505

Directory access times

The following three commands enumerate the directory access times, modification times, and creation times. The forensic analyst may wish to skip this step due to a feature of the Windows 2000 operating system. By enumerating this information these attributes may be modified.

Last Access Times
dir /t:a /o:ng /s c:\ | cryptcat xxx.xxx.xxx.xxx 2505

Last Modified Times
dir /t:w /o:ng /s c:\ | cryptcat xxx.xxx.xxx.xxx 2505

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Creation Times
dir /t:c /o:ng /s c:\ | cryptcat xxx.xxx.xxx.xxx 2505

Event Logs

Dumpel.exe is a tool provided by Microsoft in the Windows 2000 resource kit that creates a report from the data in the windows logs.

Security Event Log
dumpel -l security | cryptcat xxx.xxx.xxx.xxx 2505

Application Event Log
dumpel -l application | cryptcat xxx.xxx.xxx.xxx 2505

System Event Log
dumpel -l security | cryptcat xxx.xxx.xxx.xxx 2505

With the short-lived data preserved, the machine must be shut down. There are two schools of thought in this matter. First you can yank the plug. This in essence freezes the disk activity where it was at the last time of writing. This can result in file system damage, or lost data due to disk caches not being written. The other opinion is to do an OS shutdown procedure. This ensures that the system is correctly shut down, but can result in certain files being deleted or modified. Additionally there is the possibility of malicious programs being run that destroys data. Whatever procedure the analyst chooses, be sure to record the action in the event log.

Disk Imaging

There are several methods to produce a forensic grade image of a hard disk. This paper can by no means cover all of them. Several commercial tools are available that are dedicated to such a task. Usually these tools are extremely expensive, but their features are designed specifically to assist the forensic analyst. Common disk maintenance tools such as Symantec's Norton Ghost or the GNU DD command can be used as well. Care must be taken though to ensure that the correct command options are used so the data is not modified in any manner. When working with IDE hard disks in computers other than the system in which their file systems were created, it is vital that the analyst ensure that the BIOS of the analysis computer correctly recognizes the physical cylinder, head, sector (CHS) geometry parameters. Additionally it is vital that the BIOS correctly calculate the LBA CHS parameters.

Cryptographic verification of the data before and after the imaging process is a necessary step in ensuring that the data remains consistent. GNU MD5sum is the most common tool used to cryptographically verify data. Three independent checks should be computed and recorded. The first check should be made against the source data before any other tool is run. The second check should be computed on the source data after the disk imaging process has completed, thereby validating that the imaging

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

process did not corrupt the original content. Finally the recipient data image should be checked and the results matched to the source data.

Commercial tools complete these verifications on the fly thereby reducing the possibility of user error. If available they should be used whenever possible. DD is a common UNIX command and has several revisions. Before performing a disk imaging process, record the version of the DD tool that will be used. Check this version for possible bugs or errata if you have not previously done so. There are versions of the DD tool that are optimized for use in forensic analysis (Garner). These tools are streamlined to allow for faster imaging operation, and better capacity for verification. The standard DD command can produce forensic grade data, but the convenience of specialized tools can make the process much more efficient.

Common Tasks

Before performing the disk image process there are a few preliminary tasks. First you need to record the physical disk geometry and the LBA geometry parameters. The computer that is being analyzed should never be allowed to reach the boot stage after the analyst shuts it down, or receives it in a powered down state. This may require the analyst to modify the boot order so that the CDROM is the first bootable device in the computers BIOS setup program. When writing to a recipient hard disk, ensure that all sectors on the recipient disk have been overwritten with 0's. This will prevent a challenge of preexisting data. Some BIOS versions allow the hard disk to be placed into read only mode. Enabling this option is suggested, as it will prevent accidents from contaminating the data. Now boot the computer up using the Gentoo Linux OS CD. If you are using the PCMCIA ATA controller card, be sure to pass the dopcmcia parameter when you enter in your kernel type.

```
# gentoo dopcmcia

*List of services as they startup*

#
```

The first IDE hard disk in the system is designated hda. The other IDE channels are designated in by descending letters, hdb,hdc,hdd. Partitions on each disk will be designated 1,2,3,4,etc. In order to list the partitions on a given disk use fdisk –l

#fdisk –l /dev/hda

```
Disk /dev/hda: 240 heads, 63 sectors, 2184 cylinders
Units = cylinders of 15120 * 512 bytes

Device Boot    Start      End    Blocks   Id  System
/dev/hda1          1       14    105808+   7 HPFS/NTFS
```

It is necessary to record the Physical and LBA CHS parameters of the hard disk

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

#hdparam –ig /dev/hda1

/dev/hda:
geometry = **1245/255/63**, sectors = 20005650, start = 0

Model=ST310212A, FwRev=3.02, SerialNo=5EG19TH2
Config={ HardSect NotMFM HdSw>15uSec Fixed DTR>10Mbs RotSpdTol>.5% }
RawCHS=16383/16/63, TrkSize=0, SectSize=0, ECCbytes=4
BuffType=unknown, BuffSize=512kB, MaxMultSect=32, MultSect=32
CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=20005650
IORDY=on/off, tPIO={min:240,w/IORDY:120}, tDMA={min:120,rec:120}
PIO modes: pio0 pio1 pio2 pio3 pio4
DMA modes: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 *udma4
AdvancedPM=yes: unknown setting WriteCache=enabled
Drive Supports : Reserved : ATA-1 ATA-2 ATA-3 ATA-4 ATA-5

In the event log record these two parameters

LBA CHS= 1245/255/63
RawCHS=16383/16/63

Now the analyst must create the md5sum hash for the original data set.

#md5sum –b /dev/hda1
d0c8829c73334997937438dfd9c450689 */dev/hda1

Now the drive is ready for disk imaging. The next three sections will provide the individual procedures for performing different types of disk imaging operations.

Disk to disk copy using Commercial tool

In this scenario the hard drive has been removed from the original computer. The analyst will not have access to the original computer, just the disk. The hard drive will be slaved into a lab computer and the drive will be cloned to another disk. Symantec Ghost 2002 will be used to perform the imaging process (Brozycki).

Set source disk to IDE master
Attach disk to the Secondary IDE Chain
Set disk recipient disk as IDE master
Attach recipient disk to the Primary IDE Chain

Boot computer from bootable Ghost floppy disk

Start the Ghost application with the –ir option to enable image raw mode

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A:\ghostpe -ir

Select the source disk as the source
Select the recipient disk as the destination
Begin the disk copy

After the copy completes, boot to Gentoo Linux CD and verify the md5sum of the original disk has not changed, and then calculate the md5sum on the recipient disk.

#md5sum –b /dev/hdc1
d0c8829c73334997937438dfd9c450689 */dev/hdc1

#md5sum –b /dev/hda1
d0c8829c73334997937438dfd9c450689 */dev/hda1

PCMCIA ATA controller using DD

In this scenario the analyst has full access to the laptop, but limited access to a lab or network resources. After shutting the system down the analyst will install a PCMCIA ATA controller with a recipient hard disk attached. DD will be used to image the data from the original data disk to the second disk.

Install PCMCIA controller
Boot Computer from Gentoo Linux CD
At the startup screen choose the gentoo kernel with PCMCIA options

#gentoo dopcmcia

Make a directory entry in \mnt for the drive that will receive the image file

#mkdir /mnt/hd2

Mount the second drive to the file system

#Mount –t ext3 /dev/hde /mnt/hd2

Use DD command to copy data to recipient drive

#dd if=/dev/hda1 of=/mnt/hd2/date-case-image.bin conv=notrunc,noerror,sync bs=512

Verify the md5sum for the source disk has not changed.

#md5sum –b /dev/hda1
d0c8829c73334997937438dfd9c450689 */dev/hda1

Now perform a md5sum on the image file to verify an exact copy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

#md5sum –b /mnt/hd2/date-case-image.bin
d0c8829c73334997937438dfd9c450689 **/mnt/hd2/date-case-image.bin*

Network Copy using DD

In this scenario the analyst has access to the laptop, a trusted network, and a lot of time. After shutting down the system the analyst will boot into Gentoo and create a netcat connection. DD will then be piped across the network connection to a trusted network computer. One serious limitation of this procedure involves the inability of some Operating Systems to write files in excess of 2 gigabytes. Modern file systems such as ext3, Reiserfs version 3.6, XFS, and NTFS support massive single file sizes. Fat32 supports up to a 4-gigabyte file, a bit small for disk image work. This should not be an issue on most modern operating systems, but it is a possible problem for the unaware. This example assumes that the receiving computer has executable versions of dd and netcat available. Due to a compiler incompatibility between Gentoo, and cryptcat, netcat was used. Netcat was built on a Gentoo Linux 1.4 rc4 install and the binary was copied to a floppy disk. This binary is available at http://www.knology.net/~mattspierce/nc.html

On a secured network resource you will need to run netcat in listen mode in order to receive the image. The only additional switch here is the –w 120, which causes netcat to disconnect if there is no activity for 300 seconds. This allows you to close the image file after the transfer has completed. It also means that you only have 5 minutes to start the image transfer after starting the server side.

nc –l –w 300 –p 2505 | dd of=/casefile/date-case-image.bin

Connect laptop to trusted network
Boot Computer from Gentoo Linux CD
At the startup screen choose the gentoo kernel

#gentoo dopcmcia

Depending on your network architecture you will either need to DHCP a network address or manually assign an IP address.

#dhcpcd eth0

If you have to manually assign an IP address, enter the following commands. You will need to know the IP address, broadcast address, netmask, and the default gateway address. The analyst will also need to know the DNS server address in order to create a resolve.conf file.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

 # ifconfig eth0 $IPNUM broadcast $BCAST netmask $NMASK
 # /sbin/route add -net default gw $GTWAY netmask 0.0.0.0 metric 1 eth0
 # nano /etc/resolv.conf
domain *domainname.com*
nameserver xxx.xxx.xxx.xxx
nameserver xxx.xxx.xxx.xxx
^X

Ping the IP address of the secure cryptcat server to ensure network connectivity

Mount the floppy that contains Netcat's executable

#mount –t vfat /dev/fd0 /mnt/floppy

Use DD command to copy data to a secure network resource. Pipe the output of DD to netcat with the IP address and port number of the secure network resource as the options.

#dd if=/dev/hda1 conv=notrunc,noerror,sync bs=512 | /mnt/floppy/nc xxx.xxx.xxx.xxx 2505

On the secure network resource perform a md5sum on the image file to verify an exact copy

#md5sum –b /casefile/date-case-image.bin
d0c8829c73334997937438dfd9c450689 **/casefile/date-case-image.bin*

The first example creates an exact duplicate disk. This is a convenient method for easy access to data, but gets a bit expensive if multiple copies are needed. The second and third examples result in a .bin file that contains all the binary data from the original disk. This file can be repackaged in many forms for wider distribution. This type of binary image can be analyzed using several commercial analysis tools. Additionally, the loopback device function in Linux can be used to mount the .bin image as a block device. From there it can be analyzed using a multitude of file system tools. The methods used in these examples illustrate commonly available tools and their use in performing forensics on a laptop computer. It is strongly recommended that specialized forensic tools be used in this task if available. The results of the commonly available tools are just as reliable, but the process for obtaining that reliability requires a great deal of time and effort from the analyst. In either case the result is the production of verifiable information concerning the activities on the computer in question.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Jones, Shema, and Johnson. Anti-Hackers Toolkit.
http://www.amazon.com/exec/obidos/tg/detail/-/0072222824/qid=1056024470/sr=8-1/ref=sr=8%20-1/002-3714599-8046433?v=glance&s=books&n=507846

(ATA) ATA 40pin to 50pin adapter
http://delphys.net/d.holmes/hardware/ata_interface_1.html

Brozycki, John. Norton Ghost 2003 as a Forensic Image Acquisition Tool
http://www.giac.org/practical/GCFA/John_Brozycki_GCFA.pdf

(Cryptcat) encrypted netcat tool
http://sourceforge.net/projects/cryptcat/

(DOJ) US Department of Justice vs Microsoft court documents
http://www.usdoj.gov/atr/cases/f2600/2613-1.htm

Foundstone. Fport
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

Garner, George M. Forensic Acquisition Utilities
http://users.erols.com/gmgarner/forensics/

(Gentoo) Gentoo Linux Live CD
http://www.gentoo.org/doc/en/gentoo-x86-install.xml

(IANA) IANA assigned port numbers
http://www.iana.org/assignments/port-numbers

(Moussaoui) USA vs. Zacarias Moussaoui "Government's Opposition To Standby Counsel's Reply To The Government's Response To Court's Order On Computer And E-Mail Evidence"
http://cryptome.org/usa-v-zm-email.htm

Sysinternals. PsTools
http://www.sysinternals.com/ntw2k/freeware/pstools.shtml

(Rules) Federal Rules of Evidence. Article X
http://www.law.cornell.edu/rules/fre/overview.html#article%20iv

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

Create a plain text file named Response.bat that contains the following commands (Jones):

```
@echo off
echo ****************
echo ***** Start *****
echo ****************
now
echo ******************
echo ***** ps info *****
echo ******************
psinfo
echo **********************
echo ***** ps loggedon *****
echo **********************
psloggedon
echo *****************
echo ***** ntlast *****
echo *****************
ntlast
echo **********************
echo ***** netstat -an *****
echo **********************
netstat -an
echo ******************
echo ***** arp -a ******
echo ******************
arp -a
echo ****************
echo ***** fport *****
echo ****************
fport -p
echo ******************
echo ***** ps file *****
echo ******************
psfile
echo ******************
echo ***** ps list *****
echo ******************
pslist
echo ******************
echo ***** ps services *****
echo ******************
psservice
```

© SANS Institute 2003, Author retains full rights

```
echo **********************
echo ***** nbtstat -c *****
echo **********************
nbtstat -c
echo ****************************
echo ***** Last Access Times *****
echo ****************************
dir /t:a /o:d /s c:\
echo ******************************
echo ***** Last Modified Times *****
echo ******************************
dir /t:w /o:d /s c:\
echo *************************
echo ***** Creation Times *****
echo *************************
dir /t:c /o:d /s c:\
echo ******************************
echo ***** Security Event Log *****
echo ******************************
dumpel -l security
echo *********************************
echo ***** Application Event Log *****
echo *********************************
dumpel -l application
echo ****************************
echo ***** System Event Log *****
echo ****************************
dumpel -l security
echo ********************
echo ***** ipconfig *****
echo ********************
ipconfig /all
echo ***************
echo ***** End *****
echo ***************
now
```

On the system that that is undergoing forensic analysis enter the following command

response.bat | cryptcat xxx.xxx.xxx.xxx 2505

© SANS Institute 2003, Author retains full rights

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced