Digital Forensics

Unraveling Incidents one byte at a time

Digital Forensics

Characteristics of Digital Evidence:

- Admissible – evidence must be related to the fact being proved
- Authentic – evidence must be real and related to the incident in proper way
- Complete – evidence must prove the accused actions or innocence
- Reliable – forensics must not cast doubt on the authenticity and veracity of the evidence
- Believable – evidence must be clear and understandable by the judges

Digital Forensics

Characteristics of Digital Evidence:

Admissible

If the evidence you uncover will not stand up in court, you have wasted your time and possibly allowed a guilty party to go unpunished.

Authentic

It must be directly related to the incident being investigated.

The digital forensic investigation may reveal evidence that is interesting but irrelevant.

Digital Forensics

Characteristics of Digital Evidence:

Complete

The investigator should approach the case with no preconceived notions about someone’s guilt or innocence.

Forensic methods should eliminate alternative suspects and explanations until a definite conclusion is reached.

Digital Forensics

Characteristics of Digital Evidence:

Reliable

There should be no question about the truth of the investigator’s conclusions.

Reliability comes from using standardized and verified forensic tools and methods.

Qualification (by a judge) of an investigator as an expert witness in a case will help to establish credibility and reliability.

Digital Forensics

Characteristics of Digital Evidence:

Believable

The investigator must produce results that are clear and easy to understand, even among the most non-technical members of a jury.

Have other investigators have used the same forensic techniques and reached similar conclusions?

Digital Forensics

Rules of Evidence

Affirm there has been no tampering with the evidence

- Use hashes of images to show no alteration of data since collection
- Use a write blocker during acquisition
- Maintain **Chain of Custody**
- Take copious notes on commands run during analysis or collection
- Photograph process as needed

Best Evidence Rule

- "original" is normally required
- Accurate printout from a computer deemed "original"

Digital Forensics

Rules of Evidence

Evidence: something that tends to establish or disprove a fact

- Use bit-image copies of storage devices or RAM
- Store original data or device in locked and controlled access cabinet

Forensic Principles

1. Minimize data loss
2. Take notes about everything
3. Analyze all data collected
4. Report your findings

Collect evidence in order from most volatile to least

Digital Forensics

Order of Volatility

Collect evidence in order from most volatile to least

1. Memory - /proc directory may have files or hacker created directory
2. Network status and connections
   – prevent further access from the network, but preserve ARP cache and connection list
3. Running Processes
4. Hard drive
5. Removable media - write caching means data is not always written right away

Decide which is more important network information (wait to unplug network) or disk (pull network plug right away) based on the situation

Digital Forensics

Rules of Evidence

Rule 703: Bases of Opinion Testimony by Experts

The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to the expert at or before the hearing

If of a type *reasonably relied upon* by experts in the particular field in forming opinions or inferences upon the subject, *the facts or data need not be admissible in evidence in order for the opinion or inference to be admitted*

Digital Forensics

Evidence

The Daubert Test

The Case of Daubert v. Merrill Dow Pharmaceuticals established new criteria to determine the reliability, relevancy, and admissibility of scientific evidence

This case set the precedent making digital evidence equal to printed ‘originals’ if it meets the Daubert test

Digital Forensics

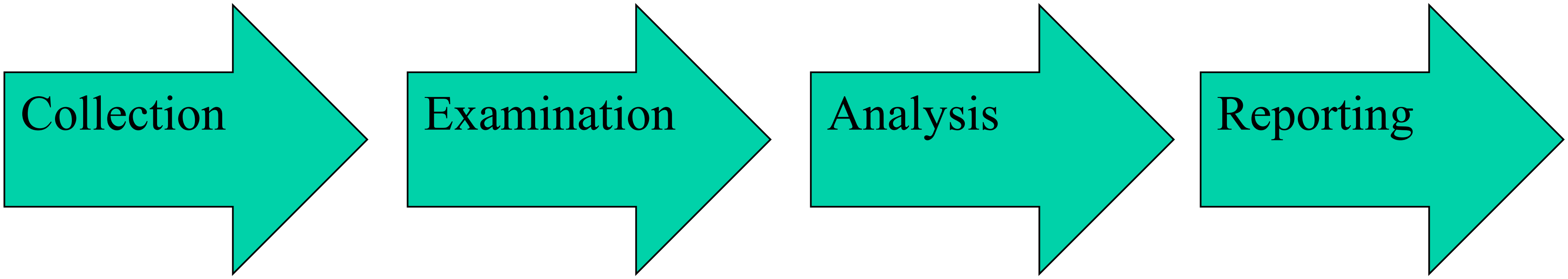
Evidence

The Daubert Test

- The theory or technique must have been tested, and that test must be replicable
- The theory or technique must have been subject to peer review and publication
- The error rate associated with the technique must be known
- The theory or technique must enjoy general acceptance within the scientific community

Digital Forensics

The Forensic Process



Collection

Examination

Analysis

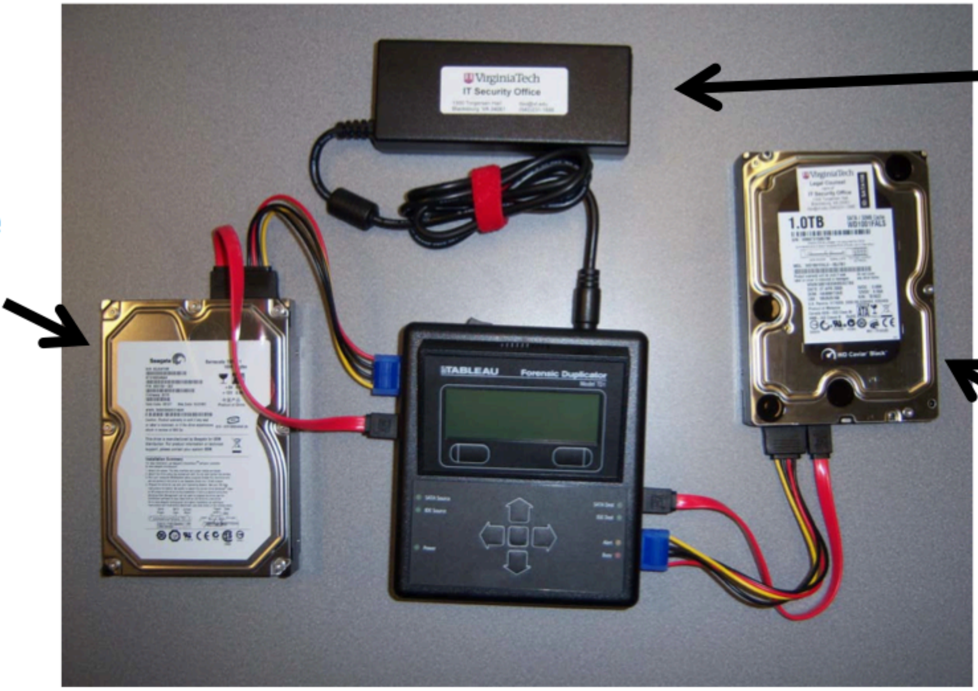
Reporting

Digital Forensics

Hardware and Software:

- Hardware write blockers Ex: Tableau
- Drive duplicators Ex: Voom Hardcopy 3P

Disk Imaging Hardware



Power Supply

Source Drive

Target Drive

Digital Forensics

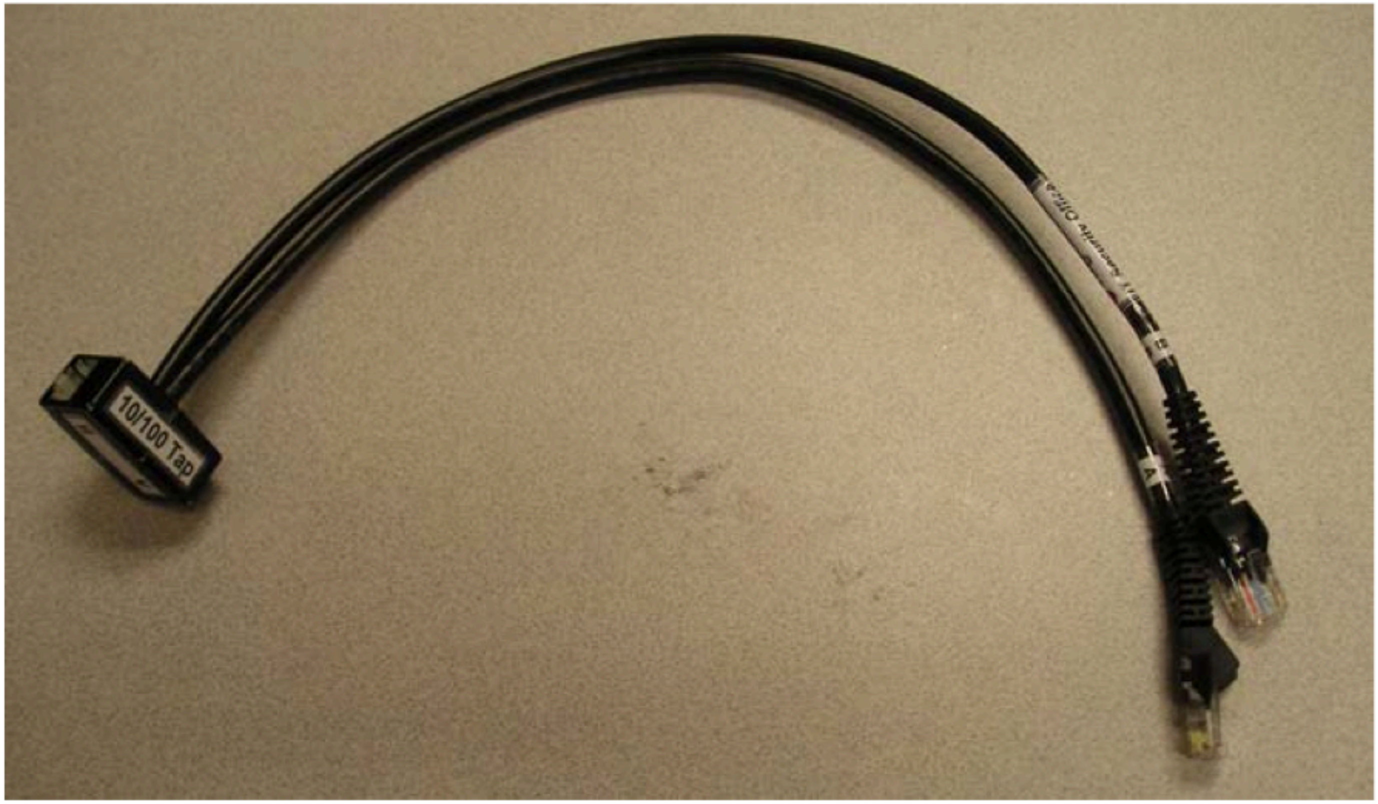
Hardware and Software:

- Hardware write blockers – Tableau
- Drive duplicators
- Disk Imaging Software – FTK imager
- Memory Imaging Software – FTK imager
- Registry dumper – regripper, regtime.pl, rip.pl
- Browser Forensics software – Mandiant Web Historian
- Memoryze – memory image analyzer
- Volatility – python scripts for analyzing memory
- SIFT workstation – prebuilt VMWare image of forensics tools available for free from forensics.SANS.org
- CAINE LiveCD – bootable Linux CD of forensic tools

Digital Forensics

Hardware and Software:

Passive Ethernet Tap



Digital Forensics

Hardware and Software:

The Wireless StrongHold Bag
by Paraben

www.Paraben.com

A Faraday cage
built into an evidence bag
for the safe collection of
wireless devices in incident response

Digital Forensics

What are we investigating?

- Identity theft
- Fraud and embezzlement
- Software piracy and hacking
- Blackmail and extortion
- Child pornography and exploitation
- Prostitution, infidelity, domestic violence
- Terrorism and national security
- Theft of intellectual property and trade secrets

Digital Forensics

What evidence can we recover?

Computer Fraud Investigations

- Accounting software and files
- Credit card data
- Financial and asset records
- Account data from online auctions
- E-mail, notes, and letters

Digital Forensics

What evidence can we recover?

Child Exploitation Investigations

- Chat logs
- Photos and digital camera software
- Internet activity logs
- Movie files
- Graphic editing and viewing software
- User-created directory and file names to classify images

Digital Forensics

What evidence can we recover?

Network Intrusion and Hacking Investigations

- Network usernames
- Internet protocol (IP) addresses
- Executable files (including viruses and spyware)
- Security logs
- Configuration files
- Text files and other documents containing sensitive information such as passwords

Digital Forensics

What evidence can we recover?

Identity Theft Investigations

- Identification Templates
  (Birth certificates, driver’s licenses, Social Security cards)
- Electronic images of signatures
- Credit card numbers
- Credit card reader/writer/scanner
- Online trading information

Digital Forensics

What evidence can we recover?

Harassment and Stalking Investigations

- Victim background research
- Maps to victim locations
- Photos
- Diaries
- Internet activity logs
- E-mails, notes, and letters

Digital Forensics

What evidence can we recover?

An example:

Dennis Rader was identified as the “BTK Killer” due to evidence that connected him to an incriminating Microsoft Word document e-mailed to a TV station

- The evidence that led to Rader’s conviction was actually contained within the “metadata” (data about data) that is created by default in Microsoft Office documents

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- Much of the U.S. Federal law involving computer crime can be found in Title 18 of the United States Code.
- 18 U.S.C. § 1029: Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- 18 U.S.C. § 1030 makes Denial of Service Attacks a federal crime

- 18 U.S.C. § 1030(a)(5)(A) transmission of program, information, code, or command, resulting in damage is unlawful

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- 18 U.S.C. § 1030 makes Substitution or Redirection of a Web site a federal crime

- 18 U.S.C. § 1030(a)(5)(A)(i) transmission of program, information, code, or command, resulting in damage

- 18 U.S.C. § 1030(a)(5)(A)(ii)-(iii)
  accessing a computer without authorization, resulting in damage

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- 18 U.S.C. § 2252B makes certain Use of a Misleading Domain Name a federal crime

- 18 U.S.C. § 2252B refers to using a misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- 18 U.S.C. § 1030 makes Internet Fraud ("phishing") a federal crime

- 18 U.S.C. § 1030(a)(4) mentions accessing a computer to defraud and obtain something of value

Digital Forensics

Federal Cybercrime Laws

Title 18 U.S.C.

- 18 U.S.C. § 2261A makes Cyberstalking a federal crime

- 18 U.S.C. § 2261A refers to using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family

Digital Forensics

Incident Handling

Incident response happens BEFORE the forensic analysis begins

Incident response is the response to a computer crime, security policy violation, or similar event

Digital evidence is secured, preserved, and documented in this phase

Digital Forensics

Forensic Response

If the computer is on, LEAVE IT ON.

If the computer is off, LEAVE IT OFF.

“Pull the Plug” vs. “Shut Down”

Pulling the plug immediately halts processing, but destroys anything in memory and can corrupt files.

Shutting down protects files from corruption, but writes entries into the systems activity logs and therefore changes the state of the evidence

Digital Forensics

Forensic Response

Live forensics

Especially if the systems are on a network, incident response begins with some live forensics to collect:

- System time
- Command history
- Process to port mapping
- Clipboard contents
- Process memory
- Open files
- Process list
- Logged on users
- Service/driver information

Digital Forensics

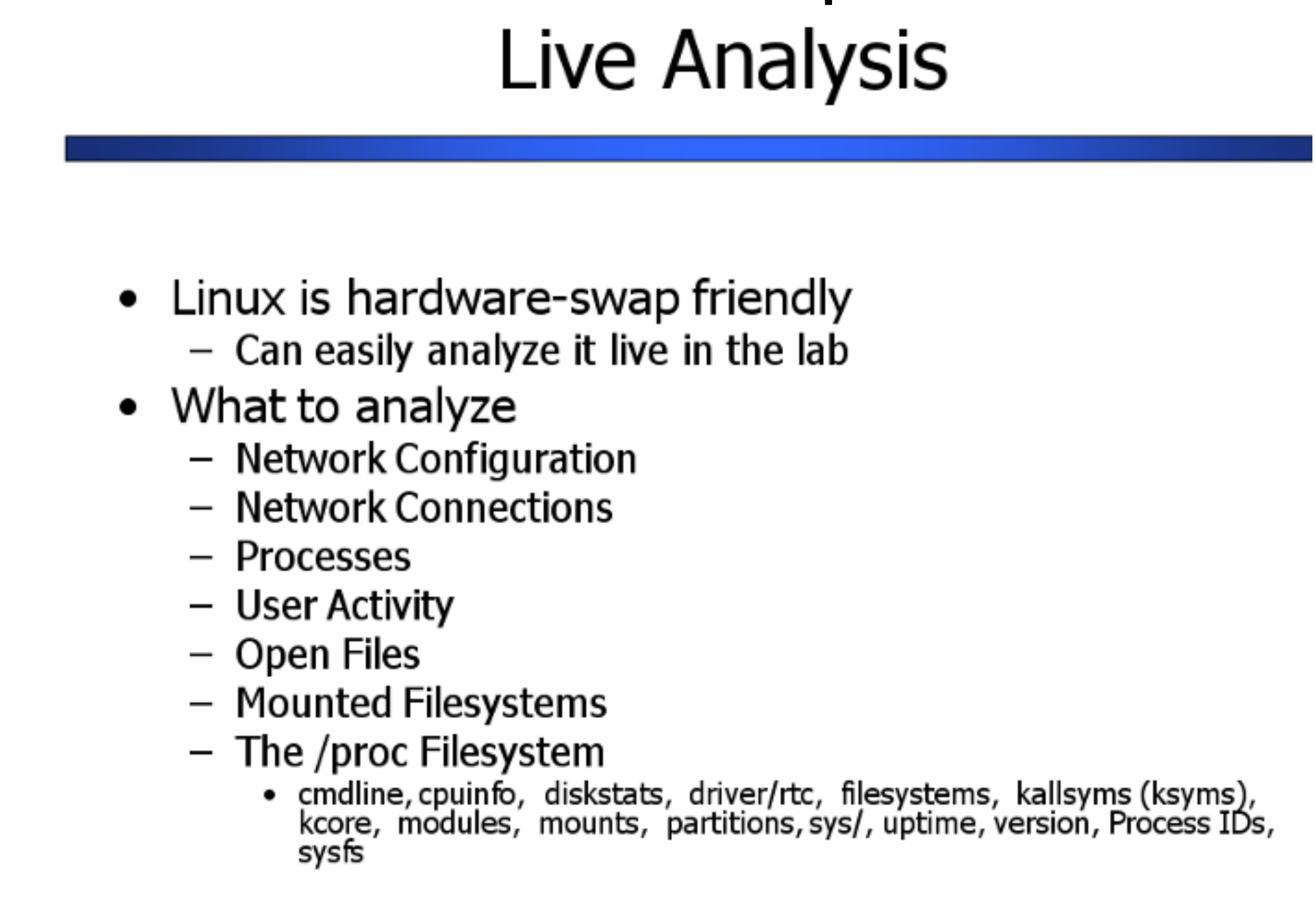
Forensic Response

Offline forensics

- Hidden files
- Slack space
- Swap file
- Index.dat files
- Unallocated clusters
- Unused partitions
- Hidden partitions
- Registry settings
- Event logs
- Alternative data streams

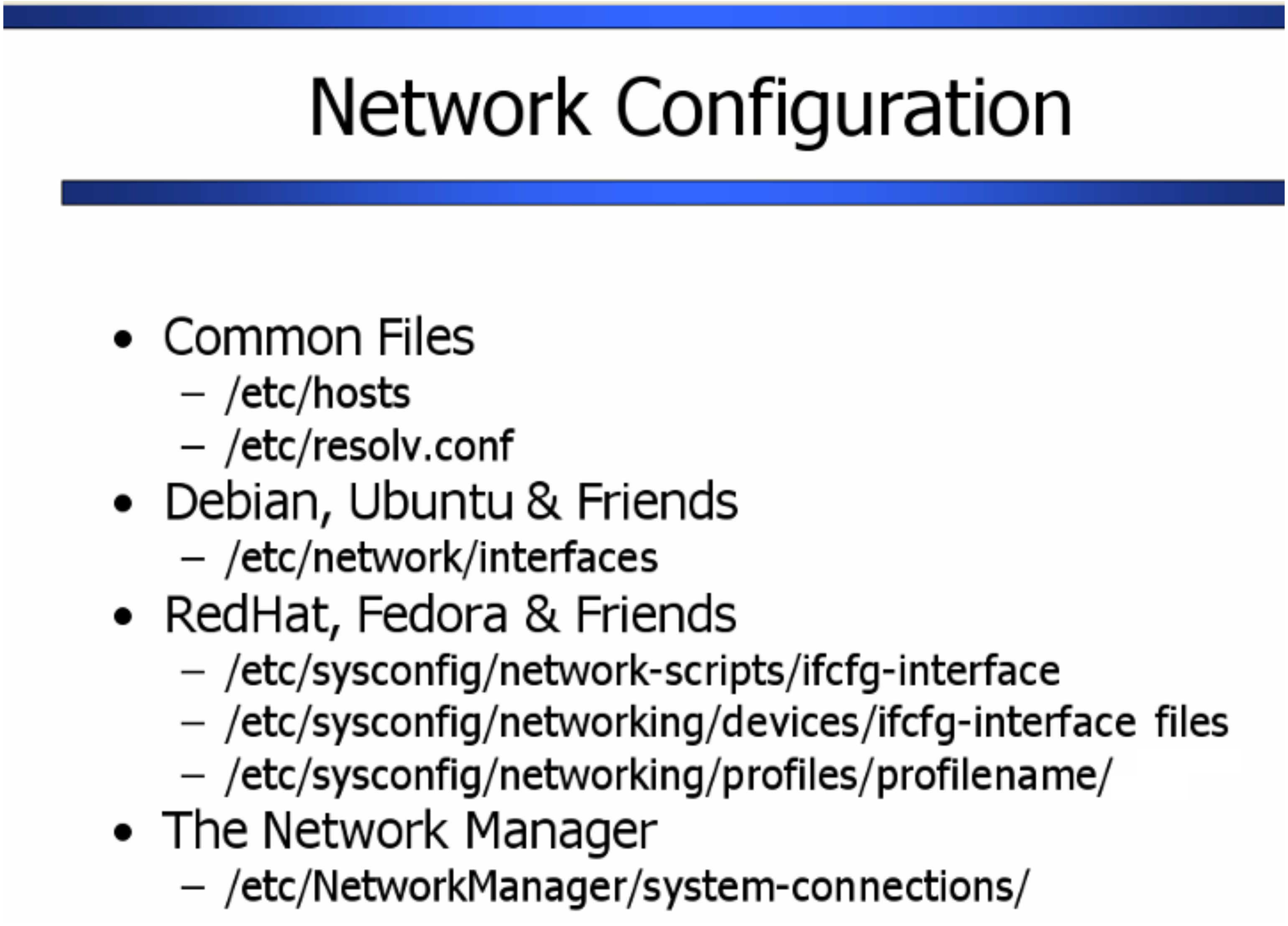
Digital Forensics

Forensic Response



Live Analysis

- Linux is hardware-swap friendly
  - Can easily analyze it live in the lab
- What to analyze
  - Network Configuration
  - Network Connections
  - Processes
  - User Activity
  - Open Files
  - Mounted Filesystems
  - The /proc Filesystem
    - cmdline, cpuinfo, diskstats, driver/rtc, filesystems, kallsyms (ksyms), kcore, modules, mounts, partitions, sys/, uptime, version, Process IDs, sysfs

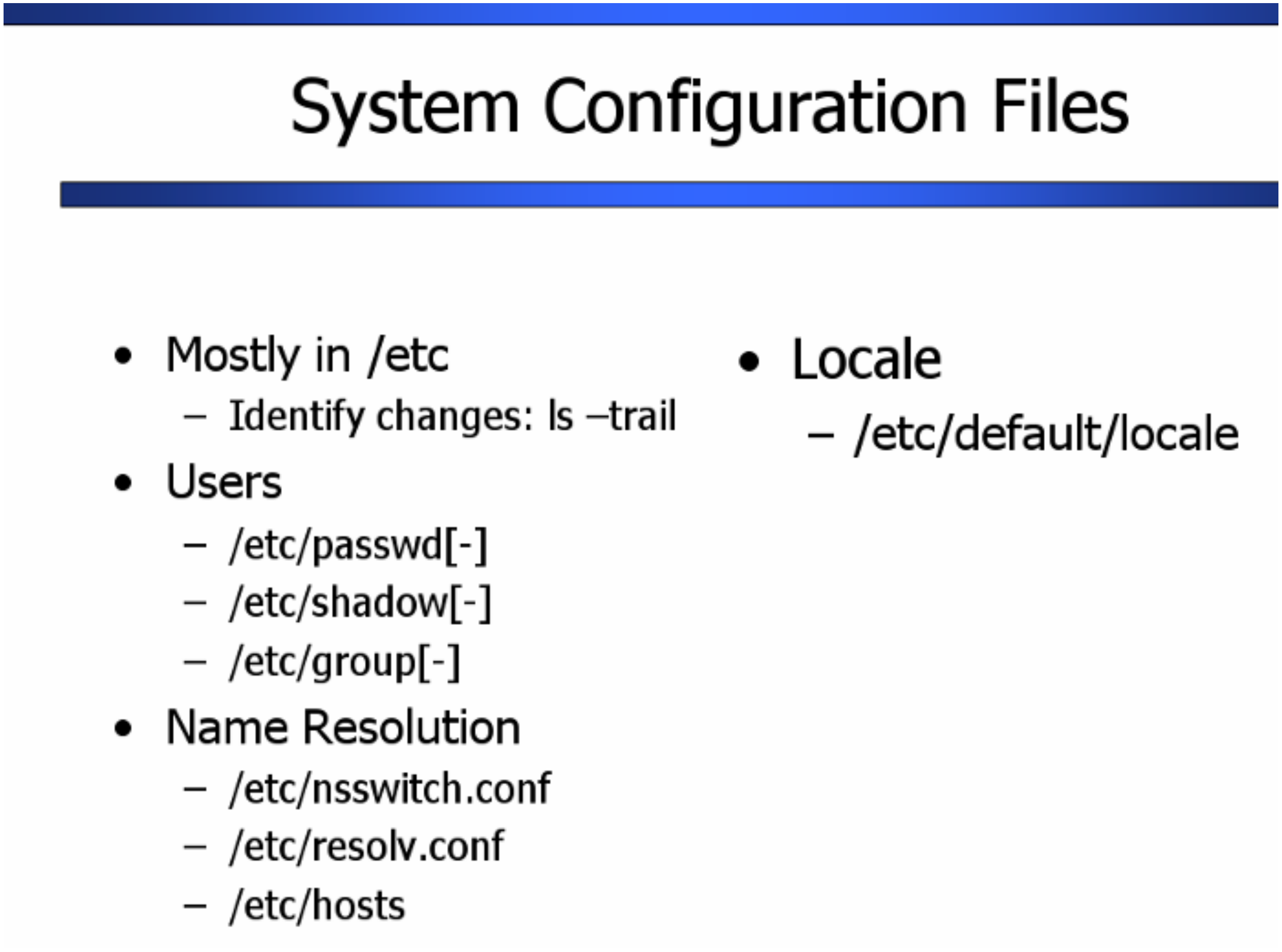


Network Configuration

- Common Files
  - /etc/hosts
  - /etc/resolv.conf
- Debian, Ubuntu & Friends
  - /etc/network/interfaces
- RedHat, Fedora & Friends
  - /etc/sysconfig/network-scripts/ifcfg-interface
  - /etc/sysconfig/networking/devices/ifcfg-interface files
  - /etc/sysconfig/networking/profiles/profilename/
- The Network Manager
  - /etc/NetworkManager/system-connections/

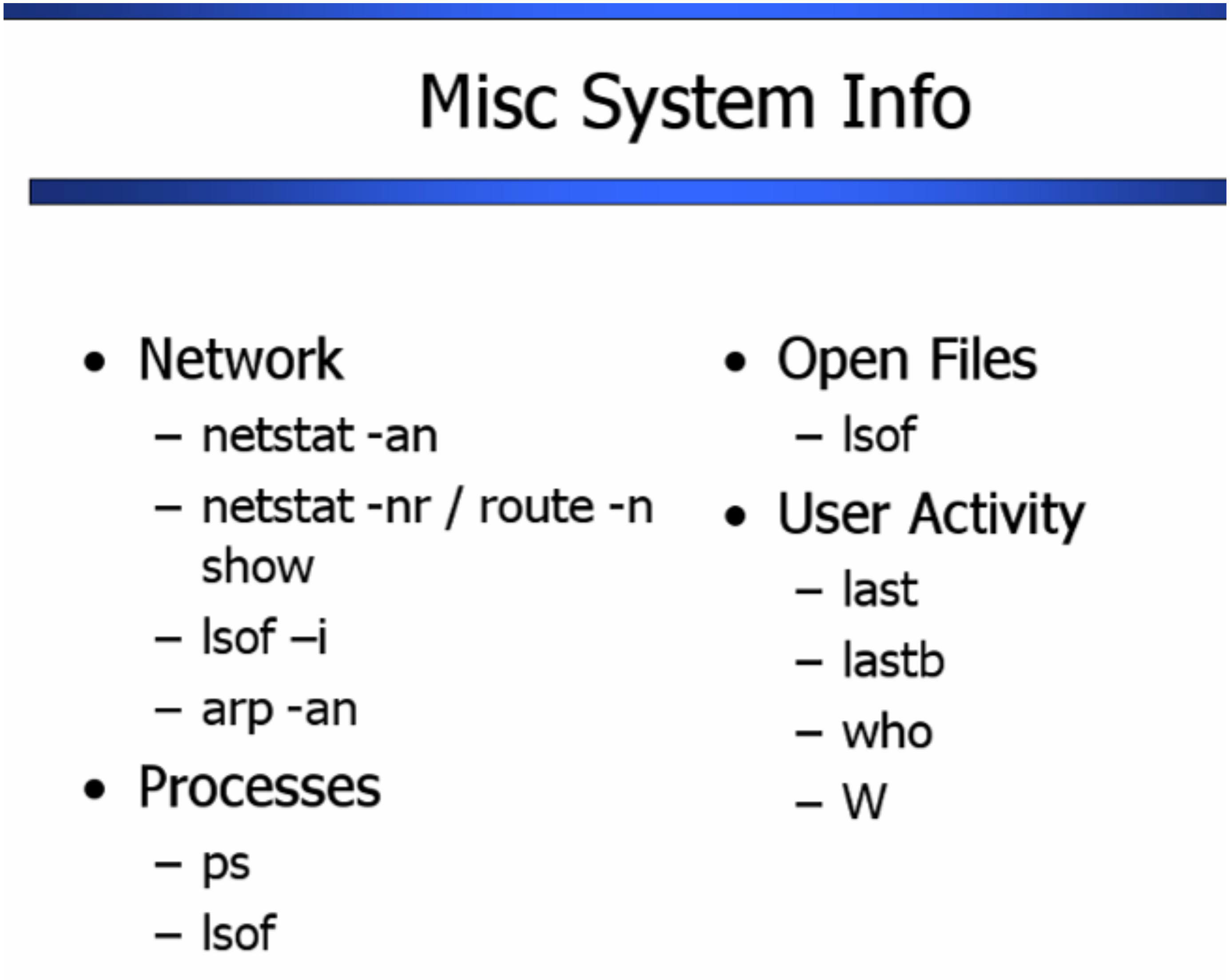
Digital Forensics

Linux Forensics



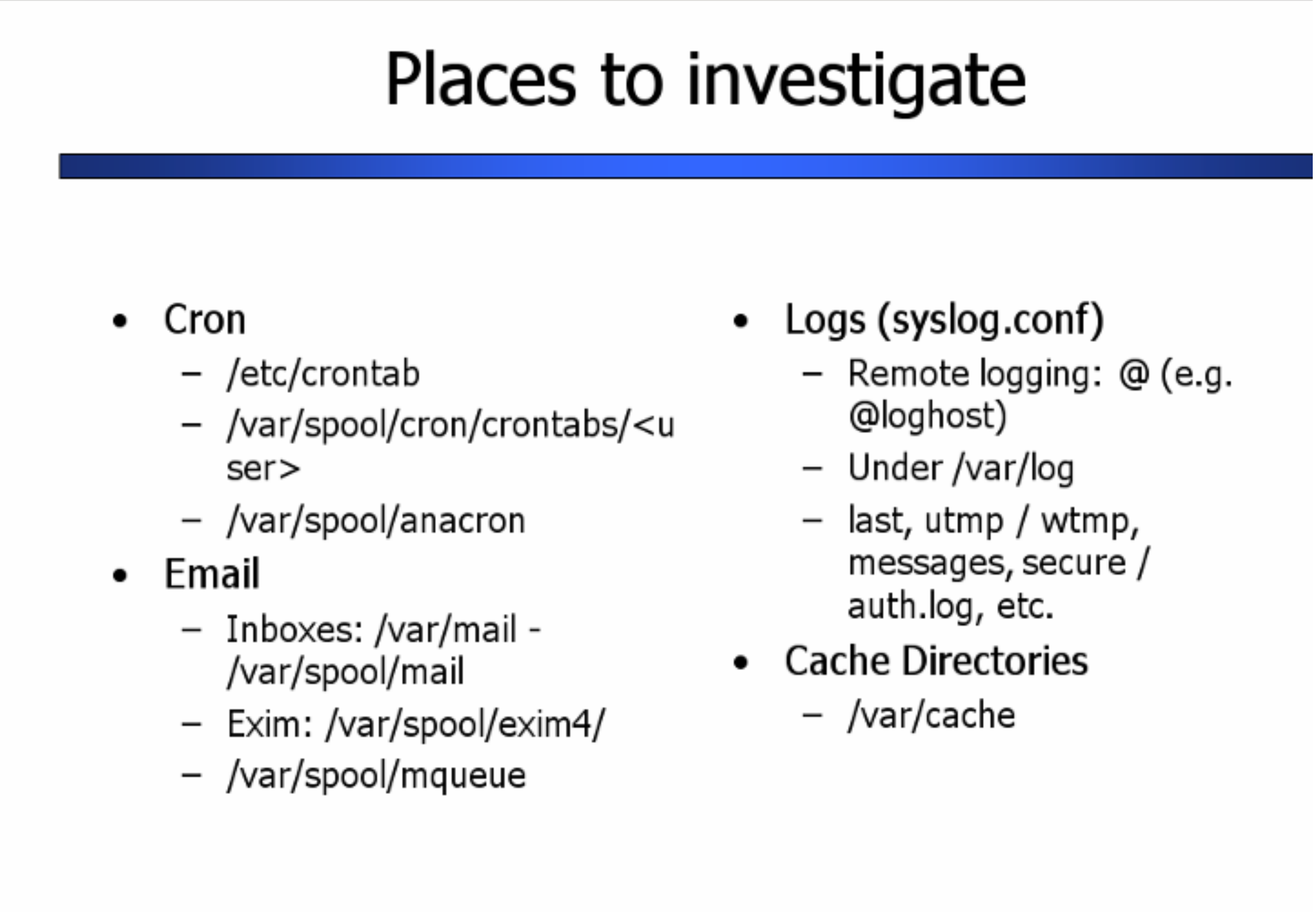
System Configuration Files

- Mostly in /etc
  - Identify changes: ls –trail
- Users
  - /etc/passwd[-]
  - /etc/shadow[-]
  - /etc/group[-]
- Name Resolution
  - /etc/nsswitch.conf
  - /etc/resolv.conf
  - /etc/hosts
- Locale
  - /etc/default/locale



Misc System Info

- Network
  - netstat -an
  - netstat -nr / route -n show
  - lsof –i
  - arp -an
- Processes
  - ps
  - lsof
- Open Files
  - lsof
- User Activity
  - last
  - lastb
  - who
  - W

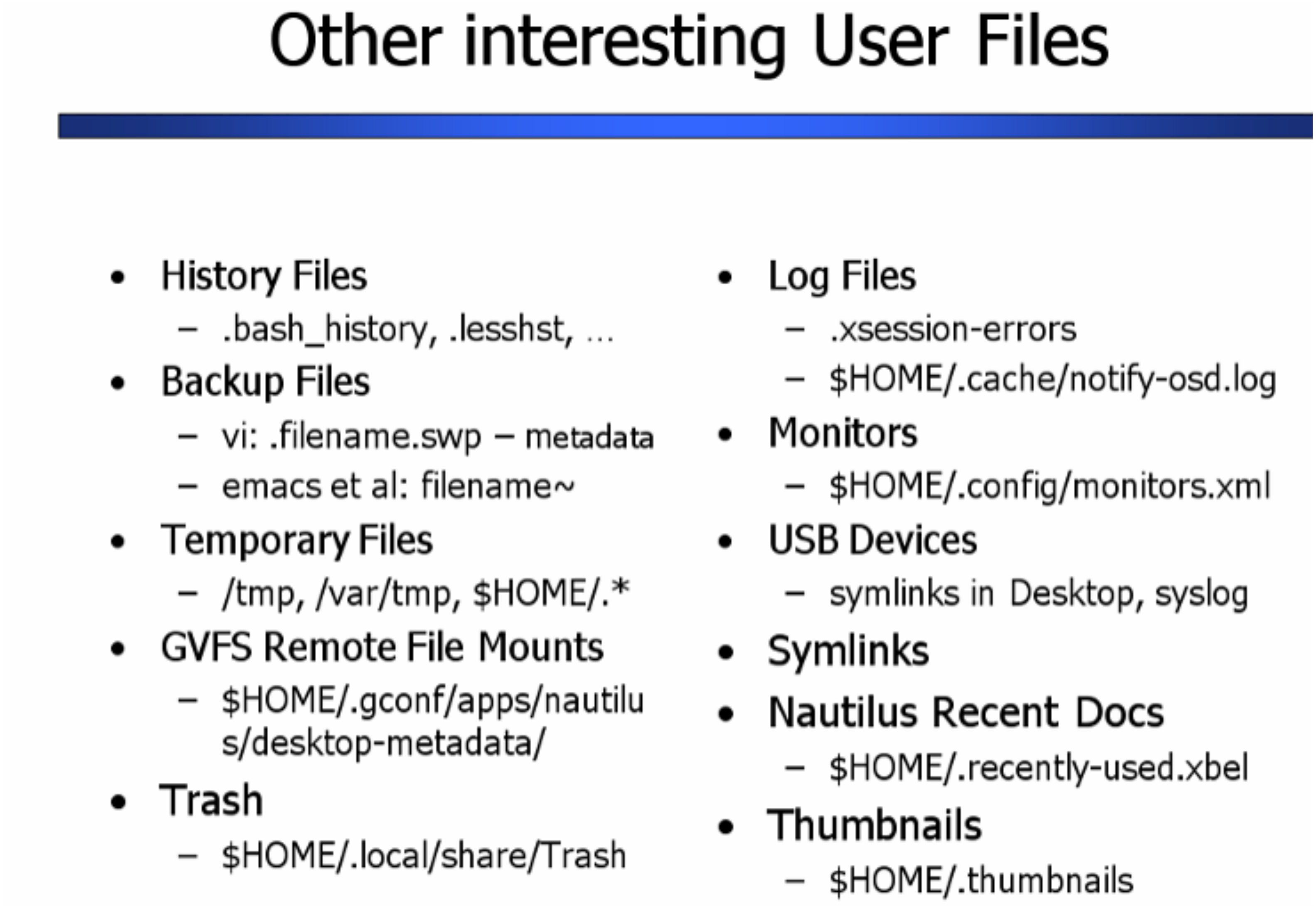


Places to investigate

- Cron
  - /etc/crontab
  - /var/spool/cron/crontabs/<user>
  - /var/spool/anacron
- Email
  - Inboxes: /var/mail - /var/spool/mail
  - Exim: /var/spool/exim4/
  - /var/spool/mqueue
- Logs (syslog.conf)
  - Remote logging: @ (e.g. @loghost)
  - Under /var/log
  - last, utmp / wtmp, messages, secure / auth.log, etc.
- Cache Directories
  - /var/cache

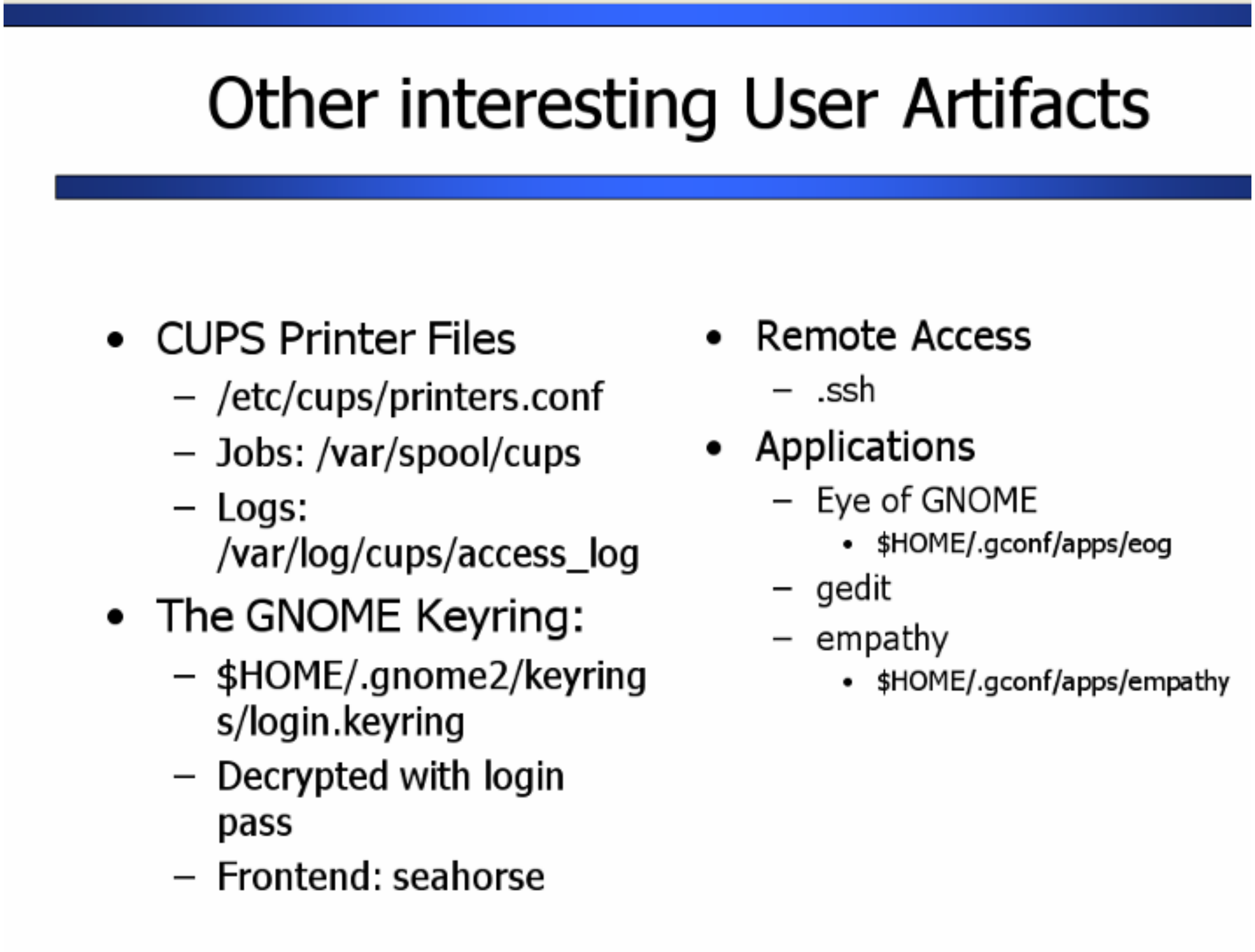
Digital Forensics

Linux Forensics



Other interesting User Files

- History Files
  - .bash_history, .lesshst, …
- Backup Files
  - vi: .filename.swp – metadata
  - emacs et al: filename~
- Temporary Files
  - /tmp, /var/tmp, $HOME/.*
- GVFS Remote File Mounts
  - $HOME/.gconf/apps/nautilus/desktop-metadata/
- Trash
  - $HOME/.local/share/Trash
- Log Files
  - .xsession-errors
  - $HOME/.cache/notify-osd.log
- Monitors
  - $HOME/.config/monitors.xml
- USB Devices
  - symlinks in Desktop, syslog
- Symlinks
- Nautilus Recent Docs
  - $HOME/.recently-used.xbel
- Thumbnails
  - $HOME/.thumbnails

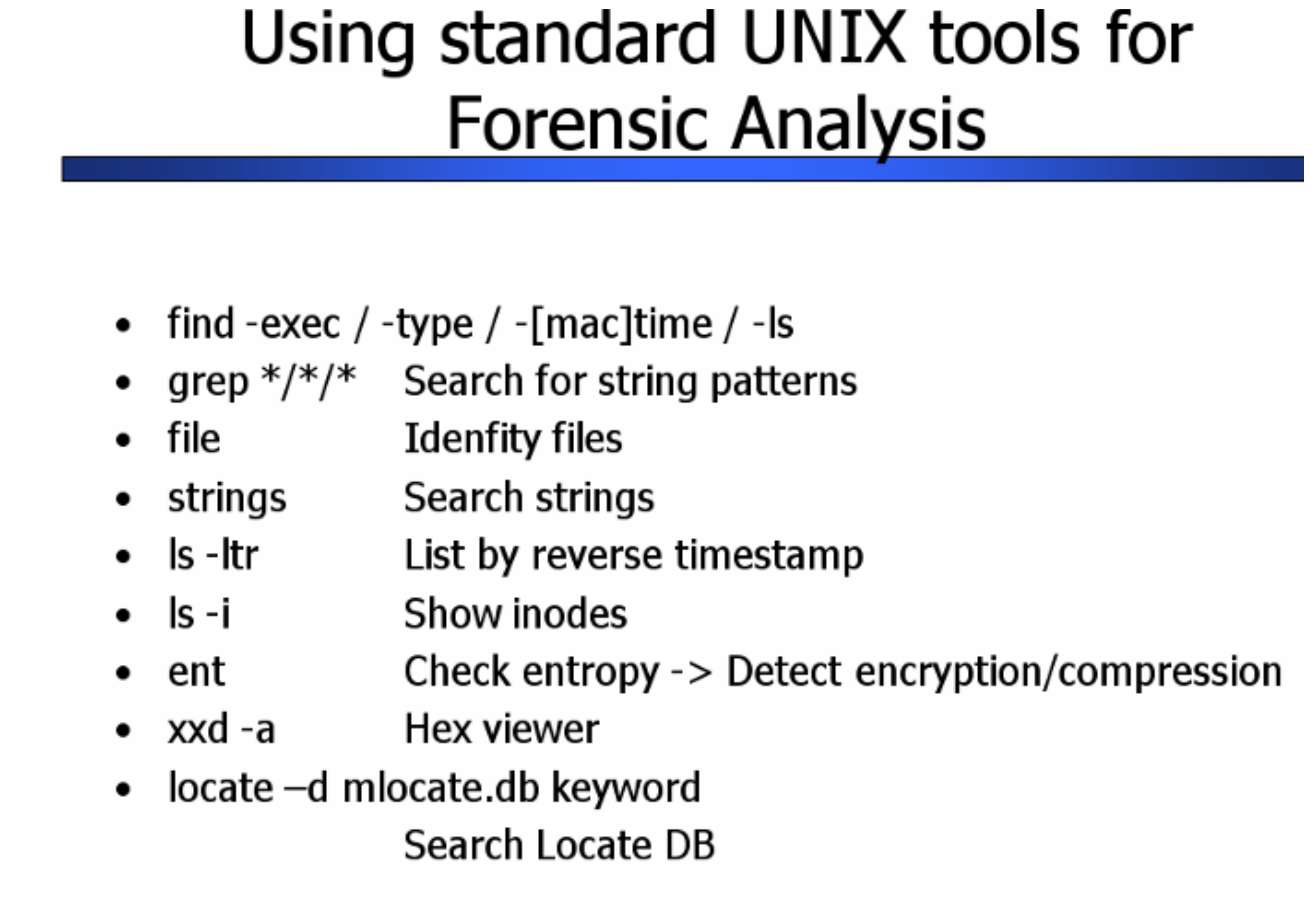


Other interesting User Artifacts

- CUPS Printer Files
  - /etc/cups/printers.conf
  - Jobs: /var/spool/cups
  - Logs: /var/log/cups/access_log
- The GNOME Keyring:
  - $HOME/.gnome2/keyrings/login.keyring
  - Decrypted with login pass
  - Frontend: seahorse
- Remote Access
  - .ssh
- Applications
  - Eye of GNOME
    - $HOME/.gconf/apps/eog
  - gedit
  - empathy
    - $HOME/.gconf/apps/empathy

Digital Forensics

Linux Forensics



Using standard UNIX tools for Forensic Analysis

• find -exec / -type / -[mac]time / -ls	
• grep */*/*	Search for string patterns
• file	Idenfity files
• strings	Search strings
• ls -ltr	List by reverse timestamp
• ls -i	Show inodes
• ent	Check entropy -> Detect encryption/compression
• xxd -a	Hex viewer
• locate –d mlocate.db keyword	
	Search Locate DB

Digital Forensics

Forensics Response

Offline forensics

- Hidden files
- Slack space
- Swap file
- Index.dat files
- Unallocated clusters
- Unused partitions
- Hidden partitions
- Registry settings
- Event logs
- Alternative data streams

Digital Forensics

What are Alternative Data Streams?

Making ADS files:

Create file with notepad ads.txt

Add some text and save

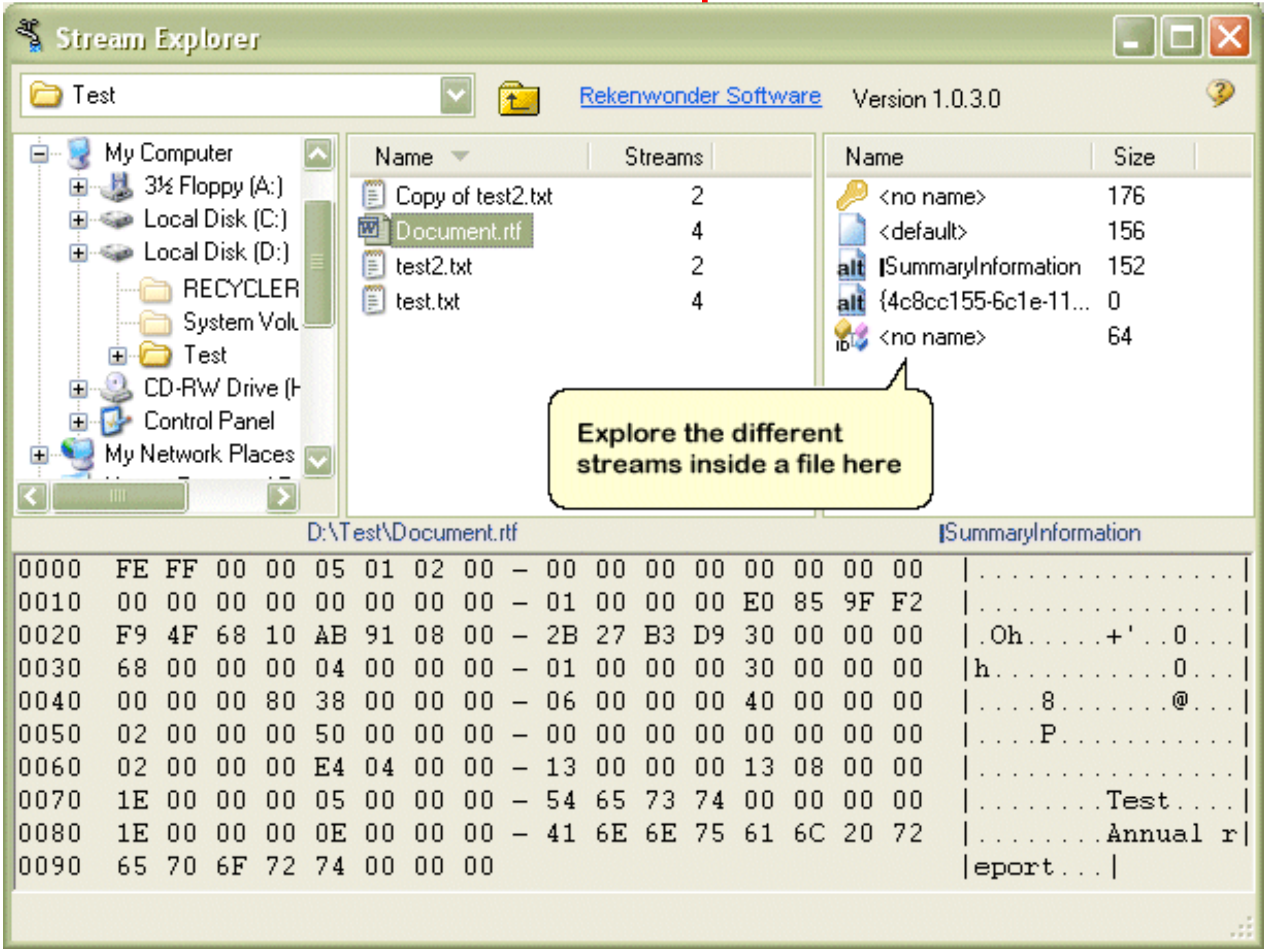
Add ADS notepad ads.txt:hidden.txt

- Size of ads.txt will not change and hidden.txt will not show up in directory
- Moving the file to another volume moves both frontend file and hidden file
- View ADS with Stream Explorer – rekenwonder software

- Http://www.sandersonforensics.com/Files/ZoneIdentifier.pdf

Digital Forensics

View ADS with Stream Explorer – rekenwonder software



Name	Streams
Copy of test2.txt	2
Document.rtf	4
test2.txt	2
test.txt	4

Name	Size
<no name>	176
<default>	156
♣SummaryInformation	152
{4c8cc155-6c1e-11...	0
<no name>	64

Explore the different streams inside a file here

D:\Test\Document.rtf

♣SummaryInformation

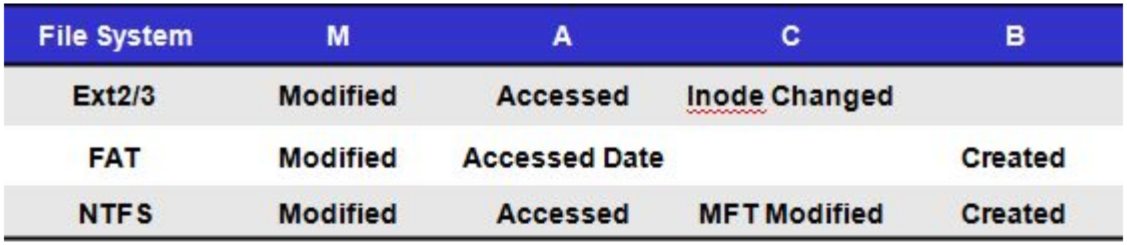
```
0000  FE FF 00 00 05 01 02 00 - 00 00 00 00 00 00 00 00  |................|
0010  00 00 00 00 00 00 00 00 - 01 00 00 00 E0 85 9F F2  |................|
0020  F9 4F 68 10 AB 91 08 00 - 2B 27 B3 D9 30 00 00 00  |.Oh.....+'..0...|
0030  68 00 00 00 04 00 00 00 - 01 00 00 00 30 00 00 00  |h...........0...|
0040  00 00 00 80 38 00 00 00 - 06 00 00 00 40 00 00 00  |....8.......@...|
0050  02 00 00 00 50 00 00 00 - 00 00 00 00 00 00 00 00  |....P...........|
0060  02 00 00 00 E4 04 00 00 - 13 00 00 00 13 08 00 00  |................|
0070  1E 00 00 00 05 00 00 00 - 54 65 73 74 00 00 00 00  |........Test....|
0080  1E 00 00 00 0E 00 00 00 - 41 6E 6E 75 61 6C 20 72  |........Annual r|
0090  65 70 6F 72 74 00 00 00                            |eport...|
```

Digital Forensics

Filesystem Timestamps

Timeline analysis essentially takes the metadata time values for each existing and unallocated metadata structure in the file system and sorts it, in order from earliest to most recent, to be analyzed.

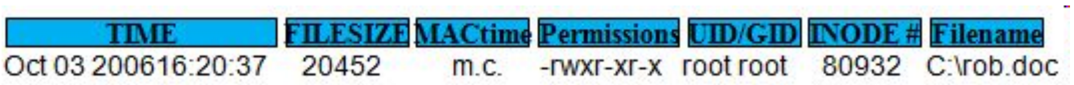
Timeline Data is based off of the timestamps stored in the metadata of the filesystem. Here are the timestamps stored for some of the most common filesystems you might encounter:



File System	M	A	C	B
Ext2/3	Modified	Accessed	Inode Changed	
FAT	Modified	Accessed Date		Created
NTFS	Modified	Accessed	MFT Modified	Created

Once a timeline is created, it will be sorted based off of the above timestamp data into a file.

Each line will have an output that will include the majority of the metadata associated with it.



TIME	FILESIZE	MACtime	Permissions	UID/GID	INODE #	Filename
Oct 03 200616:20:37	20452	m.c.	-rwxr-xr-x	root root	80932	C:\rob.doc

Digital Forensics

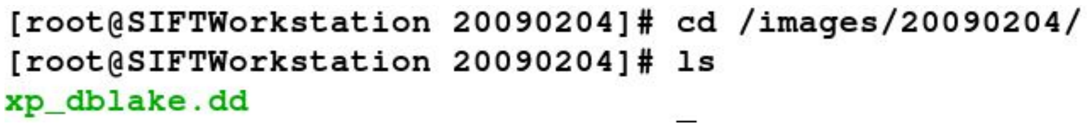
Timeline Analysis

The overall goal is to create a timeline of registry, file system, and other time stamped data. This combination makes a very powerful analysis mechanism for examining changes to the system around a specific time of activity on a machine.

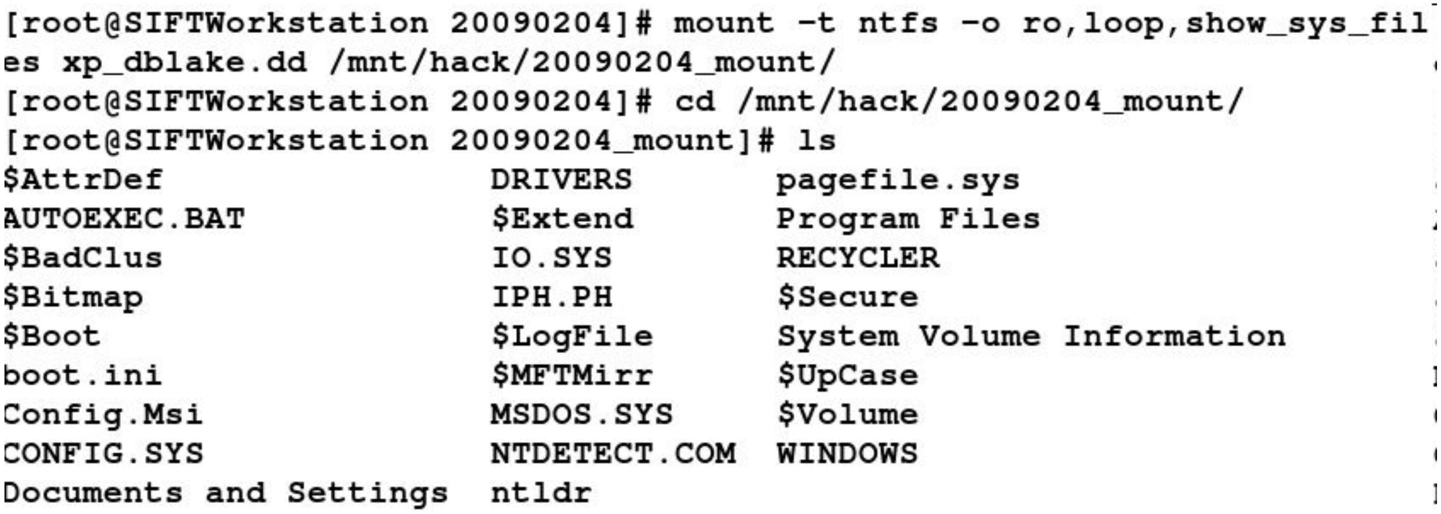
First of all we will start with a filesystem image that was acquired. This is our working copy image that is in raw (dd) format. This can come from running the actual dd command or more likely from a tool like FTK imager.

mount –t ntfs –o ro,loop,show_sys_files xp_dblake.dd /mnt/hack/20090204_mount/

In this case, the name of the file is xp_dblake.dd acquired in the 20090204 case following the YYYYMMDD case name example.   Our NTFS Raw (dd) Image



```
[root@SIFTWorkstation 20090204]# cd /images/20090204/
[root@SIFTWorkstation 20090204]# ls
xp_dblake.dd
```



```
[root@SIFTWorkstation 20090204]# mount -t ntfs -o ro,loop,show_sys_fil
es xp_dblake.dd /mnt/hack/20090204_mount/
[root@SIFTWorkstation 20090204]# cd /mnt/hack/20090204_mount/
[root@SIFTWorkstation 20090204_mount]# ls
$AttrDef                 DRIVERS        pagefile.sys
AUTOEXEC.BAT             $Extend        Program Files
$BadClus                 IO.SYS         RECYCLER
$Bitmap                  IPH.PH         $Secure
$Boot                    $LogFile       System Volume Information
boot.ini                 $MFTMirr       $UpCase
Config.Msi               MSDOS.SYS      $Volume
CONFIG.SYS               NTDETECT.COM   WINDOWS
Documents and Settings   ntldr
```

Digital Forensics

Using Log2timeline

log2timeline tool will parse all of the following data structures and more through *AUTOMATICALLY* recursing through the directories for you instead of having to manually accomplish this.

Artifacts Automatically Parsed in a SUPER Timeline:

apache2_access - Parse the content of a Apache2 access log file
apache2_error - Parse the content of a Apache2 error log file
chrome - Parse the content of a Chrome history file
evt - Parse the content of a Windows 2k/XP/2k3 Event Log
evtx - Parse the content of a Windows Event Log File (EVTX)
exif - Extract metadata information from files using ExifTool
ff_bookmark - Parse the content of a Firefox bookmark file
firefox2 - Parse the content of a Firefox 2 browser history
firefox3 - Parse the content of a Firefox 3 history file
iehistory - Parse the content of an index.dat file containing IE history
iis - Parse the content of a IIS W3C log file
isatxt - Parse the content of a ISA text export log file
mactime - Parse the content of a body file in the mactime format
mcafee - Parse the content of a log file
opera - Parse the content of an Opera's global history file
oxml - Parse the content of an OpenXML document (Office 2007 documents)

Digital Forensics

Using Log2timeline

log2timeline tool will parse all of the following data structures and more through *AUTOMATICALLY* recursing through the directories for you instead of having to manually accomplish this.

More Artifacts Automatically Parsed in a SUPER Timeline:

pcap - Parse the content of a PCAP file
pdf - Parse some of the available PDF document metadata
prefetch - Parse the content of the Prefetch directory
recycler - Parse the content of the recycle bin directory
restore - Parse the content of the restore point directory
setupapi - Parse the content of the SetupAPI log file in Windows XP
sol - Parse the content of a .sol (LSO) or a Flash cookie file
squid - Parse the content of a Squid access log (http_emulate off)
syslog - Parse the content of a Linux Syslog log file
tln - Parse the content of a body file in the TLN format
userassist - Parses the NTUSER.DAT registry file
volatility - Parse the content of a Volatility output files (psscan2, sockscan2, ...)
win_link - Parse the content of a Windows shortcut file (or a link file)
wmiprov - Parse the content of the wmiprov log file
xpfirewall - Parse the content of a XP Firewall log

Digital Forensics

Using Log2timeline

Once your images are collected, run the log2timeline command with options for the timezone, image filenames or partition filenames:

```
# log2timeline –z <timezone> -p <partition #> -i <image>
```

Additional Options:

-w Use if image is a Windows 7 system otherwise it defaults to WinXP

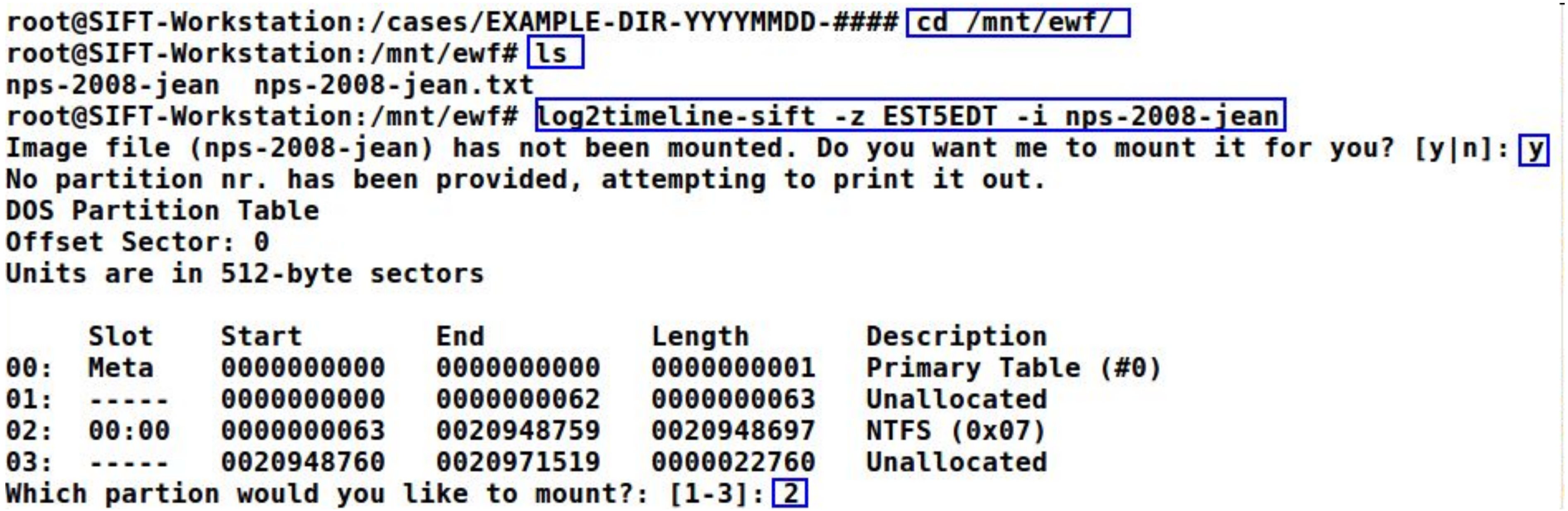
-o <type> List the partition # to parse, use 0 if partition image

Note: -z option is used to baseline convert time data stored in local time to UTC time.
IT SHOULD be the timezone of the SYSTEM being analyzed.

Digital Forensics

Using Log2timeline

When you run log2timeline on an image file, if it is not mounted, it will first ask you if you want to mount it and follow up with asking which specific partition needs to be mounted to have **log2timeline** parse:



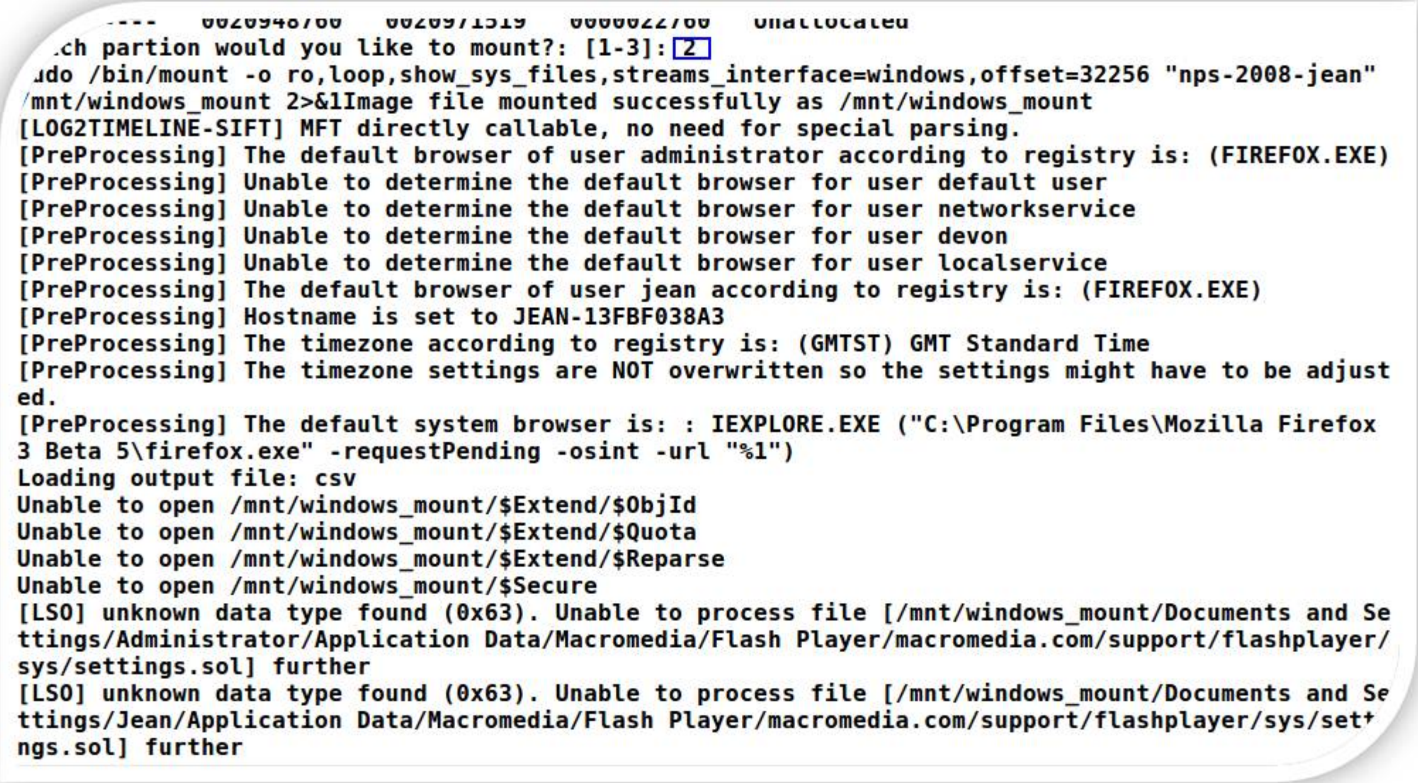
```
root@SIFT-Workstation:/cases/EXAMPLE-DIR-YYYYMMDD-#### cd /mnt/ewf/
root@SIFT-Workstation:/mnt/ewf# ls
nps-2008-jean  nps-2008-jean.txt
root@SIFT-Workstation:/mnt/ewf# log2timeline-sift -z EST5EDT -i nps-2008-jean
Image file (nps-2008-jean) has not been mounted. Do you want me to mount it for you? [y|n]: y
No partition nr. has been provided, attempting to print it out.
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0020948759   0020948697   NTFS (0x07)
03:  -----   0020948760   0020971519   0000022760   Unallocated
Which partion would you like to mount?: [1-3]: 2
```

Digital Forensics

Using Log2timeline

log2timeline will automatically parse through all of the structures to pull out a full timeline of the image.

Note that processing errors are normal and expected as the tool will attempt to look for structures that may or may not exist.

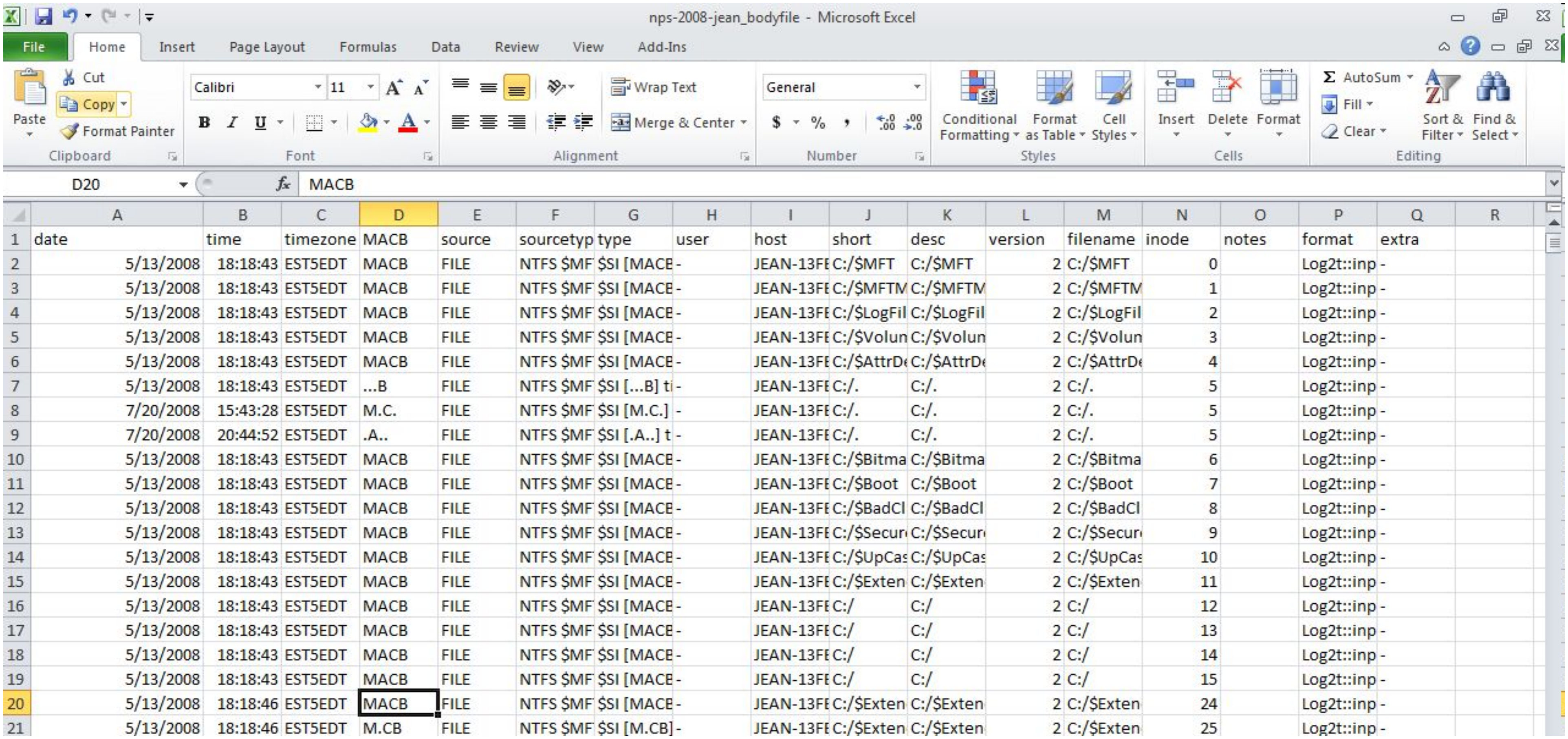


```
 ----   0020948760   0020971519   0000022760   Unallocated
ch partion would you like to mount?: [1-3]: 2
udo /bin/mount -o ro,loop,show_sys_files,streams_interface=windows,offset=32256 "nps-2008-jean"
/mnt/windows_mount 2>&1Image file mounted successfully as /mnt/windows_mount
[LOG2TIMELINE-SIFT] MFT directly callable, no need for special parsing.
[PreProcessing] The default browser of user administrator according to registry is: (FIREFOX.EXE)
[PreProcessing] Unable to determine the default browser for user default user
[PreProcessing] Unable to determine the default browser for user networkservice
[PreProcessing] Unable to determine the default browser for user devon
[PreProcessing] Unable to determine the default browser for user localservice
[PreProcessing] The default browser of user jean according to registry is: (FIREFOX.EXE)
[PreProcessing] Hostname is set to JEAN-13FBF038A3
[PreProcessing] The timezone according to registry is: (GMTST) GMT Standard Time
[PreProcessing] The timezone settings are NOT overwritten so the settings might have to be adjust
ed.
[PreProcessing] The default system browser is: : IEXPLORE.EXE ("C:\Program Files\Mozilla Firefox
3 Beta 5\firefox.exe" -requestPending -osint -url "%1")
Loading output file: csv
Unable to open /mnt/windows_mount/$Extend/$ObjId
Unable to open /mnt/windows_mount/$Extend/$Quota
Unable to open /mnt/windows_mount/$Extend/$Reparse
Unable to open /mnt/windows_mount/$Secure
[LSO] unknown data type found (0x63). Unable to process file [/mnt/windows_mount/Documents and Se
ttings/Administrator/Application Data/Macromedia/Flash Player/macromedia.com/support/flashplayer/
sys/settings.sol] further
[LSO] unknown data type found (0x63). Unable to process file [/mnt/windows_mount/Documents and Se
ttings/Jean/Application Data/Macromedia/Flash Player/macromedia.com/support/flashplayer/sys/sett
ngs.sol] further
```

Digital Forensics

Using Log2timeline

When analysis is complete, log2timeline writes an output file which can be parsed with other tools such as Sleuthkit, Forensic Tool Chest, Excel and some others.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	date	time	timezone	MACB	source	sourcetyp	type	user	host	short	desc	version	filename	inode	notes	format	extra	
2	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$MFT	C:/$MFT	2	C:/$MFT	0		Log2t::inp	-	
3	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$MFTM	C:/$MFTM	2	C:/$MFTM	1		Log2t::inp	-	
4	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$LogFil	C:/$LogFil	2	C:/$LogFil	2		Log2t::inp	-	
5	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Volun	C:/$Volun	2	C:/$Volun	3		Log2t::inp	-	
6	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$AttrDe	C:/$AttrDe	2	C:/$AttrDe	4		Log2t::inp	-	
7	5/13/2008	18:18:43	EST5EDT	...B	FILE	NTFS $MF	$SI [...B] ti	-	JEAN-13FE	C:/.	C:/.	2	C:/.	5		Log2t::inp	-	
8	7/20/2008	15:43:28	EST5EDT	M.C.	FILE	NTFS $MF	$SI [M.C.]	-	JEAN-13FE	C:/.	C:/.	2	C:/.	5		Log2t::inp	-	
9	7/20/2008	20:44:52	EST5EDT	.A..	FILE	NTFS $MF	$SI [.A..] t	-	JEAN-13FE	C:/.	C:/.	2	C:/.	5		Log2t::inp	-	
10	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Bitma	C:/$Bitma	2	C:/$Bitma	6		Log2t::inp	-	
11	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Boot	C:/$Boot	2	C:/$Boot	7		Log2t::inp	-	
12	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$BadCl	C:/$BadCl	2	C:/$BadCl	8		Log2t::inp	-	
13	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Secur	C:/$Secur	2	C:/$Secur	9		Log2t::inp	-	
14	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$UpCas	C:/$UpCas	2	C:/$UpCas	10		Log2t::inp	-	
15	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Exten	C:/$Exten	2	C:/$Exten	11		Log2t::inp	-	
16	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/	C:/	2	C:/	12		Log2t::inp	-	
17	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/	C:/	2	C:/	13		Log2t::inp	-	
18	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/	C:/	2	C:/	14		Log2t::inp	-	
19	5/13/2008	18:18:43	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/	C:/	2	C:/	15		Log2t::inp	-	
20	5/13/2008	18:18:46	EST5EDT	MACB	FILE	NTFS $MF	$SI [MACB	-	JEAN-13FE	C:/$Exten	C:/$Exten	2	C:/$Exten	24		Log2t::inp	-	
21	5/13/2008	18:18:46	EST5EDT	M.CB	FILE	NTFS $MF	$SI [M.CB]	-	JEAN-13FE	C:/$Exten	C:/$Exten	2	C:/$Exten	25		Log2t::inp	-	

Digital Forensics

File System Layers

Physical Layer – drive itself

File System Layer – Partition information, boot block, MBR, superblock

Data Layer – where data is stored in blocks or clusters

Metadata Layer – structure information such as EXT2/3/4, NTFS, FAT, directories, timestamps

- NTFS MFT – includes access control list, ACL
- iNode entry – including security access list
- File Allocation Table (FAT) directory entry
- File size

File Name Layer – name of the file

- MFT entry
- FAT entry

Digital Forensics

Filesystem Analysis

The **Sleuthkit utilities** installed in the SANS SIFT kit can process data in the filesystem, metadata and data layer of the filesystem.

mmls – list partitions of an image file where file is an entire drive (all sectors)

```
# mmls –t dos SDcard.dd
slot        Start(skip=)          End        Length(count=)        Description
02          000000063          001028159    0001028097              FAT32
```

Use the **dd** to carve out single partition from full image, SDcard.dd

```
# dd if=SDcard.dd bs=512 skip=63 count=1028097  of=imagefile.partion1.img
```

fsstat – list file system information on an image file of a single partition (NTFS, FAT, EXT2/3, etc.)

fls –m C: -r xp_dblake.dd   -- list filenames and timestamps from a disk image

srch_strings –t d imagefile.dd > imagefile.ascii.str   - dump all strings from an image into a text file

blkls imagefile.dd > unallocated_imagefile.blkls   -creates a new disk image of only the unallocated
data blocks from a full disk image (this contains *deleted* data and free blocks)

blkls –s imagefile.dd > imagefile.slack   - create image of only the *slack* space from a full image

Digital Forensics

Filesystem Analysis

The **Sleuthkit utilities** installed in the SANS SIFT kit can process data in the filesystem, metadata and data layer of the filesystem.

blkcat - display bytes of a disk block

blkstat - display block status, allocated or unallocated

ils - display inode details

ils imagefile.dd

istat - display information about a specific inode

icat - display contents of blocks allocated to an inode

ifind - determine which inode contains a specified block

ifind imagefile.dd –d block_num

ffind - find the filename that is using the inode

ffind imagefile.dd inode_num

Digital Forensics

Registry times

Creating Timeline of Registry Hives

regtime.pl is a tool that was created by Harlan Carvey and can be found in the SANS SIFT Workstation to parse the registry and pull all of the last write times from every key.
It will output in the sleuthkit "bodyfile" format that can be added to the filesystem bodyfile or analyzed separately using the **mactime** tool.

```
# perl regtime.pl —m hivename —r hivefile > bodyfile
```

[Useful Options]

-r Registry hive file to parse
-m Name of for Mactime Bodyfile

Example hivename: HKLM-SAM, HKEY-USER-NAME

The benefits of identifying when specific keys are last updated and comparing that to what is occurring on the filesystem is a very informative investigative technique.

You can use this to easily identify when files are saved, USB keys are inserted, programs are executed and more.

Digital Forensics

Registry times

Remember where the Windows registry hives are stored on the windows filesystem?

The regtime.pl program will require you to point the (-r) option at the specific registry hive you would like to parse.

-m HKLM-SAM | HKLM-SYSTEM | HKLM-SECURITY | HKLM-SOFTWARE | HKUSER-USER-username

Remember, HKEY_LOCAL_MACHINE hives are located in

```
C:\WINDOWS\system32\config\SECURITY
C:\WINDOWS\system32\config\SAM
C:\WINDOWS\system32\config\SYSTEM
C:\WINDOWS\system32\config\SOFTWARE
```

The HKEY-USER hives are located in C:\Users\ *username* \NTUSER.DAT

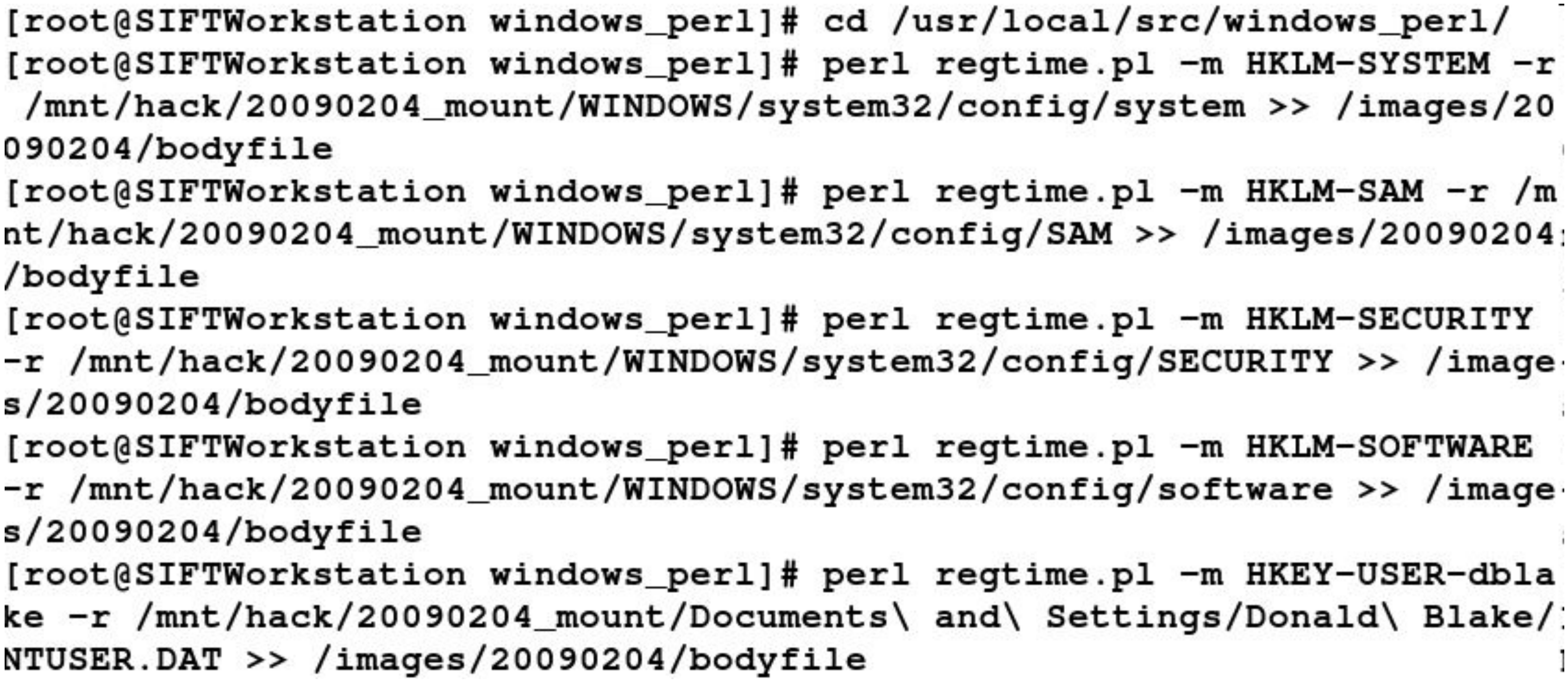
Digital Forensics

Registry times

This is an example of using regtime.pl to pull bodyfile data from the core HKEY_LOCAL_MACHINE hives (system, SAM, SECURITY, software) located in /WINDOWS/system32/config/ directory.

Notice how in each execution it is appending to the existing bodyfile using the (>>) as a part of the command. Each of the 4 core hives and the user hive (NTUSER.dat) will be added to the overall bodyfile located in this example in /images/20090204/bodyfile.

Adding Core Registry Hives and the User Hive to the Bodyfile



```
[root@SIFTWorkstation windows_perl]# cd /usr/local/src/windows_perl/
[root@SIFTWorkstation windows_perl]# perl regtime.pl -m HKLM-SYSTEM -r
 /mnt/hack/20090204_mount/WINDOWS/system32/config/system >> /images/20
090204/bodyfile
[root@SIFTWorkstation windows_perl]# perl regtime.pl -m HKLM-SAM -r /m
nt/hack/20090204_mount/WINDOWS/system32/config/SAM >> /images/20090204
/bodyfile
[root@SIFTWorkstation windows_perl]# perl regtime.pl -m HKLM-SECURITY
-r /mnt/hack/20090204_mount/WINDOWS/system32/config/SECURITY >> /image
s/20090204/bodyfile
[root@SIFTWorkstation windows_perl]# perl regtime.pl -m HKLM-SOFTWARE
-r /mnt/hack/20090204_mount/WINDOWS/system32/config/software >> /image
s/20090204/bodyfile
[root@SIFTWorkstation windows_perl]# perl regtime.pl -m HKEY-USER-dbla
ke -r /mnt/hack/20090204_mount/Documents\ and\ Settings/Donald\ Blake/
NTUSER.DAT >> /images/20090204/bodyfile
```

Digital Forensics

File Carving

Foremost - Locate files based on headers, footers and max length

```
foremost –o outputdir /path/to/foremost.conf  data_file.img
```

Scapel – automates some of the foremost processes

- uses same concepts as foremost

Bulk Extractor – find IP addresses, domain names, email addresses, credit card numbers, encryption keys and more

Digital Forensics

Memory Image Analysis

One source of memory images are the Windows crashdump and Linux coredump files.

Additional memory analysis tools:

PoolTools – PTfinder, poolgrep, poolfinder

Volatility - python scripts for analyzing raw memory captures for:
sockets, process list, semaphores, dll list, kernel modules, registry objects, file handles, dump a process

Memoryze – free memory analyzer - http://www.mandiant.com/products/free_software/memoryze/
Updated for all versions of Windows

Digital Forensics

Memory Image Analysis

What is possible with memory forensics?

- Enumerate all running processes (EXE and DLL) (including those hidden by rootkits).
- List all network sockets that the process has open, including any hidden by rootkits.
- Output all strings in memory on a per process basis.
- Identify all drivers loaded in memory, including those hidden by rootkits.

- Hashing the driver, exe or DLL and comparing with a clean system allows detection of rootkits or code injection by malware

- Output all strings in memory on a per driver base.
- Report device and driver layering, which can be used to intercept network packets, keystrokes and file activity.
- Identify all loaded kernel modules by walking a linked list.
- Identify hooks (often used by rootkits) in the System Call Table, the Interrupt Descriptor Tables (IDTs) and driver function tables (IRP tables).
- View video card memory images
- See passwords, encryption keys, web pages, clipboard contents, IM chat, and more

Network Forensics

Steps of Investigation

1. Identify sources of digital evidence
2. Preserve digital evidence
3. Identify tools and techniques to use
4. Process Data
5. Interpret analysis results

   If needed, collect more evidence and repeat
6. Report findings

Network Forensics

Identify sources of digital evidence

What forensic data do we have to work with?

- PCAP
- netflow
- logs (from security tools and applications logs - syslog)

Obtaining good logs – DNS, Firewall (blocks, drops, alerts, allows), Web history, Web server logs, DHCP logs, Web application logs, DB logs, Antivirus logs, Authentication logs (VPN, LDAP, Domain Controller), FTP logs, Email server logs

Where to capture traffic?

Hashing the PCAP, logs, etc. – if planning to work with law enforcement or e-discovery is likely

Network Forensics

3. Identify tools and techniques to use
4. Process Data
5. Interpret analysis results

If needed, collect more evidence and repeat

Prepare before the incident:

- What does your network look like? (baseline)
- What do attacks look like? (anomalies)

Malware incident – exploit kit, click fraud, ransomware

Email attack – phishing

Web Server Attack – word press plug-in scan and breach, shellshock

Data Exfiltration – database behind web server (Havij), FTP ex-fil?

Network Anomalies

- DDOS – DNS reflection, NTP reflection
- incoming requests for non-authoritative domains
- SYN flooding, HTTP flooding
- RST scanning, FIN scan, SYN scanning, ACK scanning, PING scan

Port scan/ port sweep

Network Forensics

Tools

Wireshark – packet analyzer

Bro – protocol analyzer, file extractor, logs most common protocols

SNORT – Intrusion Detection using Deep Packet Inspection

Tcpdump – packet capture and filtering

SiLK – netflow analysis tool

Logstash – log collector

Elastic Search – log search tool

Kibana – displays Elastic search results in tables, pie charts, time lines

Xplico – open source network forensics tool

NAFT – open source network appliance forensic tool

Network Miner – packet analyzer, protocol analyzer

Network Forensics

Findings

Who or what sent the packet / file / artifact?

Who or what received the packet / file / artifact?

Where did the packet / file / artifact come from?

- Logical network location, physical location

When was it sent?

What else happened around that time? at those locations?

Analyzing malware – VirusTotal, Total hash, Malwr.com, hybrid analysis

Does metadata or artifacts suggest connections to other events?

Network Forensics

Reporting

- How did it get compromised?
- When did it get compromised? Building a timeline (log2timeline tool?)
- Where did the attack come from?
- What did the user/application do with the item?