ITU Session Four:
Device Imaging And Analysis

Mounir Kamal
Q-CERT

Applying Forensic Science to Computer Systems

“Like a Detective, the archaeologist searches for clues in order to discover and reconstruct something that happened. Like the detective, the archaeologist founds no clues, too small or insignificant.

And like the detective, the archaeologist must usually work with fragmentary and often confusing information.

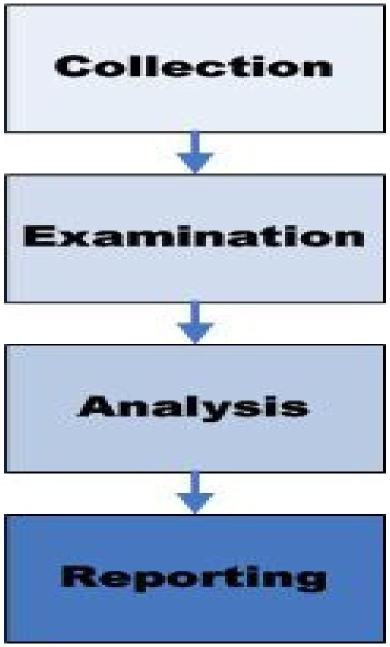
Finally, the detective and the archaeologist have their goal the completion of a report, base on a study of their clues, that not only tell us what happened but prove it.”

(1966 Meighan “Archaeology)

The Forensic Process

The nature of the electronic evidence is such that it poses special challenges for its admissibility in Court.

To meet these challenges, follow proper forensic procedures including and not limited to



Collection

Examination

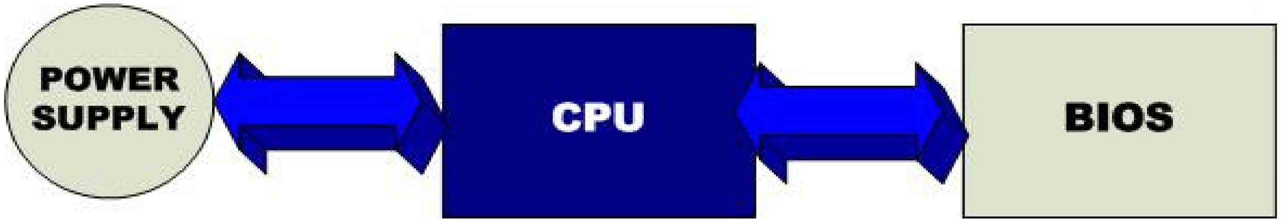
Analysis

Reporting

Central Processing Unit

The CPU is the Core of any Computer system, including all new devices especially the one we would like to Collect, Examine, or Analyze

- The first stage in the boot process is to get the CPU started
- With an electrical pulse coming from the power supply
- Once the CPU is started, it goes to the basic input and output system (BIOS)



POST and CMOS

-Bios contains a program called the power-on self test (POST).

-Post tests the fundamental components of the computer.

-Computers use CMOS RAM chips to retain the date, time, hard drives, and others

“When collecting digital evidence from a computer, it is often necessary to interrupt the boot process and examine the CMOS setting such as Date, Time, Hard Drive configuration, And Boot Sequence”

CASE EXAMPLE (UNITED STATES v. ZACARIAS MOUSSAOUI 2003

- During the trial of convicted terrorist Zacarias Moussaoui:
  - The laptop had lost all power including CMOS battery;
  - The government examined its contents, making it more difficult to authenticate the associated digital evidence;
  - The loss of all power means the original date and time can not be retrieved;
  - Nor the type of port and peripherals enabled;
  - And it lost the setting of hard disk parameters and the controller as well.

- Fortunately the CMOS settings were recorded when the laptop was originally processed by Secret Service Agency on SEP 11,2001 before the power was lost.

System Boot

- Operating System extends the functions of the BIOS, and acts as an interface between the computer and the outside world.
- The ability to prevent a computer from using the operating system on the hard disk is important when the disk contains evidence.

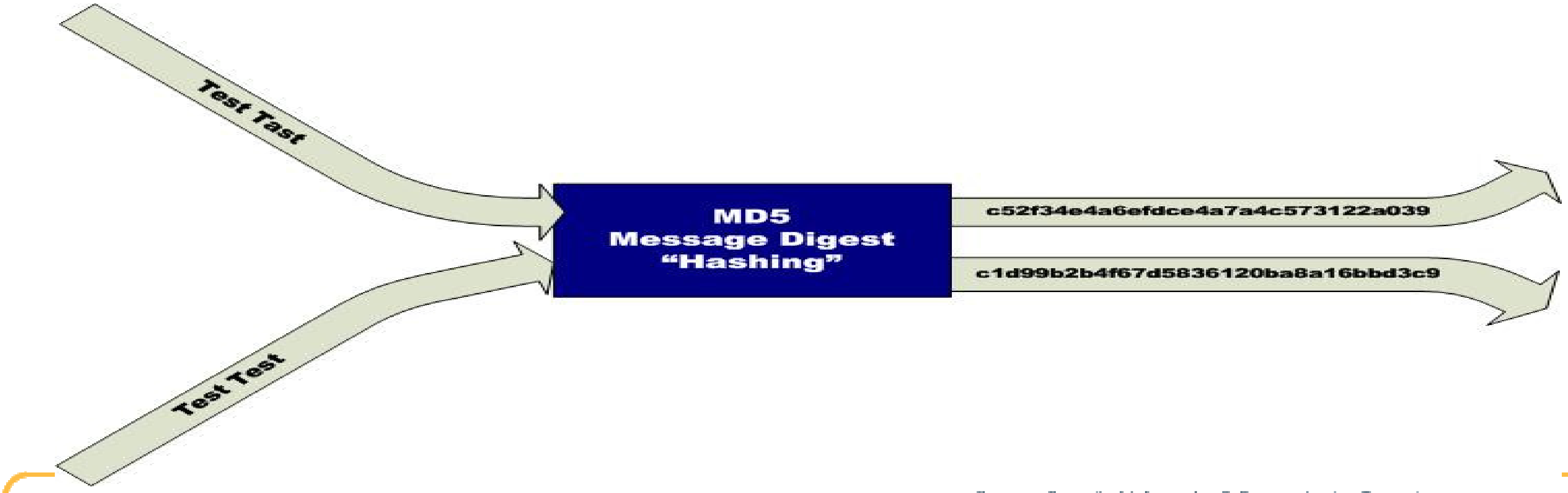
" Knowing How to Change The Boot Sequence of a Computer Before Power-on IS A MUST"

- In one case a technician was asked to note the system time of a computer before removing the hard disk. He booted and tried to interrupt the boot process to access the CMOS, not using the correct Hotkey. As a result, the system booted from the evidentiary hard drive, altering the date-time stamps of files

Cryptographic Hash Function

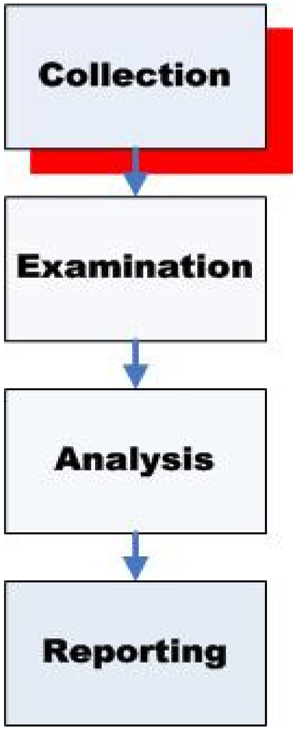
… is a Transformation that takes an input of string or message of any length and produce a fixed length string as output sometimes termed a message digest or a digital fingerprint.

This near uniqueness makes hashing algorithms like MD5 important tools for documenting Digital evidence.


Test Tast
Test Test
MD5
Message Digest
"Hashing"
c52f34e4a6efdce4a7a4c573122a039
c1d99b2b4f67d58361 20ba8a16bbd3c9

Collection and Preservation

The goal of digital preservation is to maintain the ability to display, retrieve, and use digital collections in the face of rapidly changing technological and organizational infrastructures and elements.



Collection

Examination

Analysis

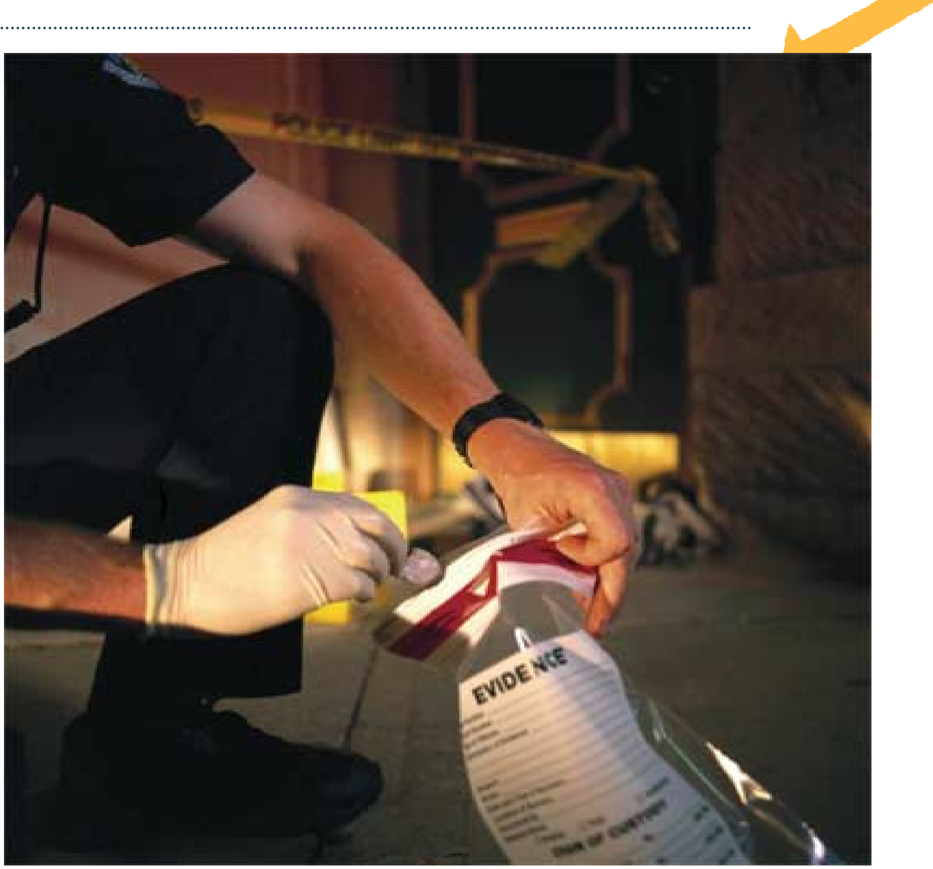
Reporting

CASE EXAMPLE

“In one homicide case, law enforcement seized the victim's computer but instead of treating it as they would any other piece of evidence, they placed the computer in an office, turned it on and operated it to see what they could find thus altering the system and potentially destroying useful date-time stamp information and other data. Additionally, they connected to the victim's Internet account, thus altering data on the e-mail server and creating log entries that alarmed other investigators because they did not know who had accessed the victim's account after her death.”

Collection Options

- Collect Hardware
- Collect all digital evidence, leave hardware
- Only collect the digital evidence that you need



Collect Hardware

- Relevant Cybercrime Categories
  - Hardware as Fruits of crimes
  - Hardware as instrumentality
  - Hardware as evidence
  - Hardware contains large amount of digital evidence
- Advantage
  - Requires little technical expertise
  - The method is relatively simple and less open to criticism
  - Hardware can be examined later in a controlled environment
  - Hardware is available for others to examine at a later date
- Disadvantage
  - Risks damaging the equipment in transit
  - Risks not being able to boot (BIOS password)
  - Risks not being able to access all evidence on the drive (e.g. EFS)
  - Risks liability for unnecessary disruption of business
  - Develops a bad reputation for heavy handedness
  - It will not be applicable in some cases like investigation of servers

Collection options

Collect All digital evidence, leave hardware

- Relevant Cybercrime Categories
  - Information as Fruits of crimes
  - Information as instrumentality
  - Information as evidence
- Advantage
  - Digital evidence can be examined later in a controlled environment
  - Working with a copy prevents damage of original evidence
  - Minimizes the risk of damaging hardware and disrupting business
- Disadvantage
  - Requires equipment and technical expertise
  - Risks not being able to access all evidence on the drive (e.g. EFS)
  - Risks missing evidence (Protected Area)
  - Risks destroying evidence (Content of RAM)
  - Time Consuming
  - Methods are more open to criticism than collecting hardware because more can go wrong

Collection options

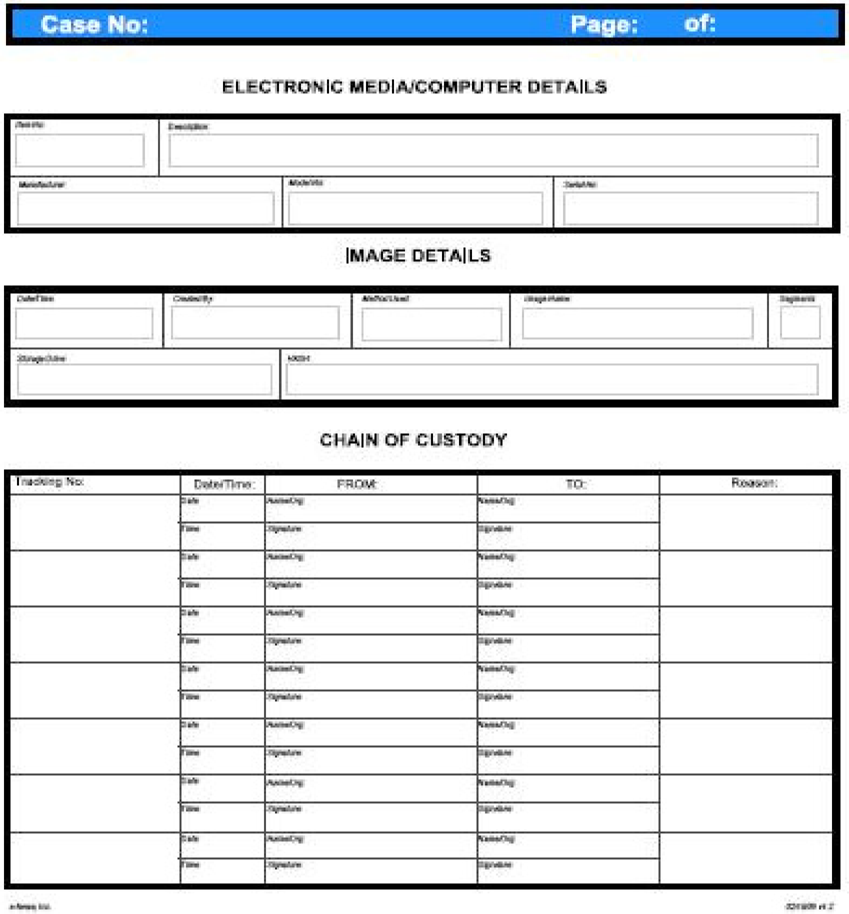
Only collect the digital evidence that you need

- Relevant Cybercrime Categories
  - Information as Fruits of crimes
  - Information as instrumentality
  - Information as evidence
- Advantage
  - Allows for a range of expertise
  - Can ask for help from system admin/owner
  - Quick and inexpensive
  - Avoids risks and liabilities of collecting hardware
- Disadvantage
  - Can miss or destroy evidence (e.g. rootkit)
  - Methods are most open to criticism because more can go wrong than collecting all of the evidence

Chain of Custody

- Refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence .

- For evidence to be used in court to convic persons of crimes, it must be handled in an intensively careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal.



Case No: **Page:** **of:**

ELECTRONIC MEDIA/COMPUTER DETAILS

Item No:	Description:	
Manufacturer:	Model No:	Serial No:

IMAGE DETAILS

Date/Time:	Created By:	Method Used:	Image Name:	Segments:
Storage Drive:	HASH:			

CHAIN OF CUSTODY

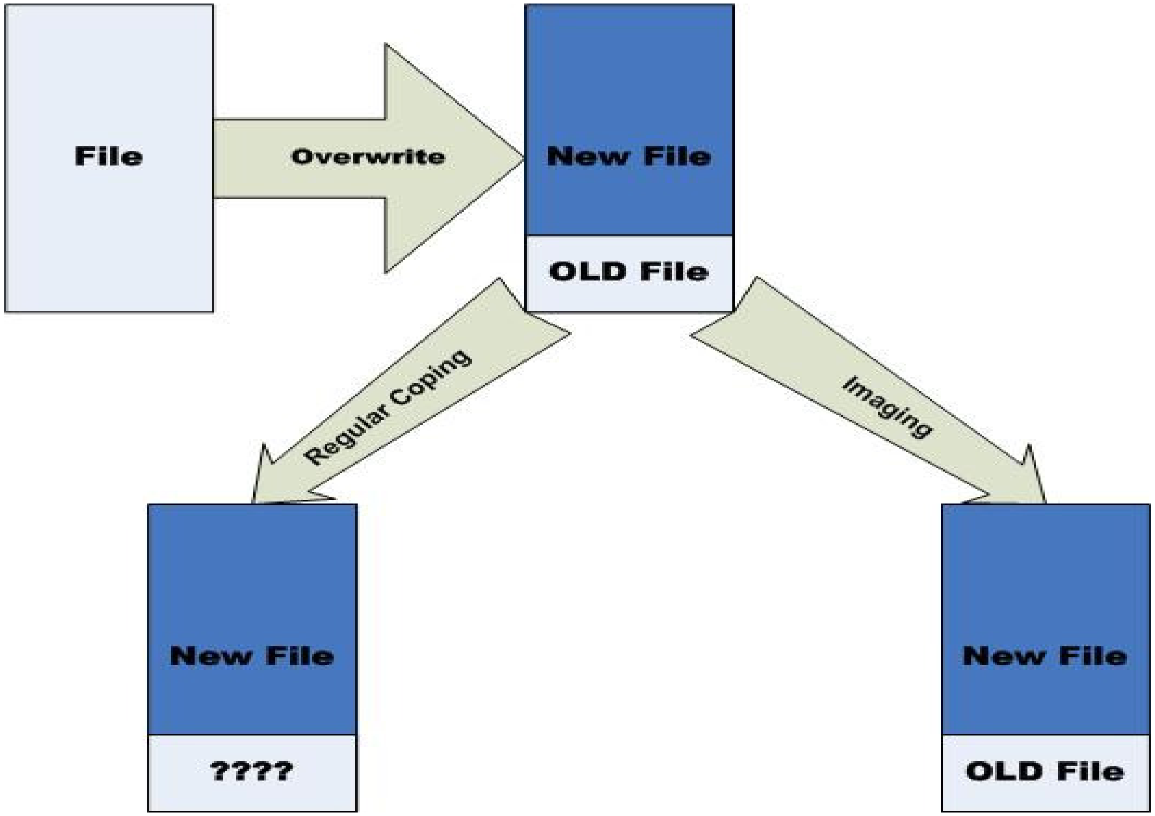
Tracking No:	Date/Time:	FROM:	TO:	Reason:
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	

CASE EXAMPLE

“A group of computer intruders gained unauthorized access to an IRIX server and used it to store stolen materials, including several credit card databases stolen from e-commerce Web sites. A system administrator made copies of the stolen materials along with log files and other items left by the intruders. The system administrator combined all of the files into a large compressed archive and transferred the archive, via the network, to a system with a CD-ROM burner. Unfortunately, the compressed archive file became corrupted in transit but this was not realized until the investigators attempted to open the archive at a later date. By this time, the original files had been deleted from the IRIX system. It was possible to recover some data from the archive file but not enough to build a solid case. ”

Preserving The Evidence

Bitstream Copying (Imaging) V. Regular Copying



Bitstream Copying (Forensic Image)

Bitstream copying duplicates everything in the cluster including anything that is in the slack space and unallocated space.

Important Rules when doing Forensic Image:

- Use a Write Blocker whenever you interact with the digital evidence
  - To be sure no alteration will be done to your evidence

- Hash digital evidence before imaging it
  - To verify the digital evidence imaging process

- Create at least two images from two different tools of the Digital Evidence
  - To make sure at least one of the images was successful

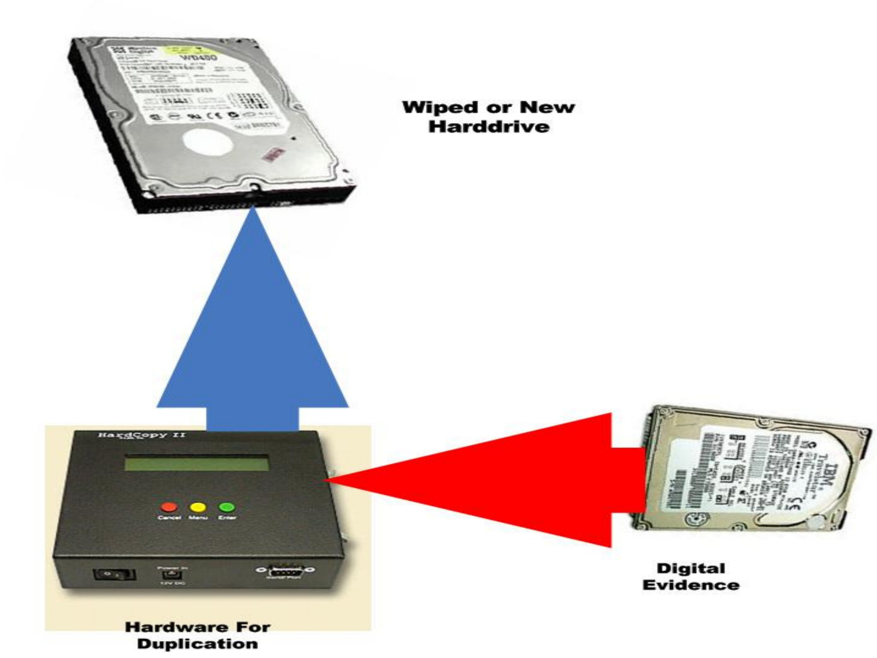
Imaging Computer Storage

Methods of imaging Computer Storage:

- Hardware Duplication Device
- Forensic Workstation
- Evidence Acquisition Boot Disk with direct device connected
- Evidence Acquisition Boot Disk with Network Connection

Hardware Duplication Device

- Images Drives up to 5.5 GB per minutes
- Stores entire images in single ISO file (DD type files)
- Hashing (MD5) to ease forensic validation Of the data
- Use specific converter to work with Image laptop drives or SATA drives



The Main benefit of Using Hardware Duplication Device is that It Cuts your Imaging Time In Half

Forensic Workstation

Forensic Workstation with Write Blocker Built-in

- Image a wide range of Harddisk Storage
- Use any imaging software like DD, Encase, FTK
- Use any Hashing algorithms you require

The main benefit of Using Forensic Workstation is flexibility

Video Clip

Write Blocker

Evidence Acquisition Boot Disk with direct device connected

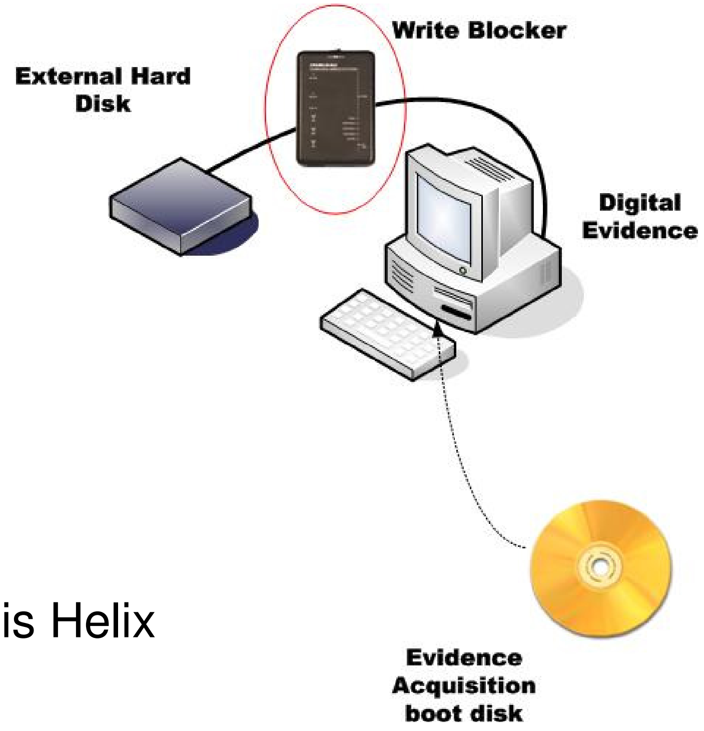
- Use any imaging software like DD, FTK imager

- Use any Hashing algorithms you required

- Use other forensic tools for fast investigation

- One of the best open source CDs to do these functions is Helix

- You do not need to open the digital evidence and remove the harddisk



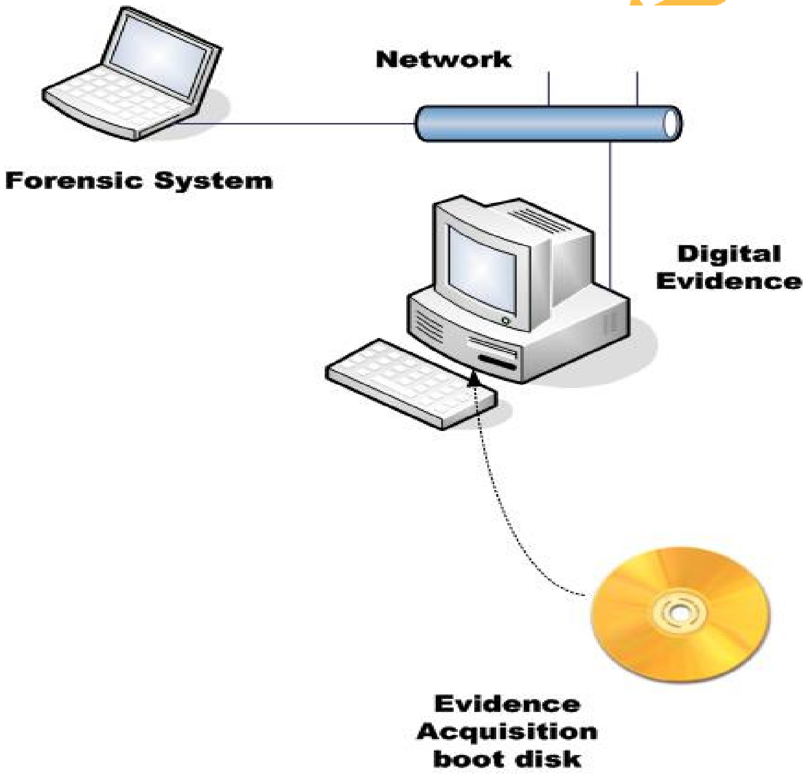
Evidence Acquisition Boot Disk with Network Connection

- Use any imaging software like DD, FTK imager

- Use any Hashing algorithms you required

- Use NetCat to transfer the Image from the evidence to the Forensic System

- You do not need to open the digital evidence and remove the harddisk



Evidence Acquisition- Others

In the Field of computer forensics, you deal with gathering digital evidence available in different types of devices such as

- Flash Memory
- CD/DVD
- PDA
- Mobile Phone
- iPod
- Printer
- Scanner
- Camera
- Fax Machine

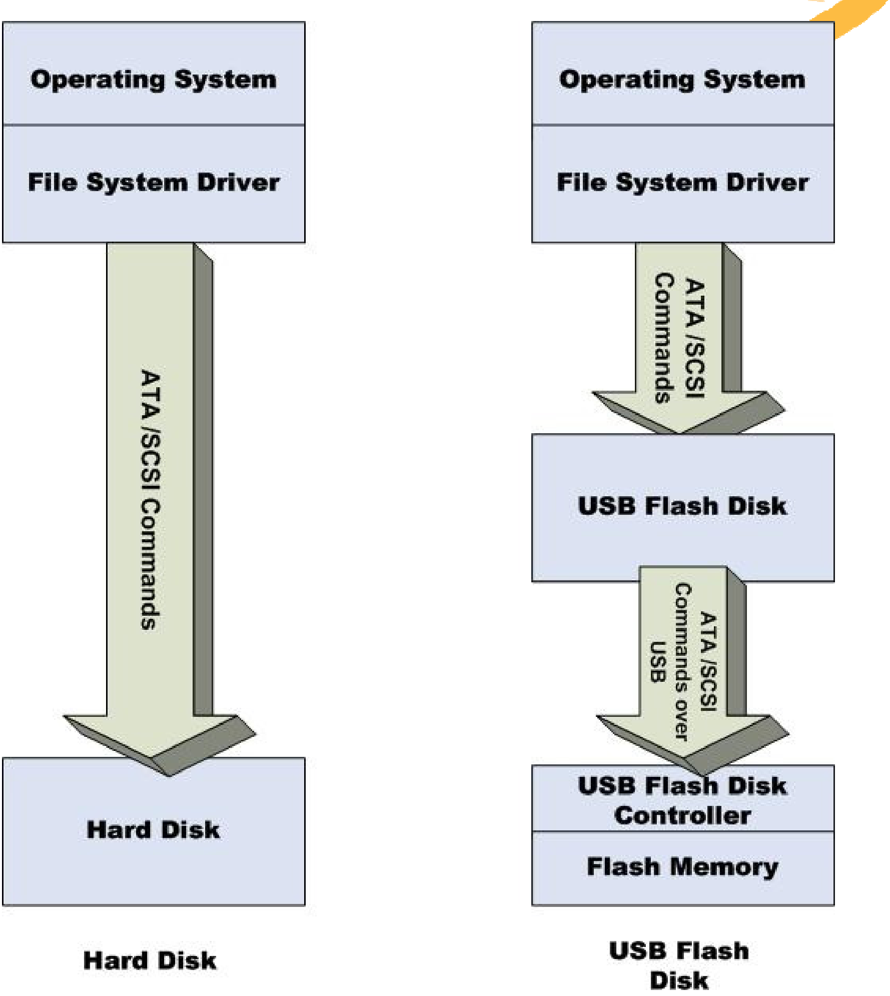
Evidence Acquisition- Flash Memory

How OS accesses Flash File Systems

-In Case of Hard disk the OS accesses the hard disk through File system Driver “FSD”. The FSD issues Commands to the hard disk for ATA command to read sector or logical block address.

-A USB flash disk presents itself to the OS as disk storage, then the FSD commands are channeled to the USB through the USB flash Disk, the USB flash controller interprets the access commands in flash memory.

-The LBA and ATA commands will not be the same as the physical address in a flash chip. The information for mapping an LBA to a Physical location is stored in the flash Memory.



Evidence Acquisition- Flash Memory

Tools used for Flash Memory acquisition

-DD Command

-Encase

-FTK imager

-Sleuth kit & Autopsy
(Open Source forensic tools)

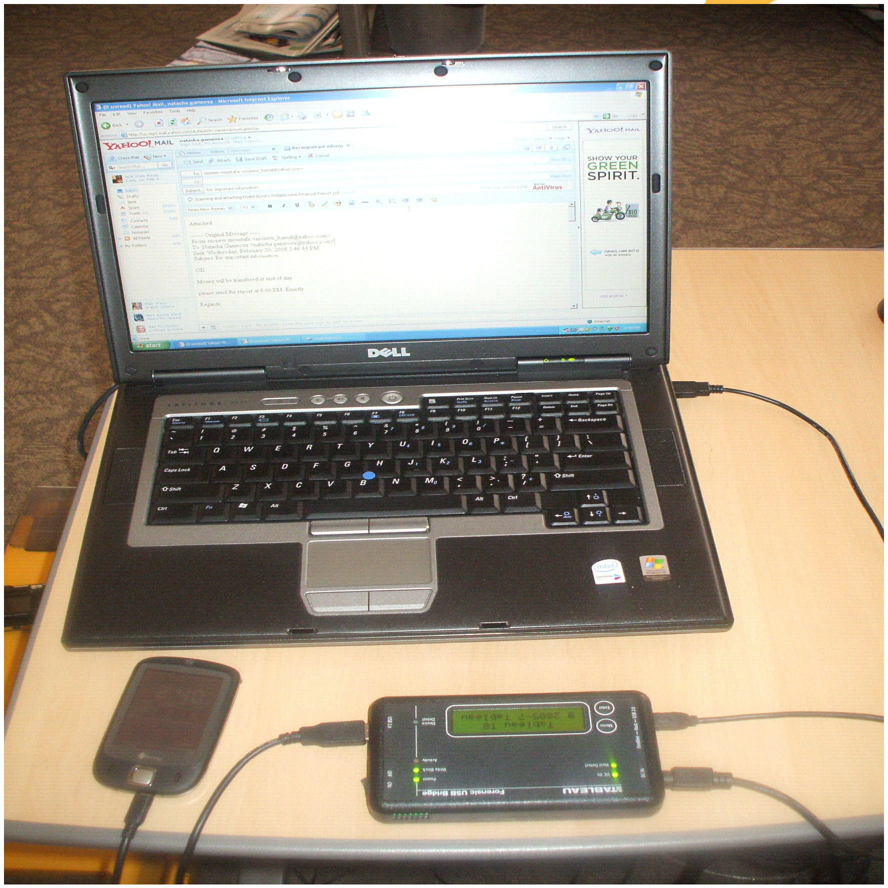
Notes: Write blocker must used when Imaging flash memory

Video Clip

Evidence Acquisition- PDA

- Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, WiFi, mobile phone, camera, global positioning system, basic computing capabilities, Internet etc.

- Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery operated and store data in volatile memory. A PDA is never really turned off as long as it has sufficient battery power. Evidence residing in PDA is highly volatile in nature.



Evidence Acquisition- PDA

Forensic tools acquire data from a PDA device in one of two ways:

Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a disk drive or RAM chip).

logical acquisition implies a bit-by-bit copy of logical storage objects (e.g. directories and files).

physical acquisition is preferable, since it allows any data remnants present (e.g., unallocated RAM or unused file system space) to be examined.

Some Tools Used in PDA Acquisition and Analysis:

- EnCase
- PDA Seizure
- Paraben for PDA
- POSE

Evidence Acquisition- Mobile Phone

- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

- Mobile Phone forensics includes the analysis of both SIMM and Phone Memory … each requires a separate procedure.

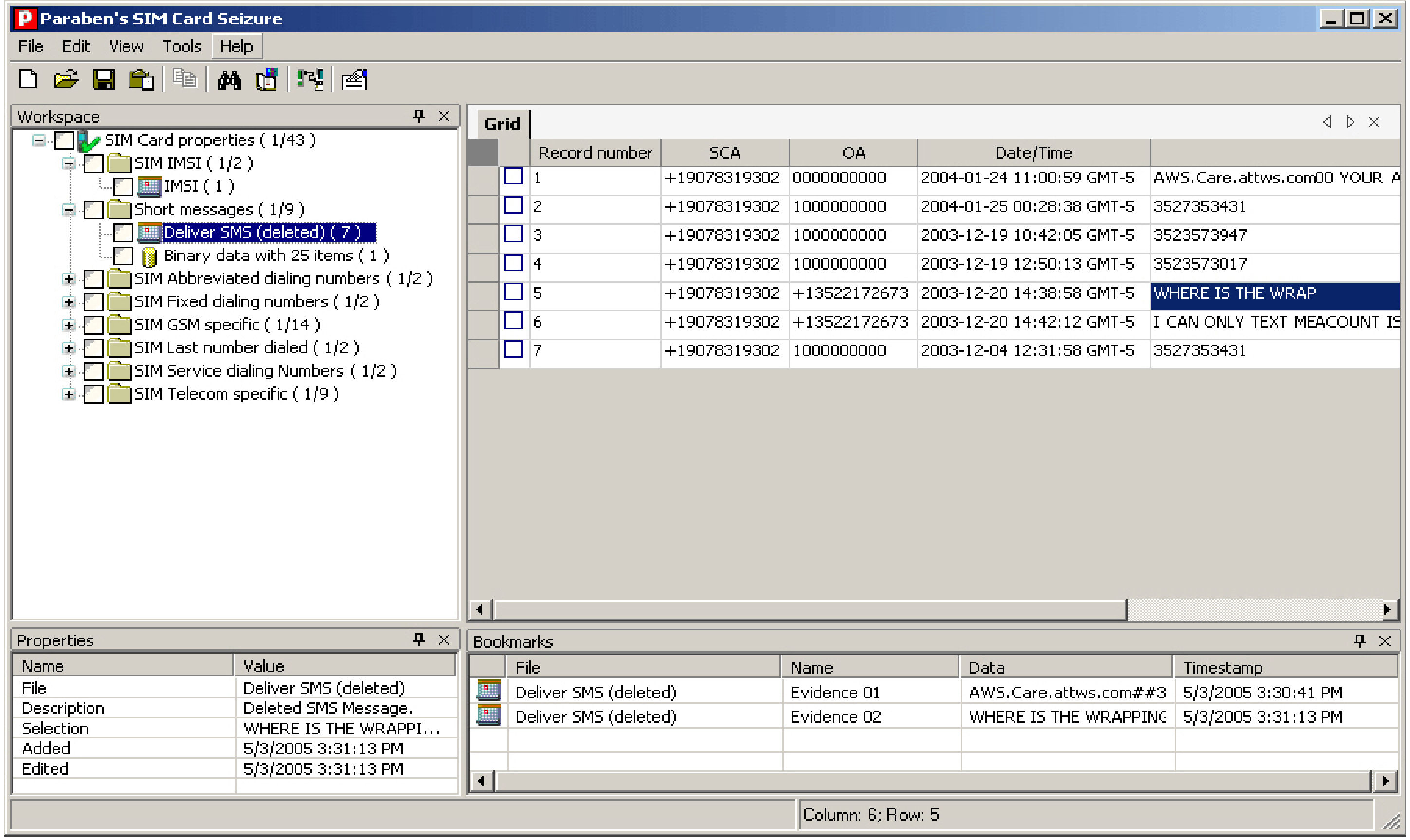
- Information Stored in Mobile Phone

  -Phone numbers and Addresses
  -Photo, Video, and Voice Records
  -SMS, MMS Messages and Emails
  -Notes
  -Meting Schedule and Tasks
  -Call Log

Evidence Acquisition- Mobile Phone

Some Tools Used in Mobile Phone Acquisition and Analysis:

-Oxygen
-Paraben
-Cell Seizure
-MOBILEedit!
-OPM
-TULP2G



Paraben's SIM Card Seizure

Workspace

- ☐ SIM Card properties (1/43)
  - ☐ SIM IMSI (1/2)
    - ☐ IMSI (1)
  - ☐ Short messages (1/9)
    - ☐ Deliver SMS (deleted) (7)
    - ☐ Binary data with 25 items (1)
  - ☐ SIM Abbreviated dialing numbers (1/2)
  - ☐ SIM Fixed dialing numbers (1/2)
  - ☐ SIM GSM specific (1/14)
  - ☐ SIM Last number dialed (1/2)
  - ☐ SIM Service dialing Numbers (1/2)
  - ☐ SIM Telecom specific (1/9)

Grid

	Record number	SCA	OA	Date/Time	
☐	1	+19078319302	0000000000	2004-01-24 11:00:59 GMT-5	AWS.Care.attws.com00 YOUR A
☐	2	+19078319302	1000000000	2004-01-25 00:28:38 GMT-5	3527353431
☐	3	+19078319302	1000000000	2003-12-19 10:42:05 GMT-5	3523573947
☐	4	+19078319302	1000000000	2003-12-19 12:50:13 GMT-5	3523573017
☐	5	+19078319302	+13522172673	2003-12-20 14:38:58 GMT-5	WHERE IS THE WRAP
☐	6	+19078319302	+13522172673	2003-12-20 14:42:12 GMT-5	I CAN ONLY TEXT MEACOUNT IS
☐	7	+19078319302	1000000000	2003-12-04 12:31:58 GMT-5	3527353431

Properties

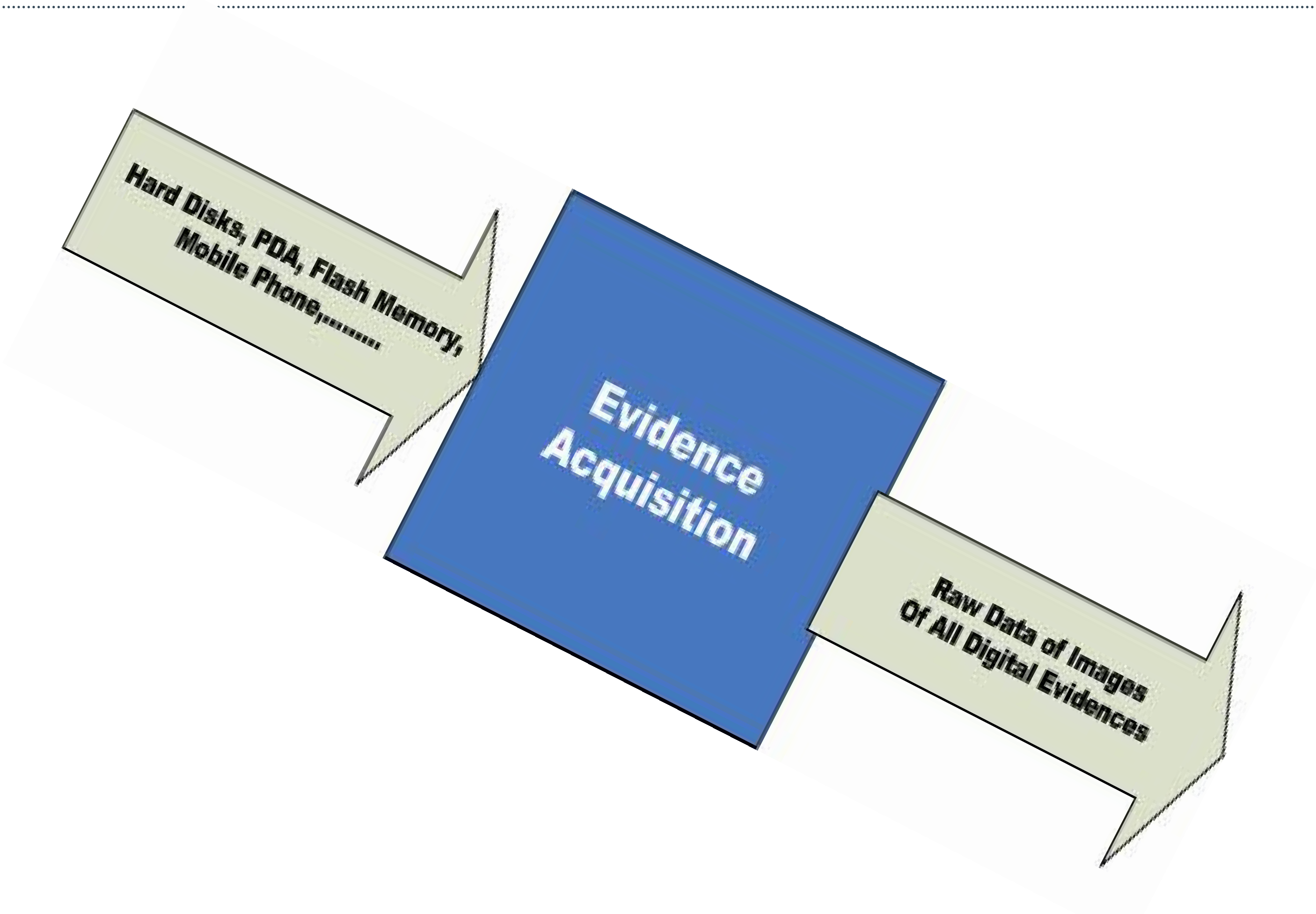
Name	Value
File	Deliver SMS (deleted)
Description	Deleted SMS Message.
Selection	WHERE IS THE WRAPPI...
Added	5/3/2005 3:31:13 PM
Edited	5/3/2005 3:31:13 PM

Bookmarks

File	Name	Data	Timestamp
Deliver SMS (deleted)	Evidence 01	AWS.Care.attws.com##3	5/3/2005 3:30:41 PM
Deliver SMS (deleted)	Evidence 02	WHERE IS THE WRAPPING	5/3/2005 3:31:13 PM

Column: 6; Row: 5

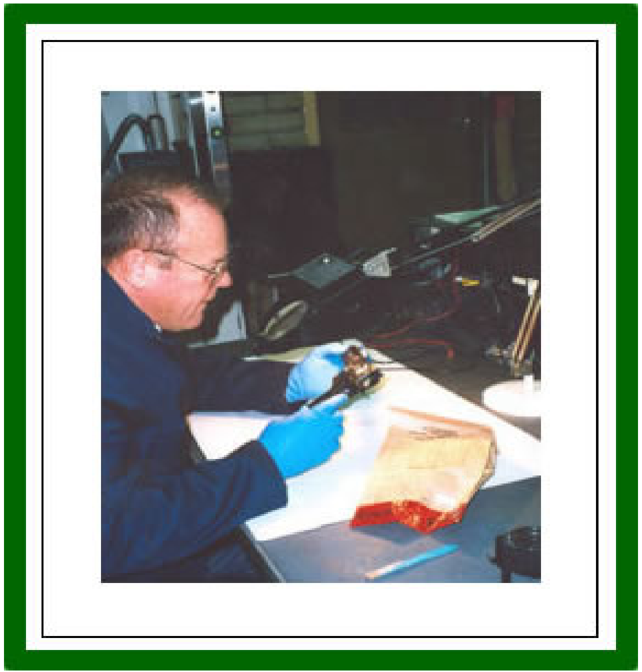
Evidence Acquisition Output



Examination and Analysis

Examination is preparing digital evidence to facilitate the analysis stage.

“Preservation, traceability, validation and filter techniques, pattern matching, hidden data recovery and extraction “ (DFRWS Model)



It includes

- Filter/Reduction
- Class/Individual characteristics
- Data Recovery / Salvage

Data Recovery /Salvage already known for the most of US

Examination   Filter and Reduction

- Eliminating valid system files and other known entities that have no relevance to the investigation.
- Focusing on investigation on the most probable User-Created data

"Less methodical data reduction techniques such as searching for specific keywords or extracting only certain type of files, may not only miss important clues but can still leave the examiners floundering in a sea of superfluous data"

Examination Class characteristics

Two important questions when examining digital evidence

- What is it classification/identification?
- Where did it come from (evolution of source)?

"To Determine if file with a ".doc" is Microsoft Word or Word Perfect

It is class characteristic and in this case you have to examine the header of the file"

EXAMPLE:

"a virus/worm called Melissa hit the Internet. Melissa traveled in a Microsoft Word document that was attached to an e-mail message. This virus/worm propagated so quickly that it overloaded many e-mail servers, and forced several large organizations to shut down their e-mail servers to prevent further damage. It was widely reported that David Smith, the individual who created the virus/worm, was tracked down with the help of a feature of Microsoft Office and GUID filed in the word file".

Examination   Data Recovery

- Recovery using Automated tools to re-link the recent deleted file to the FAT (Tools: FTK, EnCase, and Norton)

- File Carving by searching in the unallocated space and swap file for class characteristic such as file header (Tools: FTK, EnCase, Easy Recovery, and OnTrack)

- Recovery from Password protection and Encryption
  - Many tools can recover files protected by passwords
  - Password logon when performing function reconstruction using restored clone of Windows 2000/NT/XP using L0ptcrack will be useful
  - The most powerful tools currently available are PRTK and DNA from Access Data

Live View Demo **is developed by CERT, Software Engineering Institute**

Live View is a Java-based graphical forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image out physical disk.

- Full disk raw images
- Bootable partition raw images
- Physical Disks (attached via a USB or Firewire bridge)
- Windows 2003, XP, 2000, NT, Me, 98
- Linux (limited support)

Video Clip

Analysis Example: Microsoft Windows

- Log files
  - log files can record which account was used to access a system at a given time. User accounts allow two forms of access to computers.
- File System Traces
  - An individual's actions on a computer leave many traces that digital investigators can use to glean what occurred on the system.
- Registry
  - The Registry on Windows NT/2000/XP is comprised of several hive files located in "%systemroot%\system32\config" and a hive file named "ntuser.dat" for each user account.
  - Windows systems use the Registry to store system configuration and usage details

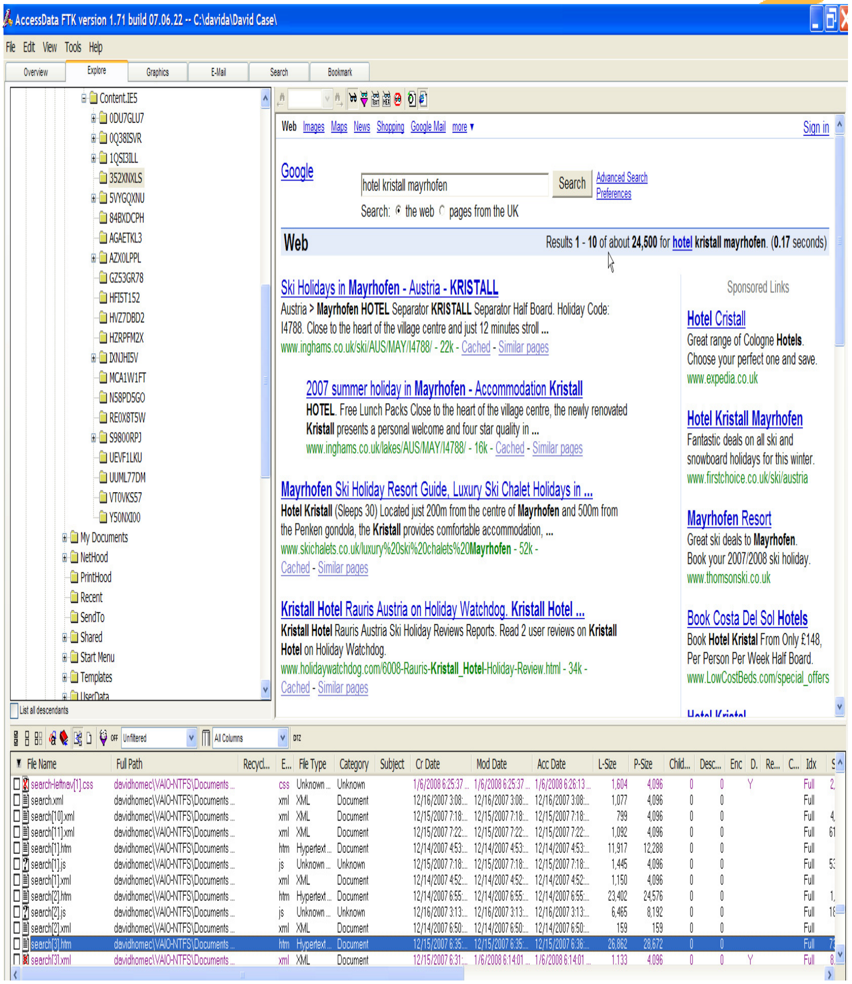
Analysis Example: Microsoft Windows-2

- Internet Traces
  - Accessing the Internet leaves a wide variety of information on a computer including Web sites, and contents viewed.
  - **Web Browser:** When an individual first views a Web page the browser caches the page and associated elements such as images on disk such as:
    - **Cached pages and images**
    - **Internet History activity**
    - **Cookies files for Internet Browsing**

  Pasco is one of the open source tools for analyzing the Index.dat Files

  Web Historian is a free tool analyzing the web history

  FTK is commercial software to reconstruct the visited web sites



AccessData FTK version 1.71 build 07.06.22 -- C:\davida\David Case\

Content.IE5
0DU7GLU7
0Q38ISVR
1QSI3ILL
352XNXLS
5VYGQXNU
84BXDCPH
AGAETKL3
AZX0LPPL
GZ53GR78
HFI5T152
HVZ7DBD2
HZRPFM2X
IXNJHI5V
MCA1W1FT
N58PD5GO
RE0X8T5W
S9800RPJ
UEVF1LKU
UUML77DM
VT0VKS57
Y50NXI00
My Documents
NetHood
PrintHood
Recent
SendTo
Shared
Start Menu
Templates
UserData

□ List all descendants

Web Images Maps News Shopping Google Mail more ▾ Sign in

Google

hotel kristall mayrhofen Search Advanced Search Preferences

Search: ● the web ○ pages from the UK

Web Results **1** - **10** of about **24,500** for hotel **kristall mayrhofen**. (**0.17** seconds)

Ski Holidays in **Mayrhofen** - Austria - **KRISTALL**
Austria > **Mayrhofen HOTEL** Separator **KRISTALL** Separator Half Board. Holiday Code: I4788. Close to the heart of the village centre and just 12 minutes stroll **...**
www.inghams.co.uk/ski/AUS/MAY/I4788/ - 22k - Cached - Similar pages

2007 summer holiday in **Mayrhofen** - Accommodation **Kristall**
HOTEL. Free Lunch Packs Close to the heart of the village centre, the newly renovated **Kristall** presents a personal welcome and four star quality in **...**
www.inghams.co.uk/lakes/AUS/MAY/I4788/ - 16k - Cached - Similar pages

Mayrhofen Ski Holiday Resort Guide, Luxury Ski Chalet Holidays in **...**
Hotel Kristall (Sleeps 30) Located just 200m from the centre of **Mayrhofen** and 500m from the Penken gondola, the **Kristall** provides comfortable accommodation, **...**
www.skichalets.co.uk/luxury%20ski%20chalets%20**Mayrhofen** - 52k - Cached - Similar pages

Kristall Hotel Rauris Austria on Holiday Watchdog. **Kristall Hotel ...**
Kristall Hotel Rauris Austria Ski Holiday Reviews Reports. Read 2 user reviews on **Kristall Hotel** on Holiday Watchdog.
www.holidaywatchdog.com/6008-Rauris-**Kristall_Hotel**-Holiday-Review.html - 34k - Cached - Similar pages

Sponsored Links

Hotel Cristall
Great range of Cologne **Hotels**. Choose your perfect one and save.
www.expedia.co.uk

Hotel Kristall Mayrhofen
Fantastic deals on all ski and snowboard holidays for this winter.
www.firstchoice.co.uk/ski/austria

Mayrhofen Resort
Great ski deals to **Mayrhofen**. Book your 2007/2008 ski holiday.
www.thomsonski.co.uk

Book Costa Del Sol **Hotels**
Book **Hotel Kristal** From Only £148, Per Person Per Week Half Board.
www.LowCostBeds.com/special_offers

Hotel Kristal

File Name	Full Path	Recycl...	E...	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Child...	Desc...	Enc	D.	Re...	C...	Idx	S
search-leftnav[1].css	davidhomec\VAIO-NTFS\Documents ...		css	Unknown ...	Unknown		1/6/2008 6:25:37 ...	1/6/2008 6:25:37 ...	1/6/2008 6:26:13 ...	1,604	4,096	0	0		Y			Full	2,
search.xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/16/2007 3:08:...	12/16/2007 3:08:...	12/16/2007 3:08:...	1,077	4,096	0	0					Full	
search[10].xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/15/2007 7:18:...	12/15/2007 7:18:...	12/15/2007 7:18:...	799	4,096	0	0					Full	4,
search[11].xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/15/2007 7:22:...	12/15/2007 7:22:...	12/15/2007 7:22:...	1,092	4,096	0	0					Full	61
search[1].htm	davidhomec\VAIO-NTFS\Documents ...		htm	Hypertext ...	Document		12/14/2007 4:53:...	12/14/2007 4:53:...	12/14/2007 4:53:...	11,917	12,288	0	0					Full	
search[1].js	davidhomec\VAIO-NTFS\Documents ...		js	Unknown ...	Unknown		12/15/2007 7:18:...	12/15/2007 7:18:...	12/15/2007 7:18:...	1,445	4,096	0	0					Full	5:
search[1].xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/14/2007 4:52:...	12/14/2007 4:52:...	12/14/2007 4:52:...	1,150	4,096	0	0					Full	
search[2].htm	davidhomec\VAIO-NTFS\Documents ...		htm	Hypertext ...	Document		12/14/2007 6:55:...	12/14/2007 6:55:...	12/14/2007 6:55:...	23,402	24,576	0	0					Full	1,
search[2].js	davidhomec\VAIO-NTFS\Documents ...		js	Unknown ...	Unknown		12/16/2007 3:13:...	12/16/2007 3:13:...	12/16/2007 3:13:...	6,465	8,192	0	0					Full	1f
search[2].xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/14/2007 6:50:...	12/14/2007 6:50:...	12/14/2007 6:50:...	159	159	0	0					Full	
search[3].htm	davidhomec\VAIO-NTFS\Documents ...		htm	Hypertext ...	Document		12/15/2007 6:35:...	12/15/2007 6:35:...	12/15/2007 6:36:...	26,862	28,672	0	0					Full	7:
search[3].xml	davidhomec\VAIO-NTFS\Documents ...		xml	XML	Document		12/15/2007 6:31:...	1/6/2008 6:14:01 ...	1/6/2008 6:14:01 ...	1,133	4,096	0	0		Y			Full	8.

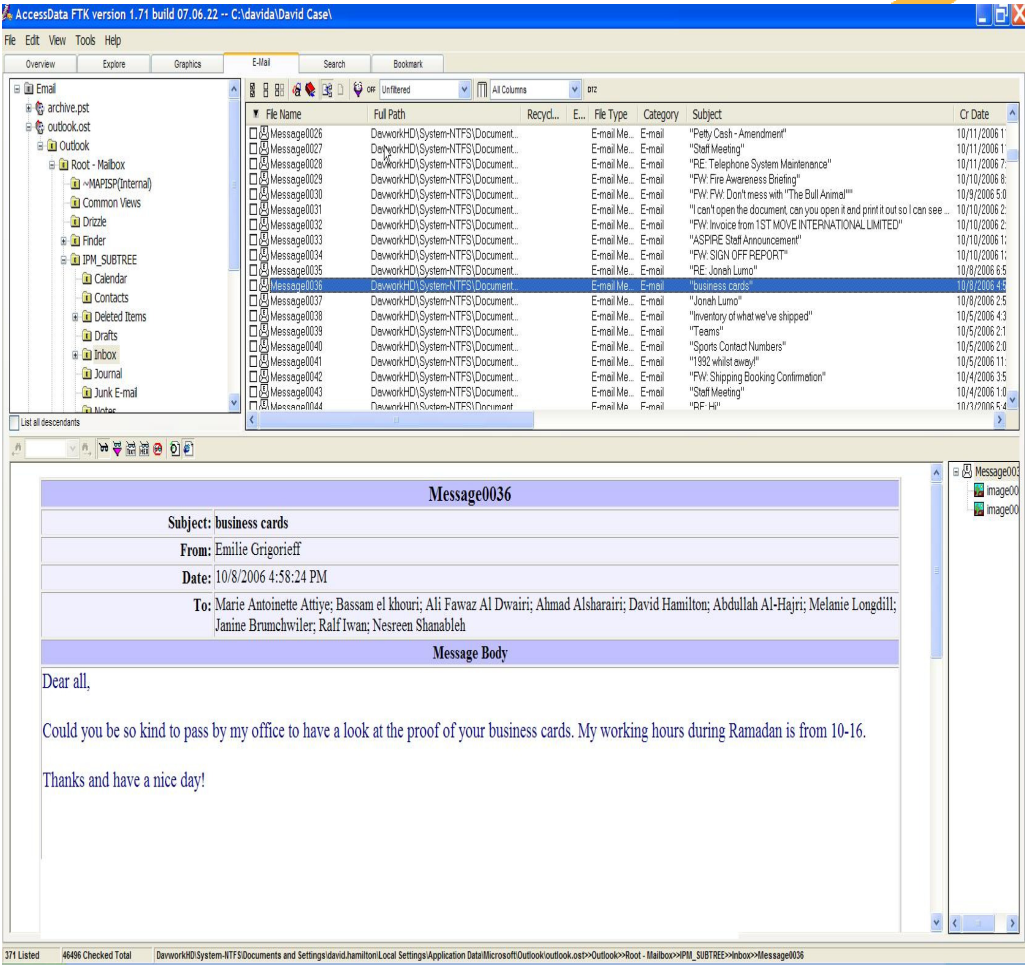
Analysis Example: Microsoft Windows-3

- **E-mail clients** often contain messages that have been sent from and received at a given computer.

FTK is used to view a file containing e-mail with Word document attachments.

FTK can interpret a variety of proprietary formats, including Outlook.

EnCase can also interpret some of these proprietary formats using the View File Structure feature.



File Name	Full Path	Recycl...	E...	File Type	Category	Subject	Cr Date
Message0026	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Petty Cash - Amendment"	10/11/2006 1
Message0027	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Staff Meeting"	10/11/2006 1
Message0028	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"RE: Telephone System Maintenance"	10/11/2006 7:
Message0029	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"FW: Fire Awareness Briefing"	10/10/2006 8:
Message0030	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"FW: FW: Don't mess with "The Bull Animal""	10/9/2006 5:0
Message0031	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"I can't open the document, can you open it and print it out so I can see ...	10/10/2006 2:
Message0032	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"FW: Invoice from 1ST MOVE INTERNATIONAL LIMITED"	10/10/2006 2:
Message0033	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"ASPIRE Staff Announcement"	10/10/2006 1:
Message0034	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"FW: SIGN OFF REPORT"	10/10/2006 1:
Message0035	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"RE: Jonah Lumo"	10/8/2006 6:5
Message0036	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"business cards"	10/8/2006 4:5
Message0037	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Jonah Lumo"	10/8/2006 2:5
Message0038	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Inventory of what we've shipped"	10/5/2006 4:3
Message0039	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Teams"	10/5/2006 2:1
Message0040	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Sports Contact Numbers"	10/5/2006 2:0
Message0041	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"1992 whilst away!"	10/5/2006 11:
Message0042	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"FW: Shipping Booking Confirmation"	10/4/2006 3:5
Message0043	DavworkHD\System-NTFS\Document...			E-mail Me...	E-mail	"Staff Meeting"	10/4/2006 1:0
Message0044	DavworkHD\System-NTFS\Document			E-mail Me	E-mail	"RE: Hi"	10/3/2006 5:4

Message0036

Subject:	**business cards**
From:	Emilie Grigorieff
Date:	10/8/2006 4:58:24 PM
To:	Marie Antoinette Attiye; Bassam el khouri; Ali Fawaz Al Dwairi; Ahmad Alsharairi; David Hamilton; Abdullah Al-Hajri; Melanie Longdill; Janine Brumchwiler; Ralf Iwan; Nesreen Shanableh

Message Body

Dear all,

Could you be so kind to pass by my office to have a look at the proof of your business cards. My working hours during Ramadan is from 10-16.

Thanks and have a nice day!

371 Listed | 46496 Checked Total | DavworkHD\System-NTFS\Documents and Settings\david.hamilton\Local Settings\Application Data\Microsoft\Outlook\outlook.ost>>Outlook>>Root - Mailbox>>IPM_SUBTREE>>Inbox>>Message0036

Reconstruction

Investigation reconstruction leads to a more complete picture of a crime

What happened, who caused the events when, where, how, and why

Three types of reconstruction:

- Functional Analysis
- Relational Analysis
- Temporal Analysis

Functional Analysis

There are several purpose to assigning how a computer system functioned

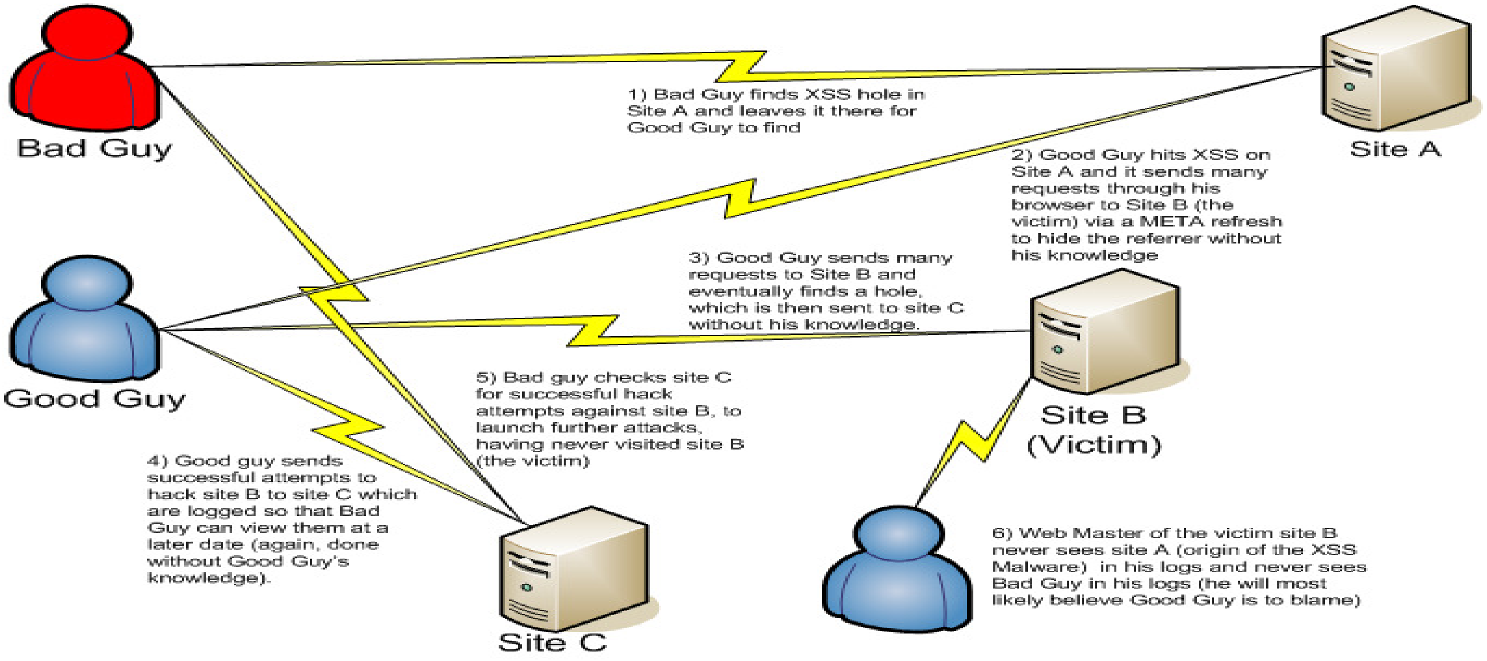
- To Determine if the individual or computer was capable of performing actions necessary to commit the crime.
- To gain a better understanding of a piece of digital evidence or the crime as a whole.
- To prove that digital evidence was tampered with.
- To gain insight into an offender’s intent and motive.
- To determine the proper working of the system during the relevant time period.

Reconstruction

Relational Analysis

To identify relationships between suspect, Victim, and Crime Scene

It will be useful to create nodes representing places, e-mail, IP addresses used, Telephone number,….



1) Bad Guy finds XSS hole in Site A and leaves it there for Good Guy to find

2) Good Guy hits XSS on Site A and it sends many requests through his browser to Site B (the victim) via a META refresh to hide the referrer without his knowledge

3) Good Guy sends many requests to Site B and eventually finds a hole, which is then sent to site C without his knowledge.

4) Good guy sends successful attempts to hack site B to site C which are logged so that Bad Guy can view them at a later date (again, done without Good Guy's knowledge).

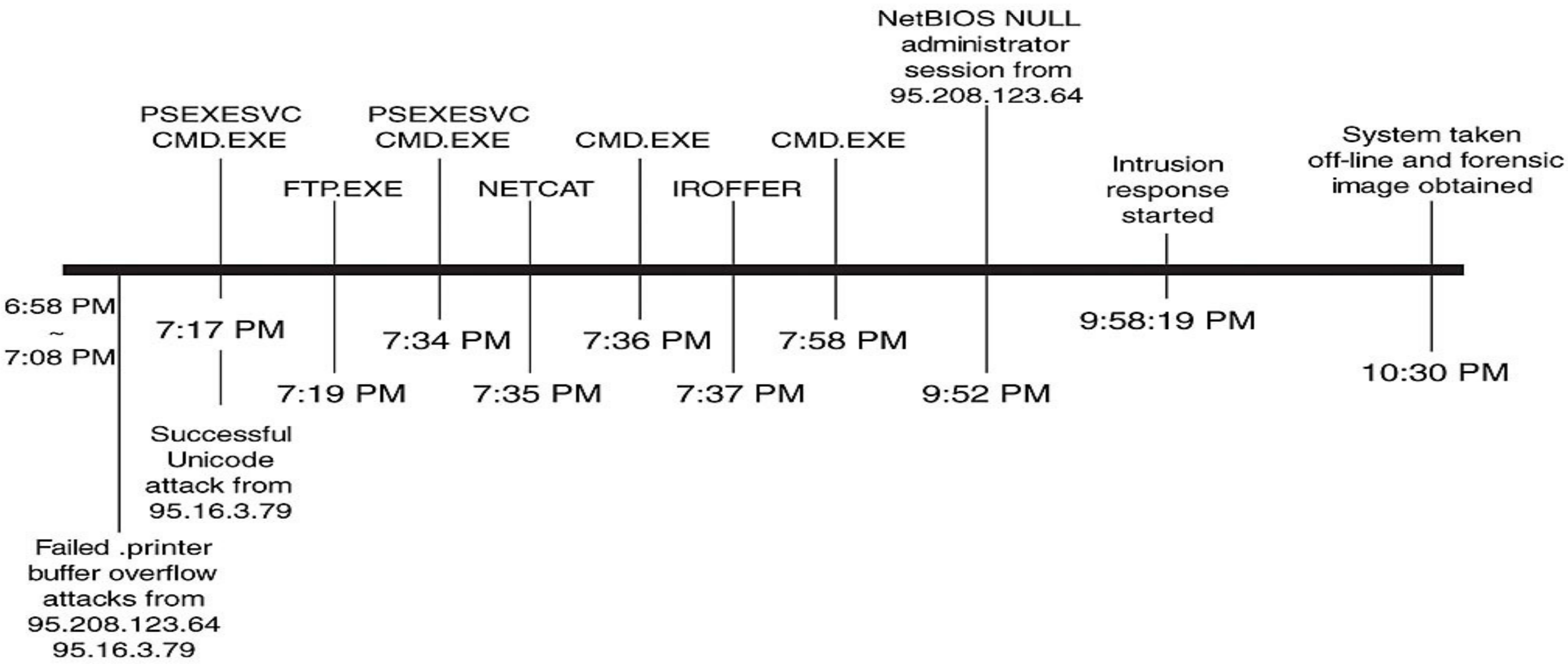
5) Bad guy checks site C for successful hack attempts against site B, to launch further attacks, having never visited site B (the victim)

6) Web Master of the victim site B never sees site A (origin of the XSS Malware) in his logs and never sees Bad Guy in his logs (he will most likely believe Good Guy is to blame)

Temporal Analysis

When Investigating a crime, it is usually desirable to know the time and sequence of events.

Most operating systems keep track of the creation, last modification and access time of files and folders.


NetBIOS NULL administrator session from 95.208.123.64
PSEXESVC CMD.EXE
PSEXESVC CMD.EXE
CMD.EXE
CMD.EXE
FTP.EXE
NETCAT
IROFFER
Intrusion response started
System taken off-line and forensic image obtained
6:58 PM ~ 7:08 PM
7:17 PM
7:19 PM
7:34 PM
7:35 PM
7:36 PM
7:37 PM
7:58 PM
9:52 PM
9:58:19 PM
10:30 PM
Successful Unicode attack from 95.16.3.79
Failed .printer buffer overflow attacks from 95.208.123.64 95.16.3.79

References

- Digital Evidence and Computer Crime-Forensic Science
  (Eoghan Casey)

- Electronic Crime Scene Investigation
  (US Department Of Justice)

Thank You

www.qcert.org