

Digital Evidence - Technical Issues



Adv Prashant Jhala
p12jhala@gmail.com

What is Digital Evidence ?

Is the discovery, analysis & reconstruction of Evidence extracted from and / or contained in a computer, computer system, computer network, computer media or computer peripheral

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination

Thus trying to link the criminal with the crime

Types of electronic devices secured from the crime scene

➤ *Storage Devices*

➤ *Handheld Devices*

➤ *Peripheral Devices*

➤ *Network Devices*

➤ *Other potential source of digital evidence*



Storage Devices

Hard Drives



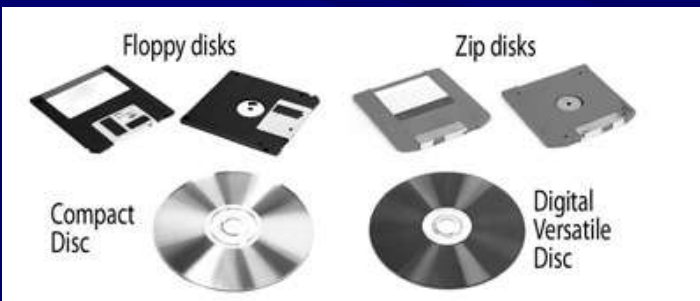
External Hard Drives



Memory Cards



Removable Media



Thumb Drives



Potential evidence: E-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, financial records, and event logs that can be valuable evidence in an investigation or prosecution

Handheld Devices



Potential evidence: Software applications, data, and information such as documents, e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, and financial records that are valuable evidence in an investigation or prosecution.

BEWARE !!!!!

- Digital evidence may be lost if power is not maintained.
- Digital evidence can be overwritten or deleted while the device remains activated.
- Software activated remotely to render the device unusable and make the data it contains inaccessible.

Peripheral Devices



Potential evidence: The devices themselves and the functions they perform or facilitate are all potential evidence. Information stored on the device regarding its use also is evidence, such as incoming and outgoing phone and fax numbers; recently scanned, faxed, or printed documents; and information about the purpose for or use of the device. In addition, these devices can be sources of fingerprints, DNA, and other identifiers.

Network Devices



Network hub



Laptop network card and ethernet cable



Internet modems



Network switch and power supply

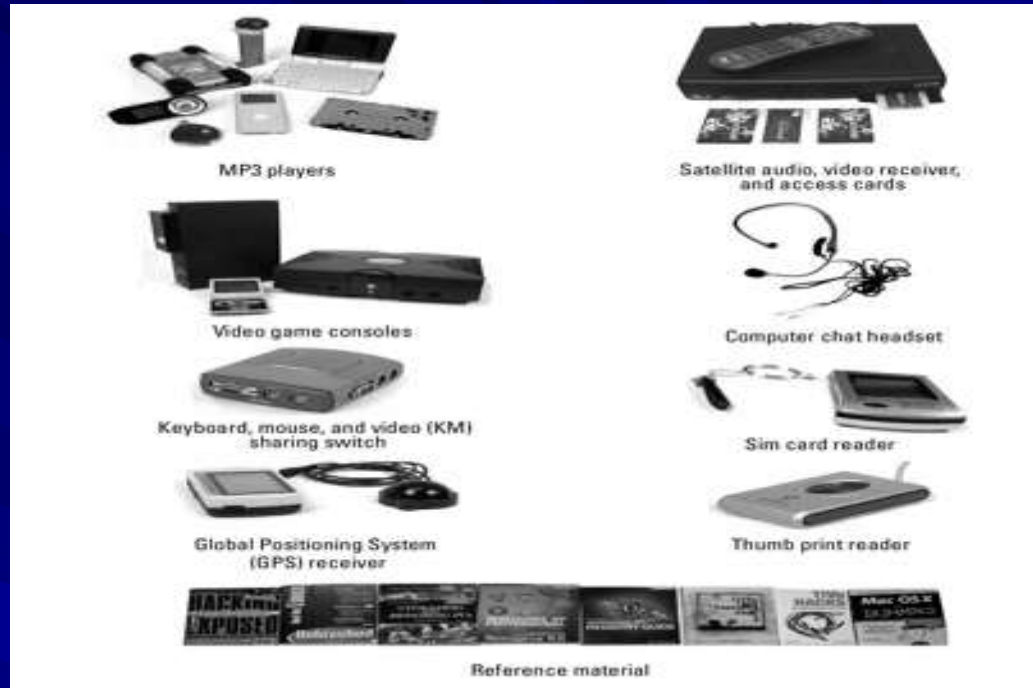


Wireless access points

Wireless network server

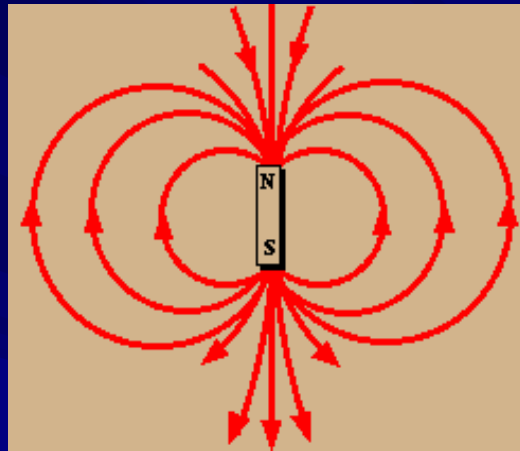
Potential evidence: The connected devices themselves. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including Internet protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses may all be useful as evidence.

Other potential source of digital evidence



Potential evidence: The device or item itself, its intended or actual use, its functions or capabilities, and any settings or other information it may contain is potential evidence.

Digital Evidence is Sensitive to



- Static Electricity
- Magnetic Fields
- Shock
- Moisture

Tools & Material for Collecting Digital Evidence

- ✓ Cameras (photo and video).
- ✓ Cardboard boxes.
- ✓ Notepads.
- ✓ Gloves.
- ✓ Evidence inventory logs.
- ✓ Evidence tape.
- ✓ Paper evidence bags.
- ✓ Evidence stickers, labels, or tags.
- ✓ Crime scene tape.
- ✓ Antistatic bags.
- ✓ Permanent markers.
- ✓ Nonmagnetic tools.



Securing and Evaluating the Crime Scene for Digital Evidence



Figure 2-1 The crime scene



Securing and Evaluating the Crime Scene for Digital Evidence



- Follow departmental policy for securing crime scenes.
- Immediately secure all electronic devices.
- Ensure that no unauthorized person has access to any electronic devices.
- Refuse offers of help or technical assistance from any unauthorized persons.
- Remove all persons from the crime scene
- Ensure that the condition of any electronic device is not altered.
- **STOP!** Leave a computer or electronic device off if it is already turned off



Preserve components such as keyboard, mouse, removable storage media for evidence such as fingerprints, DNA, or other physical evidence that should be preserved.

Securing and Evaluating the Crime Scene for Digital Evidence



If a computer is on or the power state cannot be determined , we check

- Sound of fans , drives spinning, or check to see if light emitting diodes are on.
- Display screen for signs that digital evidence is being destroyed. Words to look out for include "delete," "format," "remove," "copy," "move," "cut," or "wipe."
- Indications that the computer is being accessed from a remote computer or device.
- Active communications with other computers instant messaging or chat rooms.
- Web cameras (Web cams) and determine if they are active.

Securing and Evaluating the Crime Scene for Digital Evidence

Relevant information along with the digital evidence to be recorded is

Purpose of the computer

Computer / Login Names

Document / Email / Login Passwords

Security software / provisions

Internet connectivity details

User details



Destructive processes can be any functions intended to obliterate data on the hard drive or data storage device. Terms like "format," "delete," "remove," and "wipe" can be indicative of destructive processes. Document these indicators in reports.

DO NOT
turn the computer
or device on.

Secure scene and move everyone away from computers and electronic devices.

NO
Is the computer powered on?

YES

Are law enforcement personnel with specific computer seizure training available?

YES

NO

Is the system a networked business environment?

YES

NO

STOP! DO NOT
turn computer or device off. Contact personnel trained in network seizure.

Are destructive processes running?

YES

NO

Is information of evidential value visible onscreen?

YES

Request assistance and follow recommendations of personnel with specific digital evidence seizure training.

Thoroughly document and photograph all information on the screen.

NO

Remove power cord from back of computer and connected devices.

Label all connections on computers and devices as well as cables and power supplies.

Locate and secure all evidence within the scope of authority for the specific circumstances.

Document, log, and photograph all computers, devices, connections, cables, and power supplies.

Log and secure all evidence according to

Digital Evidence
Packaging , Transportation and
Storage Procedure

Packaging Procedure



- ✓ Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packaging.
- ✓ Pay special attention to latent or trace evidence and take actions to preserve it.
- ✓ Pack magnetic media in antistatic packaging (paper or antistatic plastic bags).
- ✓ Avoid using materials that can produce static electricity, such as standard plastic bags.
- ✓ Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, and tapes.
- ✓ Ensure that all containers used to hold evidence are properly labeled.

Transportation Procedure



- ✓ Keep electronic evidence away from magnetic sources.
- ✓ Avoid storing electronic evidence in vehicles for prolonged periods of time.
- ✓ Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- ✓ Ensure that computers and other components that are not packaged in
- ✓ Containers are secured in the vehicle to avoid shock and excessive vibrations.
- ✓ Maintain the chain of custody on all evidence transported.

Storage Procedure



- ✓ Ensure that evidence is inventoried in accordance with departmental policies.
- ✓ Store evidence in a secure area away from temperature and humidity extremes.

Note: Be aware that potential evidence such as dates, times, and systems configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail.

Therefore, appropriate personnel (e.g., evidence custodian, lab chief, forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

Chain of Custody Form

"Chain of custody" refers to the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence. A chain of custody is the process of validating how any kind of evidence has been gathered, tracked and protected. A piece of evidence is worthless without a chain of custody.

A chain of custody form must answer the following questions:

1. What is the evidence?
2. How did the analyst get it?
3. When was it collected?
4. Who all have handled it?
5. Why did the mentioned persons handle it?
6. Where all has the evidence traveled?
7. Where the evidence was ultimately stored?

CONTROL NO: M

10015141

INVESTIGATOR'S RECEIPT: Tear along perforated line and retain for your records.

Case Number: _____
Evidence Bag Sealed by: _____ Date Sealed: _____
Description of Enclosed Evidence: _____

▲
Glue Line

▲
Glue Line

CONTROL NO: M

10015141

EVIDENCE

(TO BE OPENED BY AUTHORIZED PERSONNEL ONLY)

NOTE

- A) Do not use this bag for any evidence that has wet/damp body fluids on it.
- B) To seal bag, peel off blue release liner, then seal bag by pressing down on red glue line.

Case Number: _____

Description of Enclosed Evidence: _____

Submitting Agency: _____

Telephone Number: _____

Evidence Recovered By: _____ (PRINT NAME)

Victim's Full Name: _____

Suspect's Full Name: _____

Evidence Bag Sealed By: _____ (PRINT NAME)

Date Sealed: _____ Time Sealed: _____ AM
PM

CHAIN OF CUSTODY

FROM	TO	DATE

FOR CRIME LAB PERSONNEL ONLY

CONDITION OF EVIDENCE BAG UPON RECEIPT AT LAB:

SEALED OTHER _____ (DESCRIBE)

CRIME LAB CASE NO: _____

NOTES: _____

CUT HERE TO OPEN

Digital Evidence is Fragile





Hash Result : 9046216413E94651BD0A6710629AF09B

After altering only one pixel in the original image.



Hash Result : E0AA50C70414562B29C6DB660FA9BC2A



Date of Creation : 3 Jan 2010

Hash Result : AFE57B9D7AC0D161BF87C0A7EECC35F9

After accessing the doc file directly from suspect drive



Date of Access : 23 March 2010

Hash Result : D0AF512F32D05B6D80E3AD9FF73092B4



SUSPECT HARD DISC

Hash Result :e83fd31b3a275e653146a6ed0de7fca09bd2ae565d8



After erroneously booting from Suspect Hard Disc



SUSPECT HARD DISC

Hash Result :68105f7fa96166ed3173e700a3bdc7d1603ccdd2f9b

Probable Reasons:

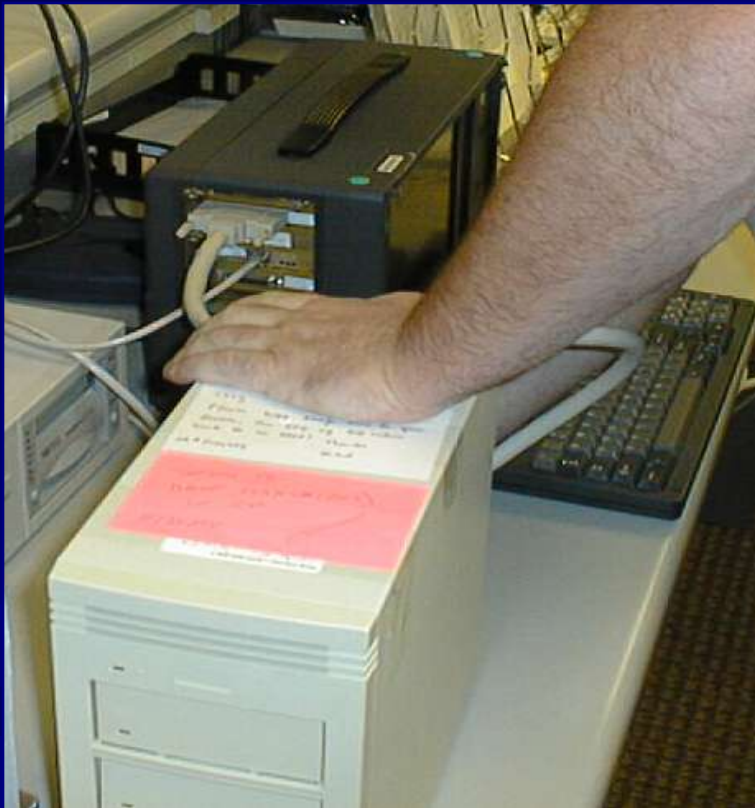
- 1. Startup program executed.**
- 2. Access date & time of OS files changed._**





Best Practices for Cyber Forensics Procedure

Cyber Forensic Process



- ✓ Acquire
- ✓ Authenticate
- ✓ Analyze
- ✓ Document

Sanitizing investigator's media for storing images of suspect media for investigation



SANITIZE HARD DRIVES AT 7GB/MIN



Sanitizes hard drives at speeds exceeding 3GB/Min for 9 drives simultaneously

Imaging with Care

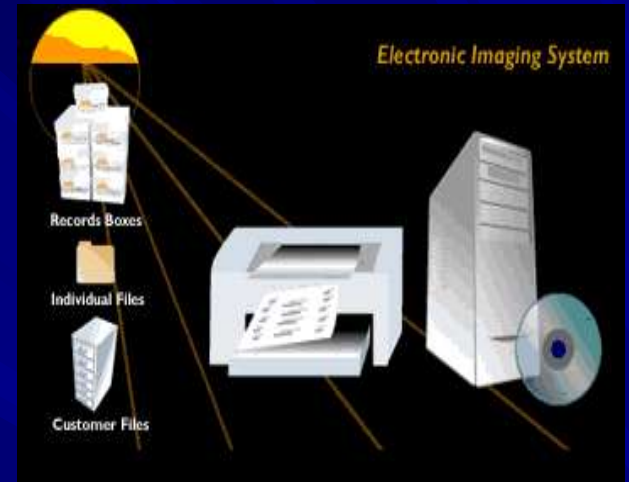


- Attaching suspect storage media to forensic workstation for imaging.



Imaging & Data Retrieval Tools

- ✓ Winhex
- ✓ Norton Ghost 2000
- ✓ Byte back
- ✓ Encase
- ✓ FTK
- ✓ These tools can retrieve data from deleted files, hidden files, files with changed extensions, stego & camouflage files, encrypted files etc
- ✓ It is believed that even after formatting the system for up to 7 levels, some traces of data can yet be retrieved



Imaging & Data Retrieval Tools

- Data can also be retrieved from hard discs that are damaged, burnt , broken, submerged in water
- Mobiles- it is possible to retrieve data from damaged, burnt, broken Sim cards & mobile phones
- Deleted Sms's can also be retrieved from sim cards (stored in PDU format- Protocol Distribution Unit)

Imaging Devices



Tower for multiple hard disc imaging

Imaging Devices



“Image Master” device for Imaging

Imaging Devices



Portable devices for Forensic Analysis

Imaging Devices



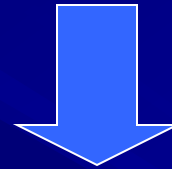
Portable suitcase for Forensic Analysis

Authenticate



Hash Value

=



Hash Value

IMAGE FILE

If acquisition hash equals verification hash, image is authentic.

Cyber Forensics Documentation

- **A forensic examination report must**
 - * **Software used & their versions**
 - * **Be in simple language**
 - * **List the hash results**
 - * **List all storage media numbers, model, etc**
 - * **Supported by photographs**



- **Case analysis details must have**
 - * **Introduction**
 - * **Background of the issue**
 - * **Detailed steps of forensic analysis carried out**
 - * **Certificate of the cyber forensic expert.**



Potential digital evidence
in various cases.

Child Abuse and Exploitation Cases



Computers

Mobile communication devices

External data storage devices

Video and still photo cameras and media

Printed e-mail, notes, and letters and maps

Web cameras and microphones

Internet activity records

Photo editing and viewing software

References to user-created folders and file names that classify images

Digital camera software

Printed images or pictures

Thank You