



Digital Forensics



Chapter 1 - Digital Forensics & Investigations

Introduction

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. Digital forensics encompasses much more than just laptop and desktop computers. Mobile devices, networks, and “cloud” systems are very much within the scope of the discipline. It also includes the analysis of images, videos, and audio (in both analog and digital format). The focus of this kind of analysis is generally authenticity, comparison, and enhancement.

While digital forensics techniques are used in more contexts than just criminal investigations, the principles and procedures are more or less the same no matter the investigation. While the investigation type may vary widely, the sources of evidence generally do not. Digital forensic examinations use computer-generated data as their source. Historically, this has been limited to magnetic and optical storage media, but increasingly snapshots of memory from running systems are the subjects of examination. Digital forensics is alternately (and simultaneously) described as an art and a science. In *Forensic Discovery*, Wietse Venema and Dan Farmer make the argument that at times the examiner acts as a digital archaeologist and, at other times, a digital geologist. Digital archaeology is about the direct effects from user activity, such as file contents, file access time stamps, information from deleted files, and network flow logs. Digital geology is about autonomous processes that users have no direct control over, such as the allocation and recycling of disk blocks, file ID numbers, memory pages or process ID numbers.

The main goal of computer forensics is to identify, collect, preserve, and Analyze data in a way that preserves the integrity of the evidence collected.

1.1 Locard's Principal as applicable to Digital Forensics

Locard's Exchange Principle In performing live response, investigators and first



responders need to keep a very important principle in mind. When we interact with a live system, whether as the user or as the investigator, changes will occur on that system. On a live system, changes will occur simply due to the passage of time, as processes work, as data is saved and deleted, as network connections time out or are created, and so on. Some changes happen when the system just sits there and runs. Changes also occur as the investigator runs programs on the system to collect information, volatile or otherwise. Running a program causes information to be loaded into physical memory, and in doing so, physical memory used by other, already running processes may be written to the page file.

As the investigator collects information and sends it off the system, new network connections will be created. All of these changes can be collectively explained by Locard's Exchange Principle. Changes that occur to a system as the system itself apparently sits idle are referred to as "evidence dynamics" and are similar to rain washing away potential evidence at a crime scene.

In the early 20th century, Dr. Edmond Locard's work in the area of forensic science and crime scene reconstruction became known as Locard's Exchange Principle. This principle states, in essence, that when two objects come into contact, material is exchanged or transferred between them. If you watch the popular CSI crime show on TV, you'll invariably hear one of the crime scene investigators refer to possible transfer. This usually occurs after a scene in which a car hits something or when an investigator examines a body and locates material that seems out of place.

This same principle applies in the digital realm. For example, when two computers communicate via a network, information is exchanged between them. Information about one computer will appear in the process memory and/or log files on the other. When a peripheral such as a removable storage device (a thumb drive, an iPod, or the like) is attached to a Windows computer system, information about the device will remain resident on the computer. When an investigator interacts with a live system, changes will occur to that system as programs are executed and data is copied from the system. These changes might be transient (process memory, network connections) or permanent (log files, Registry entries).

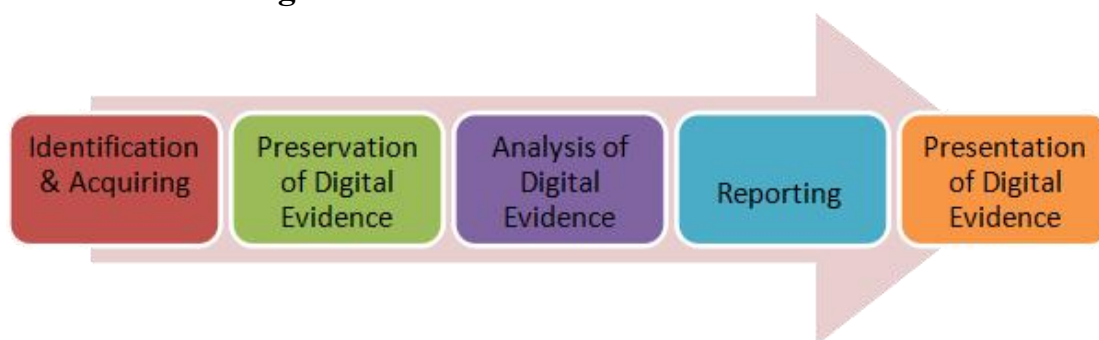
Programs that we use to collect information might have other effects on a live system. For example, a program might need to read several Registry keys, and the paths to

those keys will be read into memory. Windows XP systems perform application prefetching, so if the investigator runs a program that the user has already run on the system, the last access and modification times of the prefetch file (as well as the contents of the file itself) for that application will be modified. If the program that the investigator runs hasn't been used before, a new prefetch file will be created in the Prefetch directory.

Investigators not only need to understand that these changes will occur but also must document those changes and be able to explain the effects their actions had on the system, to a reasonable extent. For example, as an investigator you should be able to determine which .pf files in the XP Prefetch directory are a result of your efforts and which are the result of user activities. The same is true for Registry values. As with the application prefetching capabilities of Windows XP, your actions will have an effect on the system Registry. Specifically, entries may appear in the Registry, and as such the LastWrite times of the Registry keys will be updated.

Some of these changes might not be a direct result of your tools or actions, but rather are made by the shell (i.e., Windows Explorer), due simply to the fact that the system is live and running. By testing and understanding the tools you use, you will be able to document and explain what Artifacts found on a system are the result of your efforts and which are the result of actions taken by a user or an attacker.

1.2 Phases of Digital forensics



Identification & Acquiring of Digital Evidence: Knowing what evidence is present, where it is stored and how it is stored is vital in determining which processes are to be employed to facilitate its recovery. In addition, the cyber forensic examiner must be able to identify the type of information stored in a device and the format in which it is stored in which it is stored so that the appropriate technology can be used to extract it.



After the evidence is identified the cyber forensic examiner/investigator should image/clone the hard-disk or the storage media.

The Preservation of digital evidence is a critical element in the forensic process. Any examination of the electronically stored data can be carried out in the least intrusive manner. Alteration to data that is of evidentiary value must be accounted for and justified.

The analysis of digital evidence: The extraction, processing and interpretation of digital data is generally regarded as the main element of cyber forensics. Extraction produces a binary junk, which should be processed, to make it readable by a human being.

Reporting means giving the findings in a simple lucid manner so that any person can understand. The report should be in simple terms, giving the description of the items, process adopted for analysis & Chain of custody, the hard and soft copies of the findings, glossary of terms etc.

The presentation of digital evidence involves deposing evidence in the court of law regarding the findings and the credibility of the processes employed during analysis.

1.3 Classification of Digital Forensics

- **Disk Forensics:** Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.
- **Mobile Forensics:** Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.
- **Network Forensics:** Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.
- **Malware Forensics:** Deals with Investigating and Analyzing Malicious Code for identification of Malware like viruses, Trojans, worms, keylogger's etc and to study their payload.



- **Email Forensics:** Deals with recovery and analysis of e-mails including deleted e-mails, calendars and contacts.
- **Memory Forensics:** Deals with collecting data from system memory (e.g., system registers, cache, RAM) in raw form and carving the data from the raw dump.
- **Wireless forensics:** Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze wireless network traffic data. The data collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations.
- **Database Forensics:** Database forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.

1.4 Digital Forensics Best Practices

The best practices for collecting, acquiring, analyzing and documenting the data found in computer forensic examinations.

1.4.1 Evidence Collection

General guidelines concerning the collection of digital evidence are provided as follows:

- Consult with the investigator to determine the details of the case and potential evidence to be collected.
- Determine the necessary equipment to take to the scene.
- Review the legal authority to collect the evidence, ensuring any restrictions are noted. If necessary during the collection, obtain additional authority for evidence outside the original scope.
- Occasionally, there may be a need to conduct traditional forensic processes on media (e.g., DNA and latent prints). These are case dependent and should be

discussed with the investigator to determine the need for such processing as well as the order in which the processes should be performed.

- When evidence from the scene cannot be removed, it should be copied or imaged on-site.
- All individuals not involved in the collection process should be removed from the proximity of digital evidence.
- Individuals who may have relevant information (e.g., user names, passwords, operating systems and network credentials) should be identified and interviewed.
- The scene should be searched systematically and thoroughly. Searchers should be able to recognize different types of devices that may contain digital evidence (e.g., novelty USB drives, servers and wireless storage devices).
- The possibility of anti-forensics techniques (e.g., destructive devices and wiping software) should be considered.

1.4.2 Evidence Handling

- Document the condition of the evidence.
 - o Photograph (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area.
 - o Determine if the computer is in stand-by mode and follow procedures as if it was powered on.
- Document the external component connections.

1.4.3 Evidence Triage/Preview

- Evidence triage may not be appropriate for all situations.
- Evidence preview may miss items of evidentiary value.
- Time and date stamps may be affected by the evidence triage/preview process on live systems.
- An evidence preview/triage shall not take the place of a complete exam.

1. Powered-On Systems

The examiner should:

- Examine the computer for any running processes. If it is observed running a destructive process, the examiner should stop the process and document any



actions taken.

- Capture RAM and other volatile data from the operating system.
- Determine if any of the running processes are related to cloud or off-site storage. When encountered, the examiner should coordinate with the appropriate legal authority to ensure the scope covers the off-site acquisition.
- Document and hibernate any running virtual machines.
- Consider the potential of encryption software installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the unencrypted data before the computer is powered off.
- Save any opened files to trusted media.
- Evaluate the impact of pulling the plug vs. shutting the computer down. This is typically dependent upon the operating system and file system encountered.
- Isolate the computer from any network connectivity.
- Use a triage tool to preview data.

2. Powered Off Systems

If the computer is powered off, **do not** turn on the computer.

- Only personnel trained to preview/triage computers should power on the computer and preview/triage data.
- Disconnect all physical network connectivity.
- Consider the possibility of Wake on Wireless LAN (WoWLAN) and BIOS timed booting sequences.
- Verify the computer system for compatibility with triage tools and software.
- Identify and document evidence, if applicable.
- Export evidence to trusted media.

3. Loose media

- When possible, use write blocking devices to collect and document evidence.

4. Computers

- Disconnect all power sources by unplugging from the back of the computer.
- Laptop batteries should be removed.

5. Servers

- Determine whether to get logical files, logical images, or physical images.
- If possible, consideration should be given to the collection of backup tapes and



their associated drives, as the tapes may contain additional evidence.

- Unless the situation warrants it, capturing volatile data may not be necessary.

Warning: Pulling the plug on a server may severely damage the system, disrupt legitimate business and/or create organizational liability.

1.4.4 Evidence Packaging /Transport

- Each piece of evidence should be protected from damage or alteration, labelled and a chain-of-custody maintained as determined by organizational policy.
- Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity.

1.4.5 Equipment Preparation

- Equipment refers to the non-evidentiary hardware and software the examiner utilizes to conduct the forensic imaging or analysis of evidence.
- The examiner should ensure that the equipment is adequate for the task and in proper working condition. The condition of the equipment should be documented.
- Hardware and software must be configured to prevent cross contamination.
- The manufacturer's operation manual and other relevant documentation for each piece of equipment should be available if needed.
- Analysis/Imaging software should be validated prior to its use.

1.4.6 Acquisition

- Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.
- All items submitted for forensic examination should be inspected for their physical integrity.
- Methods of acquiring evidence should be forensically sound and verifiable, method deviations shall be documented.
- Digital evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved.
- Forensic image(s) should be archived to trusted media and maintain consistent with organization policy and applicable laws.



- Any errors encountered during acquisition should be documented.
- Steps should be taken to ensure the integrity of the data acquired, this may include one or more of the following:
 - o Hash values (e.g., MD5, SHA-1 and SHA-256)
 - o Stored on read-only media (e.g., CD-ROM and DVD-R)
 - o Sealed in tamper-evident packaging

1.4.7 Forensic Analysis/Examination

- Examiners should review documentation provided by the requestor to determine the processes necessary to complete the examination.
- Examiners should review the legal authority (e.g., consent to search by owner, search warrant or other legal authority).
- Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic copies or images.
- Appropriate controls and standards should be used during the examination procedure.
- Examination of the media should be completed logically and systematically consistent with organizational policy.

1.4.8 Documentation

Documentation should include all required information and be preserved according to the examiner's organizational policy.

1.4.9 Report of Finding

- Information should be presented in a format that may be read and understood by non-technical individuals.
- Examiners should be able to explain all information contained within the report.
- Should include any relevant information contained within the acquisition and/or evidence handling documentation.
- Reports issued by the examiner should address the requestor's needs and
 - o Document the scope and/or purpose of the examination.
 - o Give a detailed description of the media examined (e.g., hard disk, optical media or flash drive).
 - o Include any supplemental reports related to the examination.



- o Provide the examiner's name and date of exam.
- o Be reviewed according to organizational policy.

1.4.10 Review

The examiner's organization should have policies for technical, peer and administrative reviews.

1.5 Computing Devices

An electronic device for processing information and performing calculations follows a program to perform sequences of mathematical and logical operations.

Many electronic devices contain embedded, specialized computers. These computers allow the devices to do specialized computing tasks.

Examples:

- ATM machine
- Digital Alarm Clock
- Microwave Oven
- Cell Phone
- CD Player
- Computer

1.6 Storage Media

Storage media are devices that store application and user information. The primary storage media for a computer is usually the internal hard drive. Most internal drives are regular IDE hard drives that come with the computer. A removable drive is another popular storage device that is usually connected by firewire, USB, or parallel port (e.g. portable Zip drives, Jaz drives, or CD/DVD drives). Newer forms of external storage include USB thumb drives and camera storage media.

Most external drives enable flexible data transfer from one computer to another. A computer that has had external drives connected to it usually has evidence in the computer's registry of using the subject device. When performing a forensic examination during discovery proceedings for litigation, determining if external drives were connected to the computer may help in obtaining additional evidence for discovery.



Storage devices vary in size and the manner in which they store and retain data. First responders must understand that, regardless of their size or type, these devices may contain information that is valuable to an investigation or prosecution. The following storage devices may be digital evidence:

Hard drives: Hard drives are data storage devices that consist of an external circuit board, external data and power connections and internal magnetically charged glass, ceramic, or metal platters that store data. First responders may also find hard drives at the scene that are not connected to or installed on a computer. These loose hard drives may still contain valuable evidence.

External hard drives: Hard drives can also be installed in an external drive case. External hard drives increase the computer's data storage capacity and provide the user with portable data. Generally, external hard drives require a power supply and a universal serial bus (USB), FireWire, Ethernet, or wireless connection to a computer system.

Removable media: Removable media are cartridges and disk-based data storage devices. They are typically used to store, archive, transfer, and transport data and other information. These devices help users share data, information, applications, and utilities among different computers and other devices.

Thumb drives: Thumb drives are small, lightweight, removable data storage devices with USB connections. These devices, also referred to as flash drives, are easy to conceal and transport. They can be found as part of, or disguised as, a wristwatch, a pocket-size multitool such as a Swiss Army knife, a keychain fob, or any number of common and unique devices.

Memory cards: Memory cards are small data storage devices commonly used with digital cameras, computers, mobile phones, digital music players, personal digital assistants (PDAs), video game consoles, and handheld and other electronic devices.




1.7 Digital Evidence & its Sources








Digital evidence or electronic evidence is “any probative information stored or transmitted in digital form that a party to a court case may use at trial”⁴. Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as “any information

of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines”.

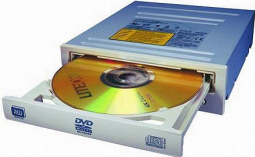

The main characteristics of digital evidence are, it is latent as fingerprints and DNA, can transcend national borders with ease and speed, highly fragile and can be easily altered, damaged, or destroyed and also time sensitive. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. When dealing with digital evidence, the principles that should be applied are, actions taken to secure and collect digital evidence should not change that evidence, persons conducting the examination of digital evidence should be trained for this purpose and activity relating to the seizure, examination, storage, or transfer of digital evidence should be fully documented, preserved, and available for review.

1.7.1 Sources of Digital Evidence

S.N O	Digital Device		Potential Evidence
1.	A Desktop Computer Cabinet		The device itself may be evidence of component theft, counterfeiting etc. The device contains digital devices with all the files and folders stored including deleted files and information, which may not be seen normally. Cyber forensics is used to image, retrieve and analyse the data.
2.	Display Monitor (CRT/LCD/TFT etc) Screens of Mobile Phones, If Switched on.		All the graphics and files that are open and visible on the screen in switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs, and through description in seizure memo.
3.	Smart Cards, dongles, biometric scanners etc.		The device itself, along with identification/authentication information of the card and the user, level of access, configurations and Permission.

4.	Answering Machines		The device can store voice messages and sometimes, the date and time information when the message was left. It may have details such as last number called, memos, phone numbers & names, caller identification information, deleted messages.
5.	Digital Cameras		The device can be looked for images, videos, sounds, removal cartridges, time and date stamps.
6.	Handheld devices(Personal Digital Assistant(PDAs), Electronic Organizers, Smart Phones)		Much information can be obtained from these devices like address book, appointment calendars / information, documents, emails, phone book, messages (text and voice), email passwords etc.
7.	Hard drives		The device in itself, as it stores all the information.
8.	Local area Network (LAN) card or Network Interface Card (NIC).		The device itself and also MAC (Media Access Control) address can be obtained.
9.	Modems, Routers, Hubs and Switches.		The device itself. In routers, configuration files contain information related to IP Addresses etc.
10.	Servers		Information like last logins, mails exchanged, contents downloaded, pages accessed etc can be obtained.

11.	Network Cables and Connectors.		Network cables are used to trace back their respective computers. Connectors help in identifying the types of devices that are connected to the computers.
12.	Pagers		The device can be looked for address information, text messages and phone numbers.
13.	Printers		The device has data like number of prints last printed & some maintain usage logs, time and date information. If attached to a network they may store network identity information. In addition, It can also be examined for fingerprints.
14.	Removable Storage Media and Devices.		All new generation mobile phones, Cameras etc., use these. These devices store files in which evidence can be found.
15.	Scanners		The device itself, having the capability to scan may help prove illegal Activity.
16.	Telephones		Many telephones can store names, messages (text and voice), memos, passwords, phone numbers and caller identification information. Additionally some cellular tele phones can store appointment information, and may act as a voice recorder.
17.	Copiers		Copiers may contain some documents both physical and electronic, user usage logs, time and date stamps.

18.	CD and DVD drives		These devices store files/data, in which evidence can be found.
19.	Credit Card Skimmers		Tracks of Magnetic Strips contain Cardholder's information which may include: Card Expiration date, User's Address, Credit Card Numbers, User's Name.
20.	Digital Watches		Some latest Digital Watches contain information like address book, notes, appointment Calendars, Phone numbers, emails etc.
21.	Facsimile Machines		These devices contain some documents, phone numbers, send/receive logs, film cartridges that can be considered.
22.	Global Positioning System (GPS)		The device may provide travel logs, home location, previous destinations, way point coordinates, way point name etc.,
23.	Keyboard & Mouse		These devices can be examined for Fingerprints.

1.8 Potential Digital Evidence

Storage devices such as hard drives, external hard drives, removable media, thumb drives, and memory cards may contain information such as 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.

Handeld devices such as mobile phones, smart phones, PDAs, digital multimedia (audio and video) devices, pagers, digital cameras, and global positioning system



(GPS) receivers may contain 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.

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.

- Desktop Computers
- Laptop Computers
- Networked CPUs
- Floppy Diskettes
- CD / DVD
- Hard Drives- External and Internal
- Solid State drives
- Thumb drive/Flash Memory/SD cards
- Digital watches
- Tapes
- PDAs
- Cell Phones
- Digital Cameras

1.9 Search & Seizure

1.9.1 Steps in Crime Scene Investigation

Cyber crime scene is completely different from the conventional crime scene. As mentioned earlier, the digital evidence is highly fragile, and it can be tampered easily and stealthily. Utmost care and, precautions are required during search, collection, preservation, transportation and examination of evidence.

The sequences of steps for digital crime scene investigations are:

- Identifying and securing the crime scene
- 'As is where is' documentation of the scene of offence
- Collection of evidence



- ✓ Procedure for gathering evidences from Switched-off Systems
- ✓ Procedure for gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labelling and, documenting of the evidence
- Packaging, and transportation of the evidences

The identification and securing of crime scene has been dealt in detail in the Pre-investigation assessment of the Crime and, various guidelines / instructions have been given to ensure capturing of the situation at the scene of crime scene through, as is where is documentation process.

1.9.2 Seizure Proceedings

Panchanama and seizure procedure is as important in cyber crime investigation as in any other crime. The Investigating Officer may have to take additional care while conducting Panchanama and seizure of digital evidences, keeping in mind the nature of digital evidences. Understanding the basics of digital devices and, ability to conduct a thorough pre-investigation assessment will be of great relevance for a proper search and seizure of relevant and admissible evidences from crime scene.

Below are few guidelines specific to cyber crime. The sequence of steps prescribed above for digital crime scene investigations, should be reflected in the Panchanama.

- Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.
- Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment at the scene of crime.
- Time Zone/System Time play a very critical role in the entire investigation. Please make sure this information is noted carefully in the Panchanama, from the systems that are in 'switched on' condition.
- Please DON'T switch ON any device.
- Please make sure a serial number is allotted for each device and the same should be duly noted not only in the Panchanama but also in the Chain of



Custody and Digital Evidence Collection forms.

- Make sure each device is photographed before starting of the investigation process at their original place along with respective reference like cubicle number or name room soundings, etc.
- Make sure to photograph the Hard Disk Drive or any other internal part along with the system, once removed from the system.
- If possible, please paste the serial number along with PF number/Crime number/section of law.
- Capture the information about the system and data you are searching and seizing in the Panchanama.
- Brief the witnesses regarding the tools used to perform search and seizure of the digital evidence.
- Make sure that the Panchanama have some knowledge and ability to identify various digital devices.
- Document the Chain of Custody and Digital Evidence Collection forms explained below, apart from your regular Panchanama as a 'best practice', for digital evidences.
- Please make sure all the details mentioned in the forms are completely filled.

1.9.3 Assess the Situation

After identifying the computer's power status, follow the steps listed below for the situation most like your own:

Situation 1: The monitor is on. It displays a program, application, work product, picture, e-mail, or Internet site on the screen.

1. Photograph the screen and record the information displayed.
2. Proceed to "If the Computer Is ON".

Situation 2: The monitor is on and a screen saver or picture is visible.

1. Move the mouse slightly without depressing any buttons or rotating the wheel. Note any on screen activity that causes the display to change to a login screen, work product, or other visible display.
2. Photograph the screen and record the information displayed.
3. Proceed to "If the Computer Is ON".



Situation 3: The monitor is on, however, the display is blank as if the monitor is off.

1. Move the mouse slightly without depressing any buttons or rotating the wheel. The display will change from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and record the information displayed.
3. Proceed to “If the Computer Is ON”.

Situation 4a: The monitor is powered off. The display is blank.

1. If the monitor’s power switch is in the off position, turn the monitor on. The display changes from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and the information displayed.
3. Proceed to “If the Computer Is ON”.

Situation 4b: The monitor is powered off. The display is blank.

1. If the monitor’s power switch is in the off position, turn the monitor on. The display does not change, it remains blank. Note that no change in the display occurs.
2. Photograph the blank screen.
3. Proceed to “If the Computer Is OFF”.

Situation 5: The monitor is on. The display is blank.

1. Move the mouse slightly without depressing any buttons or rotating the wheel; wait for a response.
2. If the display does not change and the screen remains blank, confirm that power is being supplied to the monitor. If the display remains blank, check the computer case for active lights, listen for fans spinning or other indications that the computer is on.
3. If the screen remains blank and the computer case gives no indication that the system is powered on, proceed to “If the Computer Is OFF”.

If the Computer Is OFF:

For desktop, tower, and minicomputers follow these steps:

1. Document, photograph, and sketch all wires, cables, and other devices connected to the computer.
2. Uniquely label the power supply cord and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire, or USB drive occupies on the computer.



3. Photograph the uniquely labelled cords, cables, wires, and USB drives and the corresponding labelled connections.
4. Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip, or battery backup device.
5. Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.
6. Place tape over the floppy disk slot, if present.
7. Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
8. Place tape over the power switch.
9. Record the make, model, serial numbers, and any user-applied markings or identifiers.
10. Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
11. Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

For laptop Computers Follow these Steps:

1. Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.
2. Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.
3. Photograph the uniquely labelled cords, cables, wires, and devices connected to the laptop computer and the corresponding labelled connections they occupied.
4. Remove and secure the power supply and all batteries from the laptop computer.
5. Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.
6. Place tape over the floppy disk slot, if present.
7. Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.



8. Place tape over the power switch.
9. Record the make, model, serial numbers, and any user-applied markings or identifiers.
10. Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
11. Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

If the Computer Is ON:

For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the computer display, however, you may need to request assistance from personnel who have experience in volatile data capture and preservation.

In the following situations, immediate disconnection of power is recommended:

1. Information or activity on screen indicates that data is being deleted or overwritten.
2. There is indication that a destructive process is being performed on the computer's data storage devices.
3. The system is powered on in a typical Microsoft® Windows® environment. Pulling the power from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands, and other valuable information.

In the following situations, immediate disconnection of power is NOT recommended:

Data of apparent evidentiary value is in plain view on screen. The first responder should seek out personnel who have experience and training in capturing and preserving volatile data before proceeding.

4. Indications exist that any of the following are active or in use:

- ❖ Chat rooms.
- ❖ Open text documents.
- ❖ Remote data storage.
- ❖ Instant message windows.
- ❖ Child pornography.
- ❖ Contraband.



- ❖ Financial documents.
- ❖ Data encryption.
- ❖ Obvious illegal activities.

For mainframe computers, servers, or a group of networked computers, the first responder should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems.

1.10 Forensic acquisition of digital devices

Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

Acquire the original digital evidence in a manner that protects and preserves the evidence. The following bullets outline the basic steps:

- Secure digital evidence in accordance with departmental guidelines.
- Document hardware and software configuration of the examiner's system.
- Verify operation of the examiner's computer system to include hardware and software.
- Disassemble the case of the computer to be examined to permit physical access to the storage devices.
 - Take care to ensure equipment is protected from static electricity and magnetic fields.
- Identify storage devices that need to be acquired. These devices can be internal, external, or both.
- Document internal storage devices and hardware configuration.
 - Drive condition (e.g., make, model, geometry, size, jumper settings, location, drive interface).
 - Internal components (e.g., sound card, video card, network card, including media access control (MAC) address, personal computer memory card international association (PCMCIA) cards).
- Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.



- Retrieve configuration information from the suspect's system through controlled boots.
 - Perform a controlled boot to capture CMOS/BIOS information and test functionality.
- Boot sequence (this may mean changing the BIOS to ensure the system boots from the floppy or CD-ROM drive).
- Time and date.
- Power on passwords.
- Perform a second controlled boot to test the computer's functionality and the forensic boot disk.
- Ensure the power and data cables are properly connected to the floppy or CDROM drive, and ensure the power and data cables to the storage devices are still disconnected.
- Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.
- Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.
- Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.
- Drive configuration information includes logical block addressing (LBA), large disk, cylinders, heads, and sectors (CHS) or auto-detect.
- Power system down.
- Whenever possible, remove the subject storage device and perform the acquisition using the examiner's system. When attaching the subject device to the examiner's system, configure the storage device so that it will be recognized.
- Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system:
 - RAID (redundant array of inexpensive disks). Removing the disks and acquiring them individually may not yield usable results.
 - Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.
 - Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.



- Equipment availability. The examiner does not have access to necessary equipment.
- Network storage. It may be necessary to use the network equipment to acquire the data.

When using the subject computer to acquire digital evidence, reattach the subject storage device and attach the examiner's evidence storage device (e.g., hard drive, tape drive, CD-RW, MO).

- Ensure that the examiner's storage device is forensically clean when acquiring the evidence.

Write protection should be initiated, if available, to preserve and protect original evidence.

Note: The examiner should consider creating a known value for the subject evidence prior to acquiring the evidence (e.g., performing an independent cyclic redundancy check (CRC), hashing). Depending on the selected acquisition method, this process may already be completed.

- If hardware write protection is used:

- Install a write protection device.
- Boot system with the examiner's controlled operating system.

- If software write protection is used:

- Boot system with the examiner-controlled operating system.
- Activate write protection.

- Investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas (e.g., nonhost specific data such as the partition table matches the physical geometry of the drive).

- Capture the electronic serial number of the drive and other user-accessible, host-specific data.

- Acquire the subject evidence to the examiner's storage device using the appropriate software and hardware tools, such as:

- Stand-alone duplication software.
- Forensic analysis software suite.
- Dedicated hardware devices.

- Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.



1.11 Digital evidence handling

There are a number of discreet elements that accompany the collection and handling of digital evidence.

Step 1- Identifying digital evidence : Evidence discovered in digital format may be the first sign that something is wrong. For instance, a security administrator to a bank might consider an investigation may be needed where the intrusion detection system sets off an alarm, or where the email logs indicate that a particular member of staff is receiving an excessive number of emails during a day or over an extended period. In such a case, the source and reliability of the information needs to be assessed, which requires an investigation into the facts.

Step 2- Gathering digital evidence : Once it has been established that it is necessary to seize or gather evidence in digital format, a further set of procedures should be in place to guide the digital evidence specialist in respect to the scene itself, including the identification and seizure of the evidence if necessary. It is important not to permit anybody to disturb the hardware or the network, or work on a computer that is liable to being seized and retained, and it is admissible that the police officers that are engaged in searching for digital evidence should be properly trained. Data can be deleted on a remote server or cloud storage before it can be secured.

There are two fundamental principles in relation to copying digital evidence that a digital evidence specialist should be aware of :

- (a) The process of making the image should not alter the original evidence. This means that the appropriate steps should be taken to ensure that the process used to take the image should not write any data to the original medium.
- (b) The process of copying data should produce an exact copy of the original. Such a reproduction should allow the specialist to investigate the files in the way they that existed on the original medium.

Step 3 - Preserving digital evidence : Digital evidence in particular needs to be validated if it is to have any probative value. A digital evidence specialist will invariably copy the contents of a number of disks or storage devices, in both criminal and civil matters. To prove the digital evidence has not been altered, it is necessary to put in place checks and balances to prove the duplicate evidence in digital format has



not been altered since it was copied. The method used to prove the integrity of data at the time the evidence was collected is known as an electronic fingerprint. The electronic fingerprint uses a cryptographic technique that is capable of being associated with a single file, a floppy disk or the entire contents of a hard drive. As digital evidence is copied, so a digital evidence specialist should use software tools that are relevant to the task.

Step 4 - The chain of custody : However, the chain of custody, in both civil and criminal matters, should be considered very carefully in respect to digital evidence. The reason for taking particular care with digital evidence is because it is easy to alter. It is necessary to demonstrate the integrity of the evidence and to show it cannot have been tampered with after being seized or copied. There is another reason for being meticulous about ensuring the chain of evidence is correctly recorded. In a case involving a number of items of hardware and more than one computer, it will be necessary to ensure there is a clear link between the hardware and the digital evidence copied from the hardware. In this respect, the record should address such issues that who collected the evidence, how and where it was collected, the name of the person who took possession of the evidence, how and where it was stored, the protection afforded to the evidence while in storage and the names of the people that removed the evidence from storage, including the reasons for removing the evidence from storage.

Step 5- Transporting and storing digital evidence : Consideration should be given to the methods by which any hardware and digital evidence is transported and stored. Computers need to be protected from accidentally booting up consideration should be taken to ensure that hardware is clearly marked to prevent people from using the equipment unwittingly and loose hard drives, modems, keyboards and other such materials should be placed in anti-static or aerated bags. Storage conditions should be appropriate. Hardware and digital evidence should be protected from dirt, humidity, fluids, extremes of temperature and strong magnetic fields. It is possible for data to be rendered unreadable if the storage media upon which the digital evidence is contained are stored in a damp office or overheated vehicle during the summer.



1.12 Chain of Custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analysing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the concerned person. It is possible that defence may level charges of tampering and fabrication of evidence and, it would be difficult to prove the integrity of the evidence, if the chain of custody is not properly maintained.

Important Points to remember for Foolproof Chain of Custody:

- Physically inspect the storage medium — take photographs and systematically record observations.
- Guard against hazards like theft and mechanical failure. Use good physical security and data encryption. House multiple copies in different locations.
- Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and data to a minimum.
- Always accompany evidence with their chain-of-custody forms.
- Give the evidence positive identification at all times that is legible and written with permanent ink.
- Establishing the integrity of the seized evidence through forensically proven procedure by a technically trained investigating officer or with the help of a technical expert will enhance the quality of the evidence when the case is taken forward for prosecution. The integrity of the evidence available on a digital media can be established by using a process called as “Hashing”.
- Establish a baseline of contents for authentication and proof of integrity by calculating hash value for the contents. An identical hash value of the original evidence seized under Panchanama and, the forensically imaged copy, helps the IO to prove the integrity of the evidence. Similarly, the seized original evidence can be continued to be checked for its integrity by comparing its



hash value, to identify any changes to it.

- A reliable hash proves that the media contents have not been altered. Hashing program produces a fixed length large integer value (ranging from 80 – 240 bits) representing the digital data on the seized media. Any changes made to the original evidence will result in the change of the hash value.

1.13 Legal Report Writing

The results of forensic related investigations are often detailed in a forensic report. These reports are often used as proof of what was found or not found. These reports are very important to a case, since the improper processing of the data or missing key evidence can mean the difference between winning and losing a case. The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination. All documentation should be complete, accurate, and comprehensive. The resulting report should be written for the intended audience.

What does a Forensic Report consist of?

A good forensic report typically contains several sections to help the reader understand not only what was found (or not found) by the investigator but also to detail the steps performed to acquire the data and analyse the data. This process is commonly referred to as the “Chain of Custody” and is very important in showing proper evidence handling. The first step in documenting proper Chain of Custody is detailing in the forensic report how the data got to the investigator and what steps were taken to secure its transit. This can include notes regarding secure delivery via courier, secure file transfer, or forensic collection. The report should also list all software and hardware used to process the data, including versions of the software tools. The investigator will often detail in the report, the time zone the evidence was set to run in, and will process the data in that time zone. So that date and time stamped items will be read in their correct time zone. A very important item that should exist in all reports is a verification of the original data via “hashing” to show that the data being examined is an exact replica of the original.

After that, a typical report will detail everything the investigator does to process the



data and search for what is needed. The steps are usually documented in chronological order with screen shots as needed to help the reader understand what was happening at the time. Also included in a typical report is notes regarding any encrypted files that were found and what was done to them, meaning whether they were decrypted to find out their contents, or left encrypted and not processed or examined.

Keyword searching is another common task performed by investigators, and the keywords are usually agreed to in advance by the client asking for the investigation. It is customary to document those keywords in the forensic report in case they are ever needed in the future or if any questions come up. At the end of the forensic report, a section should be included that is a summary or conclusion of the investigation. This summary will state any facts or conclusions that the investigator has identified that need to be reviewed.

1.13.1 Examiner's notes

Documentation should be contemporaneous with the examination, and retention of notes should be consistent with departmental policies. The following is a list of general considerations that may assist the examiner throughout the documentation process.

- Take notes when consulting with the case investigator and/or prosecutor.
- Maintain a copy of the search authority with the case notes.
- Maintain the initial request for assistance with the case file.
- Maintain a copy of chain of custody documentation.
- Take notes detailed enough to allow complete duplication of actions.
- Include in the notes dates, times, and descriptions and results of actions taken.
- Document irregularities encountered and any actions taken regarding the irregularities during the examination.
- Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.
- Document changes made to the system or network by or at the direction of law enforcement or the examiner.
- Document the operating system and relevant software version and current installed patches.
- Document information obtained at the scene regarding remote storage, remote



user access, and offsite backups.

Note: During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the case agent because the information may be needed to obtain additional search authorities.

1.13.2 Examiner's report

This section provides guidance in preparing the report that will be submitted to the investigator, prosecutor, and others. These are general suggestions that the departmental policy may dictate report writing specifics, such as its order and contents.

The report may include:

- ✓ Identity of the reporting agency.
- ✓ Case identifier or submission number.
- ✓ Case investigator.
- ✓ Identity of the submitter.
- ✓ Date of receipt.
- ✓ Date of report.
- ✓ Descriptive list of items submitted for examination, including serial number, make, and model.
- ✓ Identity and signature of the examiner.
- ✓ Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
- ✓ Results/conclusions.

1.13.3 Summary of findings

This section may consist of a brief summary of the results of the examinations performed on the items submitted for analysis. All findings listed in the summary should also be contained in the details of findings section of the report.

1.13.4 Details of findings

This section should describe in greater detail the results of the examinations and may include:

- Specific files related to the request.



- Other files, including deleted files that support the findings.
- String searches, keyword searches, and text string searches.
- Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity.
- Graphic image analysis.
- Indicators of ownership, which could include program registration data.
- Data analysis.
- Description of relevant programs on the examined items.
- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.

1.13.5 Structure of a Digital Forensic Report

Generally, the forensic report is outlined as follows:

- 1) Brief summary of information.
- 2) Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool.
- 3) Evidence Item #1: Employee A's work computer.
 - a) Summary of evidence found on Employee A's work computer
 - b) Analysis of relevant portions of Employee A's work computer
 - i) Email history
 - ii) Internet search history
 - iii) USB registry analysis
 - c) Repeat steps above for other evidence items, including work computers and mobile devices etc.
- 4) Recommendations and Next Steps for counsel to continue or cease investigation based on the findings in the report.

The report should not volunteer superfluous information which may be vulnerable to scrutiny under cross-examination. Further, all findings should be accurately qualified as to the limitations of the particular tool(s) used, the applicability of the current technology and industry-standard best practices, the methodology or techniques (such as search criteria or formulae), and the scope of the investigation.

The scope of the investigation is limited by relevancy and also by budget (i.e., time), which almost always places legitimate and significant constraints on what data is



Chapter 1 - Digital Forensics & Investigations

found or not found and the inferences to be drawn there from. Moreover, the digital forensic report only investigates those areas where responsive evidence can be found (e.g., in a case investigating the theft of proprietary software code, it would be irrelevant to discuss a search for pornography on said hard drive, and law enforcement officials may require a separate warrant to conduct such a search).

Further, when evaluating a digital forensic report, a reviewer should evaluate the substance of the report to ascertain if there is information overload. The digital forensic report should provide a cohesive and logical framework on its face and not delve into the underlying technical minutiae that could distract from its conclusions.

Examiners must resist overtures by attorneys, however well-intended or abstract, to submit any testimony or work product that is disrespectful of the truth, including overstating, understating, or omitting findings. The findings should be concise and carefully circumscribed. The report cannot be tailored to support a particular outcome, as a material omission may constitute fraud.