

# Digital Forensics

By Viral Parmar





# Who Am I

@viralparmarhack

Viral Parmar

ComExpo Cyber Security Foundation

Cyber Security Researcher

Mozilla Reps, Mozilla Foundation

Given 700+ session all over the world

Solved 500+case of cyber crime and aware more then  
10 lakh people about privacy and security

Motto: **Know hAckiNG, but no HaCKing.**



# History

- **1970s-1980s:** First Computer Crime
- In **1978** the first computer crime was recognized in Florida Computer Crime Act
- included legislation against unauthorized modification or deletion of data on a computer system
- over the time, due to the advancement of technology, the range of computer crimes being committed also increased
- To deal with crimes related to copyright, privacy and child pornography, various other laws were passed
- **1980s-1990s:** known as the Development Decade
- the first ever investigation (1986) in which Cliff Stoll tracked the hacker named Markus Hess happened
- two kind of digital forensics disciplines:
  - ad-hoc tools and techniques developed by practitioners as a hobby
  - developed by scientific community

- **2000s-2010s:** Decade of Standardization
- The need for making some specific standards that can be followed while performing investigations arose
- Scientific agencies and bodies started publishing guidelines for digital forensics
- **2002:** Scientific Working Group on Digital Evidence (SWGDE) published a paper named “Best practices for Computer Forensics”

# Digital Forensics

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from the digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

**Definition** Application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation

# Objectives of Digital Forensics

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

# Challenges for Digital Forensics

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

# Process of Digital Forensics

## Identification

- Identify the purpose of investigation
- Identify the resources required

## Preservation

- Data is isolate, secure and preserve

## Analysis

- Identify tool and techniques to use
- Process data
- Interpret analysis results

## Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

## Presentation

- Process of summarization and explanation of conclusions is done with the help to gather facts.



# Locard's Principle

**Edmund Locard** (1877–1966) was the director of the first (according to some) crime lab, in Lyon, France

Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it can diminish its value.

**Locard's Exchange Principle:** in the physical world, when perpetrators enter or leave a crime scene, they will leave something behind and take something with them.

# Digital Evidence

Digital evidence act, The Bureau of Indian Standards Act, Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital evidence.

# Forensics Organizations

Scientific Working Group on Digital Evidence (SWGDE)

<http://www.swgde.org/>

- Made up of federal government agency, state or local law enforcement agency involved in the digital and multimedia forensic profession

American Academy of Forensic Sciences (AAFS)

<http://www.aafs.org/>

- Considered the premier forensic organization in the world
- Members of the Academy work for the National Institute of Standards and Technology (NIST) and National Academy of Sciences (NAS)

American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)

<http://www.ascl-d-lab.org/index.htm>

Oldest and most well known crime/forensic laboratory accrediting body in the world

## American Society for Testing and Materials (ASTM)

<http://www.astm.org/Standards/E2763.htm>

Global organization that has developed approximately twelve thousand standards

Improve product quality, enhance safety, facilitate market access and trade, and build consumer confidence.

## National Institute of Standards and Technology (NIST)

<http://www.nist.gov/itl/ssd/computerforensics.cfm>

- Founded in 1901
- Part of the U.S. Department of Commerce
- The first federal physical science research laboratory

### 1.National Initiative Cyber Security Education (NICE)

cybersecurity education program

### 2.National Software References Library

collection of known software file signatures

can be used by forensic examiners to quickly exclude files that have no investigative value

### 3.Computer Forensic Tool Testing

develop testing methodologies and standards for forensic hardware and software

# International Organization on Computer Evidence

The International Organization on Computer Evidence (IOCE) was established in 1995

Provides international law enforcement agencies a forum for the exchange of information concerning computer crime investigation and other computer-related forensic issues

IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendations for consideration by its member agencies

## IOCE International Principles

The international principles developed by IOCE for the standardized recovery of computer-based evidence are governed by the following attributes

- Consistency with all legal systems
- Allowance for the use of a common language
- Durability
- Ability to cross international boundaries
- Ability to instil confidence in the integrity of evidence
- Applicability to all forensic evidence
- Applicability at every level, including that of individual, agency, and country

These principles were presented and approved at the International Hi-Tech Crime and Forensics Conference in October 1999. They are as follow:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

# Classification of Cyber Forensics

## **Disk forensics**

- deals with extracting data/information from storage media
- searching active, deleted files and also from unallocated, slack spaces.

## **Network forensics**

- 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.
- Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

## **Wireless forensics**

- sub-discipline of network forensics.
- main goal is to provide the methodology and tools required to collect and analyze wireless network traffic data.
- 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**

Branch of digital forensic science relating to the forensic study of databases and their related metadata. 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.

### **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.

### **Mobile device forensics**

deals with examining and analysing mobile devices like mobile phones, pagers to retrieve addresses book, call logs (Missed, Dialed, Received), Paired Device History, Incoming/Out Going SMS/MMS, Videos, Photos, Audio.etc.



### **GPS forensics**

also known as SatNav Forensics, relatively new discipline within the fast paced world of Mobile Device Forensics

used for examining and analysing GPS devices to retrieve Track Logs, Track points, Waypoints, Routes, Stored Location; Home, Office, etc,.

### **E-mail 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.

# Live Acquisition of Evidence

A live acquisition is where data is retrieved from a digital device directly via its normal interface; for example, switching a computer on and running programs from within the operating system. This has some level of risk, as data is likely to be modified. This process is rapidly becoming the more common approach as disk drive capacities increase to the point where they are impractical to 'image' and technology such as 'cloud computing' means that you cannot even access the hardware in many cases

Order of volatility of digital evidence

1. CPU, cache and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system / swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

# Hashing

Hash analysis. You have used the MD5 and/or SHA1 hash to verify acquisitions of digital evidence, such as hard drives or removable media. You'll use that same MD5 and/or SHA1 hash to derive hash values of individual files and compare them to known databases of hash values. In this manner, you can identify known files by their MD5 and/or SHA1 hash. If they are known safe files, such as program files, they can be eliminated from further analysis. If they are known contraband files, they can be quickly identified and bookmarked.

**Tools:** Hex Editor, Win Hex, Hash Check, Igorware, Garry kesler database of file signatures, Hash File database, HashMyFiles

# Imaging & Analysis of Logical & Physical Drives

We never do a forensic investigation on a live system's disk (can also be done in some special cases to be discussed later). So, that the original disk can be prevented from any alteration or modification which can occur during Forensic Analysis. Disk Imaging, it is the process in which, we use tools that make an exact copy of the hard disk that can be examined using some special forensic investigation tools covered in the later sections.

**Tools:** The Sleuth Kit Autopsy, Helix, Access Data FTK Imager, EnCase Tool, Magnet forensics tool, X-Ways Forensics, Shadow explorer, USB Write Blocker, Guymager

# Retrieving & Reviewing Logs

Logging consists of recording information about what a system—for instance, an application—does when executing. We write these recordings to some persistent medium, such as a database table or a file in the disk. That way, we can access such information afterward and review it, but why would that be a desirable thing? The primary use for logging of any kind is troubleshooting. Reading through log entries gives you this sort of time-travel power. By reading application logs, for instance, you can retrace the actions a user performed in an application, so you can understand and fix a problem

**Tools:** Process Explorer, PE Viewer , Log Parser, LastActivityView, Dependency walker, Registry Explorer, Resource Hacker

# OS Forensics

Operating System Forensics is that the process of retrieving useful information from the OS (OS) of the pc or mobile device in question. The aim of collecting this information is to accumulate empirical evidence against the perpetrator. “OS Forensics” involves forensic examination of the OS of the pc . the foremost commonly used operating systems are Windows, Mac, and Linux. it’s highly likely that the forensic investigators may encounter one among these operating systems during any crime investigation. it’s imperative that they need thorough knowledge about these operating systems, their features, methods of processing, data storage and retrieval also as other characteristics.

**Tools :** OS Forensics

# Extracting Information from File

Metadata, often described as data about data, allows digital or computer forensic investigators to understand the history of a particular electronic file, including when the file was created, modified and accessed, among other information that can be used to describe the file. The file can be in any digital format, ranging from a document file to a spreadsheet, image, video and audio, as well as web pages.

Just like a regular investigator would follow a paper trail, which is a series of written evidence, computer forensic investigators would follow a digital trail instead. This means reviewing digital data and their metadata, the unique identifying markers associated with each digital file, to look for evidence that can help a legal argument.

**Tools:** E-Discovery, Exif Data Viewer, Ghirio, Photorec, Agent Ransack, NFI Defraser, Forensic User Info, Jeffrey's Metadata viewer, Mosses Forensics Tool, Forensically, Fotoforensics, Tineye Reverse Image Search

# Volatile Memory Forensics

The ability to analyze RAM/volatile memory is one of the reasons to never shut down computers at the time of their acquisition. Forensic specialists acquiring a running PC should always capture appropriate memory dumps before unplugging the PC and extracting the hard drive. However, even if the PC has not been acquired properly, volatile memory content can still be available for analysis in the form of page file(s) and hibernation file.

**Tools:** Volatility, Dumpit, RamDump, Magnet Ram capture, FTK Imager, Belkasoft Live RAM Capturer, WindowsScope



# USB Forensics

Universal Serial Bus flash drives, commonly known as USB flash drives are the most common storage devices which can be found as evidence in Digital Forensics Investigation. The digital forensic investigation involves following a defined procedure for investigation which needs to be performed in such a manner that the evidence isn't destroyed.

**Tools :** USB Deview, USB Historian

# 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. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation. It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

**Tools:** NMAP, Wireshark, Xplico, Cacti Network Forensics Tool, Angry IP Scanner, Network Miner, packet analyzer

# Multimedia Forensics

Multimedia Forensics includes a set of scientific techniques recently proposed for the analysis of multimedia signals (audio, videos, images) in order to recover probative evidences from them; in particular, such technologies aim to reveal the history of digital contents identifying the acquisition device that produced the data, validating the integrity of the contents, retrieving information from multimedia signals.

**Tools :** Hide n Send, wbStego, invisible secret, Sonic visualizer, Openpuff, Netcross, Spammimic

# Browser & Email Forensics

Browsers have become an inherent part of our virtual life and we all make use of browsers for surfing the internet in some or the other way. Also, browsers can be used not only for surfing, we can make use of browsers for navigating through the file system of the OS. Also, browsers do contain downloaded media like Images, Videos, Exe's, documents etc. Bookmarks and browser history gives an idea of a user's surfing habit and interest. You might have realised browsers store a lot of sensitive information about users and its surfing habit. Thus they play a very important role in forensics due to the nature and amount of data they store with them.

**Tools:** Bulk extractor, Browser History, Dumpzilla, Mail Examiner, Email tracker

# Mobile Forensics

Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices. “Forensically sound” is a term used extensively in the digital forensics world to qualify and justify the use of a particular forensic technology or methodology. The central principle for a sound forensic examination is that the original evidence must not be modified. It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

**Tools:** Oxygen forensics, Google Maps Investigator, Mobiledit

# Malware Forensics

Investigating and Analyzing Malicious Code covers the complete process of responding to a malicious code incident. Written by authors who have investigated and prosecuted federal malware cases, this book deals with the emerging and evolving field of live forensics, where investigators examine a computer system to collect and preserve critical live data that may be lost if the system is shut down. Unlike other forensic texts that discuss live forensics on a particular operating system, or in a generic context, this book emphasizes a live forensics and evidence collection methodology on both Windows and Linux operating systems in the context of identifying and capturing malicious code and evidence of its effect on the compromised system.

**Tools:** PE Studio, OllyDbg, Malware Database, Sandboxie, Cuckoo

# Cloud Forensics

It is the application of digital forensics in the cloud and it is a subset of network forensics and preserve evidence in a way that is suitable for presentation in a court of law. It is harder to identify evidence in cloud infrastructure since the data are located in different geographical areas. Some examples of evidence sources are system log, application log, user authentication log, database log, etc.

**Tools** : Encase, FTK, Forst, UFED, Docker Forensics Toolkit & Docker Explorer

# Data Recovery

Data recovery is a process of salvaging (retrieving) inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a usual way. The data is most often salvaged from storage media such as Internal or external hard disk drives (HDDs), Solid-state drives (SSDs), USB flash drives, Magnetic tapes CDs, DVDs, RAID subsystems and other electronic devices.

**Tools :** Foremost, Recuva, Mini tool power data recovery, EaseUS, EDB Viewer, Disk Drill, ISOBuster



# Anti-Computer Forensics

Anti-forensics has only recently been recognized as a legitimate field of study. Within this field of study, numerous definitions of anti-forensics abound. One of the more widely known and accepted definitions comes from Marc Rogers of Purdue University. Rogers uses a more traditional "crime scene" approach when defining anti-forensics. "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.

**Tools:** CCleaner, Evidence Eliminator, Privacy Eraser, DBAN (Darik's Boot and Nuke), Blancco, Minitool partition wizard, KillDisk, Eraser, Disk Wipe, PC Shredder, DeleteOnClick

# Computer Forensics Best Practices

Forensic examiners adhere to specific standards and rules for conducting examinations that are designed to insure that the original evidence is not altered while in their custody, and to insure that their evidence is later admissible in court. Most best practices and policies are written with those goals in mind.

Whenever possible, do not examine the original media. Write protect the original, copy it, and examine only the copy.

- Use write blocking technology to preserve the original while it is being copied.
- Computer forensic examiners must meet minimum proficiency standards.
- Examination results should be reviewed by a supervisor and peer reviewed on a regular schedule.
- All hardware and software should be tested to insure they produce accurate and reliable results.
- Forensic examiners must observe the highest ethical standards.
- Forensic examiners must remain objective at all times.
- Forensic examiners must strictly observe all legal restrictions on their examinations.

# Setup Forensics Lab

The need to forensically boot computers still exists, regardless of how much technology has advanced over the years. Traditionally, booting a computer to a modified floppy disc for imaging was the most commonly accepted practice. Today, forensic analysts have options in identifying, collecting, and preserving data from evidence computers. One of these options is still booting the machine to a forensic operating system.

**Tools:** Santoku OS, DEFT OS, Parrot OS, SOF-ELK, SANS Investigative Forensic Toolkit (SIFT), CAINE (Computer Aided INvestigative Environment ) + Win UFO (Windows Ultimate Forensics Outflow)

# Toolkits and Bootable Suites

The Coroner's Toolkit (or TCT) is a suite of free computer security programs by Dan Farmer and Wietse Venema for digital forensic analysis.







**Tools:** NirSoft launcher, Windows Sysinternal Tool Suite, FAW (Forensics Acquisition of Websites), Toolsley







# Incident Response

Introduction to the Incident Response Process What Is a Computer Security Incident? , What Are the Goals of Incident Response? , Who Is Involved in the Incident Response Process? , Incident Response Methodology, Pre-Incident Preparation, Detection of Incidents, Initial Response, Formulate a Response Strategy, Investigate the Incident, Reporting, Resolution.

**Tools:** FireEye RedLine, Cyber Triage, Alien Vault, IBM QRadar, Splunk , Solar winds

# Digital Evidence

SI No	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 analyze 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 and biometric scanners etc.		The device itself, along with the identification/ authentication information of the card and the user, level of access, configurations and permissions.
4	Answering Machines		The device can store voice messages and sometimes, the time and date information about 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, removable cartridges, time & date stamps.
6	Handheld Devices(Personal Digital Assistants [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), e-mails passwords etc.

SI No	Digital Device		Potential evidence
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 to 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

SI No	Digital Device		Potential evidence
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 stripe contain Cardholder's information which may include: I Card expiration date. I User's address. I Credit card numbers. I 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 Systems (GPS)		The device may provides travel logs, home location, previous destinations, way point coordinates, way point name etc.
23	Keyboard & Mouse		These devices can be examined for fingerprints.



13	Printers		The device has data like number of prints last printed and some maintain usage logs, time & 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 telephones can store appointment information, and may act as a voice recorder.

# Forensic Duplication

**Forensic duplication:** bit stream imaging of data from the digital media

**Storage:** computers, smart phones, GPS devices, USB drives etc.

We need to retrieve the information without changing the information on the devices

## **Two techniques for copying:**

Logical backup:

- Copies the directories and files of a logical volume
- Does not capture other data that may be present on the media
- Deleted files or residual data not captured

Bit stream imaging:

- Also known as disk imaging or cloning
- Generates a bit-for-bit copy of the original media
- Require more storage space and take longer to perform than logical backups

# Network Drives Imaging and Logical File Collection

There are scenarios in which it is not possible to take the evidence machine offline,

- like the machine may be a file server or a database server
- services business-critical applications
- In the course of the interview, we need to determine if the machine has any relevant data and if so, where it is stored.

Data is copied to external drives using forensic tools

- Another method of acquiring hard drive's data is via a network cable between
- a machine containing the target media, booted to forensic tool for DOS
- a second machine running forensic tool in the Windows environment
- Sometimes removing a hard drive from a laptop is problematic due to physical access or other concerns, such as proprietary security schemes attaching the hard drive to the mother-board.

A network cable acquisition is also very handy when the owner or user of the target hard drive is not physically present

- connect the examination laptop to the target machine via a network cable
- boot to forensic tool for DOS
- preview or acquire if needed
- quickly acquire data from the target hard drive

Network cable to be used:

- A “yellow” crossover cable
- Often a crossover cable has a tag or label to denote it
- A crossover cable is a network cable used for special purposes
- One purpose is to enable two computers to have network connectivity by connecting directly to each other via a single network cable

# Gathering Evidence

Crime scene investigators document the crime scene. They take photographs and physical measurements of the scene, identify and collect forensic evidence, and maintain the proper chain of custody of that evidence. Once the crime scene has been thoroughly documented and the locations of the evidence noted, then the collection process can begin. The collection process will usually start with the collection of the most fragile or most easily lost evidence. Special consideration can also be given to any evidence or objects which need to be moved. Collection can then continue along the crime scene trail or in some other logical manner. Photographs should also continue to be taken if the investigator is revealing layers of evidence which were not previously documented because they were hidden from sight.

# Guidelines for collecting evidence

- 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.

### **Hashing program**

- produces a fixed length large value (ranging from 80 – 240 bits)
- Represents the digital data on the seized media
- Any changes made to the original evidence will result in the change of the hash value
- Hashing is applying a mathematical algorithm
- A file/disk/storage media
- Produce a value that is unique like fingerprint to that file/disk/dataset
- Any changes that will be made in the file/dataset will in turn change/alter the hash value
- Hash value is usually alphanumeric

# Forensic Collection of Digital Media

Identifying/Seizing of the devices needs to be forensically imaged for analysis

- Pre-investigation assessment must be complete and accurate before commencing the Crime Scene Investigation
- Be ready to identify all the relevant parties and equipment at the scene
- If the person at the scene of crime is not able to tell if the device is relevant for investigation, seize it
- Documentation tools
- Pen and paper for notes
- Stick-on labels etc.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types
- Screwdrivers
- Wire cutters etc.
- Packaging and transporting supplies
- Bubble wraps
- Sturdy boxes etc.
- Other miscellaneous items
- Gloves
- Magnifying glass
- Small flashlight



Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	

Computer Information			
<input type="checkbox"/> Laptop	<input type="checkbox"/> Desktop	Manufacturer	
<input type="checkbox"/> HDD Only	<input type="checkbox"/> External HDD	Model Number	
<input type="checkbox"/> Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	

Acquisition Information			
<input type="checkbox"/> IDE	<input type="checkbox"/> SCSI	Manufacturer	
<input type="checkbox"/> SATA	<input type="checkbox"/> Other	Model Number	
		Serial Number	
		HDD Size	

Collection Details		Destination Drive Details	
Software used		Manufacturer	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

# Evidence Handling

Collecting and handling digital evidence is a crucial part in performing digital forensics. Not collecting the right evidence or mishandling evidence can lead to a perpetrator not getting convicted for their crime. Everything from the way digital evidence is collected to the way it is worked with and even stored plays a vital role in court proceedings. For example, once an incident is made apparent, it is advised that evidence gathering procedures be initiated. In this way, you will be more likely to gather all pertinent evidence before they become lost or deleted.

# Chain of custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence

- People who have seized the equipment
- People in charge of transferring the evidence from the crime scene to the forensic labs
- People in charge of analysing the evidence etc.

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number.....	Date of Seizure.....
Name of the I.O.....	Time.....
P.F.Number.....	

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

--

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

# Packaging and labelling of the evidence

Package and labeling refers to collection of the evidence

- Numbering them in a way that it would be easy to go back and retrieve the data at a later date/time
- Every piece of evidence needs to get a tag number
- Contains all the visible details on the evidence
- This information goes into evidence Database
- The IO has to choose packaging that is of proper size and material, to fit into the evidence

Various types of evidence need special packaging,

- Need to come to the scene prepared with a variety of evidence envelopes, bags, and containers
- The packaging should also be clean, and preferably new, to avoid contamination
- Each piece of evidence should be packaged separately
- Should be properly labeled, sealed, and documented
- Use anti-static bags to transport evidence
- These will protect and prevent any localized static electricity charge from being deposited onto the devices as the bags are handled

# Transportation of the evidences

The dispatch and transportation of evidences is another crucial aspect that has to be kept in mind by the IOs

- Poor dispatching and transportation practices can physically damage the evidences collected and thereby rendering them useless
- Sometimes, the poor handling may result in alteration of the contents of the digital evidences due to shock and external electro-magnetic interferences

Two things to ensure while sending the evidences to the Forensic Science Laboratories

- The suspected computer storage media is carried by a special messenger and not by Registered / Insured post
- A fresh hard disk of approximately same capacity should also be submitted for forensic imaging along with the suspected storage media.

# PF - PreFetch

PF number:

- In windows, there are prefetch artifacts
- In order to improve customer experience, Microsoft introduced a memory management technology called Prefetch

This mechanism

- analyses the applications that are most frequently used
- preloads them in advance
- done in order speed the operating system booting and application launching
- The Prefetch files are stored in %SYSTEMROOT%\Prefetch directory and have a .pf extension

Why is prefetch important in forensic analysis?

- Prefetch files keep track of programs that have been executed in the system even if the original file is no longer present
- Prefetch files can tell us
- when the program was executed,
- how many times and from which path



# Legal procedure post-seizure of evidence

Once the digital evidence is seized during the course of investigation, it has to be brought to the notice of the jurisdictional court

- Obtain orders of the competent court to retain the seized properties in the custody of the investigating officer for the purpose of investigations
- Obtain necessary orders from the competent court to image the data
- Send the digital evidence for forensic analysis and expert opinion

In cases where the accused persons or the owners of the property seized approaches the court for release of the impounded properties

- IO should carefully prepare objections for such applications
- Ensure that no original evidences are returned which have a bearing on the prosecution of the case
- Unless the court specifically orders, releasing seized properties means releasing a forensically imaged copy

# Four principles for dealing with digital evidence

1. No actions performed by investigators should change data
2. Individuals accessing original data must be competent to do so
3. An audit trail must be created and preserved documenting each investigative step
4. The person in charge of the investigation has overall responsibility for ensuring the laws and guidelines of the government

# Expert Opinion from the Forensic Examiner

The forwarding letter to the FSL for scientific analysis and opinion should mention information like:

- Brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of crime
- The condition of the computer system (on or off) at the scene of crime
- Is the photograph of the scene of crime taken?
- Is it a stand-alone computer or a network?
- Does the computer have any Internet connection or any means to communicate with external computers?
- Were the BIOS date and time stamps taken, or not? If taken the date and time should be mentioned

# Annexure 5-5: Requisition letter to FSL

## Forwarding Note

(In all cases where examination of any material is required at the laboratory, a copy of this form duly filled in should accompany the exhibits.)

Case No.-    /20xx	Police Station -
Section of Law -	Dist.-
Date -        /        /	State -

### I. Nature of Crime

Nature of Crime.....

.....

Brief History .....

.....

Any other relevant details.....

### II – List of Exhibits for Examination

Sr. No. / Barcode	Description of Exhibits	How, when, and by whom found	Source of exhibits	Remarks

### III – Nature of Examination required

Sr. No. / Barcode	Description of Exhibits	Nature of Examination required	Date or any keyword or filter	Remarks

IOs are advised to pay additional attention to this section, as this plays a critical component in the investigation. Apart from requesting the information required for the investigation like files, deleted information, etc., from the digital evidence, lot of other information, which can be developed as supporting ( secondary) evidence in the investigations like login time, users list, various applications installed, IP address, printers connected, etc.

IOs are suggested to contact the forensic lab professionals to understand what kind of information can be retrieved from these digital media which can be vital evidence.

Sr. No.	Full Name	Occupation	Sex	Date and Time of arrest	Whether bailed, court or Police Custody

Seal	Rank and Sign. of the I. O.
O/W No.- .....	Date - .....
Forwarded to the Director,.....	
Specimen Seal/s impression/s on exhibits or parcel/s	Sign and Designation of Forwarding Officer

**Certificate of Authority**

Certified that the Director .....  
has the authority to examine the exhibits sent to him in connection with Case No.  
..... u/s ..... Pol. St .....  
Date ..... of .....State versus .....

Date:	
Place:	Sign and Designation of Forwarding Authority

# Performing Digital Forensics

- Acquisition
- Validation & Verification
- Extraction
- Reconstruction
- Reporting

# Acquisition

- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote, live, and memory acquisitions



# Validation & Verification

**Validation:** a way to confirm that a tool is functioning as intended

**Verification:** proves that two sets of data are identical by calculating hash values or using another similar method

## **Filtering**

- Related process
- Involves sorting and searching through investigation findings
- Separate good data and suspicious data

# Extraction

- Data viewing
- Keyword searching
- Decompressing
- Carving: technique of reassembling files from raw data fragments when no filesystem metadata is available
- Decrypting
- Bookmarking or tagging

# Reconstruction

## **Purpose**

Re-create a suspect drive to show what happened during a crime or an incident  
Create a copy for other digital investigators if a

## **Methods of reconstruction**

- Disk-to-disk copy
- Partition-to-partition copy
- Image-to-disk copy
- Image-to-partition copy
- Disk-to-image copy
- Rebuilding files from carving

# Reporting

To perform a forensics disk analysis and examination, we need to create a report

- Bookmarking or tagging
- Log reports
- Timelines
- Report generator

# Quality of Computer Forensics

- Legal Authority
- Integrity of Evidence
- Forensic Documentation
- Administrative Review
- Technical Review
- Validation Testing

# Digital Evidence Assessment

The type of crime that we want to prove or disprove determines

- What evidence we need to analyse
- How the recovered information is to be used
- Related to inculpatory and exculpatory evidences

1. Evidence acquisition
2. Evidence examination
3. Documenting and reporting digital evidence

# Evidence acquisition

- The physical removal of storage devices
- Using controlled boot discs to retrieve sensitive data without affecting existing stored data
- Ensuring functionality
- Taking appropriate steps to copy and transfer evidence to the investigator's evidence repository
- Document and authenticate the chain of evidence

# Evidence examination

Digital forensics investigators typically examine data from designated archives

- use a variety of methods and approaches to analyse information
- include utilising analysis software to search massive archives of data for specific keywords or file types
- retrieve files that have been recently deleted
- analyse data tagged with times and dates
- suspicious files or programs that have been encrypted or intentionally hidden



# Documenting and reporting digital evidence

- Accurate record of all activity related to the investigation
- all methods used for testing system functionality and retrieving,
- copying, and storing data,
- all actions taken to acquire, examine and assess evidence

## **Purpose:**

- Demonstrate how the integrity of user data has been preserved
- Ensures that proper policies and procedures have been adhered to by all parties involved
- The purpose of the entire process is to acquire data that can be presented as evidence in a court of law
- An investigator's failure to accurately document his or her process could seriously compromise the validity of that evidence and ultimately, the case itself

# Time zone conversion

A time zone is a region of the earth that has uniform standard time, usually referred to as the local time. By convention, time zones compute their local time as an offset from UTC (Greenwich Mean Time).

For each computer system/server, time zone is set to its current location/local time. It is very important to know the time zone of that system to establish the exact time of offence, subsequent actions of the crime as supportive evidence.

Since the time zone/difference may vary more than 12 hours for few locations, for example United States of America vs India, the date of the occurrence of the crime may also change. This is very critical and important especially in crimes involved in sending e-mails from servers out of India.

Used for converting all the acts and incidents to one common time (usually the local time), so that the offences and the offender can be clearly linked.

A useful link is <http://www.timeanddate.com/worldclock/meeting.html>

# E-mail Headers

Each e-mail whether it is a company e-mail or Web-based e-mail like hotmail, yahoo, etc., carries lot of information about that e-mail.

Information like sender IP address, e-mail address, time and date when the e-mail sent, through which server it passed, etc.

E-mail message headers are digital histories that are attached to every e-mail message that are sent and received.

Headers include servers that the e-mail has travelled through, and the date and time that the message was received or forwarded

E-mail Header components collection

Message headers are easiest to view if you copy and paste them in a text program, such as Notepad

Get them printed with along with the subject line in the presence of the IO and witnesses, to avoid allegations of tampering at a later date

For header analysis, it is best if you delete out the message description from the header as it is not necessary for investigation

# Limitations of E-mail Headers as Investigative Tools

It may not be always possible to trace the originating IP address of the email message under investigation due to various reasons:

- Mail Service Providers like Google mask the originating IP address of the email
- simple header analysis cannot give the IO any clue regarding the origin of the email
- IO has to rely upon the information furnished by the mail service provider to trace the origin of the mail
- I.P spoofing and proxy servers can mislead the Investigating Officer
- by directing them to a wrong origin of the mail location
- in some cases no useful conclusion can be drawn from the header analysis
- IO should seek expert help to further proceed with the investigations

# Gathering information from external agencies/companies

Information can be gathered from several external sources to help with the investigation:

- Information from ISPs
- Information from e-mail service
- Information from Mobile service providers
- Information from Social networking sites like facebook etc.
- Information from Financial institutions/Internet banking institutions
- Information from Web site domain/hosting providers
- Information from VoIP service providers

From: Name of the Investigating Officer or Supervisory Officer (Police Inspector or above) Provide Full address, phone number and Official Mail ID.		Place Date
--------------------------------------------------------------------------------------------------------------------------------------------------------------	--	---------------

**NOTICE UNDER SECTION 91 CrPC**

To,

The Manager  
ABC Company  
ISP Division, Mumbai.

**Sub: Request to furnish the details about the IP address.**

Ref: Crime Number: xxxxxxxxxx u/s xxxxxxxxx of ITAA2008 of xxxxxxxx Police Station, xxxxxxxx City / District

With reference to the above cited subject, the undersigned is investigating officer of the criminal case mentioned above. For the purposes of investigation, details of the subscriber and his/her physical address details are required as per below mentioned IP addresses.

203.94.218.220 on 07 Feb 2008 at 05:01:24 pm GMT (22:31:24 in IST)

Please treat the matter as most urgent.



(Signature of the Investigating Officer or  
Supervisory Officer Demanding Information)

# What Information Can you get from a Service Provider? Overview.

## Subscriber Information

- Subscriber information supplied by the user at the time of registration, including name, location, date account created, and services used.
- IP addresses associated with log-ins to a user account.
- Registration IP address data available for IDs.

## Mail

- IP address of computer used to send email
- Contents of the email
- Can not search for or produce deleted emails

## Information from e-mail service

- User name
- Details of all incoming and outgoing e-mails along with mails stored in Draft folder
- The IP address from where the e-mail ID is accessed.
- Registration details like IP address, date and time, other services availed, secondary e-mail ID etc.
- User activity, i.e., date and time of logged in and time it is active, etc.

# Instant Messaging System

- Friends List
- Time, date, and IP address logs for Chat and Messenger use for limited period.
- Archives of Messenger communications may be available on the user's computer if the user has chosen to archive communications.
- Archives of Messenger communications may be stored in service providers servers if at least one party to the communication chose to archive communications
- Message Archive may not contain attachments to messages

## Groups

- Member list, email addresses of members, and date when members joined the Group.
- Information about Group moderators.
- Contents of the Files, Photos, and Messages sections.
- Group activity log describing when members subscribe and unsubscribe, post or delete files, and similar events.



### Information from ISPs:

- All the service providers enable queries by e-mail from pre-registered e-mail ids of the IOs and, such e-mail have to be from their official e-mail id
- ISP will typically provide the following information
- User name
- Telephone number
- Personal details like name, e-mail ID, address, etc., mentioned in the CAF
- Day-wise activity i.e., when and how long used, etc.
- Physical address of the IP address
- Sample letter to third party, companies, and service providers

### Information from Mobile service providers

- Customer Acquisition Forms (CAF) Forms — Personal details like name, address. etc.
- Calling number, called number, time, type of call (ISD/STD/Local/SMS, etc.)
- Roaming to other cities, etc.
- Tower locations — Latitude and Longitude of the tower

Information from Social networking sites like facebook etc.

- User name
- Personal details updated in the profile
- The IP address from where the profile is accessed
- User activity, i.e., date and time of logged in and duration of the active sessions, etc.
- Friends and groups with which the user is associated, etc.
- E-mail IDs updated in the personal information

Information from Financial institutions/Internet banking institutions

- Personal details updated in the profile of the account holder
- Transactional details
- CAF and other supporting documents submitted by the customer along with the introducer details
- IP address from where the transaction happened in case of Internet banking

### Information from Web site domain/hosting providers

- Registration details
- Access details
- FTP logs
- Payment details
- Technical/administrative/owner of the domain
- Details of Web site developer

### Information from VoIP service providers

- Registration details
- Access details
- IP addresses
- Payment details
- Called/Calling numbers

# Correlating the external data with lab findings

- A two-way correlation is required after collecting external data
- need to support the third-party information collected with the lab findings
- support the lab findings with the additional evidence collected from the third party, as well as our own investigation findings
- Build the integrity of the case as well as fully reconstruct the crime
- The Investigating Officer is required to follow the procedure in collecting the external data under proper notice/request letter as per the Law to make the evidence admissible in the court of law

Tasks we want to achieve

- Acquisition
- Validation and verification
- Extraction
- Reconstruction
- Reporting

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools  
The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by

- development of general tool specifications,
- test procedures,
- test criteria,
- test sets,
- test hardware

Requirement: forensic software tools consistently produce accurate and objective test results

The results are 3-fold:

- provide necessary information for toolmakers to improve tools,
- for users to make informed choices about acquiring and using computer forensics tools,
- for interested parties to understand the tools capabilities

# Acquisition

## Acquisition:

- first task in digital forensics investigations
- making a copy of the original drive
- This procedure preserves the original drive to make sure it doesn't become corrupt and damage the digital evidence

## Sub-functions:

- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote, live, and memory acquisitions

ISO standard 27037 states the most important factors in data acquisition are

- the DEFR's (Digital Evidence First Responders) competency
- use of validated tools
- includes guidelines on how to approach acquisition in different situations
- document what was done and why

Examples:

- if you're acquiring data at a scene with hazardous materials, speed is critical
- might decide to forgo acquiring RAM
- focus on collecting devices
- acquiring volatile memory
- encrypted devices or mission-critical systems that can't be turned off

Two types of data-copying methods

- physical copying of the entire drive
- logical copying of a disk partition

Disk acquisition formats vary from raw data to vendor-specific proprietary

A raw-format imaging tool can copy data from one drive to another disk or to segmented files

- In the past, examiners performed a bit-by-bit copy from one disk to another disk the same size or larger
- As a practical way to preserve digital evidence, vendors (and some OS utilities, such as the Linux/UNIX dd command) made it possible to write bit-stream data to files
- This copy technique creates simple sequential flat files of a suspect drive or data set
- The output of these flat files is referred to as a raw format.



# Validation & Verification

**Verification:** proves that two sets of data are identical by calculating hash values or using another similar method

- FTK validates MD5 and SHA-1 hash sets during data acquisition
- EnCase prompts you to calculate the MD5 hash value of acquired data
- Make sure that the tool used has a hashing function for verification purposes

## Filtering

- Related process
- Involves sorting and searching through investigation findings
- Separate good data and suspicious data

When performing filtering:

- Good data consists of
  - known files, such as OS files, common applications (Microsoft Word, for example),
  - standard files used in a company's day-to-day business
- Can also use hash values to create a known good hash value list
- An investigator could ignore all files on this known good list and focus on other files that aren't on this list.
- The National Software Reference Library (NSRL) has compiled a list of known file hashes for a variety of OSs, applications, and images that you can download

- NSRL collects software from various sources and incorporates file profiles computed from this software into a Reference Data Set (RDS) of information
- The Reference Data Set (RDS) can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS
- Helps in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations
- The RDS is a collection of digital signatures of known, traceable software applications.
- There are no hash values of illicit data

**Validation:** a way to confirm that a tool is functioning as intended

- Use forensic images that have been created for desktop and mobile devices
- These files are posted on Web sites such as NIST's CFTT or the Scientific Working Group on Digital Evidence (SWGDE)
- The sites tell what the tool should find as evidence on the drives
- Also give ranges of results
- We can determine that a tool works well for acquiring Linux images but has problems with older Windows versions
- The sites also publish the results of testing hardware acquisition tools
- After validating a tool, we must also make sure all forensic copies of a particular device have the same hash value.

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData.

- It scans a hard drive looking for various information.
- It can, for example,
- potentially locate deleted emails
- scan a disk for text strings to use them as a password dictionary to crack encryption
- FTK is also associated with a standalone disk imaging program called FTK Imager

## The Sleuth Kit Autopsy

Autopsy is open source

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Database Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX
- Tagging and reporting features.

# Extraction

- Recovery task in a digital investigation
- most challenging of all tasks to master
- Recovering data is the first step in analysing an investigation's data

Sub-functions of extraction:

- Data viewing
- Keyword searching
- Decompressing
- Carving: technique of reassembling files from raw data fragments when no filesystem metadata is available
- Decrypting
- Bookmarking or tagging

Many digital forensics tools include a data-viewing mechanism for digital evidence

- Offer several ways to view data
- logical drive structures, such as folders and files
- display allocated file data and unallocated disk areas
- Forensics tools have functions for searching for keywords of interest to the investigation
- With some tools, you can set filters to select file types to search, such as searching only PDF files

Analyzing, recovering, and decrypting data from encrypted files

- Encryption can be used on a drive, disk partition, or file
- Many e-mail services, such as Microsoft Outlook, provide encryption protection for .pst folders and messages
- Encryption can be platform specific

Password decryption

- Passwords are typically stored as hash values, not in plaintext
- One-way hashes: we cannot apply an algorithm to break them
- Many password recovery tools have a feature for generating potential password lists for a password dictionary attack
- OSForensics is a forensics tool, and has a built-in password cracker

# Reconstruction

## Purpose:

- Re-create a suspect drive to show what happened during a crime or an incident
- Create a copy for other digital investigators if a drive has been compromised by malware or a suspect's actions

## Methods of reconstruction:

- Disk-to-disk copy
- Partition-to-partition copy
- Image-to-disk copy
- Image-to-partition copy
- Disk-to-image copy
- Rebuilding files from carving
- One free tool is the Linux dd command

Disadvantage: it produces a flat, uncompressed file that is the same size as the source drive

# Reporting

To perform a forensics disk analysis and examination, we need to create a report

The following are sub-functions of the reporting function:

- Bookmarking or tagging
- Log reports
- Timelines
- Report generator

As part of the validation process, we need to document the steps we took to acquire data from a suspect drive

Sometimes we use a single tool, sometimes multiple tools are used to acquire data

Many forensics tools can

- produce a log report that records an investigator's activities
- incorporates evidence that was bookmarked or tagged during extraction
- A built-in report generator is then used to create a report in a variety of formats

Can add a log report to the final report as documentation of the steps we took during the examination

- useful if repeating the examination is necessary
- confirm during peer review what activities were performed and what results were found in the original analysis and examination

Investigator's report:

- Written by the investigator in detail
- Report shall contain the sequence of steps, and decisions taken
- Reports generated by tools are not sufficient



# Forensic Workstations

Forensic workstations can be tailored to meet the investigation needs

Forensic workstations can be divided into the following categories:

Stationary workstation—A tower with several bays and many peripheral devices

Portable workstation—A laptop computer with almost as many bays and peripherals as a stationary workstation

Lightweight workstation—Usually a laptop computer built into a carrying case with a small selection of peripheral options



# FRED Workstation



# Using a Write-Blocker

- Write-blockers protect evidence disks by preventing data from being written to them
- Forensic investigators need to absolutely assure of the fact that the data they obtain as digital evidence is not altered during the capture, analysis, and control
- Attorneys, judges, jurors need to feel confident that digital evidence has not been tampered and is legitimate

According to the NIST:

- Use an operating system and other software that is trusted to not to write anything to the disk without any explicit instruction
- Use hard disk write block tools to prevent any hard disk writes
- Software and hardware write-blockers perform the same function but in a different fashion
- Both guarantee the protection of the chain of custody (if used correctly)

# Software write-blockers

- A software write blocker tool operates by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface
- They provide the ability to
- simultaneously write-block as many disk devices as are connected to a computer
- no need for multiple expensive hardware write blocking devices

## Example:

- Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode
- PDBlock changes interrupt-13 of a workstation's BIOS to prevent writing to the specified drive.
- If anyone attempts to write data to the blocked drive, an alarm sounds, advising that no writes have occurred

## Features:

- The user can control automatic write blocking policies for fixed and/or removable disks.
- The user can have write blocking tool remember each fixed device's blocked or un-blocked status for ease of use on media repeatedly used on a workstation/laptop.
- Some of the write blocking tools provide a GUI interface that allows the user the ability to block and unblock any disk or flash storage device.

# Hardware write-blockers

- Hardware write-blockers are used to intercept and block any modifying command from ever reaching the storage device
- With hardware write-blockers, we can connect the evidence drive to the workstation and start the OS as usual
- They prevent the OS from writing data to the blocked drive

## Features:

- They offer monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device
- Hardware write blockers can connect to different types of storage with adapters
- Hardware devices that write-block also provide a visual indication of function through LEDs and switches. easy to use, clear functionality to users.

## Disadvantages:

- Hardware write blocking devices are very expensive
- Awkward to use since they require a physical connection
- different connector for each type of interface



# Write Block Device Tubule



A forensic disk controller or hardware write-block device is a specialized type of computer hard disk controller made for the purpose of gaining read-only access to computer hard drives without the risk of damaging the drive's contents. The device is named forensic because its most common application is for use in investigations where a computer hard drive may contain evidence.

# Hard Disk Cloner ( Imaging )



Disk cloning is the process of copying the contents of one computer hard disk to another disk or to an "image" file. This may be done straight from one disk to another, but more often, the contents of the first disk are written to an image file as an intermediate step, then the second disk is loaded with the contents of the image



# Forensic Toolkit ( FTK )



Is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can for example locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

# Encase Tools



Encase is a suite of digital forensics products by Guidance Software. The software comes in several forms designed for forensic, cyber security and e-discovery use.

Encase contains tools for several areas of the digital forensic process; acquisition, analysis and reporting. The software also includes a scripting facility called EnScript with various API's for interacting with evidence.

# Encase Tableau



# XRY Mobile Forensic



XRY is a digital forensics product by Micro Systemation used to analyze and recover information from mobile devices such as mobile phones, smartphones, GPS navigation tools and tablet computers. It consists of a hardware device with which to connect phones to a PC and software to extract the data.



# UFED Mobile forensic

UFED Ultimate provides access to deleted data inaccessible by logical methods











# Paraben Forensics Tools





# Falcon Neo Forensics Tool



**Table 6-1** Comparison of forensics tool functions

Function	Magnet Forensics AXIOM, demo version	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Acquisition				
Physical data copy	✓	✓	✓	✓
Logical data copy	✓	✓	✓	
Data acquisition formats	✓	✓	✓	✓
Command-line processes				✓
GUI processes	✓	✓	✓	✓
Remote acquisition		✓	✓	✓

**Table 6-1** Comparison of forensics tool functions

Function	Magnet Forensics AXIOM, demo version	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
<b>Validation and verification</b>				
Hashing	✓	✓	✓	✓
Verification	✓	✓	✓	✓
Filtering	✓	✓	✓	✓
Analyzing file headers	✓	✓	✓	✓
<b>Extraction</b>				
Data viewing	✓	✓	✓	✓
Keyword searching	✓	✓	✓	✓
Decompressing	✓		✓	✓
Carving	✓	✓	✓	✓
Decrypting	✓	✓	✓	
Bookmarking	✓	✓	✓	✓

**Table 6-1** Comparison of forensics tool functions

Function	Magnet Forensics AXIOM, demo version	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
<b>Reconstruction</b>				
Disk-to-disk copy	✓	✓	✓	✓
Partition-to-partition copy	✓	✓	✓	✓
Image-to-disk copy	✓	✓	✓	✓
Image-to-partition copy	✓	✓	✓	✓
Disk-to-image copy	✓	✓	✓	✓
Rebuilding files	✓	✓	✓	✓
<b>Reporting</b>				
Bookmarking/tagging	✓	✓	✓	✓
Log reports	✓	✓	✓	✓
Timeline	✓	✓	✓	✓
Report generator	✓	✓	✓	✓

# Validating and Testing Forensics Software

Using National Institute of Standards and Technology Tools

Using Validation Protocols

Need to make sure the evidence we recover and analyze can be admitted in court

Using National Institute of Standards and Technology Tools

The National Institute of Standards and Technology (NIST)

- publishes articles,
- provides tools,
- creates procedures for testing and validating computer forensics software
- Software should be verified to improve evidence admissibility in judicial proceedings

A lab must meet the following criteria and keep accurate records:

- Establish categories for digital forensics tools—Group digital forensics software according to categories, such as forensics tools designed to retrieve and trace e-mail
- Identify forensics category requirements—For each category, describe the technical features or functions a forensics tool must have

Develop test assertions—Based on the requirements, create tests that prove or disprove the tool’s capability to meet the requirements

- Identify test cases—
- Find or create types of cases to investigate with the forensics tool
- Identify information to retrieve from a sample drive or other media.

For example, use the image of a closed case file created with a trusted forensics tool to test a new tool in the same category and see whether it produces the same results.

- Establish a test method—Considering the tool’s purpose and design, specify how to test it
- Report test results—Describe the test results in a report that complies with ISO17025, which requires accurate, clear, unambiguous, and objective test reports
- **Repeatable results:** if you work in the same lab on the same machine, you generate the same results
- **Reproducible results:** if you’re in a different lab working on a different machine, the tool still retrieves the same information

## Using Validation Protocols

- After retrieving and examining evidence data with one tool, we should verify our results by performing the same tasks with other similar forensics tools

Example: after we use one forensics tool to retrieve disk data, we use another to see whether we retrieve the same information

- Question in court: How did you verify your results?
- need at least two tools to validate
- tool we use to validate the results should be well tested and documented

## Digital Forensics Examination Protocol

- First, conduct your investigation of the digital evidence with one GUI tool
- Then perform the same investigation with a disk editor to verify that the GUI tool is seeing the same digital evidence in the same places on the test or suspect drive's image.
- If a file is recovered, obtain the hash value with the GUI tool and the disk editor, and then compare the results to verify whether the file has the same value in both tools
- Many investigators in both the public and private sectors use FTK and EnCase as their choice of forensics software suites
- They do not rely on them solely: investigators' software libraries often include other forensics utilities to supplement these tools' capabilities

## Digital Forensics Tool Upgrade Protocol

- After verification with two different tools, should test all new releases and OS patches and upgrades
- Make sure the upgrades are reliable and do not corrupt evidence data
- If you determine that a patch or upgrade isn't reliable, do not use it on your forensic workstation until the problem has been fixed
- Can file an error report with the vendor
- not being able to read old image files with the new release
- disk editor generating errors after you apply the latest service pack etc.
- In most cases, the vendor addresses the problem and provides a new patch



# Digital Device Forensics

## Desktops:

- Specially built for personal use at home or work
- Equipped with two primary hardware solutions —the monitor and a casing
- In the casing, CPU is housed, the motherboard, the graphic card, storage devices, buses, power supply etc.

## Laptop:

- Also known as notebook computer, is a smaller computer
- It has all the components like monitor, keyboard, mouse, and speakers, etc., in a single unit.
- It is powered through an AC adapter and can store the energy in a rechargeable battery.

## Server:

- A computer which can provide services to a group of computers either inside an organization or to public users across Internet.
- Many servers have dedicated functionality, such as Web servers, file servers, print servers, database servers, mail servers, etc.
- Sometimes, they have different kinds of hardware and operating systems that makes them efficient in providing services

# Digital Storage Device

Hard drives:

- Hard drives or hard disks are the main storage devices that are used in the computer to store the data
- The data stored in hard drive is non-volatile
- Come in different varieties based on their speed, size, and connecting types
- The common types of hard drives that are usually encountered are 1) IDE, 2) SATA, 3) SCSI, and 4) ZIF/SSD

IDE hard drive:

- IDE (Integrated Drive Electronics) hard drives, also known as Parallel ATA (PATA) were the most commonly used hard drives
- First developed by Western Digital and Compaq in 1986
- An IDE hard drive uses 40 or 80 pin flat ribbon cables to transfer data.
- Normally appears as an internal computer storage interface

ATA: AT Attachment

AT: Advanced technology

SATA hard drive:

- Serial ATA
- Similar in mechanism to that of IDE drive
- The connecting interface is different.
- Seven conductors instead of 40 or 80
- The data transfer is done serially and is faster than IDE drives.

SCSI hard drives:

- SCSI stands for Small Computer System Interface
- A set of American National Standards Institute (ANSI) standard electronic interfaces
- Allow personal computers to communicate with peripheral hardware such as disk drives, tape drives, CD-ROM drives, printers and scanners faster and more flexibly than previous parallel data transfer interfaces used in servers and RAID systems
- Can be connected as arrays both internally and externally

### ZIF Drives:

ZIF stands for zero insertion force.

Connectors to these drives do not need any force to insert and extract from the sockets or other connections. This kind of storage devices are now being used in several laptop computers.

### CDS ,DvDS:

- CDs and DVDs are optical storage devices that are used to store data like audio, video, and several other types of files
- CDs can be written once (CD-R-Recordable) or data can be erased and re-written (CD-RW-Rewritable)
- The maximum size of a CD is 800 Megabytes and that of a DVD is 9.0 Gigabytes

### Blu-ray:

- Name of a new optical disc format developed to enable recording, rewriting and playback of high-definition video (HD)
- Can store large amounts of data
- Can hold up to 25GB on a single-layer disc and 50GB on a dual-layer disc

### Floppy disks:

- Floppy disks are magnetic storage media that are encased in a rectangular plastic case.
- They usually come in three different sizes 8 inches, 5 1/2 inches, and 3 1/2 inches. 8 and 5 1/2 inches have become obsolete now.
- Floppy disks have a write-protection option or read-only option
- Floppy disks are read from and written to by a floppy disk drive (FDD)

### Flash drives:

- Flash drives are generally flash memory data storage devices that are integrated with a USB interface
- Flash memory:
  - non-volatile memory chip used for storage and for transferring data
  - electronically reprogrammed and erased
- Removable and portable media
- Rewritable and are much smaller in size than the typical floppy disk drive

### NAS:

- Network attached storage (NAS)
- storage system that allows computers on network to share large amounts of data across high-speed Local Area Network (LAN) networks
- can store data in the files such as e-mail boxes, Web content, and remote system backups
- usually composed of an array of hard drives that are connected to a computer system

### Printers and Scanners:

- Usually have cache memory which temporarily lines up (spools) the files or pages that are currently being printed
- Once switched off, that memory is usually lost
- Some large printers and scanners have inbuilt hard drives

# Hand Held Device

## Pagers:

- A Pager is a device that is used for short messages.
- Pagers can be one way, which can send or receive messages
- Contain limited digits or they can be alphanumeric,
- Two-way pagers which can even send and receive messages etc.

## Personal Digital Assistant (PDA):

- PDAs are Palm top computers that function as personal information manager or organizer
- Can store several types of personal data, browse Internet, etc.
- PDAs also have expandable memory and wireless Internet connectivity

## Ipads/tablets:

- Ipads are tablet computers manufactured by Apple Computers.
- It has the same operating system as iPhone and iPod (iOS).
- This can be used as a typical computer to store data, browse Internet, make phone calls, play games, read e-books, etc.

## Electronic readers/e-readers:

- Electronic readers are devices that are used to store, download, and read e-books and play games.
- These devices are wireless Internet enabled and come in different storage capacities.

# Network Device

## Hub:

- In computer networking, a Hub is a small device that joins multiple computers together.
- Ethernet hubs vary in the speed they support

## Switch:

- A network switch is a hardware device that joins multiple computers within one LAN.
- Network switches allows network packets from them
- Also examines or inspects them to determine their source and destination

## Router:

- In Network environment, a Router is a physical device that joins multiple wired or wireless networks together.
- Routers are usually located at gateways.
- It intercepts the data packets and decides where the signals have to go
- A Router can have different interface connections for different types of physical networks.

RAID(Redundant Array of Inexpensive Disks) is method of storing the same data in different places (thus, redundantly) on several hard disks



### Firewall:

- Found in a computer system or network
- device that allows only authorized traffic (data) into or out of a computer or a computer network.
- continuously inspects the data packets that are going in and out of a computer network
- blocks any unauthorized and malicious traffic and serves as a security mechanism
- can be hardware, software, or a combination of both

### Intrusion Detection system/Intrusion Prevention system(IDS and IPS):

- An IDS is a security mechanism that monitors all the incoming and outgoing traffic of computer network
- identifies suspicious files, programs, and patterns in the traffic
- also detects the misuse and errors in using certain computer resources like software
- IPS detects threats and attacks in the network, also prevents or blocks them
- usually sends the alarm, resets the connections, drops the malicious data packet, or blocks the attacker's IP address

# Communication Device

## Telephones:

- These communication devices are also sometimes the best source of digital evidence.
- Desk phones may contain information like last dialed numbers, frequently dialed numbers,
- voicemail messages that are left by callers
- alternative phone numbers in case of any call diversions, etc.

## Answering machines:

- Devices that are used with desk telephones.
- These devices will play a message to the caller when the call cannot be answered
- The caller can leave a message which will be recorded in the answering machine.
- All the messages recorded in such a way can be played later directly from the machine itself.

## Fax Machines:

- Fax is any document sent over a telephone line.
- It is received by the recipient's fax machine and gets printed.
- In many corporate environments, fax servers are installed, which can store the incoming fax messages electronically and sends them through e-mail to the users or prints them on the paper.

### Mobile phones:

- Mobile phones are used to make phone calls, send text messages, voice and picture/video messages (Multimedia messages —MMS),
- Take pictures and videos, etc.
- Usually has a SIM card specific to the service provider.

### Smart phones:

- Smart phones are advanced type of mobile phones
- Offers services like high-speed Internet, advanced computing, and connectivity
- They run on complete operating system software like typical computers and can be considered as a pocket computer.
- Provide services like Internet, e-mail, Wi-Fi etc.

# MISC. Device

## Digital cameras:

- cameras that can take pictures and videos and records them digitally on to the memory present in them.
- they also support expandable memory by using multimedia cards
- more advance cameras have hard drives that can store pictures and videos

## Camcorders:

- Camcorders are the digital video recorders used to capture video footages and record them digitally on to CDs, Cassettes, Multimedia cards, hard drives, etc.

## Photocopiers:

- A Photocopier is a machine that can reproduce a document and make multiple copies of it quickly.
- Advanced photocopiers have features like sending the photocopy electronically to the e-mail
- stores documents in the hard drives when large numbers of documents are to be copied.

### Global positioning devices:

- Satellite-based navigation system
- Provides the exact location and time information anywhere on the earth
- GPS devices have receivers for GPS satellite and provide information, such as location, directions, traffic conditions,
- Also nearby facilities like restaurants, fuel stations, etc.,
- Receives though maps and text and voice.

### Digital watches:

- Digital watches are instruments that show time in digital format
- also have other facilities like compass, temperature sensors, music players, and in some embedded cameras also.
- Some advanced digital watches also have USB data connectivity to store and transfer data.

# Digital Evidence Assessment

Assessment of potential evidence in cyber crime.

Details of the case at hand is required to effective processing of evidence

The type of crime that we want to prove or disprove determines

- What evidence we need to analyse
- How the recovered information is to be used
- Related to inculpatory and exculpatory evidences

Main components:

- Evidence acquisition
- Evidence examination
- Documenting and reporting digital evidence

# Evidence Acquisition

Rigorous, detailed plan for acquiring evidence

Extensive documentation is needed prior to, during, and after the acquisition process

General methods:

- The physical removal of storage devices
- Using controlled boot discs to retrieve sensitive data without affecting existing stored data
- Ensuring functionality
- Taking appropriate steps to copy and transfer evidence to the investigator's evidence repository
- Document and authenticate the chain of evidence

# Evidence Examination

Procedures must be in place for retrieving, copying, and storing evidence within appropriate databases

Digital forensics investigators typically examine data from designated archives

- use a variety of methods and approaches to analyse information
- include utilising analysis software to search massive archives of data for specific keywords or file types
- retrieve files that have been recently deleted
- analyse data tagged with times and dates
- suspicious files or programs that have been encrypted or intentionally hidden



# Documenting and Reporting Digital Evidence

Document information related to hardware and software specifications

Accurate record of all activity related to the investigation

- all methods used for testing system functionality and retrieving,
- copying, and storing data,
- all actions taken to acquire, examine and assess evidence

Purpose:

- demonstrate how the integrity of user data has been preserved
- ensures that proper policies and procedures have been adhered to by all parties involved

The purpose of the entire process is to acquire data that can be presented as evidence in a court of law

An investigator's failure to accurately document his or her process could seriously compromise the validity of that evidence and ultimately, the case itself

# Mobile Forensics

The following information might be stored on a mobile phone depending upon the model used:

Incoming, outgoing, and missed calls

- Multimedia Message Service (MMS; text messages)
- Short Message Service (SMS) messages
- E-mail accounts
- Instant messaging (IM) logs
- Web pages
- Photos, videos, and music files
- Calendars and address books
- Social media account information
- GPS data
- Voice recordings and voicemail
- Bank account logins
- Access to the home

- Many people store more information on smartphones and tablets than on computers
- Mobile devices used to be seized at the time of arrest
- Police used to look through them as a routine matter
- Prohibited now

U.S. Supreme court ruling :

- A search warrant is required before an arresting officer can begin examining a phone's contents
- <https://newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped>
- Phones often contain private or sensitive information
- Any information that does not pertain to the case must be redacted from the public record
- Investigating smartphones and other mobile devices is a challenging task in digital forensics because:
- No single standard exists for how and where phones store messages (many phones use similar storage schemes)
- New phones come out about every six months, and they are rarely compatible with previous models
- The cables, software, and accessories used for forensics acquisitions can become obsolete in a short time

# Windows File System

A file system gives an OS a road map to data on a disk.

- The type of file system an OS uses determines how data is stored on the disk.
- When you need to access a suspect's computer to acquire or inspect data related to your investigation, you should be familiar with both the computer's OS and file system so that you can access and modify system settings when necessary.

# Understanding the Boot Sequence

- To ensure that you don't contaminate or alter data on a suspect's Windows or DOS PC, you must know how to access and modify a PC's Complementary Metal Oxide Semi- conductor (CMOS) and Basic Input/ Output System (BIOS) settings
- A computer stores system configuration and date and time information in the CMOS when power to the system is off
- When a subject's computer starts, you must make sure it boots to a forensic floppy disk or CD,
- booting to the hard disk overwrites and changes evidentiary data
- You access the CMOS setup by monitoring the subject's computer during the initial bootstrap process to identify the correct key or keys to use
- The bootstrap process is contained in ROM and tells the computer how to proceed
- CMOS depends on the computer's BIOS.
- The popular BIOS manufacturer AMI use the Delete key to access CMOS

## CMOS:

- Stands for "Complementary Metal Oxide Semiconductor."
- It is a technology used to produce integrated circuits.
- CMOS circuits are found in several types of electronic components, including microprocessors, batteries, and digital camera image sensors.
- "CMOS" refers to both a particular style of digital circuitry design and the family of processes used to implement that circuitry on integrated circuits (chips).

## BIOS

- BIOS is the program a computer's microprocessor uses to start the computer system after it is powered on.
- Also manages data flow between the computer's operating system (OS) and attached devices, such as the hard disk, video adapter, keyboard, mouse and printer.

# Disk Drives

Understand how data is organized on a disk so that you can find data effectively

- Disk drives are made up of one or more platters coated with magnetic material
- Data is stored on platters in a particular way

## Geometry

- Geometry refers to a disk's logical structure of platters, tracks, and sectors.

## Head

- The head is the device that reads and writes data to a drive.
- There are two heads per platter that read and write the top and bottom sides.

## Tracks

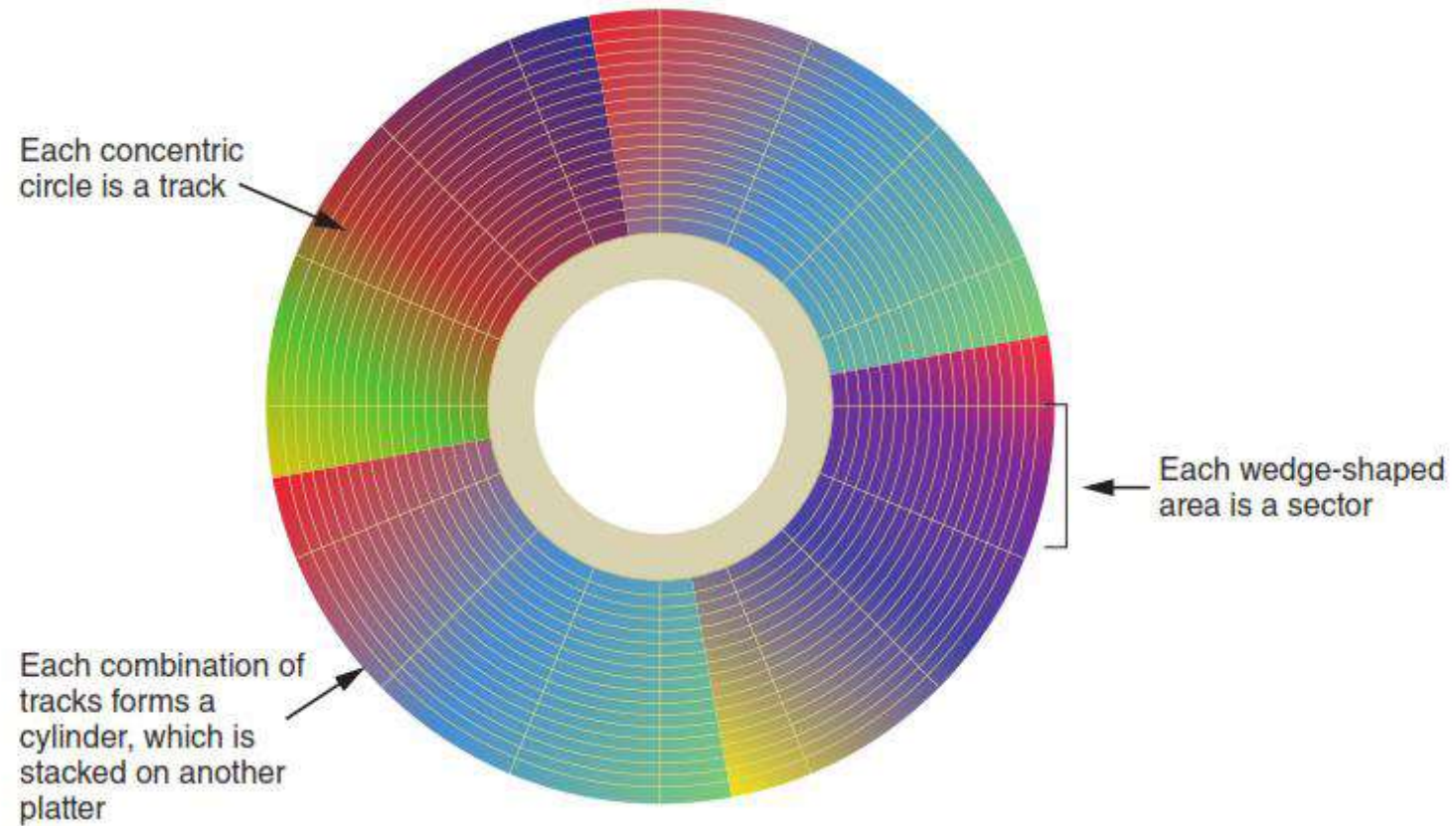
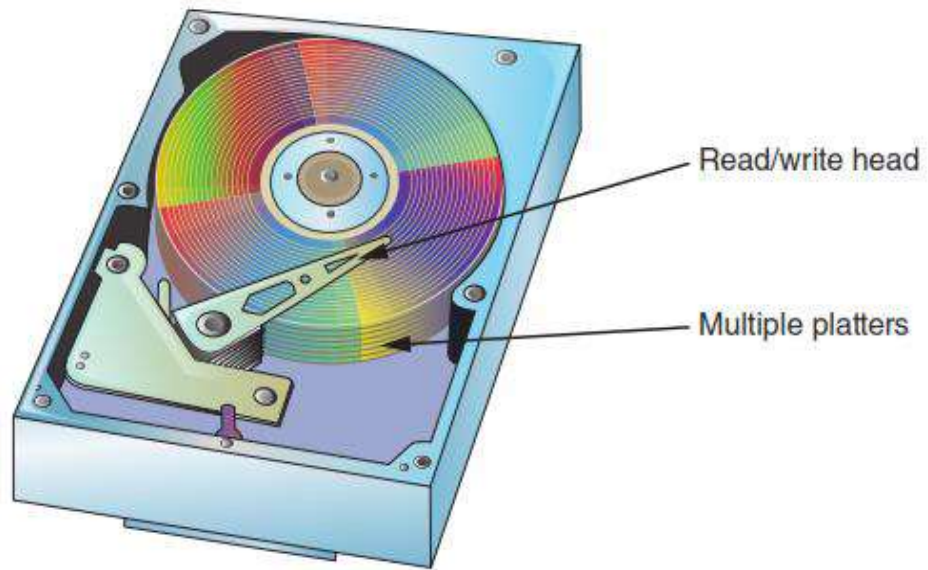
- Tracks are concentric circles on a disk platter where data is located.

## Cylinders

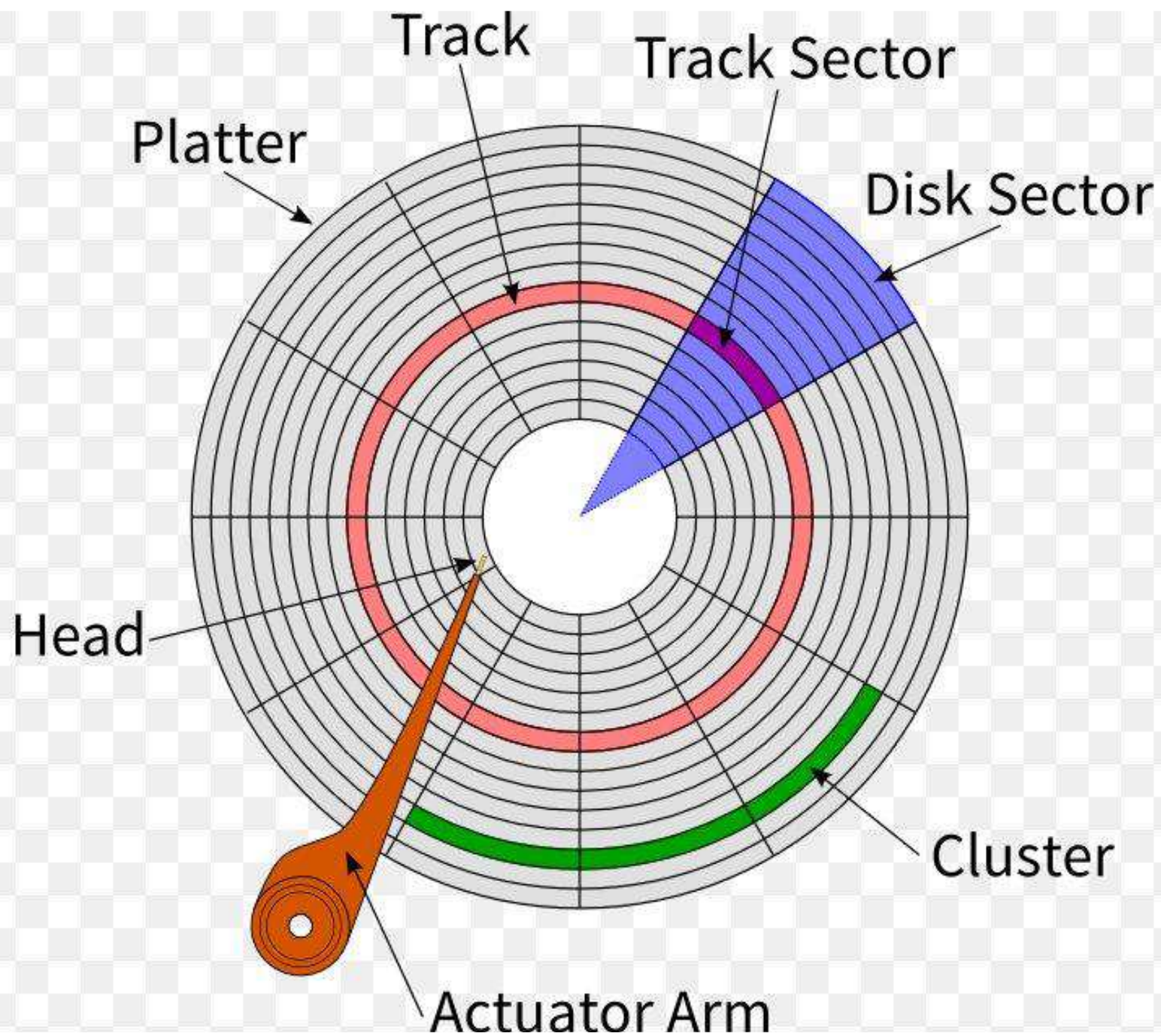
- A cylinder is a column of tracks on two or more disk platters.
- Typically, each platter has two surfaces: top and bottom.

## Sectors

- A sector is a section on a track, usually made up of 512 bytes.







# Solid-State Storage Devices

- Flash memory storage devices used in USB drives, laptops, tablets, and cell phones can be a challenge for digital forensics examiners
- If deleted data isn't recovered immediately, it might be lost forever.
- The reason is a feature all flash memory devices have: wear-leveling.
- When data is deleted on a hard drive, only the references to it are removed, which leaves the original data in unallocated disk space.
- With forensics recovery tools, recovering data from magnetic media is fairly easy; you just copy the unallocated space.
- USB drives and other solid-state drive systems are different
- Memory cells shift data at the physical level to other cells that have had fewer reads and writes continuously.
- The purpose of shifting (or rotating) data from one memory cell to another is to make sure all memory cells on the flash drive wear evenly
- Memory cells are designed to perform only 10,000 to 100,000 reads/writes, depending on the manufacturer's design.
- When they reach their defined limits, they can no longer retain data.
- When you attempt to connect to the device, you get an access failure message.

# Microsoft File Structures

Two structures: File Allocation Table (FAT), and NT File System (NTFS)

- The method an OS uses to store files determines where data can be hidden.
- When you examine a computer for forensic evidence, you need to explore these hiding places to determine whether they contain files or parts of files that might be evidence of a crime or policy violation.
- In Microsoft file structures, sectors are grouped to form clusters, which are storage allocation units of one or more sectors.
- The OS groups one or more sectors into a cluster.
- Clusters are numbered sequentially, starting at 0 in NTFS and 2 in FAT.
- The OS assigns numbers to these cluster, referred to as logical addresses.
- Sector numbers, however, are referred to as physical addresses because they reside at the hardware level and go from address 0 (the first sector on the disk) to the last sector on the disk.
- The first sector of all disks contains a system area, the boot record, and a file structure database.
- Clusters and their addresses are specific to a logical disk drive, which is a disk partition.

# Disk Partition

- Many hard disks are partitioned, or divided, into two or more sections.
- A partition is a logical drive.
- Windows OSs can have three primary partitions followed by an extended partition that can contain one or more logical drives.
- Someone who wants to hide data on a hard disk can create hidden partitions or voids: large unused gaps between partitions on a disk drive.
- For example, partitions containing unused space can be created between the primary partitions or logical partitions.
- This unused space between partitions is called the partition gap
- It's possible to create a partition, add data to it, and then remove references to the partition so that it can be hidden in Windows.
- Another technique is to hide incriminating digital evidence at the end of a disk by declaring a smaller number of bytes than the actual drive size.
- With disk-editing tools, however, we can access these hidden or empty areas of the disk.
- Both tasks involve analyzing the key hexadecimal codes the OS uses to identify and maintain the file system.
- The partition table is in the Master Boot Record (MBR), located at sector 0 of the disk drive.
- In a hexadecimal editor, such as WinHex, you can find the first partition starting at offset 0x1BE (446 in decimal, 676 in Octal).



WinHex - [Hard disk 2]

File Edit Search Navigation View Tools Specialist Options Window Help

19.2 SR-0

Hard disk 2

Partitioning style: MBR

0+0+4 files, 4 partitions

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Start sectors		1.0 MB					0
Partition 1 (G:)	NTFS	97.7 GB					2,048
Partition 2 (H:)	NTFS	48.8 GB					204,802,048
Partition 3 (I:)	FAT32	5.9 GB					307,202,048
Partition gap		1.0 MB					319,490,048
Partition 4 (J:)	FAT16	500 MB					319,492,096
Unpartitioned space		313 GB					320,516,096
Unpartitionable space		1.8 MB					976,703,805

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0000000000	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C	SÄZB*  QP P d%
0000000010	BF	1B	06	50	57	B9	E5	01	F3	A4	CB	BD	BE	07	B1	04	z PW-ä ömE+0% ±
0000000020	38	6E	00	7C	09	75	13	83	C5	10	E2	F4	CD	18	8B	F5	8n   u fÄ ÄöI <ö
0000000030	83	C6	10	49	74	19	38	2C	74	F6	A0	B5	07	B4	07	8B	fE It 8,tö u " <
0000000040	F0	AC	3C	00	74	FC	BB	07	00	B4	0E	CD	10	EB	F2	88	ä-< tû» " I eö-
0000000050	4E	10	E8	46	00	73	2A	FE	46	10	80	7E	04	0B	74	0B	N eF s*pF €~ t
0000000060	80	7E	04	0C	74	05	A0	B6	07	75	D2	80	46	02	06	83	E~ t q uöEF f
0000000070	46	08	06	83	56	0A	00	E8	21	00	73	05	A0	B6	07	EB	F fV è! s q è
0000000080	BC	81	3E	FE	7D	55	AA	74	0B	80	7E	10	00	74	C8	A0	4 >p)U*t €~ tE
0000000090	B7	07	EB	A9	8B	FC	1E	57	8B	F5	CB	BF	05	00	8A	56	- eQ<u W<öEz Šv
00000000A0	00	B4	08	CD	13	72	23	8A	C1	24	3F	98	8A	DE	8A	FC	" I x#šÄ?šbšg
00000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	EE	42	F7	E2	39	56	C=ä<N+Ö± ÖIB+ä9V
00000000C0	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C	w#r 9F s . »
00000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A	<N <V I sQOtN2aš
00000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD	V I eäšV "»*U'Ai
00000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60	rë üU*uoöÄ t+a~
0000000100	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A	j j Ÿv Ÿv j h  j
0000000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B	j 'B<öI aas Ot
0000000120	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61	2ašV I eöaüÄInva
0000000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	lid partition ta
0000000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	ble Error loadin
0000000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
0000000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	em Missing opera
0000000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	ting system
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000001B0	00	00	00	00	00	2C	44	63	83	A1	04	00	21	0E	00	20	,Dcf; !
00000001C0	21	00	07	FE	FF	FF	00	08	00	00	00	35	0C	00	FE	00	! pŸŸ s p
00000001D0	FF	FF	07	FE	FF	FF	00	08	35	0C	00	80	1A	06	00	FE	ŸŸ pŸŸ s € p
00000001E0	FF	FF	0C	FE	FF	FF	00	88	4F	12	00	80	BB	00	00	FE	ŸŸ pŸŸ "ö €» p
00000001F0	FF	FF	0F	FE	FF	FF	00	08	0B	13	00	50	2C	27	55	AA	ŸŸ pŸŸ P, 'U*
0000000200	00	80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Sector 1 of 976,707,584

Offset: 20F

= 0 Block: n/a Size: n/a

First sectors converted to decim

$0 \times 800$	=	2048
$0 \times 0C350800$	=	204,802,048
$0 \times 124F8800$	=	307,202,048
$0 \times 130B0800$	=	319,490,048

Partition offsets

1st partition offset	$0 \times 1BE$
2nd partition offset	$0 \times 1CE$
3rd partition offset	$0 \times 1DE$
4th partition offset	$0 \times 1EE$

# Examining FAT Disks

- File Allocation Table (FAT) is the file structure database that Microsoft designed for floppy disks.
- It is used to organize files on a disk so that the OS can find the files it needs.
- Since its development, other OSs, such as Linux and Macintosh, can format, read, and write to FAT storage devices such as USB drives and SD cards.
- The FAT database is typically written to a disk's outermost track and contains filenames, directory names, date and time stamps, the starting cluster number, and file attributes (archive, hidden, system, and read-only).
- There are three current versions of FAT—FAT16, FAT32, and exFAT (used for mobile personal storage devices)
- Three older FAT formats, which are FATX, Virtual FAT (VFAT), and FAT12

FAT12: This version is used specifically for floppy disks, so it has a limited amount of storage space.

FAT16: To handle larger disks, Microsoft developed FAT16, which is still used on older Microsoft OSs

FAT32: When disk technology improved and disks larger than 2 GB were developed, Microsoft released FAT32, which can access larger drives.

exFAT:

- Developed for mobile personal storage devices, such as flash memory devices, and memory sticks.
- The exFAT file system can store very large files, such as digital images, video, and audio files.

VFAT:

- Developed to handle files with more than eight-character filenames and three-character extensions; introduced with Windows 95.
- VFAT is an extension of other FAT file systems.

FATX:

- Modified version of the FAT32 file system format.
- The FATX file system format is used on the Xbox video game console hard disk.
- Unrecognizable by the Windows operating system.

# Cluster Sizes

Cluster sizes vary according to the hard disk size and file system.

Minimum size allocated for any file

**Table 5-2** Sectors and bytes per cluster

Drive size	Sectors per cluster	FAT16
8–32 MB	1	512 bytes
32–64 MB	2	1 KB
64–128 MB	4	2 KB
128–256 MB	8	4 KB
256–512 MB	16	8 KB
512–1024 MB	32	16 KB
1024–2048 MB	64	32 KB
2048–4096 MB	128	64 KB



- Microsoft OSs allocate disk space for files by clusters.
- This practice results in drive slack
- unused space in a cluster between the end of an active file's content and the end of the cluster.
- leads to file slack space
- When the OS stores data in a FAT file system, it assigns a starting cluster position to a file.
- Data for the file is written to the first sector of the first assigned cluster.
- When this first assigned cluster is filled and runs out of room, FAT assigns the next available cluster to the file.
- If the next available cluster isn't contiguous to the current cluster, the file becomes fragmented.
- In the FAT for each cluster on the volume, the OS writes the address of the next assigned cluster: linked list of (occupied, next)

## **Deleting FAT Files**

- When a file is deleted in Windows Explorer or with the MS-DOS delete command, the OS inserts a HEX E5 (0xE5) in the filename's first letter position in the associated directory entry.
- This value tells the OS that the file is no longer available and a new file can be written to the same cluster location
- The data in the file remains on the disk drive.
- The area of the disk where the deleted file resides becomes unallocated/free disk space
- Forensics tools can recover data still residing in this area.

## **Examining NTFS Disks**

- New Technology File System (NTFS) was introduced when Microsoft created Windows NT
- Still the main file system in Windows 10.
- NTFS offers substantial improvements over FAT file systems.
- provides more information about a file,
- includes security features, file ownership, and other file attributes.
- The system keeps track of transactions such as file deleting or saving.
- This journaling feature is helpful because
- records a transaction before the system carries it out
- in a power failure or other interruption, the system can complete the transaction or go back to the last good setting

- In NTFS, everything written to the disk is considered a file.
- On an NTFS disk, the first data set is the Partition Boot Sector, which starts at sector [0] of the disk
- Immediately after the Partition Boot Sector is the Master File Table (MFT)
- the first file on the disk
- An MFT file is created at the same time a disk partition is formatted as an NTFS volume
- NTFS results in much less file slack space.
- Clusters are smaller for smaller disk drives.

**Table 5-3** Cluster sizes in an NTFS disk

Drive size	Sectors per cluster	Cluster size
7-512 MB	8	4 KB
512 MB-1 GB	8	4 KB
1-2 GB	8	4 KB
2 GB-2 TB	8	4 KB
2-16 TB	8	4 KB
16-32 TB	16	8 KB
32-64 TB	32	16 KB
64-128 TB	64	32 KB
128-256 TB	128	64 KB

# FAT vs NTFS

- Fault Tolerance: NTFS automatically repairs files/folders in the case of power failures or errors. FAT32 maintains two different copies of the FAT in the case of damage.
- Security: FAT32 only offers shared permissions, while NTFS allows you to set specific permissions to local files/folders.
- 
- Compression: FAT32 does not offer any compression option. NTFS does allow for individual compression of files and folders so you don't slow down the system.
- Compatibility: NTFS is compatible with operating systems back to Windows XP. For Mac OS users, however, NTFS systems can only be read by Mac, while FAT32 drives can be both read and written to by the Mac OS.

# Windows Artifacts

## **Deleted Data**

- Hitting the delete key doesn't do anything to the data itself
- “Deleting” a file only tells the computer that the space occupied by that file is available if the computer needs it.
- Data can be extracted from these unallocated spaces

## **Hibernation File(Hiberfile.Sys)**

- Hibernation save data to the hard drive as opposed to just holding it in RAM (like “sleep”)
- Data written to the hard-drive itself are more persistent and can be recovered.
- It is possible that files deleted by a suspect could still be found here.

## **Registry**

- registry is a database for configuration files.
- keeps track of user and system configuration and preferences
- Items of interest include:
  - search terms,
  - programs that were run or installed,
  - Web addresses,
  - files that have been recently opened, etc.

## **Recycle Bin**

- Normally, users count on the trash can to erase their evidence.
- Deleted files can be recovered from the recycle bin

## **Metadata**

- Defined as data about data.
- There are two kinds of metadata: application and file system.
- The file system keeps track of our files and folders as well as some information about them.
- File system metadata include the date and time a file or folder was created, accessed, or modified.

## **Thumbnail Cache**

- Windows creates smaller versions of the photos called thumbnails for ease of browsing
- Most users are completely unaware that these files even exist.
- These files remain even after the original images have been deleted.
- Even if we don't recover the original image, thumbnails can serve as the next best evidence.
- Their mere existence tells us that those pictures existed at one point on the system.

## **Most Recently Used (MRU)**

- shortcuts to applications or files that have recently been used.

## **Restore Points**

- Restore points (RPs) are snapshots of key system settings and configuration at a specific moment in time (Microsoft Corporation).
- These snapshots can be used to return the system to working order.
- Three ways by which RPs are created:
- They can be created by the system automatically before major system events, like installing software.
- They can be scheduled at regular intervals, such as weekly.
- They can be created manually by a user
- They are normally hidden from the user.
- These RPs have metadata (data about the data) associated with them.
- This information could be valuable in determining the point in time when this snapshot was taken.
- If the RP contains evidence, this can tell us exactly when that data existed on the system in question.

## **Prefetch**

Prefetch files can show that an application was indeed installed and run on the system at one time.

Example:

- a wiping application such as “Evidence Eliminator.”
- programs like this are designed to completely destroy selected data on a hard drive.
- we may not be able to recover the original evidence as it has been wiped
- the mere presence of “Evidence Eliminator” can prove to be almost as crucial as the original files themselves

## **Link Files**

- Link files are shortcuts in microsoft
- They point to other files
- The computer itself creates them in several different places
- Recent option in the file menu tab
- Link files have their own date and time stamps showing when they were created and last used.
- Link means that someone actually opened the file in question.

## **Attribution**

- A windows PC will set up two accounts by default, the administrator and a guest account.
- The administrator has all rights and privileges on the machine.
- The guest generally has less authority.
- Each account on the machine is assigned a unique number called a security identifier or SID.
- Many actions on the computer are associated with, and tracked by, a specific SID.
- It's through the SID that we can tie an account to some particular action or event.
- Run the command 'whoami /user' from command line to get the SID for the logged in user.



## **External Drives**

- Theft of intellectual property is a huge concern
- One way that would-be thieves could easily smuggle data out of an organization is by way of one of these external storage devices, such as a pen-drive.
- Additionally, these devices can also be used to inject a virus or store child pornography.
- Examiners are often asked to determine whether any such device has been attached to a computer
- Whether or not such a device was attached can be determined by data contained in the registry.

## **Print Spooling**

- In some investigations a suspect's printing activities may be relevant.
- The delay observed after clicking the 'print' button is an indication of a process called spooling.
- Spooling temporarily stores the print job
- Windows creates a pair of complementary files
- Enhanced Meta File (EMF) which is an image of document to be printed
- Spool file which contains information about the print job itself.
- Spool file (.spl): printer name, computer name as well as the user account
- Normally deleted automatically after the print job is finished

Exception:

- some kind of problem and the document didn't print.
- computer that is initiating the print job may be set up to retain a copy
- Copies of extortion letters, forged contracts, stolen client lists, and maps to body dump sites are few pieces of evidences

# Examining Linux File Structures

- The most widely used distributions include Ubuntu, CentOS, Mint, Fedora, and Gentoo.
- UNIX was created in the early 1970s to be a multiuser, multithreaded, secure OS.
- The Linux kernel is usually packaged with other software components, such as a GUI and applications, so that users don't have to combine several open-source elements to create a working environment.
- The term "kernel" is often used when discussing Linux because technically, Linux is only the core of the OS.
- Linus Torvalds, the inventor of Linux, maintains the official kernel.
- All other tools, graphical interfaces, and so forth are maintained and developed by others

**Table 7-2** Core top-level directories of a Linux system

Directory	Contents
/usr	Most applications and commands are in this directory or its subdirectories <code>bin</code> (stands for "binary" and contains binary files required at boot time) and <code>sbin</code> (which requires superuser permission to run the binaries in it).
/etc	Most system configuration files are stored in this directory.
/home	The home directories for all users, usually named after their usernames.
/root	The home directory for the root user (superuser), which is kept separate from other user home directories.
/dev	Device files that act as stand-ins for the devices they represent, as
/var	Subdirectories such as <code>log</code> (often useful for investigations), <code>mail</code> (storing e-mail accounts), and <code>spool</code> (where print jobs are spooled).

**Table 7-1** Linux system files

System file	Contents
/etc/exports	File systems exported to remote hosts; might include remote drive mappings
/etc/fstab	File system table of devices and mount points
/var/log/lastlog	User's last logon
/var/log/wtmp	Logon and logoff history information
/var/run/utmp	Current user's logon information
/var/log/dmesg	System messages log
/var/log/syslog	System log, occasionally called <code>system.log</code> or <code>kernel.log</code>
/etc/shadow	Master password file, containing hashed passwords for the local system
/etc/group	Group memberships for the local system
/etc/passwd	Account information for the local system

# File Structures in Ext4

Linux supports a wide range of file systems.

- The early standard was Second Extended File System (Ext2)
- Then Third Extended File System (Ext3) replaced Ext2 in most Linux distributions.
- Its major difference from Ext2 was being a journaling file system, which has a built-in file recovery mechanism used after a crash.
- Fourth Extended File System (Ext4)
- added support for partitions larger than 16 TB,
- improved management of large files,
- offered a more flexible approach to adding file system features
- In UNIX and Linux, everything is considered a file, including disk drives, monitors, tape drives, network interface cards, system memory, and directories.
- Linux has four components defining the file system: boot block, superblock, inodeblock, and data block.
- A block is the smallest disk allocation unit in the UNIX/Linux file system and can be 512 bytes and up
- Block size depends on how the disk volume is initiated.

Boot block:

- contains the bootstrap code—instructions for startup
- A UNIX/Linux computer has only one boot block, on the main hard disk

## **Superblock**

- contains vital information about the system and is considered part of the metadata
- specifies the disk geometry and available space
- keeps track of all inodes
- also manages the file system
- configuration information, such as block size
- file system names,
- blocks reserved for inodes,
- volume name
- Multiple copies of the superblock are kept in different locations on the disk to prevent losing such important information

## **Inode blocks**

- contain the first data after the superblock
- an inode is assigned to every file allocation unit.
- as files or directories are created or deleted, inodes are also created or deleted.
- the link between inodes associated with files and directories controls access to those files or directories.

### **Data block**

- directories and files are stored on a disk drive in this block
- this location is linked directly to inodes.
- the Linux file system on a PC has 512-byte sectors.
- a data block is equivalent to a cluster of disk sectors on a FAT or NTFS volume.
- blocks range from 1024 to 4096 bytes each on a Linux volume.

# Linux file system

## Inodes

- Inodes contain file and directory metadata
- When a file or directory is created on a Linux file system, an inode is assigned
- Contains the following information:
  - The mode and type of the file or directory
  - The number of links to a file or directory
  - The number of bytes in the file or directory
  - The file's or directory's last access time and last modified time
  - The inode's last file status change time
  - The block address for the file data
  - The indirect, double-indirect, and triple-indirect block addresses for the file data
  - Current usage status of the inode
  - The number of actual blocks assigned to a file

- The only pieces of metadata not in an inode are the filename and path.
- Inodes contain modification, access, and creation times, not filenames.
- An assigned inode has 13 pointers that link to data blocks and other pointers where files are stored.
- Pointers 1 through 10 link directly to data storage blocks in the disk's data block and contain block addresses indicating where data is stored on the disk.
- These pointers are direct pointers because each one is associated with one block of data storage.
- As a file grows, the OS provides up to three layers of additional inode pointers.
- In a file's inode, the first layer of pointers are called indirect pointers.
- The pointers in the second layer are called double-indirect pointers, and the pointers in the last or third layer are called triple-indirect pointers.





## **Indirect Pointers**

- To expand storage allocation, the OS initiates the original inode's 11th pointer, which links to 128 pointer inodes.
- Each pointer links directly to 128 blocks located in the drive's data block.
- If all 10 pointers in the original inode are consumed with file data, the 11th pointer links to another 128 pointers.
- The first pointer in this indirect group of inodes points to the 11th block.
- The last block of these 128 inodes is block 138.

## **Double-indirect Pointer**

- If more storage is needed, the 12th pointer of the original inode is used to link to another 128 inode pointers.
- From each of these pointers, another 128 pointers are created.
- This second layer of inode pointers is then linked directly to blocks in the drive's data block.
- The first block these double-indirect pointers point to is block 139.

## **Triple-indirect pointer**

- If more storage is needed, the 13th pointer links to 128 pointer inodes
- each pointing to another 128 pointers
- and each pointer in this second layer points to a third layer of 128 pointers
- then we encounter data blocks

## **Bad block inode**

- All disks have more storage capacity than the manufacturer states.
- For example, a 240 GB disk might actually have 240.5 GB free space because disks always have bad sectors.
- Windows does not keep track of bad sectors, but Linux does in an inode called the bad block inode.
- The root inode is inode 2, and the bad block inode is inode 1.
- Some forensics tools ignore inode 1 and fail to recover valuable data for cases.
- Someone trying to mislead an investigator can access the bad block inode, list good sectors in it, and then hide information in these supposedly “bad” sectors.

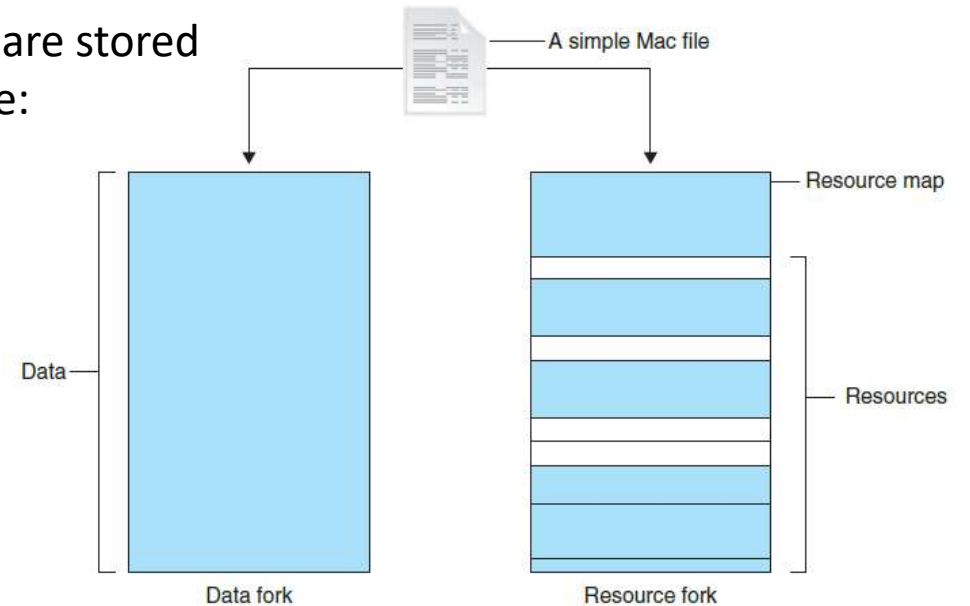
# Understanding Macintosh File Structures

- The current Macintosh OS is macOS, version 10.13, code-named High Sierra.
- Other versions still in use include 10.12.5 (Sierra), 10.11 (El Capitan), 10.9 (Yosemite), 10.6 (Snow Leopard), 10.7 (Lion), and 10.8 (Mountain Lion).
- macOS is built with the new Apple File System (APFS).
- Apple's OSs have been developing since 1984 with the introduction of Apple System 1.
- In 1997, Apple introduced Mac OS 8, followed by Mac OS 9 and then OS X.
- With OS X, Macintosh moved to the Intel processor and became UNIX based.
- Before OS X, the Hierarchical File System (HFS) was used, in which files are stored in directories (folders) that can be nested in other directories.
- With Mac OS 8.1, Apple introduced Extended Format File System (HFS+).
- The main difference between HFS and HFS+ is that HFS was limited to 65,536 blocks (512 bytes per block) per volume, and HFS+ raised the number of blocks to more than 4 billion.
- Consequently, HFS+ supports smaller file sizes on larger volumes, resulting in more efficient disk use.

# An Overview of Mac File Structures

In older versions of macOS, a file consists of two parts:

- a data fork, where data is stored,
- a resource fork, where file metadata and application information are stored
- Both forks contain the following essential information for each file:
  - Resource map
  - Resource header information for each file
  - Window locations
  - Icons



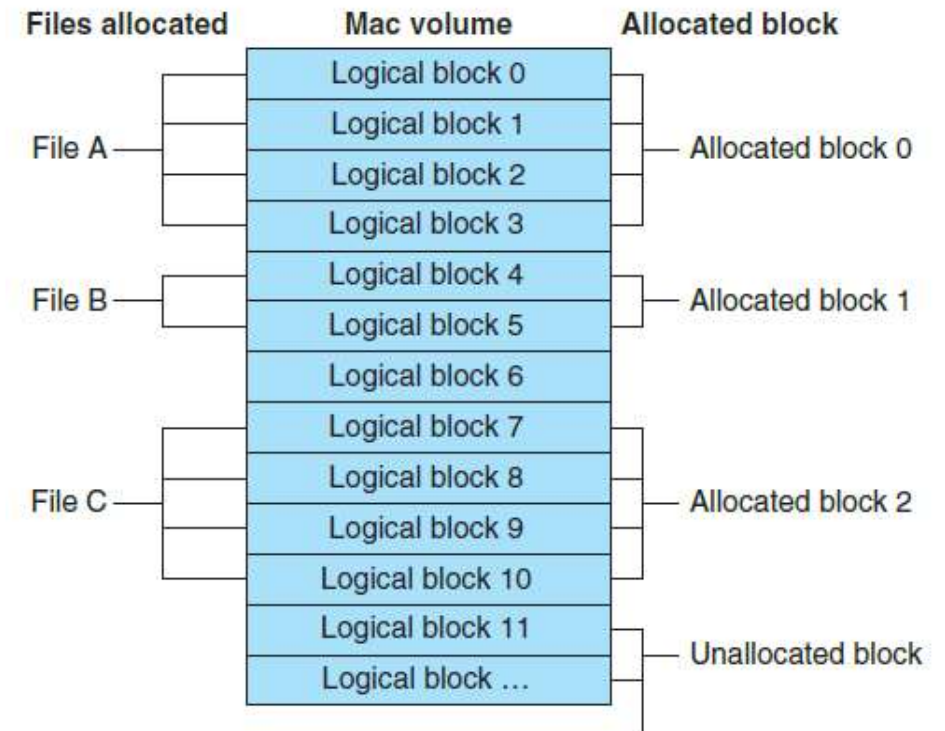
- The data fork typically contains data the user creates, such as text or spreadsheets.
- Applications, such as Microsoft Word or Excel, also read and write to the data fork.
- When you're working with an application file, the resource fork contains additional information, such as menus, dialog boxes, icons, executable code, and controls.
- In macOS, the resource or data fork can be empty.

# Volume

- A volume is any storage medium used to store files.
- It can be all or part of the storage media for hard disks
- In Mac OS 9 and earlier, a volume on a floppy disk was always the entire floppy.
- With larger disks, the user or administrator now defines a volume.
- Volumes have allocation blocks and logical blocks.
- A logical block is a collection of data that cannot exceed 512 bytes.
- When you save a file, it is assigned to an allocation block, which is a group of consecutive logical blocks.

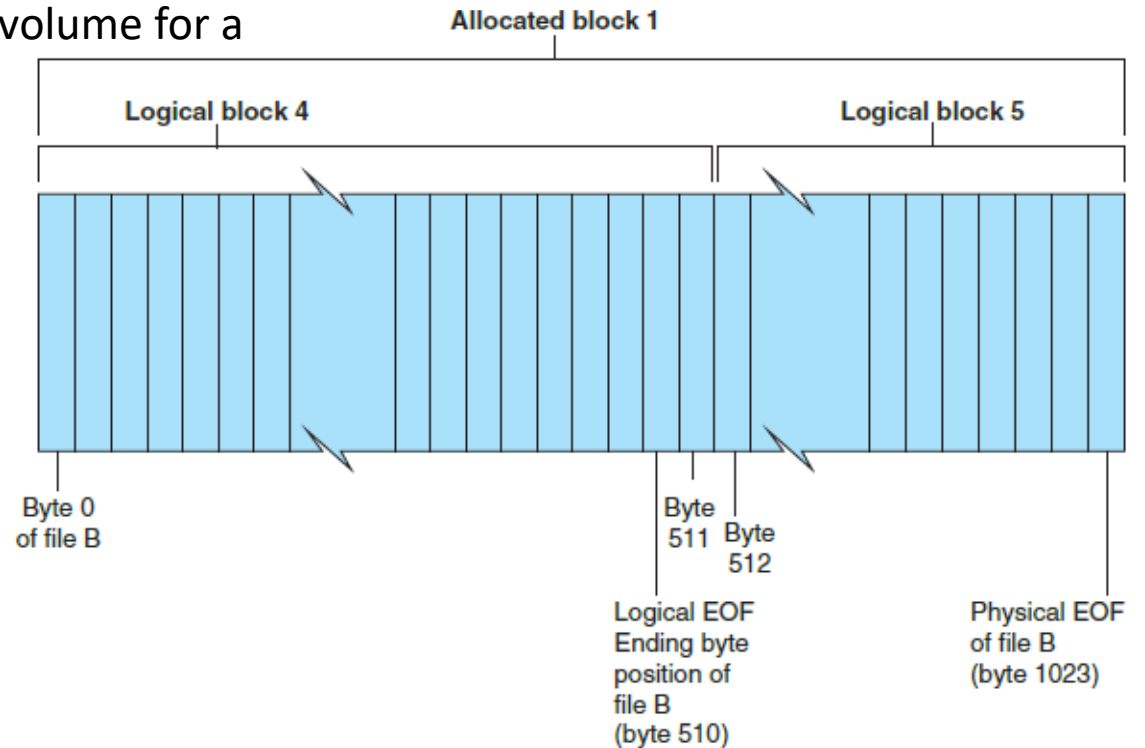
As volumes increase in size, one allocation block might be composed of three or more logical blocks

- If a file contains information, it always occupies one allocation block.
- For example, if a data fork contains only 11 bytes of data, it occupies one allocation block (512 bytes) on a disk, which leaves more than 500 bytes empty in the data fork.



# End of file

- The HFS and HFS+ file systems have two descriptors for the end of a file (EOF)—
- the logical EOF
- the physical EOF.
- The logical EOF is the actual ending of a file's data,
- if file B has 510 bytes of data, byte 510 is the logical EOF
- The physical EOF is the number of bytes allotted on the volume for a file,
- for file B, it's byte 1023



- For older HFS-formatted drives, the first two logical blocks, 0 and 1, on the volume are the boot blocks containing system startup instructions.
- Optional executable code for system files can also be placed in boot blocks.
- Older Mac OSs use the Master Directory Block (MDB) for HFS, which is the Volume Information Block (VIB) in HFS+.
- All information about a volume is stored in the MDB and written to it when the volume is initialized.
- A copy of the MDB is also written to the next-to-last block on the volume to support disk utility functions.
- Utility software is software designed to help to analyze, configure, optimize or maintain a computer.
- Perform disk and disk-volume-related tasks on the macOS operating system
- When the OS mounts a volume, some information from the MDB is written to a Volume Control Block (VCB), stored in system memory
- When a user no longer needs the volume and unmounts it, the VCB is removed.



# Acquisition of Digital evidence

## Introduction

- Data acquisition is the process of copying data
- For digital forensics, it is the task of collecting digital evidence from electronic media
- There are two types of data acquisition: static acquisitions and live acquisitions.

## Static acquisitions:

- capture data that is not accessed by other processes that can change it
- if you have preserved the original media, making a second static acquisition should produce the same results.
- the data on the original disk is not altered, no matter how many times an acquisition is done

## Live acquisitions:

- file metadata, such as date and time values, changes when read by an acquisition tool
- making a second live acquisition while a computer is running collects new data because of dynamic changes in the OS.

# Understanding Storage Formats for Digital Evidence

- The data a forensics acquisition tool collects is stored as an image file, typically in an open-source or proprietary format
- Each vendor has unique features, so several different proprietary formats are available
- Depending on the proprietary format, many forensics analysis tools can read other vendors' formatted acquisitions.
- Many acquisition tools create a disk-to-image file in an older open-source format, known as raw, as well as their own proprietary formats.
- The new open-source format, Advanced Forensic Format (AFF), is gaining recognition from some forensics examiners.

# Raw Format

In the past, examiners performed a bit-by-bit copy from one disk to another disk the same size or larger

- As a practical way to preserve digital evidence, vendors made it possible to write bit-stream data to files
- This copy technique creates simple sequential flat files of a suspect drive or data set.

The output of these flat files is referred to as a raw format.

## Advantages

- fast data transfers
- capability to ignore minor data read errors on the source drive
- most forensics tools can read the raw format, making it a universal acquisition format for most tools

## Disadvantage

- requires as much storage space as the original disk or data set
- some raw format tools, typically freeware versions, might not collect marginal (bad) sectors on the source drive
- Several commercial acquisition tools can produce raw format acquisitions
- Typically perform a validation check by using Cyclic Redundancy Check (CRC32), Message Digest 5 (MD5), and Secure Hash Algorithm (SHA-1 or later) hashing functions

# Proprietary Formats

Most commercial forensics tools have their own formats for collecting digital evidence.

Proprietary formats typically offer several features that complement the vendor's analysis tool

Some features include:

- The option to compress or not compress image files of a suspect drive, thus saving space on the target drive
- The capability to split an image into smaller segmented files for archiving purposes, such as to CDs or DVDs, with data integrity checks integrated into each segment
- The capability to integrate metadata into the image file, such as date and time of the acquisition, hash value (for self-authentication) of the original disk or medium, investigator or examiner name, and comments or case details

Disadvantage

- Inability to share an image between different vendors' computer forensics analysis tools.

# Advanced Forensic Format

Dr. Simson L. Garfinkel developed an open-source acquisition format called Advanced Forensic Format (AFF).

This format has the following design goals:

- Capable of producing compressed or uncompressed image files
- No size restriction for disk-to-image files
- Space in the image file or segmented files for metadata
- Simple design with extensibility
- Open source for multiple computing platforms and OSs
- Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata.
- Because AFF is open source, digital forensics vendors have no implementation restrictions on this format.

# Determining the Best Acquisition Method

There are two types of acquisitions: static acquisitions and live acquisitions.

- Typically, a static acquisition is done on a computer seized during a police raid, for example.
- If the computer has an encrypted drive, a live acquisition is done if the password or passphrase is available
- the computer is powered on and has been logged on to by the suspect.
- Static acquisitions are always the preferred way to collect digital evidence.
- Limitations in some situations
- encrypted drive that is readable only when the computer is powered on
- computer that is accessible only over a network

Data can be collected with four methods:

1. creating a disk-to-image file,
2. creating a disk-to-disk copy,
3. creating a logical disk-to-disk or disk-to-data file,
4. creating a sparse copy of a folder or file

# Disk-to-image file

- Most common method and offers the most flexibility for investigation
- Can make one or many copies of a suspect drive
- These copies are bit-for-bit replications of the original drive
- Can use many commercial forensics tools to read the most common types of disk-to-image files you create
- These programs read the disk-to-image file as though it were the original disk.

# Disk-to-disk copy

- Sometimes you cannot make a disk-to-image file because of hardware or software errors or incompatibilities
- This problem is more common when you have to acquire older drives.
- We create a disk-to-disk copy of the suspect drive.
- Several imaging tools can copy data exactly from an older disk to a newer disk.
- These programs can adjust the target disk's geometry (its cylinder, head, and track configuration) so that the copied data matches the original suspect drive.



# Logical disk-to-disk

- Collecting evidence from a large drive can take several hours
- A logical acquisition captures only specific files of interest to the case or specific types of files.

Example:

an e-mail investigation that requires collecting only Outlook .pst or .ost files.

# Sparse copy of a folder or file

- A sparse acquisition is similar to logical acquisition but also collects fragments of unallocated (deleted) data
- Used only when we do not need to examine the entire drive.

# Anti Forensics

Anti-forensics is an approach used by cybercriminals to challenge evidence gathering and analysis processes

Digital forensics has been very successful in investigations

As such, there is also a keen interest in obstructing these types of investigations

To combat these anti-forensics techniques, examiners must become familiar with the various ways to hide and destroy data.

John Barbara defines it this way “an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time consuming, or virtually impossible”

AntiForensics.com is a “community dedicated to the research and sharing of methods, tools, and information that can be used to frustrate computer forensic investigations and forensic examiners.”

The use of antifoensics techniques is not limited to terrorists

Corporate executives have put them to use as well, using these tools and techniques to hide or destroy incriminating e-mails, financial records, and so on

Even everyday applications such as web browsers have features that could be used to obstruct a forensic examination—clearing the Internet history, for example

Most newer browsers come with a “private browsing” mode that does not record things such as web sites visited and searches.

For Cyber Forensic Investigators

From an investigative perspective, it is important to know that there are legitimate uses of these antforensic tools and techniques

Proving the intent, therefore, is critical.

Suspects could assert that the wiping application was used only to protect their privacy or they used the defragmentation utility to improve performance

Types:

Hiding data

Password Attacks

Steganography

Data Destruction

## Data Hiding

- Some techniques applied for data hiding are:
- Changing file names and extensions,
- burying files deep within seemingly unrelated directories,
- hiding files within files,
- encryption

## Encryption

- The legitimate use of encryption has enabled us to enjoy many of the Internet services that we now take for granted
- For example, encryption used in ecommerce permits us to do online shopping
- It can also have serious consequences when used by criminals, terrorists, unfriendly nations, etc.

# What Is Encryption?

- Encryption is the conversion of data into a form, called cipher text, which cannot be easily understood by unauthorized people
- Encryption starts with plain text
- the original, unencrypted message
- is in the clear and can be read by anyone
- A cryptographic algorithm is then applied to the plain text, producing cipher text.
- Cipher text is basically a scrambled version of plain text that is unintelligible
- The algorithm is the method used to encrypt the message
- The key is data used to encrypt and decrypt the information.
- A password or passphrase is commonly used as the key.
- Fundamentally, there are two types of encryption algorithms: symmetrical and asymmetrical.
- Symmetrical encryption uses the same key to encrypt and decrypt the data.
- In contrast, asymmetrical encryption uses two separate and distinct keys
- The encryption algorithms themselves are open and well published
- Best practice in cryptography states that the security of algorithms should be “independent of their secrecy”
- the key should be the only secret

# Key Space

- Key space is a metric that is often discussed when talking about the strength of a particular encryption scheme
- The key space or key length has a direct impact on our ability to break the encryption, particularly with a brute force attack.
- Longer the key, more time it takes to find the correct combination
- Longer the keyspace, longer can be our key
- A brute force attack tries to break the password by attempting every possible key combination until the right one is found.



## Types of Encryption

- Encryption tools are now included with some versions of the newer operating systems
  - BitLocker is for Windows 7, FileVaultis for Apple OS X
  - These encryption schemes can be applied selectively, only encrypting certain files or folders
  - They can also be used to encrypt an entire drive.
  - This is known as full or whole disk encryption.
- 
- Operating systems in their course of normal operation will leave artifacts scattered across the drive
  - Even though we encrypt an entire folder containing our sensitive files, remnants (or the entire file) could be located in other places
  - Full disk encryption takes care of these data “leaks.”

Drawback:

Performance will likely suffer as the data are being encrypted and decrypted

# Password Attacks

- Breaking passwords, or cryptanalysis, can be encountered during an investigation
- Avoiding encryption is always preferable to having to attack passwords.
- There are tools and techniques we can use to increase our chances of success
- One thing working in our favor is the vulnerability that humans bring
- long random strings of letters, numbers, and characters make for excellent passwords
- they are also tough for people to remember
- most passwords are based on actual words, recognizable patterns, or both

Options include

- brute force attacks
- resetting passwords
- dictionary attacks

## Brute Force Attacks

- Use as much computing power as we can muster to guess the correct password
- The more computers (processors) we can use, the faster we can break it

## Password Reset

- Sometimes we will go after the software rather than the password.
- Some applications have vulnerabilities that can be exploited to simply reset the password, giving us the access we need.

## Dictionary Attack

- A dictionary attack is more precise, using words and phrases that can be collected from multiple sources
- Example: a forensic application can create an index of all the words found on a suspect's hard drive
- These words would come from both the allocated and unallocated space.
- Intelligence, the background information on our suspect or target, can really increase our chances of success.
- This information can be used to build a dictionary of potential passwords
- Gathering this information starts at the scene.

## Steganography

- Steganography, or stego for short, comes from the Greek words “Stegos” meaning covered and “Graphie” meaning writing
- Its exact roots equate to covered writing.
- A definition of steganography: “the hiding of a secret message within an ordinary message and the extraction of it at its destination”

There are two files composing the finished stegofile

Carrier file

Payload

- The file that contains the secret message is called the carrier file.
- Carrier files can be image files, video files, audio files, and word processing documents, just to name a few. The embedded secret document is called the payload.
- Carrier file types are used because they have a significant amount of redundant data, also known as “noise”
- The redundant data are replaced with the data composing the hidden message.
- Payload files do not necessarily have to be text based.
- An image file can be inserted into another image file.

Why stego is a challenge?

It is very difficult to detect.

Once discovered it is very tough, if not impossible, to extract the payload without knowing the stego application and password used to create it.

## Data Destruction

- Sometimes hiding data is not enough, and perpetrators try to destroy the data instead
- Destroying the data is a little more complicated than hitting the delete key
- Many drive wiping tools can be very effective in removing data completely
- Using utilities such as these can leave telltale signs of their use, providing substantial evidence even without the original data in question.

## Drive Wiping

- Drive wiping utilities are used to overwrite data on a hard drive in such a way as to make them unrecoverable
- Most of these applications are promoted and/or intended to keep personal or corporate information private.
- Using these tools is not an “all or none” proposition
- They can wipe only specified files while leaving others untouched
- Operating system files, for example, could be left intact.
- They can target specific files and folders as well as potentially incriminating system values like those found in the Windows Registry.

- From an evidentiary or investigative perspective, the presence or use of these applications can serve as the next best thing to the original evidence.
- Suspects may find it hard to explain why “Evidence Eliminator” software was installed and run on their computer the day before their computer was searched.
- The figure showing windows registry entry is an indicator that this software was installed on the machine.
- Wiping utilities can leave telltale signs of their use.
- When looking at the drive at the bit level, a distinct repeating pattern of data may be seen.
- This is completely different from what would normally be found on a hard drive in everyday use.



LOGOUT





# Contact Me



Viralparmarhacker@gmail.com



Facebook.com/viralparmarhacker



Twitter.com/viralparmarhack



Instagram.com/viralparmarhacker



Linkedin.com/in/viral-parmar



www.viralparmarhacker.com



+91 8980808222, +91 8866827872



**COMEXPO  
CYBER SECURITY  
FOUNDATION**

**Stay Connected  
Stay Safe**

A blue rectangular button with a white border. Inside, the word "LOGOUT" is written in a bold, black, sans-serif font. The two 'O's are replaced by circular icons composed of small, multi-colored segments (red, orange, yellow, green, blue, purple).

LOGOUT

is the hardest  
button to click.



**#LogOutNow**