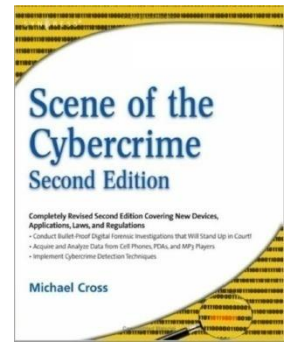


Chapter – 5

“The Computer Investigation Process”

Book Reference: Shinder L. D., Cross M., Scene of the Cybercrime, Syngress.



Course Objectives: To maintain an appropriate level of awareness, knowledge and skill required to understand and recreate the criminal terminology and Cyber Forensics investigation process.

Introduction to Cybercrime: Defining Cybercrime, Understanding the Importance of Jurisdictional Issues, Quantifying Cybercrime, Differentiating Crimes That Use the Net from Crimes That Depend on the Net, working toward a Standard Definition of Cybercrime, Categorizing Cybercrime, Developing Categories of Cybercrimes, Prioritizing Cybercrime Enforcement, Reasons for Cybercrimes.

Understanding the People on the Scene: Understanding Cybercriminals, Profiling Cybercriminals, Categorizing Cybercriminals, Understanding Cyber victims, Categorizing Victims of Cybercrime, Making the Victim Part of the Crime-Fighting Team, Understanding Cyber investigators, Recognizing the Characteristics of a Good Cyber investigator, Categorizing Cyber investigators by Skill Set.

Computer Investigation Process: Demystifying Computer/Cybercrime, Investigating Computer Crime, How an Investigation Starts, Investigation Methodology, Securing Evidence, Before the Investigation, Professional Conduct, Investigating Company Policy Violations, Policy and Procedure Development, Policy Violations, Warning Banners, Conducting a Computer Forensic Investigation, The Investigation Process, Assessing Evidence, Acquiring Evidence, Examining Evidence, Documenting and Reporting Evidence, Closing the Case.

Acquiring, Duplicating and Recovering Deleted Files: Recovering Deleted Files and Deleted Partitions, recovering "Deleted" and "Erased" Data, Data Recovery in Linux, Recovering Deleted Files, Recovering Deleted Partitions, Data Acquisition and Duplication, Data Acquisition Tools, Recovering Data from Backups, Finding Hidden Data, Locating Forgotten Evidence, Defeating Data Recovery Techniques.

Collecting and Preserving Evidence: Understanding the Role of Evidence in a Criminal Case, Defining Evidence, Admissibility of Evidence, Forensic Examination Standards, Collecting Digital Evidence, Evidence Collection, Preserving Digital Evidence, Preserving Volatile Data, Special Considerations, Recovering Digital Evidence, Deleted Files, Computer Forensic Information, Understanding Legal Issues, Searching and Seizing Digital Evidence

Building the Cybercrime Case: Major Factors Complicating Prosecution, Difficulty of Defining the Crime, Jurisdictional Issues, The Nature of the Evidence, Human Factors, Overcoming Obstacles to Effective Prosecution, The Investigative Process, Investigative Tools, Steps in an Investigation, Defining Areas of Responsibility.

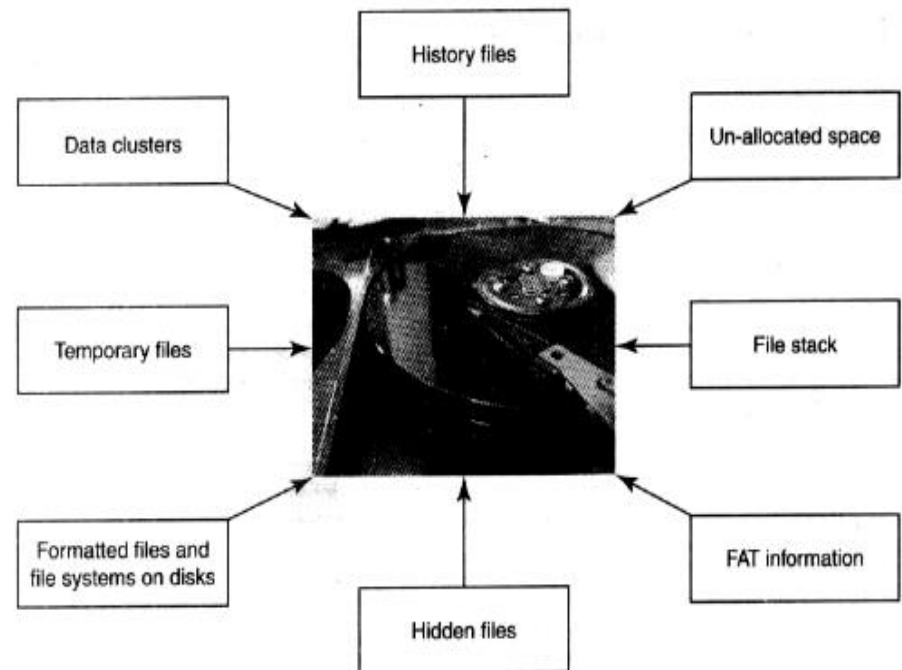
Chapter 5

Outline

- Demystifying Computer/Cybercrime
- Investigating Computer Crime
- How an Investigation Starts
- Investigation Methodology
- Securing Evidence
- Before the Investigation
- Professional Conduct
- Investigating Company Policy Violations
- Policy and Procedure Development
- Policy Violations
- Warning Banners
- Conducting a Computer Forensic Investigation
- The Investigation Process, Assessing Evidence
- Acquiring Evidence
- Examining Evidence
- Documenting and Reporting Evidence
- Closing the Case

Introduction

- The word *forensics* means “*characteristics of evidence*” that :
 - *satisfies its suitability for admission as fact , and*
 - *its ability to persuade based upon its proof.*
- It is derived from a Latin term meaning a *forum in which legal disputes are settled*. It is an *art or study of argumentation and formal debate*
- *Computer forensics refers to an systematic investigation process of “identification”, “acquisition”, “preservation” and “analysis “ of digital evidence* after an unauthorized/illegal use of computer has taken place.
- *Computer forensics* is applied to *establish facts* so that *accurate testimony and evidence can be later presented in court*. It is important to note that *any work an investigator performs will be scrutinized* in the court.
- A *computer forensic technician* uses *specialized methods, techniques, and tools* to acquire digital data stored on Hard Disks, RAM, Universal Serial Bus (USB) flash drives, or other Electronic Communication Device(ECD).
- After digital data is acquired from a device, it is examined to identify *which files, folders, or information may be useful as evidence*, and can provide facts about the case.



- Although computer forensics is commonly used in criminal cases but it can also be used in civil disputes or corporate investigations, such as when *internal policies have been violated*.

For Example:

When an employee is suspected of using a computer to perform some action that violates policies, the files, e-mail, and other data on the computer may be inspected.

- Because it is possible that the violations could lead to application of criminal charges or civil actions against the employee, it is important that proper forensic procedures are followed for evidence collection and analysis.
- Collecting digital evidence can take a considerable amount of time to ensure that evidence is collected correctly.
- It is vital that the data isn't modified as it's acquired, or afterward when the data is examined for evidential value. Because it may establish the identity of a culprit or may be used to establish the innocence of people.
- In addition to this, every action and result needs to be meticulously documented as this information is required in the court. By documenting the forensic procedure adopted, a computer crime can be effectively investigated with a higher degree of success later in the court.

Demystifying Computer/Cybercrime

- With the high acceptance of computer technology within the society, a new world of opportunity has been added to the criminal element that constantly looks for new ways to exploit people through time-proven scams and tactics and a person can be threaten of his life. Many crimes require **the use of inherent capabilities of the computer** for its commission.

For Example :

- *An e-mail phishing scam* where a bad guy generates a fictitious e-mail for the sole purpose of enticing people to a spoofed site where they are conned into entering sensitive personal information.
- A suspect might use the computer to scan and generate fake bank checks, currency, or create fake identification.
- **Methodology used:** physical access to victim machine, exploit vulnerabilities in system and network, deceiving victims to allow their system access, gathering the victims information.
- **The key to a successful investigation of a computer crime is :**
 - ❑ The **development** (what ,when, where, who, how, why) and **follow-up of case leads**.
 - ❑ To gain at least some basic **computer knowledge and skills** to put you ahead of the average computer user; skills that allow you to apply **traditional policing skills and procedures to the case**.
 - ❑ Familiarity with **policies and procedures** of the company.
- When investigation begins, the investigator must define **the type of evidence sought**.

Investigating Computer Crime

- As computers are so commonly used in homes and businesses, they are prominent **source of evidence**.
- Almost any type of crime may result in some type of **evidence being stored on a computer**. **Files stored on computers** may contain a relevant information that can be used to convict a suspect or prove his/her innocence.

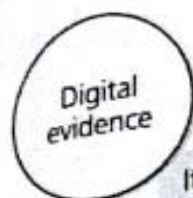
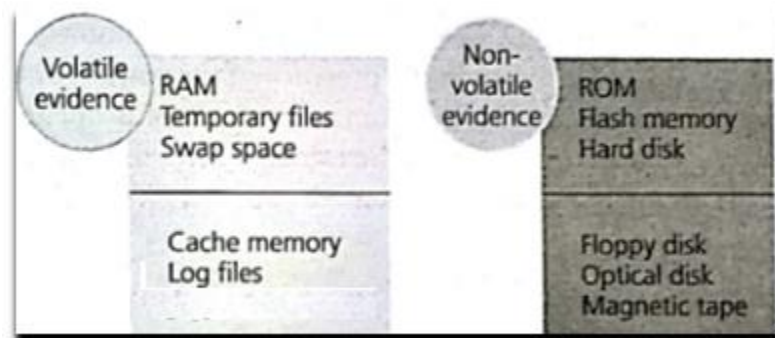
For example :

A suspect may have written about his or her plans in a file on the computer, or in a blog on the Internet. Conversely, if a person was accused of sending e-mail threats, a simple check of the messages on his or her machine could establish whether the accusations are true or false.

- There are a number of cybercrimes that demand a detailed computer forensic examination:
 - **Theft of intellectual property/ copyright violations/data leak/**
 - **Threatening e-mails, threat to life circumstances**
 - **Harassment**
 - **Online Fraud**
 - **Hacking , dissemination of viruses, Denial of Services**
 - **Child pornography and digital contrabands**
- When crimes are committed using computers, often the **only evidence available to prosecute** the culprit is in **digital format** such as:
 - ☐ Illegal images will be stored only on a hard disk or other medium
 - ☐ proof of an intruder's activities may be stored in system /network logs
 - ☐ documents containing evidence/indicators of the crime
- By examining the digital contents of the computers, an investigator can
 - ☐ **reach a successful conclusion about prosecuting the suspect/culprit** and
 - ☐ using the information acquired from the investigation to **make existing systems more secure**.

Digital Evidence

- Digital evidence is defined as information and data that is stored , received or transmitted by an electronic device which is of investigative value to a case.
- Digital evidence exist in two forms
 - **volatile**
 - **Nonvolatile**
- Digital evidence is different from physical evidence.



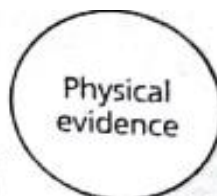
It can be duplicated and the duplicated copy can be used in the place of the original.

Any tampering or modification of its contents can be identified in comparison with the original using appropriate software.

It cannot be deleted easily and can be recovered even if deleted.

It can be reproduced if the duplicated copy is destroyed intentionally.

It is less tangible in nature.



It cannot be duplicated like digital evidence.

Any tampering or modification cannot be identified.

It cannot be recovered if it is deleted.

It cannot be reproduced if it is destroyed intentionally.

It is more tangible in nature.

Digital evidence can be sought from different sources:

- Bookmarks and Favorites
- Browser history /cache / accounts
- Contact lists/ Calendars / Sticky notes
- Compressed archives and Databases
- Configuration files (may contain account information, last access dates) and registry content
- Documents (doc,txt, pdf, jpg, png...etc) and their metadata /deleted files /encrypted files / password protected files /shared files
- File systems and deleted partitions
- Email messages and attachments
- Events and System logs
- Hidden files and folders
- Multimedia Content – audio/video/pictures(text written in pictures)
- Virtual machines / installed programs/ running processes
- Temporary Files
- Harddisks/pendrives/memory cards/ Ram/Registers/ swap space/unallocated spaces/ slack space
- Cloud storages/ CD-DVD/External Harddisks
- Mobile Devices and their backups stored on computers
- Network Communications: Evidence at Application ,Network and Transport Layer

- Law enforcement officers may sought **forensic services** from IT/ Professionals

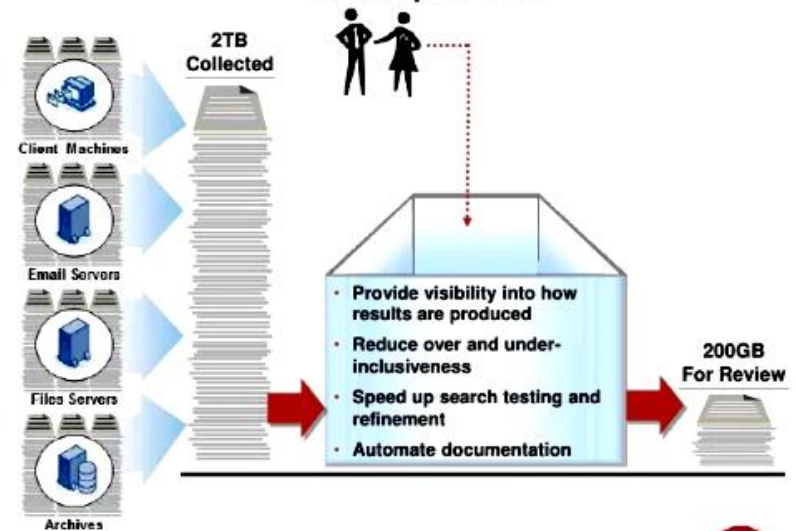
Such computer forensics services include the following:

1. Data culling and targeting;
2. discovery/subpoena process;
3. production of evidence;
4. expert affidavit support;
5. criminal/civil testimony;
6. cell phone forensics;

Specific client requests for forensics evidence extracting solution support include:

1. Index of files on hard drive;
2. index of recovered files;
3. MS Office/user generated document extraction
4. unique E-Mail address extraction;
5. Internet activity/history;
6. storage of forensics image
7. keywords search;
8. chain of custody
9. mail indexing;
10. deleted file/folder recovery;
11. office document recovery;
12. metadata extraction;
13. log extraction;
14. instant messaging history recovery;
15. password recovery;
16. network acquisitions.

E-Discovery Search Needs to Become More Transparent



Data Culling Methods

Most common data culling methods include:

- **DeNisting** : DeNisting is the process of removing documents from a review because they hold no evidentiary value. **For Example:**
 - DeNIST is a list of common system files compiled by the National Institute for Standards and Technology. De-NISTing is the process of removing all so-called system files that are deemed to have no evidentiary value, like executables, OS Files, DLLs, etc
- **Deduplication** : Deduplication (or "De-dupe") is the process of identifying and removing or suppressing duplicate documents from a review.
- **Custodian:** Data custodians are "persons having administrative control of a document or electronic file." So, identifying documents by owner, user, group.
- **Email threading:** email threading involves identifying the relationships within emails by parsing through threads, people, and attachments. Investigating teams can eliminate the whole chain at once if immaterial.
- **Search terms:** Search terms are the words or phrases that you use to search for documents in a review.
- **Filtering** : Filter relevant documents by file type, by date, Keywords, Domain (junk mail, newsletters, etc)

Obstacles/Challenges with digital evidence:

- Digital data obtained from storage media is huge and extracting the right piece of data of evidential value is a big challenge.
- Digital evidence is volatile and susceptible to alteration and would demand high level of expertise/skill, valid tools for its acquisition, preservation and analysis.
- The working environment will bring challenges such as files that have been renamed, password protected, hidden(language, misspell keywords, files stored as graphics etc), deleted, encrypted, disk space formatted/wiped out/overwritten, faulty hardware.
- A single evidence may be incomplete and more evidence may be demanded in order to come to a concrete conclusion.
- The collected evidence should completely map the crime committed (correct Criminal --- Victim). For example: In organizations, computers are reissued when employee joins the company. Computers that is continuously used may destroy the incriminating evidence against a former disgruntled employee who may have used the reissued computer. Constant use of computers may raise question as to when and who created the incriminating evidence.

- Acquisition of evidence is both legal and technical problem.

It requires:

- What particular piece of digital evidence is required for examination, (physical context –should reside on specific piece of media)
- Where that piece of digital evidence logically located relative to file system.(logical context)
- What that piece of digital evidence interpret? (Legal context –looking at the evidence as machine language – For ex: ASCII)

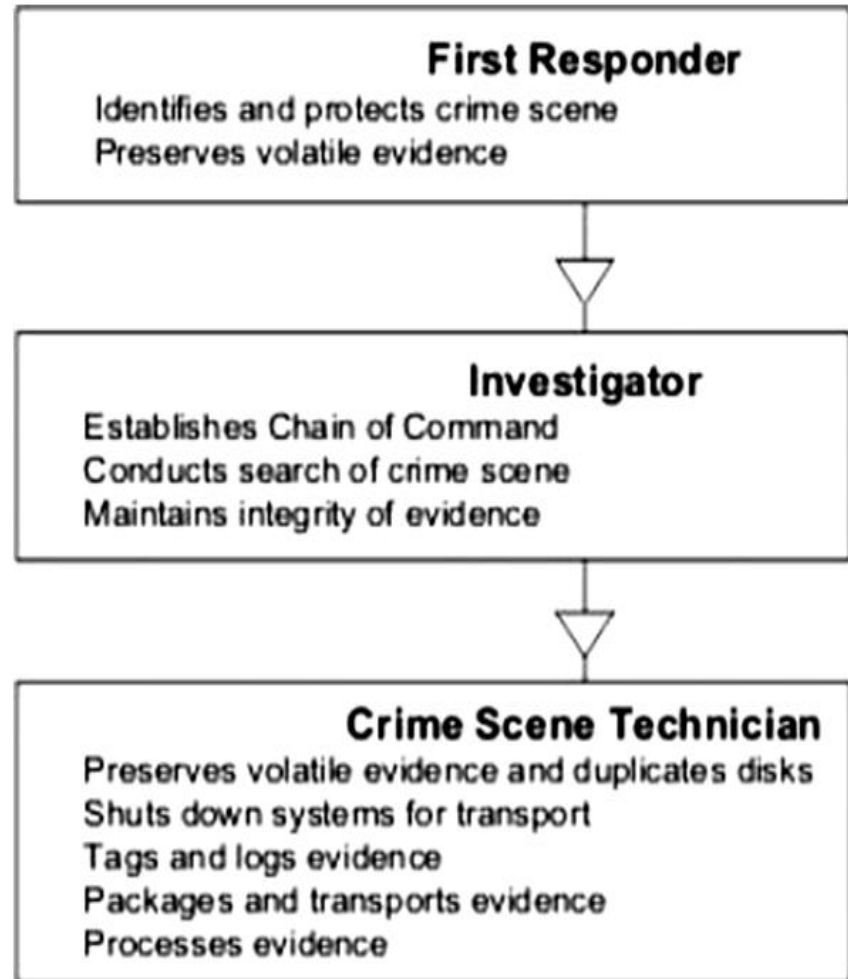
Offset	Hexadecimal	ASCII
00000000	00 60 94 A5 27 FF 00 04-AC EA 03 B9 08 00 45 00E
00000010	00 A3 04 03 40 00 40 06-82 FA C0 A8 01 03 C0 A8	...@.@
00000020	01 04 00 50 C0 5D B8 74-D9 30 9C C8 F3 12 50 18	...P.]t.O...P.
00000030	83 2C A0 6D 00 00 48 54-54 50 2F 31 2E 30 20 32	...m..HTTP/1.0 2
00000040	30 30 20 4F 4B 0D 0A 53-65 72 76 65 72 3A 20 47	00 OK..Server: G
00000050	6F 53 65 72 76 65 2F 32-2E 35 30 0D 0A 43 6F 6E	oServe/2.50..Con
00000060	74 65 6E 74 2D 54 79 70-65 3A 20 74 65 78 74 2F	tent-Type: text/
00000070	68 74 6D 6C 0D 0A 43 6F-6E 74 65 6E 74 2D 4C 65	html..Content-Le
00000080	6E 67 74 68 3A 20 34 32-35 31 0D 0A 43 6F 6E 74	ngth: 4251..Cont
00000090	65 6E 74 2D 54 72 61 6E-73 66 65 72 2D 45 6E 63	ent-Transfer-Enc
000000A0	6F 64 69 6E 67 3A 20 62-69 6E 61 72 79 0D 0A 0D	oding: binary...
000000B0	0A 00 00 00 00

How an Investigation Starts

- Investigations always start with the following two factors:
 1. A crime being committed
 2. Someone taking a notice of it.
- If these two factors aren't in place, an investigation will never occur. **For Example:**
A situation where a man has downloaded obscene content to his computer.
 - ❖ Now, If the people posing in these images are of legal age, it may not be illegal for this man to save the images to his hard disk, but if the images depict minors, the pictures are illegal and a crime has been committed. **However, even though a crime has been committed, this doesn't mean this man will ever be investigated.**
- For an investigation to occur, **someone must notice that some illegal activity has happened**, and **report it to the appropriate authorities**.
- If no complaint is made, the person gets away with the crime. The **complainant plays a key role in any investigation**.
- The **complainant** provides essential information about what he or she has discovered. The complainant may have seen illegal materials stored on a coworker's computer and can identify which computer contained the evidence.
- If the **complainant** was repairing a computer and found illegal files in a particular directory, he or she **can assist in an investigation by indicating where the files are stored**.
- The statements made by a **complainant** can also be **used to acquire search warrants** and can be used as the basis for further **testimony in court**.
- If the **complainant** notices that his or her home computer has been involved in a criminal offense, then the complainant is the victim and the computer is a target of a crime.

Primary Roles in an Investigation Involving Computer Forensics

- **Incident Response (IR)** is the effort to quickly **identify an attack**, **minimize its effects(contain damage)** and **remediate the cause** to reduce the risk of future incidents.
- Almost every company , at some level, has a process for incident response.
- Response is a part of Incident Handling which in turn looks at the **planning, preparation, logistics, communications, synchronicity** required to resolve an incident.
- The incident management work is generally done by the **Computer Security Incident Response Team (CSIRT)**
- Its role includes **protect, detect and respond**.
- To be effective, it is important that the **incident is identified and reported on time**.



Protect

- ❑ This refers to making sure an organization has taken the necessary measures and precautions to secure itself before any cyber security problems arise. This area focuses on proactive strategies rather than reactive strategies.
- ❑ Some of those protection strategies are:
 - Create an organizational incident response plan.
 - Perform risk assessments or analysis.
 - Create an up-to-date asset inventory management
 - Implement vulnerability scanning tools and intrusion detection systems (IDS).
 - Provide security awareness training for all employees.
 - Build configuration, vulnerability and patch management
 - Develop and update security plans, policies, procedures and incident response training materials.
 - Detail guidelines for users on what security issues should be reported and outline a process for making a report.
 - Create incident response playbooks for common incident types.
 - Deploy internal and external defensive measures that are regularly updated based on current threats.
 - Reevaluate the effectiveness of procedures every time an incident occurs.

Detect

- ❑ Incidents cannot be responded to unless they are detected. Effective detection takes time and effort.
- ❑ A common detection strategy is to implement a defensive network architecture using technology such as routers, firewalls, intrusion detection and prevention systems, network monitors and security operations centers (SOC).
- ❑ Common questions that need to be answered prior to developing a detection strategy include:
 - What applications are always in use?
 - What are the user privileges and permissions?
 - What does normal network traffic look like?
 - Which network protocols are in use?
 - Which network protocols should never appear on the network?
 - What are bandwidth utilization patterns?
 - What devices are supposed to be attached to the network?
 - Who are the system and data owners for these attached hosts and devices?

Respond

- Once a computer security incident/breach has been detected, formal incident response can commence.
- Critical steps that need to be followed to prevent loss of data before forensic experts arrive:
 - Immediately record observations about the crime scene, so that any useful information is not missed out for experts to analyze.
 - Do not allow anyone to touch the machine without forensic training or certification.
 - Click pictures of the scene from all the sides.
 - Do not change the current state of the device i.e.
OFF to be kept OFF, ON to be kept ON.
 - Do not plug any external storage media in the device before the forensic experts arrive.
 - Do not copy anything to or from the device.
 - Do not open anything like pictures, application or files on the device.
 - Do not install any new application on the device

For Forensic experts

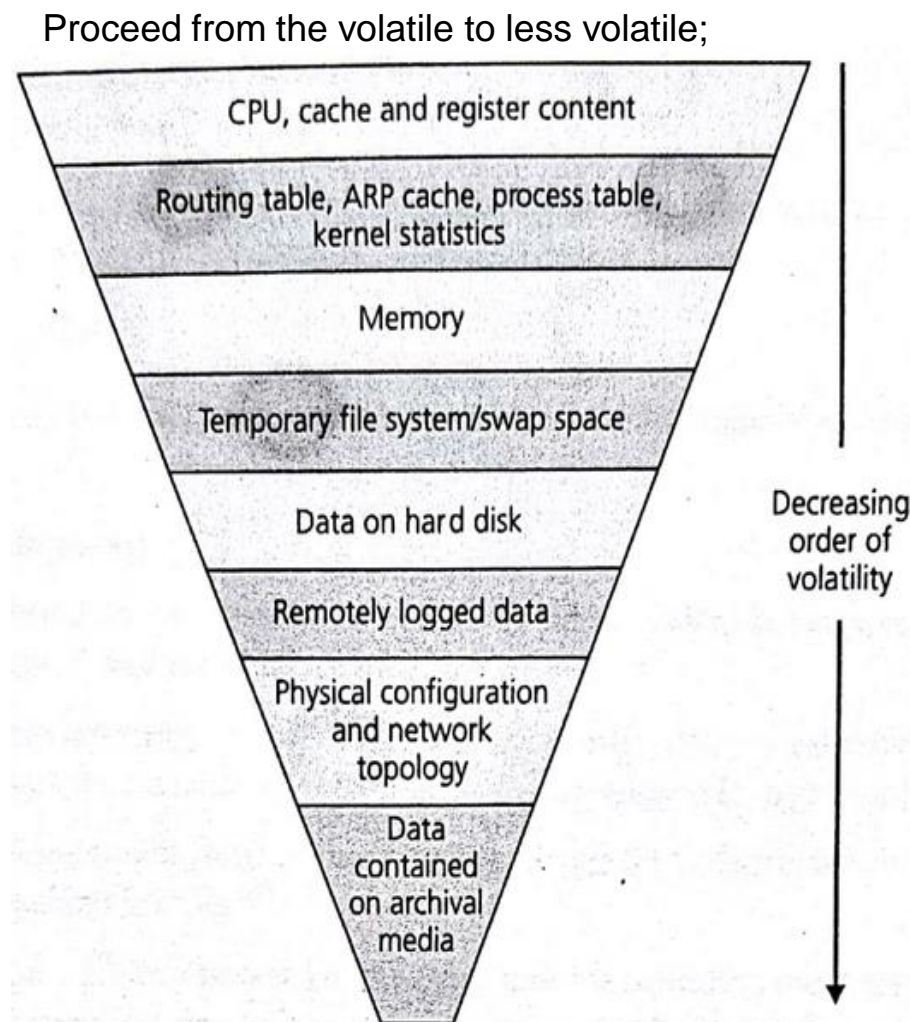
- ❑ It is very important to ensure that the crime scene is fully secure before and during the search.
 - Identify the number and type of computers.
 - Interview the system administrator and users.
 - Identify and document the types and volume of media: This includes removable media also.
 - Determine if a network is present.
 - Document the information about the location from which the media was removed.
 - Identify offsite storage areas and/or remote computing locations.
 - Identify proprietary software.
 - Determine the operating system in question.

Investigation Methodology

- *Investigation methodology* is the practices, procedures, and techniques used to collect, store, analyze, and present information and evidence that is obtained through a computer forensic investigation.
- The individual steps to perform these tasks can vary from case to case and may depend on the types of software and equipment being used, many common practices will always be consistent.
- The methodology of a computer forensic investigation into three basic stages:
 1. Acquisition
 2. Authentication
 3. Analysis

1. **Acquisition** is the act or process of gathering information and evidence.

- Evidence pertains **not only to a computer that's been seized**, but also to the **data stored on that computer**.
- It is the data on a computer that will be used to further provide insight into the details of a crime or other incident.
- Evidence should be collected in the **decreasing order of volatility**.--->
- **Computer forensic software** can be used to acquire data from a machine, and make an exact copy (image of the data) of everything stored on the hard disks along with user data.
- It includes **system and configuration files**, **executable programs**, and **other files that are installed with the operating system and other application software's files**.
- The investigator/ computer forensic technician **study the image** of the computer's data and the machine's original data is kept unaltered during examination.



How would the court know that anything found was really on the original machine?

2. Authentication is a process of ensuring that the acquired evidence is the same as the data that was originally seized. Authentication means satisfying the court that :-

(a) the contents of the record have remained unchanged,

(b) that the information in the record does in fact originate from its purported source, whether human or machine.

(c) that extraneous information such as the apparent date and time of the record is accurate.

- **PROBLEM:-**If the data that's been acquired from a computer was corrupted, modified, or missing from the imaging process, it would not only affect your ability to accurately examine the machine's contents, but also could make all of the evidence you find on the computer inadmissible in court.
- To authenticate the data that's acquired from a suspect computer, verification features such as hashing included in forensic software can be used to compare the data that's duplicated in the imaging process to the original data on a suspect's computer.
- It may be sufficient for an individual/expert who is familiar with the digital evidence to testify to its authenticity. For instance, the individual who collected the evidence can confirm that the evidence presented in court is the same as when it was collected or Testimony of a witness with knowledge can be taken into consideration.
- To authenticate digital evidence, it may also be necessary to demonstrate that a computer system or process that generated digital evidence was working properly during the relevant time period.
- Once these steps have been completed, the content of the computer can then be inspected for individual pieces of evidence that will later be used in court or other disciplinary processes.

Chain of Custody

- All evidence presented in a court of law must exist in the same condition as it did when it was collected i.e. it needs to be proven in the court that the evidence did not change during investigation.
- The documentation that chronicles every move and access of evidence is called the *Chain of Custody (CoC)*. The chain starts when you collect any piece of evidence.
- The court expects the chain of custody to be complete and without gaps. Even small deviations from the published chain logs can render evidence inadmissible. Defense attorneys will look for such mistakes to take it as an advantage.
- You need to demonstrate a complete chain of custody from collection to appearance in court by providing the chain of custody evidence log that shows every access to evidence. The CoC form must be kept up-to-date.
- Sample:-> Download sample custody form: www.nist.gov/document/sample-chain-custody

Chain of Custody Log

Line	Item	Date	Time	Who	Description
1	Hard disk drive, ser #123456	7/15/04	10:15 AM	M. SOLOMON	Seized hard drive from scene, permission provided by business owner
2	Hard disk drive, ser #123456	7/15/04	10:45 AM	M. SOLOMON	Transported HDD to evidence locker in main office
3	Hard disk drive, ser #123456	7/16/04	7:30 AM	M. SOLOMON	Removed HDD to create analysis copy
4	Hard disk drive, ser #123456	7/16/04	9:15 AM	M. SOLOMON	Returned HDD to evidence locker

- The key to providing a chain of custody that a court will accept is. [meticulous documentation----->](#)
- You must enter notes into an **evidence log**, listing all information pertinent to the access of the evidence.
- Each and every time evidence is accessed (including initial collection) the evidence log should contain at least the following information:

- ◆ Date and time of action
- ◆ Action type
 - ◆ Initial evidence collection
 - ◆ Evidence location change
 - ◆ Remove evidence for analysis
 - ◆ Return evidence to storage
- ◆ Personnel collecting/accessing evidence
- ◆ Computer descriptive information
 - ◆ Computer make and model
 - ◆ Serial number(s)
 - ◆ Location
 - ◆ Additional ID information
 - ◆ BIOS settings specific to disk drives
- ◆ Disk drive descriptive information
 - ◆ Disk drive manufacturer and model number
 - ◆ Drive parameters (heads, cylinders, sectors per track)
 - ◆ Jumper settings
 - ◆ Computer connection information (adapter, master/slave)
- ◆ Handling procedure
 - ◆ Preparation (static grounding, physical shock, etc.)
 - ◆ Contamination precautions taken
 - ◆ Step-by-step events within action
 - ◆ Inventory of supporting items created/acquired (i.e., hash or checksum of drive/files)
- ◆ Complete description of action
 - ◆ Procedure used
 - ◆ Tools used
 - ◆ Description of each analysis step and its results
 - ◆ Reason for action|
 - ◆ Notes
 - ◆ Comments that are not specifically requested anywhere else in the log
 - ◆ Notes section can provide additional details as the investigation unfolds

- The chain of custody form should answer the following questions:
- **What is the evidence?:** For example- digital information includes the files and its metadata, Hardware and its configuration like serial number, capacity etc, multimedia content and its description, network related indicators of crimes.
- **How did you get it?:** For example- Bagged, tagged or pulled from the desktop.
- **When it was collected?:** Date, Time
- **Who has handle it?** Member of CERT Team
- **Why did that person handled it?** Authorized or not
- **Where was it stored?:** This includes the information about the physical location in which proof is stored or information of the storage used to store the forensic image.
- **How you transported it?:** For example- in a sealed static-free bag, or in a secure storage container.
- **How it was tracked?**
- **Who has access to the evidence?:** This involves developing a check-in/ check-out process.

3. *Analysis is the process of examining and evaluating gathered information believed to be possible evidence against the culprit.*

- The person examining the machine **must filter (data culling) through all the computer files: hidden, deleted , configuration files,..etc** to find evidence related to his or her investigation.
- *When examining computer files, it is vital that they aren't modified in any way. Modification* refers to not only changing the information in the file itself (such as by accidentally changing the values entered in a spreadsheet), **but also modifying the properties of the file.**
 - - **For example**, opening a file could change the date and time property that shows when the file was last accessed. If it is to be proven when a suspect last viewed this image, **that information would be lost to you**, and a suspect could then argue that he or she never saw the file.
- Therefore, it is important to use tools that won't modify data in any way, and **that analysis occurs after the data is acquired and authenticated by imaging the suspect hard disk.**
- Analysis **will involve experimentation/usage of all the possible forensic methods and data carving techniques/tools** to get results of valid proof of crime.
- Analysis also **looks for information from individuals associated with the case** to determine the type of forensic tools required to look for relevant evidence.
- During analysis , **every action performed on the evidence needs to be well documented** to ensure the procedure is repeatable and capable of yielding the same result.

Securing Evidence

- If data and equipment are to be used as evidence, you will need to ensure that their integrity hasn't been compromised. **Preservation of data involves practices** that protect data and equipment from harm so that original evidence is preserved in a state as close as possible to when it was initially acquired.
- If during investigation and analysis, data is lost, altered, or damaged, **you may not even be able to mention it in the court.**
- Worse yet, **the credibility of how evidence was collected and examined may be called into question**, making other pieces of evidence inadmissible as well.
- Evidence must be secure throughout the investigation. **Securing evidence is a process that begins when a crime is first suspected, and continues after the examination has been completed.**
- If a trial, civil suit, or disciplinary hearing has ended, **the evidence must remain secure in case of an appeal or other legal processes** and a **retention date** should be set for all equipment and data that is retained as evidence.
 - **For example**, the police may retain evidence files acquired from forensic software for many years after a person has been convicted. Similarly, a company may retain such files for a few years after firing an employee, in case the person attempts to sue company for wrongful dismissal.
- The **retention date provides a guideline as to how long a forensic technician should retain the data** before deleting it, or allowing equipment to be released or destroyed.
- To determine specified dates, a company should **consult legal counsel**, and continue to be in contact with the investigator to determine whether the data acquired from an examination can be deleted or may still be needed.

Steps to be taken for Securing the evidence

A. Securing the Crime Scene

- **The first responder** is responsible for establishing the scale of the crime scene, and then securing that area.
- It can be as simple as securing a server closet or server room, whereas in some situations it may be as complex as dealing with computers and devices spread across a network.
- Once the suspected systems have been identified, it is important to **prevent individuals from entering the area**, and **protecting systems so that equipment isn't touched and data isn't manipulated or lost**.
- Anyone who does have access to affected systems **may be required to testify or at least explain his or her presence at the scene**. In worst-case scenarios, they may even be considered suspects.
- As part of securing the crime scene, **a list of anyone who has attempted to or has achieved access to the area should be developed**. This should include
 - ☐ the name of the person,
 - ☐ the time he or she entered and left the area,
 - ☐ the purpose of his or her presence.
- Important to adhere to the **site's security policy** and engage the appropriate **incident handling and law enforcement personnel**.

B. During the Investigation of a Machine

- Use Disk imaging software's to create an exact duplicate of a disk's contents, and therefore can be used to make copies of hard disks, CDs, DVDs, floppies, and other media.
- Disk imaging creates a bitstream copy, whereby each physical sector of the original disk is duplicated. The image is compressed into an image file, which is also called an *evidence file*.
- Once an image of the disk has been made, investigator should confirm that it's an exact duplicate.
- Authentication is vital to ensuring that the data that's been acquired is identical to that of the suspect's or victim's computer.
- Many computer forensic programs that create images of a disk have the built-in ability to perform integrity checks, whereas others will require you to perform checks using separate programs. Such software may use a cyclic redundancy check (CRC), using a checksum or hashing algorithm to verify the accuracy and reliability of the image.
- When investigator is ready to perform an examination, copies of data should be made/kept on media that's *forensically sterile* i.e. the disk has no other data on it, and has no viruses or defects.
- This will prevent mistakes involving data from one case mixing with other data, as can happen with cross-linked files or when copies of files are mixed with others on a disk.
- When providing copies of data to investigators, defense lawyers, or the prosecution, the **media used to distribute copies of evidence should also be forensically sterile.**

There are common/general sequence of steps that can follow to protect the integrity and prevent loss of evidence:

1. Photograph the computer screen(s) to capture the data and time displayed there at the time of seizure. Be aware that more than one monitor can be connected to a single computer;
2. Take steps to preserve volatile data-do not install new software, do not switch off the PC if ON.
3. Make an image of the disk(s) to work with so that the integrity of the original can be preserved. Investigator should take this step *before the system is shut down, in case the owner has installed a self-destruct program to activate on shutdown or startup.*
4. Check the integrity of the image to confirm that it is an exact duplicate, using a CRC or other program that uses a checksum or hashing algorithm to verify that the image is accurate and reliable.
5. After acquisition, shut down the system safely according to the standard procedures for the operating system that is running.
6. Photograph the system setup before moving anything, including the back and front of the computer showing cables and wires attached.
7. Unplug the system and all peripherals, marking/tagging each piece as it is collected.
8. Use an antistatic wrist strap or other grounding method before handling equipment, especially circuit cards, rams, disks, and other similar items.
9. Place circuit cards, disks, and the like in antistatic bags for transport.
10. Keep all equipment away from heat sources and any external magnetic fields.





C. When the Computer Is Not Being Examined

- **Computer must be stored in a secure location.** Once the computer has been transported from the original crime scene, it should be stored in a locked room or closet that has limited access. In police departments, this may be a **property room** or an area of the lab in which electronic evidence is acquired and examined.
- The room should be selected in the building with CCTV Surveillance and security personals at entry and exit points.
- For internal investigations conducted in a corporate environment, it should be treated with the same level of respect, and also stored in a location with limited access.
- Image of data acquired from a computer can be stored on a server or another computer that has very limited access.
- Lawyers, police investigators, and members of the IT staff fixing a computer, printer, or other device in the room may need to access the secure location from time to time. Keep track of those entering the room, you should maintain a log showing who entered the room or secure area, the dates and times they were there, and any other information(purpose of visit). By having people sign in and sign out, you can keep track of who had access should it ever come into question.
- If required, frisk a person on entry and exit to the limited access area.

Before the Investigation

- Investigating computer crimes demand lot of work to be done before they occur.
- The training and tools used in this type of investigation must be in place prior to examining any computer.
- The person examining the computer must be knowledgeable in computer forensics and different areas of IT, and the equipment and software used to perform the examination of a machine must already be available to him or her.
- When a crime does occur, certain actions must also be taken before attempting to acquire evidence from a machine. The investigator should be aware of the jurisdictional guidelines, Organization policy and Standard Operating Procedures(SOP).
- Interviews of victims /witnesses must be conducted. If this isn't done, time may be wasted searching for evidence that doesn't exist, or is located in other areas of a hard disk or even a different computer.
- Search warrants may needs to be obtained. In the worse case, if certain steps aren't followed, any evidence that is acquired may be inadmissible in court, making the entire process a waste of time.

Preparing for an Investigation

- It is important to take a **Proactive approach**
 - **Proactive Approach** – formal approach suitable for audit as well as fulfillment of forensic requirements such as : **Resilience** ensures accountability (insiders) by deploying security configurations and controls to detect and prevent security incidents. **Provenance** ability to trace any activity back to its source (time and location).
 - Proactive approach generates reliable evidence by logging and monitoring user action thus helps in audit.
- Computer forensics **requires**
 - **Knowledge of procedures, and expertise with forensic software and hardware that's being used to acquire and study the data.**
 - Additional experience with network components and technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP) are also essential, as is knowledge of computer hardware, as it's common to remove hard disks or other devices before connecting them to the investigator's computer to duplicate the data.
 - Obtain training through courses and **by studying under those with more experience in performing live investigations.** **Certification** in these various areas is often useful, especially when providing testimony as an expert witness in court. 
- It is important to **maintain reference materials that can be consulted when needed.** **For example :** manuals and other books dealing with software and hardware useful in troubleshooting and looking up for extra features/settings. 

- Other resources that should be maintained are **prepared documents (forms)** that may be used during an investigation. **For Example**
 - ❑ **Chain of Custody forms** may be used to keep track of *who had possession of evidence at any given time.*
 - ❑ **Property forms** may also be used to maintain information on *who is ultimately responsible for evidence that's stored in a secure location.*
 - ❑ **Contact lists** are also useful, providing a **listing of individuals with specific skills**. Such lists should also contain information on **how to contact certain legal departments or individuals incharge of abusing services at certain web sites or companies.**
For example, if a case involved a free e-mail account at a mail service provider, it would be useful to keep a request form that can be completed when requesting information on a particular account, and phone numbers to contact during the investigation.
- In many cases, these documents can be **stored on a computer or server or drives** that can be readily used for forensic examinations so that the **information is always handy** in an electronic format.
- It is also important to have a **computer forensic lab** set up prior to conducting an investigation. The lab should be of **adequate size**, and **should have a server/workstation, adequate hardware tools or media resources** (such as empty CDs,DVDs, disk drives,pendrives,) on which to store evidence files, with **storage locker facilities that allow computers to be locked** in a secure location when not being examined.

The forensic lab must have equipment that can be used in the facility or taken in the field locations where the crime has taken place. This would include such items as:



- **Laptop computer or workstation** The laptop/workstation should have forensic software installed on it, and should include additional hardware that may be used to acquire data.
- **Boot disk and CD or USB flash drive or tools such as Write Blockers** The **boot disk** is used to start a computer from a floppy disk or CD or USB so that files aren't modified when the computer starts. A CD or other medium containing various **utilities can also be useful to acquire data** from a machine. Make sure ,any tools that are included should not unknowingly modify data.
- **Digital camera** This can be used to **photograph what's displayed on a computer screen**, and to photograph the scene of the crime. Before taking the computer from the crime scene, the back of the computer should be photographed to show where cables were plugged into the machine so that it can be set up the same way.
- **Evidence and antistatic bags, tags, and stickers** **Evidence bags** are tamper proof bags in which items can be stored to prevent unauthorized handling or contamination by fingerprints, DNA, or other taint evidence. **Once sealed, the bag must be ripped open to access the contents**. To safely transport hard disks and any circuit boards, they should also be stored in **antistatic bags**. Tags and stickers can also be used to identify the contents of the bag, showing the incident number or other information that associates items with a particular criminal case or incident.
- **Pens, notepad, and masking tape** It is important to document the actions taken in removing peripherals attached to the computer prior to transporting it. You can use masking tape to mark which cables were attached to the suspect computer and where they were connected.

Obtaining Search Warrants : Before you collect evidence, you must make sure you have the right to either search or seize the evidence in question.

- A *search warrant* is a legal document that permits members of law enforcement to search a specific location for evidence related to a criminal investigation, and *seize that evidence* so that it may be analyzed and possibly used in court.
- For the warrant to be legal, it *must be signed by a judge or magistrate*, such as a justice of the peace or another type of judicial officer.
- A *valid reason needs to be given as to why a search warrant should be granted*. This requires law enforcement officials to provide a *sworn statement* in which the *location to be searched* is specified, and may list *the type of property being sought*.
- Documentation on the complaint that initiated an investigation, and other written information that validates the request needs to be attached along. The key point of this process is to *protect the rights of the individual*, and to provide *reasonable grounds for why permission should be given* to invade a person's privacy and property.
- Search warrants protect the privacy of their citizens by *requiring authorities to prove the necessity for the search* and seizure of a person's property. An *example* of legislation that is used to prevent unreasonable searches and seizures of property is :
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, or things to be seized."
- Here, *probable cause* is the primary basis for issuing a search warrant and is *a standard of proof that must be shown in which a cautious person* would find reasonable grounds for suspicion. *This assures that investigations aren't conducted in an authoritarian or oppressive manner*. Without probable cause, the request for a search warrant is denied.
- If the search warrant is issued, *its use is limited*. The warrant can be executed only within a set amount of time. If a search warrant isn't used in that time, a new one will need to be obtained.
- Also, an officer may *search only those areas that are outlined in the court order* and generally cannot seize items that aren't included in the applicant document.

Searching without Warrants

- **Warrants are not necessary in every situation where evidence could be obtained.** Requesting a search warrant to acquire every piece of evidence in every criminal and civil case would become an **administrative nightmare**, so exclusions to needing a warrant are provided in statutes (law made by government).
- For law enforcement, there are a number of exceptions to where a search warrant is needed, although few apply to computer forensics. **For example**, an officer can frisk a suspect, checking his or her clothes for weapons or contraband.
- In terms of computer forensics, a primary reason why a search warrant could be excluded is **when the evidence is in plain view, and an officer can see it from a reasonable vantage point**, it is often reasonable for the officer to seize the item immediately, rather than leave it and take the risk of it being hidden, altered, or destroyed.
- The need for a search warrant is also **excluded when consent is given by the owner, or by an authorized person** who is in charge of the area or item being searched.

For Example, if the victim of a cybercrime wanted to have his or her own computer searched for evidence, a search warrant wouldn't be necessary.

- Similarly, **the senior staff members of a company** or the manager of an IT department **could give permission** to have servers and workstations in a company examined. The key is **whether the person owns the property or has proper authorization**, which can sometimes be less than clear.

For example:

- ❑ On a college campus, a student in hostel might be able to give permission to search the room he or she occupies, but wouldn't be able to give permission to search his or her roommate's computer.

- Because **a search conducted on a computer without a warrant could make any evidence that's collected inadmissible in court**, it's vital to determine **who can give permission** before seizing or examining a computer.

Preparing for Searches

- Because search warrants aren't required in all situations, it is necessary to identify whether warrant is needed early in the investigation. In doing so, the following questions can be considered:
- **Does the company or complainant own the computer?** If so, permission can be given to search the machine.
- **Does the company have a legitimate reason for searching the computer?** If not, the employee using the computer could have reason for civil litigation.
- **Have employees been warned that the company has the right to search the machine?** By warning employees that computers may be searched at any time, the employee has little to no recourse if anything has been found on his or her machine.
- If there are no legal grounds to search the computer without a warrant, **statements and any documented evidence pertaining to the incident should be collected.**
- **Statements** should include as many details as possible, providing a timeline of when events took place and what occurred.
- Statements should be **gathered from anyone associated with the incident**, and this should be done before the memories of the event aren't diluted over time.
- Recorded statements will provide information that **can be used to obtain a search warrant**, and can be used as evidence later on if the case goes to trial.

Subpoena

- In the cases where you do not have voluntary consent to search or seize evidence, you'll have to ask for permission from a court. The first option using a court order is a subpoena.
- A common use of a subpoena is when the equipment owner is unwilling to surrender evidence.
- A subpoena compels the individual or organization that owns the computer equipment to surrender it.
- A subpoena is appropriate when it is unlikely that notifying the computer equipment owner will result in evidence being destroyed.

Professional Conduct

- At all times in an investigation, whether you are working as a member of the police force or as an employee of a company, you are acting as a technical representative of the organization, **it is important to maintain professional conduct.**
- The level of **ethical behavior** that's displayed will indicate how the case as a whole will be handled. This will also showing that the investigation will be handled with integrity.
- A balance of **morality and objectivity** **must be maintained throughout the investigation.** If potentially offensive materials are found on the computer, **showing interest in the material is unprofessional** and can be used to undermine the findings in court.
- Investigator should also **display objectivity**, and **not make judgments** on what is found during an examination of evidence, or when interviewing those involved in the investigation. Investigator should avoid making any kinds of jokes or comments about what is found, and **focus on the tasks involved in performing the investigation** with professionalism.
- In performing these tasks, it is important to remain detached from the incident. **Professional detachment** involves placing all of your attention on the work, rather than the emotional or psychological stress factors that may be involved.
- **Confidentiality** is another important component of professional conduct. Throughout the investigation, it is important to keep information about the case private, and **to not reveal information to those who aren't directly involved** in investigating the incident. **Crucial Information should not be shared with witnesses, coworkers, or others outside the case, especially if they show interest in what has occurred.**
- The investigator may also work with public relations or a media representative in the company or police to **determine what will be revealed to the public.** In such situations, **crime technicians and anyone else involved in the investigation should limit their comments to information** that has been approved for public release, and keep any additional facts to themselves.

Investigating Company Policy Violations

- Corporate investigations are different from other types of criminal investigations , as a crime might never have been committed even though an investigation is required..
- When criminal activity occurs on a home computer, generally the police are called to conduct an investigation.
- In companies where an IT staff is available, policies may exist that designate a person or team of people with specialized skills to initially respond to the incident.
- The incident response team may contact law enforcement eventually, but this will often depend on the type of incident and what is found in their initial investigation.
- Anyone who has worked for a company knows that Employers will impose certain rules and practices that must be followed by employees as conditions of their employment.
- A number of regulations may be implemented to address how computers and other equipment are to be used in the workplace, and breaking these rules could result in an investigation and in having computers and other devices used by the employee undergo a forensic examination.
- IT policies and procedures establish guidelines for the use of information technology within an organization. In other words, it outlines what everyone is expected to do while using company assets.

Policy and Procedure Development

- A **policy** is used to address concerns and identify risks to a company, whereas **procedures** are used to provide information on how to perform specific tasks and/or deal with a problem. **For example,**
 - A policy may **be created to deal with the potential threat of unauthorized access** to restricted areas, and procedures may be implemented that state how a visitor should be signed into a building and escorted to a particular department.
- Through the policy, an issue that is pertinent to the organization is explained and dealt with. Through the procedure, people are shown how to abide by policies by following specific instructions.
- An organization may have many different types of policies and procedures implemented. Regardless of the type, however, each should have the following features:
 - ❑ It **should be straightforward**, stating points clearly and understandably. If areas of a policy can be interpreted in different ways, it can be disputed when attempting to enforce it.
 - ❑ It **must define what actions should be taken**. policies must outline the actions that may be taken if the policy is violated and procedures must lay out the steps needed to complete a task.
 - ❑ It **cannot violate any applicable law**. If a policy does violate any existing legislation, it cannot be adequately enforced. In addition, the company may face civil or criminal charges, because it implemented a policy that forced employees to break the law.
 - ❑ It **must be enforceable**. If a policy isn't enforced each time it is violated, or if it can't be enforced for some reason (such as because it violates contractual agreements with individuals or unions), the policy becomes worthless to the company.

When implementing policies,

- Companies should also **devise methods** to **confirm that employees have read and agreed to comply with them**. There can be different methods for the same :
 1. To have employees **read and sign copies of certain policies when they are hired**. However, if there are changes to the policy, each person already hired must be approached, and must reread and sign the policy.
 2. The **policies can be posted on the corporate intranet**, enabling employees to read them at their convenience.
 3. **e-mail copies of policies to all of the employees'** internal e-mail addresses, and requesting them to respond stating they have read and agree with the terms of the policies.
- Policy can be of two types:
 1. **Acceptable Use Policy**
 2. **Incident Response Policy**

1. Acceptable Use Policy

- *A policy that employees should be required to acknowledge as having read and one with which they should comply* is an acceptable use policy.
- This type of policy **establishes guidelines on the appropriate use of resources/technology**. It is used to outline what types of **activities are permissible** when using a computer or network, and what an organization considers proper behavior.
- Acceptable use policies not only protect an organization from liability, but also provide employees with an understanding of what they can and cannot do using company resources.
- Acceptable use policies will **restrict certain actions**, including what types of Web sites or e-mail an employee is allowed to access on the Internet at work.
- Acceptable use policies would also **specify methods of how information can be distributed** to the public, to avoid sensitive information from being “leaked.”
- ***Imposing rules on the dissemination of information might include:***
 - ☐ Specifications that prohibit classified information from being transmitted via the Internet (for example, via e-mail or File Transfer Protocol [FTP])
 - ☐ Provisions on how content for the Web site is approved
 - ☐ Rules on printing confidential materials
 - ☐ Restrictions on who can create media releases, and so on.
- Through this, important information is protected, and employees have an understanding of what files they can or cannot e-mail, print, or distribute to other parties.

Some of the key available use policies applicable to IT departments:-

- **IT Asset Management Policies**

- These policies describe the guidelines to be practiced with regards to the IT assets in an organization. It should have specific protocols on what types of assets are admissible for specific tasks. You also need to have a BYOD (bring your own device) policy that describes whether employees are allowed to use their own devices to connect to an organization's network.

- **IT Software Management Policies**

- These policies help companies manage their software tools effectively. From specifying the list of authorized tools to software automation, you need to have comprehensive policies that outline the appropriate usage of the software. You also need to focus on patching policies to ensure all your software tools are updated at the right time.

- **IT Security Policies**

- IT security involves various aspects, including information security, password management, remote access and security training. You need strong policies for both risk prevention and damage mitigation. You also need to provide regular training to your employees to make sure security efforts are imparted in the right way.

- **IT Employment Policies**

- Specific policies should be drafted and implemented for people who work in IT. Most importantly, it should set clear expectations of what needs to be performed in their specific job roles. Good policies need to be established for regular training, responsibilities, access to critical information, performance and more. This helps you manage expectations from the everyday performance of your employees.

2. Incident Response Policy

- **Incident response policies** are implemented to provide an understanding of **how certain incidents are to be dealt with**.
- The policy **should identify an incident response team**, who is to be notified of issues, and who has the knowledge and skills to deal with them effectively.
- **Members of the team should be experienced in handling issues** relating to unauthorized access, denial or disruptions of service, viruses, unauthorized changes to systems or data, critical system failures, or attempts to breach the policies and/or security of an organization.
- If the incident is of a criminal nature, **the policy should specify at what point law enforcement should be contacted** to take control of the investigation.
- **A good incident response policy will outline who is responsible for specific tasks** when a crisis occurs. It will include such information as:
 - ☐ **Who will investigate or analyze incidents** to determine how an incident occurred and what problems are faced because of it.
 - ☐ **Which individuals or departments are to fix particular problems** and restore the system to a secure state.
 - ☐ **How certain incidents are to be handled**, and references to other documentation.

The policy should also provide steps on what users are supposed to do when identifying a possible threat.

- Upon realizing that some issue exists, an individual should notify his or her supervisor, a designated person, or a department that can then contact the incident response team.
- While awaiting the team's arrival, the scene of the incident should be vacated and any technologies involved should be left as they were.
- The users should also document what they observed when the incident occurred, and list anyone who was in the area when the incident occurred.
- To address how a company should handle intrusions and other incidents, it is important that the incident response policy includes a contingency plan.
- The contingency plan will address how the company will continue to function during the investigation, such as when critical servers are taken offline during forensic examinations.
- Backup equipment may be used to replace these servers or other devices so that employees can still perform their jobs and (in such cases as e-commerce sites) customers can still make purchases.
- By having such practices in place, any investigation can avoid (as much as possible) negatively impacting normal business practices.

Policy Violations

- When policies are violated, it doesn't necessarily mean that a full police investigation is required.
- In many situations, the violation may require disciplinary actions against the employee, whether it is a reprimand, fine, demotion, or termination.
- The severity of the actions will often depend on the past performance and current conduct of the person. Despite the end result, computer forensics may still be incorporated.
- Using forensic procedures to investigate the incident creates a tighter case against the employee, thereby making it difficult for the employee to argue the facts.
- In any investigation, it is important to treat the case as though it were going to court, as you never know what you'll find. For example, an employee may have violated a company's acceptable use policy by viewing questionable Web Sites during work hours. If it was found that the person was downloading obscene content/indulging in illegal betting/ running fraudulent scheme online etc, the internal investigation becomes a criminal one.
- Any actions taken in the investigation would be scrutinized, and anything found could be evidence in a criminal trial.
- Policy violations can also extend investigations beyond the machines owned by a company. Many people have their own blogs or personal Web sites, or social networks.
- On such sites, people can publish text and pictures to the Internet. If the person makes derogatory comments about coworkers or portrays the company in a negative manner, it may seem that little can be done. After all, the information isn't on a corporate computer, but on another server entirely.

- ❑ Today, institutions do realize that **cyberbullying** can escalate into more violent actions and thus do not tolerate the **hostile working environments**.
- *Hostile working environments* are workplaces where a person fears intimidation, harassment, physical threats, humiliation, or other experiences that create a non-workable atmosphere.
- One common example of a hostile working environment is sexual harassment. If a person had to view sexual images displayed on a computer, or received derogatory messages sent through e-mail, SMS or blatant sexual remarks, he or she could feel objectified and humiliated by the atmosphere.
- In such cases, internal disciplinary tribunals, criminal charges, or civil suits may be the only way to stop such actions. **When these activities are received, transmitted, or displayed using technologies issued by the company, it is simple to acquire evidence by looking at information stored on the devices or on hard disks.**
- ❑ Another most devastating types of policy violation is **Industrial Espionage**, which is also a criminal act.
- *Industrial espionage* is the selling of trade secrets, intellectual property, or other classified information to competitors.
- If the wrong person has access to such information, it could be detrimental to the organization, as releasing it to the public or competitors could undermine confidence in the organization, and even jeopardize its ability to remain solvent.
- *Source code of programs, secret recipes/scripts, and other critical information* that is often limited to the most trusted insiders could be devastating if released.
- Information must be kept secure, and any suspected leaks must be dealt swiftly and demand rigorous investigation for further prosecution.

Warning Banners

- *Warning banners* are brief messages that are used to inform users of policies and legislation regarding the use of a system and the information it contains.
- Warning banner advises a user about key elements of proper usage, and may even provide references to existing laws and policies; it serves as a legal notice to users of the system.
- They are generally displayed at the startup of programs and operating systems, or when accessing the default page of intranets and public Web sites.
- Warning banners can come in different formats, including splash screens or message boxes that pop up when software is started, or information appearing in graphics or other content on Web sites.
- It also informs the user that any activities on the site may be monitored. By using the Web site, the user agrees to these actions. Hence, anyone committing a criminal act has consented to having information gathered in logs, which could then be used against him or her as evidence.
- Warning banner essentially dissolves any excuse of a user not knowing that what he or she did was wrong. The user is given a warning, so any violations of it can be proven as being intentional.
- The message should provide the following points of information and the user may have read and agreed to as part of his or her employment:
 - ☐ A brief outline of what is considered proper usage of the system
 - ☐ Expectations of privacy, and that the system may be monitored for illegal or improper activity.
 - ☐ Any penalties or possible punishment that may result from noncompliance.
- Adding such messages when users log on to an operating system is relatively simple, and should be implemented on any computers that are part of a corporate network. **For Example:** Computers running Windows can have information added to the Registry that will cause a message box to appear with a warning before the user logs on.



The Investigation Process

- Although **investigations will often vary** in the type of incident or crime that has occurred, many **elements are common** in any investigation such as:
 - the evidence that's available
 - the environment in which evidence is collected
- Eventually, **any investigation will end up in court**, where the evidence and process in which it was collected may be challenged. Therefore, it is **important to always follow the standard procedures in the investigative process**.
- Once gone through the process of securing a crime scene and interviewing witnesses, the evidence is collected, preserved and transported.
- Later, each piece of evidence must then be assessed, with digital evidence acquired from hard disks and other media, before being examined.
- Throughout this process, documentation is essential, as any actions that are taken should be included in a statement and/or final report.
- This can be a lengthy process with **procedures that must be followed to prevent any evidence from becoming inadmissible**, or important pieces of evidence being overlooked altogether.

Conducting a Computer Forensic Investigation: Business Environment

- The process of conducting a computer forensic investigation can be a hectic experience, especially in a **business environment** where the systems are online to maintain the business.

For example



- if the company used an e-commerce site to make sales, **taking the whole system down to perform an examination could cost lot of money to the company.**
- During such instances, **while ensuring forensic procedures are followed, no time should be wasted wondering which steps should be performed next.**
- To perform an investigation properly, it is important that Set of Procedures (SoPs) are followed that detail the steps to be taken.
- In the investigation process , the following six steps need to be taken:
 1. Preparation
 2. Detection
 3. Containment
 4. Eradication
 5. Recovery
 6. Follow-up

1. Preparation

- Preparation is the **key to handling and investigating incidents**.
- It is important to take a **proactive approach** towards threats by putting safeguard measures(Resilience) in place before problems occur.
- Preparation **requires that logging is activated on systems**. Logging information to a file is provided for operating systems, and for certain software and equipment.
- Logs provide a great deal of information, **revealing indicators** that may show whether an incident has occurred which can be further used as evidence that can be testified in the court.
- An incident response team can waste valuable time trying to get organized, if the **necessary policies, procedures, and tools** are unavailable when responding to an incident.
- It is important that **people are properly trained in how to identify and report problems**, and that they have a **thorough understanding of the tasks** they're expected to perform.
- In addition, companies should **develop communication plans** that provides contact information on who will need to be called in case of emergency or when problems are first reported. Such information should be left with a centralized source.
- **Passwords are another piece of information that should be available in emergencies**. Members of the IT staff or the incident response team may have varying levels of security, and may be unable to get into certain areas of the network or certain systems.
For example:
 - Not having passwords to access administrative functions in certain systems, or workstations and servers may limit the detection of crime.
- For utilization under emergency, copies of passwords should be written down, sealed in an envelope, and stored in a locked container (such as a safe).

- Also, a company will need to do business after an incident has occurred, but in some incidents data may be altered, corrupted, or deleted. When this happens, the data may be irrevocably lost, unless **backups have been regularly performed** beforehand.
- By performing regular backups, you can restore the data on a server or workstation as needed. This is especially important if a particular machine is seized as evidence **or data prior to the investigation date needs to be reviewed.**
- To make it easier for members of the team to restore the data, **recovery procedures should be tested and documented thoroughly**, allowing members to follow the understandable steps to restore systems to their previous state.
- **Develop Threat intelligence capabilities.** This will help an organization understand the kinds of threats it should be prepared to respond to.

2. Detection

- Determining whether an **incident has actually occurred** is the next step of the incident investigation process.
- **For Example:**
 - **Every reporting is not a crime.** A user could report that files have been deleted, and although it could be indicative of hacking, it could just mean the user is too embarrassed to admit he or she deleted them by accident. The detection phase of incident investigation examines such reports, and determines what further actions (if any) are required.
- **Detection requires**
 - looking at the existing safeguards and auditing controls
 - determining whether anomalies exist?
- **System logs** may show errors related to **security violations**, **hardware failure**, or other potential problems. **Firewall logs** should also be analyzed to identify **indications of attempted hacking** from the Internet, policy breaches, or other damaging events.
- **Event Log analysis** can **help an investigator draw a timeline based on the logging information** and the discovered artifacts. 
- Members of the IT staff or information security personnel should **check logs on a regular basis**, and determine whether **indications of problems have been recorded**.
- Software's specifically designed to deal with certain incidents, or elements of an incident, can be used in the detection process.
- **AV software packages** can be used to detect viruses, malwares, unauthorized connections, and can be configured to automatically deal with them upon detection. 
- **Intrusion detection systems** can also be used to identify whether system security has been violated, systems have been misused, or accounts have been used or modified. For Example : SNORT IDS

- In addition to the logs created by systems on the network, the IT staff should also keep a **manual logbook**. This should include **record of dates, times, observations, the name of the person** who reported the incident and **the names of people who had access to systems** should also be recorded.
- Another reason for maintaining a logs is that it can **reveal patterns**. It may make several attempts to hack into a network or assessing into a secured area, and being able to reference information on these previous occurrences can be valuable in identifying vulnerabilities, finding who is making these attempts, and can be used in the prosecution of that person.
- Logs are also useful in identifying **training issues**, such as when multiple mistakes by the same person result in damaged data, invalid data entry, or erroneous reporting of incidents.
- **When an incident is confirmed**, then it is **important that an image of the affected system is made as soon as possible**. Even opening a file can alter information (such as the date/time of when it was last opened), and can negatively affect any further investigation or future prosecution.
- There can be more than one incidents. It is important that **Incident should be prioritized**. Score incidents on the impact it will have on the business functionality, the confidentiality of affected information, and the recoverability of the incident.

3. Containment

- It is important to **limit the extent and significance of an incident** so that it doesn't spread to other systems and continue doing damage. Allowing viruses/worms to spread across the network increases the level of damage. **Containment limits the scope of such incidents**, preventing the damage from spreading.
- **How an incident is contained** will depend on
 - **type of incident that has occurred**,
 - **what is affected**, and
 - **importance of systems to the business**.
- If someone had hacked into a network file server, it might be prudent to remove that server from the network, such as by unplugging the network cable from the adapter.
- In doing so, the hacker would be unable to do further harm, and would be unable to modify or delete any evidence he or she left behind.
- In other situations, such as an employee sending threatening e-mails, it would not be justified to prevent everyone from using network resources.
- In this case person may be detained, having a member of the incident response team stay with that person until the Law enforcement arrive, so as to prevent them from using a computer, would probably suffice.

4. Eradication

- Just as it's important to prevent further damage by containing an incident, **it is equally important to remove its cause.**
- Eradication **removes the source of a threat** so that further damage isn't caused or repeated.
- In doing so, the system is left more secure, and further incidents may be prevented.
- Eradication may occur through a variety of methods. **For example,**
 - If a virus is detected on systems, eradication would require removing the virus from all media and systems. For example using a Anti Virus software.
 - In situations involving violations of law or policy, the eradication phase of incident investigation might require disciplinary action (such as terminating the employee) or pressing criminal charges.
- Therefore, the appropriate method of eradicating an incident depends on what or who is being dealt with.

5. Recovery

- Recovery is important because data may be modified, deleted, or corrupted during incidents, and configurations of systems may be changed.
- Once an incident has been handled, the company's IT staff will need to ensure that any data, software, and other systems are restored back to normal or to a state previous to the incident.
- Other problems that may result include malicious code that was planted on systems. Such code may be triggered by certain events, or may activate at a later date when everything is presumed to be fine.
- Because of the possibility of future threats, it is important to determine whether any remnants of an attack exist, and quantify what may have been damaged by the incident.
- Systems may be restored in a variety of ways:
 - The system may need to be completely restored from backups or to factory settings.
 - Systems may need to be reconfigured to the way they were before the incident (snapshot of the system) , data may need to be validated to verify that it is correct.

6. Follow-up

- The follow-up to an incident investigation is done **where it is determined that improvements can be made to incident handling procedures.**
- The **previous phases of the investigation are reviewed: what was done and why.**
- The follow-up requires an analysis of following details:
 - ☐ Preparation for the investigation, and **whether additional preparation is needed.**
 - ☐ Steps taken during the investigation, and problems identified , determining **whether the incident was detected quickly and accurately.**
 - ☐ **Whether the incident was adequately contained** or it spread to different systems.
 - ☐ **Whether communication was effective**, or if information was not conveyed in a timely fashion.
 - ☐ Evaluating tools used in the investigation and **whether new tools would result in Improvements.**
- It is also **important for companies to identify how much the incident cost**, so changes to budgets can be made to effectively manage the risks associated with certain incidents.
- This includes the *cost of downtime, personnel costs, the value of data that was lost, hardware that was damaged, and other costs related to the investigation.*
- By determining the financial costs associated with an incident, **insurance claims can then be filed** to reimburse the company and cost/benefit analyses can be updated.

Process of Digital Evidence

- The **Crime Scene Technician is responsible for processing digital evidence** that is collected by him/ her during an investigation.
- The process of digital evidence goes through a four-part set of procedures consisting of :
 - A. Assessment
 - B. Acquisition
 - C. Examination
 - D. Documentation

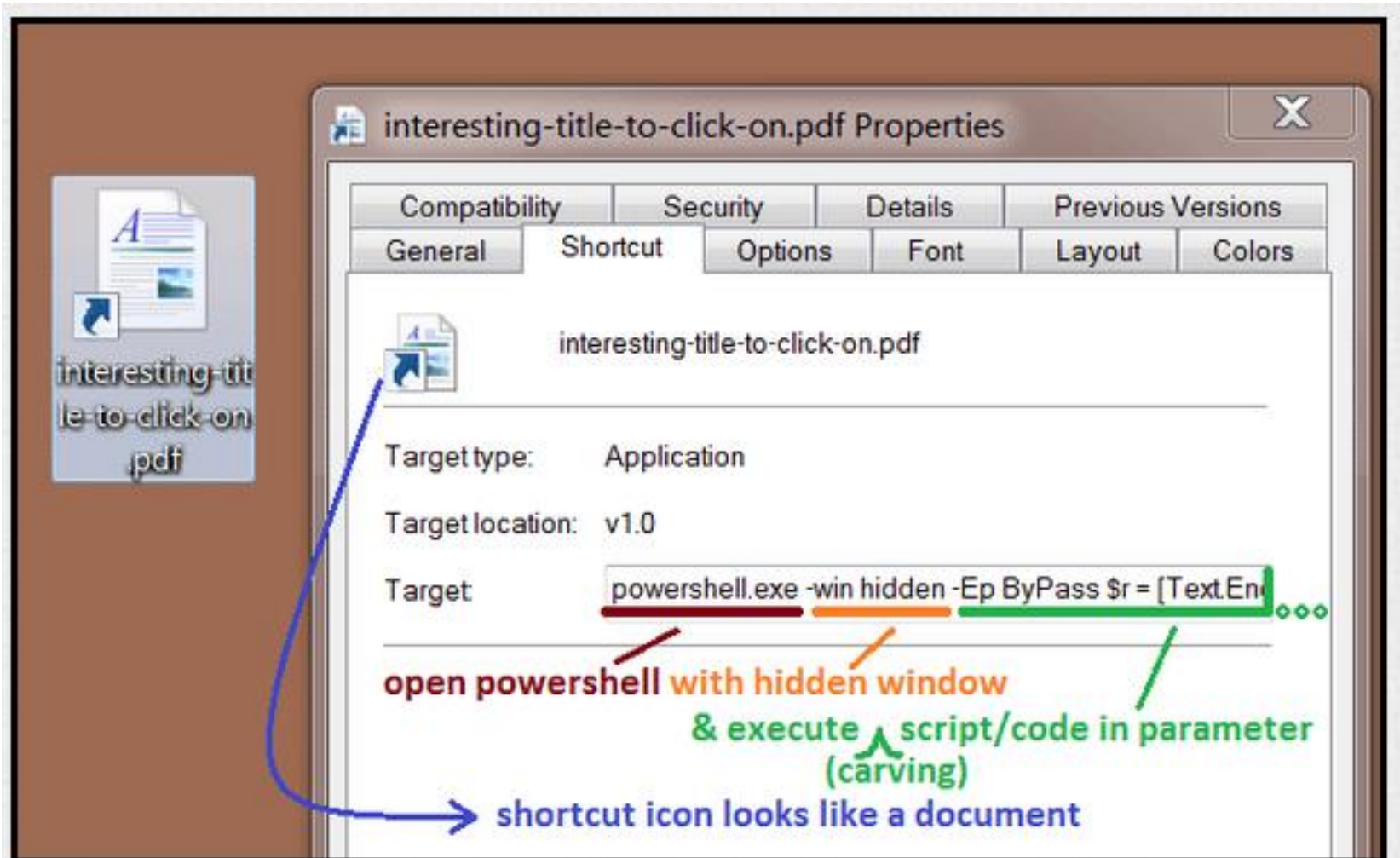
A. Assessing Evidence

- **Evidence assessment** is the first part of this process, and it involves evaluating issues related to the case and the digital evidence that's being sought.
- It requires reviewing the search warrant or details of legal authorization to obtain the evidence, the details of the case, hardware and software that may be involved, and the evidence you hope to acquire for later evaluation.
- After completing these steps, you should be able to determine the best course of action to take in obtaining the evidence, based on the scope of the case.
- **Case Assessment**
 - When an incident occurs that requires a computer forensic investigation, the investigator for the case will request the services of the crime scene technician.
 - It is important that the technician reviews the request and identifies the legal authority for his for her involvement in the investigation.
 - This request for assistance should be in writing, and include information such as:
 - Who is making the request for service, designation and contact information to call or e-mail this person
 - The incident or case number
 - Any available information regarding the suspect
 - Who owns the machine
 - Whether the data has been already viewed or analyzed by anyone prior to your examination.
 - What kind(s) of forensic services are being requested and time frame within which to report findings.

- A request for service form that allows an investigator to provide this information is useful for several reasons:
 - ❑ First, it provides an easy reference that connects evidence to a particular case.
 - ❑ The form will provide information on whether a search warrant is required (based on who owns the computer), and can be useful in identifying information to search for.
 - ❑ Also, if the request for services are illegitimate i.e. the request is made for personal reasons, you at least have an official form that will protect you from disciplinary actions.
- Because the computer may have been accessed prior to your acquiring the data and examining it, you should also request the complete chain of evidence documentation.
- If there are any questions regarding data, you can then contact any parties who previously had custody of the machine to determine whether they accessed any files or performed any actions with the machine.
- Before getting involved, It is important to discuss what you can and cannot do in an investigation, and what may or may not be discovered.

- **In addition, IT professionals /technicians should discuss:**
 - ❑ **Is there a need for the use of other types of forensics?** Has the evidence been checked for fingerprints, DNA, trace evidence, or other forensic evidence? **Waiting before touching the computer is better until other evidence has been collected.**
 - ❑ **Has an attempt been made to acquire evidence from non-computer sources?** Because evidence is so often found on computers, it is possible that other sources of evidence have been overlooked.
For example:
 - digital cameras and cell phones that take pictures can be useful in child pornography cases, whereas checking paper documents, printing devices, and other items may be useful in financial crimes.
 - ❑ **Is there a need to acquire evidence from other systems?** In cases involving the Internet, **it is desirable to obtain logs and account information** from Internet service providers (ISPs), who may have logged when the person connected to the Internet, **what sites he or she visited, e-mails that were sent and received, remote storage locations,** and other information.
- You should also **discuss specific details of the case that can be used to narrow your search for information on a computer.** **Beforehand information will waste less time when examining the computer.**
- If it is known why a person is being investigated, and the type of evidence the investigator is searching for, it can decrease the amount of time required in finding that evidence. **For example :**
 - **Banking fraud cases** will often involve searching for spreadsheets and financial records, child pornography cases will require looking for photographs/videos, and hacking cases will often require looking at system files, logs, source code and specific applications installed.
- **Information about the suspect should also be available to you,** such as the suspect's name, e-mail address, aliases, and user account information. **It will be useful to determine the person's computer skills.** Different suspects will have varying levels of expertise with computers, with more advanced users possibly incorporating encryption or **booby traps** or **kill switches**(foreg: usbskill).
- A **booby-trap** is usually a hostile piece of computer code that wipes out files or damage files that can be used as evidence.
- **usbskill** is an anti-forensic kill-switch that waits for a change on your USB ports and then immediately shuts down your computer Demo: <https://www.youtube.com/watch?v=3hbuhFwFsDU>

Example

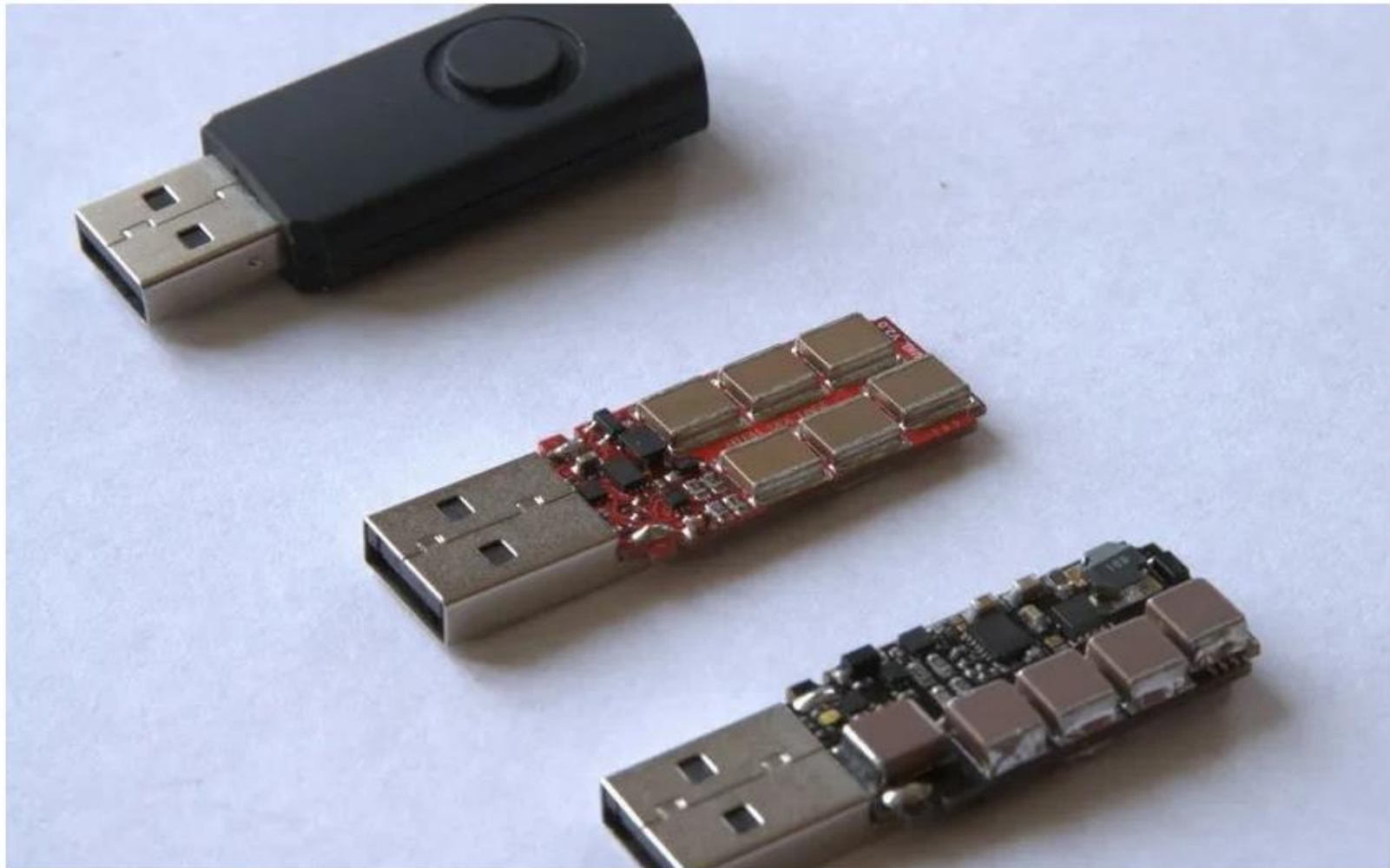


Booby trapped shortcut looks like an innocent document until its properties are inspected.

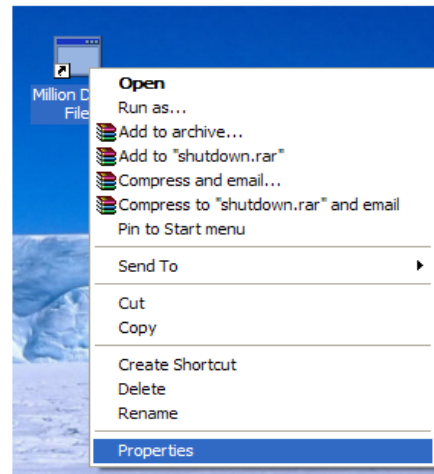
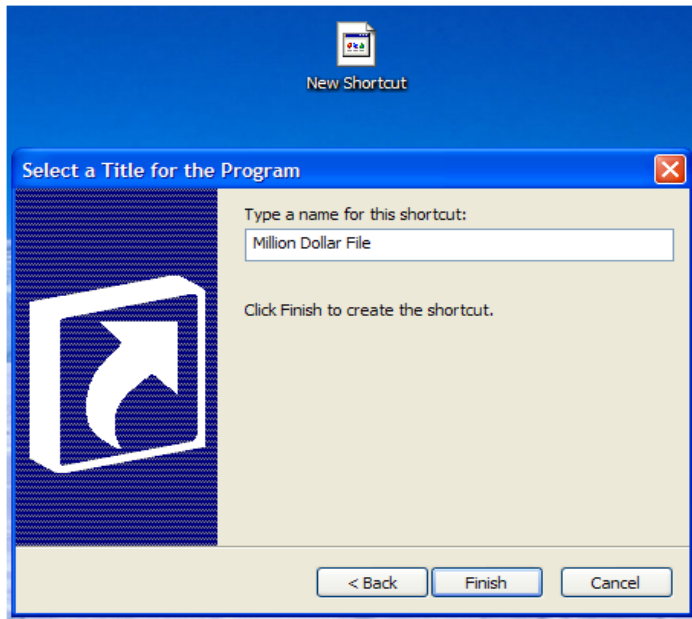
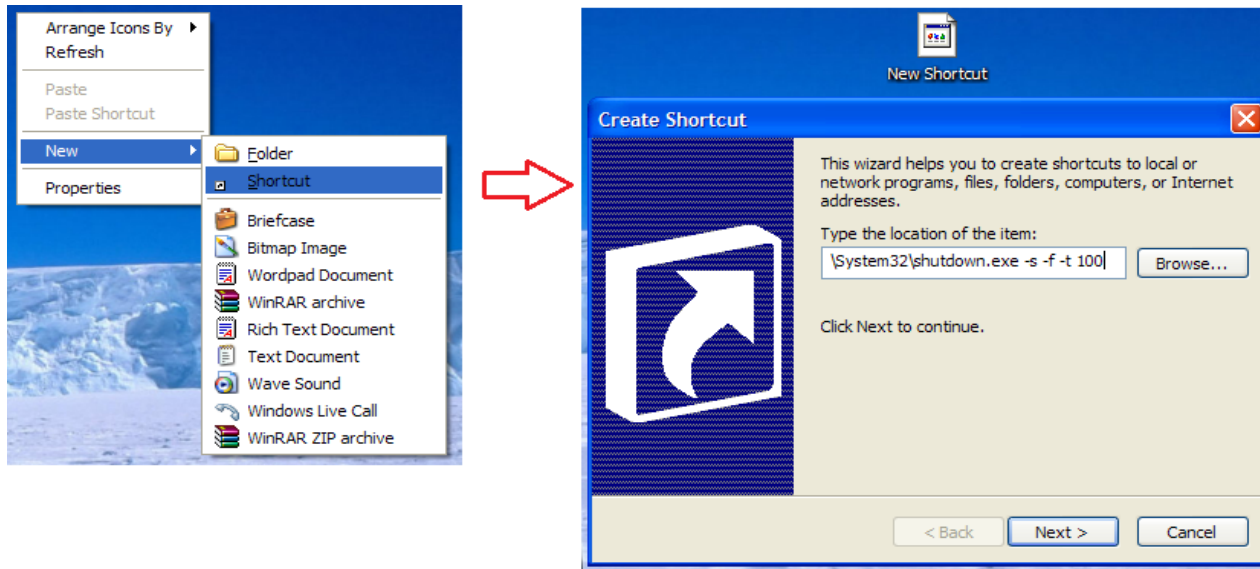
Booby-trapped USB stick fries your computer hardware

Plugging in the USB stick unleashes a negative 220-volt surge

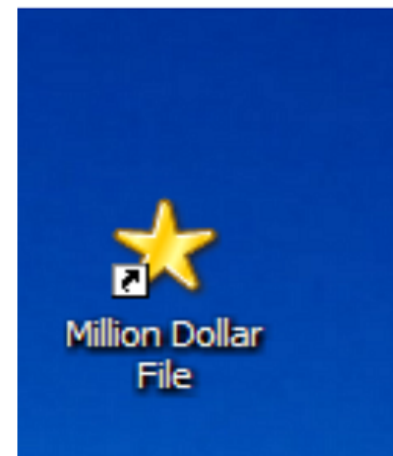
Fancifully dubbed the “USB Killer version 2.0,” the device uses a DC-to-DC converter to charge hidden capacitors (from the USB port that it’s attached to) and then re-directs that power into the computer, causing the process to loop indefinitely until the circuitry fails.



Example: A Trap to shutdown PC



Wait for Someone to Take the Bait!



Processing Location

- By understanding the location in which an investigation will take place, you can better prepare for factors that will impact your ability to collect and examine evidence.
- In many cases,
 - The evidence will be examined in a forensic lab, where you'll be working with equipment in your own work area.
 - Or, a scene of the crime is visited. Sometimes this will be an easily controlled environment, such as a server room that limits the number of people who can enter and have access to evidence.
 - Other situations may require you to collect evidence from a kiosk, a computer in a public Internet café, or the scene of a homicide where you need to wait for other forensic professionals to gather evidence like fingerprints, blood samples etc.
 - By understanding where the evidence needs to be gathered, you'll be better prepared to determine the type of equipment you'll need to bring, or whether other personnel (such as police officers) will need to be present.
- When assessing the location, a number of factors needs to be considered. It may take considerably longer to collect evidence from some scenes compared to others, so an estimate should be provided to the investigator.
- If it will take a while to collect the evidence, you should try to determine how your presence will impact the business.
- In some situations, it is better to remove a hard disk from a server, and to allow members of the company's IT staff to restore systems. However, even in the best of circumstances, a computer may be unavailable for some time, requiring personnel at the company to use other systems.
- Equipment and training may also be an issue in certain circumstances. For example: In a homicide scene, you may be exposed to blood patters or other biological matter. In such cases, you may need to work in a suit that will protect you from biological hazards, or at the very least wear a mask and latex or vinyl gloves.
- The same could also apply if a computer is located in a scene like chemical laboratory with chemicals or allergens present.


Evidence Assessment

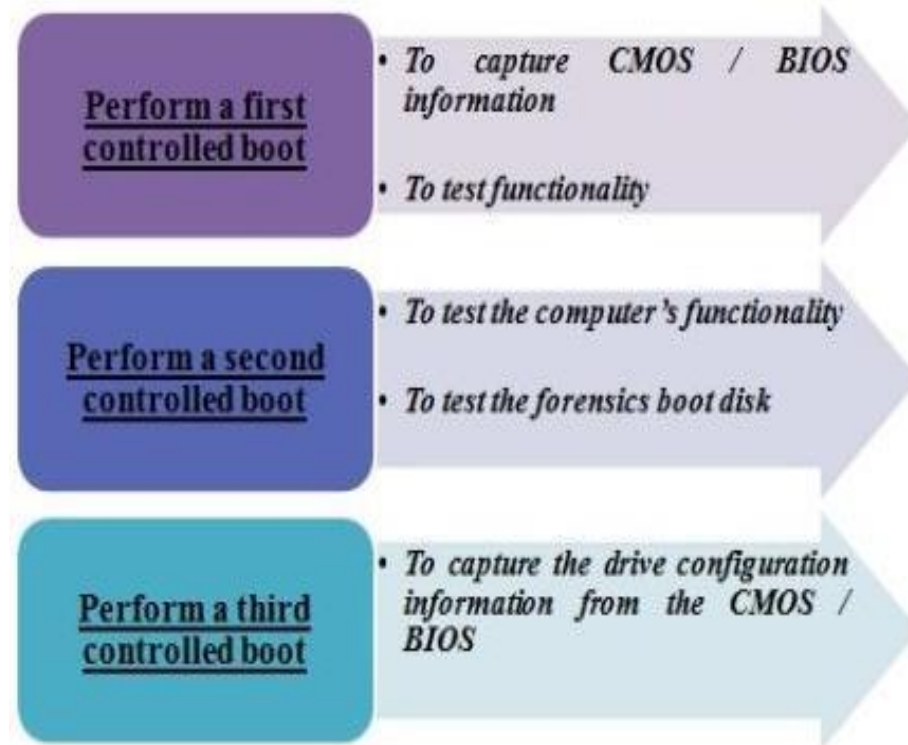
- The final step in evidence assessment specifically deals with the evidence itself.
- You should **collect the most volatile evidence first before moving to nonvolatile evidence**.
- In doing so, you **should prioritize the collection of evidence** so that the evidence that is most likely to contain what you're searching for is examined first.
For example, you would obviously want to acquire evidence from the laptop and examine it first, before moving on to any CDs, DVDs, and other media that may also have been collected.
- Throughout this process, **you should document any actions taken**, and determine the best methods of relating that information i.e. by **taking notes, making diagrams, photographing items**, or **utilizing features available through forensic software**.
- When evidence needs to be transported, you **should evaluate the condition and vulnerability of the items**.
- Certain devices such as tablets, cell phones, and laptops **could simply be packaged in an evidence bag**, whereas circuit boards and individual hard disks **must first be stored in antistatic bags**.
- In some cases, an investigator **may also need power banks to provide continuous electric power to battery-operated devices** such as laptops, mobiles, tablets etc. that are low in power so that any volatile evidence isn't lost before it is delivered to you.
- Identify **the secure location** that is free of electromagnetic interference where the evidence will be stored /transported after acquisition process.

B. Acquiring Evidence

- The second phase of processing evidence is acquisition.
- **Acquiring evidence** is the *process of obtaining digital evidence from its original source*.
- It is vital that the **original data isn't altered, damaged, or destroyed when making a copy** from which the forensic technician can work.
- **The first step** in acquiring evidence from a computer **is to document as much information about the machine as possible**. This is especially important when there is a backlog of cases, and the computer may have been stored until the examiner had time to work on the machine.
- **In documenting information**, you should **review information on any hardware and software configurations that were noted when the machine was seized**, in case this needs to be duplicated on the examiner's machine.
- **If dealing with a hard disk that has already been removed from a computer, the tasks in acquiring evidence are easier**. Simply attach the hard disk to the examiner's workstation in a forensic lab, or to a write protection device such as FastBloc (used with EnCase software), and then use forensic software to acquire its contents.
- However, generally entire computer or laptop are seized and not with individual components.

- Further, **disassembling the computer case will provide physical access to these devices**, so you should ensure that you have taken precautions against static discharge and that you do not have the equipment close to any strong magnetic fields. During the disassembly you should wear an antistatic wristband or stand on an antistatic mat.
- Once the case has been opened, you can **identify what hard disks and other components (for example, PC Card, network card, and so on) are installed**, and you can begin to take steps to remove the storage devices.
- Before removing any storage devices, **you should note down how they are installed and configured so that they can later be reinstalled exactly as they were before** (Taking photographs of the opened case is advisable).
- Once done, then remove the power connector or data cable from the back of the drive or motherboard. Doing so will prevent the destruction, damage, or modification of any data on the storage device in steps that follow.
- After disconnecting the storage device, **you should make a note of the make, model, size, jumper settings, location, drive interface, and any other information you can see that will identify the hard disk and its settings**.
- Once you've removed the power connector or data cable from the hard disk, **you can then take steps to retrieve information stored on the computer through a series of controlled boots**.
- To perform a controlled boot and **capture data stored in the CMOS/BIOS**, you would start the computer and press the particular key (such as the Del or F10 or F11 key or any other specific key) on the keyboard that allows you to access the BIOS Setup for that particular machine.
- Once you've entered the BIOS Setup, you can view the configuration information for that machine. You should **note the date and time of the system**, whether **power on passwords** has been set up, and **the boot sequence of the machine**.
- If the boot order of the machine is not configured to **first try and boot from a floppy disk or the CD-ROM or forensic boot USB stick**, you may need to change this.
- However, **before modifying these settings, document what the original settings were, and what changes have been done afterward**.

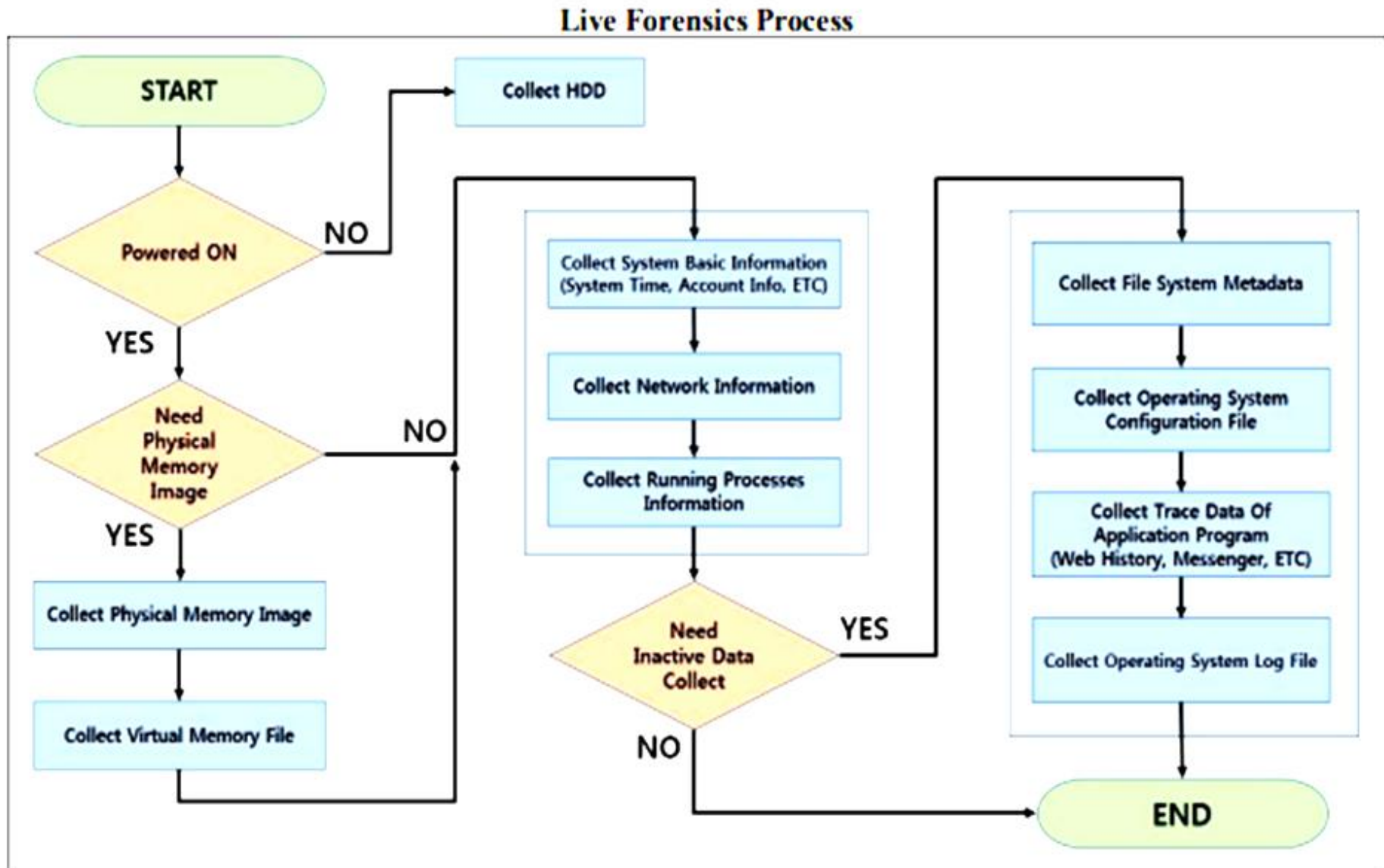
- After ensuring that the system is configured to first boot from a CD/DVD-ROM, **then test your forensic boot disk to make sure the computer will boot from that CD drive/floppy properly.**
- With the data cable still removed from the storage devices(HDD), you would insert the boot disk, and then boot the computer. **If it boots from the floppy or CD-ROM, shutdown the computer and then reconnect the storage devices to prepare for a third boot.**
- When the computer boots this time, **document the drive configuration information**,  including the logical block addressing (LBA), Cylinders, Heads, and Sectors (CHS), and whether the computer is configured to auto-detect any hard disks that are installed. **Once this is documented, power the system down.**
- If possible, it is **best to physically remove the hard disk from the computer** that's been seized and connect it to a forensic workstation in a forensic lab, or to a device such as FastBloc(write blocker) that prevents disk writes and works between the examiner's computer and the hard disk.
- If hard disk is attached to the machine that will perform the acquisition, **then information acquired earlier from the CMOS/BIOS is used to properly configure the storage device so that it will be recognized.**
- In some situations, it may be easier or possible to read the hard disk only by leaving it installed on the suspect's machine.
For Example:
Removing the disk from the laptop may be difficult, and reading the disk may not be possible if the appropriate adapter to connect the drive to a ribbon cable is unavailable.



Evidence collection from switched off computer

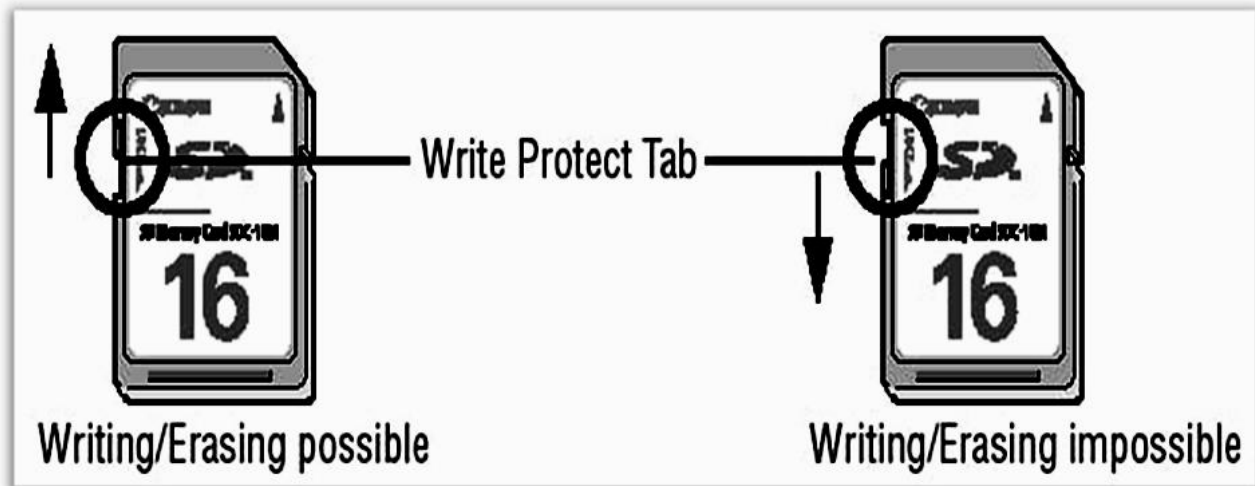
- Secure the scene of crime and disable all the modems, network connections etc. Unplug the power and all other devices from sockets. Never switch on the computer, in any circumstances. Allow printers to finish printing, pending if any.
- Confirm that the computer is switched off. As sometimes the screen may mislead, that should be done from the hard drive and monitor activity lights. Some laptops switch on, only by opening the lid. So, remove the battery if required.
- Label and photograph (or video) all the components in-situ. Label the in & out port cables so as if required, the computer could be reconstructed in future.
- Open the side casing of CPU/Laptop carefully and detach the hard disk from the mother board by disconnecting the data transfer cable and power cable.
- Take out the Hard disk carefully and record the identifiers(like- make, model, serial number etc.). Take signature of the accused & witnesses with date & time on the Hard disk, by a permanent marker. All other items/documents should also be signed and pasted with exhibit labels.
- Ask the user for the passwords, operating system, application package running on the suspected system, details of the other users and the off –site data storage, if any.
- After the Hard disk is removed, switch on the system and go to BIOS. Note down the date and time shown in BIOS. Prepare detail notes of “when, where, what, why & who” and overall actions taken in connection with the computer system.
- The suspected hard drive should be connected to the investigator computer only through a ‘write-block device’ for forensic preview/copy.

Evidence collection from a running computer



- Check for Extra equipment requirements, such as when the disk is used for network storage and a network equipment is needed to access the data, or when other equipment (such as the adapters mentioned previously) are not available to the technician performing the examination.
- Redundant Array of Inexpensive Disks (RAID) technology may need to be left in an array itself, as attempting to acquire data from such disks individually may not provide results that are usable.
- Legacy equipment. In some cases, older drives may not work with newer systems, making it impossible to read the data.
- Once the facts about the disk have been recorded, you can begin to acquire the data using methods that won't modify data on the disk, such as by using disk imaging software to duplicate the data.
- Write protection is an important part of acquiring data, as it will prevent any data from being written to the suspect hard disk.
- If hardware-based write protection is used, it should be installed prior to starting the computer, whereas software-based write protection should be activated immediately after booting the system with the examiner's operating system or boot disk.
- You should attempt to capture and document any electronic identifiers the disk might have, such as its electronic serial number.

Examine the USB flash drive or memory card for a switch like below. If available, you can move the switch to the locked or unlocked position to enable or disable write protection for the device.



Enable or Disable Write Access to Removable Disks in Local Group Policy Editor

→ Computer Configuration\Administrative Templates\System\Removable Storage Access

Local Group Policy Editor

TenForums.com

File Action View Help

1

Remote Assistance

Remote Procedure Call

Removable Storage Access

Scripts

Server Manager

Service Control Manager Settings

Shutdown

Shutdown Options

Storage Health

Storage Sense

System Restore

Troubleshooting and Diagnostics

Trusted Platform Module Services

User Profiles

Windows File Protection

Windows Time Service

Windows Components

All Settings

User Configuration

Software Settings

Windows Settings

Administrative Templates

2

Setting

State

Comment

Set time (in seconds) to force reboot

Not configured

No

CD and DVD: Deny execute access

Not configured

No

CD and DVD: Deny read access

Not configured

No

CD and DVD: Deny write access

Not configured

No

Custom Classes: Deny read access

Not configured

No

Custom Classes: Deny write access

Not configured

No

Floppy Drives: Deny execute access

Not configured

No

Floppy Drives: Deny read access

Not configured

No

Floppy Drives: Deny write access

Not configured

No

Removable Disks: Deny execute access

Not configured

No

Removable Disks: Deny read access

Not configured

No

Removable Disks: Deny write access

Not configured

No

All Removable Storage classes: Deny all access

Not configured

No

All Removable Storage: Allow direct access in remote sessions

Not configured

No

Tape Drives: Deny execute access

Not configured

No

Tape Drives: Deny read access

Not configured

No

Tape Drives: Deny write access

Not configured

No

WPD Devices: Deny read access

Not configured

No

WPD Devices: Deny write access

Not configured

No

Extended

Standard

19 setting(s)

Enable or Disable Write Protection for Disk using Diskpart Command

```
Administrator: Command Prompt - diskpart
Microsoft Windows [Version 6.4.9879]
(c) 2014 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 6.4.9879

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: WIN-F8GQFUPLIAR

DISKPART> list disk

   Disk ###  Status              Size               Free              Dyn  Gpt
   -----  -
   Disk 0      Online              238 GB             2048 KB            *
   Disk 1      Online             3919 MB              0 B

DISKPART> select disk 1

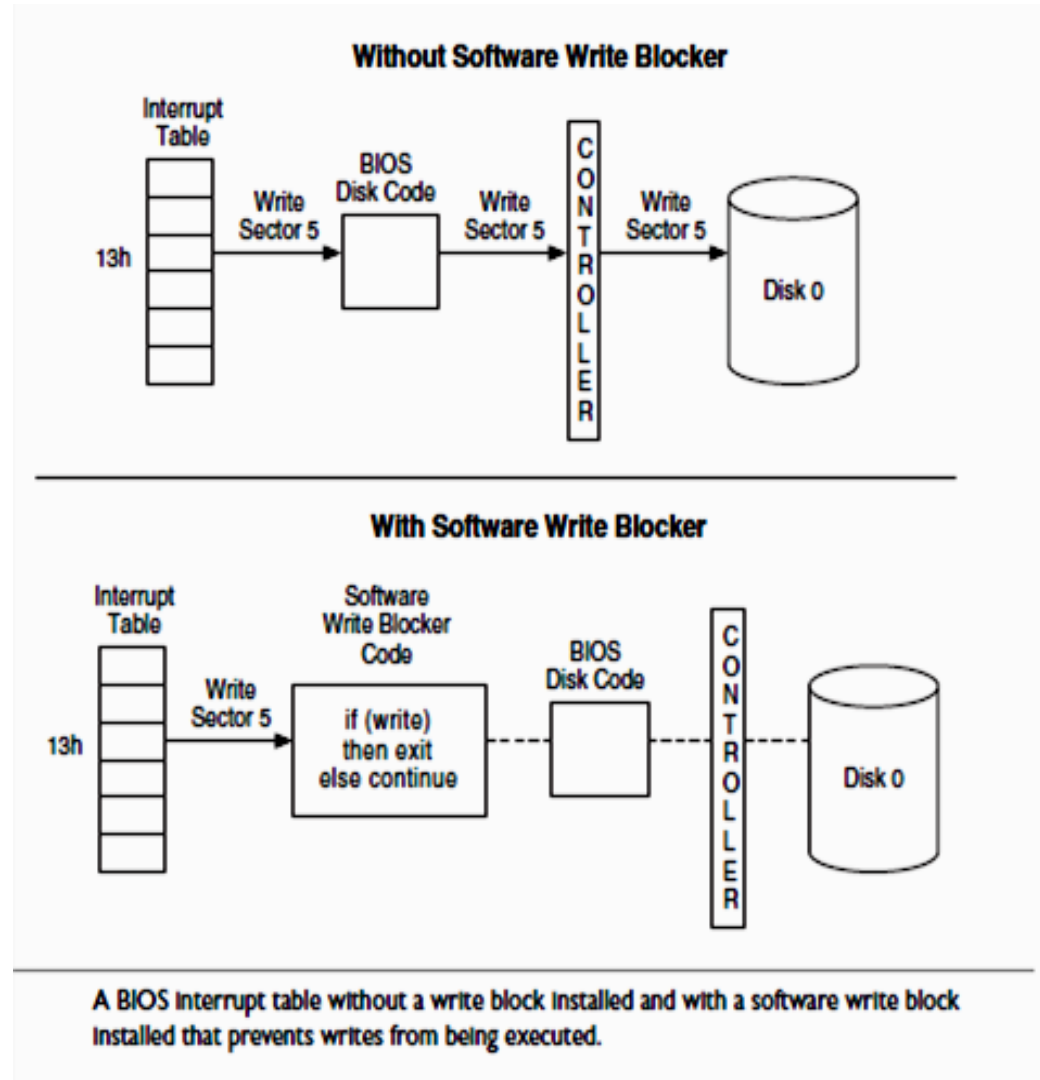
Disk 1 is now the selected disk.

DISKPART> attributes disk set readonly ←
Disk attributes set successfully.

DISKPART> _
```

Software Write Blockers

- The software write blockers **work by modifying the interrupt table**, which is used to locate the code for a given BIOS service.
- The interrupt table has an entry for every service that the BIOS provides, and each entry contains the address where the service code can be found.
- **For example**, the entry for **INT13h** will **point to the code that will write or read data to or from the disk**.
- A software write blocker modifies the interrupt table so that **the table entry for interrupt 0x13 contains the address of the write blocker code instead of the BIOS code**.
- When the operating system calls INT13h, the write blocker code is executed and examines which function is being requested.



Disk Imaging

- **Disk imaging** is a standard practice in computer forensics to preserve the integrity of the original evidence. *Disk imaging refers to the process of making an exact copy of a disk.*
- Disk imaging **differs from creating a standard backup** of a disk (for fault-tolerance purposes) in that **ambient data** is not copied to a backup; only active files are copied.
- Because a backup created with popular backup programs such as the Windows built-in backup utility is not an exact duplicate (in other words, a physical bitstream image), **these programs should not be used for disk imaging.**
- Some Programs such as Norton Ghost include switches that allow you to make a bitstream copy.
- But these programs were not originally designed for forensic use and do not include the features and analysis tools that are included with stand-alone imaging systems designed especially for forensic examination.

Bitstream Copies

- The first step is to immediately make a complete bitstream image of the media on which the evidence is stored.
- A **bitstream image** is a copy that records every data bit that was recorded to the original storage device, including all hidden files, temp files, corrupted files, file fragments, and erased files that have not yet been overwritten.
- Here, **every binary digit is duplicated exactly onto the copy media.** Bitstream copies (sometimes called *bitstream backups*) use CRC / hash computations to validate that the copy is the same as the original source data.
- **In some cases**, evidence could be limited to a few data files that can be copied individually rather than creating a copy of the entire disk.

- *Disk imaging differs from just copying all the files on a disk in that the disk structure and relative location of data on the disk are preserved.*
- When you copy all the data on a disk to another disk, that data will usually be stored on the new disk in contiguous clusters as there is room to store it.
- That way, all the data on the two disks will be identical, but the way that the data is distributed on the disks will not.
- So when a disk image (a bitstream copy) is created, each physical sector of the disk is copied so that the data is distributed in the same way.
- Then, the image is compressed into a file called an *image file*. *This image is exactly like the original, both physically and logically.*
- **There are a number of different ways to create a bit-level duplicate of a disk, including:**
 - ☐ **Removing the hard disk** from the suspect computer and attaching it to another computer (preferably a forensic workstation) to make the copy.
 - ☐ **Attaching another hard disk** to the suspect computer and making the copy
 - ☐ **Using a stand-alone imaging** device such as the DIBS Rapid Action Imaging Device
 - ☐ **Using a network connection** (Ethernet connection, crossover cable, null modem cable, USB, or the like) to transfer the contents of the disk to another computer or forensic workstation.
- Selection of methods depend on the equipment that is currently available. A portable forensic workstation or stand-alone imaging device is probably the best solution, but it's also the most expensive.

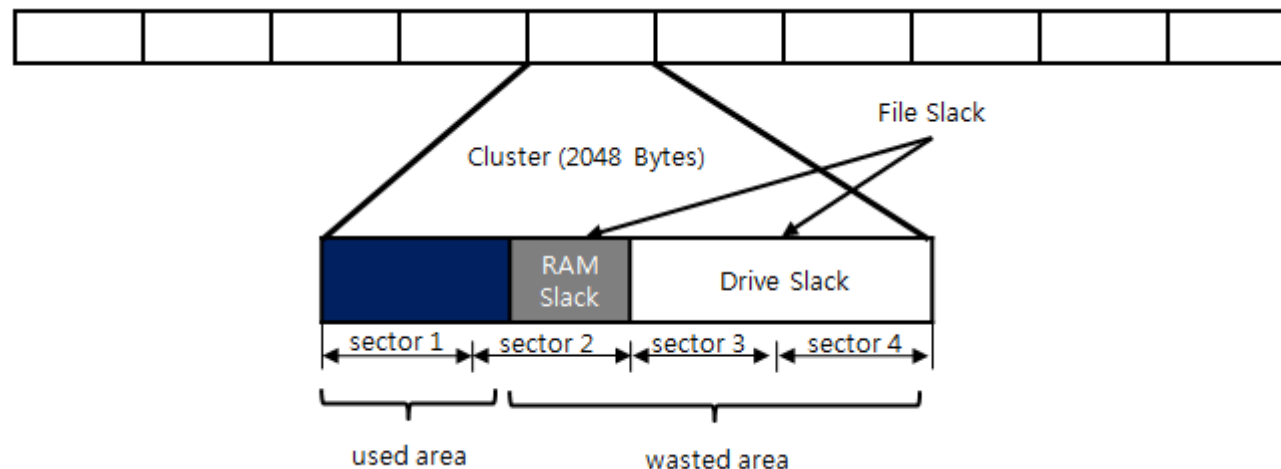
C. Examining Evidence

- The examination of evidence occurs after it has been acquired using forensic software.
- Working from an image of the original machine, **you can extract files and other data from the image** to separate files, which the examiner can then review. **For example:**
 - a Microsoft Word document found in the image of the suspect machine could be extracted, allowing it to be opened and viewed in MS Word without modifying the original data or that available through the disk image.
- Extracting data from the machine isn't limited only to files that are available to the operating system, file system, or other software that may have been installed on the machine.
- By viewing various areas of the disk, examine the file fragments and data that has been corrupted or deleted.
- Extraction of evidence from a hard disk can occur at either of two levels:
 - ☐ Logical extraction
 - ☐ Physical extraction

- A **logical extraction** is used to identify and recover files based on the **operating system(s), file system(s), and application(s) installed** on the computer.
- This type of extraction allows you to identify what data is stored in active files, deleted files, slack space, and unallocated file space.
- This type of examination **would find information that is available to the operating system, and/or is visible to the file system** on the suspect's computer. When this type of extraction occurs, any or all of the following actions might be performed:

- ❑ **Extraction of file system information.** This is done to identify the structure of folders, as well as the names, locations, sizes, attributes, dates, and timestamps of files.
- ❑ **Extraction of files relevant to the investigation,** which would be based on the name, extension, header/footer, content, and/or location of the file on the drive.
- ❑ **Extraction of data that is encrypted,** password-protected, and/or compressed.
- ❑ **Extraction of data in the file slack.**

- A **cluster** is a group of disk sectors where data is stored, and to which the operating system assigned a unique number to keep track of files. Because the cluster is a fixed size in operating systems such as Windows, the entire cluster is reserved for a file even if the file doesn't fill that amount of space. This unused space is referred to as **slack space**.



- ❑ **Extraction of data in unallocated space.** Unallocated disk space is the part of a hard disk that is not part of any partition. Even though it hasn't been allocated to a partition, it may still contain damaged or deleted data.

- **A physical extraction** *is used to identify and recover files and data across the entire physical hard drive.*
- Because it occurs at the physical level, the file system used on the hard disk doesn't matter.
- A physical extraction may involve a number of different methods to find data that is stored on the computer, including:
 - ❑ **Keyword searching** Extracting data in this way involves searching for specific data using specific keywords.
 - ❑ **File carving** In this case, utilities will recover files or file fragments by looking for file headers/footers and other identifiers in the data. This is particularly useful when attempting to find data that has been damaged or deleted, was located in corrupt directories on the disk, or was stored on damaged media.
 - ❑ **Partition table and unused space examinations** Examining the partition structure can help you to identify the file system being used and determine whether the physical size of the hard disk is accounted for.

- Once the data has been extracted from the computer, **it is analyzed**.
- This involves looking at the data and **determining whether it's relevant and significant** to the case.
- The person examining the machine will **filter the amount of information** that is later provided to the investigator of the case.
- Various types of analysis include:
 1. **Time frame analysis**
 2. **Data hiding analysis**
 3. **Application and file analysis**
 4. **Ownership and possession analysis**

1. Time Frame Analysis

- Timeframe analysis is used to determine **when** files were downloaded, viewed, or modified on a machine. A time frame can be established from these facts that shows when particular events occurred.
- It can be useful in **constructing a sequence of events**, or associating a particular user to a time period (when a file was created, last accessed, or modified).
- In addition to this, dates and times stored in logs and other system files can show when a particular user logged on to a system or performed some action.

2. Data Hiding Analysis

- Data hiding analysis involves looking for **data that may be hidden on the hard disk.**
- By concealing the information, the person who hid the information hopes it will avoid detection from casual or forensic detection.
- Some techniques for hiding data may require special tools, others may be simple to detect if you're aware of the methods being used.
- *Steganography refers to a method of hiding data—not just concealing its contents as encryption does, but concealing its very existence.* Steganography is usually used in conjunction with encryption for added protection of sensitive data.
- This method ameliorates one of the biggest problems of finding relevant data—the fact that it is encrypted draws the attention of people who are looking for confidential or sensitive information.

3. Application and File Analysis

- Application and file analysis is used
 - to identify **what kinds of programs** the suspect is using,
 - to identify **common file types** used for specific purposes relevant to the investigation, and
 - **to associate files that have been located on the drive with particular software.**
- Often, people will use certain patterns to name files or directories, whether it is to be as specific and detailed as possible (**for example**, TaxReturn2007.q07) or to hide the contents by using a specific code (for example, cp13yf.jpg to indicate obscene child pics depicting a 13-year-old girl).
- By identifying these patterns and their relevance, search can be expanded to other files with these features.
- **Some files can be associated with specific applications**, to identify what programs are commonly being used. **For example**,
 - Identify files in a Temporary Internet Files directory to those used with Internet Explorer.
 - Similarly, reviewing the Internet history and messages in the e-mail software, correlation between files can be found that have been saved to those sent or received via e-mail, or downloaded from a particular Web site.
- To identify what is depicted in an image, or the data in a spreadsheet or document, you will need to view the contents and **establish their relevance to the case.**

4. Ownership and Possession Analysis

- Ownership and possession analysis is used to identify **who created, modified, or accessed files on a computer.**
- By identifying the individual who created, viewed, or downloaded a particular file, **you can associate the existence of a file to the actions of a person. For example:**
 - if a person said that he or she hadn't seen a file, you could show that the file's ownership belonged to that person's user account, and by identifying the last time it was accessed, you could show that the person had reasonable knowledge of its existence.
- This type of analysis can easily be used with time frame analysis to show when a particular person used the computer and had access to a particular file.
- Ownership of a file can be displayed through the properties of a file.
- If multiple users are on a machine, you can associate who owns the file with the person who uses that particular account.
- Logs or other resources to obtain additional information about the user's actions .

D. Documenting and Reporting Evidence

- **Documentation** provides a clear understanding of what occurred to obtain the evidence, and what the evidence represents.
- Irrespective of your role in an investigation, one must document any observations and actions that were made.
- Information should include:
 - ☐ The date and time.
 - ☐ Conversations pertinent to the investigation.
 - ☐ Names of those present or who assisted.
 - ☐ **Tasks that were performed to obtain evidence and perform analysis.**
 - ☐ Anything else that was relevant to the forensic procedures(actions taken) that took place.

Closing the Case

- Once the analysis has been completed and a sufficient amount of time has passed, then what has been found is accepted and another case investigation is taken up.
- If certain evidence has been found, it may even be decided that additional evidence on the computer is necessary or not for the case. **For example,**
 - If crucial evidence is found in the case (such as obscene pictures of minors, counterfeit notes in printers, recovery of deleted confidential files etc.), additional evidence may be unnecessary for further conviction.
- **Once the analyses performed are complete and there's little to nothing else to find, it is usually time to stop.**
- After a final report has been prepared and submitted to the investigator and/or prosecutor, **follow up must be made** to identify what actions (if any) are being taken regarding the case.
- In some situations, **new information that can be used to search for evidence may become available**, and need to revisit the machine or examine new sources of data may arise.
- By following up with investigators, **you will be able to determine what will occur next in the case.** At some point, any evidence you've acquired and analyzed will no longer be needed.
- Policies dealing with the destruction and disposal of evidence should be in place, to provide a guideline for **how long you should keep evidence.**
- In some situations, evidence will be retained in the event of an appeal or delays in hearing the case in court or other hearings.

Thank you



Hard disk configuration

```
ubuntu@ubuntu:~$ sudo hdparm -I /dev/sdb | more
```

```
/dev/sdb:
```

```
ATA device, with non-removable media
```

```
Model Number:      SAMSUNG HD321KJ
Serial Number:     S0MQJ1DP405761
Firmware Revision: CP100-10
Transport:         Serial, ATA8-AST, SATA 1.0a, SATA II Extensions, SATA Rev 2.5
```

```
Standards:
```

```
Used: ATA-8-ACS revision 3b
Supported: 8 7 6 5
```

```
Configuration:
```

	max	current
Logical cylinders	16383	16383
heads	16	16
sectors/track	63	63

```
--
```

```
CHS current addressable sectors: 16514064
LBA user addressable sectors: 268435455
LBA48 user addressable sectors: 625142448
Logical/Physical Sector size: 512 bytes
device size with M = 1024*1024: 305245 MBytes
device size with M = 1000*1000: 320072 MBytes (320 GB)
cache/buffer size = 16384 KBytes (type=DualPortCache)
```

```
Capabilities:
```

```
LBA, IORDY(can be disabled)
Queue depth: 32
Standby timer values: spec'd by Standard, no device specific minimum
R/W multiple sector transfer: Max = 16 Current = ?
Recommended acoustic management value: 254, current value: 0
DMA: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 udma5 *udma6 udma7
Cycle time: min=120ns recommended=120ns
PIO: pio0 pio1 pio2 pio3 pio4
Cycle time: no flow control=120ns IORDY flow control=120ns
```

```
Commands/features:
```

```
Enabled Supported:
```

- * SMART feature set
- Security Mode feature set
- * Power Management feature set
- * Write cache



Certifications –Vendor Neutral

- CDFE (Certified Digital Forensics Examiner): NICCS (National Initiative for Cybersecurity Careers and Studies)
- CHFI (Computer Hacking Forensic Investigator): EC-Council
- CFCE (Certified Forensic Computer Examiner): IACIS
- GCFE (GIAC Certified Forensic Examiner): SANS
- GIAC Certified Incident Handler (GCIH)
- GASF (GIAC Advanced Smartphone Forensics): SANS
- GIAC Reverse Engineering Malware (GREM)
- GIAC Response and Industrial Defense (GRID)

Vendor Specific

- EnCE (EnCase Certified Examiner): OpenText
- EnCEP (EnCase Certified eDiscovery Practitioner): OpenText
- Paraben corporation

Source:

<https://www.giac.org/certifications/>

<https://cybersecurityguide.org/programs/cybersecurity-certifications/digital-forensics/>

<https://www.computer-forensics-recruiter.com/degrees/computer forensics certifications/>



- [Links to the manufacturers](#) of computers, cell phones, hard disks, and other devices **will enable to look up information on:-**
 - how to properly remove a hard disk from a particular make and model of computer
 - how to access the Basic Input Output System (BIOS) / UEFI settings
 - how to bypass certain security features or access information stored in the device.

Sample
Manual
Page

Beep Code	Possible Problem
One	Possible motherboard failure - BIOS ROM checksum failure
Two	No RAM detected NOTE: If you installed or replaced the memory module, ensure that the memory module is seated properly.
Three	Possible motherboard failure - Chipset error
Four	RAM read/write failure
Five	Real Time Clock failure
Six	Video card or chip failure
Seven	Processor failure
Eight	Display failure

Network Problems

Wireless Connections

If the wireless network connection is lost — The wireless router is offline or wireless has been disabled on the computer.

- Check your wireless router to ensure it is powered on and connected to your data source (cable modem or network hub).
- Ensure that wireless is enabled (see "Enable or Disable Wireless" on page 12).
- Re-establish your connection to the wireless router (see "Setting Up a Wireless Connection" on page 15).
- Interference may be blocking or interrupting your wireless connection. Try moving the computer closer to your wireless router.

Wired Connections

If the network connection is lost — The cable is loose or damaged.

- Check the cable to ensure it is plugged in and not damaged.

Forensic Workstations



Forensic Workstation |


Road MASter™ - 3 x 2

FORENSICS

POWERFUL PORTABLE FORENSIC EVIDENCE SEIZURE, PREVIEW AND ANALYSIS SYSTEM

FEATURES:

1. High-end Processing Power
2. Multiple Drive Interface Support
3. Multiple Built-In ports
4. Rugged Design
5. Programmable "Suspect" Drive Ports
6. Multi-Session Capability
7. Multiple Operational Modes
8. Multiple Hash Verifications
9. External Storage
10. Upload and Download Images to Storage Area Network
11. "On the fly" Drive Image Encryption
12. ICS Digital Forensic Storage Solutions (DFSS)
13. Color Display
14. Modular Design
15. Ease of Use
16. Suspect Data Preview
17. Network Storage Support
18. EMI Shielding
19. Built-in Cooling Fans
20. Powerful Analysis Tool Support
21. Logs and Auditing
22. Cell Phone Acquisition Support
23. Convenient and Easy Upgrades



Intelligent Computer Solutions

Make the intelligent choice...
www.ics-iq.com

RoadMASter-3 x 2

Digital Forensic kit

crimescene.com/store/product/digital-investigators-kit/

FREE SHIPPING FOR ORDERS OVER \$60 IN THE USA.

Contact Us

Crime Scene

Search

LOGIN

CART / \$ 0.00

search
detective
investigation



DISCOVER
DATA
HIDDEN
INSIDE
ANY
ANDROID
DEVICE



**DIGITAL
INVESTIGATORS
KIT**

EXTRACT
AND
EXAMINE
DATA
FROM ALL
IPHONES
IOS 1 -
IOS 13



- iRecovery Stick for iPhone
- Phone Recovery Stick for Android
- Sim Card Seizure
- Data Recovery Stick for Windows OS
- Porn Detection Stick for Windows OS
- Chat Detection Stick for Windows OS
- Voicellogger for Windows OS
- Multiple Cables for cellphone connectivity
- Sim Card Adapter to investigate all types of Sim Cards
- 64GB USB Drive – Save evidence directly to your own case drive.



Event Viewer displays these types of events:

- **Error:** A significant problem, such as loss of data or loss of functionality. **For example**, if a service fails to load during startup, an error will be logged.
- **Warning:** An event that is not necessarily significant, but may indicate a possible future problem. **For example**, when disk space is low, a warning will be logged.
- **Information:** An event that describes the successful operation of an application, driver, or service. **For example**, when a network driver loads successfully, an Information event will be logged.
- **Success Audit:** An audited security access attempt that succeeds. **For example**, a user's successful attempt to log on to the system will be logged as a Success Audit event.
- **Failure Audit:** An audited security access attempt that fails. **For example**, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Event Viewer (Local)' tree with 'System' selected under 'Windows Logs'. The right pane shows a list of events for the System log, with a total of 58,416 events. The events are displayed in a table with columns: Level, Date and Time, Source, Event ID, and Task Category.

Level	Date and Time	Source	Event ID	Task Category
Information	14/3/2022 10:39:22 AM	Service Control Manager	7036	None
Information	14/3/2022 10:31:19 AM	Service Control Manager	7036	None
Information	14/3/2022 10:29:22 AM	Service Control Manager	7036	None
Information	14/3/2022 10:19:37 AM	Service Control Manager	7036	None
Information	14/3/2022 10:16:14 AM	Service Control Manager	7036	None
Information	14/3/2022 10:14:36 AM	Service Control Manager	7036	None
Information	14/3/2022 10:11:33 AM	Service Control Manager	7036	None
Error	14/3/2022 10:06:53 AM	Schannel	36887	None
Error	14/3/2022 10:06:53 AM	Schannel	36887	None
Error	14/3/2022 10:06:52 AM	Schannel	36887	None
Error	14/3/2022 10:06:51 AM	Schannel	36887	None
Error	14/3/2022 10:06:51 AM	Schannel	36887	None
Error	14/3/2022 10:06:51 AM	Schannel	36887	None



Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Administrative Events
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
 - ACEEventLog
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - Media Center
 - Microsoft
 - Microsoft Office Diagnostics
 - Microsoft Office Sessions
 - Windows PowerShell
 - Subscriptions

System Number of events: 58,416 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	14/3/2022 9:20:54 AM	Service Control Manager	7036	None
Information	14/3/2022 9:20:54 AM	Service Control Manager	7036	None
Information	14/3/2022 9:20:00 AM	Service Control Manager	7036	None
Warning	14/3/2022 9:19:47 AM	Kernel-Processor-Power	37	(7)
Warning	14/3/2022 9:19:47 AM	Kernel-Processor-Power	37	(7)
Warning	14/3/2022 9:19:47 AM	Kernel-Processor-Power	37	(7)
Warning	14/3/2022 9:19:47 AM	Kernel-Processor-Power	37	(7)
Warning	14/3/2022 9:19:47 AM	Kernel-Processor-Power	37	(7)

Event Properties - Event 37, Kernel-Processor-Power

General Details

The speed of processor 1 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 17 seconds since the last report.

Log Name: System

Source: Kernel-Processor-Power

Event ID: 37

Level: Warning

User: SYSTEM

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 14/3/2022 9:19:47 AM

Task Category: (7)

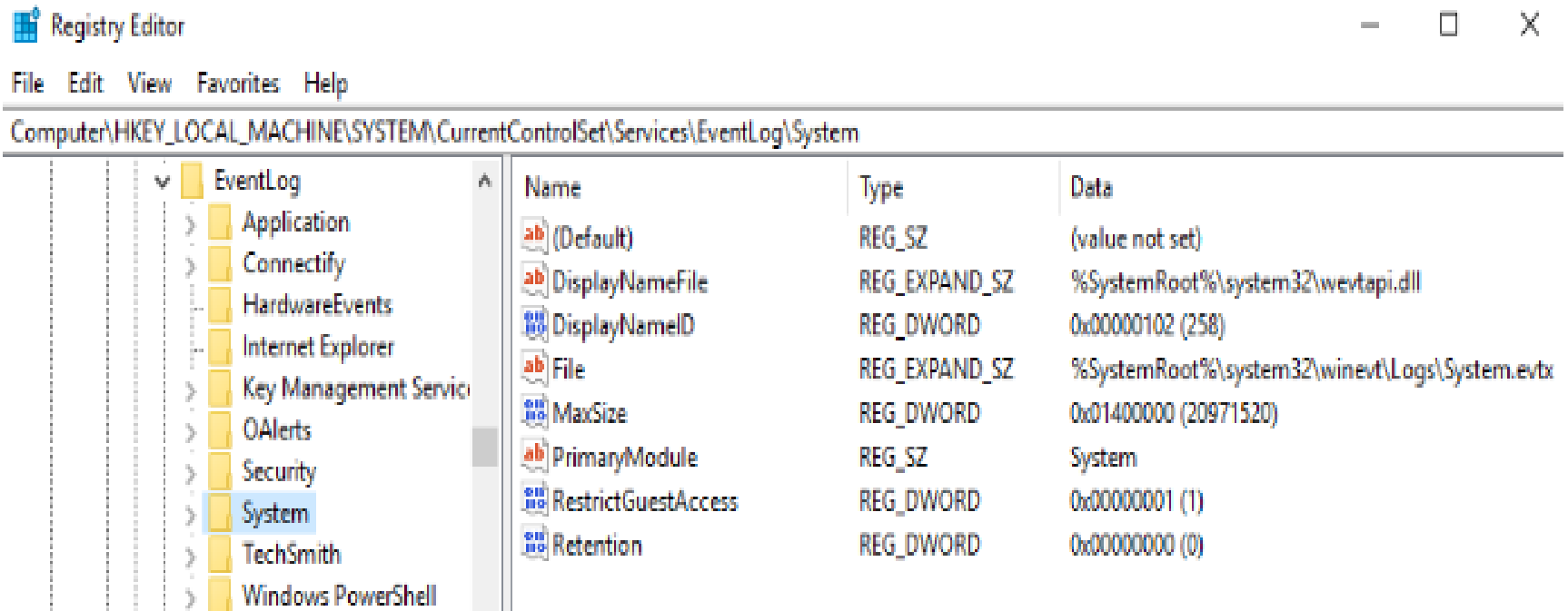
Keywords:

Computer: waheguru-PC

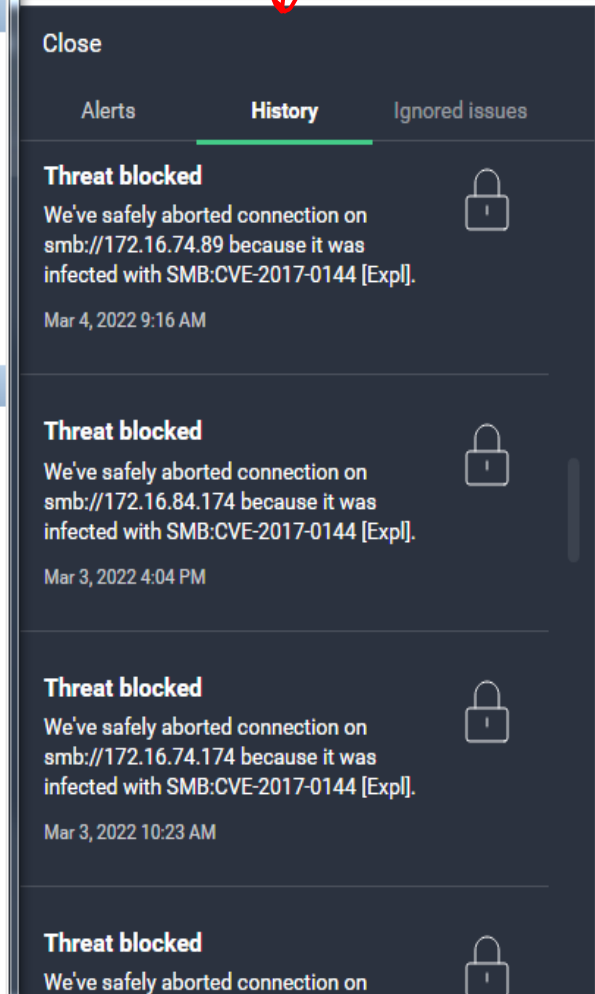
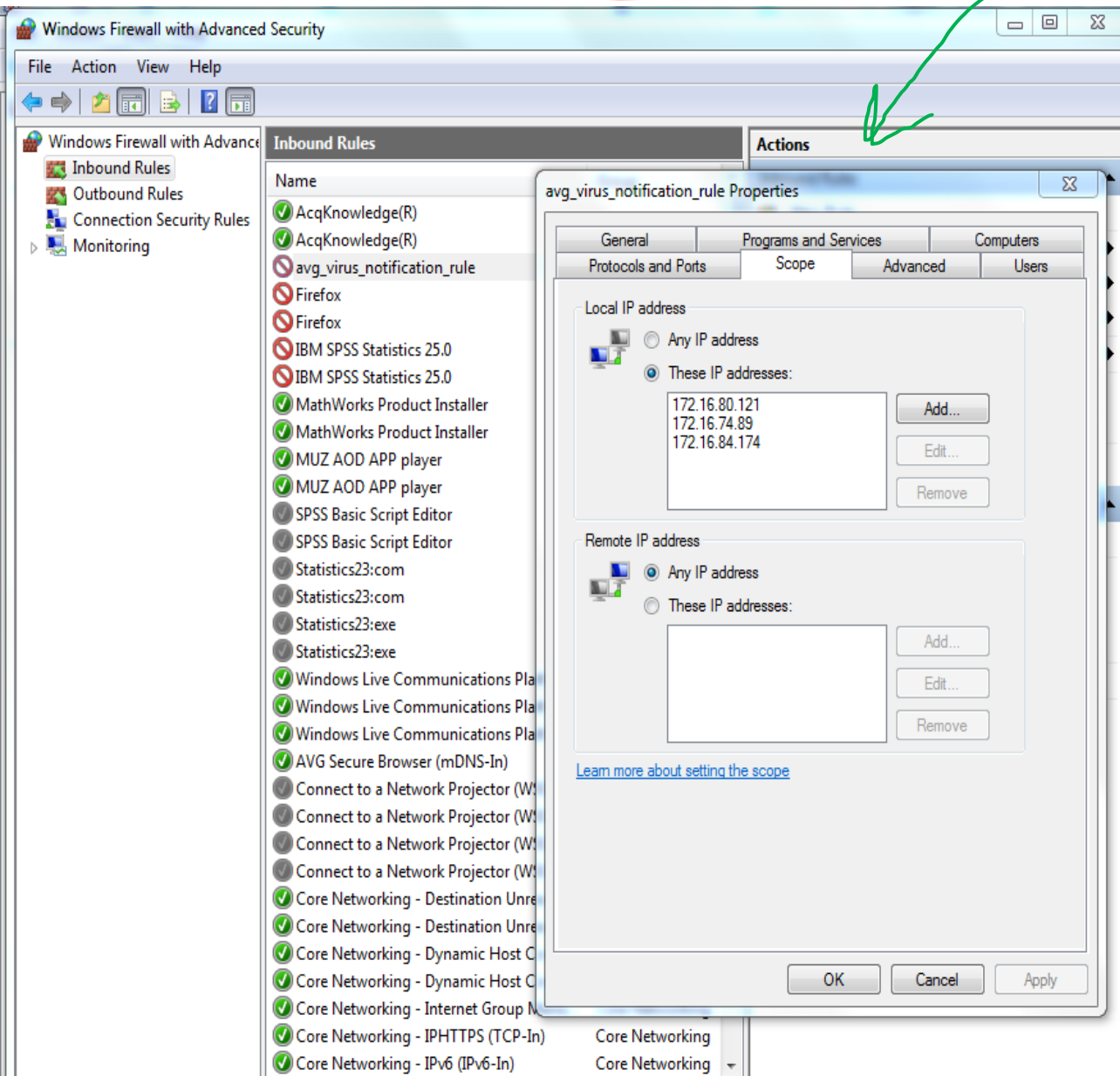
Copy Close



Windows Event logs location in windows registry



Antivirus and Firewall Rules





Examine Running Processes

Windows Task Manager

File Options View Help

Applications Processes Services Performance Networking Users

Image Name	User Name	CPU	Memory (...)	Description
wup.exe		37	5,712 K	
instup.exe	waheguru	11	27,152 K	AVG Antivirus Installer
taskmgr.exe	waheguru	01	3,916 K	Windows Task Manager
Core Temp.exe	waheguru	00	5,248 K	CPU temperature and system information utility
45de073220d50c54b2720a748e83e265.exe		00	12,644 K	
conhost.exe		00	2,016 K	
jucheck.exe *32	waheguru	00	4,328 K	Java Update Checker
conhost.exe		00	2,016 K	
conhost.exe		00	2,020 K	
injector.exe		00	688 K	
csrss.exe		00	18,224 K	
CCC.exe	waheguru	00	1,300 K	Catalyst Control Centre: Host application
jusched.exe *32	waheguru	00	2,056 K	Java Update Scheduler
WebcamDell2.exe *32	waheguru	00	3,392 K	WebcamDell2.exe
BTTray.exe	waheguru	00	6,084 K	Bluetooth Tray Application
RAVCpl64.exe	waheguru	00	6,560 K	HD Audio Control Panel
rundll32.exe	waheguru	00	2,416 K	Windows host process (Rundll32)
RAVBg64.exe	waheguru	00	5,000 K	HD Audio Background Process
MOM.exe	waheguru	00	1,660 K	Catalyst Control Center: Monitoring program
4dffc7ad915f065bd3b59f478caf4e38.exe		00	14,948 K	
conhost.exe		00	2,016 K	
wisptis.exe	waheguru	00	88 K	
taskhost.exe	waheguru	00	2,712 K	Host Process for Windows Tasks
explorer.exe	waheguru	00	40,168 K	Windows Explorer
dwm.exe	waheguru	00	16,728 K	Desktop Window Manager
atiedxx.exe		00	2,828 K	
winlogon.exe		00	3,240 K	
csrss.exe		00	2,616 K	
SnippingTool.exe	waheguru	00	2,744 K	Snipping Tool

Show processes from all users

Injector.exe is a Trojan Coin Miner that utilizes the contaminated computer's resources to mine electronic money without your authorization.




Control Panel > All Control Panel Items > Windows Firewall > Allowed Programs

View Tools Help

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click **Change settings**.

What are the risks of allowing a program to communicate?

 **Change settings**

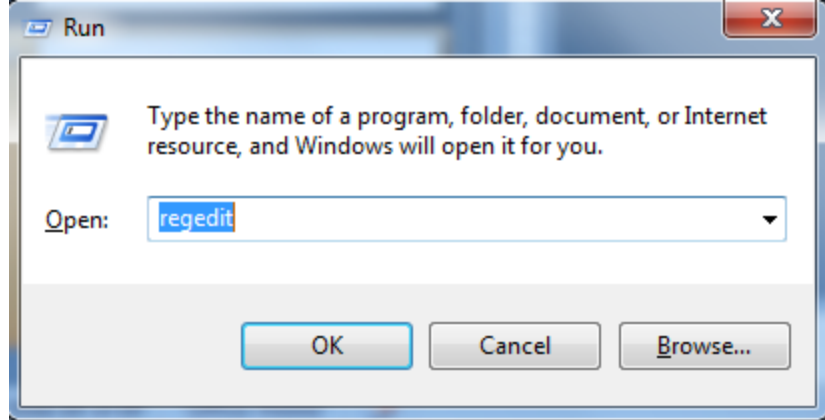
Allowed programs and features:

Name	Home/Work (Private)	Public
<input checked="" type="checkbox"/> AcqKnowledge(R)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> AVG Secure Browser	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> avg_virus_notification_rule	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Connect to a Network Projector	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> File and Printer Sharing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Firefox	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Google Chrome	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> HomeGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> IBM SPSS Statistics 25.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>

Details...

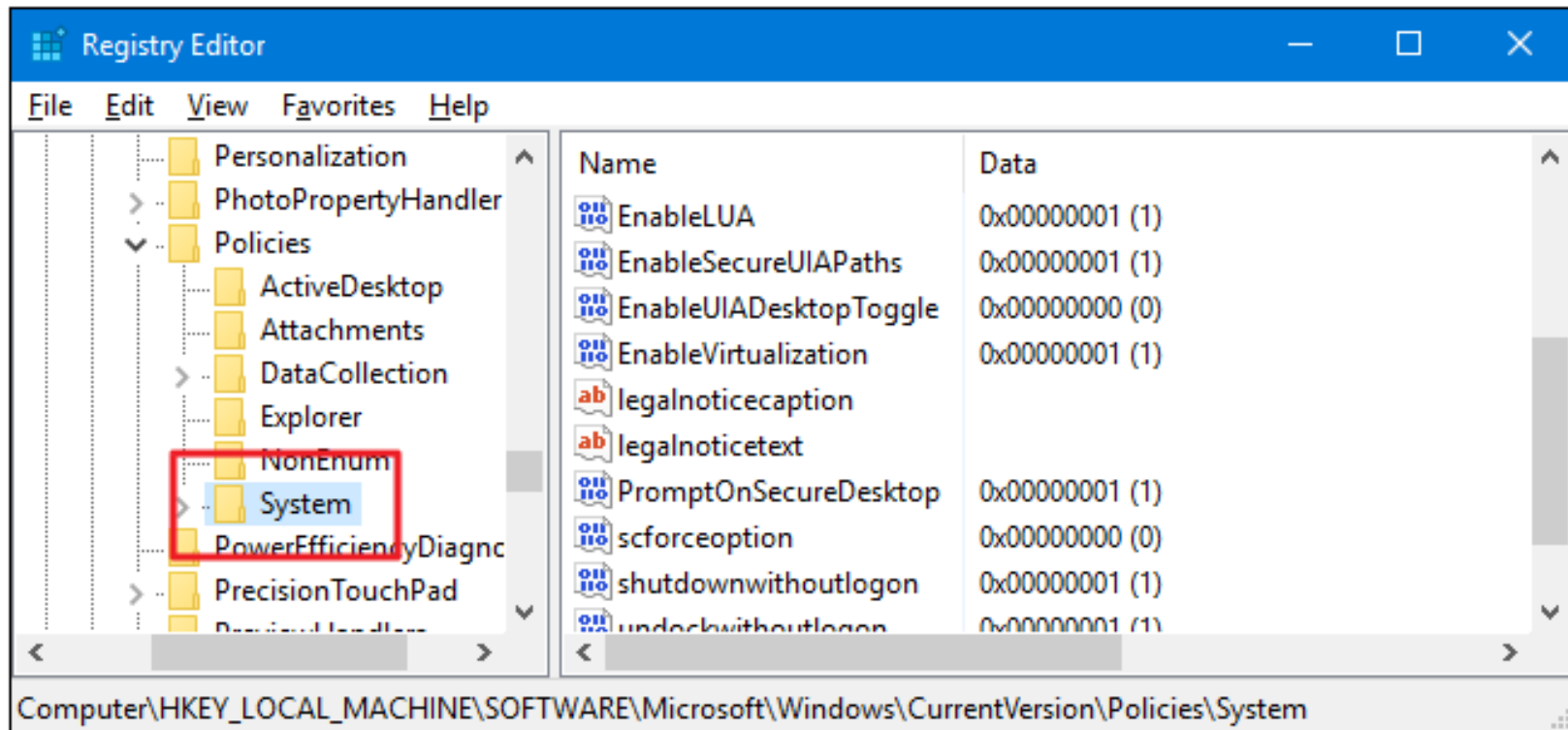
Remove

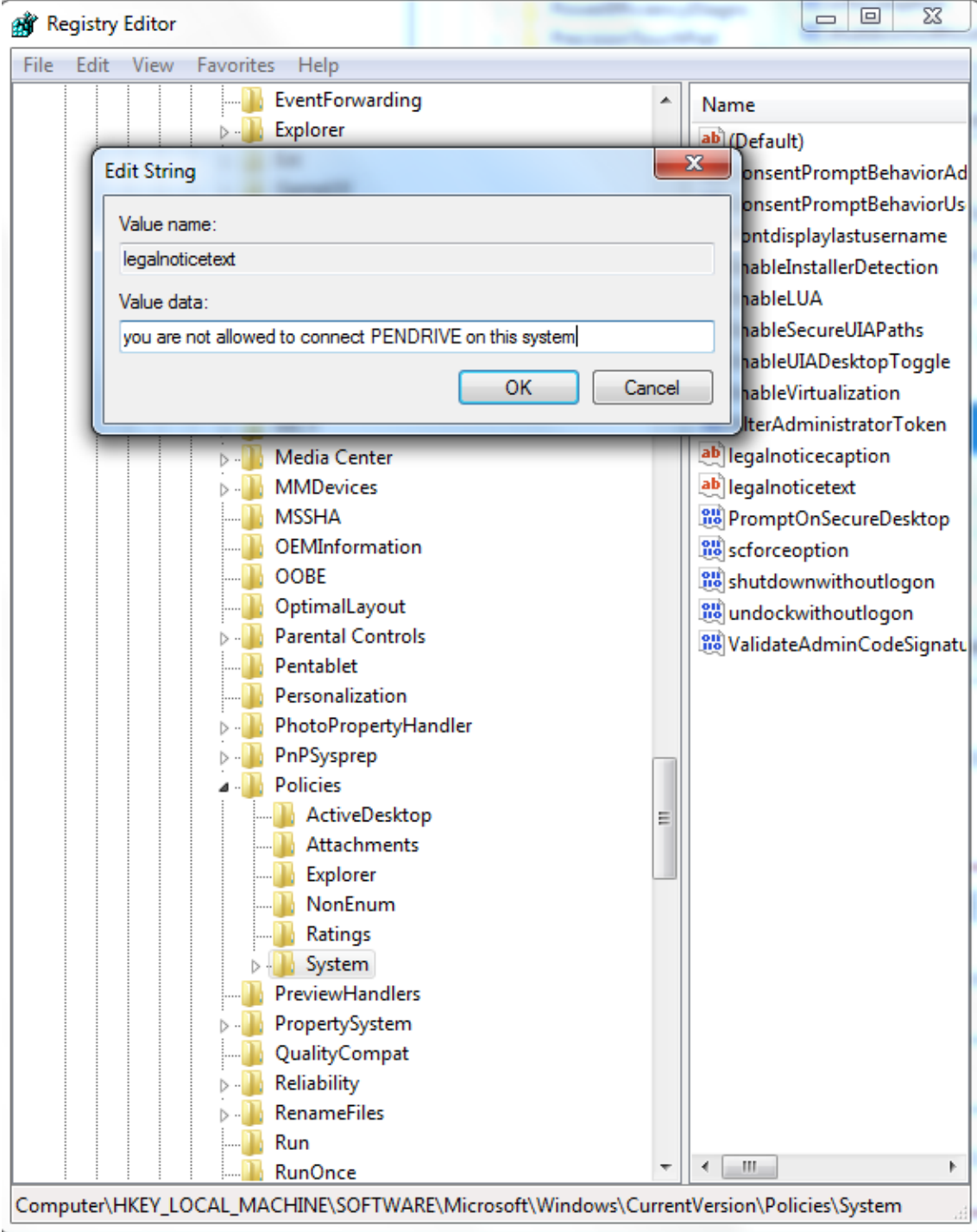
Allow another program...

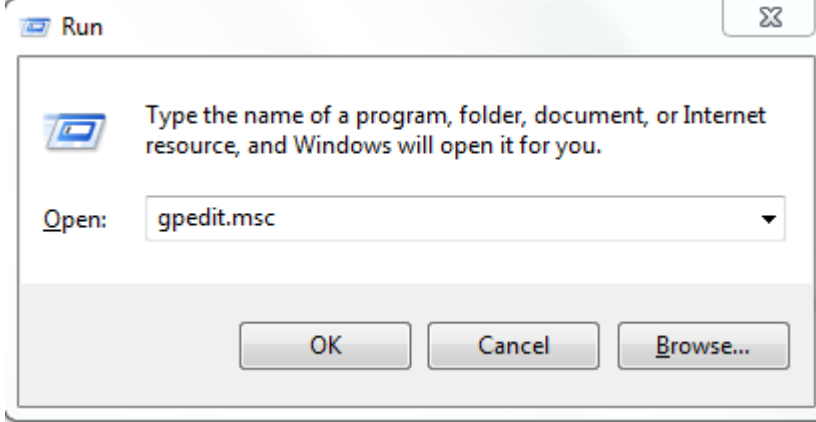


Message on logon

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
```







Local Group policy Editor

Windows settings > Security Settings > Security options ----> Interactive logon

