Unit-1

Contents

- Introduction of Cyber Crime
- Computer roles in Crime
- Introduction to Digital Forensics and its uses.
- Forensics Evidence, Collection, Processing
- Phases of forensics investigation
- Types of Computer Forensics

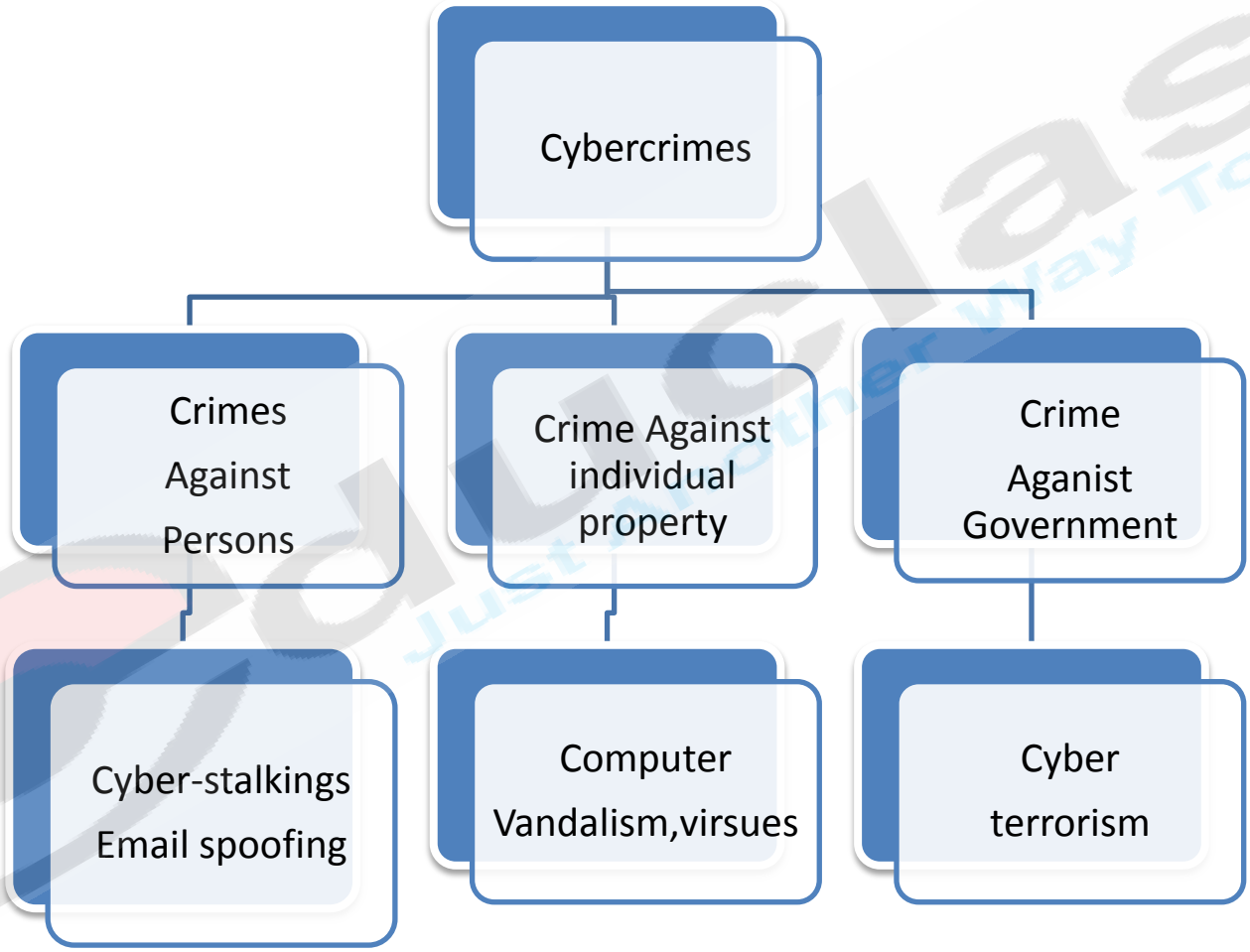
Introduction of Cyber Crime

- A crime conducted in which a computer was directly or significantly instrumental
- Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.
- Computer related crime, Computer crime, Internet crime, E-crime, High-tech crime etc. are synonymous terms

Few definition of Cyber Crime

- A crime committed using a computer and the Internet to steal person's identity
- Crime completed either on or with a computer
- Any illegal activity done through the Internet or on the computer
- All criminal activities done using the medium of computers, the Internet, cyberspace and WWW

Categories of Cybercrime



- Cyber crimes can be basically divided into 3 major categories:
  1. Cybercrimes against persons.
  2. Cybercrimes against property.
  3. Cybercrimes against government

Cybercrimes against persons

- This committed against persons include various harassment of any one with the use of a computer such as e-mail.
- Cyber harassment is a distinct Cybercrime.
- Harassment can be racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes.
- Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens.
- No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

Cybercrimes against property

- The second category of Cyber-crimes is that of Cybercrimes against all forms of property.
- These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.
- E.g. : A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy

Cybercrimes against government

- The third category of Cyber-crimes relates to Cyber crimes against Government.
- Cyber terrorism is one distinct kind of crime in this category.
- The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country.
- This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.
- The Parliament attack in Delhi and the recent Mumbai attack fall under this category.

Types of Cybercrime

- Broadly divided as:

1. **Violent or potentially violent cybercrimes**: pose a physical risk to some character or persons. They can be categorized as:
   a. Cyber terrorism
   b. Cyber talking
   c. Assaults by threat
   d. Child pornography
2. **Non-violent cybercrimes**: do not directly pose a physical risk to some character or persons, but indirectly they do pose a risk. They can be categorized as:
   a. Cyber theft
   b. Cyber trespass
   c. Cyber fraud
   d. Destructive cybercrimes

The Role of Computer Forensics in Crime

1. **A computer can be the *object of*** *a crime. When a computer is affected by* the criminal act, it is the object of the crime (e.g., when a computer is stolen or destroyed).
2. **A computer can be the subject of a crime. When a computer is the environment** in which the crime is committed, it is the *subject of the crime* (e.g., when a computer is infected by a virus or impaired in some other way to inconvenience the individuals who use it).
3. **The computer can be used as the *tool for conducting or planning a crime.***

   For example, when a computer is used to forge documents or break into other computers, it is the instrument of the crime.
4. **The *symbol of the computer itself can be used to intimidate or deceive. An*** example given is of a stockbroker who told his clients that he was able to make huge profits on rapid stock option trading by using a secret computer program in a giant computer in a Wall Street brokerage firm. Although he had no such programs or access to the computer in question, hundreds of clients were convinced enough to invest a minimum of $100,000 each.

Hacking

- Hacker as an artless coder.
- A hacker as a clever programmer.
- A "good hack" is a clever solution to a programming problem and "hacking" is the act of doing it.
- Raymond lists five possible characteristics that qualify one as a hacker:
  1. A person who enjoys learning details of a programming language or System
  2. A person who enjoys actually doing the programming rather than just theorizing about it
  3. A person capable of appreciating someone else's hacking
  4. A person who picks up programming quickly
  5. A person who is an expert at a particular programming language or system.

1. Viruses and Worms : Viruses are programs that attach themselves to a computer or a file. They then circulate themselves to other files and to other computers on a network. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory

2. Denial-of-Service-Attacks These attacks occur when a person or a group of people try to prevent a internet site from functioning effectively either temporarily or on a long term basis.
3. Malware : Malware means malicious software. It is designed to secretly access an individual's computer without his/her permission. Most malware are software's created with the intent of stealing data. Using these software's, which are usually disguised as harmless pop-ups and such, information about the users is collected without their knowledge

4. Hacking: Hacking is unauthorized access over a computer system, and it usually involves modifying computer hardware or software to accomplish a goal outside the creator's purpose.
5. Software Piracy : Unauthorized copying of purchased software is called software piracy. Making copies of the software for commercial distribution, or resale is illegal. However software piracy is still rampant around the globe, because it is almost impossible to put an end to it.

6. Fraud : Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space.

   Some of the cases of online fraud and cheating that have come to light are those relating to credit card crimes, bank fraud, contractual crimes, internet scams, identity theft, extortion etc

7. Cyber stalking : Cyber stalking involves following a person's movements across the Internet by posting threatening messages on the bulletin boards frequented by the victim, entering the chatrooms frequented by the victim, and constantly bombarding the victim with emails.

9. Harassment : Any comment that may be considered degratory or offensive is considered harassment. Harassment via the internet occurs in chat rooms, social networking sites, and emails.
10. Trafficking : Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms or weapons. These forms of trafficking are carried on under pseudonyms, encrypted emails, and other internet technology.

11. Computer Vandalism : Vandalism means deliberately destroying or damaging property of another. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer, or by physically damaging a computer or its peripherals.
12. Spam : The unwanted sending of bulk e-mail for commercial purposes is called spam. Although this is a relatively minor crime, recently new antispam laws have cropped up to restrict the sending of these e-mails.
13. Online Betting: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc

What is Forensics?

- Forensic: "…a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence)."
- The aim of forensic science is: "…to demonstrate how evidence can be used to reconstruct a crime or incident, identify suspects, apprehend the guilty, defend the innocent, and understand criminal motivations."

Rules of Computer/Digital Forensic

- Performing digital forensic investigator rules are:
  - Minimal handling of the original
  - Account for any change
  - Comply with the rules of evidence
  - Do not exceed your knowledge

What is Digital Forensics?

- “Tools and techniques to recover, preserve and examine digital evidence on or transmitted by digital devices.”
- Devices include computers, PDAs, cellular phones, videogame consoles, copy machines, printers, smart devices…

Why Digital Forensics?

- Deleted files aren't securely deleted
  - Recover deleted file + when it was deleted!
- Renaming files to avoid detection is pointless
- Formatting disks doesn't delete much data
- Web-based email can be (partially) recovered directly from a computer
- Files transferred over a network can be reassembled and used as evidence
- Uninstalling applications is much more difficult than it might appear…
- "Volatile" data hangs around for a long time (even across reboots)
- Remnants from previously executed applications
- Using encryption properly is difficult, because data isn't useful unless decrypted
- Anti-forensics (privacy-enhancing) software is mostly broken
- Basic enabler: Data is very hard to kill

Who uses Computer Forensics?

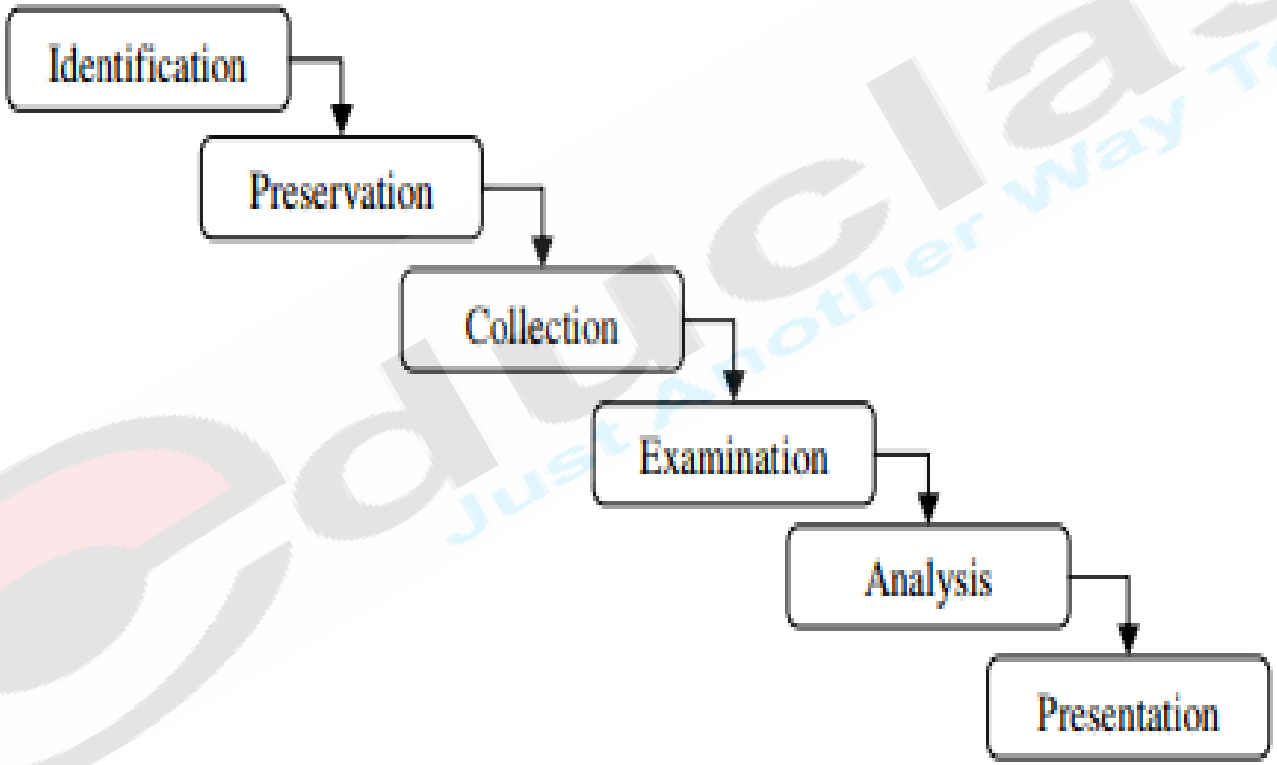
- Law Enforcement
- Private Computer Forensic Organizations
- Military
- University Programs Computer
- Security and IT Professionals

Digital Forensic Models

1. DFRWS(Digital Forensics Research Workshop) Investigative Model
2. Integrated Digital Investigation Process Model(IDIP)
3. Enhanced Digital Investigation Process Model (EDIP)
4. Computer Forensics Field Triage Process Model (CFFTPM)
5. Common phases of computer forensic investigation models(CPCCFIM)

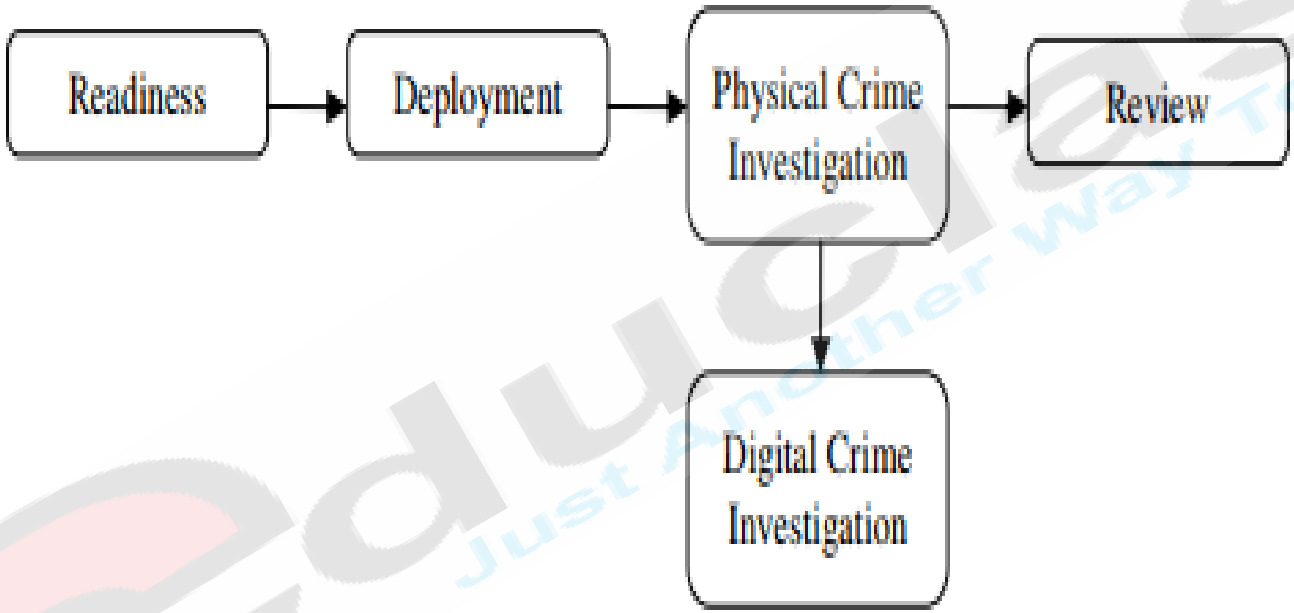
DFRWS Investigative Model:

- In 2001, the 1st Digital Forensics Research Workshop (DFRWS) proposed a general purpose digital forensics investigation process. It comprises of 6 phases:
- DFRWS Investigative model started with an **Identification** phase, in which profile detection, system monitoring, audit analysis, etc, were performed.
- It is immediately followed by **Preservation** phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody. This phase is crucial so as to ensure that the data collected is free from contamination.
- The next phase is known as **Collection**, in which relevant data are being collected based on the approved methods utilizing various recovery techniques.
- Following this phase are two crucial phases, namely, **Examination** phase and **Analysis** phase. In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc, were performed.
- The last phase is **Presentation**. Tasks related to this phase are documentation, expert testimony, etc.



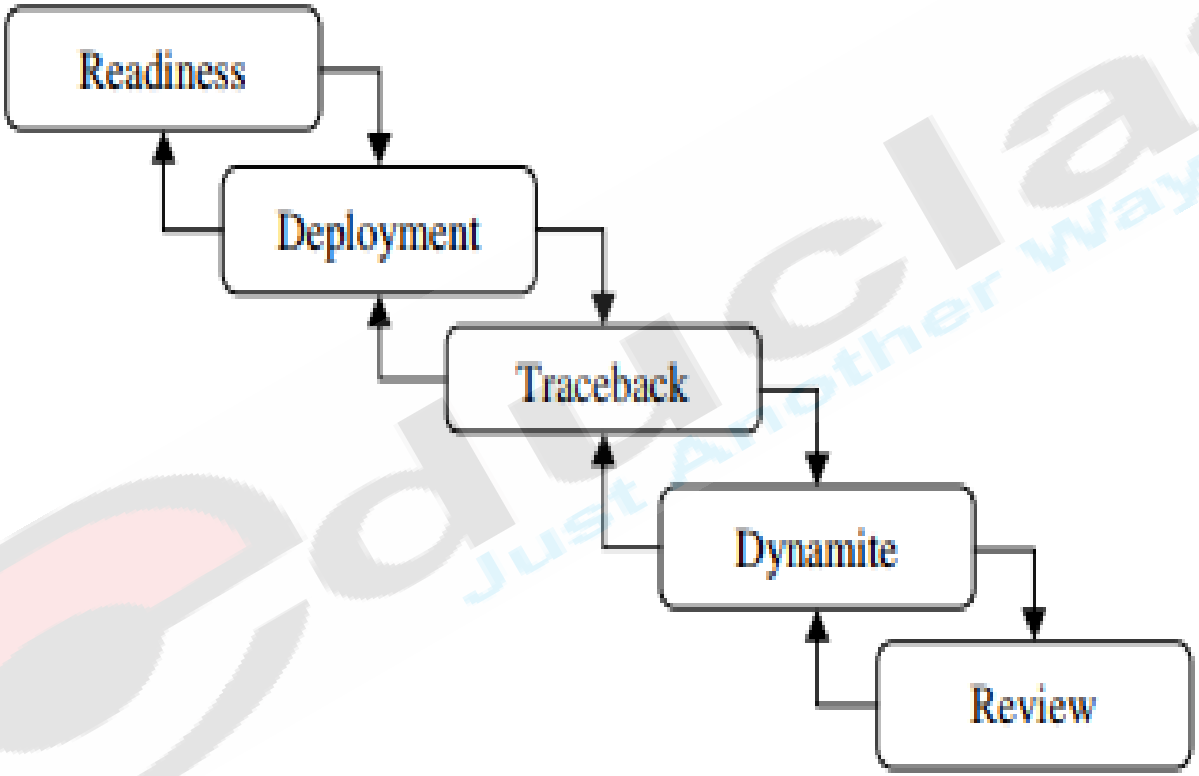
Integrated Digital Investigation Process Model(IDIP):

- This investigation process was proposed by Carrier & Spafford in 2003, with the intention to combine the various available investigative processes into one integrated model.
- The process started with a phase that require for the physical and operational infrastructure to be ready to support any future investigation.
- In this **Readiness phase**, the equipments must be ever ready and the personnel must be capable to use it effectively. This phase is indeed an ongoing phase throughout the lifecycle of an organization. It also consists of 2 sub-phases namely, Operation Readiness and Infrastructure Readiness.
- Immediately following the Readiness phase, is **Deployment phase**, which provide a mechanism for an incident to be detected and confirmed. Two sub-phases are further introduced, namely, Detection & Notification and Confirmation & Authorization.
- Collecting and analyzing physical evidence are done in **Physical Crime** Scene Investigation phase. The sub-phases introduced are Preservation, Survey, Documentation, Search & Collection, Reconstruction and Presentation.
- **Digital Crime** Scene Investigation is similar to **Physical Crime** Scene Investigation with exception that it is now focusing on the digital evidence in digital environment.
- The last phase is **Review** phase. The whole investigation processes are reviewed to identify areas of improvement that may results in new procedures or new training requirements.



Enhanced Integrated Digital Investigation Process Model (EIDIP):

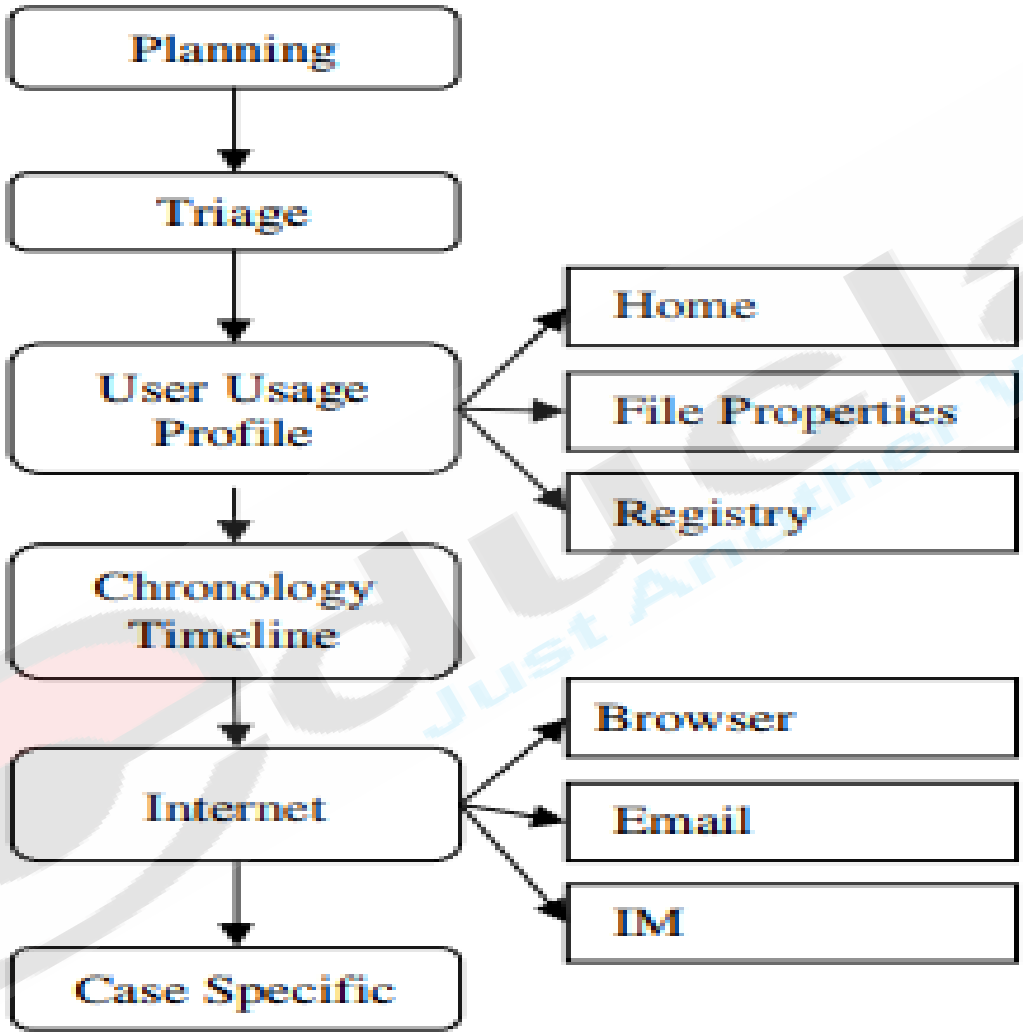
- As the name implies, this investigative model is based on the previous model, Integrated Digital Investigation Process (IDIP), as proposed by Carrier & Spafford.
- The Enhanced integrated Digital Investigation Process Model, also known as EDIP introduces one significant phase known as **Traceback phase**. This is to enable the investigator to trace back all the way to the actual devices/computer used by the criminal to perform the crime.
- The investigation process started with **Readiness phase** and the tasks performed are the same as in IDIP.
- The second phase, **Deployment phase,** provides a mechanism for an incident to be detected and confirmed. It consists of 5 sub-phases namely Detection & Notification, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Confirmation and lastly,Submision. Unlike DIP, this phase includes both physical and digital crime scene investigations and presentation of findings to legal entities (via Submission phase).
- **In Tracebak phase**, tracking down the source crime scene, including the devices and location is the main objective. It is supported by two sub-phases namely, Digital Crime Scene Investigation and Authorization (obtaining approval to perform investigation and accessing information).
- Following Traceback phase is **Dynamite phase**. In this phase, investigation are conducted at the primary crime scene, with the purpose of identifying the potential culprit(s). Consist of 4 subphases, namely, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Reconstruction and Communication. In Reconstruction sub-phase, pieces of information collected are put together so as to construct to possible events that could have happened. The Communication sub-phase is similar to the previous Submission phase. The investigation process ended with Review phase and the tasks performed are the same as in IDIP



Computer Forensics Field Triage Process Model (CFFTPM):

- The CTTTPM proposes an onsite approach to providing the identification, analysis and interpretation of digital evidence in a relatively short time frame without the need to take back the devices or media back to the lab. Nor does it require taking the complete forensic images.
- The CFFTPM consist of 6 primary phases that are then further divided into another 6 sub-phases

- CFFTPM started with a familiar phase, **Planning phase**. Proper planning prior to embarking an investigation will surely improve the success rate of an investigation.
- Following Planning phase is **Triage phase**. In this phase, the evidence are identified and ranked in terms of importance or priority. Evidence with the most important and volatile need to be processed first.
- The User **Usage Profile phase** focus its attention to analyse user activity and profile with the objective of relating evidence to the suspect.
- Building the crime case from **chronological** perspective by making use of MAC time (for example) to sequence the probable crime activities is the main objective of Chronology Timeline phase.
- In the **Internet phase**, the tasks of examining the artifacts of internet related services are performed.
- Lastly, **in Case Specific Evidence phase**, the investigator can adjust the focus of the examination to the specifics of the case such as the focus in child pornography would indeed be different than that of financial crime cases.

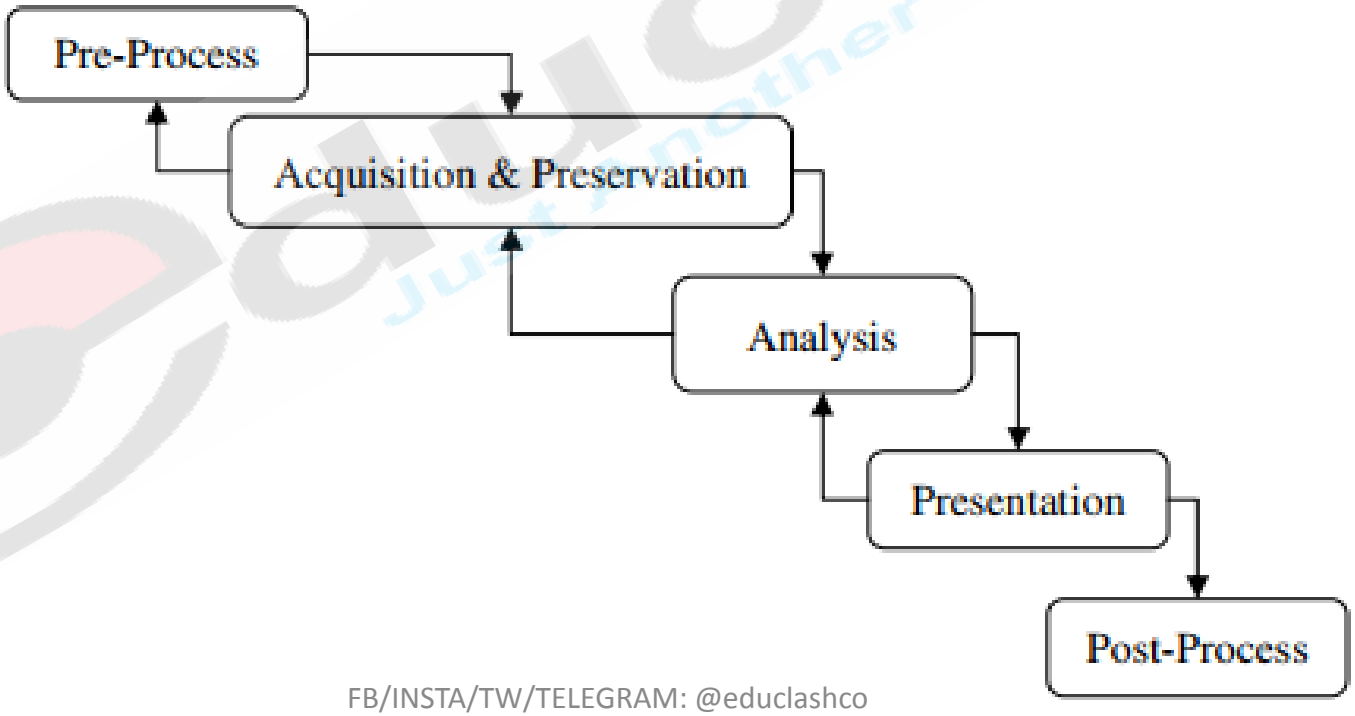


Common phases of computer forensic investigation models(CPCCFIM)

- Phase 1 of CPCCFIM is known as **Pre-Process**. The tasks performed in this phase relates to all of the works that need to be done prior to the actual investigation and official collection of data. Among the tasks to be performed are getting the necessary approval from relevant authority, preparing and setting-up of the tools to be used, etc.
- Phase 2 is known as **Acquisition & Preservation**. Tasks performed under this phase related to the identifying, acquiring, collecting, transporting, storing and preserving of data. In general, this phase is where all relevant data are captured, stored and be made available for the next phase.
- Phase 3 is known as **Analysis**. This is the main and the center of the computer forensic investigation processes. It has the most number of phases in its group thus reflecting the focus of most models reviewed are indeed on the analysis phase Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime.

•Phase 4 is known as **Presentation**. The finding from analysis phase are documented and presented to the authority. Obviously, this phase is crucial as the case must not only be presented in a manner well understood by the party presented to, it must also be supported with adequate and acceptable evidence. The main output of this phase is either to prove or refute the alleged criminal acts

• Phase 5 is known as **Post-Process**. This phase relates to the proper closing of the investigation exercise. Digital and physical evidence need to be properly returned to the rightful owner and kept in safe place, if necessary. Review of the investigative process should be done so that the lesson can be learnt and used for improvement of the future investigations.



What is Digital Evidences

- During an investigation of a computer security incident, you may be unsure whether an item (such as a floppy disk) should be marked as evidence or merely be an attachment or addendum to an investigative report.
- According to the U.S. Federal Rules of Evidence (FRE), *relevant evidence is defined as any information "having a tendency to make the existence* of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the information." (FRE 401).
- We can define evidence as *any information of probative value, meaning it proves something* or helps prove something relevant to the case. It is safest to treat any information of probative value that you obtain during an investigation as evidence.
- Any document, electronic media, electronic files, printouts, or other objects obtained during an investigation that may assist you in proving your case should be treated as evidence and handled according to your organization's evidence-handling procedures.

Digital Evidences and Devices of Modern Age

The Best Evidence Rule

- The best evidence rule essentially requires that, absent some exceptions, the original of a writing or recording must be admitted in court in order to prove its contents.
- Rule 1001(3) provides, "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"
- Under this rule, multiple copies of electronic files may each constitute an "original."
- Many computer security professionals rely heavily on FRE 1001(3), because the electronic evidence collected is often transferred to different media.
- *Best evidence as the most complete copy of evidence* that we have obtained that is closest linked to the original evidence.
- If we have the original evidence media, then it is our best evidence.
- If a client keeps the copy of the original evidence media, then the client has maintained control of the best evidence
- In this case, e treat our forensic duplication as if it were the best evidence as defined by law.

Original Evidence

- Sometimes, the course a case takes is outside the control of the client/victim.
- However, to ensure proper due diligence, we always assume a case will end up in a judicial proceeding, and we handle the evidence accordingly.
- If criminal or civil proceedings are a possibility, we often urge the client/victim to allow us to take control of the original evidence,
- we define *original evidence as the original copy of the evidence media* provided by a client/victim.
- We define *best evidence as the original duplication of the* evidence media, or the duplication most closely linked to the original evidence.
- The evidence custodian should store either the best evidence or the original evidence for every investigation in the evidence safe.

Rules of Digital Evidence

- Admissible
  - Evidence must be able to be used in court
- Authentic
  - Tie the evidence positively to an incident
- Complete
  - Evidence that can cover all perspectives
- Reliable
  - There should be no doubt that proper procedures were used
- Believable
  - Understandable and believable to a jury

Rule 103: Rule of evidence
1. Maintaining a claim of error
2. No renewal of objection or proof
3. Aim an offer of proof
4. Plain error taken as notice

Characteristics of Digital Evidence

3.4.1 Locard's Exchange Principle

According to Edmond Locard's principle, when two items make contact, there will be an interchange. The Locard principle is often cited in forensic sciences and is relevant in digital forensics investigations.

When an incident takes place, a criminal will leave a hint evidence at the scene and remove a hint evidence from the scene. This alteration is known as the Locard exchange principle. Many methods have been suggested in conventional forensic sciences to strongly prosecute criminals. Techniques used consist of blood analysis, DNA matching, and fingerprint verification. These techniques are used to certify the existence of a suspected person at a physical scene. Based on this principle, Culley suggests that where there is a communication with a computer system, clues will be left.

3.4.2 Digital Stream of Bits

Cohen refers to digital evidence as a bag of bits, which in turn can be arranged in arrays to display the information. The information in continuous bits will rarely make sense, and tools are needed to show these structures logically so that it is readable.

The circumstances in which digital evidence are found also helps the investigator during the inspection. Metadata is used to portray data more specifically and is helpful in determining the background of digital evidence.

Types of evidence

1. Demonstrative(Illustrative) evidence
2. Electronic evidence
3. Documented evidence
4. Explainable(exculpatory) evidence
5. Substantial(Physical) evidence
6. Scientific evidence
7. Testimonial

- ***Demonstrative Evidence*:** This is a common form of proof, generally having the form of the representation of an object. Examples include: photographs, videos, sound recordings, x-rays, maps, drawings, graphs, charts, simulations, sculptures, and models, among others.
- ***Digital Evidence (electronic Evidence)*:** In recent years, the use of digital evidence in trials has greatly increased. Simply put, it is any type of proof that can be obtained from an electronic source, such as emails, hard drives, word processing documents, instant message logs, ATM transactions, cell phone logs, and so forth.
- ***Documented Evidence*:** Similar to demonstrative evidence, above, documentary evidence consists of any proof that can be presented in writing (contracts, wills, invoices, etc.). However, term can technically include any number of media upon which such documentation can be recorded and stored (photographs, recordings, films, printed emails, etc.).
- ***Explainable(Exculpatory) Evidence*:** Typically used in criminal cases, this type of evidence is that which favors the defendant, either partially or totally removing their guilt in the case. In the United States, if the prosecutor or police have found evidence, it is their duty to disclose it to the defendant. Failure to do so can result in the case being dismissed.

- ***Substantial(Physical)Evidence*:** Quite simply, this type of evidence is any proof introduced in the form of a physical object, whether whole or in part. In criminal proceedings, such evidence might consist of dried blood, fingerprints, a murder weapon, DNA samples, casts of footprints or tires at the scene of the crime, and so forth.
- ***Scientific Evidence*:** Evidence submitted to the court claiming to be scientific in nature must first conform to generally-accepted principles of the scientific community. In addition, judges must now insure that such evidence is also reliable (Bergman and Berman-Barrett, 2005).
- ***Testimonial*:** This is the "spoken evidence given by a witness under oath in court or at a deposition, or written evidence given under oath through an affidavit“. Generally, a witness is called forth, solemnly swears to tell the truth under the penalty of perjury. This is one of the most common forms of evidence in the legal system.

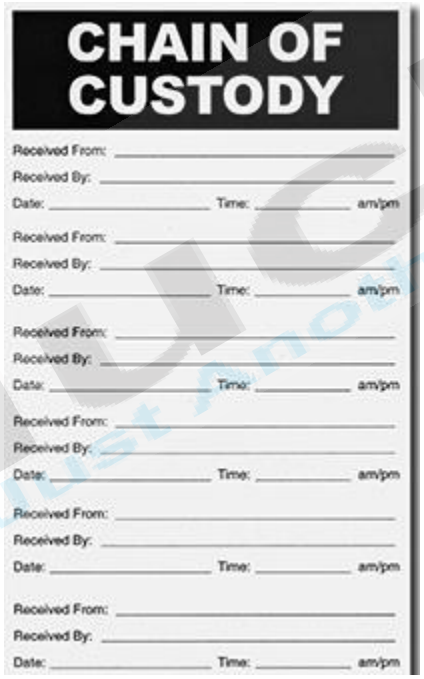
Challenges in Evidence Handling

- One of the most common mistakes made by computer security professionals is failure to adequately document when responding to a computer security incident.
- Critical data might not ever be collected, the data may be lost, or the data's origins and meaning may become unknown.
- Added to the technical complexity of evidence collection is the fact that the properly retrieved evidence requires a paper trail.
- All investigators need to understand the challenges of evidence handling and how to meet these challenges.
- That is why every organization that performs computer security investigations requires a formal evidence-handling procedure.
- The biggest challenges to evidence handling are that the evidence collected must be authenticated at a judicial proceeding and the chain-of-custody for the evidence must be maintained.
- You also must be able to validate your evidence.

1.Authentication of Evidence

- The FRE, as well as the laws of many state jurisdictions, define computer data as “writings
- and recordings.” Documents and recorded material must be authenticated before
- they may be introduced into evidence.
- *Authentication, defined in FRE 901(a), basically means that whomever collected the*
- evidence should testify during direct examination that the information is what the proponent
- claims. In other words, the most common way to authenticate evidence is to have a
- witness who has personal knowledge as to the origins of that piece of evidence provide
- testimony.
- If evidence cannot be authenticated, it is usually considered inadmissible, and that information
- cannot be presented to the judging body. You meet the demands of authentication
- by ensuring that whomever collected the evidence is a matter of record. It is
- important to develop some sort of internal document that records the manner in which
- evidence is collected.

- 2. **Chain of Custody**
- Maintaining the *chain of custody requires that evidence collected is stored in a tamper-*
- proof manner, where it cannot be accessed by unauthorized individuals. A complete
- chain-of-custody record must be kept for each item obtained. Chain of custody requires
- that you can trace the location of the evidence from the moment it was collected to the
- moment it was presented in a judicial proceeding.
- To meet chain-of-custody requirements, many police departments and federal law
- enforcement agencies have property departments that store evidence (the best evidence)
- in a secure place. Experts and law enforcement officers must "check-out" the evidence
- whenever they need to review it, and then "check-in" the evidence each time it is returned
- to storage.
- Your organization can meet the challenge of chain-of-custody requirements by maintaining
- positive control (the evidence was kept within your possession or within your
- sight at all times) of all the best evidence collected, until it can be hand carried or shipped to your evidence custodians for proper storage. Your organization's best evidence should
- always be stored within a safe or storage room that is inaccessible to anyone other than
- the appointed evidence custodians. We refer to this storage area as the *evidence safe. Any*
- access to the evidence safe should be controlled by your evidence custodians.

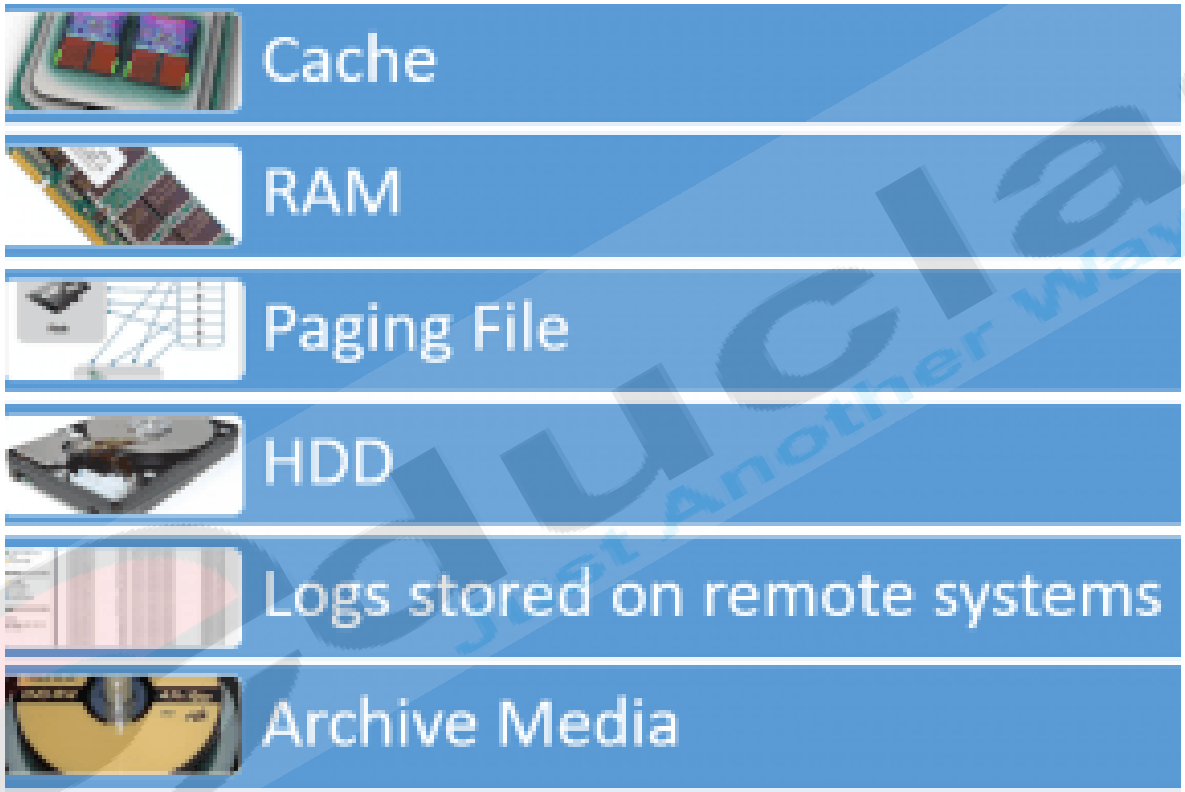


- 3. **Evidence Validation**
- Another challenge is to ensure that the data you collected is identical to the data that you
- present in court. It is not uncommon for several years to pass between the collection of evidence
- and the production of evidence at a judicial proceeding. Your organization can
- meet the challenge of validation by ensuring MD5 hashes of the original media match
- those of the forensic duplication. MD5 hash values should also be generated for every file
- that contributes to the case (every file that is evidence).
- When duplicating a hard drive with EnCase, you can use the verify function within
- the EnCase application. When using dd to perform a forensic duplication, you must record
- an MD5 hash of both the original evidence media and the binary file or files that
- compose the forensic duplication. (See Chapter 7 for details on using EnCase.)

Volatile Evidence

- Volatile data is stored in memory of a live system (or in transit on a data bus) and would be lost when the system was powered down. Volatile data resides in registries, cache,and RAM, which is probably the most significant source.
- A system's RAM contains the programs running on the system(operating -systems, services, applications, etc.) and the data being used by those programs.
- The contents of RAM change constantly and contain many pieces of information that may be useful to an investigation.
- Because RAM and other volatile data are dynamic, collection of this information should occur in real time.

Order of volatility of evidence



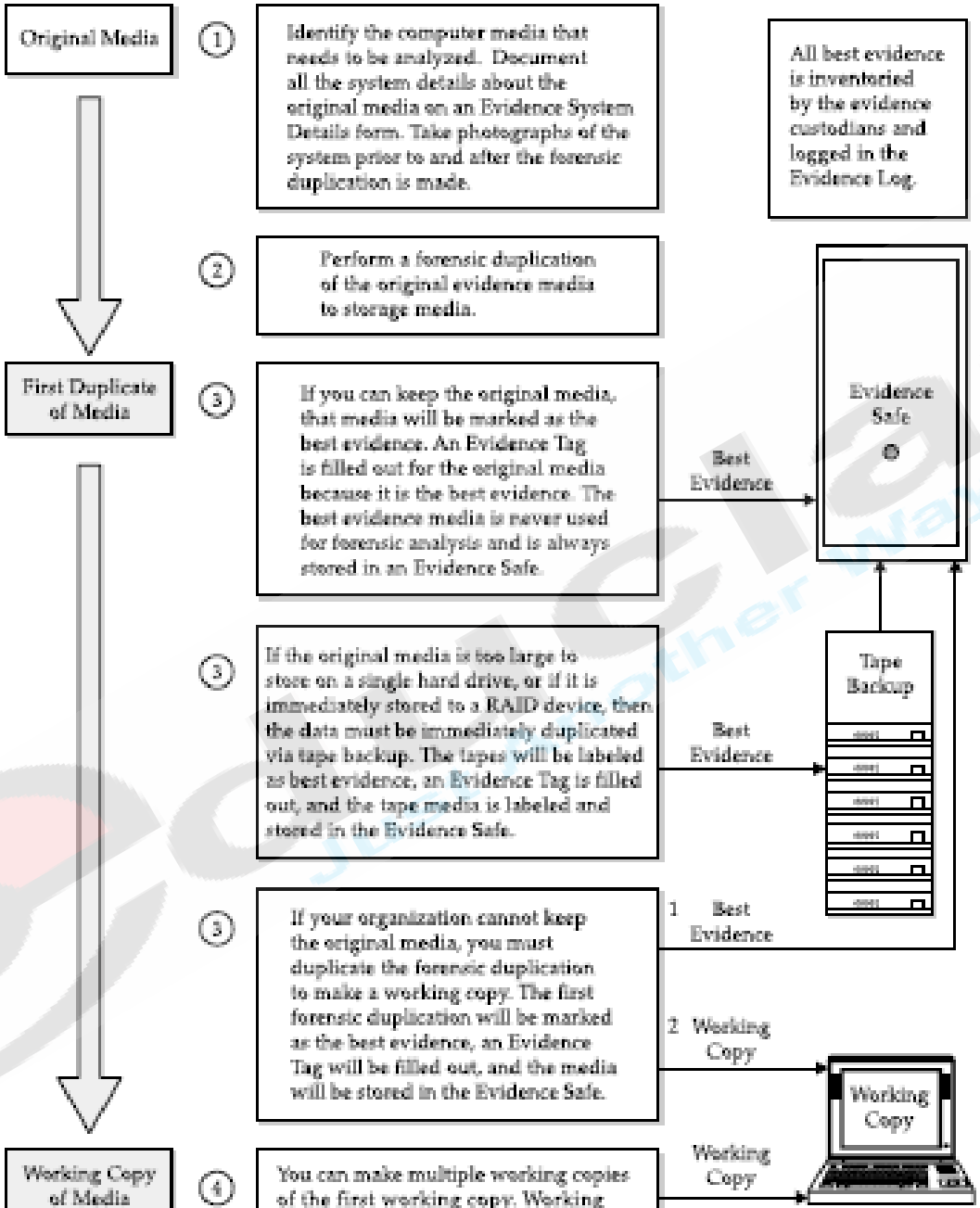
- **Cache** – Cache memory is more temporary than regular RAM. This includes central processor (CPU) cache or any other type of cache used in the system. It typically includes recently used data and information used by applications. It is more volatile than regular RAM because a system has significantly less cache memory than regular RAM so it will likely be overwritten quicker than regular RAM.
- **RAM** – RAM is slightly less volatile than cache memory. It can include information used by the system and network processes. It will be lost if the system is powered down (as will the cache memory).
- **Paging file** – This is also known as the swap file. It is an extension of RAM but it is stored on the hard drive. The paging file is rebuilt each time the system is rebooted so it is more volatile than regular data stored on a hard drive.
- **HDD** – Data stored on a hard disk drive (HDD) is semi-permanent. It remains on the hard drive even after the system is powered down and rebooted.
- **Logs stored on remote systems** – Any data stored on a remote system is less volatile than data stored on the target system. For this reason, many servers send log data to a remote system for centralized collection. Even if the server is completely destroyed, the centralized logs still have key data.
- **Archive media** – This includes any types of backups or copies of data captured for either recovery or archive purposes. They are generally offline and less likely to be destroyed or corrupted. For example, backup tapes and DVDs can be used as archive media.

Evidence Handling Procedures

- When handling evidence during an investigation, you will generally adhere to the following procedures:

1. If examining the contents of a hard drive currently placed within a computer, record information about the computer system under examination.
2. Take digital photographs of the original system and/or media that is being duplicated.
3. Fill out an evidence tag for the original media or for the forensic duplication (whichever hard drive you will keep as best evidence and store in your evidence safe).
4. Label all media appropriately with an evidence label.
5. Store the best evidence copy of the evidence media in your evidence safe.
6. An evidence custodian enters a record of the best evidence into the evidence log. For each piece of best evidence, there will be a corresponding entry in the evidence log.

7. All examinations are performed on a forensic copy of the best evidence, called a *working copy.*
8. An evidence custodian ensures that backup copies of the best evidence are created. The evidence custodian will create tape backups once the principal investigator for the case states that the data will no longer be needed in an expeditious manner.
9. An evidence custodian ensures that all disposition dates are met. The dates of evidence disposition are assigned by the principal investigator.
10. An evidence custodian performs a monthly audit to ensure all of the best evidence is present, properly stored, and labeled.



Evidence System Description

- Before any electronic evidence is gathered, certain data should be recorded regarding the status and identification of the originating computer system. The type of information typically recorded includes the following:

1. Individuals who occupy the office or room where the original evidence is found
2. Individuals who have access to the office or room where the original evidence is found
3. The users who can actually use this system (is it available for use by all users, or do only a select few individuals use it?)
4. Location of the computer in the room
5. State of the system: powered off/on, data on the screen
6. The time/date from the system BIOS
7. Network connections: network, modem
8. Individuals present at the time of the forensic duplication
9. Serial numbers, models, makes of the hard drives and system components
10. Peripherals attached to the system

This form lists the details about the computer system that should be collected.

Digital Photos

- After recording system details (or even prior to this), you may want to take several photographs of the evidence system. There are several reasons for this:

1. To protect your organization/investigators from any claims that you damaged property
2. To ensure you return the system to its exact state prior to forensic duplication
3. To capture the current configuration, such as network connections, modem connections, and other external peripherals

- You may want to take photos of all network and phone connections. You may even take photos specifically of the system serial number and hard drive label.
- Some additional guidelines we follow when taking photos for an incident are:

1. Do not include any people in your photos (if possible).
2. Label placards and place them in each photo to describe exactly what the photo is depicting (room number, name of computer owner, case number, evidence tag number, etc.). This eliminates errors associated with creating a log entry for each photo taken.
3. Keep all photos on the camera related to the case (i.e., do not mix photos of a vacation trip with case photos on the same roll of film or flash media).

Evidence Tags

- All best evidence collected should be labeled in a manner that satisfies federal and state guidelines, at a minimum. Our practice, which supplements the federal guidelines, requires recording the following information for each item we collect:

1. Place or persons from whom the item was received
2. If the item requires permission to search
3. Description of the item(s) taken
4. If the item is a storage device, the information contained within
5. Date and time when the item (evidence) was taken
6. Full name and signature of the individual initially receiving the evidence
7. Case and tag number related to the evidence (for example, if you take three floppy disks from three people, the floppies may be assigned evidence tag numbers 3, 4, and 5)

- We meet the evidence labeling requirements by using *evidence tags. Our evidence tag is* modeled after the one used by many federal law enforcement agencies.
- It provides a record of descriptive data, as well as chain-of-custody data for all evidence obtained.
- Our evidence tag also requires a list of all the people who have possessed the best evidence.
- This list will include the full name, position, and organization of the releaser and receiver; the date and time the evidence was transferred; the reason the evidence was transferred; and any notes on changes to the evidence. In this way, the evidence tag also allows us to meet the chain-of-custody requirements. This information is maintained on the back side of our evidence tag, as shown in fig:

EVIDENCE

Agency _____

Collected By _____

Item # _____ Case # _____

Date _____ Time _____

Description _____

_____

Location _____

_____

Remarks _____

_____

CHAIN OF CUSTODY

Received from _____

By _____

Date _____ Time _____

Received from _____

By _____

Date _____ Time _____

Received from _____

By _____

Date _____ Time _____

Front

Backside

Evidence Labels

- After the evidence tag is created for the best evidence, the evidence should be labeled.
- We use special labels that allow us to erase permanent marker (Sharpie pens), so we place a single label on a hard drive and change its label when needed.
- If labeling the original evidence, we suggest that you actually mark your initials and date on the original drive.
- Most people opt to use a permanent marker, but you could actually scratch your initials on the original evidence media in a discrete location.
- Your goal is to simply mark the evidence so that it is both readily identified as evidence media, and so you can immediately identify who was the individual who retrieved the evidence (for authentication purposes in court).
- After labeling the evidence, place it into an anti-static bag (if computer media), and then put it and its evidence tag in a labeled manila envelope.
- When using an envelope to contain the evidence, at a minimum, the following information must be posted on the exterior of the envelope:
  1. Case number and evidence tag number
  2. Date and time the evidence was collected
  3. A brief description of the items contained within the envelope

Evidence Storage

- The investigator collecting the evidence (and all others who have custody of the items) must maintain positive control of the evidence at all times.
- This requires that consultants working at a client site have a means to store and transport any evidence in a manner that protects the evidence and prevents unauthorized access.
- At the very least, the container must be able to show signs of tampering by parties outside the chain of custody.
- The evidence must also be protected from alteration by the environment. This means that the evidence must not be exposed to possibly damaging electromagnetic fields, or kept in areas of extreme temperatures or conditions.

Evidence Log

- The evidence custodians should receive and store all best evidence for every case your organization investigates.
- When they receive the evidence, the evidence custodians log the receipt of the evidence in the evidence log. A complete inventory of all the evidence contained within the safe should be kept in the evidence log.
- Every time an action is taken for a particular case, the following information should be logged:
  1. Evidence tag number
  2. Date
  3. Action taken
  4. Consultant performing the action
  5. Identifying information for the media being acted upon (for example, transferring the best evidence data to another media or shipping data back to the original owner)
- Therefore, the evidence log contains entries for each case where evidence was collected, following the entire life cycle of the best evidence from initial submission through final disposition.
- We use an Evidence Safe Access Log form for this purpose .
- A copy of this form can be maintained on the side of the evidence safe, since most safes are magnetic.
- The evidence log is stored within the evidence safe.

Working Copies

- Examinations are performed on working copies of the best evidence.
- The working copy does not need to be stored in the evidence safe, unless the case merits additional safeguards for the information.
- If your organization has numerous initial responders that perform forensic duplications and then forward their duplications to an evidence custodian, a good policy is to have those investigators be responsible for making the working copies of the best evidence.
- The only data that needs to be forwarded for storage in your organization's evidence safe is the best evidence.
- This relieves the evidence custodians from the burden of making working copies for analysis and distributing those copies.

Evidence Backups

- You never want to have all your eggs in one basket.
- One of the advantages digital evidence has over other types of physical evidence is that it can be forensically duplicated an infinite number of times.
- One of the disadvantages of digital evidence is that hard drives and electronic equipment may fail.
- Therefore, in order to minimize the malevolent effects of equipment failure or natural disasters, it is prudent to create backups of all electronic evidence.

- The evidence custodians should ensure that there is one tape backup of any best evidence.
- The tape backups will receive their own evidence tag and will be stored in the evidence safe, as if they were best evidence.
- During the custodial audit, the custodians must determine which cases have not yet been backed up, and then perform the necessary backups.
- If a case is not backed up, the evidence custodians must clearly mark it on the Monthly Evidence Custodian Audit form.

Evidence Disposition

- It is often convenient and necessary to practice the disposition of evidence in two stages: **initial disposition and final disposition.**
- *Initial disposition occurs when the final investigative report has been completed and the* analysis, for all practical purposes, is finished. In other words, the forensic expert or the investigator has no outstanding tasks that require the best evidence.
- All media that contained working copies of the evidence should be returned to the evidence custodian to be wiped clean and placed back into the rotation as a clean storage drive. The evidence custodian disposes of the best evidence, but not the tape backup of the best evidence.
- We adhere to a *final disposition of evidence occurring five years from the date a case* was initially opened, unless otherwise directed by law, the court, or some deciding body.
- The disposition date is recorded at the time the evidence is initially logged into the evidence log.
- The final disposition includes the disposal of all tape or CD-ROM backups containing the specified evidence. The date of the final disposition should be recorded on the evidence tag and in the evidence log.

Evidence Custodian Audits

- Evidence custodians should perform a monthly audit to ensure that all best evidence is present, properly stored, and labeled.
- Our monthly audits require the evidence custodians to ensure the readiness of our incident response hardware as well.
- While you're doing this audit, you may also elect to perform a software license inventory for your forensic software and other critical applications We have created the Monthly Evidence Custodian Audit form to foster a timely, accurate, standardized approach to monthly audits.
- This form is merely a checklist that the evidence custodians adhere to when reviewing the evidence safe and readiness of our incident response capability. This checklist ensures that the evidence custodians review the following:

1. Ensure compliance with evidence safe access procedures by reviewing the Evidence Safe Access Log forms.
2. Perform an inventory of the evidence safe, comparing the contents to the evidence log records.
3. Check the disposition requirements of any evidence to determine if evidence can be destroyed.
4. Perform a check to determine if any evidence requires a backup.

5. Ensure the organization has blank, wiped, formatted drives for future cases.
6. Perform an inventory of the EnCase and forensic toolkit dongles.
7. Review the organization's fly-away kits using the Fly-Away Kit Preparation Checklist form.
8. Review all case folders.
9. Replenish the supply of any documents required for incident response and computer forensics.

When a monthly audit has been completed, the most recent Monthly Evidence Custodian Audit form should be stored in a readily found location.

Old copies of the form should be filed appropriately and maintained for over one year. We keep only one copy of our Monthly Evidence Custodian Audit form, and we do not maintain any electronic copies. Some folks may recommend keeping two copies of the Monthly Evidence Custodian Audit forms.

Initial month(s) in which procedure is performed.	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
The Service Department handles account adjustments, maintenance, research and dispute processing for cardholders. **On-Line Transactions**												
1. An on-line system summary of all monetary on-line adjustments and maintenance processed by all Customer Service Department employees is reviewed daily by an employee independent from the input function.												
a. A hard copy print is made of all entries over $XX to review for accuracy. All entries are initialed.												
2. Any request for a PIN, replacement card or convenience balance transfer check received within XX days of an address change must come in writing. The signature is verified and the letter referred to Security.												
3. Requests for credit line increases are completed per approved matrix.												
a. The department's Help Desk performs and documents a random review.												

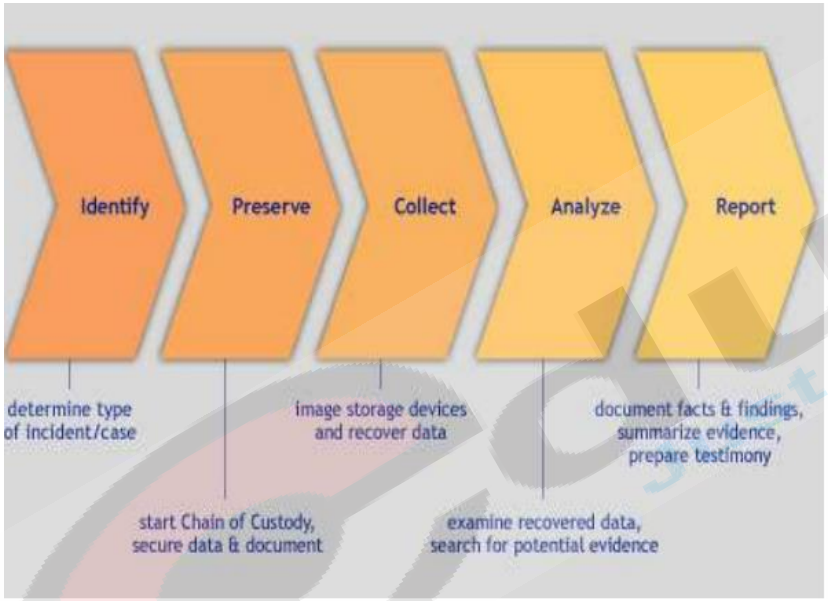
Evidence Safe

- Every organization that collects evidence as a result of any investigation requires an evidence safe.
- The evidence safe (or evidence room, vault, or other designation) prevents tampering or unauthorized access to the documents, data, or physical evidence that may be critical to your case.
- All evidence collected should be kept in the evidence safe.
- This safe should be kept locked at all times, except when it is being accessed by an evidence custodian.
- The combination or access keys to the evidence safe should be known only to the evidence custodians. This helps maintain the chain of custody, since an evidence custodian will be required to access the best evidence whenever it is going to be transferred to an individual.

Shipping Evidence Media

- When you are performing your forensic analysis off-site, you may not be able to hand deliver the best evidence to your organization's evidence custodians
- Therefore, you will evidence custodian for storage, it must be packaged in a tamper-proof, static-proof, padded container and shipped via a carrier that provides tracking capability.
- When shipping evidence, the shipping container must meet the following criteria:
  1. The container must be able to show signs of tampering.
  2. The container must prevent damage to the media therein.
  3. The container must prevent alteration to the media by the environment (electromagnetic fields or extreme temperatures).
- We have purchased hard cases specifically designed to store up to eight hard drives in a protective manner.
- Figure shows an example of a temporary storage case that can be used to transport computer media in a safe manner.

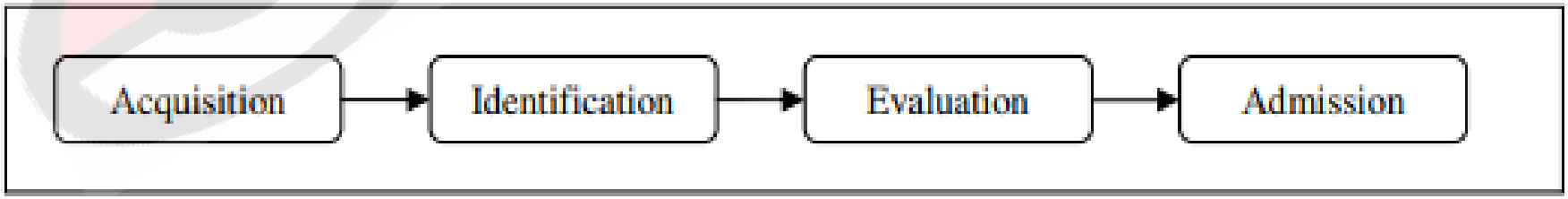
Digital Forensics Process



Stage 1 Investigation preparation	a. identify the purpose of investigation
	b. identify resources required
Stage 2 Evidence acquisition	a. identify sources of digital evidence
	b. preserve digital evidence
Stage 3 Analysis of evidence	a. identify tools and techniques to use
	b. process data
	c. interpret analysis results
Stage 4 Results dissemination	a. report findings
	b. present findings

Computer Forensic Investigative Process

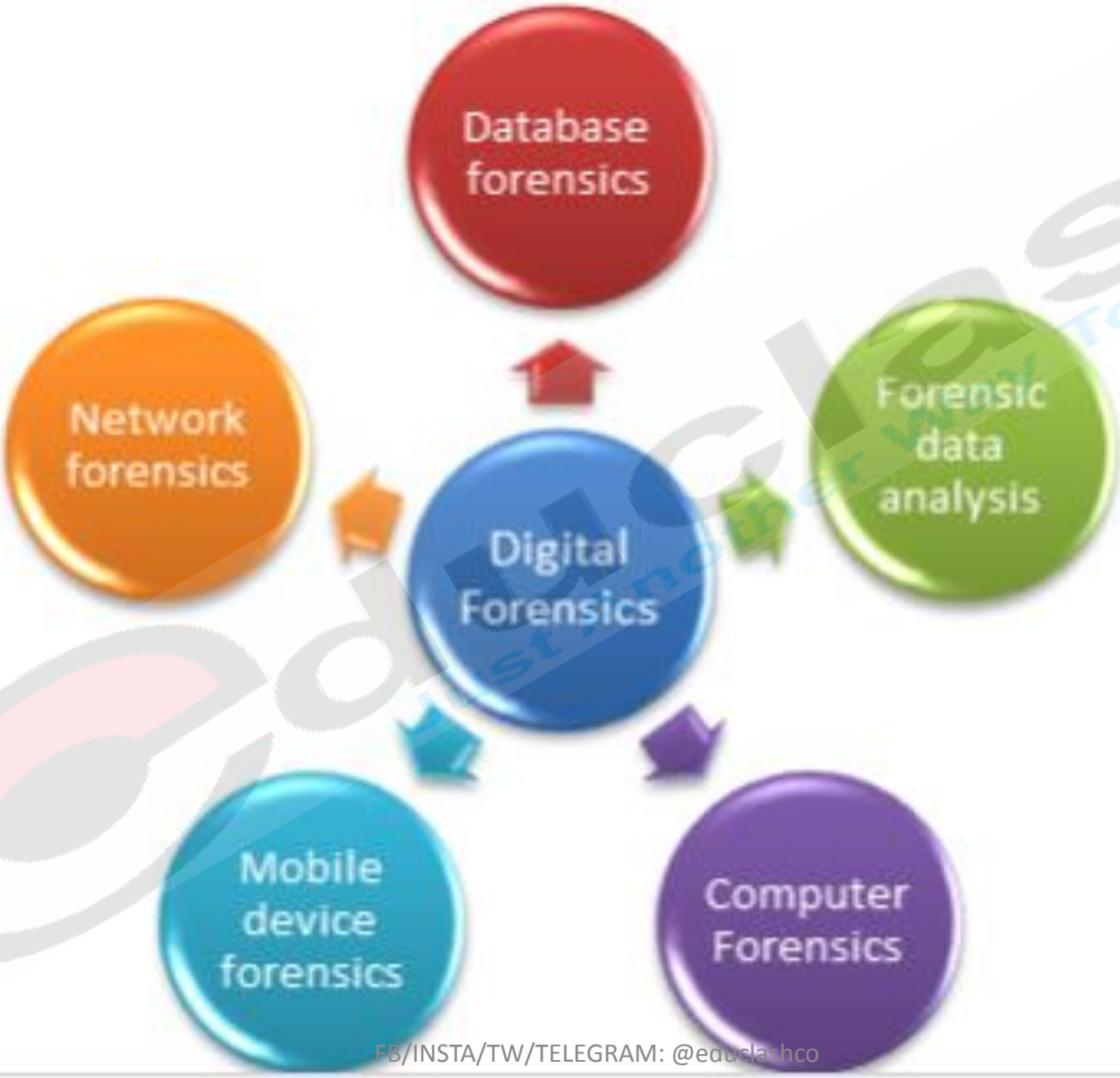
- Pollitt has proposed a methodology for dealing with digital evidence investigation so that the results with be scientifically reliable and legally acceptable. It comprises of 4 distinct phases.
- In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority. It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human. The Evaluation phase comprise of the task to determine whether the components indentified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence. In the final phase, Admission, the acquired & extracted evidence is presented in the court of law.



Types of Digital Forensics

Digital forensics is a constantly evolving scientific field with many sub-disciplines. Some of these sub-disciplines are:

- **Computer Forensics** – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
- **Network Forensics** – the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
- **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.
- **Digital Image Forensics** – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
- **Digital Video/Audio Forensics** – the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
- **Memory forensics** – the recovery of evidence from the RAM of a running computer, also called **live acquisition**.



Types of digital forensics

- **Computer forensics**
  - Reveal the current state of computer system
  - Obtain evidence from various storage medium such as computers, embedded systems, USB pen drives
  - Examine system logs and Internet history.
  - Some of the artifacts we can get from such investigations include:
    - Hidden, deleted, temporary and password-protected files
    - Sensitive documents and spreadsheets
    - File transfer logs
    - Text communication logs
    - Internet browsing history
    - Pictures, graphics, videos and music
    - Checking Event logs and System Logs
    - Checking illegal, pirated or legitimate software installations

- **Mobile device forensics**
  - Recover digital evidence from a mobile device.
  - Investigate call logs and text messages (SMS/Email)
  - Providing location information via GPS or cell site logs
  - Investigate communication stores such as BBM, WhatsApp, WeChat, etc.
  - Artifacts that can be retrieved are:
    - Phone number and service provider information
    - Incoming and outgoing call logs
    - SMS, Emails, IRC(internet relay chat) chat logs
    - Contact details from address books and calendars
    - GPS and location based data

- Network forensics
  - Monitor and analyze LAN/WAN/internet traffic (even at the packet level)
  - Retrieve and analyze logs from a wide variety of sources
  - Determine the extent of intrusion and the amount of data retrieved
- Forensic data analysis
  - Investigation for financial frauds
  - Correlating with financial documents
  - Working closely with Certified Fraud Examiners
- Database forensics
  - Forensic study of databases and their metadata.
  - Investigation on database contents, log files and in-RAM data

Needs of Computer Forensic

- To produce evidence in the court that can lead to the punishment of the actual.
- To ensure the integrity of the computer system.
- To focus on the response to hi-tech offenses, started to intertwine.

Goal of forensic

- The main goal of computer forensic experts is not only to find the criminal but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminal.

- Digital Evidence • “Any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device. It includes a display, print out or other output of that data.”

Types of Digital Evidence

(1) PERSISTANT DATA Meaning data that remains intact when the computer is turned off. E.g. hard drives, disk drives and removable storage devices (such as USB drives or flash drives).

(2) VOLATILE DATA, Meaning data that would be lost if the computer is turned off. E.g. deleted files, computer history, the computer's registry, temporary files and web browsing history.

Who Uses Computer Forensics?

- Criminal Prosecutors
  - Rely on evidence obtained from a computer to prosecute suspects and use as evidence.
- Civil Litigations
  - Personal and business data discovered on a computer can be used in fraud, harassment, or discrimination cases.
- Private Corporations
  - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases.

- Law Enforcement Officials
  - Rely on computer forensics to backup search warrants and post-seizure handling.
- Individual/Private Citizens
  - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

Skills Required For Computer Forensics Application

- Programming or computer-related experience
- Broad understanding of operating systems and applications
- Strong analytical skills
- Strong computer science fundamentals
- Strong system administrative skills
- Knowledge of the latest intruder tools
- Knowledge of cryptography and steganography
- Strong understanding of the rules of evidence and evidence handling