Chap 3 : Digital Forensics

Content

- Digital forensics
  - Introduction
  - History of forensics
  - Rules of Digital Forensics
  - Definition of digital forensics
  - Digital forensics investigation and its rule

- Forensic science plays important role in criminal justice systems.
- Applied to both criminal and civic action.

Scientific tests or techniques used in connection with the detection of crime.

Digital Forensics

"Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices."

PLUS data recovery

Definition for the Masses

"Deleted" information, on almost any kind of digital storage media, is almost never completely "gone"…

Digital Forensics **is the set of tools and techniques to recover this information in a forensically valid way (i.e., acceptable by a court of law)**

- **Objectives of computer forensics**
  - It helps **to recover, analyse, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.**
  - It helps **to represents the motive behind the crime** and **identity of the main culprit**.
  - **Designing procedures** at a suspected crime scene which helps you to ensure **that the digital evidence obtained is not corrupted.**
  - Data acquisition and duplication: **Recovering deleted** files and deleted partitions from digital media to extract the evidence and validate them.

- Helps you **to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim**

- **Producing a computer forensic report** which offers a complete report on the investigation process.

- **Preserving the evidence** by following the chain of custody.

Types of Digital Forensics

- **Disk Forensics:**
  - It deals with **extracting data from storage media** by searching active, modified, or deleted files.
- **Network Forensics:**
  - It is a sub-branch of digital forensics. It is related to **monitoring and analysis of computer network traffic** to collect important information and legal evidence.
- **Wireless Forensics:**
  - It is a division of network forensics. The main aim of wireless forensics is **to offers the tools need to collect and analyse the data from wireless network traffic**.
- **Database Forensics:**
  - It is a branch of digital forensics relating **to the study and examination of databases and their related metadata**.

- **Malware Forensics:**
  - This branch deals **with the identification of malicious code, to study their payload, viruses, worms, etc.**
- **Email Forensics**
  - Deals with **recovery and analysis of emails, including deleted emails, calendars, and contacts**.
- **Memory Forensics:**
  - It deals with collecting data from **system memory** (system registers, cache, RAM) in raw form and then collecting the data from Raw dump.
- **Mobile Phone Forensics:**
  - It mainly deals with the **examination and analysis of mobile devices.** It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

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, divorce, harassment, or discrimination cases
- Insurance Companies
  - **Evidence discovered on computer can be used to mollify costs** (fraud, worker's compensation etc)
- Private Corporations
  - Obtained **evidence from employee computer**s can be used as evidence in harassment, fraud etc. cases

Who Uses Computer Forensics? (cont)

- 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.

Steps Of Computer Forensics

- According to many professionals, Computer Forensics is a four (4) step process
  - **Acquisition**
    - Physically or remotely **obtaining possession** of the computer, all network mappings from the system, and external physical storage devices
  - **Identification**
    - This step involves **identifying what data could be recovered** and **electronically retrieving it** by running various **Computer Forensic tools** and software suites

Steps Of Computer Forensics (cont)

- **Presentation**
  - This step **involves the presentation of evidence discovered in a manner** which is understood by lawyers, non-technically,staff/management, and suitable as evidence as determined by Govt. internal laws
- **Evaluation**
  - Evaluating the information/data recovered to determine if and **how it could be used again the suspect for employment termination or prosecution in court.**

Computer Forensic Requirements

- **Hardware**
  - Familiarity with all internal and external devices/components of a computer
  - Thorough understanding of hard drives and settings
  - Understanding motherboards and the various chipsets used
  - Power connections
  - Memory
- **BIOS**
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

Computer Forensic Requirements (cont)

- **Operation Systems**
  - Windows
  - DOS
  - UNIX
  - LINUX
- **Software**
  - Familiarity with most popular software packages such as Office
- **Forensic Tools**
  - Familiarity with computer forensic techniques and the software packages that could be used

– Example: **ProDiscover Forensic**

- » Is a computer security app that allows you to locate all the data on a computer disk.
- » It can protect evidence and create quality reports for the use of legal procedures.
- » Allows you to extract information jpeg files.
- » You can search for suspicious files quickly.
- » Can create copy of entire suspected disk to keep the original evidence safe.
- » Allows you to see internet history.
- » Allows you to add comments to evidence of your interest.

Evidence Processing Guidelines

- Step 1: Shut down the computer
  - Considerations must be given to volatile information
  - Prevents remote access to machine and destruction of evidence (manual or anti-forensic software)
- Step 2: Document the Hardware Configuration of The System
  - Note everything about the computer configuration prior to re-locating

Evidence Processing Guidelines (cont)

- Step 3: Transport the Computer System to A Secure Location
  - Do not leave the computer unattended unless it is locked in a secure location
- Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks
- Step 5: Mathematically Authenticate Data on All Storage Devices
  - Must be able to prove that you did not alter any of the evidence after the computer came into your possession
- Step 6: Document the System Date and Time
- Step 7: Make a List of Key Search Words
- Step 8: Evaluate the Windows Swap File(hidden files stored with .sys in system drives)

Evidence Processing Guidelines (cont)

- Step 9: Evaluate File Slack
  - File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
  - Example 1, the file system on the hard drive may store data in clusters of four kilobytes. If the computer stores a file that is only two kilobytes in a four kilobyte cluster, there will be two kilobytes of slack space.
  - Example 2, if a user deleted files that filled an entire hard drive cluster, and then saved new files that only filled half of the cluster, the latter half would not necessarily be empty. It may include leftover information from the deleted files. This information could be extracted by forensic investigators using special computer forensic tools.
- Step 10: Evaluate Unallocated Space (Erased Files)

- Step 11: Search Files, File Slack and Unallocated Space for Key Words
- Step 12: Document File Names, Dates and Times
- Step 13: Identify File, Program and Storage Anomalies
- Step 14: Evaluate Program Functionality
- Step 15: Document Your Findings
- Step 16: Retain Copies of Software Used

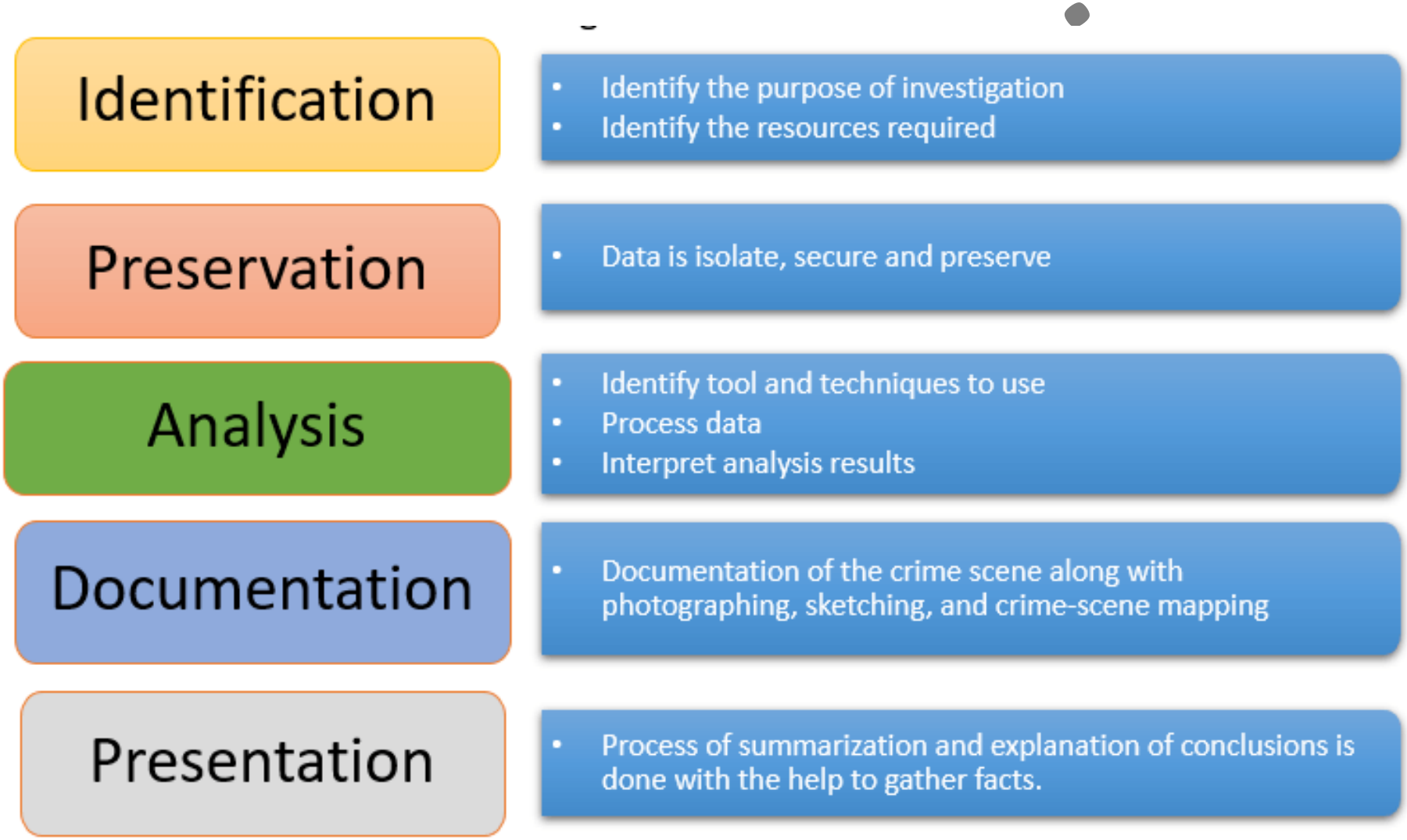
History of Forensics

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 - 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.

- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

Definition of Digital Forensics

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer or cyber crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.



Process of Digital Forensics

- **Identification**
  - It is the first step in the forensic process. **The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).**
  - Electronic storage media can be personal computers, Mobile phones, PDAs, etc.
- **Preservation**
  - In this phase**, data is isolated, secured, and preserved**. It includes **preventing people from using the digital device** so that digital evidence is not tampered with.
- **Analysis**
  - In this step, **investigation agents reconstruct fragments of data and draw conclusions based on evidence found.** However, it might take **numerous iterations of examination** to support a specific crime theory.

- **Documentation**
  - In this process, **a record of all the visible data must be created.** It helps in **recreating the crime scene and reviewing it**. **It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.**
- **Presentation**
  - In this last step, the process of **summarization** and **explanation of conclusions** is done.

Rules of digital Forensic

- Rule 1 : Examination should not be performed on the original media
- Rule 2: A copy is made onto forensically sterile media. New media should always be use if available
- Rule 3: The copy of evidence must be exact, bit by bit copy.
- Rule 4: The computer and data on it must be protected during the acquisition of the data to ensure that data is not modified.

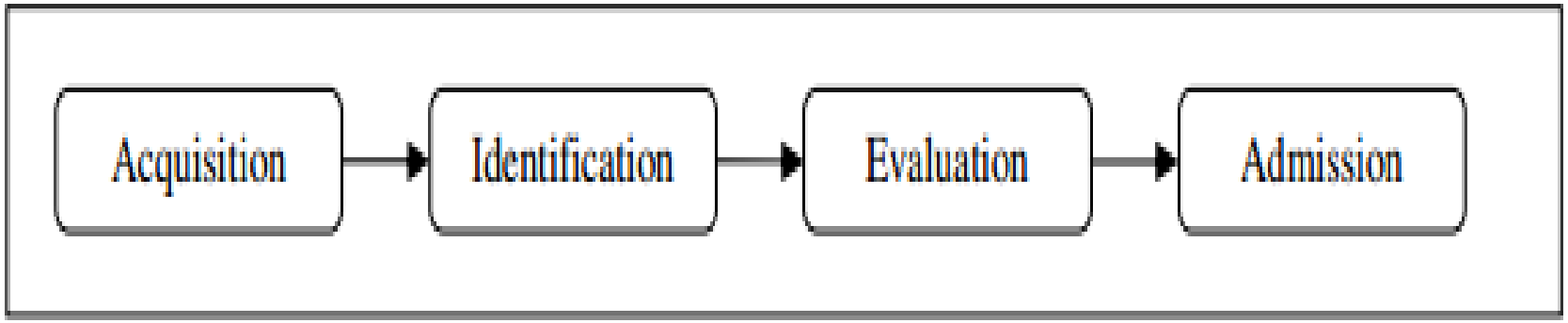
- Rule 5: The examination must be conducted in such a way as to prevent any modification of the evidence.
- Rule 6: The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

Digital Forensics investigation and its Goals

Digital forensic investigation **is a special type of investigation where the scientific procedures and techniques used will be allowed to view the result digital evidence to be admissible in the court of law**.

Computer Forensic Investigative Process

- Back **in 1984, the first methodology was proposed to deal with digital evidence** in a way to remain **scientifically reliable and legally acceptable**.
- The model **proposed was discussed in Proceeding of the National Information Security Conference,** this model consists of **four main** phases.

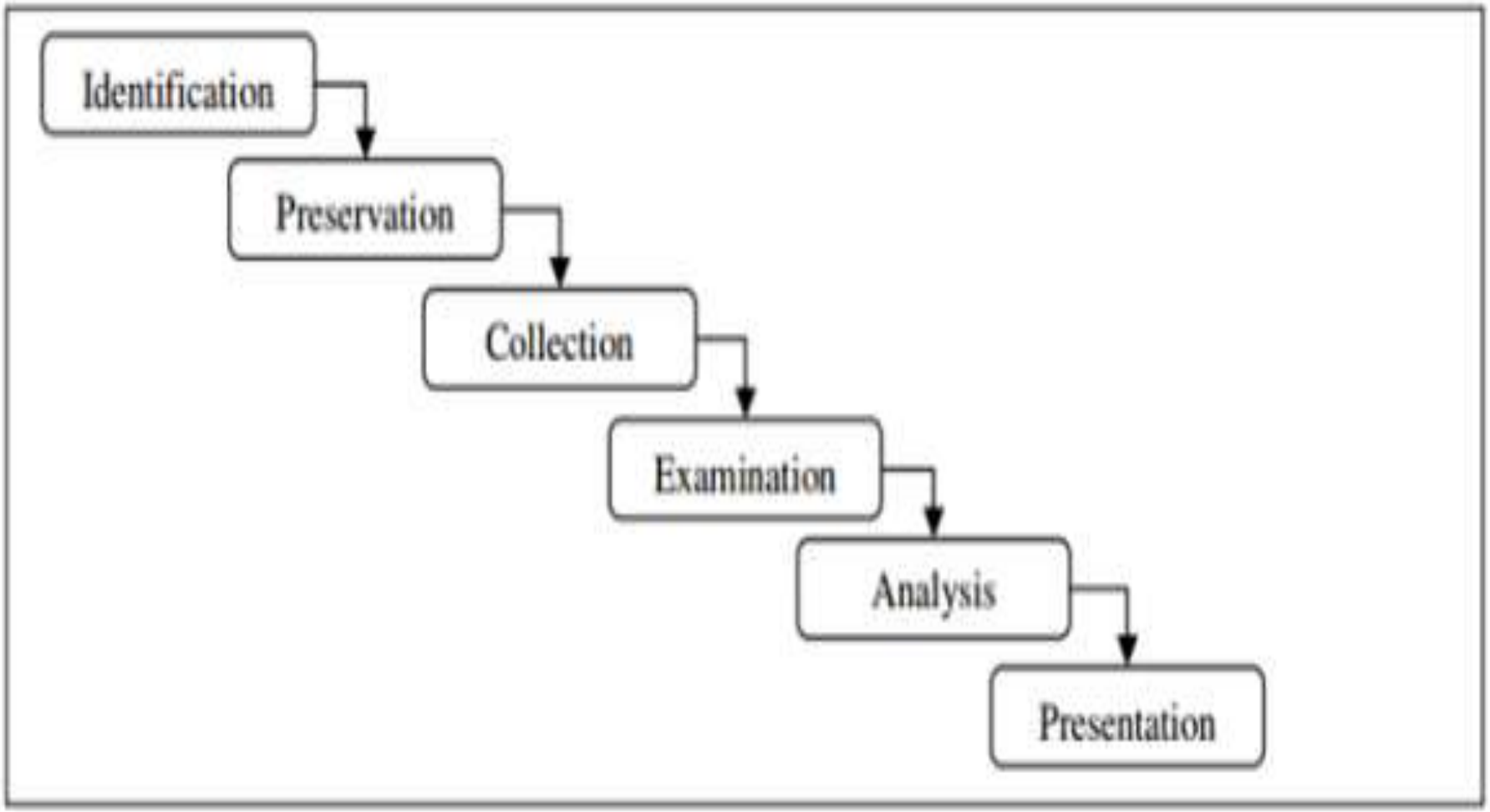


- The first phase is Acquisition, **where evidence is acquired with approval from authorities and in an acceptable manner**
- **Identification:** whereby **all evidence is transformed from digital format to a human understandable format.**
- The Evaluation phase comprises of tasks that **determinate the accuracy of gathered evidence, and if indeed they can be considered as relevant to begin the investigated case.**
- The final step is **Admission** where all extracted evidence is **presented**.

Models of Digital Forensics

- Digital Forensics Research Workshop Group(DFRWS) Investigative Model
- Abstract Digital Forensic Model(ADFM)
- Integrated Digital Investigation Process(IDIP)
- End to End Digital Investigation Process(EEDIP)
- An extended Model for Cybercrime Investigation
- UML Modeling of digital forensic process model(UMDFPM)

DFRWS


Identification
Preservation
Collection
Examination
Analysis
Presentation

- This model was the base fundament of further enhancement since it was very consistent and standardized, the phases namely:
  1. Identification,
  2. Preservation,
  3. Collection,
  4. Examination,
  5. Analysis and
  6. Presentation (then a pseudo additional step: Decision).

- **Identification :** comprises **event or crime detection**, **resolving signature**, **anomalous detection**, **system monitoring, analysis**, etc.

- **Preservation:** in which a **proper case management is set**, **imaging technologies** are used, **and all measurement are taken to ensure an accurate and acceptable chain of custody,** preservation is a guarded principle across all forensic phases.

- **Collection:** comes directly after in which **relevant data is collected based on approved methods**, **software**, and **hardware**; in this step, **we make use also of different recovery techniques and lossless compression**.

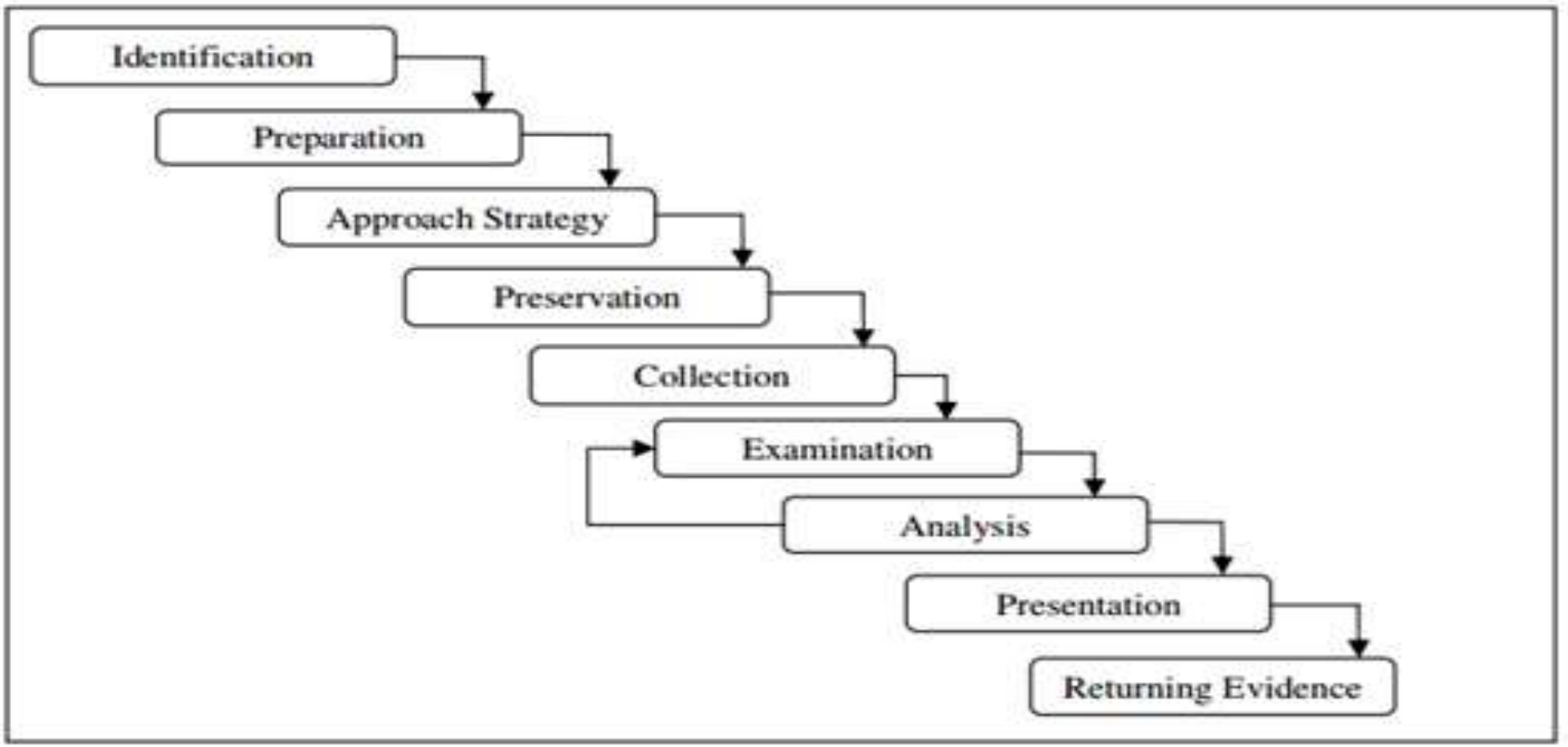
- **Examination and Analysis:** where evidence **traceability, pattern matching are guaranteed,** then **hidden data must be discovered and extracted**, at this point data mining and timeline are performed.

- **Presentation:** Tasks related to this step are **documentation, clarification, mission impact statement, recommendation and countermeasures are taken** and experts testimony.

Abstract Digital Forensics Model (ADFM)

As seen DFRWS Investigative Model was meant to be a generic "technology-independent" model

In 2002 by taking inspiration from DFRWS the new model proposed called Abstract Digital Forensic Model composed of nine phases:



- By this model, the **Identification phase** assumes that the **incident type is well recognized** and **determined**, this is an important step since all upcoming steps depend on it.

- Followed by the **Preparation step**, this is the first introduced step **where tools, techniques, search warrants, monitoring authorization and management support are prepared.**

- Preparation step is followed by the second introduced step **Approach Strategy**, this step is meant **to maximize the collection of the evidence while minimizing the impact on the victim by formulating different approaches and procedures to follow.**

- In the following phase, **Preservation**, **all acquired data must be isolated and secured to keep them in their actual state.**

- **All acquired digital evidence is duplicated, and the physical scene is recorded, based on standardized procedures**, these tasks are performed under the **Collection phase**.

- The next phase is **Examination** whereby an **in-depth systemic analysis is conducted to search the evidence relating to the current case**.

- The **probative value of the examined evidence** is **determined** in Analysis phase.

- The following step is **Presentation** where a **summary of the process is developed**

- **Returning Evidence** that **closes the investigation process by returning physical and digital evidence to the proper owner**.

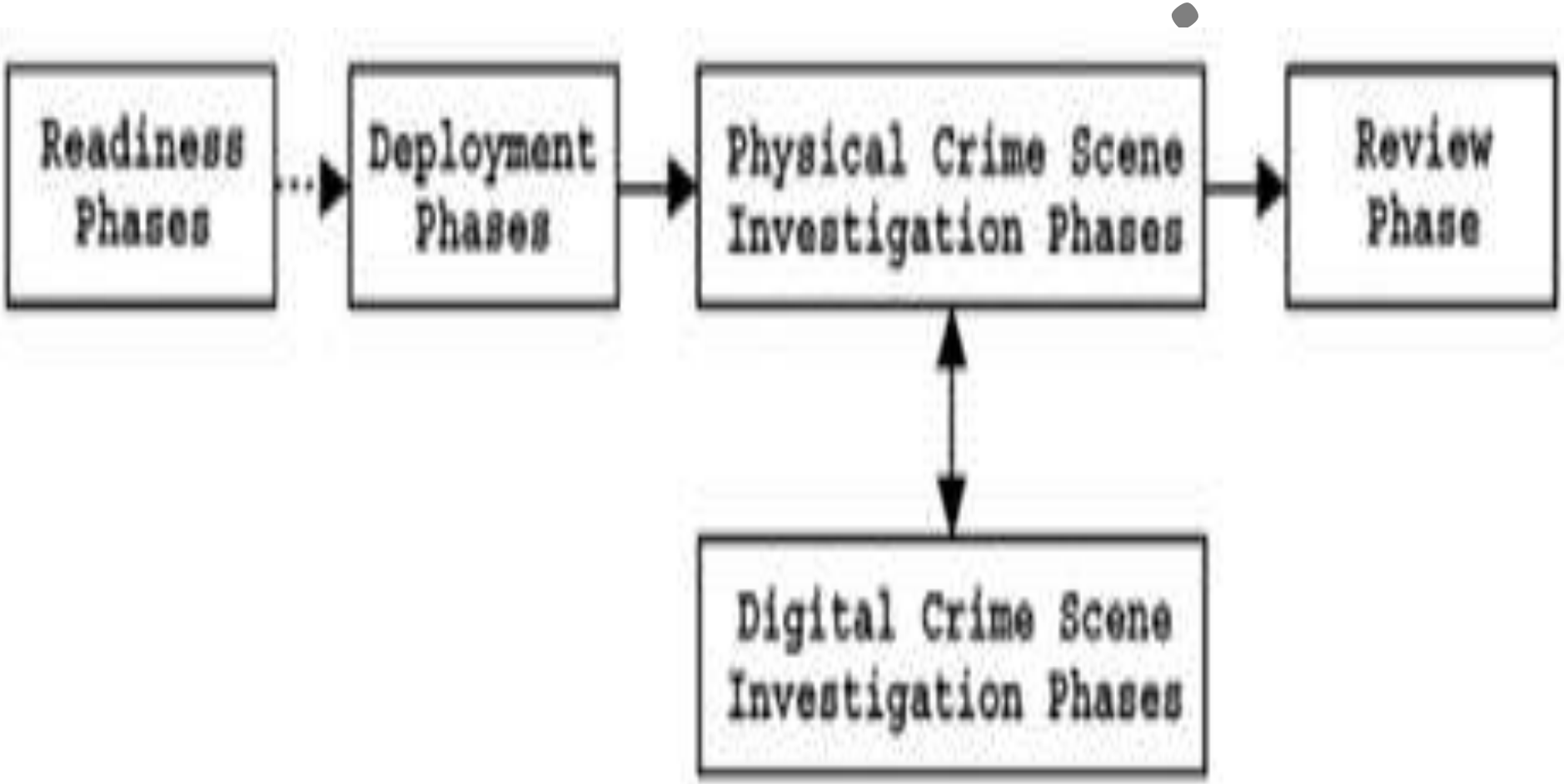
- The most important value that added this model (in contrast with DFRWS Investigative Model) **consists of a comprehensive pre and post investigation procedures**.

Integrated Digital Investigation Process (IDIP)

- The model was first proposed by Carrier and Spafford in 2003, **the goal was to "integrate" all available models and investigative procedures.**

- The effort was held to map the **digital investigative process to the physical investigative one**.

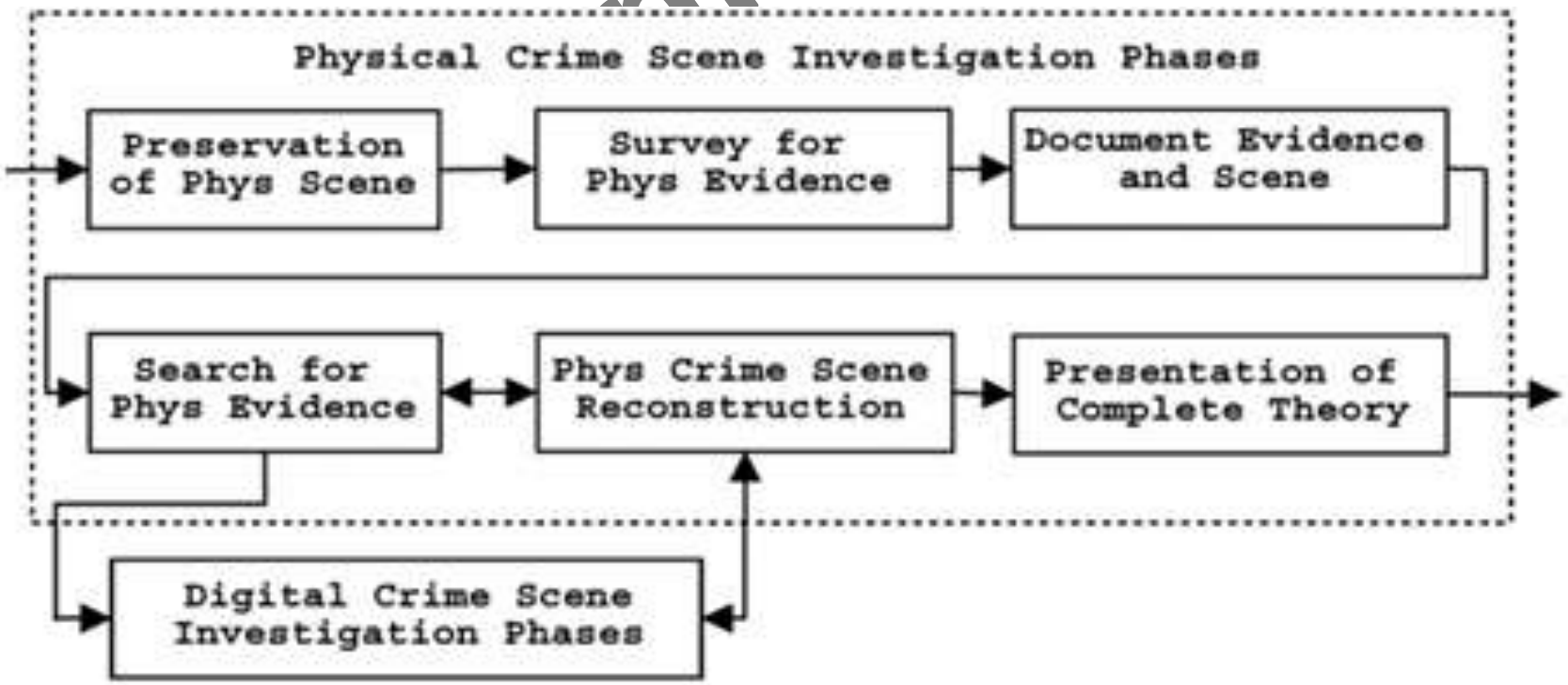
- The model itself is quite big since it organized into **five groups consisting of 17 phases**.


Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

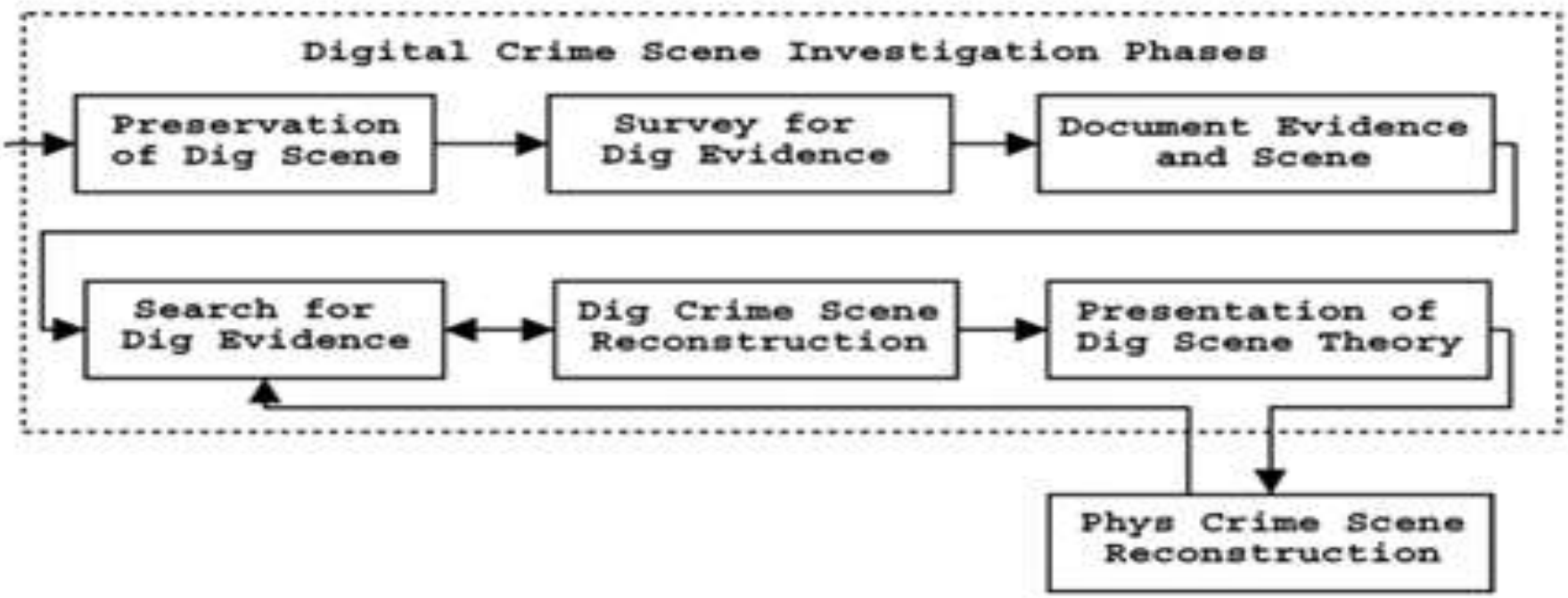
- The model starts with the **Readiness phase**, which **ensures that we are fully able to support fully the investigation**
  - **operations readiness**, a phase in which we provide **all training and equipment for investigators**
  - **infrastructure readiness** phase that ensures that the **needed data exists**.

- This is followed by the **Deployment phase**, a phase where **we provide mechanisms for an incident to be detected and confirmed**, this phase consists of
  - **detection and notification**
  - **then confirmation and authorization phases**.

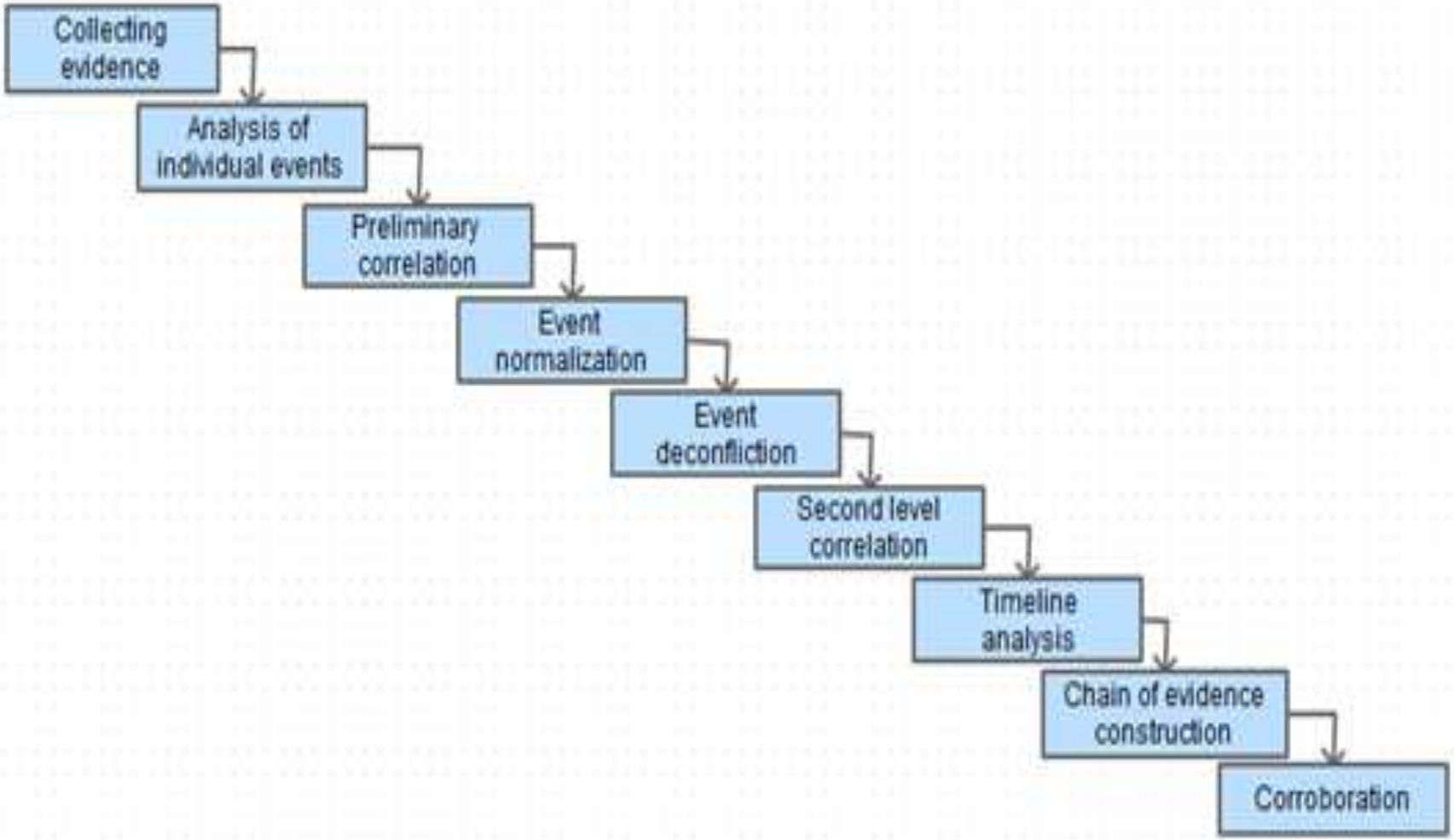
- Followed immediately by **Physical Crime Scene Investigation phase** where **we collect and analyze physical evidence**, this is meant **to reproduce the actions that took place during the incident**, this phase consists of six phases as shown below:



- After this comes the **Digital Crime Scene Investigation phase**, this model consider **each digital device as a separate crime scene**, this phase **ensure the collection of all electronic evidence**, and just like the previous, this phase contains **six 'identical' phases**:



End to End Digital Investigation



- By the same year, that is, 2003, **Peter Stephenson** (Stephenson, P. (2003). A Comprehensive Approach to Digital Incident Investigation.) **reviews the DFRWS framework and translated it into a "more" practical investigative process dubbed End-To-End Digital Investigation process (EEDI)** by extending the existing **process into nine stages**
- End-to-end because Stephenson in his model considers that ***"every digital crime has a source point, a destination point and a path between those two points"*.**

- This model **defines critical steps to do** in order **to correctly preserve, collect and analyse digital evidence.**
- **Collection of Evidence: primary and secondary evidences are collected and taken in their respective contexts**. The context here is more related to events time sensitivity
- **Analysis of Individual event**: each **individual event is isolated and analysed separately** to determine **how it can tie with other events and the potential value it can add or they can add to the overall investigation**.

- **Preliminary Correlation: individual events are linked** with each other to determine a primary chain of evidence in order to **determine what happened, when, and which devices was involved.**

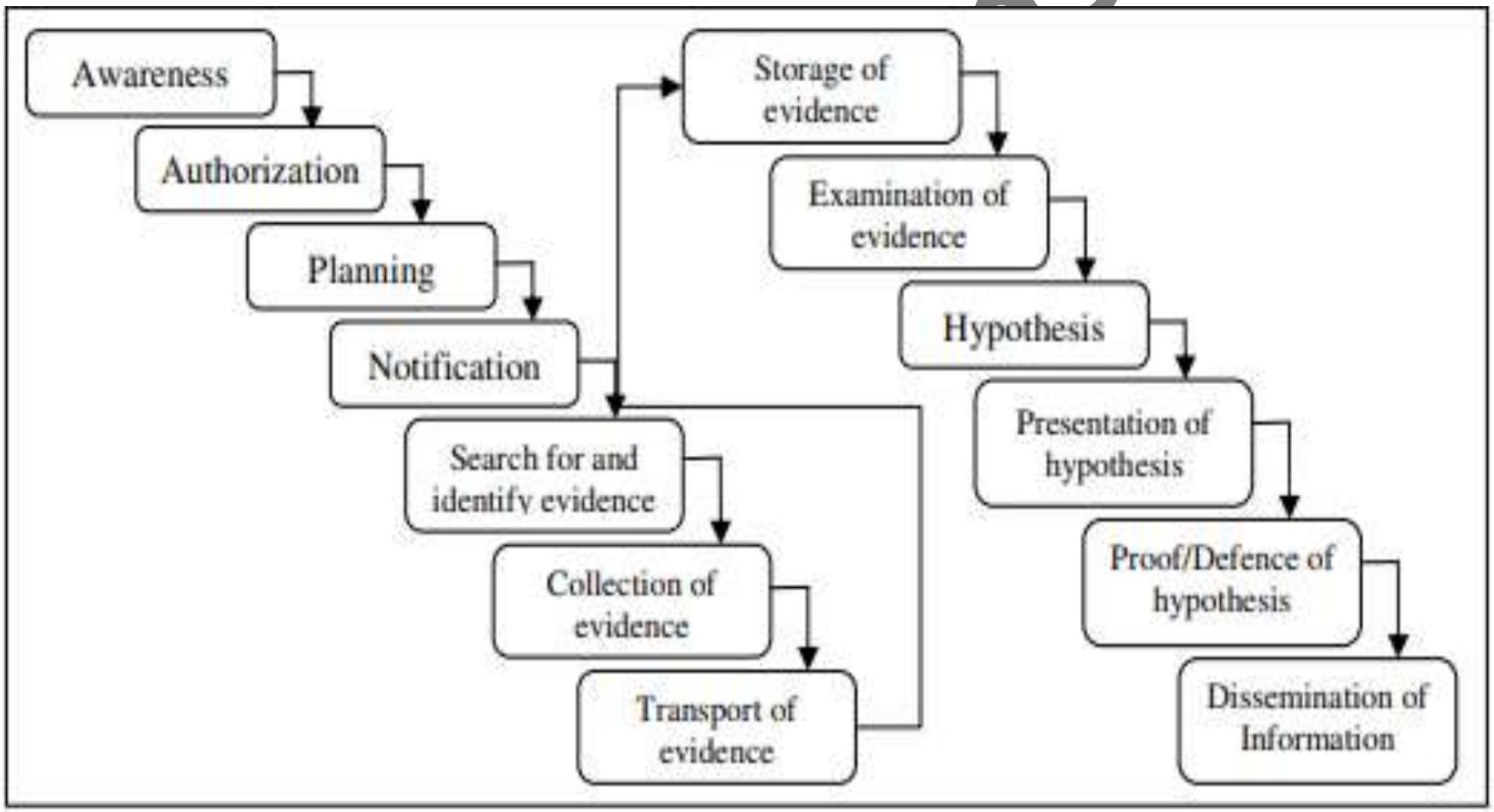
- **Event Normalization** :aims to **remove redundancy in evidentiary data** assuming that the same events could be reported separately from different sources using multiple vocabularies.

- As an extension to the normalization, **whatever how and from where they was reported, the same evidentiary events are combined into one evidentiary event** in the **Event De confliction** step; **at this stage all events and evidentiary events are refined** and a **Second-Level Correlation** can be performed.
- The previously outlined **steps result in timeline which is defined** in the **Timeline Analysis** step, the **timeline analysis is an iterative task which lasts as the investigation lasts**.

- The **Construction of a Chain of Evidence** can begin **based on the result of timeline of events, theoretically,** a **coherent chain is developed when each evident will lead to the other and this is what is meant to be done in this step.**

- The last phase of this model is **Corroboration**, where **digital investigator support, strengthen and confirm each evidence, within the chain of evidence previously developed ,with other independent or traditional events** and evidence collected in the case of conducted digital forensic investigation is in support of a group of investigators outside the digital forensic unit.

Extended Model of Cybercrime Investigation



- **Awareness**
  - The first step in an investigation is the **creation of an awareness that investigation is needed**.
  - This awareness is typically created by **events external to the organisation which will carry out the investigation**, e.g. a crime is reported to the police or an auditor is requested to perform an audit. It may **also result from internal events**, e.g. an intrusion detection system alerts a system administrator that a system's security has been compromised.

- Most **earlier models do not explicitly show this activity**, this is a **weakness** of such models because the events causing the investigation may significantly influence the type of investigation required

Authorisation:

- After the need for an investigation is identified, the next activity is to obtain authorisation to carry it out.
- **require interaction with both external and internal entities to** obtain the necessary authorisation.
- The **level of formal structure** associated with authorisation **varies considerably, depending on the type of investigation**.
- At one extreme, **a system administrator may require only a simple verbal approval from company management to carry out a detailed investigation of the company's computer systems**;
- At the other extreme, **law enforcement agencies usually require formal legal authorisation setting out in precise detail what is permitted in an investigation** (e.g. court orders or warrants).

Planning

- The planning activity is strongly **influenced by information from both inside and outside the investigating organisation**.
- From **outside**, the plans will be **influenced by regulations and legislation** which **set the general context of the investigation** and **which are not under the control of the investigators**.
- There will also be **information collected by the investigators from other external sources**.
- From **within the organisation**, **there will be the organisation's own strategies**, **policies, and information about previous investigations.**
- The planning activity **may give rise to a need to backtrack and obtain further authorisation**, for example when the scope of the investigation is found to be larger than the original information showed.

Notification

- Notification in this model refers to **informing the subject of an investigation or other concerned parties that the investigation is taking place**.
- This activity may **not be appropriate in some investigations**, e.g. where surprise is needed to prevent destruction of evidence.

Search and Identification of Evidence

- This activity **deals with locating the evidence and identifying** what it is for the next activity.
- In the simplest case, this **may involve finding the computer used by a suspect and confirming that it is the one of interest to the investigators.**
- However, in more complex environments this activity may not be straightforward; e.g. it may require tracing computers through multiple ISPs and possibly in other countries based on knowledge of an IP address.

Collection

- Collection is the activity in which **the investigating organisation takes possession of the evidence in a form which can be preserved and analysed, e.g. imaging of hard disks or seizure of entire computers.**
- Errors or poor practices at this stage may render the evidence useless, particularly in investigations which are subject to strict legal requirements.

Transport

- Following collection, **evidence must be transported to a suitable location for later examination**.
- This could be
  - simply the **physical transfer** of seized computers to a safe location
  - **transmission of data through networks**.

It is important to **ensure during transport that the evidence remains valid for later use**, i.e. that the means of transport used does not affect the integrity of the evidence.

Storage

- The collected evidence will in most cases need to be stored because examination cannot take place immediately. **Storage must take into account the need to preserve the integrity of the evidence.**

Examination

- Examination of the evidence will involve the use of a potentially large number of **techniques to find and interpret significant data**.
- Depending on the outcomes of the search/identification and collection activities, there may be very large volumes of data to be examined so **automated techniques to support the investigator are required**.

Hypothesis

- Based on the examination of the evidence, the investigators must construct **a hypothesis of what occurred.**

- The **degree of formality of this hypothesis depends on the type of investigation**.

- For example, **a police investigation will result in the preparation of a detailed hypothesis with carefully documented supporting material from the examination, suitable for use in court**.

- An internal investigation by a company's systems administrator will result **in a less formal report to management.**

Presentation

- The hypothesis must be presented to persons other than the investigators.

- For **a police** investigation the **hypothesis will be placed before a jury**

- While an **internal company investigation** will place the **hypothesis before management for a decision on action to be taken**.

Proof/Defence

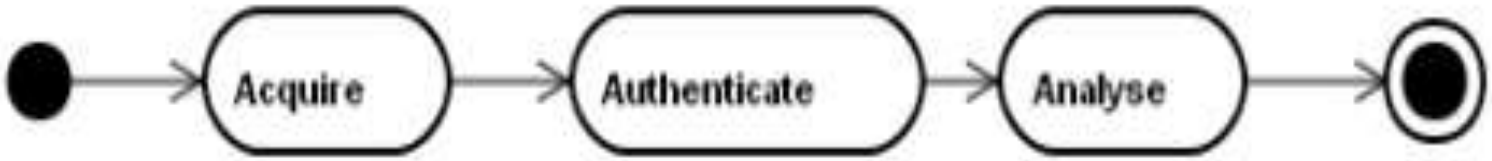
- In general the hypothesis will not go unchallenged; a contrary hypothesis and **supporting evidence will be placed before a jury**, for example.
- The investigators will have **to prove the validity of their hypothesis and defend it against criticism and challenge**. Successful challenges will probably result in backtracking to the earlier stages to obtain and examine more evidence, and **construct a better hypothesis.**

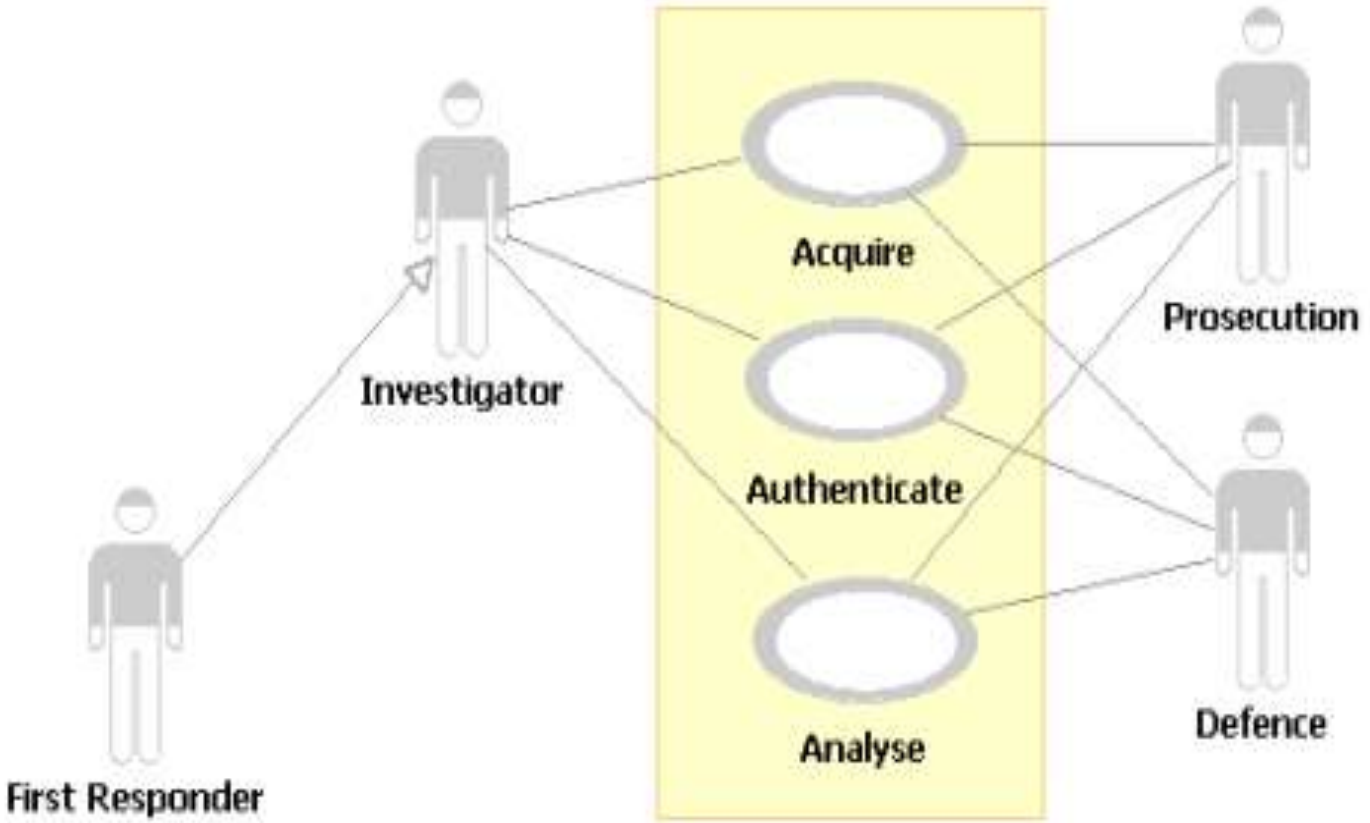
Dissemination

- The **final activity** in the model is the dissemination of information from the investigation.
- **Some information** may be made **available only within** the **investigating organisation**, while **other** information may be **more widely disseminated**.
- Policies and procedures will normally be in place which determine the details.
- The information will influence future investigations and may also influence the policies and procedures.

UML Modeling of digital forensic process model(UMDFPM)

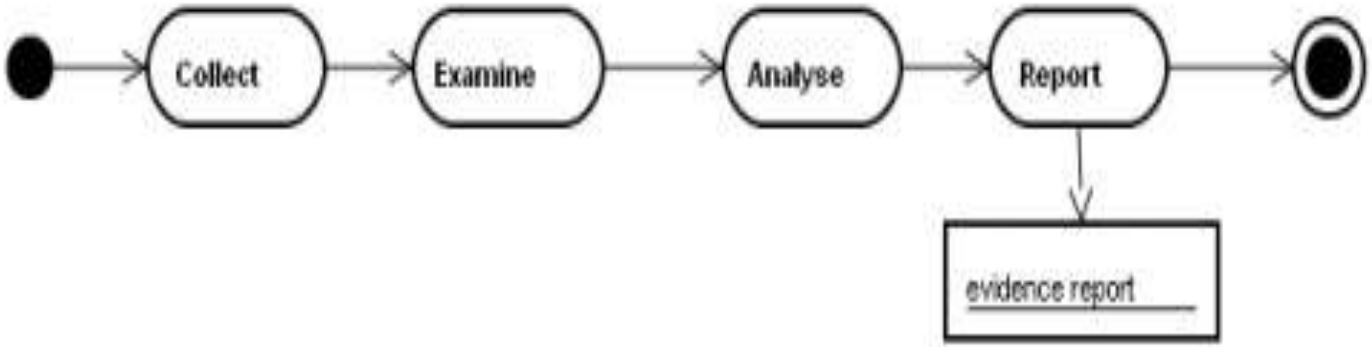
The Kruse DFPM Activity diagram

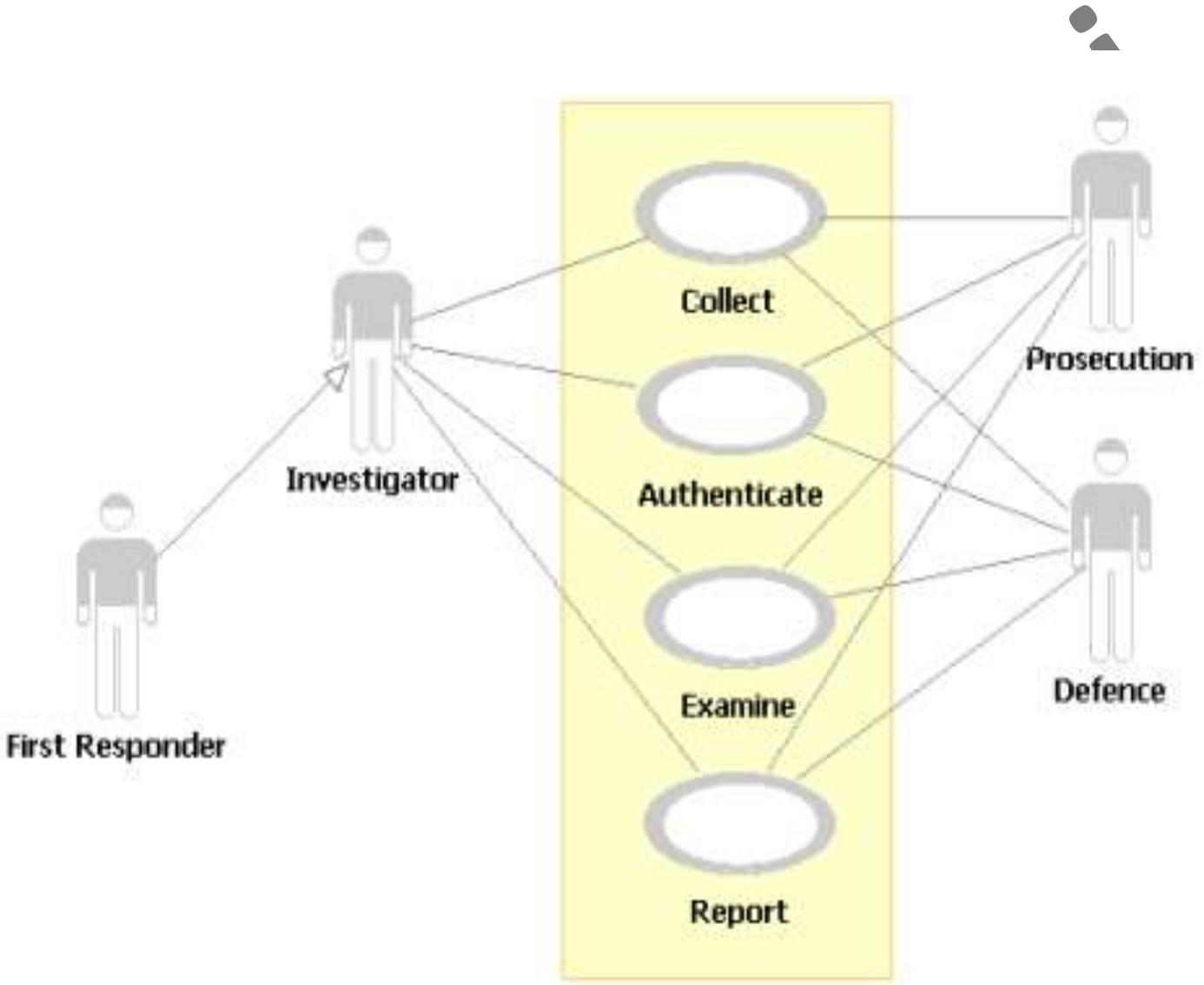




Kruse Use Case Diagram

The Activity Diagram of the USDOJ DFPM




Collect
Authenticate
Examine
Report
Investigator
First Responder
Prosecution
Defence

GOAL

- Properly investigate and assist in the prosecution of cases involving digital evidence.
- Preserve the integrity of seized digital evidence.
- Provide expert testimony in court.
- Act as an educational and training resource for the community.

Ethical issues in digital forensic

- Ethics in DF can be defined as set of moral principles that regulate the use of computers.
- Ethical decision making in DF work comprises of one or more of the following:
  - Honesty toward the investigation
  - Carefully handling the digital evidences
  - Compliance with the law and professional norms.

General Ethic Norms for instigator

- **Investigation should satisfy the following points:**
  - To contribute to the society and human being
  - To avoid harm to other
  - TO be honest and trustworthy
  - To be fair and take action not to discriminate
  - To honor property rights, including copyrights and patents.
  - To respect the privacy of others.
  - To honor confidentiality.

Unethical norms for Digital Forensics Investigation

- Investigator should not:
  - Uphold any relevant evidence
  - Declare any confidential matter or knowledge
  - Express an opinion on the guilt or innocence belonging to any party
  - Engage or involve in any kind of unethical or illegal conduct
  - Display bias or prejudice in findings or observation
  - Exceed authorization in conducting examination.

MCQ's

- Computers can play the following roles in a crime:

a. Target, object, and subject
b. Evidence, instrumentality, contraband, or fruit of crime
c. Object, evidence, and tool
d. Symbol, instrumentality, and source of evidence

b.Evidence, instrumentality, contraband, or fruit of crime

- The first US law to address computer crime was:

a. Computer Fraud and Abuse Act (CFAA)
b. Florida Computer Crime Act
c. Computer Abuse Act
d. None of the above

b.Florida Computer Crime Act

- The following specializations exist in digital investigations:

a. First responder (a.k.a. digital crime scene technician)

b. Forensic examiner

c. Digital investigator

d. All of the above

d. All of the above

- One of the most common approaches to validating forensic software is to:

a. Examine the source code

b. Ask others if the software is reliable

c. Compare results of multiple tools for discrepancies

d. Computer forensic tool testing projects

- c. Compare results of multiple tools for discrepancies

- An instrumentality of a crime is:

a. An instrument used to commit a crime

b. A weapon or tool designed to commit a crime

c. Anything that plays a significant role in a crime

d. All of the above

- d. All of the above

- Phone company records are an example of:

a. Hardware as contraband or fruits of crime

b. Information as contraband or fruits of crime

c. Information as an instrumentality

d. Information as evidence

- d. Information as evidence

- In the course of conducting forensic analysis, which of the following actions are carried out?
    a. Critical thinking
    b. Fusion
    c. Validation
    d. All of the above

- d. All of the above

- A single crime can fall into more than one of the following categories: hardware or information as evidence, instrumentality, and fruits of crime.

a. True

b. False

- a. True

- The American Society of Crime Laboratory Directors (ASCLD) is the only group to establish guidelines for how digital evidence is handled in crime labs.

a. True

b. False

- b. False

- A network can be an instrumentality of a crime.

a. True

b. False

- True

- There is a general agreement as to the meaning of the term “computer crime.”

a. True

b. False

- False

- When a computer contains only a few pieces of digital evidence, investigators are authorized to collect the entire computer.

a. True
b. False

- False

- . The terms “forensic examination” and “forensic analysis” are the same, and can be used interchangeably.

a. True

b. False

- b. False

According to the text, the most common mistake that prevents evidence seized from being admitted is:

a. Uninformed consent
b. Forcible entry
c. Obtained without authorization
d. None of the above

- Obtained without authorization

- The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:

a. Chain of custody

b. Field notes

c. Interim report

d. None of the above

- Chain of custody

- Direct evidence establishes a:

a. Fact

b. Assumption

c. Error

d. Line of inquiry

- Fact

- There is no need for any specialized training in the collection of digital evidence.

a. True

b. False

- False

- It is the duty of a digital investigator to ignore influences from any source.

a. True

b. False

- True

- Determining whether digital evidence has been tampered with is a major concern of the digital examiner.

a. True

b. False

- a. True

- The term “computer contaminant” refers to:

a. Excessive dust found inside the computer case

b. Viruses, worms, and other malware

c. Spam e-mails

d. None

- b. Viruses, worms, and other malware