BASICS OF DIGITAL FORENSICS

Module I

Prof. Yogesh Jayant Gaikwad
yogesh.gaikwad@mitwpu.edu.in

What is Digital Forensics?

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

History of Digital 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.

Objectives of computer forensics

Here are the essential objectives of using Computer forensics:

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

- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Models of Digital Forensic Investigation

Road map for Digital Forensics Research(RMDFR)

The research roadmap digital forensic framework composed of six main phases:

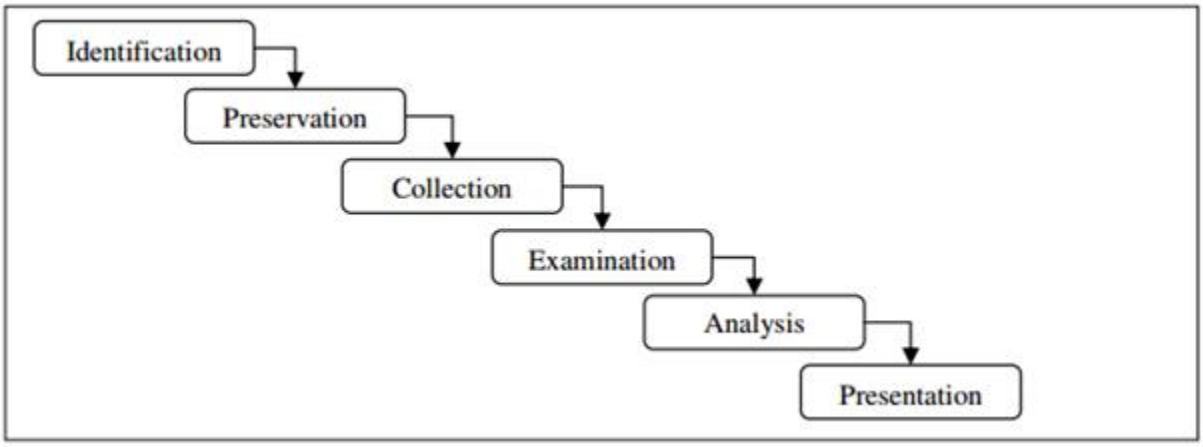


Figure 1 DFRWS Investigative Model

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

Each phase consists of some candidate techniques or methods.

1. The first is Identification and comprises event or crime detection, resolving signature, anomalous detection, system monitoring, audit analysis, etc.
2. Followed by Preservation step 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.
3. 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.
4. Following this step are two interesting and very crucial phases, Examination and Analysis, whereby evidence traceability, pattern matching are guaranteed,

then hidden data must be discovered and extracted, at this point data mining and timeline are performed.

5. The last phase of this model is 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, and in 2002 Mark Reith, Clint Carr, and Gregg Gunsch was inspired from DFRWS and presented the Abstract Digital Forensic Model an enhanced model composed of nine phases:

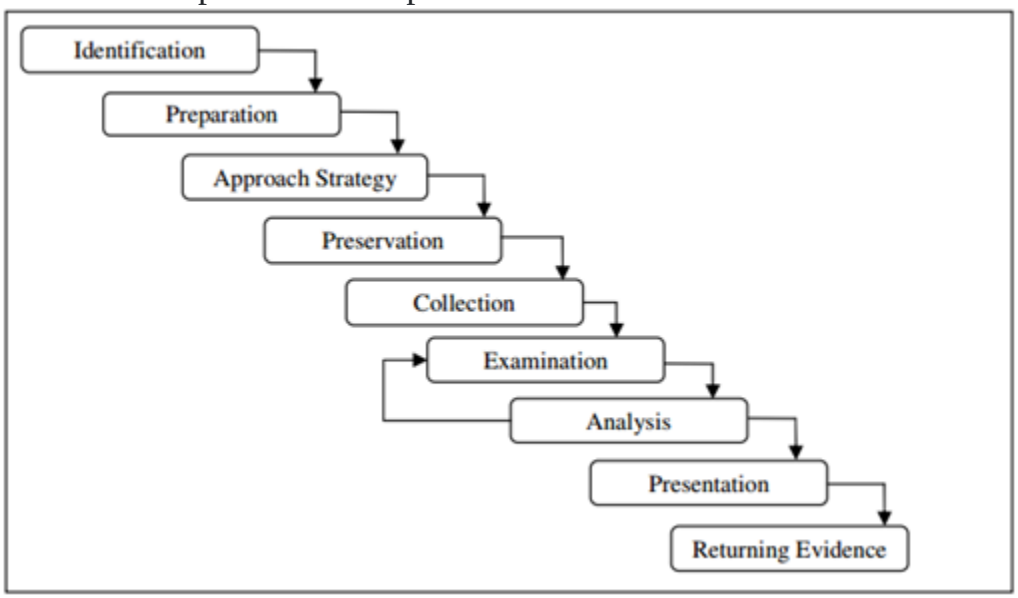


Figure 2 Abstract Digital Forensics Model (ADFM)

1. An **Identification phase** assumes that the incident type is well recognized and determined, this is an important step since all upcoming steps depend on it.
2. Followed by the **Preparation phase**, this is the first introduced step where tools, techniques, search warrants, monitoring authorization and management support are prepared,
3. This step is followed by the second introduced **Approach Strategy phase**, this phase is meant to maximize the collection of the evidence while minimizing the impact on the victim by formulating different approaches and procedures to follow.
4. In the **Preservation phase**, all acquired data must be isolated and secured to keep them in their actual state.

5. All acquired digital evidence is duplicated, and the physical scene is recorded, based on standardized procedures, these tasks are performed under the **Collection phase**.
6. The next phase is **Examination** whereby an in-depth systemic analysis is conducted to search the evidence relating to the current case.
7. The probative value of the examined evidence is determined in **Analysis phase**.
8. The following **Presentation phase** where a summary of the process is developed,
9. Then comes the third introduced step: **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.

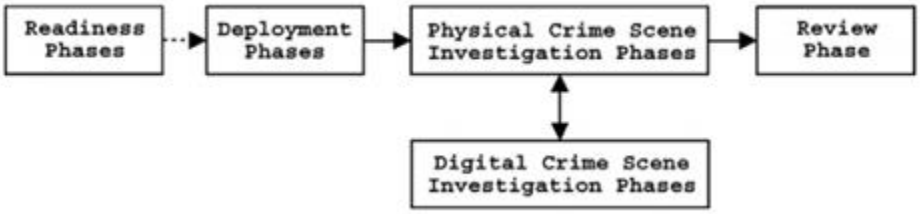
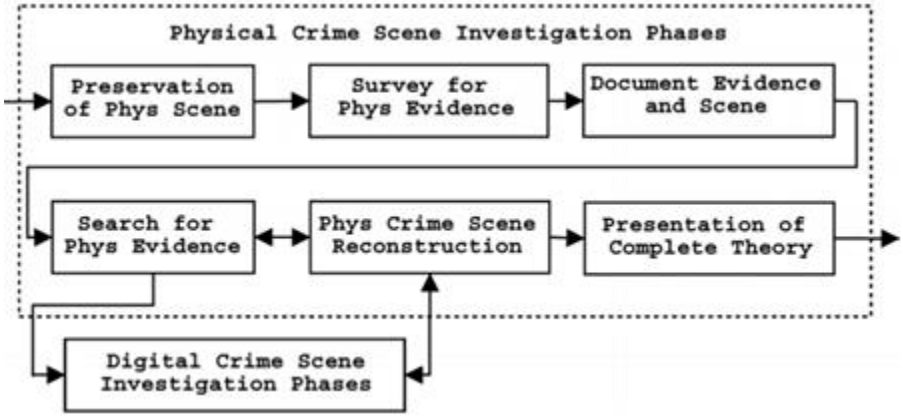


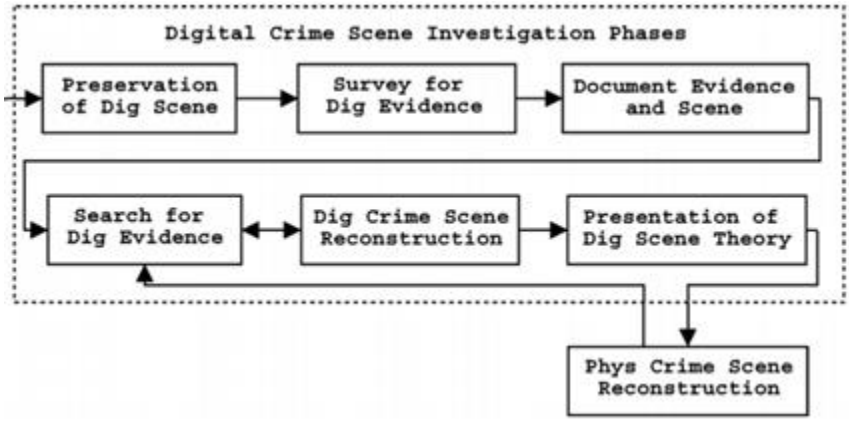
Figure 3 The five groups of phases in the IDIP model

1. The model starts with the **Readiness phase**, which ensures that we are fully able to support fully the investigation (including *operations readiness*, a phase in which we provide all training and equipment for investigators; and *infrastructure readiness* phase that ensures that the needed data exists).
2. 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.
3. 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:



Both phases include Preservation, Survey for Physical/Digital Evidence, Document Evidence and Scene, Search for Physical/Digital evidence, Physical/Digital Crime Scene Reconstruction and Presentation of Physical/Digital Scene Theory. The latest phase of the model is the Review phase in which the whole process is reviewed to find points of improvements and to identify new procedures or new training requirements.

What is the EEDI

The premise of the framework takes into count that **"every digital crime has a source point, a destination point and a path between those two points"**

(Stephenson, Getting the Whole Picture, 2002, 2003). This means EEDI takes into account the source of the incident, destination of the incident, and all the intermediate devices along the path through the network.

EEDI is a **"structured method of collecting evidence along the entire path from source to target, using each piece of evidence in that chain to corroborate other evidence (either digitally or traditionally developed) and an approach to presenting the completed chain effectively in court"** (Stephenson, Getting the Whole Picture, 2002, 2003).

The EEDI process consists of the following nine activities:

1. **Collecting evidence**
2. **Analysis of individual events**
3. **Preliminary correlation**
4. **Event normalization**
5. **Event deconfliction**
6. **Second level correlation**
7. **Timeline analysis**
8. **Chain of evidence construction**
9. **Corroboration**

1. Collecting Evidence

EEDI helped with the issue raised during the Identification and Collection phases. This issue was scoping an investigation to determine the systems involved and the data sources with potential evidentiary items. It has found the approach of viewing each case as having a source point, destination point, and a path between them to be effective when identifying the scope of an investigation.

Take the previous example of a person accessing a file. The source point is the computer the person is using, the destination point is the computer storing the file being accessed, and the path is the network between those two computers.
Following this path can help you identify the data sources with potential evidentiary items which needs to be collected.

2. Analysis of Individual Events

"This analysis step examines isolated events and assesses what value they may have to the overall investigation and how they may tie into each other" (Stephenson, Cyber Investigation, 2009). EEDI is framework to investigate security incidents so this activity's focus is on the examination of each event in a security incident. The example below shows a few examination steps for examining a computer's hard drive:

*** Analysis of individual events (or individual case)**
*** System examination**
*** Examination of volatile data**
*** Hash the files on the system**
*** Search for known malware**

3. Preliminary correlation

The "first correlation step is to examine the individual events and see how they may correlate into a chain of evidence"(Stephenson, Getting the Whole Picture, 2002, 2003). The "main purpose here is to understand in broad terms what happened, what systems or devices were involved and when the events occurred"(Stephenson, Getting the Whole Picture, 2002, 2003).

The slight change I made in the analysis of individual events trickles down into this activity. All of the evidence located through the examination of the various data sources is correlated into a chain of evidence. The chain of evidence provides an overview of the evidence in your investigation.

4. Event Normalizing

The definition of normalization is the "combining evidentiary data of the same type from different sources with different vocabularies into a single, integrated terminology that can be used effectively in the correlation process" (Stephenson, Cyber Investigation, 2009). One example of normalization is adjusting the times in order to take into account the time differences between data sources. All of the times should be normalized into a single time.

For example, if there were two computers with different times then the time stamps of the evidence from one computer should be adjusted to the time of the other computer.

5. Event Deconfliction

The definition of deconfliction is the "combining of multiple reporting's of the same evidentiary event by the same or different reporting sources, into a single, reported, normalized evidentiary event" (Stephenson, Cyber Investigation, 2009). This activity is required when an item is reported multiple times from the same source.

For example I have come across when this was required involved emails. During an email examination, I will review emails located on the email server, the person's email file, and any backup copies of the person's email file on their computer. Sometimes this results in multiple copies of the same email being found. All of the

copies of the email doesn't have to be in the chain of evidence since only one email is required.

6. Second-Level Correlation

"Second-level correlation is an extension of earlier correlation efforts. However, at this point, views of various events have been refined through normalization or deconfliction" (Stephenson, Cyber Investigation, 2009).

7. Timeline Analysis

"In this step, normalized and deconflicted events are used to build a timeline using an iterative process that should be updated constantly as the investigation continues to develop new evidence" (Stephenson, Cyber Investigation, 2009).

8. Chain of Evidence Construction

The evidence in the timeline should be used to form a chain of evidence. "Ideally, each link in the chain, supported by one or more pieces of evidence, will lead to the next link" (Stephenson, Cyber Investigation, 2009). When it is not possible to establish a direct link between evidence a lead can be used to point to the next piece of evidence. "Leads can point us to valid evidence and that valid evidence can, at some point, become the evidence link" (Stephenson, Cyber Investigation, 2009). I briefly touched on this topic in an earlier post titled Broken Chain.

9. Corroboration

In this step, "we attempt to corroborate each piece of evidence and each event in our chain with other, independent evidence or events" (Stephenson, Cyber Investigation, 2009). This final "evidence chain consists of primary evidence corroborated by additional secondary evidence" (Stephenson, Cyber Investigation, 2009).

For example, the human resource department may be conducting an investigation of an employee violating company policy and asks for a forensic analysis to help their investigation. This results in the majority of the corroboration of primary evidence with the secondary evidence being conducted by the persons performing the investigation. However, there is still some secondary evidence which can be collaborated such as information obtained through research.

References :

1. http://cybersecurity.jhigh.co.uk/digitalForensics/digitalForensicsHome.html