Forensics Data and Process

COMP 8920 - Computer and Network Forensics

Lesson 02

Outlines

- Introduction to Digital Forensics Processes Models
- Generic Digital Forensics Process Model
  - Digital Forensics Collection
  - Digital Forensics Examination
  - Digital Forensics Analysis
  - Digital Forensics Presentation
- Design A Digital Forensics Lab
- Lessons Learned from Operation Emmental (Open Discussion)

Digital Forensics Models

Digital Forensic Process Model

- The design of well-defined forensic investigation models is critical for forensic soundness.
- Any forensic investigation process or model usually support a set of forensic principles.
- These models require the availability of appropriate tools for the investigation of the causes and effects of such incidents.
- The tools used can be supported by computational methods and they will have to comply with legal requirements.

Uncertainties in Digital Forensics

How can we trust the information acquired and evidence found during a digital forensics investigation?

The uncertainties associated with potential evidence, both physical and logical, accidental and deliberate, must be addressed in any forensic investigation.

Uncertainties in Digital Forensics

Let us assume that we are investigating a cybercrime where an email message could be used as an evidence. In this cases:

The origin of the email must be considered uncertain, as must the timestamps, since they could have been tampered with while en route. If the email was in fact sent from a given system, how may one know that it was created by the system's owner and not by some intruder intentionally placing it there? What if the email was sent by a Trojan horse or other malware? This argument can be used as part of a legal defense, often referred to as the **Trojan horse defense**

Principles of a Forensics Process

A process or method can be considered forensically sound if it adheres to established digital forensics principles.

Evidence Integrity, which refers to the preservation of evidence in its original form.

Chain of custody, or the ability to document all actions done to the evidence in order to prove its authenticity and integrity.

Prove Digital Evidence Integrity

Experts are experts. What an expert says stands in court as long as:

1. He is an expert.
2. The other party cannot provide another expert, who says that the first expert is wrong, and says it in a more convincingly expertish way.

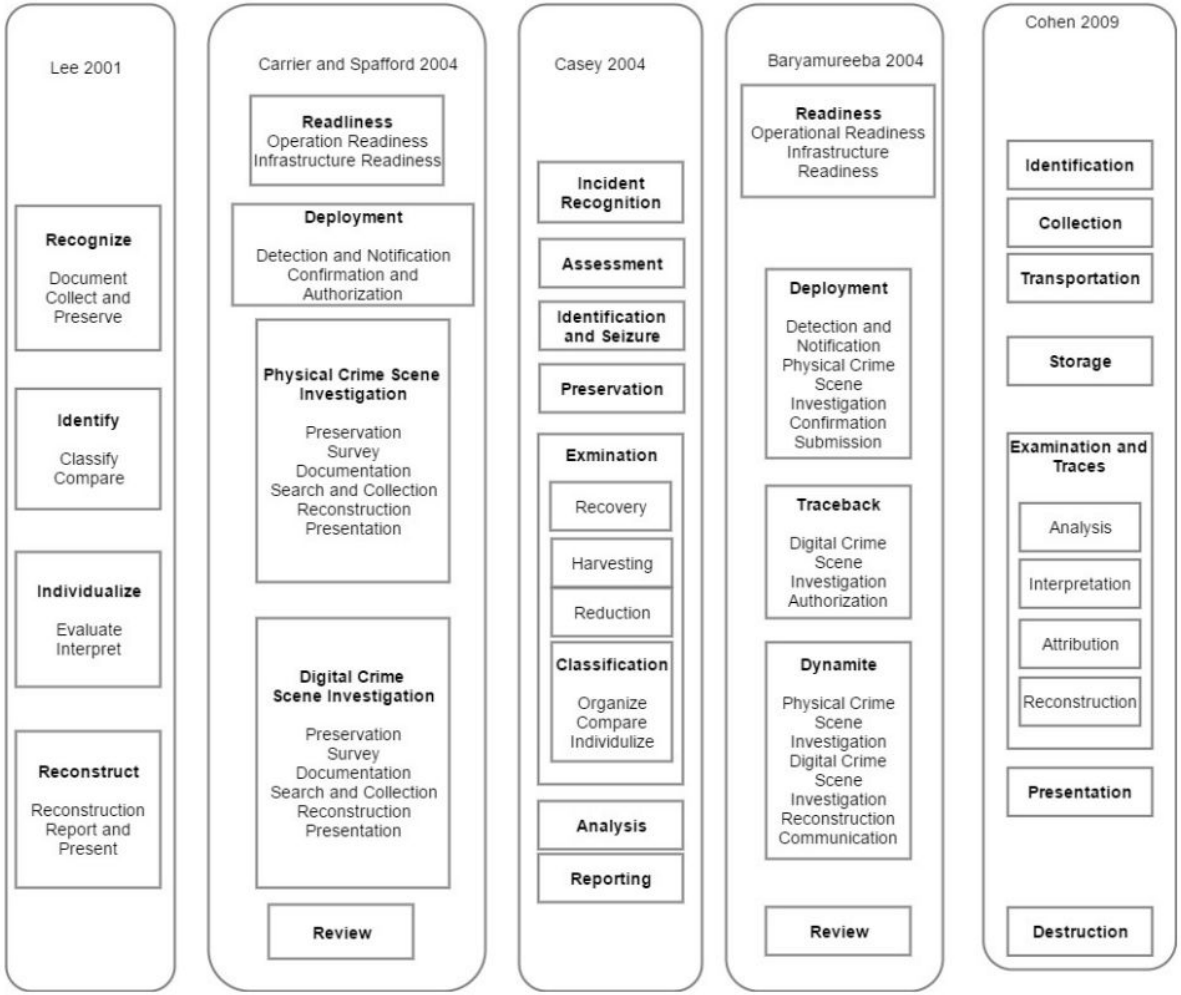
How could we prove that a given email message is sent by a specific individual?

Proving the Source of an Email Message

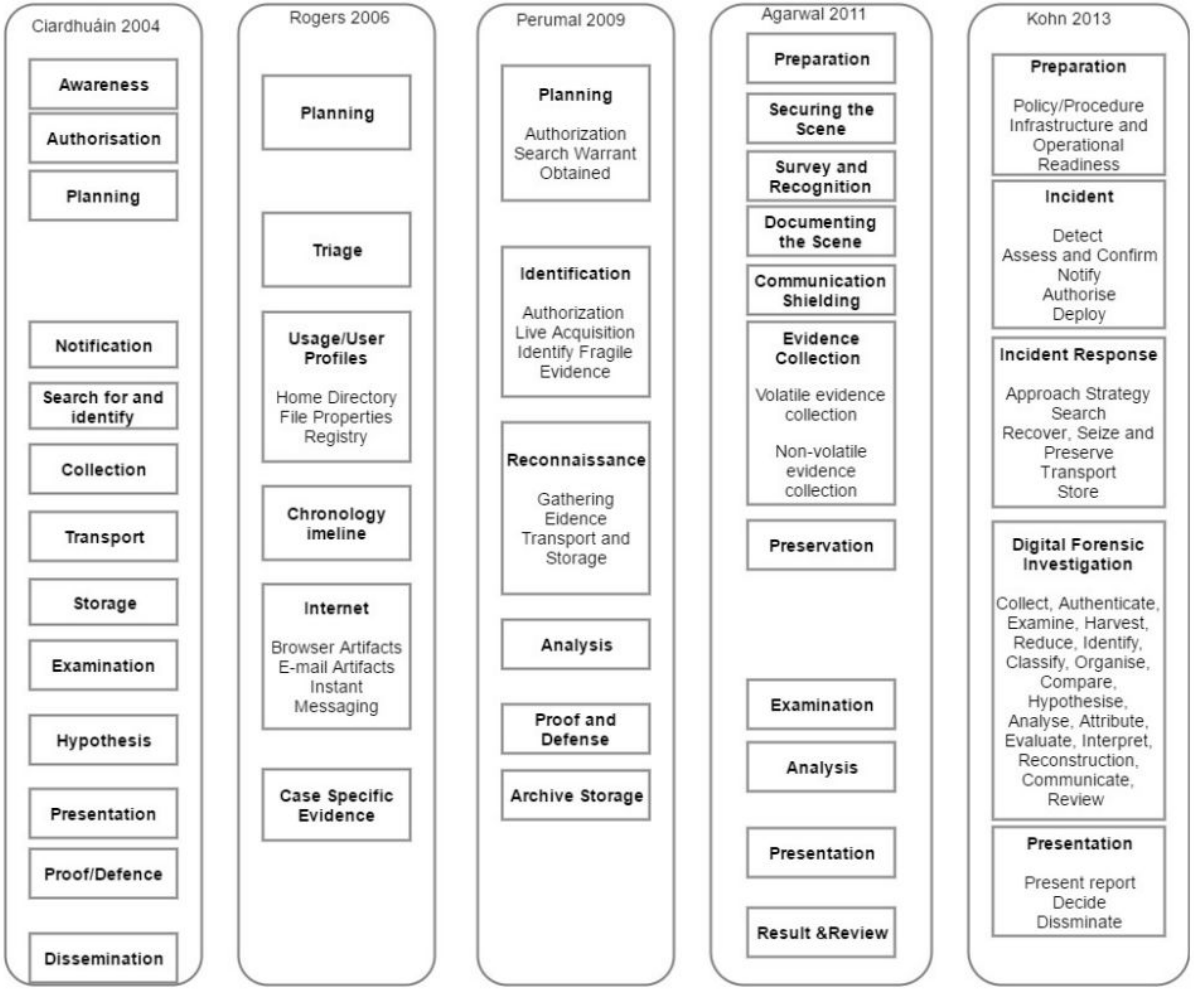
- All possible tracing techniques can be defeated in court by a clever lawyer and a tech savvy.
- Add additional proofs to whatever tracking information about the source of the email you have. For example if you can trace the IP address and link it to the suspect.
- Then you use additional proofs such as Forensic Stylometric and Authorship Analysis. Some countries accept stylometric analysis as an evidence (e.g. **Britain** and the **United States**)

https://www.brooklaw.edu/~/media/PDF/LawJournals/JLP_PDF/jlp_vol21i2.ashx

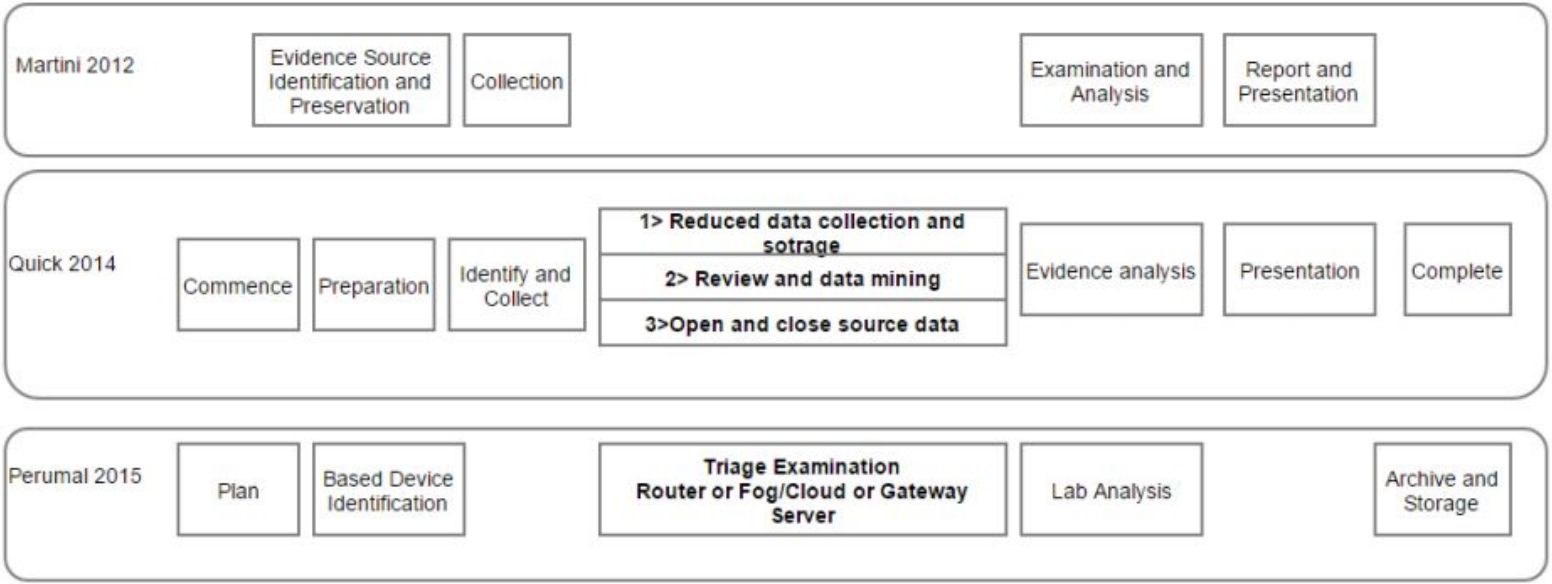
Examples of Digital Forensics Process Models



Examples of Digital Forensics Process Models

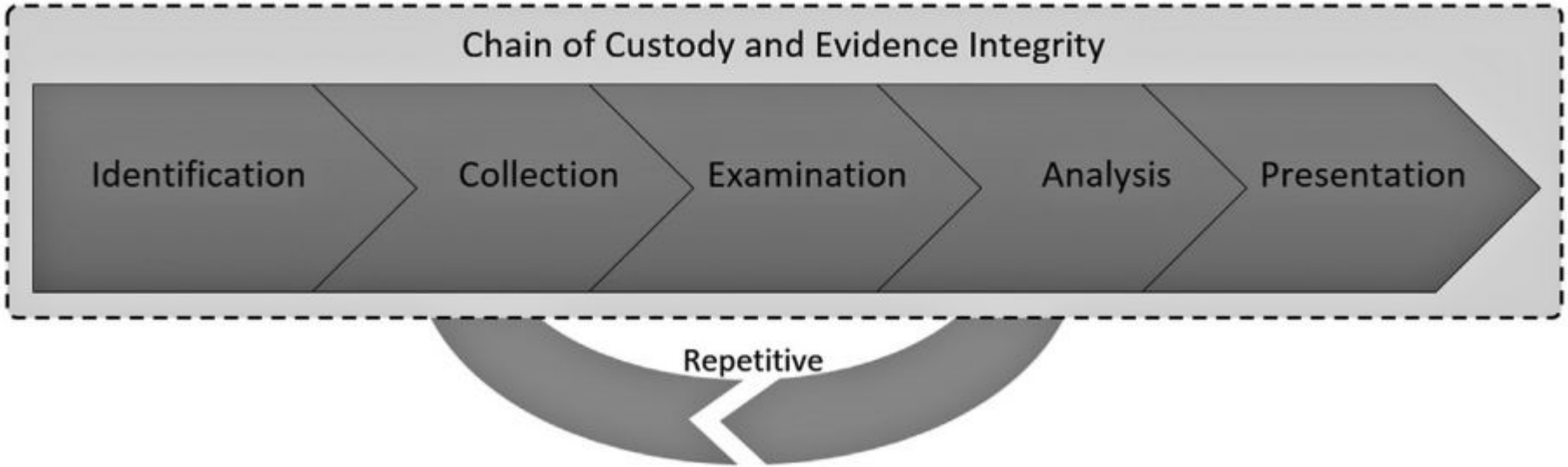


Examples of Digital Forensics Process Models



Generic Digital Forensic Process Model

Digital Forensics Process Model



Digital Forensics Process: Identification

- The task of detecting, recognizing, and determining the incident or crime to investigate.
- Incidents can be identified based on complaints, alerts, or other indications.
- The identification of an incident or a crime leads to the formation of a hypothesis about what might have happened.
- As investigators, we operate with a preliminary hypothesis about a digital device or system that may contain potential digital evidence.

Digital Forensics Process: Identification

Preparations and Deployment of Tools and Resources

- The first responder in a criminal case is typically a police officer, arriving at a physical scene of an event, such as at a crime scene. The first responders are the ones responsible for handling potential evidence, including digital devices.
- The first responder must be trained on appropriate procedures to handle digital evidence in crime senses

Crime Scene and Digital Evidence

Digital Forensics Process: Identification

Example of a First Responder Mistake

- In a murder trial in the United States, a detective at the crime scene allegedly tried to unlock the mobile phone of the suspect. While doing so, he repeatedly entered incorrect PIN and PUK codes to unlock the SIM card. This led to data relevant to the case being erased. The defense team argued that the police investigation destroyed critical evidence that would have been relevant to the case.

Digital Forensics Process: Identification

Dealing with Live and Dead Systems

Physical equipment that holds potential digital evidence is identified either as live (turned on) or dead (turned off, with no power).

Post mortem analysis is, in the context of digital forensics, associated with analysis of a “dead” (not running) computer or electronic device.

The Challenges with Live and Dead Systems

Critical data may not be retrievable if a system is turned off.

Turning on a system that was initially turned off might also lead to evidence loss. At boot time, a PC, mobile phone, or media player executes boot activities that can overwrite previously cached data.

Cell phones, media players, laptops, or any devices that can communicate over any network can potentially be altered while being seized or even after they have been seized.

Digital Forensics Process: Identification

Intentional (tampering) or unintentional (accidental) changes to digital evidence, is a risk in any digital investigation.

In order to maintain the integrity of the evidence, precautions should be taken to ensure that the tools used for acquisition, examination, and analysis of data will not modify it in any unexpected way.

Usually, we clone the raw digital data and uses digital signature and software or hardware write-blocking technology to maintain digital evidence integrity.

Digital Forensics Process: Identification

The Chain of Custody is critical principle in digital forensic investigation. Data and documents may be used for supporting the chain of custody, for example:

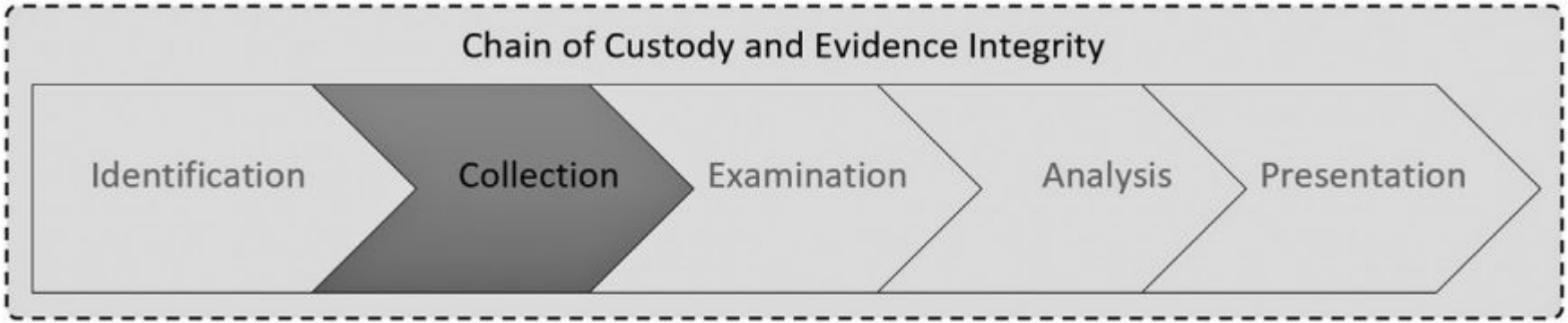
1. photographs,
2. laboratory information management systems,
3. notebooks, reports,
4. checklists,
5. log files, and
6. videos and screen captures

Digital Forensics Process: Identification

What data we should include in the chain of custody documents?

1. The person handling the evidence.
2. Processes and procedures performed.
3. The time and date of evidence acquisition.
4. Original location of the evidence collected.
5. Method of collection, examination, and analysis and the reason for collecting the evidence.

Digital Forensics Process: Collection



Digital Forensics Process: Collection

Refer to the process of collecting data from digital devices to make a digital copy using forensically sound methods and techniques.

This phase start when a forensic investigator gains access to the electronic device(s) containing raw data that has been identified as relevant for the specific case.

The data being investigated should always be copied to a separate media, and the forensic examination and analysis should always work on a copy.

Digital Forensics Process: Collection

The tools and the methods we use to collect the data depend on the type of digital evidences we are investigating. For example in online bank frauds, the digital evidences could be

1. traces of transactions from the victim's computer,
2. bank transaction records from the bank's backend systems,
3. malware evidence on victim hosts, mobile phone and the botnet,
4. server-side logs at the bank,
5. communication with a mule (email, messaging services and phone),
6. transactions made by a mule, and
7. network monitoring logs from the bank infrastructure, and internet forums.

Digital Forensics Process: Collection

What could we say about the digital evidences in online bank fraud?

1. Exists in systems physically tied to a physical locations
2. Exists within live and production and live systems
3. Multiple Evidence Sources
4. Digital data with heterogeneous formats and structures
5. Could be easily forged or damaged (intentionally, unintentionally)

Digital Forensics Process: Collection

It is important to ensure that evidence is neither accidentally nor intentionally changed when collecting digital data from an original source.

Evidence integrity can be facilitated by using hardware or software write blockers. This will prevent the tools we used to collect and copy digital data from changing the raw data on the digital media or source.

Digital fingerprinting techniques using cryptographic hash functions are applied

Digital Forensics Process: Collection

Order of Volatility

While collecting digital evidence it is important to consider the volatility of the data.

it is not just difficult but impossible to gather all the information from a computer system without changing its state.

Order of Volatility refers to the process of prioritization potential evidence source to be collected according to the volatility of the data.

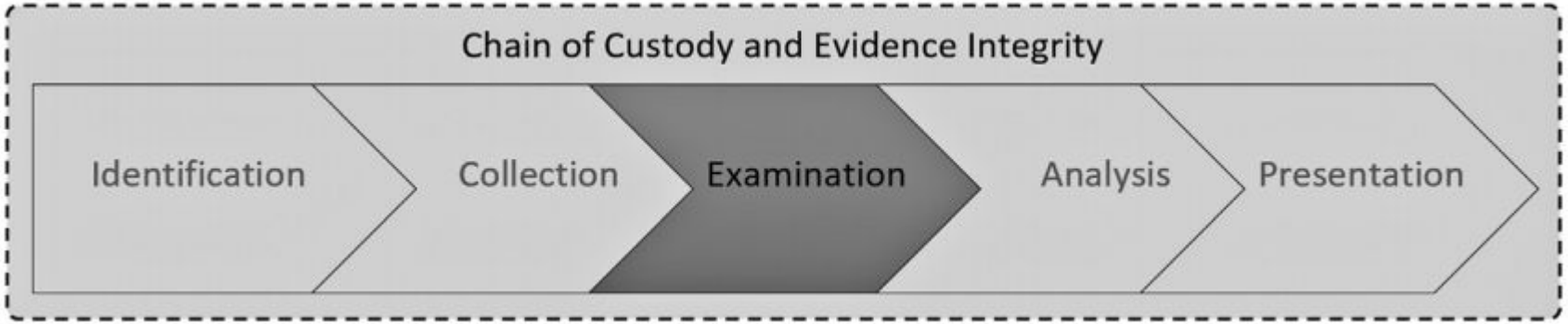
Digital Forensics Process: Collection

Dual-Tool Verification

Dual-tool verification can be applied as a means to detect errors from one tool by using another tool to confirm the results. Example when using tools to recover deleted files or email messages

In cases where dual-tool verification is conducted, tools from different vendors or organizations should be used to avoid any common vendor weaknesses or interference between the tools' capabilities.

Digital Forensics Process: Examination



Digital Forensics Process: Examination

Preparation and extraction of potential digital evidence from collected data sources.

The examination often requires restructuring, parsing, and preprocessing of raw data to make it understandable for a forensic investigator in the upcoming analysis.

Example, we collected digital objects from a hard drive seized from a crime scene by cloning the hard drive, in the examination phase we try to identify the subset of digital objects that are likely contain evidences relevant to the investigation.

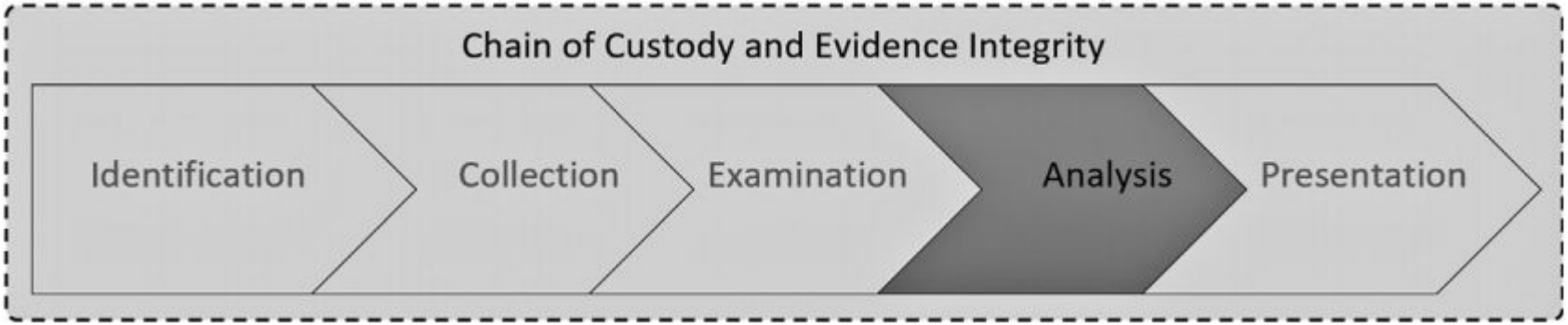
Digital Forensics Process: Examination

Common Tasks and Activities:

- Forensic File Formats and Structures
- Data Recovery
- Data Reduction and Filtering.
- Dealing with Compression, Encryption and Obfuscation Data
- Data and File Carving.

Most of the tasks in the examination phase can be automated using scripts or programs. File parsing, string searches, and extraction of compressed files will significantly reduce the manual task load on an investigator.

Digital Forensics Process: Analysis



Digital Forensics Process: Analysis

The process of reconstructing the incident/crime scenario by investigating the evidences.

The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence, and the person(s) responsible.

This is usually a manual process and the most difficult phase in the forensic investigation process.

It is time consuming and resource intensive tasks.

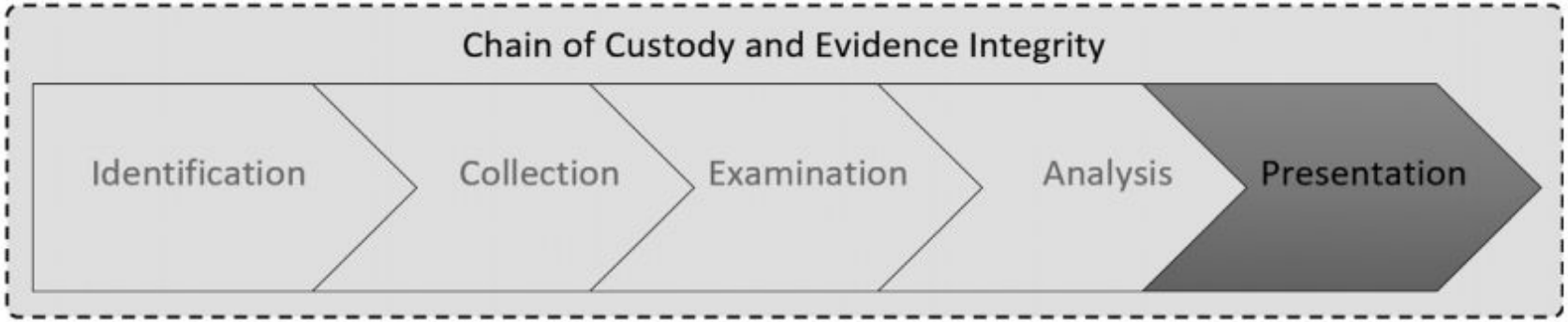
Why Analysis is Difficult?

Large data volumes, obfuscated malware, and techniques to remove their traces make it time-consuming, costly, and difficult for forensic personnel to identify and analyze relevant evidence.

In addition, to the fact that digital evidences are fragile, sophisticated cyber criminal uses anti forensic methods.

Computational Forensics is an emerging research domain that focus on improving and automating the forensics analysis process. It uses different computation methods, such as machine learning, data mining, link analysis, simulation, etc.

Digital Forensics Process: Presentation



Digital Forensics Process: Presentation

The process by which the examiner shares results from the analysis phase in the form of reports to the interested party or parties.

Poor presentation and reporting could destroy all the effort we put in the forensic investigation.

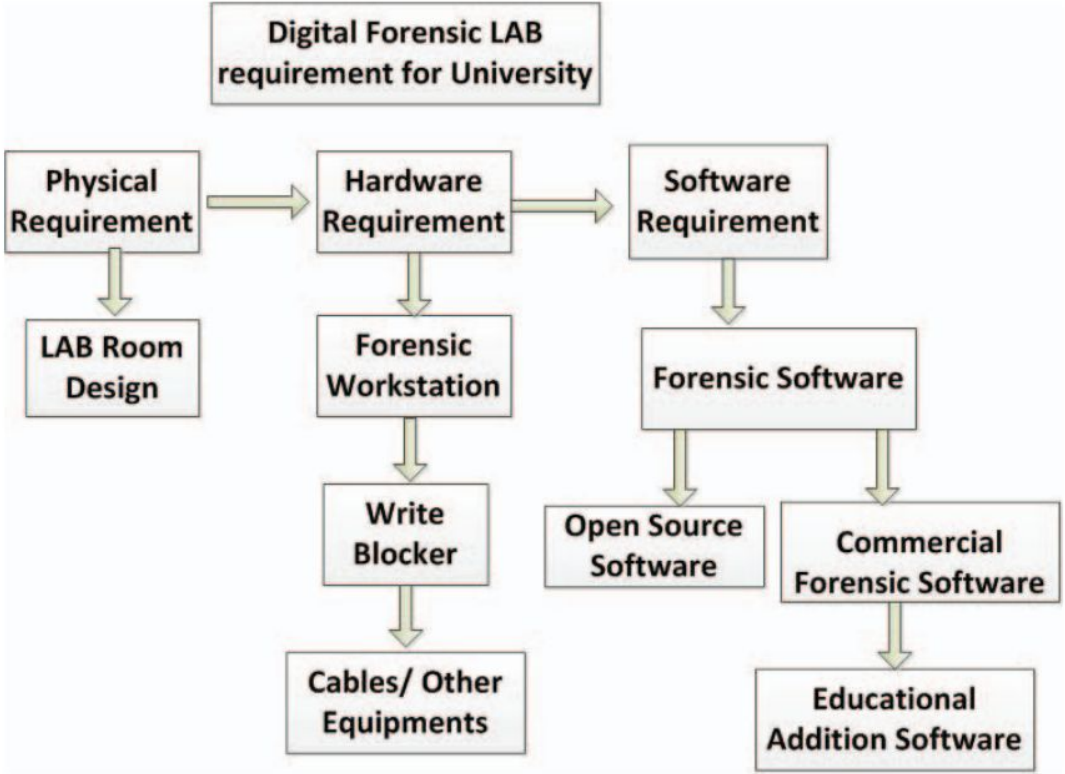
Forensics Data Visualization is an emerging research in security visualization. It focus on how efficiently data visualization techniques could be used to explain the results obtained from the analysis phase.

What should we include in the report

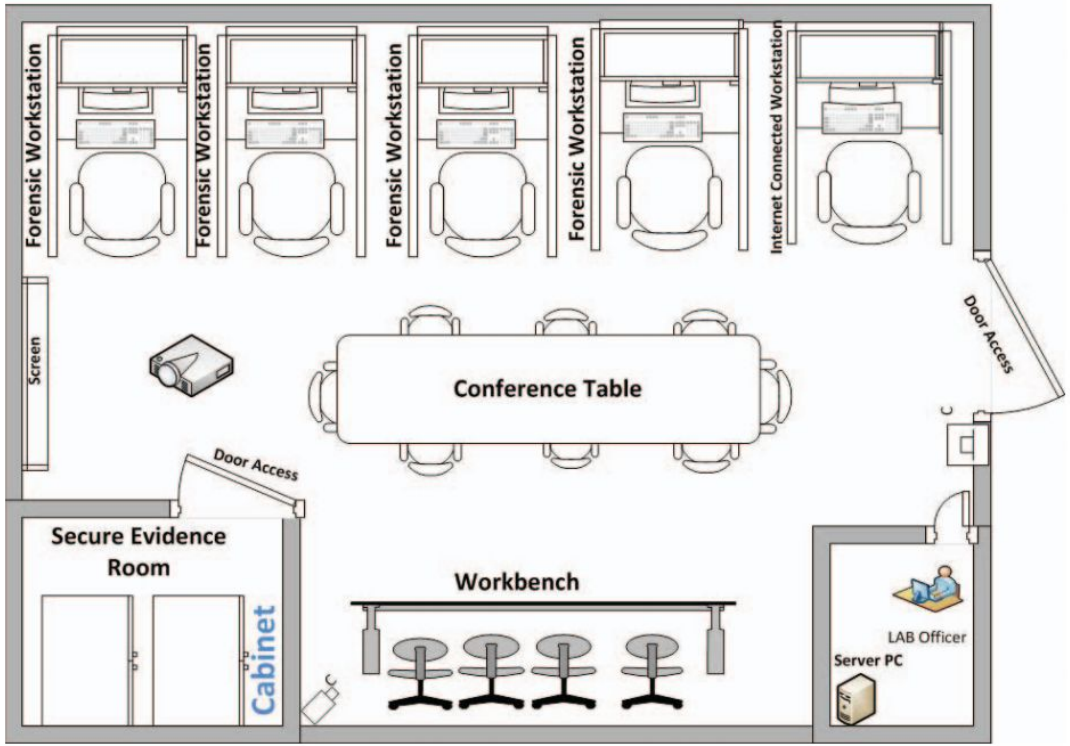
1. Description of the roles and tasks assigned for the investigation.
2. Executive summary of all information sources and evidence.
3. The forensic acquisition and analysis, which reflect chain of custody and evidence integrity.
4. Images and screenshots.
5. The information that supports repeatability or reproducibility of the analysis.
6. Visualizations and diagrams.
7. The tools used; and findings.

Design and Implementation of Low Cost Digital Forensic Laboratory

Requirements of Digital Forensic Laboratory



Lab Physical Layout



Hardware Requirements: Forensic Workstation

#	Types	Specification
1	OS	Windows 10 standard or Windows server 16 and Linux
2	CPU	I7-5820k Hex core 3.3 GHz
3	Motherboard	Gigabyte GA-X99-UD5
4	RAM	32 GB DDR4 2133 MHz
5	OS drive	SSD (256 GB)
6	Data drive	HDD (2 TB)
7	DVD	DVD-RW
8	Power supply	ATX 1200 W power supply
9	Video captured card	NVIDIA GeForce GT 710 GPU
10	Monitor	22″ Wide screen LED monitor with built-in Speakers
11	Casing (4 drive bays)	Mid tower workstation chassis

Hardware Requirements: Other Hardware/Cables

Other hardware's

1. Pen drive 32 GB
2. Pen drive 16 GB
3. Card reader
4. USB DVD writer
5. External HDD
6. 1 TB SATA drive
7. 150 GB SDD
8. 32 GB flash drive
9. Computer hand tools
10. Anti-static mats
11. Anti-static gloves

Cables

1. Power cords
2. USB3 cable 3 matter
3. Two USB A to mini 5 pin cables
4. HDMI cable
5. Mini HDMI cable
6. HDMI to VGA converter
7. VGA to HDMI converter
8. Serial to USB converter
9. DVI cable
10. Two eSATA cable
11. 12″ Micro SATA cable (long SATA cables)
12. One 8″ IDE interface cable
13. One 2″ IDE interface cable
14. Two SATA interface cable
15. Two SCSI-3 interface cable
16. One 1.8″ hard drive adapter
17. One 2.5″ hard drive adapter
18. One ZIF hard drive adapter
19. One micro SATA adapter
20. Pin hard drive Molex power plug to a Serial ATA power plug
21. SATA hard drive power cable
22. Twin serial ATA sata hard drive power cable for 2 drives
23. SATA and SATA HDD power extension cable
24. HDD power cable royalty free stock
25. SATA hard drive power cable

Software Tools For Computer Forensics

Most popular digital forensic tools

#	Tools	Features	License types
1.	Access data forensic Toolkit (FTK) [5]	Create image Registry analysis Password recovery Searching Data carving Reporting	Education edition
2.	EnCase [6]	Acquisition from different devices File recovery Signature analysis Analysis and hash analysis & reporting	Education edition
3.	ProDiscover forensic edition [7]	Deleted file recovery, exam slack space, image capture	Open source
4.	CAINE 7.0 [8]	User friendly four phase digital forensic investigation tools	Open source
5.	Helix [9]	Create image Password recovery Use for cookie viewer, internet history viewer Pictures analysis	Open Source
6.	Sleuth kit (Autophy) [10]	Make timeline of different file activity. Categories different files type, Hash database lookup etc.	Open source
7.	WinHex [11]	Work on disk editor, recovery, clone disk, compare file and encryption technique	Open source

Software Tools Mobile Forensics

#	Tool	Feature	License types
1	Oxygen forensic [16]	• Evaluate contacts from several resources and applications also retrieves data	Proposed education edition
2	Cellebrite [17]	• Bypass user locks, recover application data and reveal deleted data. • Calls, SMS, MMS, Media, emails, calendar and contact files • Location information decoded from apps.	Proposed education edition
3	Paraben [18]	• Mobile forensic • Email investigation	Proposed education edition

Summary

In this class we covered:

- Digital Forensics Models
- Digital Forensics Investigation Lifecycle
- Design of A Digital Forensic Lab

Note: Make sure to read the reading materials posted on the course website.

What is Next?

In our next Class we start talking about computational forensics topics and we will focus on memory forensics.

References

1. Notes on The Digital Forensics Process, by Anders O. Flaglien, A Security Architect at the Central Bank of Norway, 2018
2. Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon, “ Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service”, 2017
3. Md. Masud Parvez,1 Syed Akhter Hossain2 and Shaikh Muhammad Rizwan Ali, “Design and Implementation of Low Cost Digital Forensic Laboratory for University”, 2017