FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the course:

1. Introduction
2. Evolution of Computer Forensics
3. Computer Forensics process
4. Types of Computer Forensics
5. Forensics Readiness

Course 3: Computer Forensics process

3.1 Introduction

3.2 General process of Computer Forensics

3.3 Models of Computer Forensics process

3.4 Constraints and difficulties

3.1 Introduction

Forensic examiners use scientific methods to identify and extract digital evidence. Forensic examiners generally follow clear information and communication technologies based forensic process and technique based on well-defined procedures.

However, the accumulative number of digital activities using different kinds of digital devices have tightened and complicated the process of analyzing and the cleanse of target data.

3.1 Introduction

As such, evaluating digital forensic evidence is not an easy task due to the following reasons:

- ✓ The lack of clear and relevant data.
- ✓ The time required for filtering the evidence data sets.
- ✓ The constant change of the network data, cloud data, digital media devices.
- ✓ The realistic rate of the false alarm versus the detection rate as well as the capability of detecting new or hidden events.
- ✓ The manipulation of features and data attributes.

3.2 General process of Computer Forensics

The general computer forensics process includes four steps:

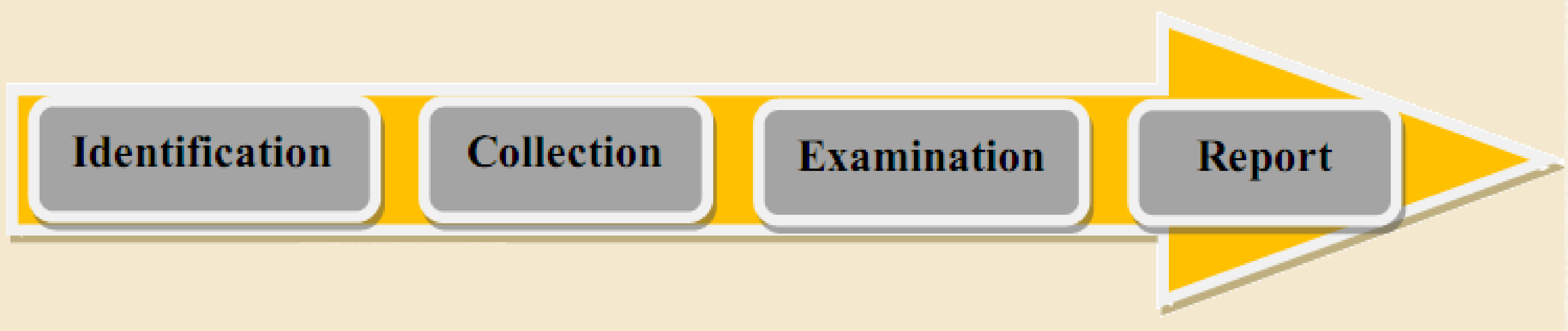
(1) Identification (Assess the situation): This step consists of analyzing the scope of the investigation and the action to be taken.

(2) Collection (Acquire the data) : Gather, protect, and preserve the original evidence.

(3) Examination (Analyze the data) : Examine and correlate digital evidence with events of interest that will help in make a case.

3.2 General process of Computer Forensics (Cont.)

(4) Report the investigation: Gather and organize collected information and write the final report.



3.2 General process of Computer Forensics (Cont.)

(1) Identification (Assess the situation):

Incident indetification

- ✓ The first process of computer forensics is to identify the scenario or to understand the case.
- ✓ At this stage, the investigator has to identify the need of the investigation, type of incident, parties that involved in the incidence, and the resources that are required to fulfil the needs of the case.
- ✓ In identification step key people involved in the case and best sources of potential evidence are identified.
- ✓ Investigator needs extensive knowledge of both computer hardware and software.

(1) Identification (Assess the situation):

Incident indetification

- ✓ Evidence has to be identified among normal files, and may be found in slack space, unallocated space, registries, hidden files, encrypted files, password-protected files, system logs, etc.

- ✓ Evidence can be found on any number of media sources such as hard drive, CD-DVD, PDA, cell phones, flash drives and random access memory (RAM).

- ✓ Search for evidence should also consider physical evidence in a non-digital format that may be of value e.g. notebooks, pieces of paper with potential passwords etc.

(2) Collection (Acquire the data) :

Obtaining evidence

This is the step where the investigators either search, if they're mandated, or simply receive the digital media to be analysed. In both cases, this procedure is accurately performed:

- ✓ Listing of hardware and software characteristics and photographed.
- ✓ If the machine is running during acquisition, a capture of the live memory (RAM) is performed, it will later be used to perform a dump analysis.

- ✓ Analysts are also performing a copy and replication of persistent memory, especially hard drives. These copies will be used to perform the analysis (i.e. which are further examined and compiled into chronological documentation (Chain of Custody)).

3.2 General process of Computer Forensics (Cont.)

(2) Collection (Acquire the data) :

Obtaining evidence

- ✓ It is recommended that we make two copies of the original disks and never work directly on the original disk. One of the copies can then be used as a backup in case the other copy malfunctions.
- ✓ After copying or duplicating a disk, always check the integrity of copied data with respect to the original disk.

Ics Solo 4 Forensic

(2) Collection (Acquire the data) :

Obtaining evidence

- ✓ Digital evidence is information of value to an investigation that is stored and transmitted in a digital form.
- ✓ The challenge faces the investigator is to know where to look for the digital evidence and what digital information is most important to the investigation in order to appropriately collect it.
- ✓ Since digital evidence can be altered or damaged easily, through improper handling during collection or examination. Creating a working copy or a forensic image of the examined data is critical.

(2) Collection (Acquire the data) :

File Imaging

Obtaining evidence

- ✓ The use of computer may cause loss of valuable information so the collection of evidence must not be delayed.
- ✓ It is critical to make identical copy of the original evidence by making an exact bit-by-bit copy using special “forensic” software and/or hardware.
- ✓ In this case the imaging process is intended to copy all blocks of data from the investigated to the practitioner's target device, however a sector by sector copy is the preferred forensic process.
- ✓ The created file called a forensic image file and it can be in various formats, including **.AFF**, **.ASB**, **.E01**, .**dd** and **.raw** or **.mem** image files, and virtual image formats such as **.VMDK** and **.VDI**.

(2) Collection (Acquire the data) :

File Imaging

Obtaining evidence

- ✓ Evidence could be altered easily while the copy is being made. The imaging utility must not introduce new data into the original evidence or the copy. Creating a forensic image is accomplished using a hardware write protection device (See Figure, i.e., an adapter that connect a hard drive through a USB cable to a computer).

- ✓ Hardware write protection devices prevents modifications to the evidence hard drive, since the device only allows data to be read from the evidence source.

SATA/IDE Forensic Bridge

(2) Collection (Acquire the data) :

Obtaining evidence

- ✓ All the recovered evidence from the investigated system should be physically secured. The package contains the evidence has to be sealed to prove that it has not been tampered during transportation.

- ✓ Generally the acquisition step is done with a file copy sub-step and with one of two approaches : **Live box** approach of collecting data on running computers, and **Dead box** approach of collecting data on turned off computers.

(2) Collection (Acquire the data) :

a) Live Box approaches

Obtaining evidence

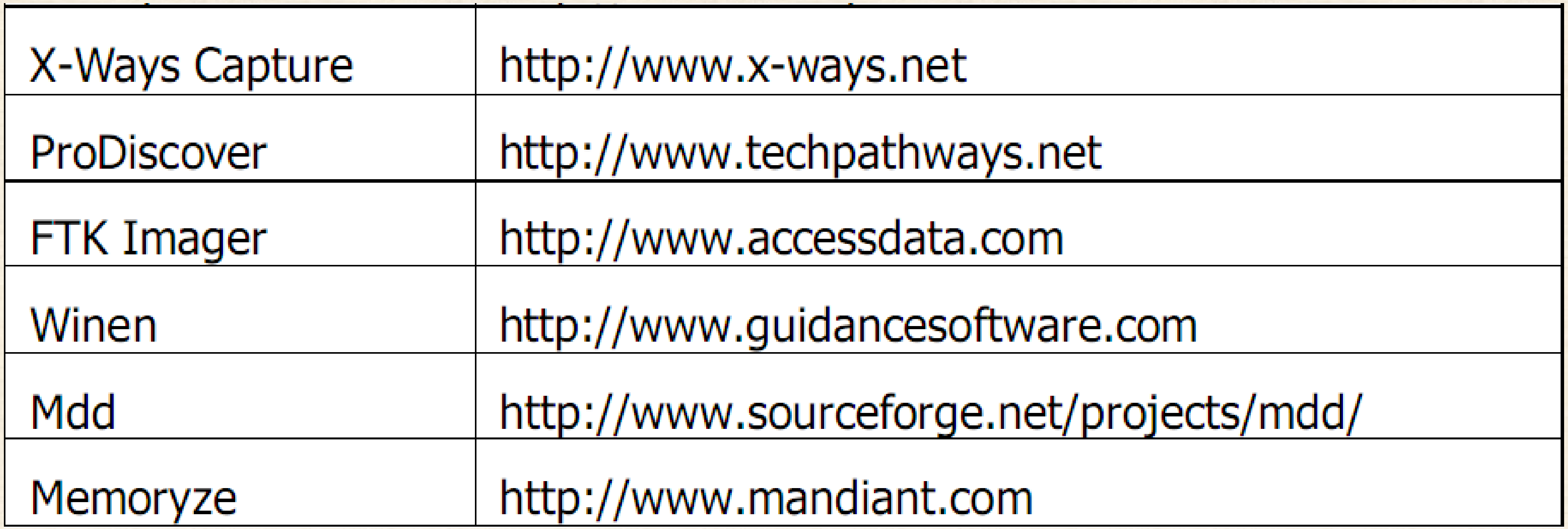
- ✓ Live acquisition approach involves collecting volatile data information from RAM, where the memory is captured as an image file.
- ✓ Before RAM acquisition operation, investigator must determine the operating system and use the suitable software or use a software that suitable for any OS.
- ✓ It is not a good practice to try several software tools during live acquisition.
- ✓ A trusted software tool should be used, otherwise the integrity of the evidence is violated and will not be accepted in the court.

(2) Collection (Acquire the data) :

a) Live Box approaches

Obtaining evidence

- ✓ Obtaining volatile physical memory may be performed with batch files or scripts to automate the process. Table below lists several applications suited for physical memory acquisition can be used by investigators:



X-Ways Capture	http://www.x-ways.net
ProDiscover	http://www.techpathways.net
FTK Imager	http://www.accessdata.com
Winen	http://www.guidancesoftware.com
Mdd	http://www.sourceforge.net/projects/mdd/
Memoryze	http://www.mandiant.com

(2) Collection (Acquire the data) :

b) Dead Box approaches

Obtaining evidence

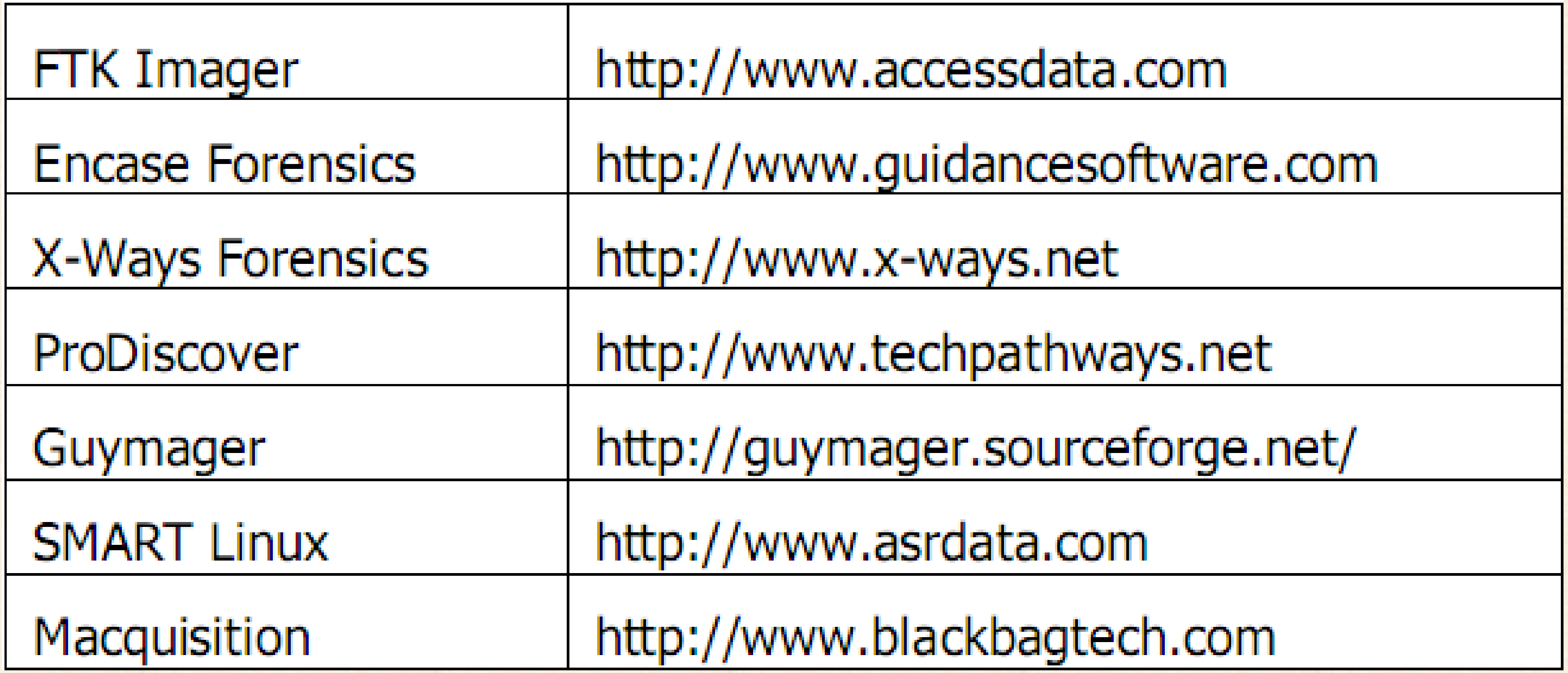
- ✓ If the investigation includes a turned off computer, the investigator should copy the hard drive using write-blocker device without turning the device on. Creating a dead box image is accomplished using a hardware write protection device.
- ✓ In conjunction with hardware write blockers, forensic analysts use applications specifically developed for creating forensic images of media.

(2) Collection (Acquire the data) :

b) Dead Box approaches

Obtaining evidence

- ✓ Table below lists several examples of commonly used imaging software applications



FTK Imager	http://www.accessdata.com
Encase Forensics	http://www.guidancesoftware.com
X-Ways Forensics	http://www.x-ways.net
ProDiscover	http://www.techpathways.net
Guymager	http://guymager.sourceforge.net/
SMART Linux	http://www.asrdata.com
Macquisition	http://www.blackbagtech.com

(2) Collection (Acquire the data) :

Chain of Custody

Obtaining evidence

✓ A chain of custody document must be associated with every piece of evidence. chain of custody is a process used to maintain and document the chronological history of the investigation.

✓ The chain of custody tracking document for a piece of evidence records information such as who handled the evidence, what procedures were performed on the evidence, when the evidence was collected and analyzed, where the evidence was found and is stored, why this material was considered as evidence, and how the evidence collection and maintenance was done.

✓ Maintaining a chain of custody of the evidence collected is crucial to protect the integrity of the evidence and argue that the evidence was not tampered while in custody.

3.2 General process of Computer Forensics (Cont.)

(3) Examination (Analyze the data):

Analysis of records

In this third step the investigator will examine the collected data by following standard procedures, techniques, tools and methodology to extract evidences. To do this, one can proceed as follows:

- ✓ Establish a timeline of events from previously acquired device: an ordered history of events for OS, applications, disks, users and others. By focusing on the period of interest given by the plaintiff during the initial exchange, this timeline can already provide leads.
- ✓ From the recovered data, we can already identify a scenario skeleton. One must browse through all available types of artefacts to identify elements that either confirm or disprove the first hypothesis. Live forensics analysis and dead forensics analysis results are to be correlated.

(3) Examination (Analyze the data):

Analysis of records

- ✓ At this point, the initial hypothesis has potentially generated new scenarios. These are also to be demonstrated on the basis of artifacts. This phase and the previous one are to be repeated until no new hypotheses can be established.
- ✓ At this stage, the investigator searches for the possible evidence against the suspect, if any. Use the tools and techniques to analyze the data. Techniques and tools should be justified legally because it helps to create and present the report in front of the court.

3.2 General process of Computer Forensics (Cont.)

(4) Report the investigation:

Evaluation of results

- ✓ At this step, an investigator needs to document the process used for the above steps.
- ✓ The investigation report also consists of the documentation of how the tools and procedures were being selected.

- ✓ The objective of this step is to report and present the findings justified by the evidence.
- ✓ Every step mentioned above can be further divided into many parts and every part has its own standard operating procedures (SOP).

(4) Report the investigation:

Evaluation of results

- ✓ At this stage, the results from the previous steps are evaluated and suspicious activities from the beginning of the attack are identified.
- ✓ The results are reported along with a detailed description of the steps taken by the client.
- ✓ This makes it possible to subsequently implement protective measures to prevent the incident from recurring.

3.2 General process of Computer Forensics (Cont.)

→ **Report edition:**

Evaluation of results

- ✓ Investigators must prepare the investigation reports taking into consideration all terms and rules of the country law.
- ✓ They first need to analyze the report by themselves to check its consistency and to ensure there are no contradictions with the law.
- ✓ They must expect to be cross-examined about the contents of the report in a court of law.
- ✓ Opposing counsel will eventually look for weaknesses and gaps in the facts presented.

→ Report edition:

Below are some generic concepts that should be considered before or during the writing process.

✓ Limiting a report to specifics: All reports must start by clearly defining the investigation goals. This will reduce the time and cost of the investigation, especially when working with a big dataset.

✓ Audience: Clearly identify the technical knowledge of the intended audience before we begin writing. This will keep we more focused on the specifics.

✓ Types of Reports: Forensics investigators should determine the type of reports they are required to create. Such as

- Formal reports (they contain facts)
- Preliminary written reports (drafts or tests that haven’t been concluded)
- Verbal report (for attorney)
- Examination plan (expected questions & answers)

3.2 General process of Computer Forensics (Cont.)

→ Report Structure:

Evaluation of results

Like any official report or scientific paper, a report structure normally includes some basic sections shown in the following list. The order varies depending on organizational guidelines:

- Report title: Each report should have a title indicating the case under investigation.
- Abstract: The abstract briefly describes the examination and presents the report's main ideas and results in a summarized form. It should be one or two short paragraphs.
- Table of contents: This includes the report roadmap, all sections, subsections, etc. It should allow for easy navigation to those parts that readers wish to review.

→ Report Structure:

Evaluation of results

- Body of report: This section is the core part of the report, it consumes most time and efforts: It consists of several parts. They are :

  - **Introduction:** This should state the report purpose and show that we are aware of its terms of reference. It contains methods used, limitations, justification why we are writing the report, so make sure we answer the question "What is the problem?" we should also give readers a map of what we are delivering

  - **Discussion sections:** Organize discussion sections logically under headings to reflect how we categorize the information and to ensure that our information remains relevant to the investigation.

→ Report Structure:

Evaluation of results

- **Conclusion:** The conclusion starts by referring to the report purpose, states the main points and draws conclusions.

- **References:** It lists the supporting material to which our work refers.
- **Glossary:** It is a comprehensive list of definitions for non-obvious terms and phrases mentioned in the report.

- **Acknowledgments:** They enable we to thank all those who have helped in carrying out the investigation.

*https://attack.mitre.org/

→ Report Structure:

Evaluation of results

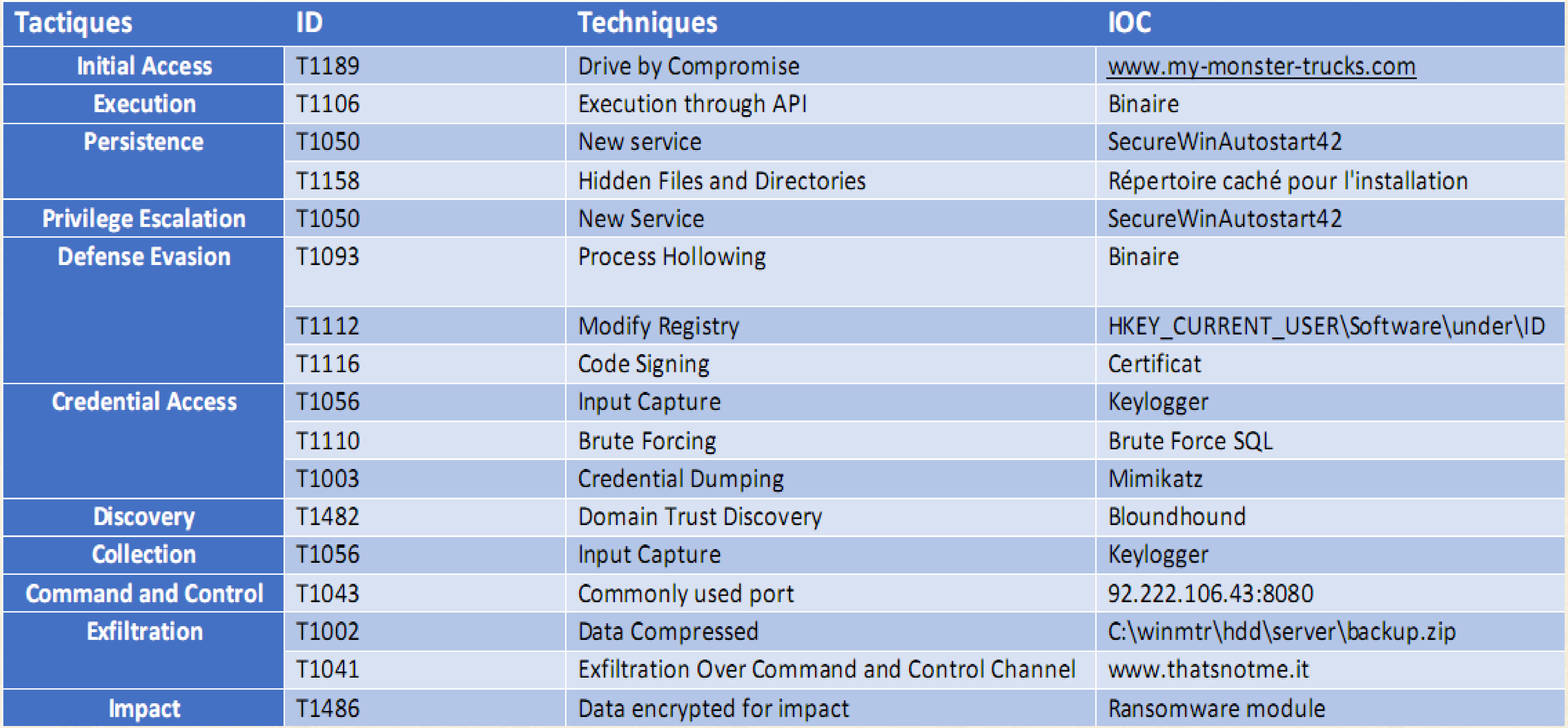
- **Appendixes:** They contain supplementary material that is not an essential part of the text itself, but which may be helpful in providing a more comprehensive understanding of the investigation.

✓ The report can be enhanced by adding the ATT&CK matrix* which allows us to identify the attacker’s tactics and technics that are used to perform a crime.

✓ It provides a set of classifications which allows to identify different stages of an attack, therefore it provides used techniques for each stage.

*https://attack.mitre.org/

ATT&CK matrix example



Tactiques	ID	Techniques	IOC
Initial Access	T1189	Drive by Compromise	www.my-monster-trucks.com
Execution	T1106	Execution through API	Binaire
Persistence	T1050	New service	SecureWinAutostart42
	T1158	Hidden Files and Directories	Répertoire caché pour l'installation
Privilege Escalation	T1050	New Service	SecureWinAutostart42
Defense Evasion	T1093	Process Hollowing	Binaire
	T1112	Modify Registry	HKEY_CURRENT_USER\Software\under\ID
	T1116	Code Signing	Certificat
Credential Access	T1056	Input Capture	Keylogger
	T1110	Brute Forcing	Brute Force SQL
	T1003	Credential Dumping	Mimikatz
Discovery	T1482	Domain Trust Discovery	Bloundhound
Collection	T1056	Input Capture	Keylogger
Command and Control	T1043	Commonly used port	92.222.106.43:8080
Exfiltration	T1002	Data Compressed	C:\winmtr\hdd\server\backup.zip
	T1041	Exfiltration Over Command and Control Channel	www.thatsnotme.it
Impact	T1486	Data encrypted for impact	Ransomware module

3.3 Models of Computer Forensics process

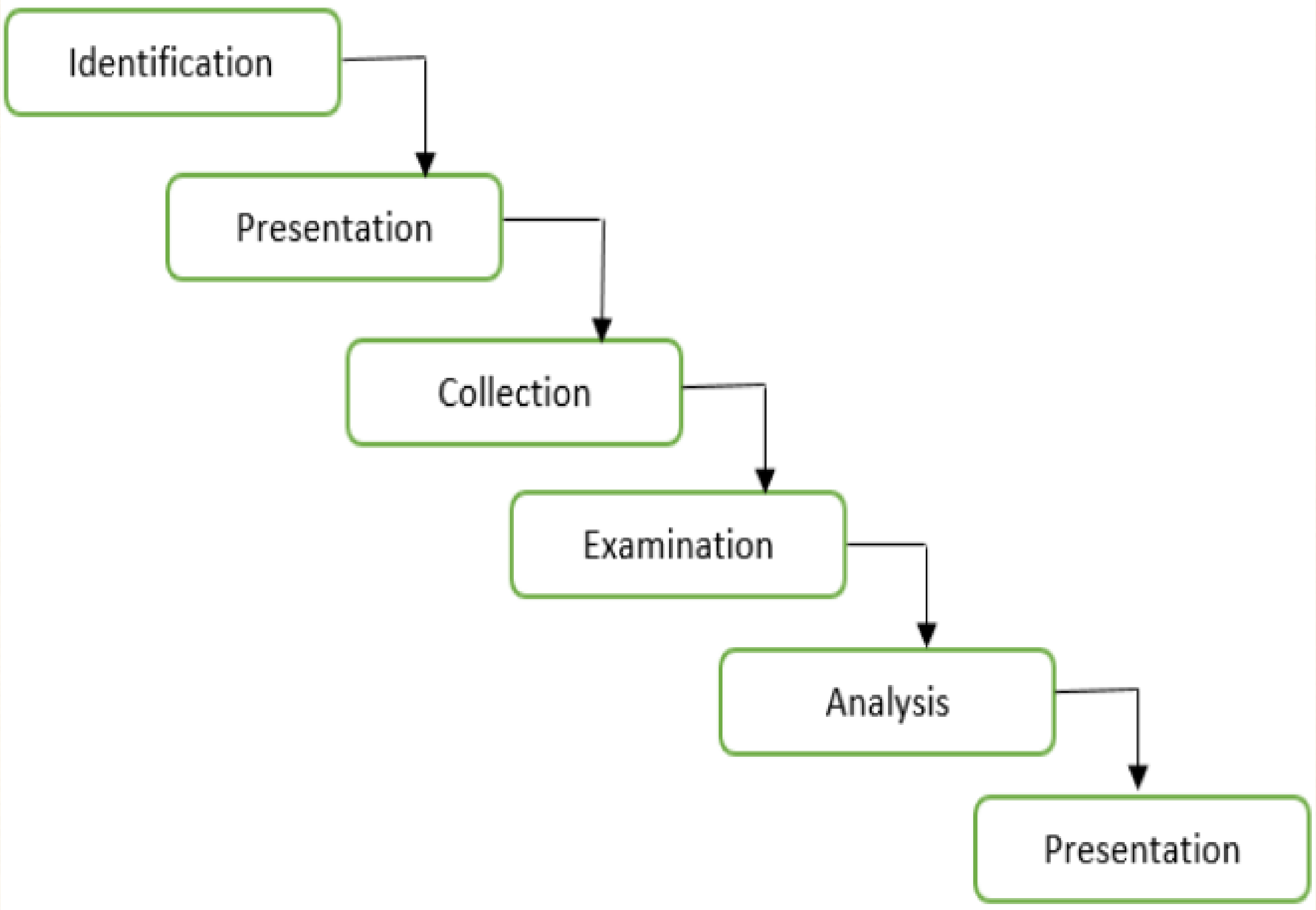
At the early beginning, the last investigation process was proposed. Later, number of investigation models were introduced. However, forensic examiners generally follow valid and case pertinent forensic procedure. Among of them we have:

→ The DFRWS forensic model

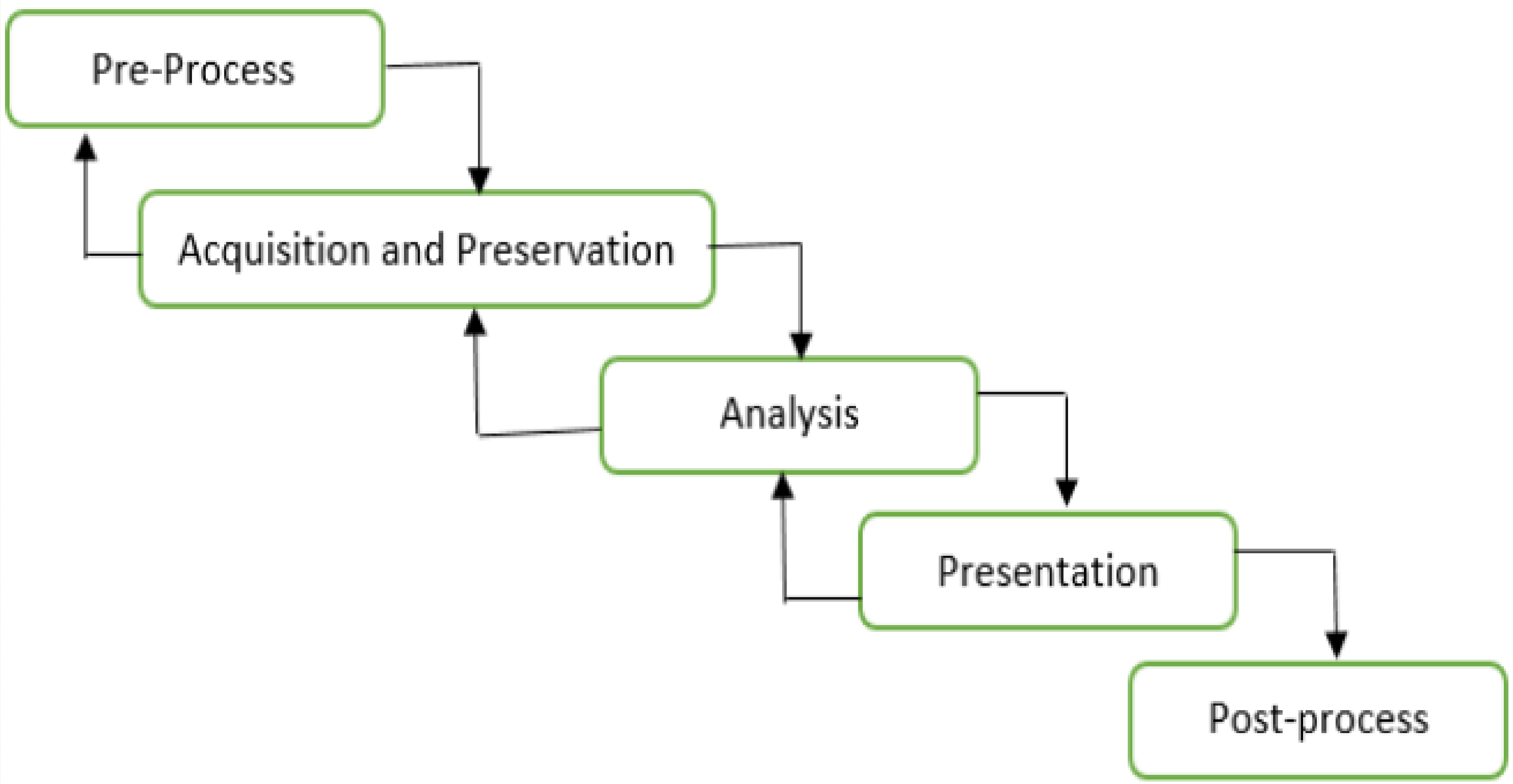
→ The Generic Computer Forensic Investigation Model

3.3.1 The DFRWS forensic model

The straightforward forensic model as defined in the Digital Forensics Research Workshop known as DFRWS investigation model is comprised of six phases as per the following in this Figure.



3.3.2 The Generic Computer Forensic Investigation Model



3.4 Constraints and difficulties

The analysis of digital evidence poses challenges to forensics investigators. Working with digital media and electronic information is important for the successful implementation of case disposition.
However a digital investigation rarely proceeds under optimal conditions, mainly due to the following difficulties:

- ✓ Impossibility to access all necessary event logs due to insufficient data retention policies.
- ✓ Impossibility to access RAM, the machines often being turned off at the beginning of investigations (this is still the right thing to do in the case of ransomware).

3.4 Constraints and difficulties

- ✓ Intervention planned for an insufficient timeframe to obtain a complete and fruitful analysis.
- ✓ Difficulties in sorting out relevant information from the large amount of data available.
- ✓ Difficulties in assessing the full extent of an attack, especially on large information systems.