Mustansiriyah University

College of Science – Department of CS/Cybersecurity

By

Prof. DR. Bashar ALEsawi

Introduction To Digital Forensics

2023-2024/ 2nd – Semester

Digital Forensics: An Introduction

Digital Forensics is the application of scientific methods in preserving, recovering, and investigating digital evidence in a Digital crime scenario. It can be correctly defined as, collection, examination, analysis, and documentation by using scientifically proven methods to investigate a digital crime and present it before the court.

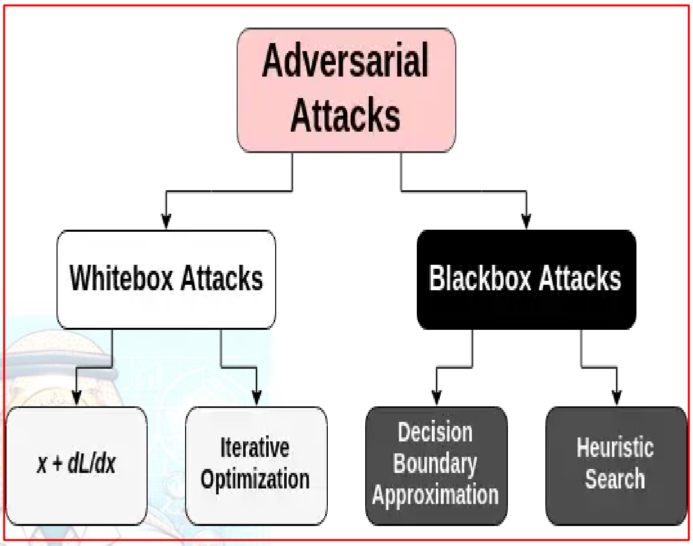
Table of Contents:

What is Digital Forensics?

Digital forensics is a branch of forensic science that uses scientific understanding to acquire, evaluate, record, and present digital evidence related to computer crime in court. The main goal is to ***figure out what happened, when it happened, and who did it***. These investigations include user laptops, computers, mobile phones, network devices, Webcams, tablets, camcorders, IoT and smart home devices, and storage media such as USB drives, CD/DVD, SD cards, and tapes, among other digital systems and devices that can send, receive, and store digital data.

Digital Forensics is also 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.

- ***Data breaches, phishing, ransomware, DoS assaults, and SQL Injunctions*** are all examples of cyberattacks on digital systems that may be investigated <u>using</u> **Digital Forensics**.
- ***Cyberespionage*** or ***Adversarial assaults*** (لتجسس الإلكتروني أو الاعتداءات العدائية) that compromise accounts and services, unauthorized system and network access, or other associated cyberattacks that cause commercial or reputational harm are all included in this category.



https://www.labellerr.com/blog/what-are-adversarial-attacks-in-machine-learning-and-how-can-you-prevent-them/

Digital Forensics Goals:

The basic goal of digital forensics is to investigate crimes committed with computer systems that store and process digital data and to extract forensic' digital evidence to present in court. This is achieved in the following ways using digital forensics:

- Follow court-approved technological methods to preserve and recover evidence.
- Assigning responsibility for an activity to the person who initiated it.
- Determining data breaches inside a company.
- Identifying the extent of any damage that may occur as a result of a data breach.
- Compiling the findings into a formal report that may be submitted in court.
- Providing expert evidence in court as a guide.

- اتباع الأساليب التكنولوجية المعتمدة من قبل المحكمة لحفظ الأدلة واسترجاعها.
- إسناد مسؤولية النشاط إلى الشخص الذي تم تحديده.
- تحديد خروقات البيانات داخل الشركة.
- تحديد مدى أي ضرر قد يحدث نتيجة لخرق البيانات.
- تجميع النتائج في تقرير رسمي يمكن تقديمه إلى المحكمة.
- تقديم أدلة الخبراء في المحكمة كدليل.

Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

◉ The increase of PC's and extensive use of internet access

◉ Easy availability of hacking tools

◉ Lack of physical evidence makes prosecution difficult.

◉ Large amount of storage into Terabytes that makes investigation job difficult.

◉ Any technological changes require an upgrade or changes to solutions.

Defining Cybercrime (Digital Crime):

Any illegal activity carried out on a computer or via a computer network, such as the internet, is referred to as cybercrime.

&

وفقا لوزارة العدل الأمريكية، يتم تعريف الجريمة السيبرانية على أنها أي سلوك غير قانوني يتم القيام به ضد أو باستخدام جهاز كمبيوتر أو شبكة كمبيوتر.

According to the US Department of Justice, cybercrime is defined as any unlawful behavior done against or with the use of a computer or computer network. The fundamental motivation for cybercrime is financial gain (for example: spreading malware to steal access codes to bank accounts).

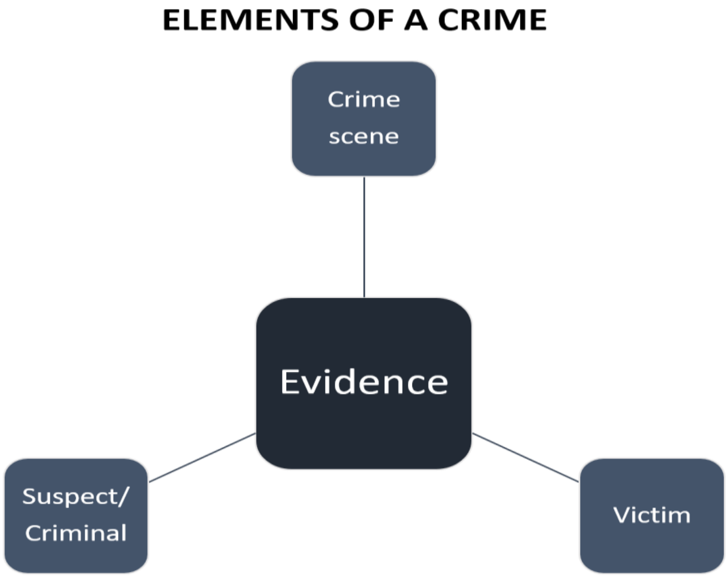
Sources of cybercrime

Insider threats and external attacks are the two primary sources of cybercrime.

- **Insider threats**: Since they might go unnoticed for a long period, this is the most significant cyber risk threatening enterprises today. Employees —or other persons working within the target company, such as former employees, third-party contractors, or business associates—with authorized access to the target organization’s computing systems and/or information about its cybersecurity procedures and defenses—commit insider attacks.
- **External attacks**: These attempts are typically carried out by skilled hackers who operate from outside the target company. These are the most typical types of cyberattacks against organizations all across the world. A black hat hacker may attempt to enter the target company’s networks from another country to get illicit access.

Elements of a Digital Crime

To prove a digital crime, as an investigator you should have the following elements to bring out a conclusion. All the elements will be related to one another in a more or so.



1) Digital Crime:

A digital crime scene refers to the virtual or electronic environment where a cybercrime or digital incident has occurred. It involves the collection, analysis, and preservation of digital evidence to investigate and understand the nature of the cybercrime. Digital crime scenes can include a wide range of scenarios, such as hacking, data breaches, computer intrusions, malware attacks, and other cybercrimes.

Key characteristics of a digital crime scene include:

1. **Virtual Nature:**
   - Unlike traditional crime scenes, digital crime scenes exist in the virtual world. They involve computer systems, networks, and digital devices where electronic evidence is stored.
2. **Data and Artifacts:**
   - Digital crime scenes contain electronic data and artifacts that can serve as evidence. This may include files, logs, system configurations, network traffic, and other digital traces left behind by cybercriminals.
3. **Dynamic Environment:**
   - Digital environments are dynamic and can change rapidly. Therefore, digital crime scene investigators must work efficiently to preserve and collect evidence before it is altered or compromised.
4. **Specialized Tools:**
   - Investigating digital crime scenes requires the use of specialized tools and techniques. Digital forensics tools help investigators collect, analyze, and preserve electronic evidence in a forensically sound manner.
5. **Remote Investigations:**
   - Digital crime scenes may involve remote systems and networks. Investigators may need to conduct remote forensic analysis or collaborate with entities across different geographical locations to gather evidence.
6. **Multidisciplinary Approach:**
   - Digital crime scene investigations often involve a multidisciplinary approach, combining expertise in computer science, cybersecurity, law enforcement, and legal procedures.
7. **Legal Considerations:**
   - Evidence collected from digital crime scenes must adhere to legal standards and be handled in a manner that ensures its admissibility in court. Chain of custody, proper documentation, and forensic best practices are crucial.

2) What is Victim:

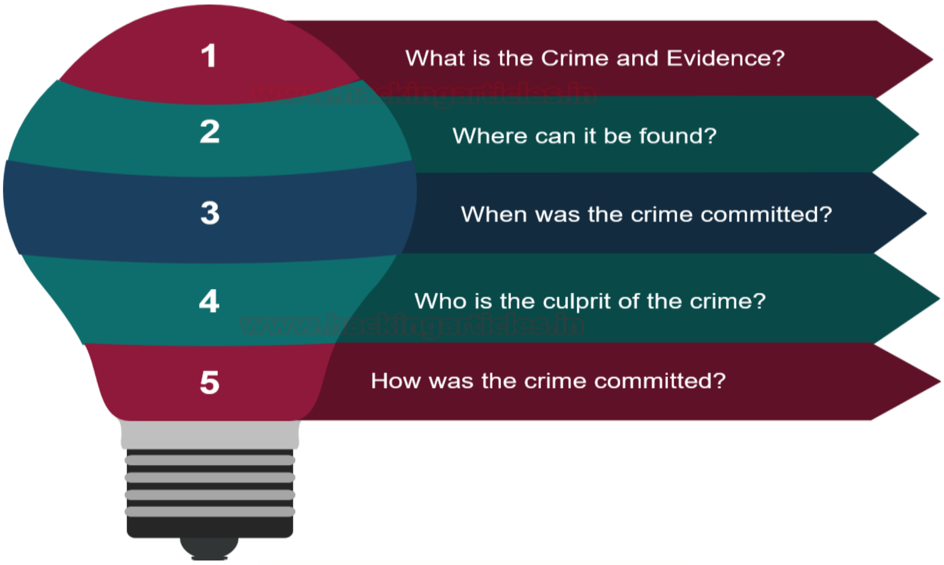
In digital forensics, a "victim" refers to an entity or individual that has experienced harm, damage, or compromise as a result of a cybercrime or digital incident. The term is used to describe the target or subject of the malicious activity, and the victim could be an individual, an organization, or even a system.

Key points related to victims in digital forensics include:

1. **Individuals or Organizations:**
    - Victims can be individuals who have had their personal information compromised or misused, or organizations that have suffered from cyberattacks such as data breaches, ransomware attacks, or other forms of digital crimes.
2. **Harm or Compromise:**
    - The harm or compromise experienced by the victim can take various forms, including unauthorized access to sensitive data, financial losses, disruption of services, reputation damage, or other negative impacts resulting from cyber incidents.
3. **Forensic Investigation:**
    - Digital forensic investigators work to uncover the details of cybercrimes and the impact on the victim. They analyze digital evidence to determine the extent of the compromise, identify the methods used by attackers, and gather information that can be used for attribution or legal action.
4. **Incident Response:**
    - In addition to forensic investigation, victims often engage in incident response activities to mitigate the impact of the cyber incident. This can include isolating affected systems, removing malware, restoring services, and implementing measures to prevent future incidents.
5. **Legal Considerations:**
    - Victims play a crucial role in legal proceedings related to cybercrimes. The evidence collected during digital forensic investigations is often used to build a case against perpetrators, and victims may be involved in legal actions or cooperate with law enforcement agencies.
6. **Notification and Communication:**
    - In cases of data breaches or other incidents involving personal information, victims may need to be notified about the breach. Effective communication with affected individuals or organizations is an essential aspect of handling digital incidents.

Goals of Digital Forensic Investigation

As a digital forensic investigator, you should have a goal for investigation. Depicted below are the five most important goals of investigation;

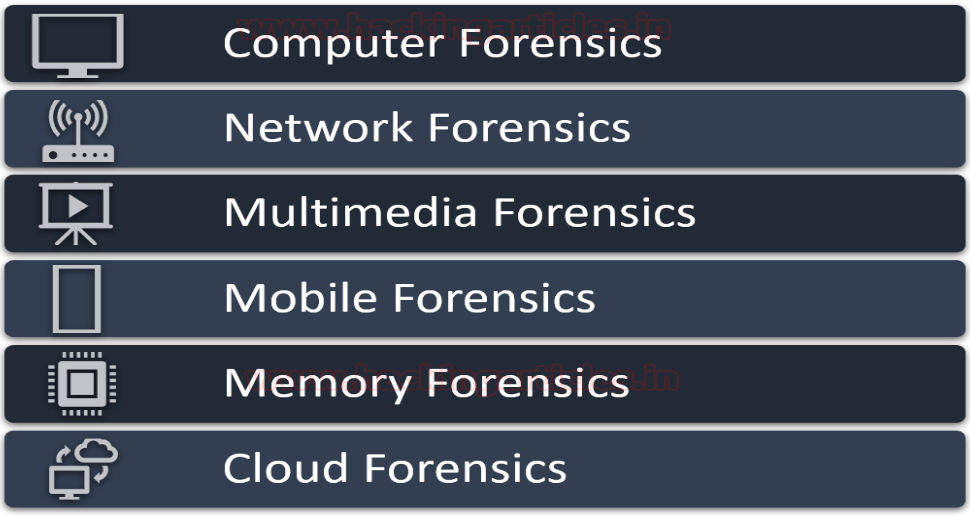

1
What is the Crime and Evidence?
2
Where can it be found?
3
When was the crime committed?
4
Who is the culprit of the crime?
5
How was the crime committed?

Classification of Digital Forensics

Digital forensics is a very broad term that has various classifications within it. The most popular forensic investigations are as follow:

1. **Computer Forensics:** It is the most primitive type of digital forensics which usually was introduced in the early evolution of computer systems. It includes investigating computers, laptops, logs, USB drives, hard drives, Operating systems, etc.
2. **Network Forensics:** It includes investigating by analyzing network events, intrusion, and data packets that were transmitted to detect network attacks.
3. **Multimedia Forensics:** It comprises of investigation of images, audio, and video files that are recovered as evidence in a digital crime scene.
4. **Mobile Forensics:** It comprises of investigation of smartphones like android, iOS, etc for finding digital evidence and recovering the deleted data important for the case.
5. **Memory Forensics:** It is the forensic investigation of the memory or ram dump of the system to find out volatile memory like chat history, clipboard history, browser history, etc.
6. **Cloud Forensics:** Considering the virtual storage are in demand, the investigation of the cloud environment also plays a key role in a digital crime scene for gathering evidence.

The classification of digital forensics isn't limited to the above diagram and as t can be classified into more depending on the cases.



Computer Forensics

Network Forensics

Multimedia Forensics

Mobile Forensics

Memory Forensics

Cloud Forensics

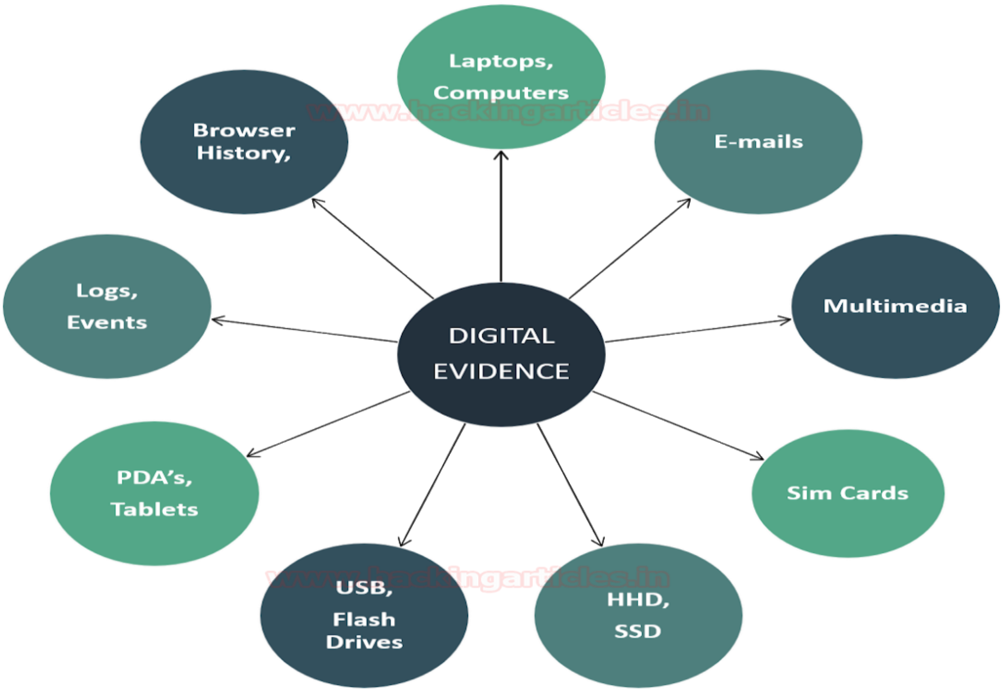
Digital Evidence

Digital evidence or electronic evidence can be defined as any object that stores digital information and transmits it in any form which was used in the act of crime or in supporting the investigation of the case in a trial before the court.

The evidence found at the crime scene should have two key properties

1. They should be admissible in the court
2. They should be authentic.

The ***digital evidence*** can be like of various types and should be availed ethically by following the prescribed guidelines of investigations. Here are a few digital evidences in the diagram below, but the list goes on.



DIGITAL EVIDENCE

Laptops, Computers

E-mails

Multimedia

Sim Cards

HHD, SSD

USB, Flash Drives

PDA's, Tablets

Logs, Events

Browser History,

Acquiring digital evidence:

It is a critical step in the digital forensic process. It involves gathering data from various sources, such as computers, mobile devices, storage media, and networks, while ensuring the preservation and integrity of the evidence. Here are some common methods of acquiring digital evidence:

1. Live acquisition: This method involves collecting data from a live or running system. It typically includes capturing volatile data such as running processes, network connections, and system information.

2. Disk imaging: Disk imaging involves creating a bit-for-bit copy or "image" of an entire storage device, such as a hard drive or solid-state drive (SSD). The imaging process ensures that all the data, including deleted or hidden files, is preserved.

3. File-level acquisition: In some cases, it may be necessary to acquire specific files or directories rather than imaging an entire storage device. This method allows for targeted collection of relevant files while reducing the amount of data to be processed. It is important to maintain the integrity of the files and document their metadata, such as timestamps and permissions.

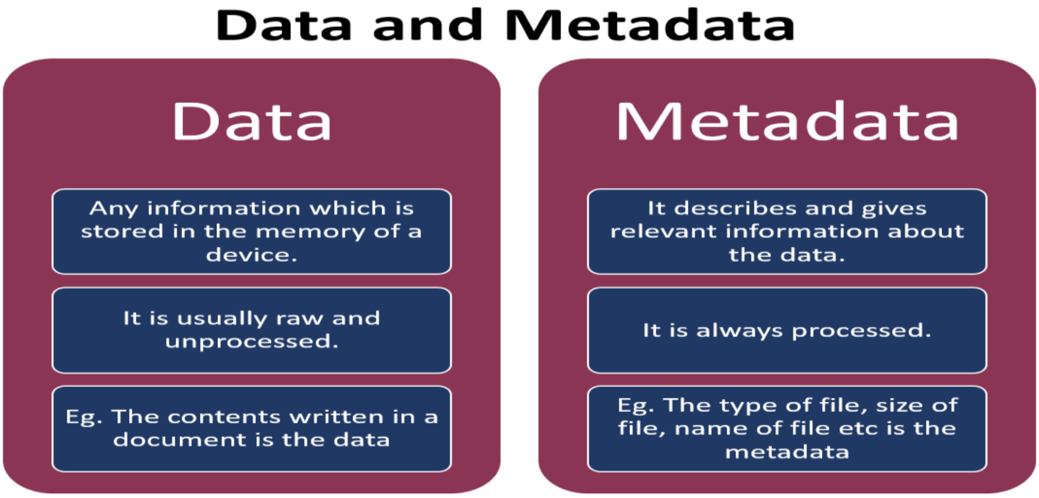
4. Mobile device acquisition: Mobile devices such as smartphones and tablets often contain valuable evidence. Specialized tools and techniques are used to acquire data from these devices. Depending on the device and its security features, acquisition methods can vary and may include logical acquisition (extracting data through the device's operating system) or physical acquisition (acquiring a bit-by-bit image of the device's storage).

5. Network traffic capture: In cases involving network-related investigations, capturing and analyzing network traffic can provide valuable evidence. This can be done using packet capture tools or network monitoring software. It allows the examiner to analyze communication patterns, identify suspicious activities, and extract relevant data from network packets.

6. Cloud-based data acquisition: With the increasing use of cloud services, it may be necessary to acquire data stored in the cloud for forensic analysis. Cloud service providers often offer APIs or tools that enable legal and authorized access to user data. The acquisition process may involve requesting data from the cloud provider or using specialized tools to extract data from cloud backups or synchronized devices.

Understanding Data and Metadata

The difference between the data and the metadata for the forensic investigation can be easily understood with the help of the diagram below;


Data and Metadata

Data

Any information which is stored in the memory of a device.

It is usually raw and unprocessed.

Eg. The contents written in a document is the data

Metadata

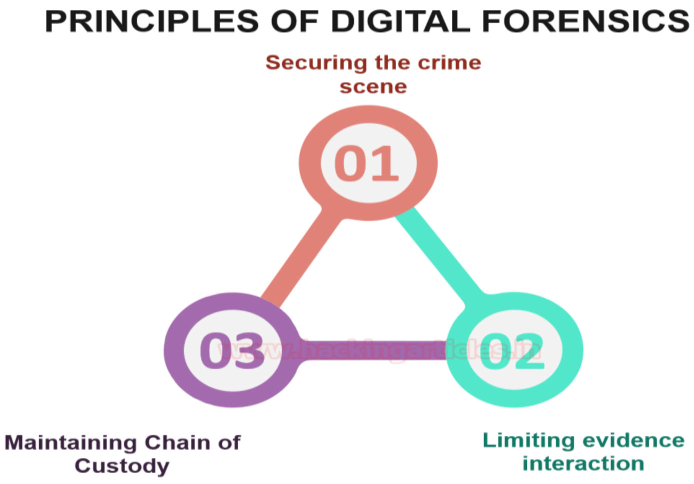
It describes and gives relevant information about the data.

It is always processed.

Eg. The type of file, size of file, name of file etc is the metadata

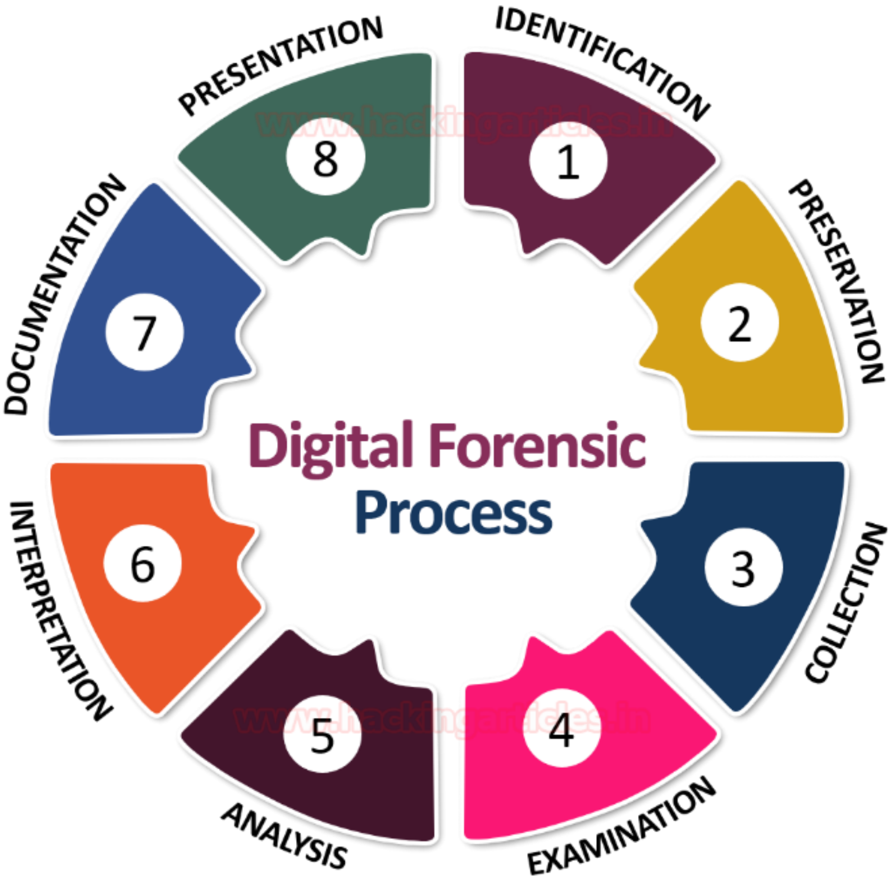
Principles of Digital Forensics

1. **Securing the Crime Scene:** This is the most primary principle of Digital Forensics. As an investigator you should prohibit any access to your suspected digital evidence, document all processes and connections, disconnecting wireless connections, etc. to keep your evidence secure.
2. **Limiting evidence Interaction:** As an investigator, you should make sure that your evidence is having a limited interaction by capturing the ram and can also perform cold boot attacks on the evidence.
3. **Maintaining Chain of Custody:** Chain of custody is a record of sequence in which the evidence was collected, date and timestamps at the collection, the investigator who accessed and handled it, etc.


PRINCIPLES OF DIGITAL FORENSICS
Securing the crime scene
01
02
03
Maintaining Chain of Custody
Limiting evidence interaction

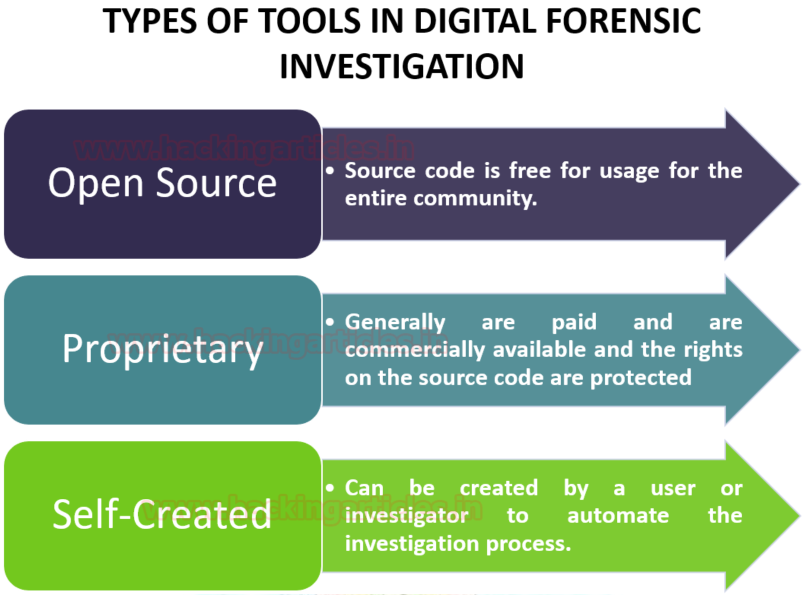
Process of Digital Forensic Investigation

1. **Identification:** This is the first step that an investigator takes at the crime scene is to identify the purpose of the investigation and recognize the potential digital evidence.
2. **Preservation:** This is the next step where the investigator has to be careful as he should make sure that the evidence has not tampered which may complicate the investigation
3. **Collection:** This step involves acquiring the evidence most appropriately without causing any harm to the evidence and packing it in a Faraday Bag.
4. **Examination:** This step is a precursor to performing any analysis of the evidence. This step requires careful inspection of the evidence for any other secondary details.
5. **Analysis:** In this step, the investigator carries out the most crucial things like joining the bits and pieces of the pieces of evidence, retrieving deleted files, etc.
6. **Interpretation:** This step involves concluding the investigation finding after reconstruction of the crime scene.
7. **Documentation:** This step usually involves preparing a detailed report or a document on the entire investigation.
8. **Presentation:** This is a mandatory step only when it is asked for cross-examination which is to be mentioned in very simple terms of understanding for commoners.



Types of Tools

An investigator needs to have the right set of tools for conducting a digital forensic investigation. It is for the investigator to decide the tool appropriate for the case. The tools also depend on the application based on hardware and software. The types of tools can be classified into three types; Open Source, Proprietary, and Self-created.



TYPES OF TOOLS IN DIGITAL FORENSIC INVESTIGATION

Open Source
- Source code is free for usage for the entire community.

Proprietary
- Generally are paid and are commercially available and the rights on the source code are protected

Self-Created
- Can be created by a user or investigator to automate the investigation process.

https://www.hackingarticles.in/digital-forensics-an-introduction/
https://www.hackingarticles.in/ctf-challenges-walkthrough/