DIGITAL FORENSICS
-AN INTRODUCTION

Table of Contents

# Abstract

There are situations where an individual or an organization may become a victim of a cyber-attack, and you might wonder what is the correct way to proceed with it. A thorough Digital Forensics investigation can provide closure for investigating these attacks. In this article, we will be learning about the fundamentals of Digital Forensics.

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.

Elements of a 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.

ELEMENTS OF A CRIME

Crime scene — Evidence — Suspect/Criminal — Victim
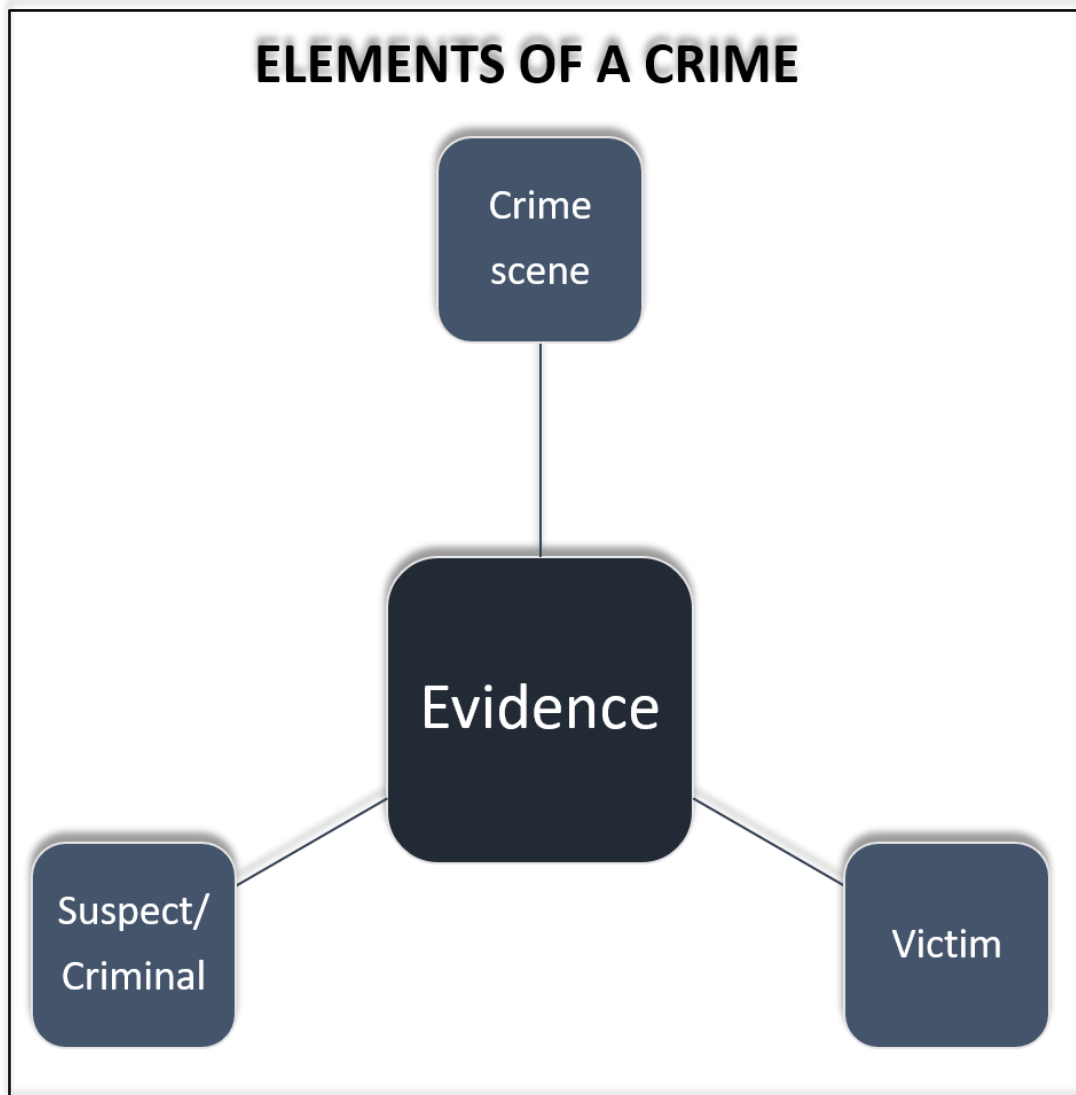
In the year 1978 the first computer crime was recognized in the Florida Computer Crime Act.

iGNITE
Technologies

Goals of a Digital Forensics Examiner

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

#	Goal
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?

European lead international treaty, the Convention on Cybercrime, came into force in 2004

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 it can be classified into more depending on the cases.

|	
🖥	Computer Forensics
📡	Network Forensics
▶	Multimedia Forensics
📱	Mobile Forensics
🔲	Memory Forensics
☁	Cloud Forensics
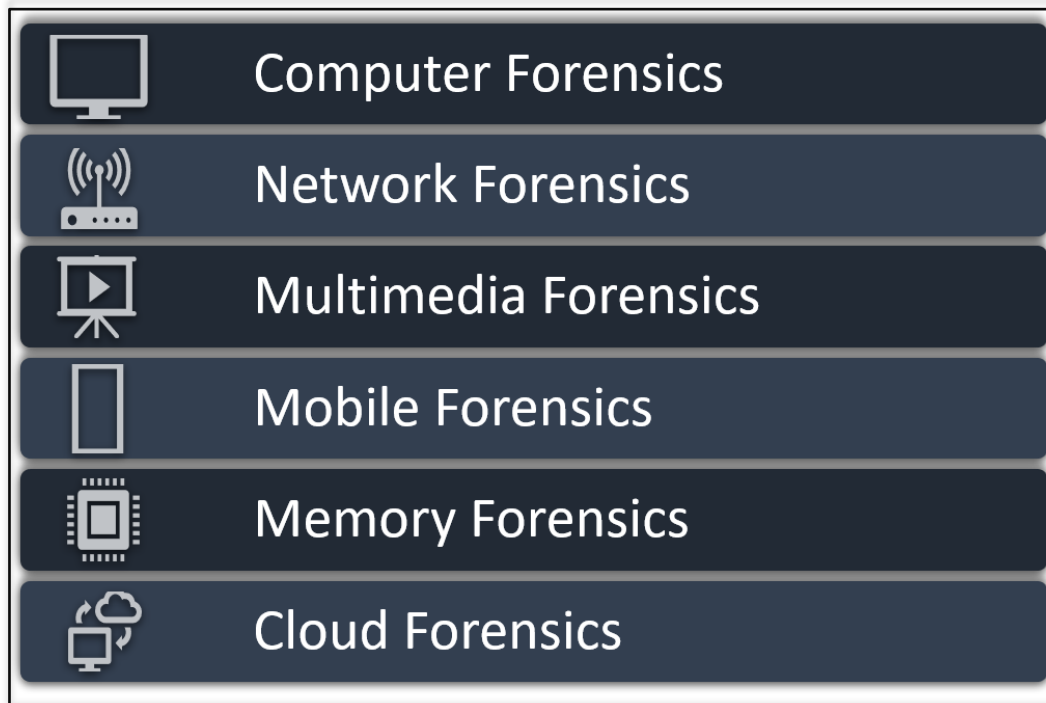
Digital Evidence

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.

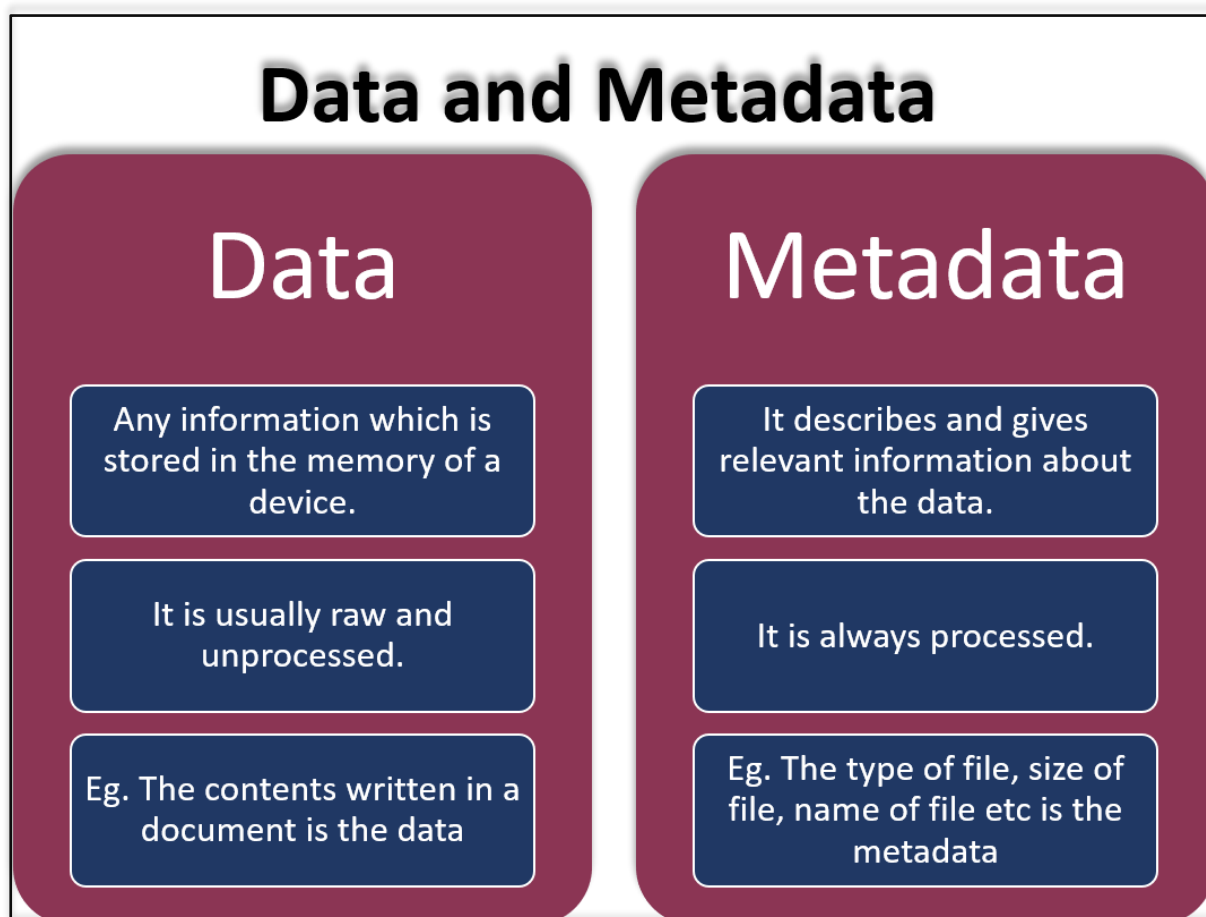**The evidence found at the crime scene should have two key properties**

a. They should be admissible in the court
b. They should be authentic.

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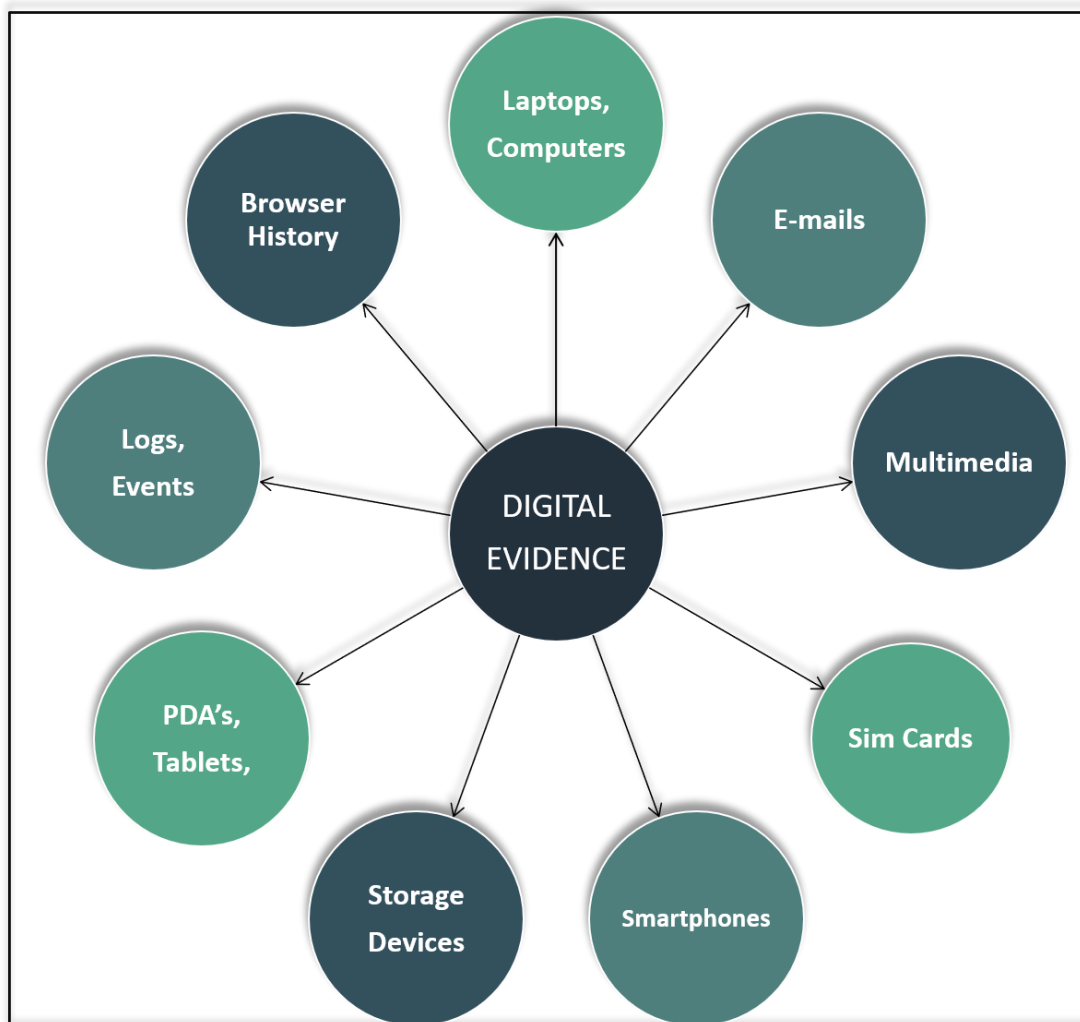
Understanding Data and Metadata

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

Metadata is often defined as Data in Data

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.
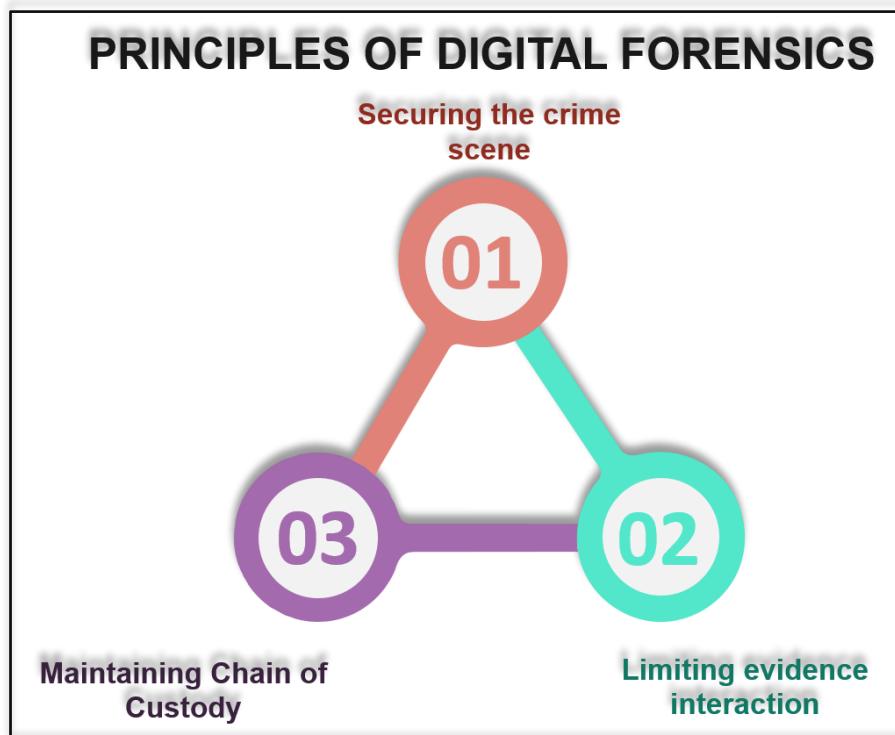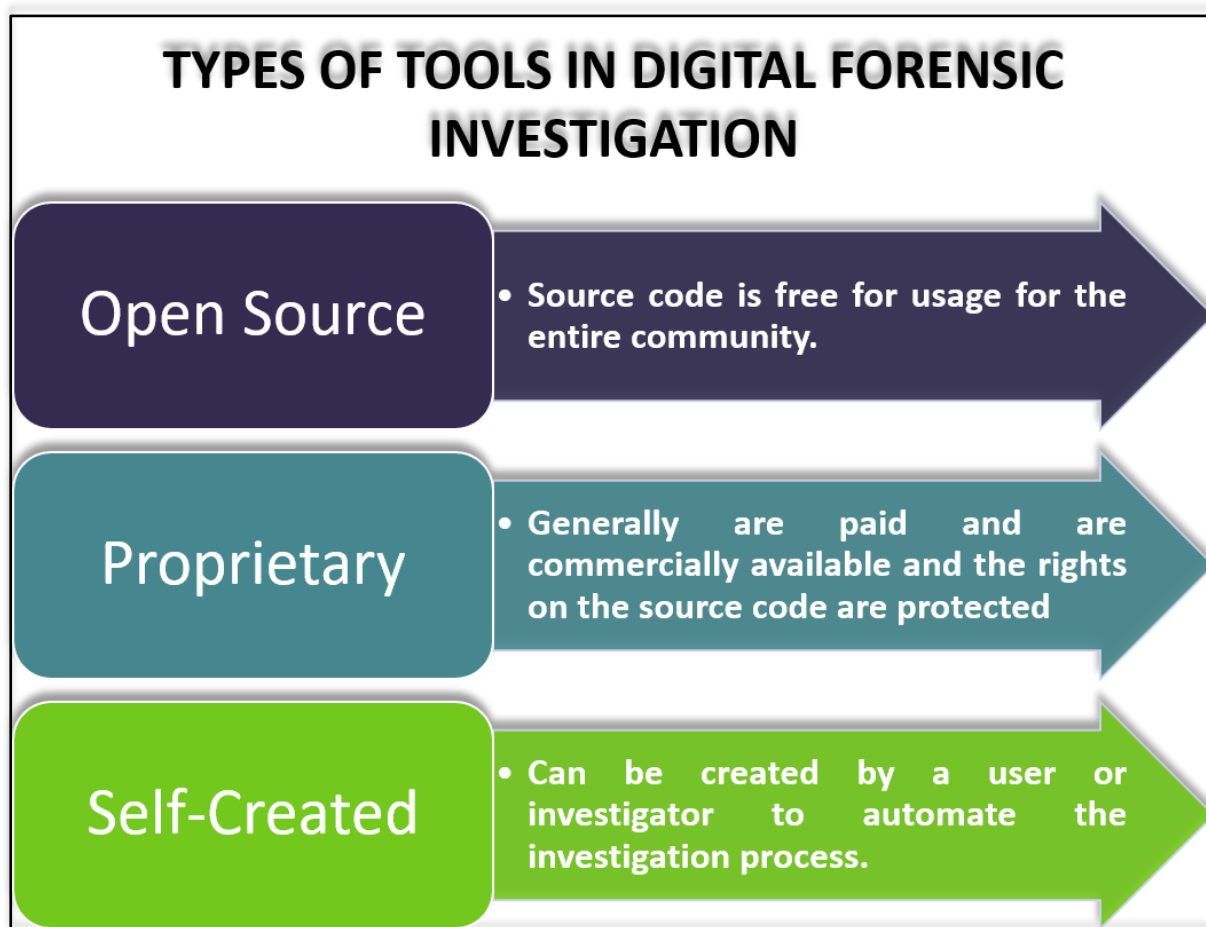
Process of Digital Forensic Investigation

- **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.
- **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
- **Collection:** This step involves acquiring the evidence most appropriately without causing any harm to the evidence and packing it in a Faraday Bag.
- **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.
- **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.
- **Interpretation:** This step involves concluding the investigation finding after reconstruction of the crime scene.
- **Documentation:** This step usually involves preparing a detailed report or a document on the entire investigation.
- **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.
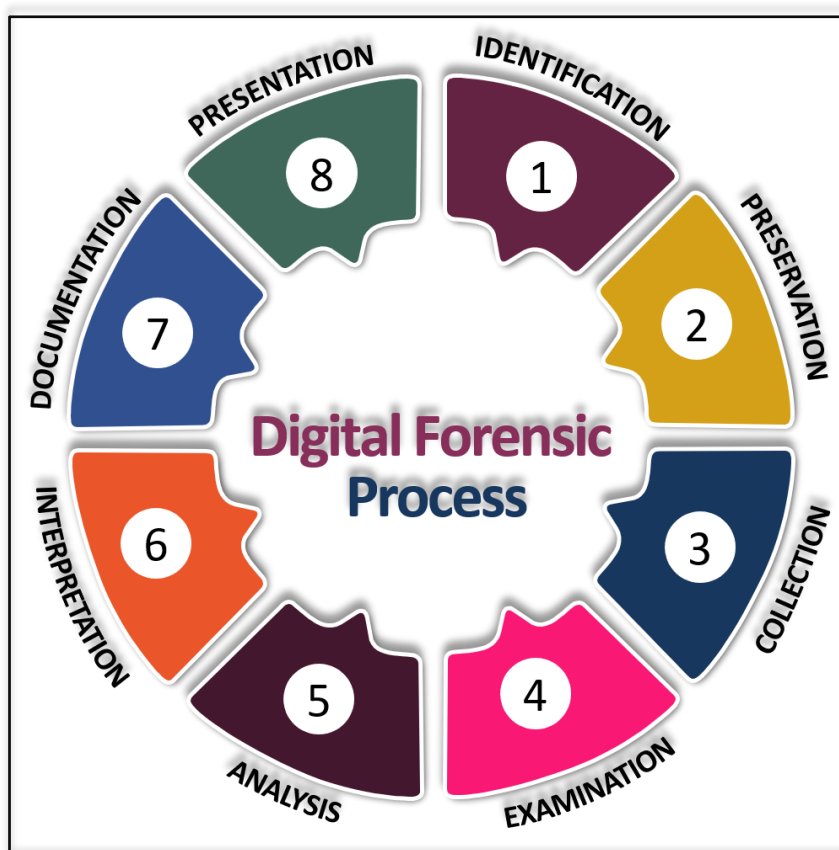
Types of Tools

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.

Difference between E-discovery and Digital Forensics

The Internet community is many times confused between these two terms. Here a few points that highlight the importance and usage of E-discovery and Digital Forensics.

E-discovery

E-Discovery stands for Electronic Discovery. It can be defined as the process involved in collecting, preparing, reviewing, interpreting, and presenting the electronic documents from hard disks and other forms of storage devices in civil litigations. The following are the key points to remember in E-discovery.

E-DISCOVERY	
🔨	Useful in Civil Litigations
◆	Does not involve erased data
🗄	Focuses on data in Allocated Spaces
📏	Limited Data Recovery
📰	Testimony is based on Facts

Digital Forensics

Digital Forensics can be defined as the process of preservation, identification, extraction, and documentation of digital evidence which is used by the court of law to facilitate criminal investigations.

DIGITAL FORENSICS	
🔗	Useful in Criminal Investigation
♻	Deleted Data can be recovered
📄	Focuses on data in Unallocated Spaces as well
🔍	Finding of data is unrestricted
👩	Testimony is based on Digital Forensic Expert

iGNITE
Technologies

www.hackingarticles.in

Methodology for DF Investigator

A Digital Forensic Investigator has a huge responsibility on his shoulders when he is investigating a case as his findings will bring justice to the innocent and punish the criminal. Therefore, there a set of steps that he should follow when he is investigating a case. The following are a generalized step of the investigation, whereas the Investigator can follow the steps prescribed by their Institution or the framework they follow.

STEP 01: **Prepare a preliminary design or a method to approach the case-** The investigator should prepare a method on how he will go about with the investigation and have a clear understanding of the crime scene.
He should make sure that at a scene where the computer or a device is in a power-on state, he should not make the mistake of turning it off, or running any program or perform any other activity.

STEP 02: **Determine the resources that are required for the case-** The investigator has to understand the requirements of tools and technologies that are required for the case to be investigated further. He should be qualified enough and should make sure that he prevents data from being over-written.

STEP 03: **Discover and obtain the evidence-** The investigator has to make sure that he does not miss out on any evidence at the scene of the crime and obtains them within the most accurate way, which does not cause any damage to the evidence.
The Investigator should make sure to collect the evidence sample in a Faraday Bag or an anti-static bag so that the evidence cannot be tampered with.
He should make sure at every moment to maintain the chain of custody.

STEP 04: **Make multiple Forensic copies of the evidence-** In Digital Forensic Investigation, it is very essential to remember that as long as possible, one should never work on the original evidence item. The investigator should make sure to create multiple copies of the same and perform analysis on the copy of the original evidence.
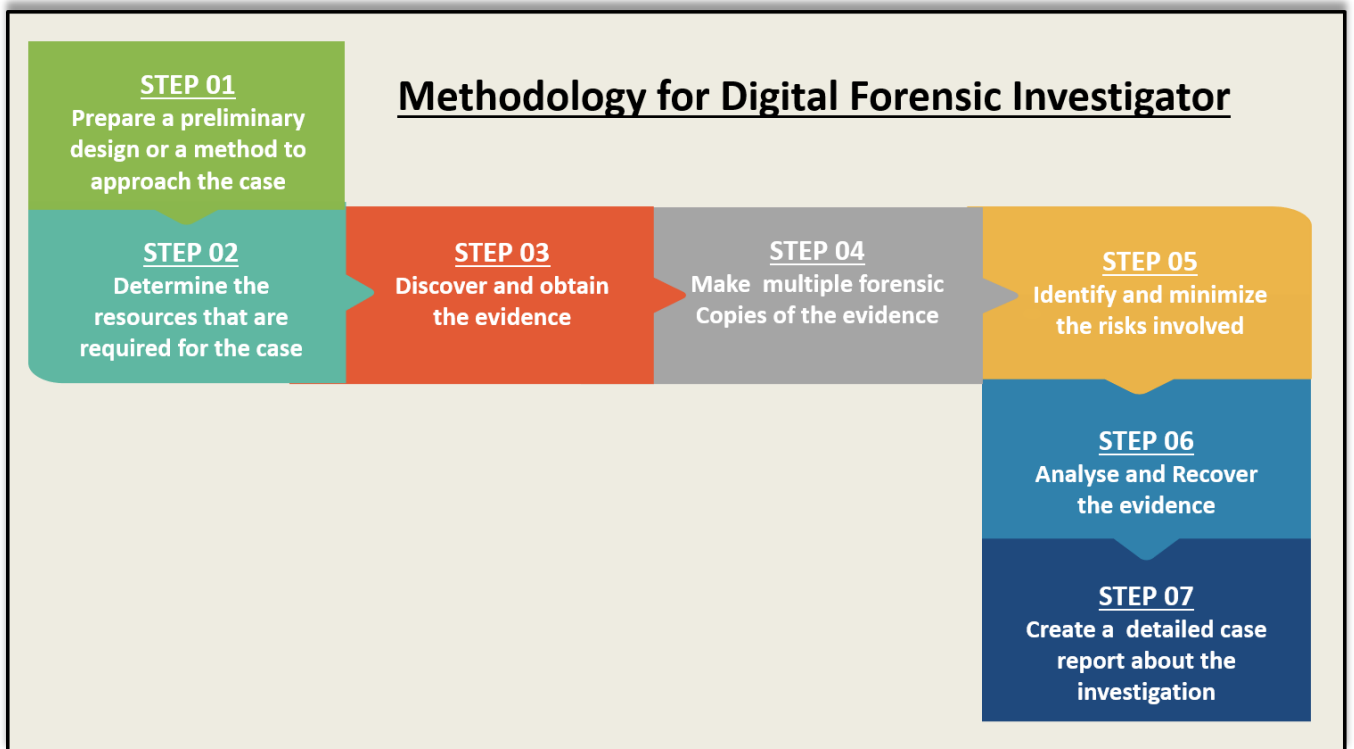Before he creates a copy of the evidence, he should always calculate the hash value of the evidence that as recovered in the original form to maintain the authenticity of the evidence.

STEP 05: **Identify and minimize the risks involved-** The investigator should remember that the evidence that is collected is not always easy to analyse. There are a huge number of risks and consequences that are involved. He should be qualified enough to estimate the amount of risk and possible damage. He should try to come up with better alternatives to minimize the risk.

STEP 06: **Analyse and Recover the evidence-** Once the investigator has the evidence, he can now start analysing the copy of the original evidence by using various commercial and open-source software that is suitable for that case. He can also use various software to recover the evidence that has been deleted.

STEP 07: Create a detailed case report about the investigation- Once the investigator has completed the analysis of the evidence and has found important artefacts on recovering data, he can then create a detailed report about his findings, methodologies, and tools used by him in the investigation.
If required by the jury or the court, the investigator has to represent himself in the court as an expert witness to give his testimony on the case in simpler terms for the people from a non-technical background to have a better understanding of the case.

Methodology for Digital Forensic Investigator

STEP 01
Prepare a preliminary design or a method to approach the case

STEP 02
Determine the resources that are required for the case

STEP 03
Discover and obtain the evidence

STEP 04
Make multiple forensic Copies of the evidence

STEP 05
Identify and minimize the risks involved

STEP 06
Analyse and Recover the evidence

STEP 07
Create a detailed case report about the investigation

Evidence Collection Methods

The method of collection of evidence terms are inter-related and almost serve the same purpose, the only important thing for an investigator to remember is that the copy should be forensically sound.

- **Image Copy:** It refers to be the duplicate of the original disk.
- **Bit-Stream Image:** It is a clone copy of the original evidence. It includes files from sectors, clusters, and retrieves deleted files of a disk.
- **Bit-Stream Copy:** A bit-stream copy can be defined as a bit-by-bit copy of the original evidence or storage medium which can be its exact copy. A bit-stream copy can also be called a Forensic Copy of the disk.
- **Mirror Copy:** A mirror copy is the precise replica (backup) of the disk.
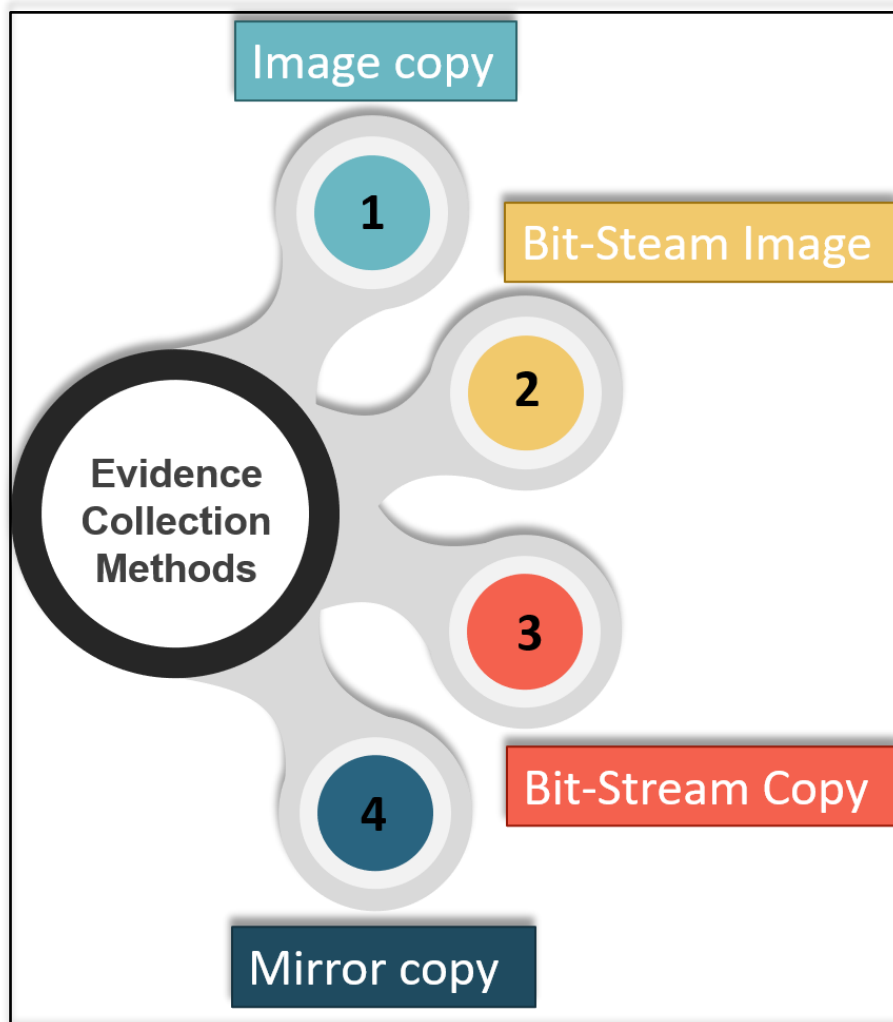
Disk Imaging and Cloning

❖ **Disk Imaging**

It is the process of making an archival or backup copy of the entire hard drive. It is a storage file that contains all the necessary information to boot to the operating system. However, this imaged disk needs to be applied to the hard drive to work. One cannot restore a hard drive by placing the disk image files on it as it needs to be opened and installed on the drive using an imaging program. A single hard drive can store many disk images on it. Disk images can also be stored on flash drives with a larger capacity.

❖ **Disk Cloning**

It is the process of copying the entire contents of a hard drive to another including all the information that can boot to the operating system from the drive. It allows you to create a one-to-one copy of one of your hard drive on another hard drive. The other copy of the hard drive is completely functional and can be swapped with the computer's existing hard drive. If the cloned drive is booted, its data will be identical to the source drive at the time it was created.

Below is a simple difference between Disk Imaging and Cloning.

DISK IMAGING & CLONING

IMAGING	CLONING
• Larger in size	• Comparatively Smaller in size
• Compressed Copy	• Uncompressed Copy
• Archival or a Backup Copy	• Replica of your Drive

Challenges faced by DF Investigator

Legal Issues: The most important issue an investigator may encounter is getting the guarantee evidence admissibility which means that it should be accepted by the court.

Nature of Digital Evidence: The advancement in technology has impacted the investigation in such a way that it detecting the digital evidence has become extremely difficult. For example, cloud storage, PDAs, IoT devices, etc.

Alteration of Evidence: The chain of custody should be maintained at all times to keep the evidence's credibility intact. If the evidence is in the wrong hands, the evidence might get altered and may lose its credibility. Therefore, having a Forensic image and the hash value of the evidence is extremely important for the investigator.

Size and Distribution of the evidence: The size and the distribution of the evidence matter because the data is no smaller. There is a huge amount of data produced regularly. In cases of Big data Forensic Investigation, the size and the widely distributed data comes up as a challenge for the investigator as he does not know where to start.

Malware Present in evidence: The criminals can outsmart the investigators and insert malware in the evidence device which can mislead or disrupt the ongoing investigation.

Steganography: In earlier times, steganography had only limited types but today, due to the availability of various tools and software on the dark web, it has become extremely difficult to detect steganography present in the evidence items. Sometimes the investigator doesn't consider it as evidence as they aren't able to get many in-depth ideas about the evidence.

Encryption: Many a time, the evidence is recovered in an encrypted form and the investigator has a hard time to decrypt the evidence with no assurance of recovery of the original contents.

Challenges In Digital Forensic Investigation

- Legal Issues
- Nature of Digital Evidence
- Alteration of Evidence
- Size and Distribution of evidence
- Malwares present in evidence
- Steganography
- Encryption

Pros of Digital Forensics 👍

- Its purpose is to make sure of the integrity of the digital system.
- It also assists in protecting the organization's valuable money.
- It benefits the organizations to record essential information in cases where the systems have been compromised.
- If the investigation is performed efficiently, it helps arrests the cyber-criminals globally.
- It helps in producing the correct evidence, which can help punish the culprit.

Cons of Digital Forensics 👎

- The digital evidence accepted into court should be proven to be tamper-free.
- Storing and producing electronic documents is expensive
- Legal practitioners lack technical knowledge.
- The evidence should be convincing and authentic.
- Unrecognized investigation tools may not be accepted by the court

Conclusion

Hence, in this article we have covered the basic topics that are required to have a better understanding of Digital Forensics for another level.

References
- https://www.hackingarticles.in/digital-forensics-an-introduction/
- https://www.hackingarticles.in/digital-forensics-an-introduction-part-2/

About us
"Simple training makes Deep Learning"

"IGNITE" is a worldwide name in the IT field. As we provide high-quality cybersecurity training and consulting services that fulfil students, government and corporate requirements.
We are working towards the vision to "Develop India as a Cyber Secured Country". With an outreach to over eighty thousand students and over a thousand major colleges, Ignite Technologies stood out to be a trusted brand in the Education and the Information Security structure.

We provide training and education in the field of Ethical Hacking & Information Security to the students of schools and colleges along with the corporate world. The training can be provided at the client's location or even at Ignite's Training Center.
We have trained over 10,000 + individuals across the globe, ranging from students to security experts from different fields. Our trainers are acknowledged as Security Researcher by the Top Companies like - Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more. Even the trained students are placed into a number of top MNC's all around the globe. Over with this, we are having International experience of training more than 400+ individuals.

The two brands, Ignite Technologies & Hacking Articles have been collaboratively working from past 10+ Years with about more than 100+ security researchers, who themselves have been recognized by several research paper publishing organizations, The Big 4 companies, Bug Bounty research programs and many more.

Along with all these things, all the major certification organizations recommend Ignite's training for its resources and guidance.
Ignite's research had been a part of number of global Institutes and colleges, and even a multitude of research papers shares Ignite's researchers in their reference.

What We Offer

Ethical Hacking

The Ethical Hacking course has been structured in such a way that a technical or a non-technical applicant can easily absorb its features and indulge his/her career in the field of IT security.

Bug Bounty 2.0

A bug bounty program is a pact offered by many websites and web developers by which folks can receive appreciation and reimbursement for reporting bugs, especially those affecting to exploits and vulnerabilities.
Over with this training, an indivisual is thus able to determine and report bugs to the authorized before the general public is aware of them, preventing incidents of widespread abuse.

Network Penetration Testing 2.0

The Network Penetration Testing training will build up the basic as well advance skills of an indivisual with the concept of Network Security & Organizational Infrastructure. Thereby this course will make the indivisual stand out of the crowd within just 45 days.

Red Teaming

This training will make you think like an "Adversary" with its systematic structure & real Environment Practice that contains more than 75 practicals on Windows Server 2016 & Windows 10. This course is especially designed for the professionals to enhance their Cyber Security Skills

CTF 2.0

The CTF 2.0 is the latest edition that provides more advance module connecting to real infrastructure organization as well as supporting other students preparing for global certification. This curriculum is very easily designed to allow a fresher or specialist to become familiar with the entire content of the course.

Infrastructure Penetration Testing

This course is designed for Professional and provides an hands-on experience in Vulnerability Assessment Penetration Testing & Secure configuration Testing for Applications Servers, Network Deivces, Container and etc.

Digital Forensic

Digital forensics provides a taster in the understanding of how to conduct investigations in order for business and legal audiences to correctly gather and analyze digital evidence.