Digital Forensics: An Introduction (Part 2)

September 24, 2020 By Raj Chandel

In the first part of this article, we have seen the Elements of a Digital Crime, Goals of Digital Forensic Investigation, Classification of Digital Forensics, Digital Evidence, Principles of Digital Forensics, Process of Forensic Investigation, Types of Tools, etc.

Digital Forensics: An Introduction

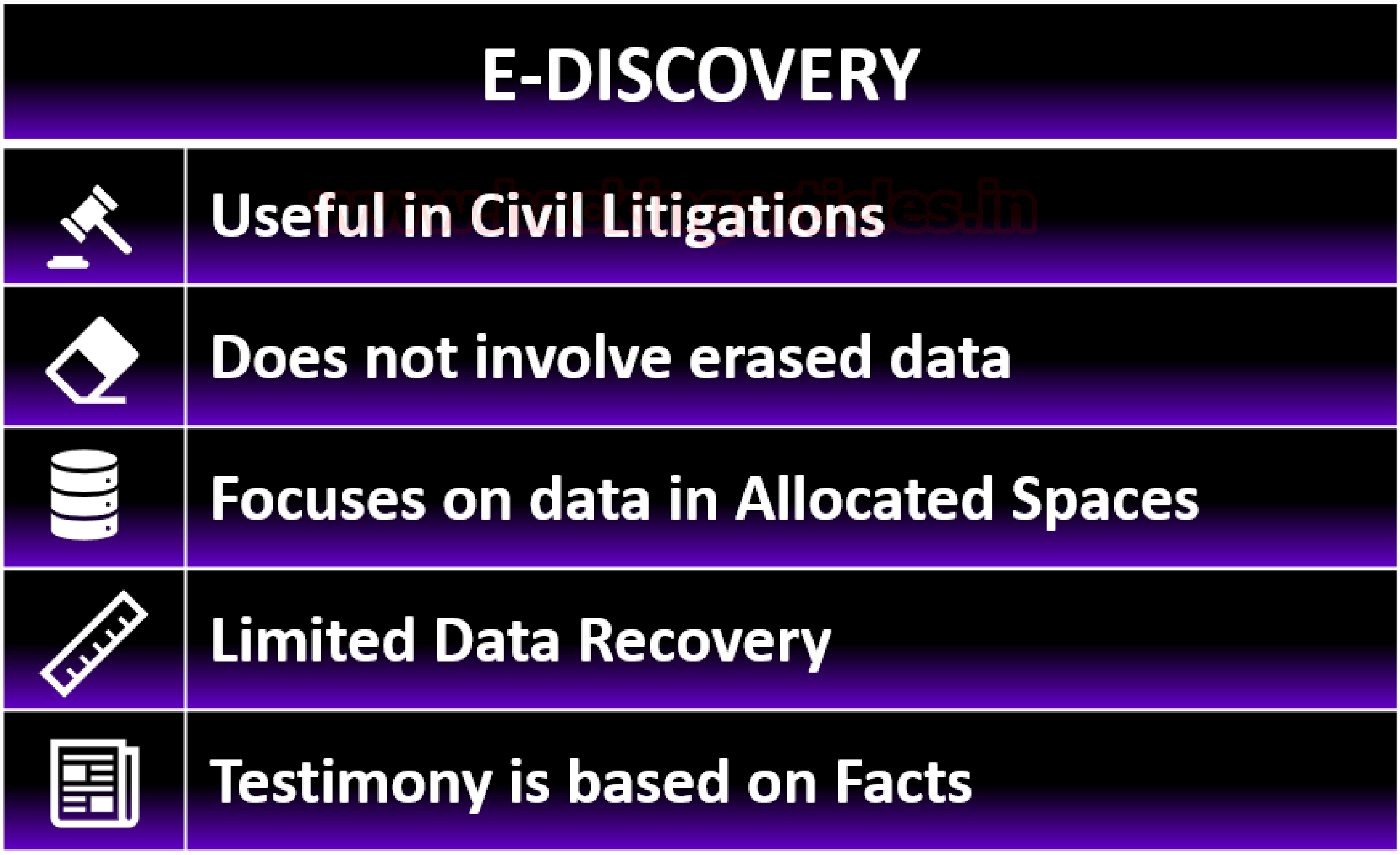
Table of Contents:

Understanding the difference between E-Discovery & 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

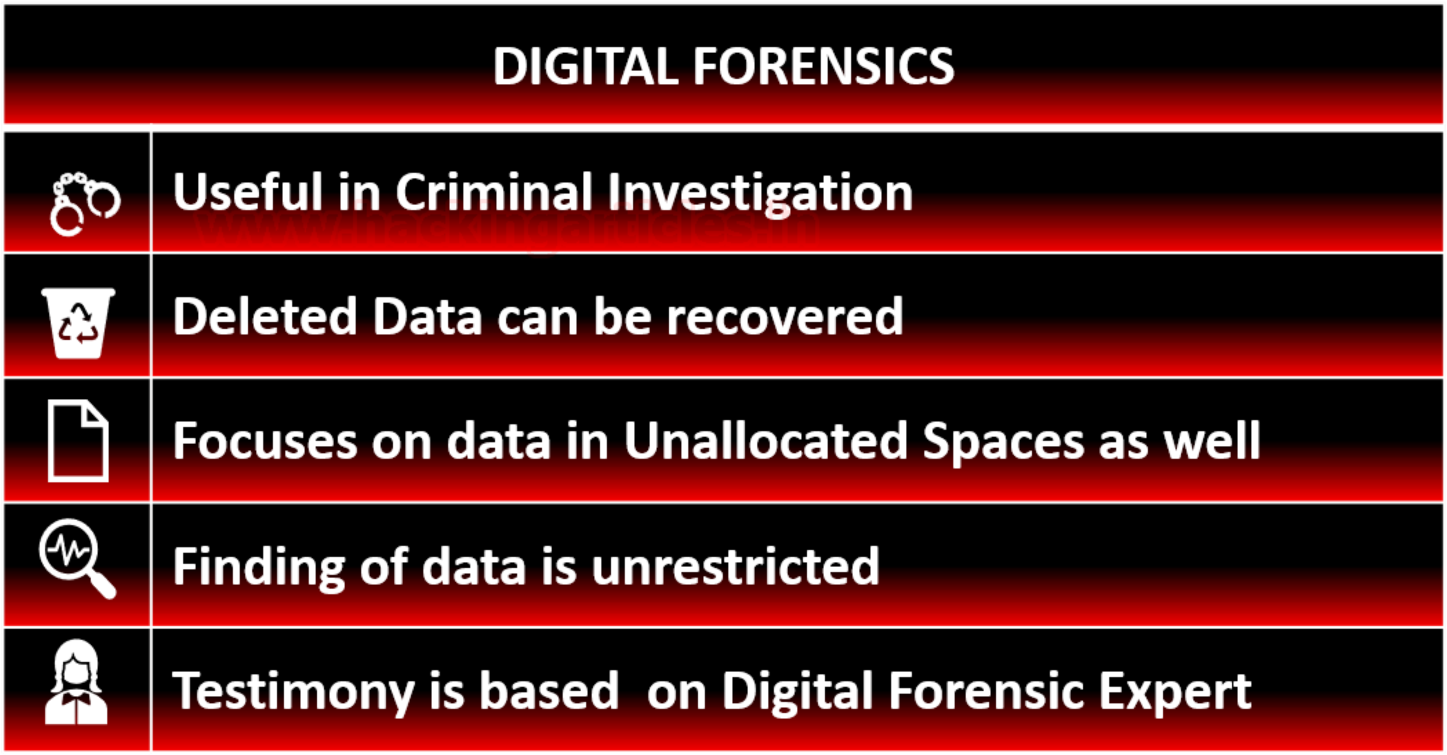
E-Discovery stands for Electronic Discovery. It can be defined as the process involved in collecting, preparing, reviewing, interpreting, and presenting the electronic documents from hard disks and other forms of storage devices in civil litigations. The following are the key points to remember in E-discovery.



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

Methodology for Digital Investigators

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.

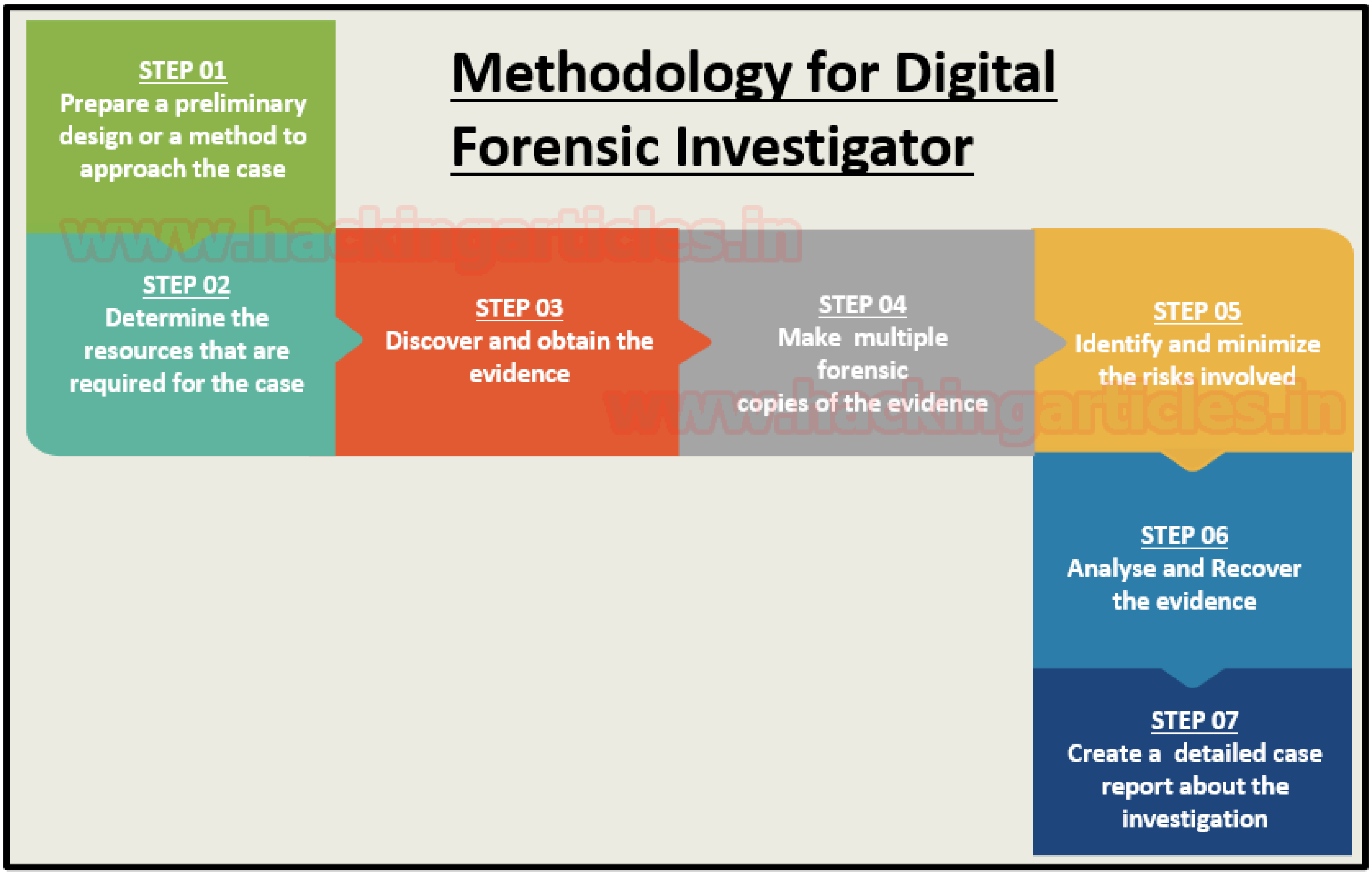
He should make sure that at a scene where the computer or a device is in a power-on state, he should not make the mistake of turning it off, or running any program or perform any other activity.

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.



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

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 analyze. There are a huge amount 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 analyzing 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 artifacts 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.

Evidence Collection Methods

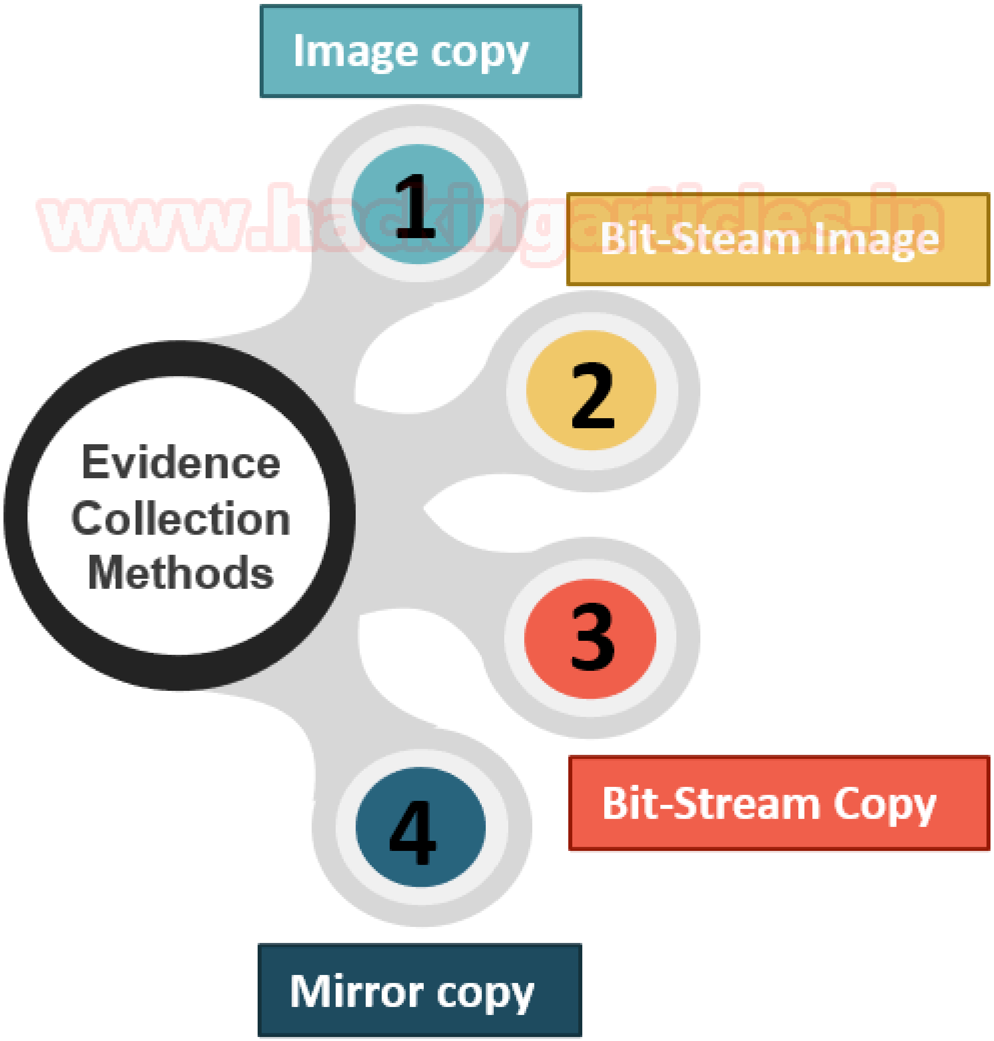
The method of collection of evidence terms are inter-related and almost serve the same purpose, the only important thing for an investigator to remember is that the copy should be forensically sound.

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 as a Forensic Copy of the disk.

Mirror Copy: A mirror copy is the precise replica (backup) of the disk.



Disk Imaging and Cloning

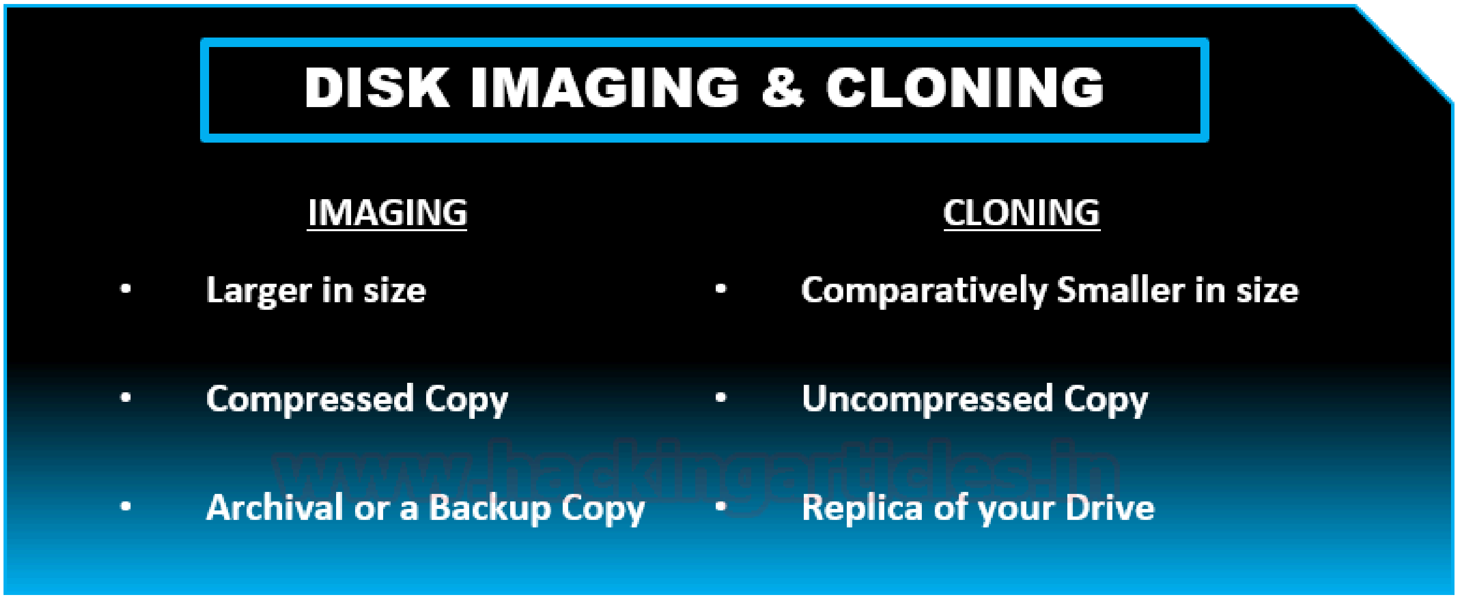
Disk Imaging

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 Digital Forensic 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.

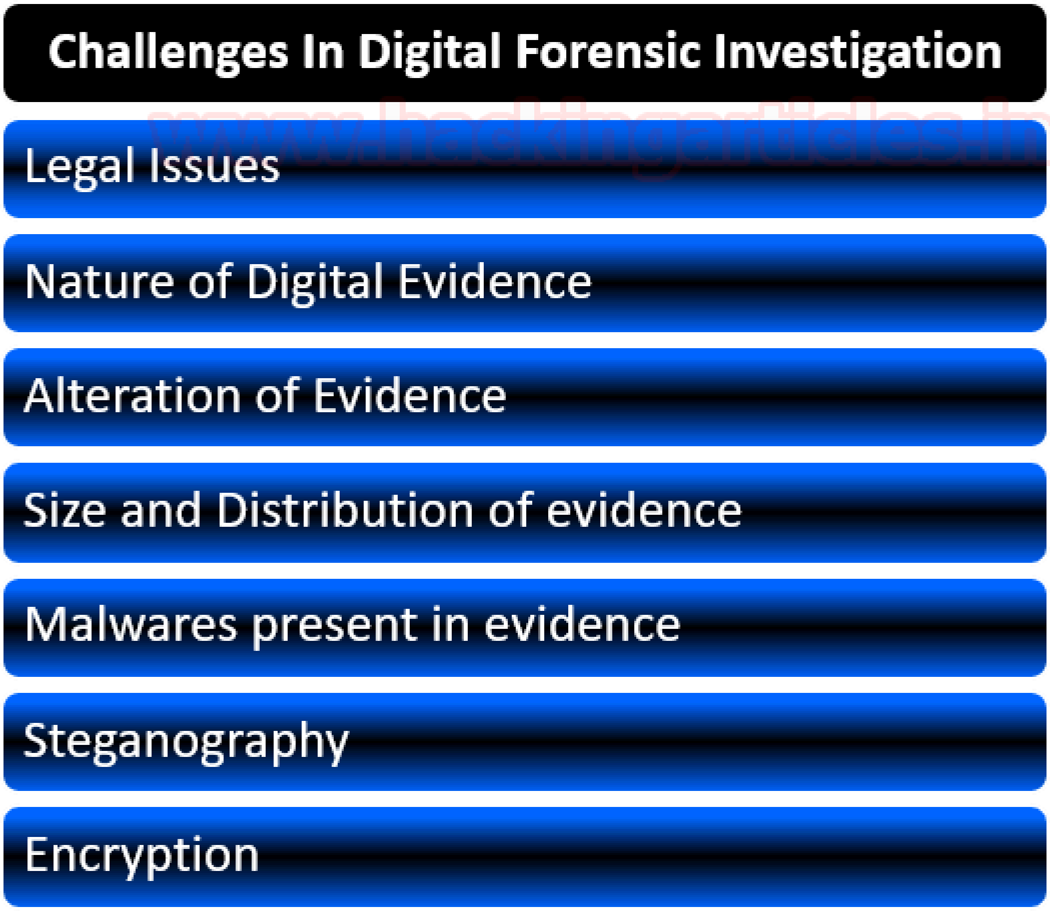
Alteration of Evidence: The chain of custody should be maintained at all times to keep the evidence's credibility intact. If the evidence is in the wrong hands, the evidence might get altered and may lose its credibility. Therefore, having a Forensic image and the hash value of the evidence is extremely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