


# What is Digital Forensics? History, Process, Types, Challenges

By : Lawrence Williams    ⌚ Updated August 30, 2023

 Ads by Google

[Stop seeing this ad](#) [Why this ad? ⓘ](#)

## What is Digital Forensics?

Digital Forensics is 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.

**Table of Content:**



## History of Digital forensics

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1882 – 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.

- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called “Best practices for Computer Forensics”.
- In 2010, Simson Garfinkel identified issues facing digital investigations.

## Objectives of computer forensics

Here are the essential objectives of using Computer forensics:

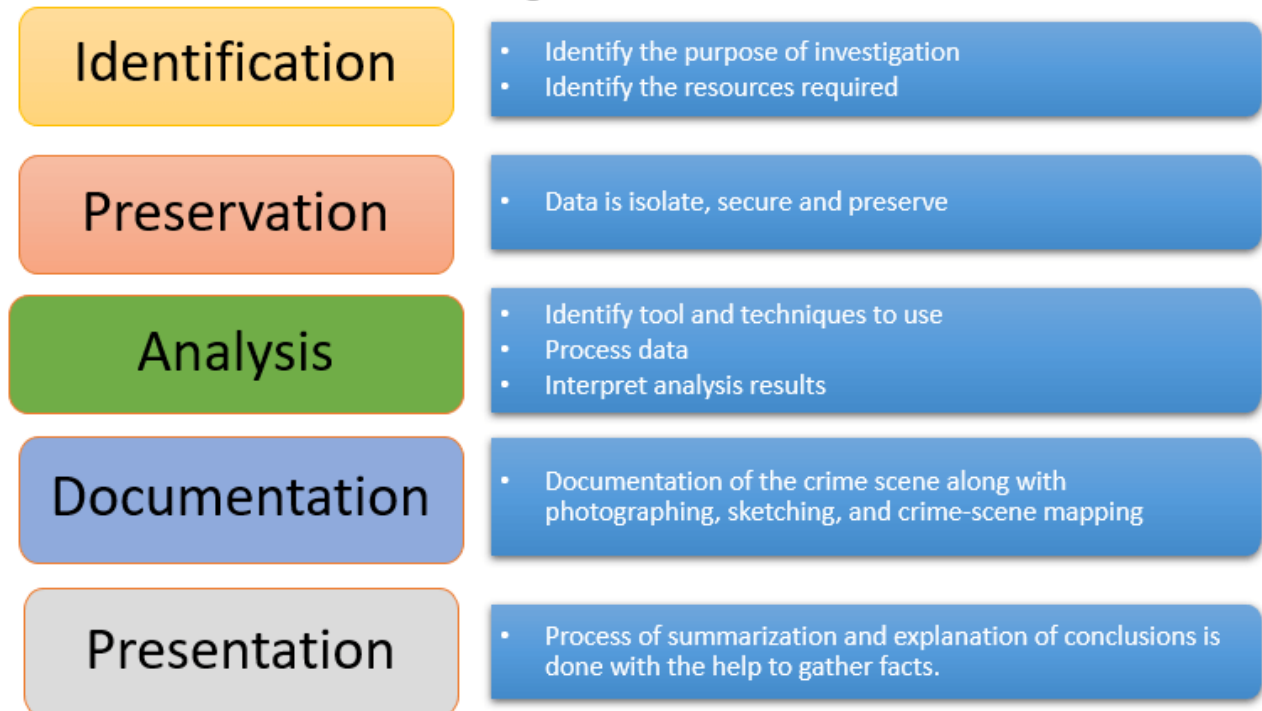
- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

## Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

© guru99.com



## Process of Digital Forensics

Let's study each in detail

### Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

### Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

### Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

## **Documentation**

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

## **Presentation**

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

## **Types of Digital Forensics**

Three types of digital forensics are:

### **Disk Forensics:**

It deals with extracting data from storage media by searching active, modified, or deleted files.

### **Network Forensics:**

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

## Wireless Forensics:

It is a division of network forensics. The main aim of wireless forensics is to offer the tools needed to collect and analyze the data from wireless network traffic.

## Database Forensics:

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

## Malware Forensics:

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

## Email Forensics

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

## Memory Forensics:

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

## Mobile Phone Forensics:

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

## 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.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

## Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

## Advantages of Digital forensics

Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

# Disadvantages of Digital Forensics

Here, are major cos/ drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

## Summary

- Digital Forensics is the preservation, identification, extraction, and documentation of computer evidence which can be used in the court of law
- Process of Digital forensics includes 1) Identification, 2) Preservation, 3) Analysis, 4) Documentation and, 5) Presentation
- Different types of Digital Forensics are Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Email Forensics, Memory Forensics, etc.
- Digital forensic Science can be used for cases like 1) Intellectual Property theft, 2) Industrial espionage 3) Employment disputes, 4) Fraud investigations.

## You Might Like:

- [What is Hacking? Types of Hackers \(Introduction to Cyber Crime\)](#)
- [Top 100+ Cyber Security Interview Questions and Answers](#)
- [What is Cybercrime? Types, Tools, Examples](#)
- [10 Best FREE DDoS Attack Tool Online \(2023\)](#)
- [21 Top Cyber Security Companies \(2023\)](#)



## About

[About Us](#)

[Advertise with Us](#)

[Write For Us](#)

[Contact Us](#)

## Career Suggestion

[SAP Career Suggestion Tool](#)

[Software Testing as a Career](#)

## Interesting

[eBook](#)

[Blog](#)

[Quiz](#)

[SAP eBook](#)

## Execute online

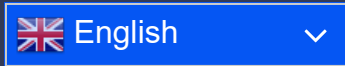
[Execute Java Online](#)

[Execute Javascript](#)

[Execute HTML](#)

[Execute Python](#)





© Copyright - Guru99 2023    [Privacy](#).  
[Policy](#) | [Affiliate Disclaimer](#) | [ToS](#)