Digital Forensics

ARIJIT BHOWMICK

Digital Forensics

>> Definition

Digital forensics is the process of retrieving, storing, analyzing and preserving electronic data that could be useful in an investigation.
This includes information from computers Hard Drives, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, IOT Devices and other digital devices.

The goal of the process is to gather, analyze and preserve evidence. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

Digital Forensics

>> 🕵 Digital Evidence

Digital Evidence is any significant information stored or transmitted in digital form that a party to a court case may use at trial. They are any digital information which are received from computers, audio files, video recordings, digital images etc. The evidence obtained is essential in computer and cyber crimes.

Digital Evidences such as word processing documents, spreadsheets, internet browser histories, databases, the contents of computer memory and computer backup can be produced in Court of law. The authentic digital evidences are accepted for the cybercrime case.

The term digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

Information that is stored and transmitted on digital devices.

Digital Forensics

>> Example of Digital Evidence

Many court have allowed the use of:

- e-mails
- Digital Photographs
- ATM Transaction Logs
- Word Processing Documents
- Message Histories
- Files Saved From Accounting Programs
- Spreadsheets
- Internet Browsing Histories
- Database Entries
- Memory Dumps
- Backup Data and Printouts
- GPS Tracks
- IoT Logs
- Media Files

Digital Forensics

>> Characteristics of Digital Evidence

✓ **Digital Evidence must be:**

- Admissible
- Authentic
- Accurate
- Complete
- Believable

Digital Forensics

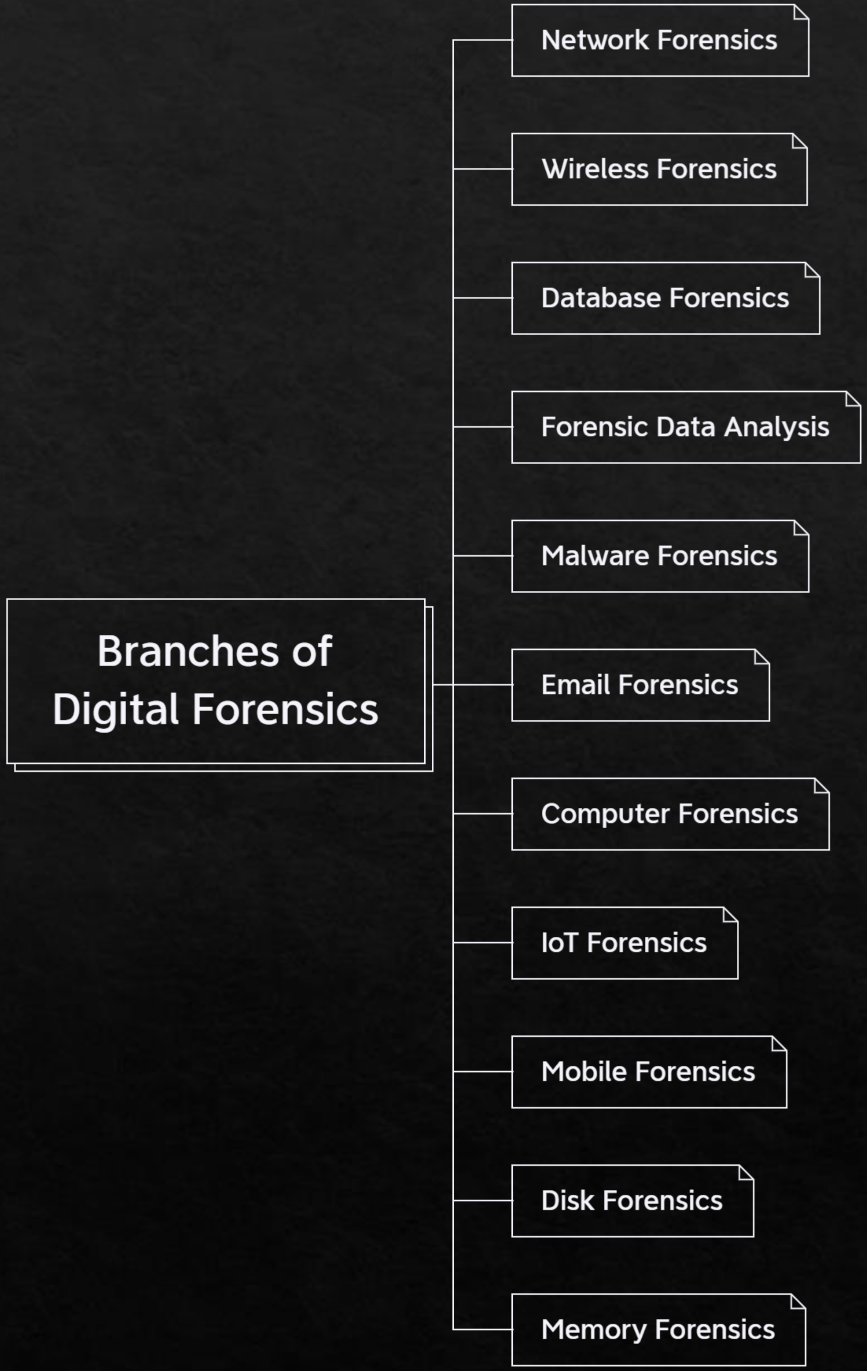
>> Why do we need Digital Forensics ?

✓ Importance of Digital Forensics:

- Identifying the cause and possible intent of an incident
- Safeguarding digital evidence collected before it becomes obsolete
- Increasing Security Hygiene, and Retracing Important Data that can be used as a Digital Evidence
- Fixing, Dumping & Cloning Data gathered from the detrimented Hardware Devices
- Identifying the duration of unauthorized access and/or modification of data in the Evidence and/or in the Network
- Geolocating the logins and mapping them to retrieve evidence about the incident

Digital Forensics

>>> Branches



Branches of Digital Forensics

- Network Forensics
- Wireless Forensics
- Database Forensics
- Forensic Data Analysis
- Malware Forensics
- Email Forensics
- Computer Forensics
- IoT Forensics
- Mobile Forensics
- Disk Forensics
- Memory Forensics

Digital Forensics

>>> Branches

>> 🖧 Network Forensics

Network Forensics is a sub-branch of Digital Forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or Intrusion Detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network Traffic is transmitted and then lost, so Network Forensics is often a pro-active investigation.

It is focused on capturing data from Networks in addition to analyzing network access and usage. This is highly relevant when analyzing cyber attacks as analyzing this information can help with reconstructing the attack strategy that was used. Law enforcement agencies use network forensics to analyze traffic from the compromised network in question and use that information to determine where any manipulation or vulnerabilities are present.

Digital Forensics

>>> 🛠 Tools

>> 🖧 Network Forensics

Network Forensics Tools

- **tcpdump**
- **Wireshark**
- Network Miner
- Splunk
- Snort
- Xplico
- PassiveDNS
- Dshell
- LogRhythm NDR
- STENOGRAPHER

Digital Forensics

>>> Branches

>> Wireless Forensics

Wireless Forensics’ main motive is to provide a methodology upon which computer forensic scientists can collect and analyze wireless communications that could potentially be used in a court of law as Digital Evidence.

Between Wi-Fi and mobile data or inter device connection with Bluetooth, wireless communications are more prevalent than ever. Some Digital forensics specialists focus on analyzing and investigating data in a wireless environment and then presenting that data to a court of law. This can be relevant for cyber security concerns as well as tracking communication related to other crimes. The types of wireless communications include WAP, SSID, Bluetooth, RFID, etc.

Digital Forensics

>>> 🛠 Tools

>> 📡 Wireless Forensics

Wireless Forensics Tools

- **Wireshark**
- Wi-Fi Pineapple
- Aircrack-ng
- KISMET
- fl0p

Digital Forensics

>>> Branches

>> Database Forensics

Database Forensics specialists work on digital databases. This may involve the data stored in databases like QuickBooks, Windows, Linux, credit card systems, healthcare systems, and more. However, these specialists focus on how and when databases have been accessed while recording changes that were made. Such metadata is often invaluable for investigating financial crimes, for example.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrongdoing, such as fraud.

Software tools can be used to manipulate and analyze data. These tools also provide audit logging capabilities which provide documented proof of what tasks or analysis a forensic examiner performed on the database.

Digital Forensics

>>> 🛠 Tools

>> 🗳 Database Forensics

Database Forensics Tools

- DF-Toolkit
- FTK-Toolkit
- Encase
- binwalk

Digital Forensics

>>> Branches

>> 🗁 Forensics Data Analysis

Forensic Data Analysis (FDA) is a branch of Digital Forensics. It examines structured data with regard to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities. Data from application systems or from their underlying databases is referred to as structured data.

Unstructured data in contrast is taken from communication and office applications or from mobile devices. This data has no overarching structure and analysis thereof means applying keywords or mapping communication patterns. Analysis of unstructured data is usually referred to as Computer forensics.

Due to the nature of the data, the analysis focuses more often on the content of data than on the file/system it is contained in.

Digital Forensics

>>> 🛠 Tools

>> 🗀 Forensics Data Analysis

Forensics Data Analysis Tools

- **Binwalk**
- **Oledump**
- Autopsy
- Digital Forensics Framework
- IsoBuster
- OSForensics

Digital Forensics

>>> Branches

>> Malware Forensics

Malware Forensics is a way of finding, analyzing & investigating various properties of malware to seek out the culprits and reason for the attack. the method also includes tasks like checking out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use etc. investigators conduct forensic investigation using different techniques and tools.

It does help to gather evidence from the infected Device that can be further analyzed and used as an evidence in court.

Digital Forensics

>>> 🛠 Tools

>> 🐞 Malware Forensics

Malware Forensics Tools

- PeStudio
- Process Hacker
- Process Monitor (ProcMon)
- ProcDot
- Autoruns
- Fiddler
- Wireshark
- gdb
- x64dbg
- Ghidra
- Radare2/Cutter
- Cuckoo Sandbox

Digital Forensics

>>> Branches

>> 📧 Email Forensics

Email Forensics is used to collect evidence from email and other email services to collect, analyze, structure and show them as an evidence in court.

This may include the message content, sender, recipient, timestamps, sources, and other metadata. Email forensics is frequently used when an organization is suspected of forging, modifying or deleting emails related to an investigation.

It comprises an in-depth forensic investigation of various email aspects such as Message-IDs, transmission routes, attached files and documents, IP addresses of servers and computers, etc.

Digital Forensics

>>> Tools

>> Email Forensics

Email Forensics Tools

- **eMailTrackerPro**
- EmailTracer
- Adcomplain
- AbusePipe
- AccessData’s FTK
- EnCase Forensic
- FINALeMAIL
- Paraben (Network) E-mail Examiner
- MailXaminer

Digital Forensics

>>> Branches

>> 🕸 IoT Forensics

IoT Forensics is a branch of Digital Forensics which deals with IoT-related cybercrimes and includes investigation of connected devices, sensors and the data stored on all possible platforms. IoT forensics is a lot more complex, multifaceted and multidisciplinary in approach than traditional forensics.

With versatile IoT devices, there is no specific method of IoT forensics that can be broadly used. So identifying valuable sources is a major challenge. The entire investigation will depend on the nature of the connected or smart device in place. For example, evidence could be collected from fixed home automation sensors, or moving automobile sensors, wearable devices or data store on Cloud.

When compared to the standard digital forensic techniques, IoT forensics portrays multiple challenges depending on the versatility and complexity of the IoT devices. Following are some challenges that one may face in an investigation:

- Variance of the IoT devices
- Proprietary Hardware and Software
- Data present across multiple devices and platforms
- Data can be updated, modified, or lost
- Proprietary jurisdictions for data is stored on cloud or a different geography

Digital Forensics

>>> 🛠 Tools

>> 🕸 IoT Forensics

IoT Forensics Tools

- **Oxygen Forensic Detective**
- E3: Universal Software
- Foremost
- Volatility
- Binwalk
- FTK

Digital Forensics

>>> Branches

>> Mobile Forensics

Mobile Forensics is used to retrieve data and other useful information from Android, iOS and other mobile devices. In the smartphone era, this is especially important since mobile devices gather an insurmountable amount of data on a regular basis, not only including texts or call logs. Because of mobile device forensics, crimes such as bomb threats, internal company threats, and more have been resolved by law enforcement agencies. Data on mobile devices include everything from contacts and texts to pictures and browsing history with everything in between.

The mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition. To achieve that, the mobile forensic process needs to set out precise rules that will seize, isolate, transport, store for analysis and proof digital evidence safely originating from mobile devices.

Digital Forensics

>>> 🛠 Tools

>> 📱 Mobile Forensics

Mobile Forensics Tools

- **Oxygen Forensic Detective**
- E3: Universal Software
- Cellebrite UFED
- Volatility
- Magnet AXIOM
- MicroSystemation XRY/XACT

Digital Forensics

>>> Branches

>> 💾 Disk Forensics

Disk Forensics is the investigation and analysis of physical storage devices such as hard drives, solid-state drives, external USB drives, and memory cards.

Forensics Analyst does recover, analyze, and present data from a physical storage medium for an investigation. Data includes everything from metadata to deleted or hidden files to tampered folders and is copied over from the original storage device into a disc image for further investigation. This type of work is often frequently used for data recovery, even if the data was accidentally lost.

Analysts carry out disk forensics across operating systems, hardware and storage devices including recovery of the data from physically or logically damaged devices.

Electronic evidences are treated as an ‘asset’ containing valuable and quantity information within them. In the examination of disk forensics it is capable of collecting forensic artifacts in the form of:

- Disk imaging,
- Metadata
- Data files and folders
- Deleted files and folders
- Hidden files and folders,
- Registry logs, etc.

Digital Forensics

>>> 🛠 Tools

>> 💾 Disk Forensics

Disk Forensics Tools

- **Sleuth Kit (+Autopsy)**
- Cellebrite Inspector
- IsoBuster
- Magnet AXIOM
- HashKeeper

Digital Forensics

>>> Branches

>> Memory Forensics

Memory Forensics is a branch of digital forensics that is focused on recovering data from a device’s digital memory, specifically random-access memory. Some techniques used by hackers and other digital criminals allow them to avoid leaving any traces of their work in permanent digital storage. However, memory forensics can often find useful information captured in temporary memory. This method only isolates the memory of specific programs running during the time of a RAM dump.

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which is non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

Digital Forensics

>>> 🛠 Tools

>> ⌨ Memory Forensics

Memory Forensics Tools

- Magnet AXIOM
- Volatility
- Windows Scope
- HashKeeper
- Rekall

Digital Forensics

>> 🙏 Thank You

# THANK YOU