

# **Digital Forensics:**

## How to Approach Digital Forensics and its Branches.

Davindernain Singh Sehgal  
*Northeastern University, Khoury College Of Computer Science,  
Boston*  
[sehgal.da@northeastern.edu](mailto:sehgal.da@northeastern.edu)

## **Abstract**

*This paper provides a brief explanation of a few types of digital Forensics as well as their uses to suit the current cybercrime curve. This paper briefly goes over what those branches are, how to approach them, and what information should new investigators should keep in mind when dealing with that branch of forensics.*

## **Introduction**

In the past couple of years, the technology industry has grown beyond any other industry and has also become an integral part of other rising industries as well. The use of these devices ranges widely from someone's personal use, or to the use of an entire given organization. These devices, be it a new generation of laptops, tablets, mobile phones, printers, or other devices, make lives easier for everyone. The use of such devices can be seen in almost every company around the globe, almost 78% of the entire world's population had a mobile device in the year 2020 and the charts only go higher. Even if big organizations aren't considered, most individuals nowadays have a smartphone that is used to browse the internet and communicate with others.

This technological growth around the world sure has its pros but it also has a dark side. It is only fair to assume that something that has so many good uses in every industry, is bound to have a few uses that could be intended for malicious motives. Computer Forensics is the study of how computers and other devices are involved in the Commission of crimes [1]. These criminal cases can range from blackmail to identity theft, to accounting fraud, to child pornography, or a case where the information available on the hard drive or another storage media can have crucial evidence of a crime. Only knowing the fact that there is a possibility of finding evidence in a given system, makes the system crucial for investigations because of the possibility of finding evidence that can prove someone guilty or innocent.

According to a survey in 2021, various different attacks have surfaced online where people have had to face several consequences. These attacks include already popular attacks like phishing, ransomware, crypto-jacking, Data breaches, and identity theft cases [2]. It is because of these incidents that cyber forensics has become of utmost importance in companies. It is needed for the investigation of crime and law enforcement where technology is involved [3]. The proof of the crime will be present in a computer system and the proofs can range from browsing history, emails, documents, etc. This information is stored in the form of data artifacts that can be analyzed by an expert in cyber forensics to avoid the loss of data during an active investigation.

The term "Digital Forensics Investigators/Expert/Analyst" is given to the individuals who have expertise in extracting valuable evidence from the forensic artifacts present in the system with the most amount of precision. These experts are responsible for not only searching, analyzing, and reporting the information extracted by the artifacts, but also have an important role in securing the same system or wiping it off to avoid the spread of the viruses and trojans. They apply advanced data retrieval and incident analysis skills to cases of organized cybercrime, hacking, fraud, terrorism, and the storage and distribution of illegal content. The Reports made by a cyber forensics investigator are not only valid in courts but also private organizations tend to hire such experts to work for their company in case they are ever needed [4].

This paper briefly goes over Digital forensics and a few of its branches and identifies the use of the types determined. This paper will go over the importance of these different types of cyber forensics and how these forensic branches are different from each other. A brief explanation of these branches would be followed by forensics criteria that make this branch different than others.

### **Digital Forensics and its Branches**

Digital forensics is the forensics science branch with deals with the recovery and analysis of any information found on digital devices. Originally, “Digital Forensics” was used as a synonym for computer forensics, but with time, it has now expanded to cover the analysis of all information found on all devices that can be stored digitally. Digital Forensics experts use their specialized forensics toolkits to help them investigate incidents and look for deep hidden data that a normal observer might miss in plain sight. Depending on the type of information and its sources, the field of digital forensics has been broken down into branches and requires specialized knowledge to perform forensic analysis on them. A few of these branches are discussed ahead in the paper [5].

### **Mobile Device Forensics**

This branch of forensics is the science of recovering digital evidence from a mobile phone device under forensics conditions using appropriate tools and methods. As the number of smartphones is rapidly increasing in this world, a large number of hackers, scammers, and other potential criminals find themselves using a mobile device to go ahead with their plans. These little devices store huge quantities of data on a daily basis as they sit in the middle of 3 incredibly popular technological trends “Big Data, Cloud Computing, and Internet of Things”, which can be extracted to facilitate an ongoing investigation. In today’s world, these mobile devices act as an extension of ourselves, using them, forensics investigators can acquire a lot of intelligence [6].

A mobile phone device contains a lot of different information inside it, including incoming, outgoing, missed call history; Internet browsing history, content, cookies; Phonebook; Media items like images, videos, audio files; notes, to-do list; passwords, account credentials; data from various different installed applications; deleted data from all the previously listed information bits. Although the forensics process with mobile devices is usually similar to that of other branches of digital forensics, It is very important to know that mobile forensics has its own particularities that need to be kept in mind during an investigation. Following the correct methodology and guidelines while dealing with a mobile forensics case, can help an investigator organize his work and get better results.

A big difference between a normal system which is in for digital forensics and mobile forensics is the fact that a mobile device can easily be remotely erased if the owner of the mobile device has set some security application on their phone. To avoid such scenarios and losing important evidence that could be found on a mobile device, isolating your device by the means of putting it on airplane mode and restricting all connectivity out of your environment is very important. A few very important points to keep in mind while examining mobile devices are that the type of a smartphone may not sound like a big chunk of useful information, but knowing about it will give

you more idea about what you must look for, like GPS data and other special features specific to the type of mobile device.

In conclusion, Mobile Device forensics is a branch of digital forensics, which should be approached delicately as it is used by users on a daily basis and has the potential to have a lot of valuable evidence. As the importance of data contained on the device increases, it is also important that these devices are put under forensics tests the right way to get the best results possible.

### **Network Forensics**

Network forensics is one of the sub-branches of digital forensics where the data being analyzed is the network traffic going to and from the system under observation. The purposes of this type of observation are collecting information, obtaining legal evidence, establishing a root-cause analysis of an event, analyzing malware behavior, and so on [8]. As part of digital forensics, network traffic to and from the system under investigation is analyzed. For example, collecting data, obtaining legal proof, evaluating virus behavior, etc.

Most attacks leave traces as they pass over the network. "Every contact leaves a trace," says Lockard's exchange principle. Network forensics is the study of finding and retrieving data related to cybercrime in a networked setting. Common forensic operations include capturing, recording, and analyzing network events to determine the source of cyberattacks. Network forensics can help identify network leaks, data theft, and abnormal network traffic. It focuses on investigating and analyzing traffic in a network suspected of being hacked. Before entering the network, data is divided into smaller units called packets [9].

To understand network forensics, one must first understand internet principles such as email, VOIP, and browsers. One must also understand ISP, IP, and MAC addresses. Investigators must understand the application and network protocols to identify attack patterns. File transfer protocols (e.g., Server Message Block/SMB and Network File System/NFS), Email protocols (e.g., SMTP) • Ethernet, Wi-Fi, and TCP/IP Because a cyberattack deviates from the ordinary, investigators can easily discover traffic anomalies.

There are two types of NFATs: "catch-it-as-you-can" systems that capture network traffic, store large volumes of data, and analyze that data in batch mode; and "stop, look, and listen" systems that analyze each packet but lack the storage capacity of the former [10]. An NFAT saves network traffic, analyzes it, and alerts security administrators to unusual activities. This is a modern tech. Like any new security tool or technology, firms must consider the benefits and drawbacks. For most businesses, this technology's limitations limit its use. NFATs may become more commonly adopted as tools like SilentRunner and NetIntercept could monitor encrypted data. If not, they at least help security administrators monitor and secure their networks with confidence.

Network forensics software is freely available. Some have a graphical user interface (GUI). Most feature a command-line interface and only work on Linux. "EMailTrackerPro" displays the location of the device from which the email is sent; Web Historian displays information about file uploads and downloads on visited websites; Wireshark can record and analyze network traffic between devices. Network forensics aids in the reconstruction of missing parts in a digital forensic examination. It can help with root-cause analysis by showing the first compromise method. As almost all nonlocal attacks happen over a network, keeping these things in mind while performing analysis on a network, will give efficient results to a forensics investigator.

### **Database Forensics**

Database forensics is a branch of digital forensic science that focuses on databases and their data. Database forensics examines who accesses the database and what they do. The issue of large data security breaches is a concern for criminal investigators. Database forensics is frequently used in modern criminal investigations to find motives, techniques, and suspects. As in a recent court disagreement between two large companies over whether database software correctly estimated the residual value of a fleet of 45,000 leased cars[11].

A database forensic analysis may investigate into the timestamps of rows in a relational table to validate a database user's activity. Another database forensics example might evaluate all transactions within a database system or application over time to detect fraud. Database forensics experts must know practically every aspect of database design and use it to preserve, authenticate, analyze, and output data from big, custom-built databases that cannot be copied and carried back to the office for further examination. Stroz Friedberg points out, "leveraging the database's infrastructure includes disabling archive and deletion functions, preserving backup tapes, or keeping existing reports" [12].

Sources of immensely valuable data are frequently neglected. While financial databases are essential in intellectual property proceedings, knowledge management systems, source code repositories, and document management systems can help defendants avoid problematic fishing expeditions and/or invalidate claims against them. These databases can examine document lifecycle and version control. Keywords, descriptions, annotations, and comments can identify a document's purpose, who produced or accessed it, and where it was routed. A qualified and perceptive specialist can also gain a new perspective on the known data. Database forensics is used in cases of IP or patent infringement, business espionage, and even intrusions like data breaches or virus infections. A database forensics expert can often locate crucial evidence in the structured ESI of a database.

In conclusion in Database forensics, it is important to note that databases can range from carrying data of a single person to a big organization. Regardless of the size of the database, new forensics investigators should keep in mind the above-stated points to not only get efficient results for their forensics analysis but also to not leave out crucial evidence.

## Conclusions

In this paper, we have provided a brief overview of digital forensics and focused on discussing three of its rapidly growing branches: network forensics, database forensics, and mobile device forensics. While these branches hold significant importance in modern investigative practices, it is crucial to recognize that the field of digital forensics encompasses even more diverse and compelling branches that are equally valuable.

Beyond the branches mentioned, there are other fascinating areas of digital forensics that play a critical role in solving cybercrimes and ensuring the integrity of digital evidence. Some examples include memory forensics, malware forensics, cloud forensics, and social media forensics, among others. Each of these areas addresses unique challenges and presents valuable opportunities for investigation.

It is essential to acknowledge that the task of handling digital data in forensic investigations is not to be taken lightly. The data collected during investigations can be of utmost importance in legal proceedings, and any mishandling or oversight can compromise the integrity and admissibility of evidence in court hearings.

To ensure the effectiveness and reliability of digital forensics results, investigators must prioritize the careful handling of all digital evidence. Adhering to established guidelines, best practices, and standard operating procedures is paramount. Following these protocols helps maintain the chain of custody and preserves the evidentiary value of digital data.

In conclusion, digital forensics is a multifaceted and ever-evolving field, encompassing various branches that are continuously evolving to meet the challenges of modern cyber threats. While we have explored network forensics, database forensics, and mobile device forensics in this paper, it is essential to keep in mind that other branches are equally valuable and worthy of exploration. By diligently following guidelines and procedures and staying abreast of advancements in digital forensics, investigators can produce efficient and reliable results in their forensic tests, ultimately contributing to a more secure digital environment and upholding the integrity of digital evidence in legal proceedings.

## 7. References

- [1] Robert Jones, "Internet Forensics", available at: <https://www.oreilly.com/library/view/internet-forensics/059610006X/ch01.html>
- [2] PurpleSec, "2021 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends", available at: <https://purplesec.us/resources/cyber-security-statistics/>
- [3] Educba, "Introduction to Cyber Forensics", available at: <https://www.educba.com/cyber-forensics/>
- [4] Cyberdegrees.org, "What is a Computer Forensics Analyst? available at: <https://www.cyberdegrees.org/jobs/computer-forensics/>
- [5] Recfaces, "Digital Forensics, what is it in 2021-22", available at: <https://recfaces.com/articles/digital-forensics#1>
- [6] InfosecInstitute, "Mobile Forensics", available at: <https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/>
- [7] Jaiswal Nipun, "Hands on Network Forensics, investigate network attacks and find evidence using common network forensics tools", 2019
- [8] Infosec, "Network forensics", available on: <https://resources.infosecinstitute.com/topic/network-forensics-overview/>
- [9] TechTarget, "Computer forensics", available on: <https://www.techtarget.com/searchsecurity/definition/computer-forensics>
- [10] Information Security magazine article from February 2002, "NFAT solutions record and store all network traffic and give tools for forensics analysis.." (King & Weiss, February 2002)
- [11] Idera, "Database Forensics", available on: <https://www.idera.com/glossary/database-forensics>
- [12] Stroz Friedberg, "Database Forensics: Incident response", available on: <https://www.aon.com/cyber-solutions/solutions/digital-forensics/>