IRJTAE

Ingenious Research Journal for Technological Advancements in Engineering
(Open Access, Peer-Reviewed, Technological Journal)
Volume:01/Issue:01/NOV-2024 www.irjtae.com

# The Role of Forensic Data in Cyber Security

1st Ayush D. Ther
*Computer Engineering*
*Government College of Engineering*
Yavatmal, India
ayushthercse@gmail.com

2nd Soham M. Sawalakhe
*Computer Engineering*
*Government College of Engineering*
Yavatmal, India
sohamsawalakhecse@gmail.com

3rd Ayush S. Shirbhate
*Computer Engineering*
*Government College of Engineering*
Yavatmal, India
ayushshirbhatecse@gmail.com

4th Bhushan S. Onkar
*Computer Engineering*
*Government College of Engineering*
Yavatmal, India
bhushanonkarcse@gmail.com

Prof. Dhiraj D. Shirbhate
*Assistant Professor*
*Computer Engineering*
*Government College of Engineering*
Yavatmal, India
dhirajshirbhatecse@gmail.com

***Abstract*- Forensic data holds a key significance in the current era of digital generation through providing evidence that is necessary for tacking each aspect involving detection, analysis and judicial course related to cybercrimes. In this paper we research further to get an understanding of the collection, preservation and analysis processes made forensic data (digital evidence) interestingly with legal and ethical point-of-view. It also discusses the constraints of forensic experts and possible future directions to improve forensics solutions.**

***Keywords- Data Hiding, Steganography, Pixel-Value Differencing (PVD), Document Security, Malware, etc.***

## I. INTRODUCTION

In the digital world, where data breaches tend to have an upward trajectory and hold a significant presence in businesses of all shapes and sizes, forensic Data analytics is more critical than ever. Forensic data, either compiled from computer systems, networks or other forms of digital device which is used to investigate crime and as evidence includes. Today, digital forensics has become a sub-discipline of cyber security and law enforcement that track down on the use of computer crimes. The paper aims to provide a thorough exploration of forensic data by explaining how it is collected, preserved, and analysed, as well as the legal and ethical considerations that relate to it.

### A. Overview

Forensic data is any kind of digital data that may be employed in a legal context for an investigation. Such data can be obtained from computers, personal and portable devices, network traffic, databases, and cloud storage. An aim of forensic data is to help ascertain the sequence of events, the offenders involved and the magnitude of the violation or breakout. Handling of the data should be done carefully since small changes can lead to the data not being allowed as evidence in a court of law.

Key types of forensic data include:

- File System Data :- Records data including time of file creation and last modification, permissions read and write on such devices or metadata regarding the file.
- Network Data :- Comprises of logs and packet that track communication within networks which is very crucial in detecting intruders or illicit transfer of data.
- Memory Data :-Taken from the volatile memory to point out the current running processes, connections as well as active sessions during capture time.
- Mobile Device Data :- It also covers telephones call logs details, SMS Data, GPS Data and the application log details in Smartphone s and tablets.

An element, Forensic Data Collection and Preservation Digital investigation starts with the collection and preservation of the forensic data. The first stage involves determination of the data to be collected and it is obtained without changing of biasing the results. This is academically referred to as making forensic images of the digital storage media, which are duplicate copies of the original media that are usable but cannot be modified by the investigators as they work on the images.

## II. LITERATURE REVIEW

Digital forensics has its advancement with the advancement seen in the case of cybercrime. Forensic practices this same time actually used to align with traditional criminal investigations that took force under physical evidence. It is the advancement in digital technology and subsequently something like the internet that called for digital forensic services. Although in its first years the interest of digital forensics was given for scrutiny over basic computer systems, with time and due to the increased sophistication of cybercriminals, it has expanded into investigating a great variety of other digital devices and data types. In today's cybersecurity, digital forensics is already considered an important field of operation which furnishes tools and techniques around which to build lawful investigations and ultimately resolve cyber incidents. It responds in a dual manner to cybersecurity; that is it is reactive when used in the post-incident analysis and proactive when used in preventing cyber threats.

In the incident response, forensic data is useful in locating the point of origin, methods, and damages caused. Threat hunting makes use of forensic data to detect patterns and anomalies that may reflect the existence of malicious activity before it matures. While the importance of forensic data in cybersecurity is pretty well-acknowledged, there are marked differences amongst digital forensics both in law enforcement and application in cybersecurity. Here it has been illustrated that while law enforcement essentially collects evidence to prosecute, cybersecurity forensics primarily ensures fast containment and mitigation of the threats. Many researchers are found to have contributed their understanding as well as excellence for forensic data in the field of cybersecurity.

Initially it was mainly associated with the traditional criminal investigations based on the physical evidence, but coming with the digital technology and the internet, digital forensics also came into need. As soon as the technology to investigate rudimentary computer systems became possible, so did all the technologies for the investigation of criminal activities. The initial digital forensics involved the investigation of rudimentary computer systems, but with the advancement and sophistication of cybercriminals, it also expanded into diversified range of digital devices and data types. Digital forensics is an area that is very critical to cybersecurity today, as it provides the tools and techniques for investigating and resolving cyber incidents. Forensic data in cybersecurity plays a two-front role; it is useful reactively during post-incident analyses yet also useful in the prevention of cyber threats.

Data forensics plays an important role in incident response because it helps in determining the source of the attack, providing understanding regarding the methods used, and resultant damage. The data can be used for hunting threats: looking for patterns and anomalies that may indict the potential for malicious activity long before the resulting breach occurs. Important as forensic data evidently would be to cybersecurity, there are significant differences between digital -forensics in law enforcement and applying this -forensics in cybersecurity. Law enforcement is more concerned with the collection of evidence for its conviction, while cybersecurity forensics puts more emphasis on the immediate control action and mitigation. Several scholars have contributed to the knowledge and development of cryptographic forensic data in cybersecurity.

There are several methodologies and tools designed within the literature to address the complexities posed by current cyber threats, though there is still a gap in research on the full integration of forensic data into comprehensive cybersecurity frameworks. This paper aims to bridge that gap by examining the theoretical as well as practical aspects of incorporating forensic data into modern cybersecurity practices. It discusses how forensic data may be used to improve the efficiency and efficacy of threat detection, response, and prevention, thereby building a stronger security infrastructure.

IRJTAE

Ingenious Research Journal for Technological Advancements in Engineering
(Open Access, Peer-Reviewed, Technological Journal)
Volume:01/Issue:01/NOV-2024 www.irjtae.com

## III. PRINCIPAL SCENARIO OF DIGITAL FORENSIC

Digital forensics is essentially a scientific process, although it is also rather new; nonetheless, changes in software and hardware repeatedly oblige the study, description, and investigation of phenomena.

A flowchart that represents the process is as shown in fig.1 (Greg Gogolin, 2013).

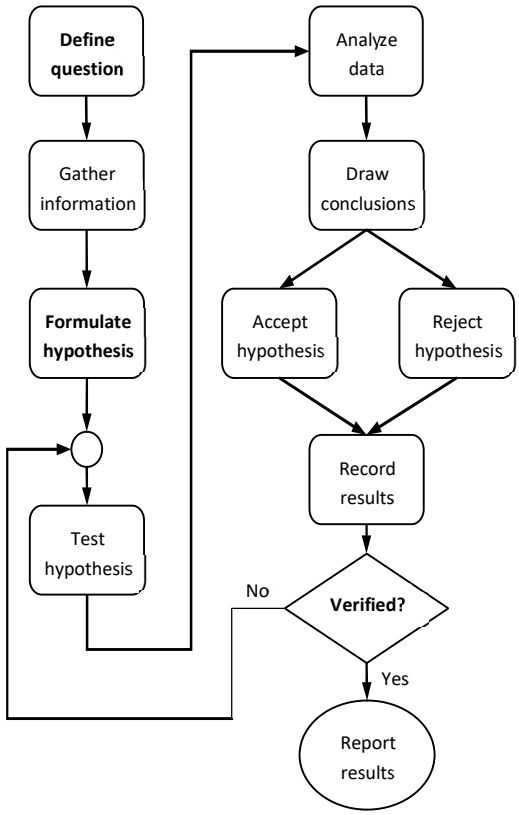


Fig. 1. The scientific process of digital forensics

The digital forensic process typically has three distinct phases: defining the question, formulating a hypothesis, and verification of the results. More emphasis is, therefore, put on defining the actual question or objective of the investigation during the very first phase, meaning identifying what one should actually look for on the device. The second step is the development of a hypothesis, basically an intelligent guess about the purpose or activity associated with the artifact, like what it could have been utilized for or who could have used it. The third is verification, in which one proves the validity and reliability of the findings by testing them in some kind of controlled environment (Greg Gogolin, 2013).

**Key principles of forensic data collection include:**

- Chain of Custody: Maintaining records of all the officers who had directly dealt with the evidence and in what capacity, how frequently and under what pretext the data was being accessed so as to ensure its originality during trial.
- Write-Blockers: Devices that would exclude any alteration on the storage devices from occurring in the process of data collection.
- Data Integrity: Through hashing algorithms such as the MD5, SHA-256, among others; special digital fingerprints of such evidence is produced then compared with existing ones to ensure that there has been no change.

However, preservation goes beyond the accumulation practice to mean the storage of data for as long as possible without deterioration or difficulty in accessing it. Normally, the forensic data is required to be kept for several years, most preferably until the legal procedures are completed as is the case with most complicated cases that are litigated in the courts.

## IV. ANALYSIS OF FORENSIC DATA

Digital forensics is the evaluation of the results of data investigation including the collected forensic data to come up with meaningful information. It is in this phase that event reconstruction and pattern recognition is done together with linking of digital activities to person or institutions.

**Key techniques used in forensic data analysis include:** Timeline Analysis: Making a timeline of events that were described using timestamps and logs, which allows to define the stages of an incident.

- File Carving: File recovery from storage media in cases where file system metadata cannot be accessed, for example, when files were removed, or file was fragmented.

- Memory Forensics: Inspecting RAM dump of the system to find the top processes, network connections and encrypted data which can be in RAM and not stored on disk.

Forensic analysis can be very time-consuming and complex, and may thus call for applications such as Encase, FTK, or Autopsy or other comparable free software and tools. Moreover, analysts need to be able to explain the analysis and its results and provide a clear idea about it to members who may no technically background like lawyers and the like.

## V. LEGAL AND ETHICALCONSIDERATIONS

The legal and ethical issues in regard to the data management are of significant importance because they determine the recognition of the evidence in court besides availing a fair chance on the investigations' results. Something that one must bear in mind is that forensic investigators are always under a legal minefield as laws across different jurisdictions differ.

Key legal considerations include:

- Admissibility of Evidence: To make sure that the forensic process complies with the law of evidence most especially the Federal Rules of Evidence in the United States, in order to meet the legal standards of admissibility.
- Privacy Rights: The dilemma of obtaining evidence while respecting the people's right to privacy including email and health information.
- Data Protection Laws: Paying heed with rules on data guarding like General Data Protection Regulation (GDPR) in European countries that have policies on how personal data can be collected, processed, and stored.

Ethical issues are also very pertinent when working on forensic investigations; the forensic investigators must make sure that they do not have any related business with the sides involved in the investigation; they also have to be impartial in their work and keep the information they gather and work on secure. Mistakes in these areas could mean being on the wrong side of the law, massive damages to the image of the company, or even loss of vital proof.

## VI. CHARACTERISTICS OF DIGITAL FORENSIC

Digital forensics generally follows a standard five-stage process: policy and procedure, evidence evaluation, evidence collection, evidence analysis, and evidence documentation and reporting (U.S. Department of Justice, https://www.ncjrs.gov). Further explanation of each stage is provided below:

### A. Policy and Procedure

The digital forensic investigation must be described in such a manner that is reliable and valid, as well as following a set of policies and procedures strictly. Policies should indicate the proper steps taken within an investigation, so these procedures are formulated by identifying the problem, evaluating solutions, testing those solutions, assessing the outcome, and validating the procedures.

### B. Evidence Assessment

In evaluating digital evidence, it is essential that the investigator evaluate the evidence in the case so he can determine how he should treat it. This encompasses a number of essential activities including prioritizing evidence, documenting evidence properly and ensuring it is both stored and transported safely so that contamination or loss does not take place.

### C. Evidence Acquisition

Digital evidence is always sensitive to alteration, corruption, or destruction unless taken care of. The collecting procedure must, therefore, be done with utmost care not to compromise the integrity of the evidence. This includes the following steps: Ensuring that the evidence is collected in accordance with the policies of the forensic unit. Ensuring disassembly of a computer to reach the storage devices. Identify and document all storage devices.

- Record the configuration of the hardware on system.

- Remove the storage device in a safe manner so that no modification and damage is made.

- Allow the data collection in a controlled boot sequence so that the data is not tampered with.

- Probe the geometry of storage devices for accessing all available space, whether it is hidden or protected.

- Use the right tools and techniques to extract data.

- Verification of acquisition by comparing the original and copied data at the sector level to check for any loss of data.

D. Evidence Analysis

Digital evidence should not be analysed at the scene of origin. The data must, therefore, first be extracted and then analysed with caution. Extraction means recovering data from a medium of storage while analysis focuses on the interpretation of the recovered data. There are two major methods of extraction:

- Literal extraction: extracts all the data available in the entire drive.

- Logical extraction: collects information from the OS, file system, and installed applications installed on the computer.

The extracted data is then placed in a working directory located on isolated media. Analysis of the log is performed through active files, deleted files, file slack, and unallocated space on the drive. The results of both extractions and analyses are then reviewed to find any relevant information.

E. Documentation and Reporting of the Evidence

Once all the evidence has been evaluated, collected, and analysed, it is then summed up and reported clearly, accurately, and in as much detail as possible to prevent any evidence from being missed or not accounted for. This ensures that every step taken to investigate a crime is documented and possibly used in court if proceedings are deemed necessary.

In short, these five steps- policy and procedure, evidence assessment, acquisition, examination, and reporting-are the key steps for carrying out a comprehensive, reliable, and legally tenable digital forensic examination.

## VII. CHALLENGES AND FUTURE DIRECTIONS

Forensic data is a very young and developing discipline due to the growing complexity of the digital world and, correspondingly, the level of the crime lords' intelligence. That apart, this evolution brings major challenges, including:However, this evolution brings major challenges, including:

- Data Volume and Complexity: The problem of the saturation of the modern digital systems implies that it is nearly impossible to collect, sort through, and analyze all the evidence pieces which could be useful for a case being examined within reasonable time.
- Encryption and Anonymity: The use of encryption and anonymity that is evident in the application of programs like Tor and VPN makes it almost impossible to captureand associate forensic data to specific users.
- Cloud Computing: The cloud service providers are geographically distributed hence seizure of evidence may involve data in different regions which may be controlled by third partyFig. 2 Multiple domains of digital forensics (M. Lasavio et al., 2016)

The future shall see the use of technological tools in performing forensic data analysis with the involvement of automation, machine learning, and Artificial intelligence in those areas where large datasets play a role and can help identify patterns much more quickly. In addition to these requirements, the methodologies also need to be developed because the digital environment today is very volatile too.

## IV CONCLUSION

The critical component of any digital investigation is forensic data, offering the crucial information that is necessary for the resolution of criminal and legal matters. It still develops despite several problems in the very same field, more related to the data itself and the legal aspects. Just as technology continues to evolve, so do the techniques utilized applied in forensic data analysis in order to enable the investigators have an upper hand against the hackers. By applying the tenets and practices of legal, a means of acquiring accessible, objective data acquisition, and adherence to the law, forensic experts contribute to making the cyberspace safer.

REFERENCES

[1] R. Kumar, S. Chand, "A Reversible High Capacity Data Hiding Scheme Using Pixel Value Adjusting Feature", Multimedia Tools and Applications, Springer, pp. 241-259,2016.

[2] A.M. Alattar, "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform", IEEE Transactions on Image Processing, IEEE, pp. 1147- 1156, 2004.

[3] N. F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, Computer Practices (1998) 26-34.

[4] W.L. Tai, C.M. Yeh, and C.C. Chang, "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE Transactions on Circuits and Systems for Video Technology, IEEE, pp. 906-910, 2009.

[5] D.M. Thodi, J.J. Rodriguez, "Expansion EmbeddingTechniques for Reversible Watermarking", IEEE Transaction on Image Processing, IEEE, pp. 721-730, 2007.

[6] X. Li, J. Li, B. Li, and B. Yang, "High-Fidelity Reversible Data Hiding Scheme Based on Pixel-Value-Ordering and Prediction-Error Expansion", Signal Process, Elsevier, pp. 198-205, 2013.

[7] F. Di, M. Zhang, X. Liao, and J. Liu, "High-Fidelity Reversible Data Hiding by Quadtree-based Pixel Value Ordering", Multimedia Tools and Applications, Springer, pp. 1–17, 2018.

[8] F. Peng, X. Li, and B. Yang. "Improved PVO-based Reversible Data Hiding", Digital Signal Process, Springer, pp. 255–265, 2014.

[9] X. Qu, H.J. Kim, "Pixel-based Pixel Value Ordering Predictor for High-fidelity Reversible Data Hiding, Signal Process, Elsevier, pp. 249–260, 2015.

[10] B. Ou, X. Li, Y. Zhao, and R. Ni, "Reversible Data Hiding Using Invariant Pixel-Value Ordering and Prediction-Error Expansion", Signal Process: Image Communication, Elsevier, pp. 760–772, 2014.

[11] H.J. Prajapati, Z. Noorani, "A Study on ARP Poisoning and Technique for Detection and Prevention", International Journal of Advance Research and Innovative Ideas in Education, IJARIIE, pp. 594-601, 2017.

[12] W.W. Choi, J.W. Chung, and S.J. Ahn, "A Study on Network Security Problem Analysis of ARP Mechanism", Journal of Korean Society for Industrial and Applied Mathematics Education, pp. 1-11, 2004.