International Journal of Innovative Research in Technology and Science

ISSN: 2321-1156 www.ijirts.org Volume 12 Issue 2, March 2024

A Study To Examine Forensic Cybercrime and the Role of Computer Forensics

Sarafatma, Rohan Singrore
sarafatma7676@gmail.com, rohankumarsinghrore12@gmail.com
Department of forensic science, School of Science, SAM Global University, Bhopal, India.

Selection and peer review of this article are under the responsibility of the scientific committee of the International Conference on Current Trends in Engineering, Science, and Management (ICCSTEM-2024) at SAM Global University, Bhopal.

Abstract:- This study delves into the intricate realm of Forensic Cybercrime and Computer Forensics, focusing on the methodologies, challenges, and advancements that encapsulate the investigation of digital crimes. As the digital landscape expands, so does the complexity and volume of cybercrimes, necessitating sophisticated forensic approaches to detect, analyse, and mitigate these offences. This research aims to dissect the procedural framework and technological tools employed in cyber forensic investigations, emphasising digital evidence extraction, preservation, and analysis. Technological advancements have both facilitated the perpetration of cybercrimes and bolstered forensic capabilities. This dual-edged nature necessitates a continuous evolution of forensic methodologies to stay ahead of cybercriminals. The research identifies emerging trends and future directions in cyber forensics, including adopting artificial intelligence and machine learning for enhanced data analysis and anomaly detection. By providing a comprehensive overview of Forensic Cybercrime and Computer Forensics, this study aims to contribute to the field's body of knowledge, offering insights for practitioners, scholars, and policymakers engaged in the ongoing battle against cybercrime. The findings underscore the importance of interdisciplinary collaboration, continuous learning, and innovation in developing effective cyber forensic strategies and tools.

Keywords:- Forensic Cybercrime, Computer Forensics, Cybercrime Investigation, Digital Evidence, Cyber Forensic Tools

1. Introduction

The study examines the importance of the Digital Forensics & Role of Computers in Digital Forensics. As the internet grows, social media cybercrime also grows explosively. So, In response to those cybercrimes, the digital forensics field has emerged. Digital forensics is the branch of forensics science which mainly focuses on carefully investigating and recovering the evidence or material found in devices related to cybercrime. Digital forensics not only includes data on your desktop or laptop mobile but also includes data that is transmitted in private networks. The term digital forensics was first used as computer forensics. Digital forensics is used to solve crimes, whether they be physical crimes or digital crimes. Cyber forensics, also known as computer forensics, is a meticulous process to extract electronic data as evidence in criminal investigations, adhering to established investigation protocols to apprehend perpetrators and present compelling evidence in court. The primary objective of cyber forensics is to preserve a coherent thread of evidence and documentation, facilitating the identification of digital criminals. Within the realm of cyber forensics, various tasks can be performed. The process can involve recovering deleted files, chat logs, emails, and other digital artefacts crucial to the investigation.

Furthermore, it possesses the capability to retrieve deleted SMS messages and phone call records, providing additional insights into suspect activities. Cyber forensics can also access recorded audio from phone conversations, potentially uncovering valuable information pertinent to the case. Moreover, cyber forensics enables investigators to ascertain user activities on computer systems, determining which user accessed specific systems and for how long, thus aiding in establishing timelines and patterns of behaviour. Additionally, it can identify the users responsible for running particular programs, offering valuable insights into the actions taken by individuals on digital platforms. Through these capabilities, cyber forensics plays a pivotal role in unravelling digital crimes and holding perpetrators accountable for their actions. Cybercrime encompasses any criminal activity involving a computer, network, or networked device. While many cybercriminals engage in such activities to generate profit, others conduct cybercrimes to damage or disable computers or devices directly.

Additionally, some individuals utilise computers or networks to disseminate malware, illegal information, images, or other materials. In certain cases, cybercriminals may employ a combination of tactics, targeting computers to infect them with viruses, which are then spread to other machines and potentially entire networks. Thus, cybercrime manifests in various forms, as shown in Figure 1, posing significant challenges to cybersecurity and law enforcement efforts.

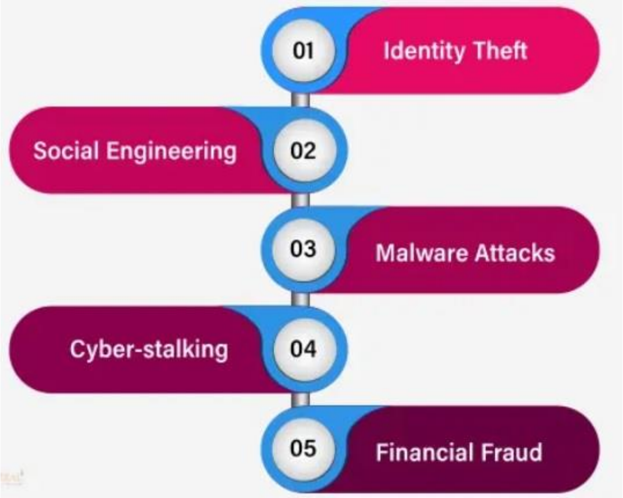

Figure 1 Type of Cybercrimes

Until the 1990s, digital forensics was known as computer forensics, with law enforcement officers being the first computer forensic technicians. As digital documentation became prevalent, data storage became a significant concern for law enforcement. Analysing such documentation proved daunting for officers, prompting the FBI to launch the first magnet media program in 1984, marking the inception of digital forensics. In 1985, under the guidance of John Austen, the Metropolitan Police established the first computer crime unit in the UK. The early 1990s witnessed a pivotal change as investigators recognised the need for standard digital forensics techniques, protocols, and procedures. This led to the establishment of modern British digital methodology through conferences organised by the Serious Fraud Office and Inland Revenue in

1994 and 1995 at the Police Staff College Bramshill. The conflicts in Iraq and Afghanistan further underscored the importance of digital forensics, with computerised crime scene investigation playing a vital role in extracting evidential data from digital devices collected by US troops during these conflicts. Cybercrime encompasses a broad spectrum of illicit activities involving computers, networks, or networked devices. While financial gain often motivates cybercriminals, some engage in activities aimed at directly damaging or disrupting computers or devices. This includes disseminating malware, illegal information, images, or other materials and infecting computers with viruses to perpetuate digital malfeasance. As digital threats continue to evolve, the study aims to shed light on the evolving landscape of cybercrime and the indispensable role of digital forensics in combating such threats.

2. Literature Review

This research paper focuses on the importance of digital forensics and their area, as shown in Figure 2. The digital forensic process is multi-staged, involving the collection of digital evidence from one or multiple crime scenes, referred to as evidence acquisition [1]. Subsequently, the collected evidence undergoes digital forensic examination using forensic toolkits, which offer varying levels of abstraction to the data. This process aims to uncover hidden, deleted, or lost data from devices and detect and decrypt encrypted data. Metadata extraction for analysis purposes is facilitated with software support. Digital forensic analysis entails examining data to comprehend the potential explanations and logical sequences of events that elucidate the state of data in digital evidence [1]. Various digital forensic process modelling attempts have been made to foster growth in the field by proposing new theories and principles for developing methodologies and forensic tools in the investigation process. This paper presents an overarching taxonomy of the digital forensic process. The author provides detailed information about digital forensics and underscores the necessity of its application.

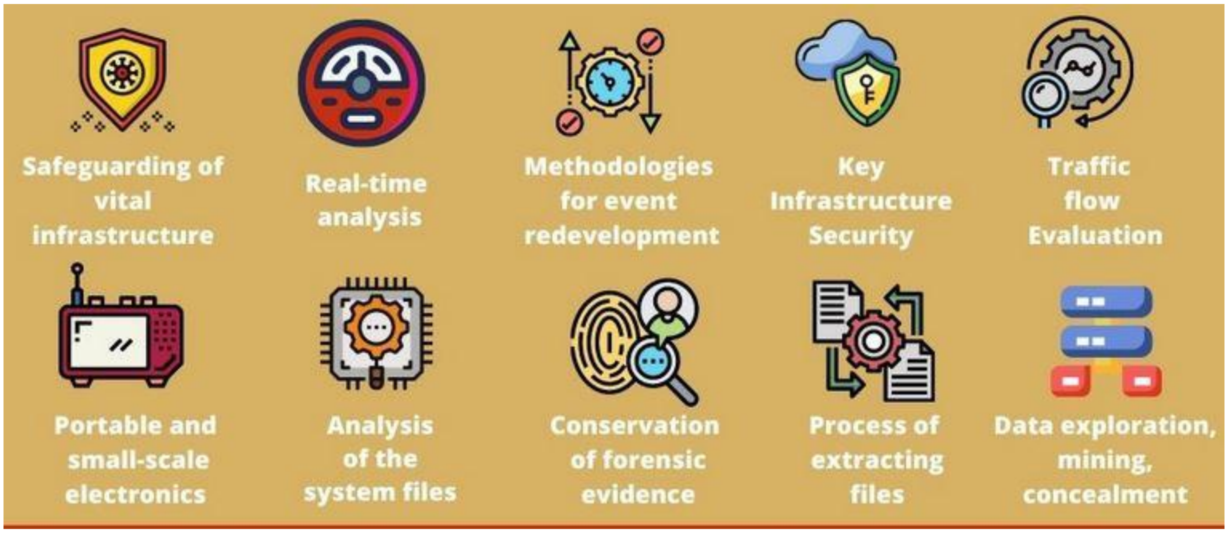
Safeguarding of vital infrastructure
Real-time analysis
Methodologies for event redevelopment
Key Infrastructure Security
Traffic flow Evaluation
Portable and small-scale electronics
Analysis of the system files
Conservation of forensic evidence
Process of extracting files
Data exploration, mining, concealment

Figure 2 Describe the area of forensics.

3. Methodology

This study aims to investigate the significance of Digital Forensics and the role of computers in this field. Given the necessity of understanding cybercrime for individuals and organisations alike, particularly in the aftermath of a cyberattack, the study emphasises the importance of digital forensics knowledge in guiding subsequent actions. The data collection process commenced with a comprehensive review of articles about digital forensics. These articles provided detailed insights into various aspects of digital forensics and underscored its significance in contemporary contexts. Additionally, several research papers related to digital forensics were consulted to deepen the understanding of the subject matter, as shown in Figure 3.

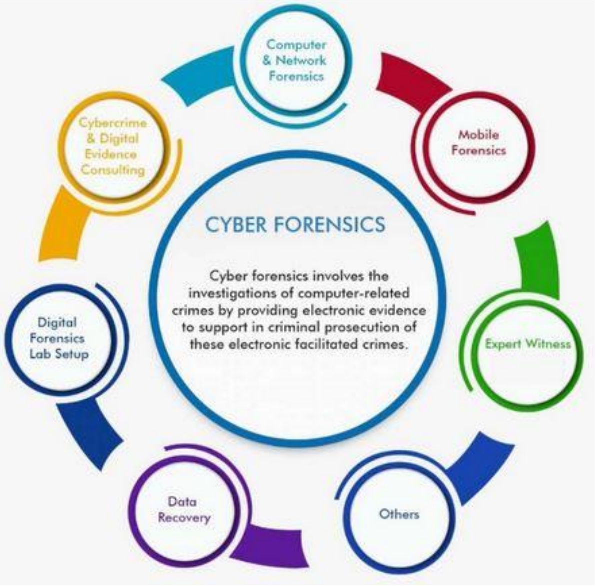
Computer & Network Forensics
Mobile Forensics
Expert Witness
Others
Data Recovery
Digital Forensics Lab Setup
Cybercrime & Digital Evidence Consulting
CYBER FORENSICS
Cyber forensics involves the investigations of computer-related crimes by providing electronic evidence to support in criminal prosecution of these electronic facilitated crimes.

Figure 3. Describe cyber forensics types

Furthermore, information crucial to the study was gathered from relevant websites, which offered valuable insights and resources for further investigation. These sources contributed to the comprehensive examination of digital forensics and its implications. The methodological approach adopted in this study prioritises synthesising information from diverse sources to gain a nuanced understanding of the importance of digital forensics and its role in addressing cybercrimes. Through the meticulous review of literature and online resources, the study aims to elucidate the critical role of digital forensics in navigating and mitigating the impact of cyberattacks.

4. ANALYSIS AND FINDINGS

Cyber forensics is a field that follows certain procedures to find evidence and reach conclusions after a proper investigation of matters. The procedures for cyber forensics are shown in Figure 4 and the details below.

1. Identification: The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.
2. Preservation: After identifying the data, the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper with the data.
3. Analysis: After getting the data, the next step is to analyse the data or system. Here, the expert recovers the deleted files, verifies the recovered data, and finds evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to conclude.
4. Documentation: Now, after analysing data, a record has been created. This record contains all the recovered and available(not deleted) data that helps recreate and review the crime scene.
5. Presentation: This is the final step in which the analysed data is presented before the court to solve cases.

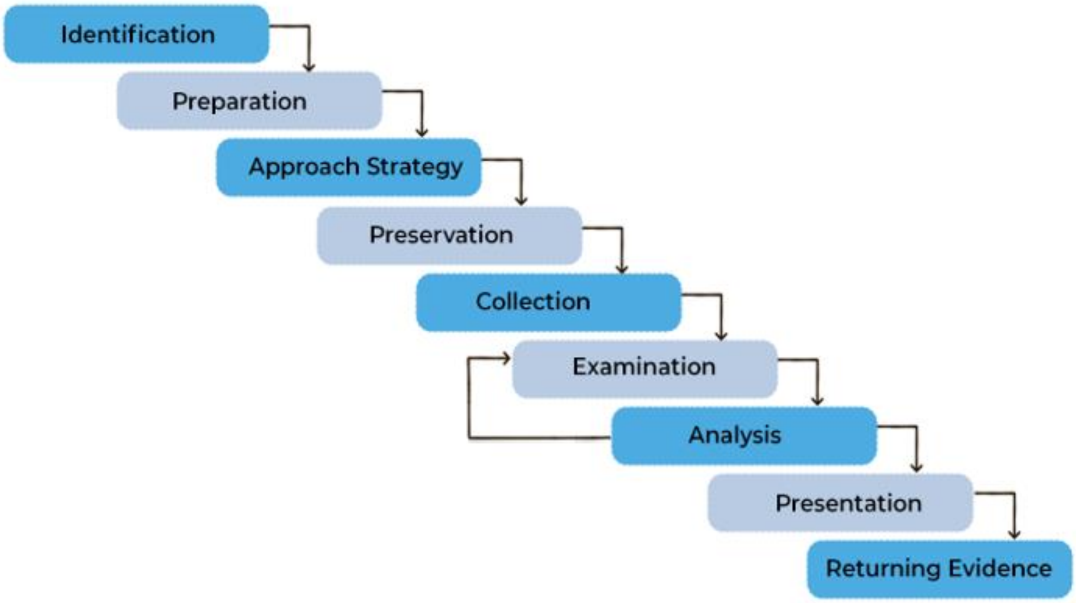

Figure 4. Steps for Cyber Forensic Experts

Types of cyber forensic

There are multiple types of computer forensics depending on the field in which digital investigation is needed.

1. Network forensics involves monitoring and analysing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.
2. Email forensics: In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract crucial information related to the case.
3. Malware forensics: This branch of forensics involves hacking-related crimes. Here, the forensics expert examines the malware trojans to identify the hacker involved behind this.
4. Memory forensics: This branch involves collecting data from the memory(like cache, RAM, etc.) in raw and retrieving information from that data.
5. Mobile Phone Forensics: This branch of forensics generally deals with mobile phones. They examine and analyse data from the mobile phone.
6. Database forensics: This branch of forensics examines and analyses the data from databases and their related metadata.
7. Disk forensics: This branch extracts data from storage media by searching modified, active, or deleted files.

Role of Computer in Digital Forensics

As technology advances, so does the crime landscape, with cybercriminal activity on the rise. In addressing cybercrimes, the discipline of digital forensics proves invaluable. Digital forensics experts utilise specialised forensic tools to gather evidence against perpetrators, while these same individuals may employ countermeasures, known as anti-forensics techniques, to conceal their illicit activities. This cat-and-mouse dynamic presents a significant challenge within the digital forensic community. When a suspect is identified, and their computing devices are seized as evidence, investigators embark on the crucial task of data extraction necessary for the investigation. In conducting these searches, strict adherence to digital forensic procedures is paramount. Unearthed information, ranging from documents to browsing histories and metadata, holds the potential to serve as critical evidence in legal proceedings. One essential aspect of digital forensics is the concept of digital footprints, which encapsulate information about a user's interactions within a system. This includes web pages visited, activity timestamps, and device usage patterns. By meticulously tracing these digital footprints, investigators can reconstruct the sequence of events and retrieve crucial data to resolve criminal cases. As a technological discipline, computer forensics employs investigative techniques to identify and preserve evidence from computing devices. This field is often instrumental in uncovering evidence admissible in a court of law, contributing significantly to the pursuit of justice. Through the systematic application of forensic methodologies, computer forensics professionals play a vital role in unravelling digital mysteries and holding perpetrators accountable for their actions.

5. CONCLUSION

In today's digital age, cyber forensics is a cornerstone in the ongoing battle against digital crime. Cybercriminals employ increasingly sophisticated techniques and methodologies as technology advances, underscoring the need for cyber forensics professionals to adapt and evolve continually. This study highlights the critical importance of integrating advanced forensic tools, interdisciplinary expertise, and legal insight to investigate and prosecute cybercrimes effectively. By examining the evolving landscape of cybercrime, the progression of computer forensics, and the challenges confronted by professionals, it becomes evident that fostering collaboration across sectors, investing in education, and advancing research are indispensable measures to stay ahead of cybercriminals. Ultimately, the efficacy of combating forensic cybercrime and advancing computer forensics relies on our ability to anticipate technological shifts, cultivate robust forensic capabilities, and uphold the tenets of justice in the digital realm.

6. REFERENCES

[1]. Shriram Raghavan, Digital Forensics Research: Current state of art. (Nov 2012)

[2]. Shraddha Vedre, Waman Parulekar, Digital Forensics and Role of Computer in Digital Forensics,(ISSN:2022-2882).

[3]. Casey, Eoghan. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet." Academic Press, 2011.

[4]. Carrier, Brian D. "File System Forensic Analysis." Addison-Wesley Professional, 2005.

[5]. Nelson, Bill, et al. "Guide to Computer Forensics and Investigations." Cengage Learning, 2020.

[6]. Singh, Sourabh Kumar, and Amarnath Mishra. "Digital Forensics and Cybersecurity Tools." Advancements in Cybercrime Investigation and Digital Forensics. Apple Academic Press, 2024. 367-382.

[7]. Sammons, John. "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics." Syngress, 2014.

[8]. Beebe, Nelson, et al. "Digital Forensic Research: The Good, the Bad, and the

Unaddressed.” Digital Investigation, vol. 6, no. S1, 2009, pp. S3-S7.

[9]. Carrier, Brian D., and Joe Grand. “Defining a Taxonomy for Computer Forensics.” Digital Investigation, vol. 1, no. 1, 2004, pp. 3-15.

[10]. Pollitt, Mark. “Digital Forensics: Digital Evidence in Criminal Investigations.” Wiley, 2011.

[11]. Casey, Eoghan. “Handbook of Digital Forensics and Investigation.” Academic Press, 2009.

[12]. Maras, Marie-Helen. “Computer Forensics: Cybercriminals, Laws, and Evidence.” Jones & Bartlett Learning, 2012.

[13]. Jones, Richard. “Introduction to Information Security: A Strategic-Based Approach.” John Wiley & Sons, 2013.

[14]. Rosenblatt, Bill. “The Art of Cyber Forensics: A Guide for IT Professionals.” Apress, 2018.

[15]. Rogers, Marcus K. “Network Forensics: Tracking Hackers through Cyberspace.” Prentice Hall, 2012.

[16]. Singh, Anuj, and Bret Hartman. “Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure.” Syngress, 2013.

[17]. Jones, Keith, et al. “Practical Forensic Imaging: Securing Digital Evidence with Linux Tools.” Syngress, 2016.

[18]. Vacca, John R. “Computer Forensics: Computer Crime Scene Investigation.” Charles River Media, 2005.