International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

CYBER FORENSICS: INVESTIGATING DIGITAL CRIMES

Sonasri.S[1], Blessy Priya Niranjana. M[2]

[1,2]Assistant Professor, Bharath Institute of Law

Abstract

Cyber forensics, also known as digital forensics, is a branch of forensic science that focuses on the identification, collection, preservation, analysis, and presentation of digital evidence to investigate cybercrimes. With the increasing reliance on digital technology, cybercrimes such as hacking, identity theft, data breaches, and malware attacks have become more sophisticated, necessitating advanced forensic techniques. Cyber forensic investigations involve various phases, including evidence identification, data acquisition, analysis, documentation, and legal presentation. Several specialized tools and methodologies aid forensic experts in retrieving and analyzing digital evidence. Tools like Autopsy, EnCase, and Forensic Toolkit (FTK) assist in disk imaging, file recovery, and system analysis, while Wireshark and Volatility facilitate network traffic monitoring and memory forensics. These tools help uncover hidden, deleted, or encrypted data that can serve as crucial evidence in legal proceedings. Additionally, forensic techniques such as file carving, data hashing, and malware analysis enhance the accuracy and integrity of cyber investigations. The legal and ethical aspects of cyber forensics play a critical role in ensuring that digital evidence is admissible in court. Maintaining the chain of custody, adhering to cyber laws and regulations, and protecting individual privacy are fundamental principles guiding cyber forensic investigations. Furthermore, with the rise of cloud computing, IoT devices, and artificial intelligence, cyber forensic methodologies are evolving to tackle new challenges. The integration of machine learning and blockchain forensics is expected to revolutionize digital investigations, making them more efficient and accurate. As cyber threats continue to grow in complexity, the importance of cyber forensics in ensuring digital security and justice cannot be overstated. The future of cyber forensics lies in continuous advancements in technology, legal frameworks, and forensic methodologies to combat emerging cyber threats effectively.

Key Words: Cyber Forensics, Digital Investigation, Principles, Blockchain techniques, Cyber Threats.

1. INTRODUCTION:

Cyber forensics is the science of collecting, inspecting, interpreting, reporting, and presenting computer-related electronic evidence. Evidence can be found on the hard drive or in deleted files. It is the process of examining, acquiring, and analysing data from a system or device so that it can be transcribed into physical documentation and presented in court. During the inspection, it is critical to create a digital or soft copy of the system's special storage cell. The purpose of carrying out a detailed cyber forensics investigation is to determine who is to blame for a security breach. The entire inquiry is carried out on the software copy while ensuring that the system is not affected. In the technological age, cyber forensics is

an inevitable factor that is incredibly important. Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings. The rapid technological advancement has led the entire world to shift towards digital domain. However, this transition has also result in the emergence of cybercrimes and security breach incidents that threatens the privacy and security of the users. Therefore, this chapter aimed at examining the use of digital forensics in countering cybercrimes, which has been a critical breakthrough in cybersecurity. The chapter has analyzed the most recent trends in digital forensics, which include cloud forensics, social media forensics, and IoT forensics. These technologies are helping the cybersecurity professionals to use the digital traces left by the data storage and processing to keep data safe, while identifying the cybercriminals. However, the research has also observed specific threats to digital forensics, which include technical, operational and personnel-related challenges. The high complexity of these systems, large volume of data, chain of custody, the integrity of personnel, and the validity and accuracy of digital forensics are major threats to its large-scale use. Nevertheless, the chapter has also observed the use of USB forensics, intrusion detection and artificial intelligence as major opportunities for digital forensics that can make the processes easier, efficient, and safe.

2. RECENT DIGITAL FORENSIC TRENDS

CLOUD FORENSICS

Cloud forensics has recently immense much attention by forensics experts due to the fact that cloud computing offers massive resource pool, cost-effective solution, dynamicity, and wide access for storage. Hybrid, private, and public models of cloud computing exists, in addition to multiple services, such as security as service, database as service, integration as service, and software as service[1]. Furthermore, most companies and organizations transfer their products and services across the cloud every day due to multiple benefits, including high scalability, reduced cost of IT infrastructure, business continuity, and access to automatic updates. As a result, cloud computing has been widely accepted in multiple governments and private companies. Likewise, Communication Service Providers have established data centres across the globe in various jurisdictions that provide cloud services for ensuring value-effectiveness and service availability. However, the rise in the number of cybercrimes and security in the cloud environment are the major hurdles for organizations to transfer their systems to this platform. Moreover, since forensics investigation in a cloud computing environment is complex, security analysts see cloud computing as a potential area of concern. Therefore, cloud forensics has gained major attention by forensics investigators to resolve cloud computing issues. Cloud forensics can be described as the potential application of digital forensics in a cloud-based environment. This field utilizes scientific principles, proven methods, and technological practices to process events in cloud environment via

[1] Dykstra, J., & Sherman, A. T. (2013). "Design and Implementation of a Cloud Forensic Toolkit." *Digital Investigation,* 10(1), S87-S95.

reporting, examination, preservation, collection, and identification of digital data, so that events can be reconstructed.

SOCIAL MEDIA FORENSICS:

The advancement in Industry 4.0 and Web 2.0 technologies has significantly increased the acceptance of social media platforms and it has become a primary source of socialization. Users actively share their information, create accounts, and get engage in social forms through these sites[2]. As a result, hackers are exposed to various opportunities to exploit user's account. In addition, different social media applications like LinkedIn, Instagram, Facebook, and Twitter have been exposed to multiple cyber threats and malware. Attacks on social media platforms can take place outside the system/network or within the network. Outside systems attack usually include DDoS, or DoS, while attacks within the network include retrieving cookies data. Besides, it is established that the database of these social media applications is most vulnerable to such attacks. Considering this situation, digital investigators have shifted their interest towards social media forensics. Social media forensics assist experts in carrying out a criminal investigation, where social media posts serve as excellent evidence to investigators. Likewise, social media platforms are a perfect source of information regarding potential offenders, suspects, and witnesses, and it is considered supreme for profiling. In addition, by combining social media with digital forensics, investigators can gain access to a modern and diverse subset of sources of data, including demographic location, photographs, contact lists, geo-location, and text messages. This network data, combined with the metadata, has the potential to assist digital forensics investigations. Furthermore, the metadata can also be used to authenticate online social networking facts. Thus, it can be contended that social media forensics is a rising trend in the digital forensics' domain due to its ability to efficiently providing adequate digital evidence.

BLOCK CHAIN FORENSICS:

Blockchain forensics is the process of analysing blockchain transactions to track illicit activities, recover stolen funds, and ensure compliance with regulatory standards. Since blockchain operates on a decentralized ledger with pseudonymous transactions, forensic experts use advanced analytical techniques to de-anonymize users and identify suspicious activities. The primary method involves transaction clustering, where multiple addresses controlled by the same entity are grouped using behavioural patterns and shared inputs[3]. Address tagging helps associate wallet addresses with known individuals, exchanges, or illicit entities based on prior investigations and on-chain data. Graph analysis is another key approach, where transaction flows are mapped visually to detect anomalies, such as money laundering schemes, ransomware payments, and darknet market activities. Forensic investigators also use heuristic analysis, where spending habits and transaction linkages reveal hidden relationships between parties. Advanced tools like Chainalysis[4], Elliptic, CipherTrace, and TRM Labs assist in tracking cross-border transactions, identifying mixing services (tumblers), and detecting illicit fund transfers in decentralized finance (DeFi)

[2] Chauhan, H. (2022). "Forensic Investigation of Social Media Crimes." *Journal of Cyber Law & Policy,* 15(3), 45-62.
[3] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf last accessed on 18th January,2025.
[4] Chainalysis (2023). *The 2023 Crypto Crime Report.* https://www.chainalysis.com/reports last accessed on 18th January 2025.

platforms. The rise of privacy coins like Monero and Zcash, along with coin-mixing services, poses new challenges, requiring AI-driven anomaly detection and machine learning models to analyze transaction metadata. Additionally, NFT and smart contract forensics have become crucial as scams and frauds increase in the crypto space. Governments and financial regulators, including those in India, are actively strengthening their blockchain forensic capabilities to combat fraud, enforce Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations, and prevent crypto-related cybercrimes. With the growing adoption of cryptocurrencies, blockchain forensics plays a vital role in ensuring transparency, security, and compliance in the digital financial ecosystem.

IOT FORENSICS:

IoT forensics is a specialized branch of digital forensics that focuses on investigating cybercrimes and security incidents involving Internet of Things (IoT) devices. As IoT devices such as smart home systems, wearable gadgets, industrial sensors, and connected vehicles become increasingly integrated into daily life, they generate vast amounts of digital data that can serve as crucial forensic evidence. IoT forensics involves the collection, preservation, analysis, and presentation of data from these interconnected devices while maintaining the integrity and chain of custody. The forensic process includes network forensics (analysing data transmission between IoT devices and cloud servers), device forensics (retrieving logs, metadata, and sensor data from IoT hardware), and cloud forensics (investigating evidence stored in remote cloud infrastructures). Challenges in IoT forensics include data volatility, proprietary protocols, limited device storage, and encryption mechanisms, which complicate evidence retrieval. Advanced forensic techniques such as firmware analysis, reverse engineering, AI-driven anomaly detection, and edge computing forensics are being developed to address these challenges. Tools like Wireshark, Volatility, and IoT-specific forensic frameworks assist in data extraction and analysis. IoT forensics is increasingly vital in cybercrime investigations, accident reconstruction (e.g., vehicle black box analysis), smart city security, and healthcare device forensics. Law enforcement agencies and cybersecurity firms worldwide, including in India, are investing in IoT forensic capabilities to combat emerging threats[5].

MOBILE FORENSICS:

Mobile forensics is a branch of digital forensics that focuses on the identification, acquisition, analysis, and preservation of digital evidence from mobile devices, including smartphones, tablets, and other mobile technologies. Given the increasing use of mobile devices for personal, professional, and social activities, mobile forensics plays a crucial role in criminal investigations, from cybercrime to traditional crimes like murder, fraud, and trafficking. Mobile devices store a wealth of data such as call logs, text messages, emails, photos, GPS locations, app usage, and even biometric information, all of which can be critical in solving crimes[6].

One of the main challenges in mobile forensics is dealing with the variety of operating systems, primarily iOS and Android, each with distinct security models, file systems, and encryption protocols. The forensic process typically involves four stages: data acquisition, data analysis, data presentation, and data preservation. Data acquisition is the first critical step, where forensic experts use specialized tools like

[5] Zawoad & Hasan (2015) on IoT forensics framework and Miller et al. (2017).
[6] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

XRY, Cellebrite UFED, or Oxygen Forensic Detective to extract data from mobile devices[7]. The extraction can be done via logical, physical, or file system methods, depending on the device's configuration and security settings. Logical extraction accesses data like contacts, messages, and call history, while physical extraction retrieves raw data, including deleted information that may still reside in the device's memory[8].

Data analysis follows acquisition, where forensic investigators examine the extracted data for relevant evidence. Mobile forensics experts must also overcome encryption methods and passcodes, and sometimes utilize brute-force attacks or bypassing techniques like jailbreaking or rooting the device. In cases of encrypted data, advanced decryption tools or cooperation from manufacturers may be required. Data preservation is a crucial step to ensure that the digital evidence remains intact for legal purposes. This involves maintaining a chain of custody and using write-blocking tools to avoid tampering with the original data.

Mobile forensics also faces challenges like over-the-air (OTA) data deletion, device remote wiping, and the rapid evolution of mobile technology, requiring constant updates to forensic methodologies. Cloud storage integration further complicates the analysis, as it stores a significant amount of data that is synchronized with the mobile device. As mobile operating systems and encryption methods evolve, forensic specialists must continually adapt to new security protocols while ensuring compliance with legal standards like the General Data Protection Regulation (GDPR)[9] and the Information Technology Act in India. Tools like Magnet AXIOM, ElcomSoft Mobile Forensic Bundle, and X1 Social Discovery are commonly used in mobile forensic investigations to ensure that the evidence is legally admissible in court.

TOOLS &TECNIQUES FOR THE CYBER FORENSIC INVESTIGATION:

Cyber forensic investigation is the process of identifying, collecting, analysing, and preserving digital evidence to investigate cybercrimes such as hacking, data breaches, fraud, and identity theft. With the increasing complexity of cyber threats, forensic experts rely on a combination of tools and techniques to retrieve critical data, analyse cyber incidents, and ensure evidence integrity for legal proceedings. Cyber forensic tools help investigators extract, analyze, and present digital evidence from computers, mobile devices, cloud systems, and networks.

Cyber forensic investigation involves the identification, collection, preservation, and analysis of digital evidence to uncover cybercrimes and malicious activities. Various tools and techniques aid investigators in this process. One of the most widely used tools is **Autopsy**, an open-source digital forensic platform that allows forensic experts to analyze hard drives, recover deleted files, and examine disk images[10]. Similarly, **FTK (Forensic Toolkit)** provides advanced disk imaging and password recovery capabilities, making it a preferred choice for forensic analysis[11].

[7] Sherman, A. T., & Dykstra, J. (2013). "The Design and Implementation of a Mobile Forensic Toolkit." *Journal of Digital Investigation,* 10(1), S87-S95.
[8] Salinas, J. (2016). "Understanding iOS and Android Forensics." *International Journal of Digital Crime and Forensics,* 8(2), 32-45.
[9] General Data Protection Regulation (GDPR), 2016. *European Union.* https://gdpr.eu Last accessed on 20th January 2025.
[10] Carrier, B. (2002). *Autopsy: Open Source Digital Forensics Platform.*
[11] AccessData. (2020). *Forensic Toolkit (FTK) User Guide.*

Another essential tool is EnCase, which enables investigators to create forensic images, analyze system artifacts, and detect suspicious activities within digital devices[12]. For memory analysis, Volatility is widely used to extract data from RAM and detect malware or unauthorized processes. Additionally, Wireshark helps capture and analyze network traffic, making it useful in detecting cyber threats and intrusion attempts[13].

Besides tools, forensic experts rely on various techniques to extract and analyze digital evidence. Live forensics involves collecting volatile data from a system before it is powered down, while dead forensics examines storage devices in an offline state to ensure data integrity[14]. File carving is a technique used to recover fragmented or deleted files, and hashing ensures data authenticity by generating unique digital fingerprints[15].

These tools and techniques, when used effectively, enable forensic experts to investigate cybercrimes, trace attackers, and present credible digital evidence in legal proceedings. Continuous advancements in forensic methodologies further enhance the accuracy and reliability of cyber investigations.

3. KEY PRINCIPLES OF CYBER FORENSICS:

1. Confidentiality: Protecting Sensitive Data

Confidentiality ensures that information is only accessible to individuals who have the necessary authorization. The goal is to protect personal, financial, and proprietary information from unauthorized access.

2. Integrity: Maintaining Data Accuracy and Reliability

Integrity focuses on ensuring that data remains accurate, consistent, and unaltered. This principle is vital to stop unauthorized individuals from changing or tampering with data, thereby ensuring that the information you rely on is credible.

3. Availability: Guaranteeing Access to Systems and Data

Availability ensures that systems and data are reachable whenever required, avoiding problems like downtime or service interruptions. DDoS (Distributed Denial of Service) attacks are a form of cyberattack that target availability by overwhelming systems with excessive traffic, leading to crashes.

[12] Guidance Software. (2018). *EnCase Forensic User Manual*.
[13] Orebaugh, A., & Ramirez, G. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*.
[14] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*.
[15] Garfinkel, S. (2010). *Digital Forensics: Hashing and File Carving Techniques*.

4. Accountability: Tracking Actions and Events

This is a crucial concept for identifying and addressing harmful or illegal activities within a network. Accountability guarantees that every action taken on a system can be traced back to the individual responsible for it.

5. Non-Repudiation: Preventing Denial of Action

Once an action or transaction has been executed, non-repudiation ensures that the parties involved cannot deny their participation. This principle is essential in legal and financial situations, where proof of actions is required to resolve disputes.

6. Risk Management: Identifying and Addressing Potential Threats

Risk management enables you to identify and assess potential threats to your data and systems, allowing you to create an effective strategy to mitigate or eliminate those threats. In cybersecurity, this is an ongoing process that involves evaluating and adapting to new and emerging risks.

7. Defense in Depth: Layered Security Approach

Defense in depth refers to the implementation of multiple security layers to protect systems and data. This concept ensures that critical assets remain secure even if one layer is breached.

8. User Training and Awareness: Empowering Self-Defense

Often, the most vulnerable aspect of cybersecurity is the human element. To ensure that individuals understand the risks and how to avoid falling victim to common threats such as phishing, weak passwords, and unsafe browsing habits, user training and awareness are crucial.

4. PHASES OF CYBER FORENSICS:

Cyber forensic investigations follow a structured approach to ensure the systematic collection and analysis of digital evidence while maintaining its integrity. The process begins with the identification phase, where investigators determine potential sources of digital evidence, such as computers, mobile devices, network logs, and cloud storage. This is followed by the collection and preservation phase, where forensic experts acquire data without altering its original state, often using disk imaging tools like FTK Imager and EnCase to create exact replicas of storage devices[16].

Next, the examination and analysis phase involves scrutinizing the collected data to uncover relevant evidence. Investigators use specialized forensic tools like Autopsy, Volatility, and Wireshark to analyze file systems, detect malware, and reconstruct digital activities[17]. Data carving, hashing, and timeline analysis help in verifying data authenticity and tracing cybercriminal activities. The documentation and

[16] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.*
[17] Carrier, B. (2002). *Autopsy: Open Source Digital Forensics Platform*.

reporting phase ensures that all findings are recorded in a structured manner, detailing the investigative process, tools used, and extracted evidence, which is crucial for legal proceedings[18].

The final phase is presentation and legal proceedings, where forensic experts testify in court and present their findings in a manner that is admissible under law. Ensuring compliance with legal frameworks such as the Digital Evidence Rule and Cybercrime Laws is critical to maintaining the credibility of forensic reports[19]. By following these phases, cyber forensic experts can systematically investigate cybercrimes while upholding the integrity and admissibility of digital evidence in legal proceedings.

5. CHALLENGES WITH CYBER FORENSICS:

The two main obstacles encountered during a digital forensic investigation are complexity and volume. The complexity issue pertains to the data being gathered at its most basic level or in an unprocessed format. Individuals without technical backgrounds may struggle to comprehend such information. Various tools can assist in converting the data from its raw state to a more understandable format. The volume issue relates to the sheer amount of data that must be scrutinized. Techniques for data reduction can be employed to categorize information or eliminate data that is already known. Such techniques for data reduction include:

- Recognizing known network packets through IDS signatures

- Detecting unknown entries during log analysis

- Identifying known files via hash databases

- Organizing files according to their types

Legal Challenges

Digital evidence is susceptible to tampering, often leaving no traces behind. Modern computers typically contain multiple disks each measuring several gigabytes. The process of seizing and safeguarding digital evidence can no longer be achieved simply by burning a CD-ROM. If evidence is not secured before opening files, it may render crucial evidence invalid. Moreover, locating pertinent evidence amid vast amounts of data can be an overwhelming task. The true legal challenges arise from the artificial constraints imposed by constitutional, statutory, and procedural matters. Numerous personnel types are involved in digital/computer forensics, such as technicians, policy makers, and professionals. Technicians possess the expertise and skills necessary to extract information from digital devices, comprehend both software and hardware, and understand networking principles. Policy makers develop forensic policies that encompass broader concerns. Professionals serve as the bridge between policy and implementation, equipped with significant technical abilities and a solid grasp of legal procedures. Digital Forensics encompasses the gathering, examination, and protection of digital evidence for use in legal proceedings or investigations. This field encounters various challenges. To tackle these difficulties, Digital Forensics experts must invest

[18] Garfinkel, S. (2010). *Digital Forensics: Hashing and File Carving Techniques*.
[19] Kruse, W. & Heiser, J. (2001). *Computer Forensics: Incident Response Essentials*.

in the necessary tools and resources, remain informed about technological innovations, and collaborate closely with the legal and investigative communities to establish standards and protocols.

Here are some of the challenges faced by Digital Forensics:

- A high level of technical skill is essential, and there is a lack of qualified forensic analysts in the industry.

- The rapid growth of digital data generation and storage complicates the task for forensic analysts trying to sift through and pinpoint relevant evidence.

- Digital devices and systems can be intricate, making the analysis and comprehension of stored data challenging.

- The increasing prevalence of encryption for safeguarding sensitive information poses additional hurdles for forensic analysts seeking access to and examination of data.

- Over time, digital data may become corrupted or lost, complicating recovery and analysis efforts.

- Techniques and tools in Digital Forensics must continually adapt to keep in line with evolving technology and new digital devices[20].

- The acceptance of digital evidence in court can present challenges; forensic analysts need to be capable of demonstrating the validity and reliability of the evidence they have gathered.

6. CONCLUSION:

The domain of digital forensics is essential for the judicial system. In today's world, technology is integral to daily life, and a significant portion of society relies heavily on it. As a result, cybercrime is expected to rise, and digital forensics is still grappling with this escalating issue. At present, the field of digital forensics is ill-equipped to handle cybercrime investigations due to the absence of universal benchmarks, the fast-paced evolution of technology, and various legal challenges. Without a common standard, there is no clear direction on what is required to become a digital forensic expert. Individuals possess diverse qualifications, educational backgrounds, and training in digital forensics. There are no universal criteria outlining the essential knowledge or the type of training and education necessary to achieve competence. The lack of standards has led to different agencies and organizations carrying out digital forensics in their unique ways, which may not always be uniform. The field is plagued by professionals employing various techniques and tools for investigations and analyses that may lack scientific validation. This inconsistency can lead to differing results, which may be inaccurate, resulting in evidence being dismissed in legal proceedings. The rapid advancement of technology poses another challenge for digital forensics. There is an ongoing necessity for digital forensic experts to stay abreast of the latest technological developments, requiring continuous learning and self-training to remain proficient. Maintaining competence as a digital forensics professional can be a demanding and time-intensive endeavor, and not all practitioners have the

[20]Challenges in Computer Forensics https://www.startertutorials.com/blog/challenges-in-computer-forensics.html last accessed on 10th march 2025.

necessary resources or capabilities to keep pace with technological advancements. Instances of cybercrime such as voter fraud, election tampering, and insider trading within the cryptocurrency sphere exemplify new technology-related offenses that necessitate staying informed. Furthermore, the legal hurdles associated with digital forensics represent yet another barrier impeding the field's progress. The intricate nature of technology has sparked considerable discussion regarding the legal handling of data. Issues related to cloud technology and encryption have introduced complications concerning jurisdiction, ownership, search and seizure, and privacy rights. Data can be unstable and prone to contamination, similar to other types of evidence, if not properly managed. In summary, the field is currently ill-prepared to address the surge of cybercrime we witness today. Digital forensics requires a standardized set of criteria grounded in reliable and scientific methods to cultivate a more competent workforce within the discipline. There must be increased training and resources to keep pace with advancing technologies. Establishing a universal set of standards would likely resolve many of the challenges currently faced by digital forensics.