LAWFOYER INTERNATIONAL

JOURNAL OF DOCTRINAL LEGAL

RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 3

2024

CYBER FORENSIC AND CRIME INVESTIGATION

Harini K[1]

I. ABSTRACT

Cyber forensics, often called digital forensics, is essential in modern crime investigations. It provides the methods & strategies to gather, analyze, and safeguard digital evidence. This field's significance has grown as digital crimes have become more complex and frequent. It includes activities like hacking, identity theft, financial fraud, cyberstalking, and even cyberterrorism. The main purpose of cyber forensics is to aid legal proceedings by ensuring that digital evidence is valid, dependable & usable in court. The admissibility of digital evidence is also a matter of concern for its probative value is called into question upon evidence is prone to be tampered. It combines knowledge from computer science, legal studies, and investigative techniques to find and document digital traces left by criminals. Cyber forensics includes various sub-disciplines: computer forensics, network forensics, mobile device forensics & cloud forensics. Each one deals with specific challenges related to different types of digital evidence. Experts in cyber forensics use special tools & software to perform tasks like disk imaging, data carving, malware analysis, and timeline reconstruction. These tasks are crucial for understanding the sequence of events in a digital crime. Nonetheless, the field encounters many challenges. Technology evolves rapidly; cybercriminals become more sophisticated; legal restrictions related to data privacy & jurisdictional issues create obstacles. Advanced technologies such as encryption and anonymization test the ability of forensic experts to gather meaningful evidence. Moreover, the international nature of cybercrime often entails complicated legal structures that demand cross-border cooperation & compliance with diverse laws and regulations.

II. KEYWORDS:

[1] LLM- I Year (Criminal law and criminal justice administration) Tamil Nadu Dr. Ambedkar Law University- School of Excellence in Law

Cyber Forensic, Digital Forensic, Digital Evidence, Investigation, Data Extraction, Data Acquisition, Data preservation.

III. INTRODUCTION

Forensics in the cyber world has changed a lot. the change reflects how fast technology is moving & how cybercrime is rising. In the past, forensic science mainly focused on collecting & analysing physical evidence from regular crime scenes. Now, with our lives more connected online, forensics has evolved to tackle new challenges in the digital space. Cyber forensics started as a specific area because there was a need to investigate crimes happening online. This shift began back in the 1980s when personal computers & the internet became popular. New kinds of crimes came up, like hacking, identity theft, and online fraud. So, forensic methods had to change too. They now include finding, keeping, & looking at digital evidence from devices, networks, & cloud services. Today, cyber forensics covers many activities. This includes recovering deleted files and checking network traffic. It also involves tracing digital footprints and gathering evidence for court cases. Because of this change, law enforcement absolutely relies on cyber forensics to fight against smart cyber threats effectively. The field has grown to include proactive steps like vulnerability checks and incident responses to stop future attacks. Furthermore, new technologies like artificial intelligence (AI) and machine learning are changing how cyber forensics works. These tools help analyze huge amounts of data quickly and accurately—this makes investigations better. As cyber threats keep evolving, forensic roles will likely grow even more important. There's a clear need for ongoing learning & skill development among people working in forensics. The paper deals about types of cyber forensic and how cyber forensics have aided in criminal investigations.

IV. HISTORICAL EVOLUTION OF CYBER FORENSICS

A. Early Beginnings: Traditional Forensics to Digital Forensics

Digital forensics began its journey in the 1980s when personal computers started to become more common. Computer-related crimes also began to appear. At its inception, strategies in digital forensics aimed at analysing computer systems &

collecting evidence for criminal investigations. By the 1990s, core techniques and formal methodologies for collecting evidence and investigating crimes were well established[2].

B. Evolution of Cybercrime: From Hacking to Advanced Persistent Threats

As Internet usage grew globally in the early 2000s, cybercrime expanded. Hackers & cybercriminals, leveraging new technologies like encryption, made it harder to trace their actions. In the early 2000s, a significant encryption method called the Advanced Encryption Standard (AES) emerged, complicating the tracking of criminals. AES became widely adopted once it was established as a federal standard in 2001, replacing the older Data Encryption Standard (DES). AES employs symmetric key encryption, meaning the same key is used for both encryption & decryption. This allows for strong data protection, making it hard for unauthorized parties to access or trace communications without the decryption key.

Another notable method from that period was RSA (Rivest-Shamir-Adleman), a public-key cryptosystem developed in 1978. Gaining popularity in the 2000s, RSA uses a pair of keys: a public key for encryption and a private key for decryption. This asymmetrical approach not only enhances security but complicates tracing encrypted communications since the decryption key isn't shared publicly. Both AES and RSA significantly impacted law enforcement and cybersecurity professionals' efforts to track and investigate cybercriminal activities during that era. These encryption methods provided robust security for sensitive information & communications, posing notable challenges for professionals in the field[3].

This situation prompted digital forensics experts to create more sophisticated decryption methods.

C. Milestones in Cyber Forensics: Key Events and Developments

[2] Champlain.edu. (2024). *The Evolution of Digital Forensics*. [online] Available at: https://online.champlain.edu/blog/evolution-digital-forensics [Accessed 6 Sep. 2024].

[3] Kime, C. (2023). *Types of Encryption, Methods & Use Cases*. [online] eSecurity Planet. Available at: https://www.esecurityplanet.com/trends/types-of-encryption/ [Accessed 6 Sep. 2024].

The establishment of the International Association of Computer Investigative Specialists (IACIS) & the National Institute of Standards and Technology (NIST) in the early 2000s aimed at guiding best practices[4]. The evolution of forensic tools. Hard drive duplicators, file viewers, and password recovery devices advanced as technology evolved to aid investigations. The emergence of cyber forensics as an official discipline during the 1980s boom of personal computers[5].

D. The Role of Technology in Shaping Cyber Forensics

Technological progress both facilitated and posed challenges for cyber forensics over time:

- Increased automation of printing & the introduction of digital media enhanced information sharing and enabled new forms of crime.
- Wireless communications, social networking & smartphones complicated the investigative landscape[6].
- Cloud computing and mobile devices made it tougher for cyber forensics specialists to keep pace with evolving technologies.
- Encryption & privacy measures restricted the investigative capacity of individual security experts.

Nevertheless, the growing need for cyber forensics driven by these challenges also catalysed the development of new tools and resources. These include free online courses and supportive communities aimed at aiding investigations.

V. FUNDAMENTAL CONCEPTS OF CYBER FORENSICS

A. Definition and Scope of Cyber Forensics

Cyber forensics, often called computer forensics, entails the process of gathering, analysing, and reporting digital data in a legally acceptable way. It covers preserving, identifying, extracting & documenting computer evidence through specialized

[4] https://online.champlain.edu/blog/evolution-digital-forensics]

[5] https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2a54509d-b6bb-43d8-8250-eae26782c392/FORC%20Book%201.pdf

[6] Ibid

methods and tools. This field investigates crimes linked to electronic devices to recover deleted files, chat logs, emails, and other digital proof[7] [8].

B. Key Terminologies in Cyber Forensics:

- **Digital evidence:** Data stored or moved using computer systems that supports or refutes a theory on how a crime happened or addresses key parts like intent or alibi.
- **Chain of custody:** Detailed records showing the seizure, custody, control, transfer, analysis & handling of evidence. For digital evidence to be admitted in court, a valid chain of custody must be established. This proves that the evidence has not been altered and has been preserved in its original form from the moment it is collected until it is presented. The evidence may be contested and perhaps declared inadmissible by the court if there are any lapses or breaks in the chain of custody[9].
- **Volatile data:** Information in computer memory that disappears when the device loses power or is switched off.
- **Non-volatile data:** Info stored on hard drives or other storage media that stays even when the device is turned off.

C. The Digital Evidence Lifecycle

In cyber forensics, the digital evidence lifecycle includes these phases:

- **Identification:** Figuring out what evidence exists and where it resides.
- **Preservation:** Storing the evidence carefully to prevent tampering.
- **Collection:** Creating a forensic image or copy of the digital data.

[7] What Is Cyber Forensics? | Splunk, Splunk (2024), https://www.splunk.com/en_us/blog/learn/cyber-forensics.html (last visited Aug 27, 2024).

[8] GeeksforGeeks, *Cyber Forensics*, GeeksforGeeks (2021), https://www.geeksforgeeks.org/cyber-forensics/ (last visited Aug 27, 2024).

[9] csdiscovery (2022). *Maintaining Chain of Custody in Digital Forensics*. [online] Cornerstone Discovery. Available at: https://cornerstonediscovery.com/maintaining-chain-of-custody-in-digital-forensics-what-you-should-know/ [Accessed 6 Sep. 2024].

- **Examination:** Looking at the gathered data to find relevant details.
- **Analysis:** Interpreting the findings to draw conclusions about the evidence.
- **Presentation:** Summarizing results in a legally acceptable report[10].

D. Importance of Cyber Forensics in Modern Investigations

Cyber forensics is crucial in today's investigations for several reasons:

- It aids in collecting digital proof to track down criminals and solve crimes involving electronic gadgets.
- Helps recover deleted files, chat logs, emails & other data inaccessible to regular users.
- Establishes an evidence chain proving who committed a crime and how it was done.
- Is used not only for cybercrimes but also real-world offenses like theft & murder.
- Businesses use it to monitor system breaches and pinpoint attackers.

As technology keeps advancing, the significance of cyber forensics will continue growing to tackle ever more sophisticated cybercrimes[11].

VI. LEGAL FRAMEWORK & ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA CONCERNING IT ACT

A. Legal Standards for Digital Evidence

The admissibility of digital evidence in India primarily relies on the Information Technology Act, 2000 (IT Act) & the Indian Evidence Act, 1872 (BSA currently). Key standards include:

[10] Rahul Awati & Ben Lutkevich, *computer forensics (cyber forensics)*, Security (2024), https://www.techtarget.com/searchsecurity/definition/computer-forensics (last visited Aug 27, 2024).

[11] GeeksforGeeks, *Cyber Forensics*, GeeksforGeeks (2021), https://www.geeksforgeeks.org/cyber-forensics/ (last visited Aug 27, 2024).

Section 2(t) of the IT Act defines "electronic record" as data, records or data generated, images or sounds stored, received, or sent in electronic form, microfilm, or computer-generated microfiche[12].

Section 4 of the IT Act mentions any information or matter can be taken as "writing" or "typewriting" if it is displayed, recorded, stored, transmitted, or received in an electronic form[13].

B. Admissibility of Digital Evidence in Court: Challenges

While the IT Act provides a framework for digital evidence, there are still challenges in its admissibility in court: Ensuring the authenticity and integrity of digital evidence is crucial. However, it can be difficult with the ease of tampering. Lack of proper procedures and trained personnel for collecting, preserving & analysing digital evidence. The transnational nature of cybercrime makes obtaining digital evidence across borders challenging[14].

C. International Legal Frameworks for Cybercrime & Cyber Forensics

Key international frameworks include:

- **Budapest Convention on Cybercrime (2001) -** the first international treaty on crimes committed via the Internet and other computer networks.
- **UNCITRAL Model Law on Electronic Commerce (1996) -** offers guidance on legal issues related to using electronic commerce.
- **ISO/IEC 27037:2012 -** provides guidelines for identifying, collecting, acquiring & preserving digital evidence[15].

D. Case Laws and Precedents in Cyber Forensics

[12] Information Technology Act, No. 21 of 2000, § 2(t), India Code (2000).

[13] Information Technology Act, No. 21 of 2000, § 4, Acts of Parliament, 2000 (India).

[14] Admissibility of Digital Evidence - Digital Forensics | Intelligence | Surveillance | Pelorus Technologies, Digital Forensics | Intelligence | Surveillance | Pelorus Technologies (2022), https://www.pelorus.in/admissibility-of-digital-evidence/ (last visited Aug 27, 2024).

[15] United Nations Office on Drugs and Crime, **Electronic Evidence: Collection, Handling, Preservation, and Presentation in Court**, at [59], https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Side%20events/RF_Electronic_Evidence_Book_2024_AHC.pdf (2024).

- **State (NCT of Delhi) v. Navjot Sandhu (2005)**[16] - confirmed the admissibility of electronic evidence under Section 65B.
- **Anvar P.V. v. P.K. Basheer (2014)**[17] - set strict conditions for admitting electronic evidence.
- **Shafhi Mohammad v. State of Himachal Pradesh (2018)**[18] - relaxed conditions for proving electronic evidence in some cases.

Cyber forensics is a crucial field in the investigation of cybercrimes. It focuses on the collection, preservation, analysis & presentation of digital evidence.

VII. TYPES OF CYBER FORENSICS

A. Computer Forensics: Investigating Computers and Storage Devices

Computer forensics involves examining computers and storage devices to uncover data linked to criminal activities. This includes desktop computers, laptops, external hard drives, USB drives, and other digital storage forms[19].

a) Key Processes

- **Data Acquisition:** The first step is creating a bit-by-bit image of the storage device to keep the original data unaltered. This maintains evidence integrity.
- **Data Analysis:** Investigators use special software tools to analyze data, searching for relevant files, deleted items & hidden information. This might involve recovering deleted files, examining file metadata & analysing system logs.
- **Reporting:** The findings are documented in a detailed report that may be presented in court. The report clearly outlines the methods used & conclusions drawn from the analysis.

[16] *State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India).* (2005).

[17] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India)

[18] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 S.C.C. 801 (India).

[19] National University, *What is Computer Forensics?*, National University (2023), https://www.nu.edu/blog/what-is-computer-forensics/ (last visited Aug 27, 2024).

b) Challenges

- **Encryption:** Many devices are protected by encryption, complicating data recovery efforts.
- **Volume of Data:** The sheer amount of data stored on modern devices can make analysis time-consuming and complex.

B. Network Forensics: Analysing Network Traffic and Protocols

a) Definition and Scope: Network forensics focuses on monitoring & analysing network traffic to identify suspicious activities. This type of forensics is essential for understanding how cybercrimes are executed over networks[20].

b) **Key Processes**

- **Traffic Capture:** Network forensics begins with capturing data packets traveling over the network using tools like Wireshark or tcpdump. This allows investigators to analyze real-time or recorded network traffic.
- **Protocol Analysis:** Investigators analyze various network protocols (e.g., TCP/IP, HTTP, FTP) to identify anomalies or malicious activities. This includes examining headers, payloads & session information.
- **Event Correlation:** By correlating network events with other logs (like firewall logs & intrusion detection system alerts), investigators build a comprehensive picture of the incident. Example: **Failed Login Attempts**: Imagine a user account showing lots of failed login tries (say, 100 unsuccessful attempts). Then, there's one successful login from the same IP address. This pattern can set off an alert. Investigators would link these events to spot a potential brute-force attack. In such an attack, someone tries to break into the account

[20] GeeksforGeeks, *Types of Computer Forensics*, GeeksforGeeks (2024), https://www.geeksforgeeks.org/types-of-computer-forensics/ (last visited Aug 27, 2024).

without permission[21]. **Firewall and IDS Alerts**: Consider when a firewall logs many blocked connections from one specific IP address, and at the same time, an intrusion detection system (IDS) flags suspicious activities coming from that same IP. By correlating these events, investigators can see a possible coordinated attack. This helps in understanding the threat landscape more deeply[22]. **Device Overheating and Network Failures**: Picture a network monitoring tool that finds a device isn't responding. Shortly after, it logs that both internal & external temperatures of the device are very high. By linking these logs, it might be concluded that the device shut down due to overheating. This is crucial for timely incident response[23].

c) **Challenges**

- **Volume of Data:** Similar to computer forensics, the volume of network traffic can be overwhelming, making it hard to pinpoint relevant evidence.
- **Encryption and Obfuscation:** The increasing use of encryption & obfuscation techniques can hinder traffic analysis effectively.

C. Mobile Device Forensics: Extracting Data from Smartphones and Tablets

Mobile device forensics involves recovering & analysing data from mobile devices like smartphones and tablets. Given the prevalence of mobile technology today, this area has gained significant importance[24].

a) **Key Processes**

[21] ManageEngine, communications@manageengine.com (2022). *ManageEngine Log360*. [online] ManageEngine Log360. Available at: https://www.manageengine.com/log-management/siem/static-dynamic-event-correlation.html [Accessed 7 Sep. 2024].

[22] Splunk. (2024). *IT Event Correlation: Software, Techniques and Benefits | Splunk*. [online] Available at: https://www.splunk.com/en_us/blog/learn/it-event-correlation.html [Accessed 7 Sep. 2024].

[23]Tushar Panhalkar (2020). *Summarize the Event Correlation | Infosavvy Security and IT Management Training*. [online] Infosavvy Security and IT Management Training. Available at: https://info-savvy.com/summarize-the-event-correlation/ [Accessed 7 Sep. 2024].

[24] Digital forensics, Open Learning (2024), https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3 (last visited Aug 27, 2024).

- **Data Extraction:** Techniques vary based on the device's operating system (iOS, Android) & security features. Methods include logical extraction (accessing data through the OS) and physical extraction (creating a complete image of the device).
- **Data Analysis:** Investigators analyze call logs, messages, emails, application data & location information to uncover relevant evidence.
- **Reporting:** Findings are compiled in a report that outlines methods used and recovered evidence.

b) **Challenges**

- **Device Security:** Many mobile devices have robust security features including biometric locks and encryption which complicate data extraction.
- **App Data:** The proliferation of applications leads to fragmented data storage making it challenging to recover and analyze information effectively.

D. Cloud Forensics: Challenges in Investigating Cloud-based Evidence

Cloud forensics involves investigating data stored in cloud environments. With more organizations migrating to cloud services understanding how to handle cloud-based evidence becomes critical.

a) **Key Processes**

- **Data Identification:** Investigators must identify which cloud services were used and what data is relevant.
- **Data Acquisition:** Acquiring data from cloud providers can be challenging often requiring legal permissions and cooperation from providers.
- **Data Analysis:** Once obtained forensic analysts examine the data for relevant evidence like user activity logs file access records & communications.

b) Challenges

- **Jurisdictional Issues:** Cloud data may be stored across different jurisdictions complicating legal processes & access.
- **Provider Cooperation:** Investigators rely on cloud service providers for access leading to delays particularly if providers have strict privacy policies.

E. Challenges by Cloud Service Model

a) Infrastructure as a Service (IaaS)

IaaS offers virtualized computing resources on the internet, making forensic investigations tricky due to several factors.

- **Multi-tenancy**: Lots of clients share the same physical resources. This sharing makes it tough to pinpoint and identify specific data for an investigation. Plus, it can lead to privacy problems and challenges in keeping evidence intact[25].
- **Dynamic environments**: Virtual machines (VMs) are temporary and can change quickly. Data can be there one moment and gone the next. Investigators might find it hard to grab relevant data before it gets deleted or changed[26].

b) Platform as a Service (PaaS)

PaaS lets users build and launch applications without handling the underlying infrastructure. The forensic challenges here include:

[25] Kumar Yadav #1, A. and Dwivedi, S. (n.d.). *Cloud Forensic as a Service: Tools, Challenges, and Opportunities*. [online] Available at: https://www.ijcsit.com/~ijcsitco/docs/volume13/vol13issue06/ijcsit2022130603.pdf [Accessed 7 Sep. 2024].

[26] Cloud Forensics challenges in this Digital Era. (n.d.). Available at: https://ciicdt.com/dx/pdf/Cloud_Forensics_challenges_in_this_Digital_Era.pdf [Accessed 7 Sep. 2024].

- **Limited access to logs**: While some PaaS providers create logs, getting access to these logs can be tough. This makes retrieving critical evidence tricky[27].
- **Dependency on third-party tools**: Investigators might have to rely on tools from the PaaS vendor. These tools may not be suited for forensic work, which limits how effective an investigation can be[28].

c) **Software as a Service (SaaS)**

SaaS provides software apps over the internet, creating both benefits and issues for forensic procedures:

- **Rich logging capabilities**: SaaS apps often keep extensive logs, which helps with investigations. However, accessing these logs is a challenge since the service provider controls them[29]
- **Data ownership and jurisdiction issues**: Where data is stored (often in different places) complicates legal cases. Different laws may apply to how data is retrieved and used[30].

Impact on the Forensic Process

Switching to cloud services requires changes in forensic methods:

- **Identification**: Investigators need to find the right cloud environments & resources involved in an incident. This task is complex because cloud services are distributed[31].

[27] Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I., **Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges**, 24 *Sensors* 433 (2024), https://doi.org/10.3390/s24020433.

[28] **Md.Y. Arafat, B. Mondal & S. Rani,** *Technical Challenges of Cloud Forensics and Suggested Solutions*, 8 **Int'l J. Sci. & Eng'g Res.** 1142 (2017), https://doi.org/10.14299/ijser.2017.08.004.

[29] Kumar Yadav, A. & S. Dwivedi, *Cloud Forensic as a Service: Tools, Challenges, and Opportunities*, 13 **Int'l J. Comp.Sci.&Info.Tech.**(n.d.),https://www.ijcsit.com/~ijcsitco/docs/volume13/vol13issue06/ijcsit2022130603.pdf.

[30]**Cloud Forensics Challenges in This Digital Era,** *CIICDT*, available at https://ciicdt.com/dx/pdf/Cloud_Forensics_challenges_in_this_Digital_Era.pdf (last visited Sept. 7, 2024).

[31] Md. Y. Arafat, B. Mondal & S. Rani, *Technical Challenges of Cloud Forensics and Suggested Solutions*, 8 Int'l J. Sci. & Eng'g Rsch. 1142 (2017), https://doi.org/10.14299/ijser.2017.08.004.

- **Preservation**: Keeping digital evidence intact is crucial. This involves capturing and storing data securely, which is hard in a multi-tenant environment where data might mix[32].
- **Examination and Analysis**: This stage needs specialized tools & techniques due to the unique nature of cloud data. Investigators must be skilled at working with cloud architectures & understanding how data flows to uncover vital evidence[33].
- **Presentation**: Forensic results must be easy to understand in legal settings. This task is tough given the technical nature of cloud computing and varying control levels over data[34].

VIII. CYBER FORENSICS TOOLS AND TECHNIQUES

A. Overview of Common Forensic Tools: Software & Hardware

Cyber forensics employs various specialized tools, categorized into software & hardware. These tools are essential for identifying, acquiring, and analysing digital evidence from multiple devices.

A. Software Tools:

- **The Sleuth Kit:** This is a bunch of command-line tools & a C library for analyzing disk images and recovering files. Often used with Autopsy.
- **FTK Imager:** Acts as a data preview and imaging software, allowing forensic investigators to assess electronic evidence promptly[35].

[32] Kumar Yadav #1, A. and Dwivedi, S. (n.d.). *Cloud Forensic as a Service: Tools, Challenges, and Opportunities*. [online] Available at: https://www.ijcsit.com/~ijcsitco/docs/volume13/vol13issue06/ijcsit2022130603.pdf.

[33] **Cloud Forensics Challenges in This Digital Era,** *CIICDT*, available at https://ciicdt.com/dx/pdf/Cloud_Forensics_challenges_in_this_Digital_Era.pdf (last visited Sept. 7, 2024).

[34] Ibid

[35] Dataexpert.eu. (2024). *Preview & Image Data with FTK Imager - DataExpert EN*. [online] Available at: https://www.dataexpert.eu/products/digital-forensics-exterro/ftk-imager/ [Accessed 8 Sep. 2024].

- **Xplico:** A network forensics analysis tool that recreates content from network traffic captured (by packet sniffers like Wireshark)[36] [37].
- **OS Forensics:** This tool digs deep into computers, finding all sorts of info, even unknown files.
- **Autopsy:** An open-source tool that reveals deleted files & raw data. It's widely used across investigative fields[38].

b) **Hardware Tools:**

Hardware tools usually help create forensic images of devices while keeping the original data intact. This includes write-blockers that prevent any modifications to the original media during imaging[39].

B. Data Acquisition: Imaging & Hashing

Data acquisition in cyber forensics means making exact copies of digital media to preserve evidence. This process includes:

- **Imaging:** Creating a bit-by-bit copy of the storage media ensures that the original data stays unchanged. Tools such as FTK Imager & OS Forensics are often used here.
- **Hashing:** A technique that produces a unique hash value for the copied data, serving as a digital fingerprint. This ensures the integrity of the data by letting investigators verify that the copied data matches the original[40].

C. Data Analysis: Techniques for Analysing Digital Evidence

[36] Xplico.org. (2021). *Xplico – About*. [online] Available at: https://www.xplico.org/about [Accessed 8 Sep. 2024].

[37] ForensicTools.dev. (2022). *Xplico*. [online] Available at: https://forensictools.dev/listing/xplico/ [Accessed 8 Sep. 2024].

[38] Sleuthkit.org. (2023). *The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools*. [online] Available at: https://www.sleuthkit.org/ [Accessed 8 Sep. 2024].

[39] Cyber Forensics - Methods & Techniques | Cyber Security Institute In Delhi, Craw Security (2021), https://www.craw.in/methods-techniques-of-cyber-forensics-best-cyber-security-institute-in-delhi/ (last visited Aug 27, 2024).

[40] Understanding Digital Forensics: Process, Techniques, and Tools, BlueVoyant (2024), https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools (last visited Aug 27, 2024).

Analysing data in cyber forensics involves diverse techniques to scrutinize acquired data for relevant evidence. Key techniques include:

- **Cross-Drive Analysis:** Correlating data across several drives to spot connections & anomalies, offering context for investigations.
- **Reverse Steganography:** Checking files for hidden data embedded using steganography methods. Reverse steganography is really important in data analysis, especially in cyber forensics because it helps find and take out hidden messages from digital stuff. It's basically the opposite of regular steganography, where info is hidden inside files like pictures or sound clips. In cyber forensics, reverse steganography helps find these hidden messages, often during investigations into bad activities or data leaks[41].
- **Deleted File Recovery:** Techniques like data carving enable forensic experts to recover fragments of deleted files from unallocated disk space.
- **Live Analysis:** Conducting analysis on a running system to capture volatile data from RAM, possibly providing insights into ongoing malicious activities[42].

D. Reporting and Documentation in Cyber Forensics

Thorough reporting and documentation are crucial in cyber forensics, ensuring findings are admissible in court.

- **Detailed Reporting:** Forensic investigators must craft detailed reports outlining the methods used, findings, & the significance of the collected evidence.

[41] Lee, H. and Lee, H.-W. (2019). Reverse Engineering-based Steganalys is of Crypto123 Tool for Automatic Detection and Extraction on Concealed Messages. *TEST Engineering & Management*, [online] 81, pp.399–411. Available at: http://testmagzine.biz/index.php/testmagzine/article/view/76 [Accessed 8 Sep. 2024].

[42] Shivanshu, *What Is Cyber Forensics?*, Intellipaat (2021), https://intellipaat.com/blog/what-is-cyber-forensics/ (last visited Aug 27, 2024).

- **Chain of Custody:** Maintaining clear records of who handled the evidence, when, and how it was stored is essential to preserving its integrity.
- **Presentation of Findings:** Reports might need presenting in court. Investigators must explain technical details understandably to non-experts[43].

IX. CYBER FORENSIC INVESTIGATIVE PROCESS

A. The Forensic Investigation Model: From Collection to Presentation

The digital forensic investigation process generally involves four main steps:

- **Collection:** This step entails acquiring digital evidence, often by seizing physical assets such as computers, hard drives, or phones. Ensuring that data is not lost or damaged during collection is critical. This requires copying storage media or creating images of the original.
- **Examination**: At this stage, relevant data must be identified and extracted. Whether working on a live system or a dead one, this involves preparing the data, extracting it, and pinpointing the pieces crucial to the investigation.
- **Analysis**: Here, the collected data is utilized to either substantiate or refute the case. Key inquiries include who created the data, when it was created, how it was created, and its relevance to the case. The objective is to piece together the fragments of data into a comprehensive narrative of events.
- **Reporting**: Finally, data and analysis are synthesized into a format understandable to laypeople. These reports are vital in conveying information to all stakeholders[44].

[43] What is Cyber Forensics? Tools, Technologies and Platform | Sangfor Technologies, Sangfor Technologies (2022), https://www.sangfor.com/blog/cybersecurity/what-cyber-forensics-tools-technologies-and-platform (last visited Aug 27, 2024).

[44] Understanding Digital Forensics: Process, Techniques, and Tools, BlueVoyant (2024), https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools (last visited Aug 27, 2024).

- **Documentation of investigation process:** Documenting every step in a forensic investigation is really important for several reasons. Mainly, it's about keeping the evidence honest, clear, & usable in court. This whole documentation process is a basic part of both digital and traditional forensics[45].

B. Incident Response: The First Step in Cyber Forensics

Incident response is fundamental in cyber forensics. Key steps include:

- **Assessing the Situation:** This involves analyzing the scope of the investigation & actions required. Notify decision-makers, review policies and laws, identify the investigation team, and prepare for evidence acquisition.
- **Acquiring the Data:** The next step involves gathering, protecting, & preserving original evidence. It includes building a computer investigation toolkit, collecting data securely storing & archiving it.
- **Analysing the Data:** Examine & correlate digital evidence with events of interest to build a strong case. Analyze network data, host data & storage media.
- **Reporting the Investigation:** Gather and organize collected information before writing the final report[46].

C. Preserving the Integrity of Digital Evidence

Maintaining the integrity of digital evidence is crucial for its admissibility in court. Essential practices include:

- Documenting steps taken to explain them to non-investigators later
- Maintaining chain of custody for evidence admissibility

[45] Mosse-institute.com. (2023). *Preparing Documentation and Evidence*. [online] Available at: https://library.mosse-institute.com/articles/2023/08/preparing-documentation-and-evidence.html [Accessed 8 Sep. 2024].

[46] Computer Forensics Investigation Process MODULE 2, https://www.cemca.org/ckfinder/userfiles/files/Module%2002%20Computer%20Forensics%20Investigation%20Process.pdf.

- Validating data accuracy using hash values (a unique fingerprint of a digital file)[47]

D. Case Management and Documentation

Effective case management & documentation are essential throughout the forensic process:

- Graphically representing directory structures storage media
- Creating a chronology of activities leading to misconduct such as data leaks or cyber espionage
- Documenting findings carefully to visualize the entire process & conclusions so investigators can explain technical details in an understandable manner to non-experts[48].

E. Applications of Cyber Forensics in Crime Investigation

Cyber forensics holds a crucial position in contemporary crime investigations. It addresses a plethora of criminal activities by analysing & retrieving digital evidence. This chapter delves into various applications of cyber forensics, including its role in cybercrime investigations, financial crimes, terrorism, and corporate probes.

X. APPLICATIONS OF CYBER FORENSICS IN CRIME INVESTIGATION

A. Cybercrime Investigations: Hacking, Phishing, and Fraud

Cyber forensics is indispensable when investigating cybercrime forms like hacking, phishing, and fraud. These crimes often exploit digital vulnerabilities. Thus, forensic experts need to scrutinize the digital traces left by offenders. Techniques such as file carving, data recovery, & network analysis are pivotal in

[47] CHAPTER 2 - THE FORENSIC INVESTIGATION PROCESS, Exterro (2024), https://www.exterro.com/basics-of-digital-forensics/chapter-2-the-forensic-investigation-process (last visited Aug 27, 2024).

[48] GeeksforGeeks, *Five Phases of Computer Forensics Investigation Procedure*, GeeksforGeeks (2024), https://www.geeksforgeeks.org/five-phases-of-computer-forensics-investigation-procedure/ (last visited Aug 27, 2024).

uncovering evidence and piecing together the crime's narrative. With cybercriminals becoming increasingly sophisticated, there is a need for advanced forensic tools & methods to trace and analyze their activities effectively. For instance (in phishing cases), experts can examine email headers & logs to pinpoint the attackers' source and techniques[49].

B. Digital Forensics in Financial Crimes: Tracing Money Laundering

In financial crime investigations, cyber forensics is vital for tracking money laundering activities. Analysts rely on digital evidence from banking transactions & online payment systems to trace illicit funds. Techniques like timeline analysis & data recovery are essential in mapping out the flow of money and identifying those involved. By integrating cyber forensics with financial crime probes, law enforcement can follow complex financial trails that often cross multiple jurisdictions. This makes building a case against culprits more manageable[50].

C. Cyber Forensics in Terrorism and National Security Cases

Cyber forensics also plays a critical role in terrorism and national security investigations. Experts analyze digital communications, social media interactions, and online behaviours to unmask networks planning or executing terrorist acts. This often involves examining metadata from communications to establish connections between suspects. The capability to quickly analyze vast data amounts is crucial in thwarting terrorist activities & ensuring national security. Cyber forensics helps agencies identify & neutralize threats before they materialize[51].

D. The Role of Cyber Forensics in Corporate Investigations

In corporate environments, cyber forensics is used to investigate internal frauds, data breaches & corporate espionage. Experts examine digital evidence from

[49] Legal Desire & Legal Desire, *Legal Desire Media and Insights*, Legal Desire Media and Insights (2020), https://legaldesire.com/digital-forensics-applications-and-challenges/ (last visited Aug 27, 2024).

[50] The Power of Cyber Forensics in Solving Crimes, Salvation DATA (2023), https://www.salvationdata.com/knowledge/cyber-forensics/ (last visited Aug 27, 2024).

[51] Shivanshu, *What Is Cyber Forensics?*, Intellipaat (2021), https://intellipaat.com/blog/what-is-cyber-forensics/ (last visited Aug 27, 2024).

company networks, employee devices & communication systems to uncover illicit actions. Techniques like malware analysis and network traffic scrutiny are frequently employed to identify breach sources and understand the damage extent[52]. The application of cyber forensics in corporate investigations aids not only in resolving incidents but also helps organizations bolster their cybersecurity measures against future breaches. By comprehending the techniques used by cybercriminals, firms can implement better security practices and training programs for employees. Cyber forensics allows organizations to carry out detailed reviews of their digital setups. By looking at logs, network traffic, & system settings, forensic experts can spot security weaknesses and potential areas of exploitation. This proactive stance helps companies shore up their defences before an attack takes place[53].

XI. CASE STUDIES IN CYBER FORENSICS

A. High-profile cybercrime cases

High-profile cybercrime cases shed light on the changing tactics and motivations of cybercriminals. By examining these incidents, cybersecurity experts & law enforcement can learn key lessons to improve their defence strategies and investigative methods. Recent notable cases offer several important insights:

a) Importance of Strong Security Measures

Cases like the MGM data breach and the UnitedHealth Group cyberattack emphasize the need for organizations to focus on cybersecurity. Using robust authentication, keeping software updated, & investing in proactive defences can greatly lower the risk of successful attacks[54].

[52] Sharma Urvashi & Mishra, *Application of Cyber Forensics in Crime Investigation*, International Journal of Research and Analytical Reviews 317 Assistant Professor in Computer Science, http://ijrar.com/upload_issue/ijrar_issue_1227.pdf.

[53] Salvation DATA. (2023). *The Power of Cyber Forensics in Solving Crimes*. [online] Available at: https://www.salvationdata.com/knowledge/cyber-forensics/ [Accessed 8 Sep. 2024].

[54] Jeremy Imlach, *Key Lessons from High-Profile Cybersecurity Breaches | FEITIAN Technologies US*, FEITIAN Technologies US (2024), https://ftsafe.us/key-lessons-from-high-profile-cybersecurity-breaches/ (last visited Aug 28, 2024).

b) Collaboration and Information Sharing

Effective cybersecurity requires collaboration and information sharing among peers, law enforcement, and security experts. The SolarWinds supply chain attack shows the benefit of collective defence against sophisticated threats[55].

c) Insider Threats and Social Engineering

Insider threats & social engineering remain significant vulnerabilities, as seen in the Twitter hack and Uber data breach. Teaching employees how to prevent phishing, enforcing strict access controls, and monitoring user activity are essential steps.

d) Continuous Improvement and Adaptation

The cybersecurity landscape is always changing. Organizations must adapt their tactics accordingly. The Optus breach illustrates why it's crucial for companies to maintain high security standards, continuously check their posture, & stay ahead of new threats. By learning from these high-profile cases and applying best practices, organizations can boost their resilience against cyber threats. This helps better protect critical assets & sensitive information[56].

B. Forensic Analysis in the Sony Pictures Hack

The 2014 Sony Pictures hack was a complex incident underlining the importance of cyber forensics in investigating & attributing attacks. North Korea-backed Lazarus Group stole sensitive data like unreleased films, employee info, and internal emails.

Forensic analysis was key in unravelling details of the attack and tracing it back to the perpetrators. Key aspects included:

- Analysing malware samples & network traffic to identify attack vectors.

[55] Consilien, Consilien | One Source | One Solution (2024), https://www.consilien.com/news/behind-the-scenes-of-a-cyber-attack-lessons-learned-from-real-life-security-breaches (last visited Aug 28, 2024).

[56] Top Cyberattacks of 2022: Lessons Learned, ISACA (2022), https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/top-cyberattacks-of-2022-lessons-learned (last visited Aug 28, 2024).

- Examining compromised systems to gather evidence & understand breach extent.
- Correlating data from sources like system logs & user accounts to build a full picture.
- Identifying digital footprints that ultimately led to North Korea's involvement.

The Sony hack showed the value of cyber forensics not only in investigating incidents but also providing evidence for attribution & legal action[57].

C. Investigating the Target Data Breach

The 2013 Target data breach exposed millions of customers' personal and financial information during the holiday shopping season. It underscored supply chain security's importance & need for solid incident response plans.

a) Forensic analysis in this case focused on:

- Identifying initial compromise point, traced to a third-party HVAC vendor.
- Analysing malware used by attackers to infiltrate systems.
- Examining network traffic & system logs to track attackers' movements.
- Identifying methods used by attackers to bypass security controls.

The investigation showed attackers were present in Target's network for months before detection—highlighting the need for continuous monitoring & threat detection[58].

D. The BTK Killer case

[57] Steinberg, S. and Stepan, A. (2021). *The Hacking of Sony Pictures: A Columbia University Case Study*. [online] Available at: https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf.

[58] Prevalent. (2024). *The 2013 Target Data Breach & Third-Party Risk Management | Prevalent*. [online] Available at:https://www.prevalent.net/blog/the-2013-target-data-breach-a-lasting-lesson-in-third-party-risk-management/ [Accessed 8 Sep. 2024].

The BTK Killer case involving Dennis Rader was notably resolved through advancements in cyber forensics. This marked a significant turning point in criminal investigations, which had previously relied heavily on traditional methods[59].

a) **Background of the Case**: The BTK Killer, known for "Bind, Torture, Kill," was responsible for at least ten murders in Kansas between 1974 & 1991. Rader taunted law enforcement and the media with letters detailing his crimes, contributing to his notoriety. After a long silence, he resurfaced in 2004, sending more letters that reignited interest in the case. These letters also provided critical digital evidence leading to his capture[60].

b) **Role of Cyber Forensics**: In 2005, the breakthrough came when Rader sent a floppy disk containing a Microsoft Word document to a local television station. This disk was pivotal because it had metadata that forensic analysts could exploit. The file was named "TestA.rtf," and its metadata revealed it had been saved by a user named "Dennis." This directly led investigators to Dennis Rader, who was the president of a local church. Using a software tool called EnCase (a popular choice in digital forensics), the team began their investigation. their surprise, they found a deleted Microsoft Word document on the disk. When a file is deleted, it's not immediately removed from the storage medium; instead, the space it occupies is marked as available for reuse until that space is overwritten by new data. The original file can often be recovered using the principle of data remains. Upon opening the recovered document, the team found metadata embedded in the file. Metadata is data about data; in this case, details about the creation of

[59] Nervous System: How Legal Tech Helped Catch the BTK Killer | Insights | Berkeley Research Group, Thinkbrg.com (2019), https://www.thinkbrg.com/insights/publications/nervous-system-how-legal-tech-helped-catch-the-btk-killer/ (last visited Aug 28, 2024).

[60] EclipseForensics, *3 Famous Cases Solved Through Digital Forensics - Eclipse Forensics*, Eclipse Forensics (2021), https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/ (last visited Aug 28, 2024).

the document. The metadata revealed that the document was last saved by a user named Dennis and was linked to a Lutheran Church. This breakthrough led investigators to tie Dennis Rader to the BTK crimes. Rader was arrested in February 2005 & confessed to all the BTK killings[61].

F. Key Forensic Techniques Used

a) **Metadata Analysis:** The forensic examination of the disk's metadata was crucial. It identified the user who saved the document, linking it directly to Rader. This marked a significant shift from traditional forensic methods that had failed to identify him over the decades.

b) **DNA Evidence:** Besides digital evidence, DNA analysis plays an essential role. Investigators had previously collected DNA from crime scenes. Once they identified Rader as a suspect, they matched his daughter's DNA with evidence collected from one of the victims, confirming his involvement[62].

c) **Surveillance Footage:** Rader's communications included drop-off points captured on surveillance cameras. This footage provided additional context for his movements and further corroborated evidence against him. In short, advancements in cyber forensics proved crucial in solving this notorious case. Through metadata analysis and DNA evidence —combined with surveillance footage—law enforcement was able to bring Dennis Rader to justice effectively.[63]

G. Digital Forensics Helped Catch the 'Craigslist Killer'

In 2009, Philip Markoff, a 23-year-old medical student gained notoriety as the "Craigslist Killer" following charges for the murder of Julissa Brisman in a Boston

[61] Forensics Colleges. (2024). *How Digital Forensics Caught the BTK Strangler - Case Study & Programs*. [online] Available at: https://www.forensicscolleges.com/blog/forensics-casefile-btk-strangler [Accessed 8 Sep. 2024].

[62] EclipseForensics, *The Gripping Case of the BTK Killer & the Role of Digital Forensics - Eclipse Forensics*, Eclipse Forensics (2021), https://eclipseforensics.com/the-gripping-case-of-the-btk-killer-the-role-of-digital-forensics/ (last visited Aug 28, 2024).

[63] How Digital Forensics Caught the BTK Strangler - Case Study & Programs, Forensics Colleges (2024), https://www.forensicscolleges.com/blog/forensics-casefile-btk-strangler (last visited Aug 28, 2024).

hotel. Brisman had advertised her services as a masseuse on Craigslist, and Markoff arranged an appointment with her under the alias "Andy M." When officers responded to Brisman's murder, they uncovered limited evidence at the scene: her body, traces of blood, a spent bullet casing & her cell phone and identification. Despite this, investigators pieced together a series of digital clues that led them to Markoff: Brisman's friend Beth informed the police that she had organized appointments for Brisman via Craigslist ads. Beth provided the phone number and email address used by Brisman's killer. The phone numbers were linked to two prepaid, disposable phones bought at a local store. The email account had been created shortly before the incident. Police traced the IP address associated with the email account to Markoff's home address in Quincy, Massachusetts. Surveillance footage from the hotel captured a man in a black leather jacket and Yankees cap entering and leaving around the time of the murder. Another victim identified this man as her attacker in a separate robbery. The authorities found Craigslist ads for both Brisman and the other victim. They traced the phone numbers and email accounts used for communication back to Markoff. Without the digital forensic evidence from phone numbers, email accounts, IP addresses & surveillance footage, identifying Markoff as the perpetrator may have been impossible. This case highlights how crucial digital clues are in solving contemporary crimes.

H. Case of Janie Lynn Ridd

The case involving **Janie Lynn Ridd** and her former roommate Rachel is about shocking betrayal. Ridd attempted to poison Rachel using a dangerous strain of bacteria purchased from the dark web.

I. Background of the Case

Rachel and Janie Lynn Ridd had maintained a long-standing friendship which evolved into a living arrangement after Rachel's health issues forced her to leave her job as a paramedic. Over the years, Ridd assumed a caregiver role, which gradually became manipulative & abusive. Rachel began experiencing mysterious health problems, including severe infections. These ailments puzzled her doctors, who couldn’t explain them. This led to suspicions about Ridd's intentions, especially after Rachel overheard Ridd discussing methods to harm someone[64].

J. FBI Intercepts Dark Web Package and Convicts Janie Lynn Ridd

The FBI became involved in the case of Jan Lynn Ridd after intercepting a package that contained Vancomycin-resistant Staphylococcus aureus (VRSA), a highly dangerous bacteria. Ridd had ordered this bacteria online from the dark web. She had falsely claimed to be a biology teacher needing the bacteria for a science experiment. However, the FBI's investigation revealed her actual intention was to harm her former roommate, Rachel. Rachel was already vulnerable due to existing health issues. During their investigation, it was discovered that Ridd had also purchased insulin from the dark web. This raised further alarms about her plans to incapacitate Rachel. Ridd's actions were meticulously planned. They involved sedating Rachel with various medications before injecting her with harmful substances.

In June 2020, Ridd pleaded guilty to several charges including aggravated abuse of a vulnerable adult & possession of a biological agent. She was sentenced to serve between one & 20 years in prison. The FBI's ability to intercept dark web packages and track down criminals like Ridd has significantly improved. This progress is due to enhanced information sharing among law enforcement agencies, which has sharpened their technical capabilities. These capabilities include taking down major illicit marketplaces and regulating the transfer of cryptocurrency transactions[65]. Moreover, law enforcement agencies have employed hacking techniques to unmask suspects' devices and locations, even if they use anonymizing software like Tor[66].

[64] Paul Nelson & Annie Knox, *Utah woman goes to prison for buying bacteria to infect roommate already in poor health*, Deseret News (2020), https://www.deseret.com/utah/2020/8/26/21402717/utah-woman-sentenced-prison-buying-bacteria-to-infect-roommate-vrsa/ (last visited Aug 28, 2024).

[65] Gemma Davies, *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers - Gemma Davies, 2020*, The Journal of Criminal Law (2020), https://journals.sagepub.com/doi/full/10.1177/0022018320952557 (last visited Aug 28, 2024).

[66] Dan Froomkin, *FBI Director Claims Tor and the “Dark Web” Won’t Let Criminals Hide From His Agents*, The Intercept (2015), https://theintercept.com/2015/09/10/comey-asserts-tors-dark-web-longer-dark-fbi/ (last visited Aug 28, 2024).

XII. SUGGESTION

- Legislation of effective laws, with regular amendments to keep up with dynamic development of digital products.
- Introduction of alarming mechanism, upon lingering of suspicious activity by internet users online.
- Infiltration of police in dark web to monitor and act swiftly any activity that might have penal effects.
- Bringing of new cyber surveillance that is well suited to deal with transnational cyber suspicious activities.
- Giving training and seminar to police force and enforcement department to use technology and preservation of digital evidence.

XIII. CONCLUSION

A. Ethical Considerations & the Future of Digital Privacy

Balancing Privacy and Security: As digital forensics evolves, there's an ongoing need to balance individual privacy rights with the requirements of law enforcement & national security. Ethical guidelines and legal frameworks will need to adapt, addressing emerging privacy concerns like the collection and storage of biometric data[67].

Addressing Cybercrime and Protecting Vulnerable Groups: Cybercrime will continue to evolve—targeting individuals, businesses, and critical infrastructure[68]. Protecting vulnerable groups such as children and the elderly from online exploitation & fraud will remain a priority. Forensic techniques must adapt to identify and prosecute these crimes.

[67] Gunjan Chaudhary, *The Future of Forensic Science: What to Expect in the Coming Years*, Lifs.co.in (2024), https://lifs.co.in/blog/future-of-forensic-science.html (last visited Aug 28, 2024).

[68] Future Cybersecurity Trends and Predictions for India [2024], Craw Security (2024), https://www.craw.in/future-cybersecurity-trends-and-predictions-for-india/ (last visited Aug 28, 2024).

Promoting Diversity and Inclusion in the Forensic Community: Fostering diversity & inclusion in the forensic community is crucial for ensuring the field reflects the diverse society it serves. Promoting educational opportunities, mentorship programs, and inclusive hiring practices will help attract and retain a talented and diverse workforce.

Maintaining Professionalism and Ethical Standards: Upholding professional & ethical standards is paramount for the future of digital forensics. Forensic experts must adhere to strict protocols, maintain impartiality, and ensure the integrity of evidence. Ongoing training & certification will help maintain high standards & public trust in this evolving field. Cyber forensic experts face a bunch of ethical dilemmas in their line of work. They're tasked with looking at sensitive evidence to help with legal investigations. Here are some big ethical considerations they have to think about: Cyber forensic experts see a ton of private info during their investigations. They gotta balance respecting people's privacy rights with getting access to crucial evidence. Having strict rules around storage & encryption of sensitive data is key. Investigative procedures need to follow proper consent & authorization. Getting into devices or data without permission, even for justice, can lead to ethical problems. Experts need to make sure they've got all the right legal permissions before starting any investigation. Cyber forensic experts must stay totally objective and unbiased when checking out digital evidence. They can't let personal opinions mess up their scientific methods or findings. Sticking to rules set by groups like ISO or NIST helps them stay objective[69].

B. Conclusion

Cyber forensics now stands as a crucial of modern crime investigation. It brings robust methods & tools to uncover digital evidence, helping resolve complex cases. Our growing dependence on digital technology in daily life has opened new paths for criminal behaviour. This demands a proactive, sophisticated approach to handle digital evidence. Cyber forensics offers a vital link between digital actions

[69] EclipseForensics (2023). *Digital Forensics: Ethical Dilemmas and Considerations - Eclipse Forensics*. [online] Eclipse Forensics. Available at: https://eclipseforensics.com/digital-forensics-ethical-dilemmas-and-considerations/ [Accessed 8 Sep. 2024].

& legal responsibility, ensuring that crimes in cyberspace don't go unpunished. Beyond the courtroom, the impact of cyber forensics reaches into wider realms like cybersecurity and digital governance. By pinpointing vulnerabilities targeted by cybercriminals, forensic investigations aid in formulating stronger cybersecurity protocols and preventive actions. Furthermore, the field emphasizes following legal & ethical standards. This underscores its role in balancing the quest for justice with safeguarding individual rights and privacy. Yet, cyber forensics faces limitations too. The rapid technological changes pose ongoing challenges, making it essential for forensic experts to stay updated with new tools, techniques, and threats. Also, tackling international cybercrime complexities requires better cooperation & harmonization of legal standards across borders for effective prosecution. The evolving nature of digital evidence—including encrypted communications and anonymization tech—poses significant hurdles that need conquering through innovation & research. Looking ahead, the future of cyber forensics will likely see more integration of AI, machine learning & advanced data analytics to automate and refine the investigative processes. These advancements could slash the time and resources needed for digital investigations, making cyber forensics more accessible and efficient. Moreover, developing standardized protocols & best practices will be key to ensuring forensic results are consistent and reliable. Overall, cyber forensics' role in crime investigation is indispensable—it's a cornerstone of efforts to fight digital crime and uphold law in our increasingly digital world.