Survey and compare the use of software and hardware tools in cybercrime investigations.

Syed Abdussami - 40185178, Tushar verma - 40221863, Darshan Malaviya - 40203241, Himanshu Mahajan - 40193970, Vraj patel - 40222248, Akash Rawat - 40197990, Rutvik Nilesh Doctor - 40224532, Vishwa Chokshi - 40204702 , Jay J Patel - 40218722, Jaimin Tejani - 40198405, Dhwanil Dixesh Patel - 40220874, Sushant padmanabhi - 40194604

Concordia Institute for Information Systems Engineering (CIISE), Information Systems Security (MEng)

***Abstract* – Cybercrime investigations are essential for detecting attackers and trends for upcoming defence methods because of the rise in cyberattacks brought on by the growth of Internet Technology (IT) and the Internet of Things (IoT). This study covers the use of hardware and software solutions for data extraction, recovery, encryption, and analytical purposes in cybercrime investigations. We examine well-known tools like Wireshark, IDA Pro, and EnCase. The research also explores growing trends, difficulties, and ethical and legal issues, and it offers suggestions for the future. To increase the effectiveness of cybercrime investigations in the face of increasing threats, it is essential to comprehend the advantages and limitations of these instruments.**

***Index Terms* – Cyber attacks, Cybercrime investigations, Forensic tools, Data extraction, Software tools, Memory forensics, Legal considerations.**

I. Introduction

The incidences and risks of cyber attacks have increased along with the use of Internet technology (IT) and the Internet of Things (IoT). However, it is very challenging to stop zero-day assaults. Cybercrime investigation is required to identify the attack and the attacker. Investigations into cybercrime aid in identifying trends for potential attacks and developing plans for a defence reaction. Investigation, analysis, and recovery of crucial forensic digital material from the attacked networks are all steps in a cybercrime investigation.[1]

For this, a variety of forensic tools that fall under the categories of hardware and software tools can be used. Data extraction, data recovery, data encryption, metadata analysis, data carving, link analysis, and virus analysis are the key functions offered by hardware tools.

Digital forensic, network forensic, virus analysis, memory forensic, log analysis, incident response, open source intelligence (OSINT), data recovery, encryption-decryption, and steganography techniques are supported by a variety of software tools. We examined a number of tools for the survey, including EnCase, IDA Pro, Wireshark, etc.

Criminal justice, national security, and private security organisations handle the majority of the cybercrime investigation. Further themes covered in the paper include a comparison of software and hardware tools, legal and ethical issues, new trends and problems, and recommendations for the future.

II. Literature Review

Due to the increase in cybercrime, a wide range of software and hardware solutions have been developed to help law enforcement, cybersecurity

professionals, and digital forensics experts conduct complete and efficient investigations. In this literature study, we emphasise the functionality, advantages, and disadvantages of the existing software and hardware technologies used in cybercrime investigations.

A. Software tools for Digital forensics

Digital forensic software tools play a pivotal role in the gathering, examination, and safeguarding of digital evidence sourced from diverse devices and origins. Numerous notable tools have arisen within this domain:

1. EnCase Forensic: EnCase Forensic is a digital forensic platform created by OpenText to assist law enforcement officials in gathering, preserving, and decrypting important data and evidence from a wide range of devices. With the use of this solution, evidence that has been hidden, deleted, or changed can now be discovered from a variety of sources, including PCs, social media platforms, cloud services, and IoT/mobile devices.[2] By merging AI-driven workflows and picture analysis, EnCase Forensic goes above and beyond, speeding investigations through clever automation.

2. AccessData provides the Forensic ToolKit (FTK), a user-friendly forensic software solution with a straightforward one-touch interface that is both affordable and accessible. AccessData has established the ACE certification based on this software, and the most recent FTK version is much more user-friendly. FTK has a setup for automated complex searches, which streamlines the procedure. As an illustration, pressing the Email button immediately fetches emails. When necessary, investigators can maintain control while the FTK report generator effectively provides meaningful reports within the software.[3]

3. Autopsy is a user-friendly, open-source tool for digital forensics that is available for free. It makes using several open-source tools from The Sleuth Kit easier. Law enforcement, military, and business analysts can use this software to help them investigate incidents involving computers.[4] Users can look over and highlight important information from forensic searches on computer volumes. The tool is largely maintained by Basis Technology Corp. in cooperation with neighbourhood programmers.

B. Hardware tools for Digital Forensics

Unlike computer forensic software, which focuses on extracting data logically and within a specific timeframe, forensic hardware is mainly utilized to physically connect a computer's components and retrieve data for utilization with forensic software.

1. FRED: A powerful workstation for safely managing, storing, and analyzing data from hard disks and other media is called FRED, or Forensic Recovery of Evidence Device. These workstations are renowned for their excellent quality and scalability. FREDs frequently work in addition to forensic programs like EnCase and FTK. The only forensic workstations having integrated capabilities like hardware write blockers for IDE, SATA, and SAS drives, as well as USB3, Firewire, and MultiMedia/Memory Card forensic write blockers, are FRED systems. [5]

2. Logicube: With speeds of up to 4 gigabytes per minute, Logicube offers incredibly quick disk-to-disk and disk-to-image transfer solutions, significantly reducing the amount of time needed for data capture. Their data capture technology provides real-time integrity checks in addition to safely retrieving data from a target media to guarantee a trustworthy forensic copy.[3] These devices are adaptable, have a variety of interfaces, and frequently come with a handy portable field kit setup.

3. Write Blockers: Write blockers, such those provided by Tableau and WiebeTech, stop data from being altered while digital evidence is being

acquired. While collecting evidence from multiple storage devices, they maintain data integrity.[6]

The continual development of software and hardware solutions has tremendously aided the field of cybercrime investigation. These tools, which range from digital forensics and network analysis software to specialised malware analysis and hardware imaging devices, have allowed investigators to find evidence, track down crooks, and create solid legal cases. However, as cybercriminals' strategies improve, so must these technologies to ensure the success of cybercrime investigation operations. To address growing difficulties and improve the capabilities of these technologies, more research and development are required. and make a change.

III. Software Tools and Cyber Crime Investigation.

Software tools are used in cybercrime investigations to collect and analyse evidence, trace suspect activity, and monitor network traffic. Forensic toolkits for data retrieval, network analyzers for detecting malicious activity, and encryption applications for decrypting files are all important tools. These tools are critical in supporting cybercrime investigators in an efficient and successful manner.[8]The ongoing fight against cybercrime is being fueled by its exponential expansion, making the use of software tools critical for conducting thorough investigations and identifying perpetrators. Our research examines the most popular software packages utilised in cybercrime investigations.

A. Digital Forensics Software:

1. Autopsy is an open-source digital forensics programme used by law enforcement and cybersecurity experts to locate cybercrime evidence, recover deleted files, and analyse email data.[8]Also its Sleuth Kit integration for low level file system analysis.

2. FTK (Forensic Toolkit): AccessData commercial programme noted for speedy and effective data processing, comprehensive search features, and compatibility with a variety of file types.[8]Integrated SQLite database for storing metadata.

3. EnCase: Guidance Software (now part of OpenText) industry-standard commercial software that securely gathers data from digital devices such as PCs, smartphones, and cloud storage while preserving evidence integrity for admission in court.[7] Proprietary file system access and decryption capabilities

4. Sleuth Kit: An open-source forensic toolkit that includes command-line apps for disc and file analysis, enabling for in-depth investigations and the recovery of deleted or concealed files.[7] Open-source library for disk and file system analysis.

B. Network Forensics Software:

1. Wireshark: An open-source network protocol analyzer commonly used for real-time network traffic monitoring and analysis, allowing the detection of suspicious activities and potential security breaches.[9]Libpcap for packet capture and protocol dissection.

2. NetworkMiner: A passive network sniffer and packet analysis programme that specialises in obtaining Open Source Intelligence (OSINT) by extracting images, documents, and executable files exchanged over the network,[9] assisting investigators in identifying cybercriminals' domain names, hostnames, and open ports. Parses PCAP files to extract files and metadata.

C. Malware Analysis Tools:

In order to detect the nature of cyber risks and create efficient mitigation methods, investigators need to be able to understand the behavior and

features of malicious software. Here are a few noteworthy malware detection tools:

1. IDA Pro: Reverse engineers and malware analysts frequently utilize the acclaimed disassembler and debugger IDA Pro to analyze binary files. Experts may examine the inner workings of malware and find potential vulnerabilities thanks to its interactive and user-friendly interface. [11]Investigators can create efficient defenses and contribute to the development of antivirus signatures by comprehending the behavior and programming of malicious software. Interactive disassembler with various processor support.

2. Cuckoo Sandbox: An open-source malware analysis tool called Cuckoo Sandbox was created to automate the examination of dubious files and URLs in a secure setting. Cuckoo Sandbox creates thorough reports on the behaviors of the malware by tracking network activity and watching malware behavior.[11] Investigators can swiftly determine the type of danger and assess its effect on the system thanks to this important tool. Automated malware analysis using virtualization.

D. Memory Forensics Tools:

When used to examine a system's volatile memory, memory forensics tools are important for giving investigators information about active programs, open network connections, and hidden malware. The following are well-known memory forensics tools:[13]

1. Volatility: Investigators can extract useful information from the volatile memory of operating systems using the potent open-source memory forensics toolkit Volatility. Traditional disk-based forensics might not be able to capture all of the evidence, but Volatility can examine RAM dumps to find hidden malware, network connections, and running programs. Volatility is an essential technique in contemporary investigations because memory forensics frequently provides crucial insights into the runtime behavior of cyber threats.[13]Memory analysis using plugins for different OSes.

2. Rekall: The well-known memory analysis program Rekall, formerly known as Volatility Framework 2, is another one. It provides a wide range of tools and plugins to examine memory dumps and find pertinent artifacts for further research.[13] Rekall's flexible nature enables researchers to create unique plugins for specific use cases, giving them the freedom to efficiently address a variety of cybercrime scenarios.Memory analysis framework with Windows support.

E. Log Analysis Tools:

Investigators can combine records, spot patterns, and quickly spot security vulnerabilities thanks to the ELK Stack (Elasticsearch, Logstash, and Kibana), three robust open-source solutions for organising and analysing enormous volumes of log data.[12]

1. Splunk: The best commercial product for log management and analysis, including real-time log monitoring, extensive search tools, data visualisation, and machine learning capabilities for proactive threat hunting.[12]

F. Incident Response Platforms:

IBM Resilient: Centralized platform streamlining incident response with automated activities, effective communication between teams, and playbook-driven methodology to reduce cyber threat impact.[10]

1. RSA NetWitness: Advanced platform combining analytics, network, and endpoint visibility to identify and investigate sophisticated threats, facilitating proactive threat hunting and rapid response.

2. Palo Alto Networks Cortex XSOAR: Comprehensive SOAR platform enhancing

communication between security teams, automating repetitive tasks, and accelerating incident response through integration with various security technologies, standardized playbooks, and thorough case management.[10]

G. Tools for encryption and decryption:

1. VeraCrypt is an open-source disc encryption programme that uses strong encryption methods like AES and Twofish to protect sensitive data and ensure the safe retention of evidence during cybercrime investigations.[12]

2. BitLocker: A full-disk encryption technology built into the Windows operating system that makes it simple to encrypt entire drives in order to safeguard data from unauthorised access.[12] This system is crucial for protecting forensic photos and evidence during criminal investigations.

H. Open Source Intelligence (OSINT) Tools: Using OSINT techniques, investigators can learn a lot from readily available sources, which also aids in the discovery of leads and an understanding of cyberthreats. Several OSINT tools that are widely used in cybercrime investigations are listed below:

1. Maltego: Maltego is a powerful OSINT tool that makes it simpler to collect and analyse information on individuals, groups, and connections.[3] It gives investigators access to a graphical user interface that makes it feasible for them to see data and relationships, facilitating in the identification of potential hazards and cybercriminal networks.[9]

2. theHarvester: Data is gathered from a number of open sources, such as search engines, social media platforms, and DNS databases, using the command-line OSINT application theHarvester.[9] Investigators may employ theHarvester during reconnaissance to obtain important data that could result in beneficial leads.

I. Data Recovery Tools:
Data recovery solutions are essential for helping investigators recover lost or destroyed data from storage media during cybercrime investigations. These tools are necessary for recovering important evidence that may have been erased unintentionally or on purpose. Some popular data recovery tools are listed below:[9]

1. Recuva: Recuva is an intuitive data recovery program that helps with the recovery of deleted files from storage media, such as hard discs, memory cards, and USB devices.[8] Recuva can be used to recover crucial evidence that may have been unintentionally or maliciously erased during a cybercrime investigation.

2. TestDisk: A strong data recovery tool called TestDisk is renowned for its capacity to restore missing partitions and fix damaged boot sectors. TestDisk is a useful tool for retrieving evidence since it allows investigators to recover deleted or lost data from a variety of file systems.[9]

J. Tools for steganography

1. Stegsolve is a Java-based tool that enables users to find and extract hidden information from images while also offering numerous visualisation techniques, such as colour inversion and bit plane slicing, for analysing image data.[10]

2. StegDetect is a command-line steganography detection tool that can identify steganography signs and find hidden data in images, alerting investigators to the possibility of such material for further examination.[10]

IV. Hardware Tools for Cyber Crime Investigation

There is a case to be made for the adoption of some sophisticated tools that complement their software counterparts as cybercriminals sharpen their evasion techniques and investigators find it

more challenging to manoeuvre the delicate yet complicated domain of safely extracting digital pieces of evidence from the suspect's devices while also maintaining data integrity and ensuring the original data is unharmed.[15]

All throughout the chain, from extraction to validation to analysis, these technologies are used, and they are a huge help to law enforcement agencies all around the world. We provide a few illustrations of these gadgets, categorised by use case and application area.

A. Evidence and Data Acquisition:
This is the first of many steps in an investigation. Officers proceed to gather and document all devices and things deemed essential to the investigation after obtaining a search warrant.[14] Second, the investigative team should include experts who have expertise in recovering any vital information from the suspect's devices without contaminating them. In order to obtain a complete snapshot of the condition of the suspects' computers, they use a variety of technologies, including Write Blockers, Disk Imagers, Mobile Device extraction, and Network Forensic Devices.

With write blocking enabled, forensic imaging tools can readily gather a bit-by-bit copy of memory storage, hard disks, SSD, CPU registers, caches, etc, and all metadata associated with files. Furthermore, all network traffic is captured and collected, including IP packets, headers, and browser history.[14] To make the task at hand easier, it is critical to plan out and quantify the scope of the gathering phase.

B. Validation:
After securely gathering all necessary data for the inquiry, it is vital to validate the data. This is usually done with custom/proprietary software, but there are some tools at our disposal to assess and methodically validate the data. To eliminate inconsistencies, the hashes of recorded forensic data are compared to the original data. This is vital for ensuring the integrity and validity of digital evidence obtained by ensuring that the data has not been altered or tampered with during the investigation process.[14] Some famous examples of such machines are

1. Tableau TX1 Forensic Imager: This hardware tool features built-in hashing and validation capabilities, allowing investigators to calculate and verify hash values of acquired images. Its user-friendly interface and reliable performance make it a preferred tool for ensuring evidence integrity.[14]

2. CRU WiebeTech UltraDock v5: This hardware tool offers hardware-based write blocking and hash calculation features. It ensures that evidence remains unaltered during acquisition and allows for subsequent validation.[14]

3. Cellebrite UFED Touch: While primarily known for mobile device forensics, Cellebrite's UFED Touch can also perform evidence validation by calculating hash values of acquired data and verifying their integrity.[14] Physical extraction using custom cables and adapters.

C. Storage and Analysis:
Following the gathering, digital evidence and data must be securely kept in dedicated devices. Transportation, handling, storage device acquisition, and cloud provisioning are all part of this process. The transit process is meticulously planned by law enforcement and forensic specialists.[15] This includes transportation methods, travel routes, security staff, and any equipment required to preserve evidence while in transit.

A chain of custody is also maintained, detailing who handled, analysed, and studied the evidence as well as the date and time of transfer. This is important because the prosecutor will have to present it to the judge along with the rest of the evidence.[15] Proper risk management measures

should be used to guarantee that evidence is transported safely from the scene to the lab or location where it will be evaluated.

Finally, fault-tolerant, data redundancy, and strong access restrictions must be maintained to guarantee that data is not purposefully destroyed or corrupted by insiders in order to influence the decision. Data duplicators, such as the Cellebrite UFED Ruggedized Storage, the Voyager M3 Evidence Drying Cabinet, and the CRU WiebeTech Digital Forensic Storage, provide a safe storage medium as well as features like encryption, in-built write-blockers, and biometric access.

Following the storage phase, the digital evidence can be reproduced and distributed to multiple forensic personnel for analysis and to expedite the inquiry. Of course, the sharing will be recorded and thoroughly documented in the chain of custody document. The following steps may be included in the analysis phase:

1. Data Extraction: The analysis process begins once the evidence has been securely stored. The initial stage tends to be to extract data from the electronic devices and media that have been seized.[15] Files, emails, photos, logs, and other pertinent data can all be extracted. Eg: Cellebrite UFED

2. Data Recovery: is used to recover deleted or hidden data that could not be recovered on the scene. For example, Magnet AXIOM [15]

3. Data Decryption: Tools like Elcomsoft Phone Breaker can be used to retrieve encrypted data from mobile devices and cloud services if the suspect's device has advanced countermeasures like data encryption. [15]It can also decrypt passwords and encrypted backups, among other things.

4. Metadata Examination: Metadata such as file timestamps and user activity logs can give useful contextual information. Hardware tools aid in the analysis of information in order to build timelines and user behaviours.[15] For example, Logicube Forensic ComboDock F8 may be used in combination with forensic software to examine information while avoiding accidental changes.

5. Data Carving: Data carving is the process of recovering lost or damaged files by extracting fragmented or unallocated data from the storage medium. For example, when integrated with forensic software, the Tableau TD3 Forensic Duplicator may be used for data carving activities to retrieve buried or destroyed data.[15]

6. Link Analysis: Link analysis uncovers correlations and patterns by identifying and visualizing connections between various pieces of data. Palantir Gotham, for example, has link analysis features that enable investigators to connect and analyse data pieces to identify these links.[15]

7. Malware Analysis: In the instance of desktops and laptops that have been infected with malware as a precautionary step by the accused, hardware-based write blockers such as Tableau Forensic Bridges can be used to collect data from infected devices for future examination in a controlled environment.[15]

Some of the real-life instances where the use of such hardware forensic tools were instrumental in solving cybercrime cases are as follows:

1. Hardware forensic tools were used extensively during the investigation into the Russian hacking of the Democratic National Committee (DNC) in the run-up to the 2016 U.S. Presidential Election. To build replicas of hacked systems, investigators employed hardware write blocks and forensic imaging tools.[15] This enabled them to scan the servers for malicious code, track down the attack

pathways, and discover evidence tying the incursion to particular hacker groups.

2. Hardware forensic tools are employed in financial fraud investigations to assess digital information connected to insider trading and other financial crimes. Investigators can unearth evidence of unlawful trading operations, communication with accomplices, and covert financial transactions by capturing forensic photographs of suspects' computers and mobile devices utilizing hardware write blocks.[15]

3. Hardware forensic techniques were critical in evaluating compromised industrial control systems in the context of the Stuxnet virus, a sophisticated cyberweapon meant to target Iran's nuclear program. To protect the integrity of compromised computers, investigators deployed specialized hardware write blocks and imaging tools.[15] Experts were able to identify the worm's origins and unearth evidence pointing to state-sponsored cyber espionage and sabotage by examining the worm's code and behavior in a controlled environment.

4. Hardware forensic methods have been utilized to recover lost or stolen digital assets in situations involving cryptocurrency-related crimes. Specialized instruments were used by investigators to examine damaged hard drives, USB devices, and storage media carrying Bitcoin wallets. They successfully recovered monies and traced transactions to identify suspects engaged in Bitcoin theft by meticulously extracting and rebuilding wallet data.[15]

V. Comparative Analysis:

In order to assist law enforcement and cybersecurity experts in identifying and reducing cyber risks, the following comparison of software and hardware tools in cybercrime investigations identifies the advantages and disadvantages of each strategy. Although both kinds of tools are essential to cybercrime investigations, their functions and uses are different. Let's look more closely at the comparison:

A. Definitions

1. Software tools are apps or programmes that operate on computers or mobile devices to carry out certain activities linked to cybercrime investigations. They consist of tools for network analysis, malware scanning, memory analysis, and digital forensics software, among others.
2. Hardware tools are tangible objects created to help with cybercrime investigations.
Write blocks, hardware-based imaging devices, network traffic analyzers, and other hardware instruments are frequently used in conjunction with software solutions.

B. Functionality:

1. Software tools: The foundation of cybercrime investigations is digital forensics software. It supports the gathering, preservation, and analysis of digital evidence from a variety of devices, including computers, smartphones, and storage devices.[16]Software tools can analyse huge data sets, automate repetitive activities, and visualise intricate relationships in the data.

2. Hardware tools are essential for gathering data from numerous devices without tampering with the original evidence. Write blocks, for instance, guarantee the integrity of the source data during the acquisition process by preventing any alterations. In the beginning of an investigation, hardware tools are frequently employed to create forensic photographs.[16]

C. Cost and Accessibility:

1. Software tools are typically more affordable and more accessible than physical solutions. A wide spectrum of customers can afford them because many digital forensics software solutions are accessible commercially or as open-source.[17]

2. Hardware tools: In order to use hardware tools successfully, specialised training may be necessary, and they can be relatively expensive.

This may make them less accessible, especially for budget-constrained or smaller law enforcement organisations.[17]

D. Automation and Speed:

1. Software tools: Software tools can automate a variety of time-consuming processes, including keyword searches, data carving, and hash computations.[18] The investigative process is substantially expedited by this technology, enabling investigators to handle more cases effectively.

2. Hardware tools: Since they work directly with the physical storage media, hardware tools, especially during the data collecting stage, can be quicker. The subsequent investigation utilising software tools, however, can take more time.[18]

E. Reliability and accuracy:

1. Software tools: Both the calibre of the algorithms and the level of experience of the investigators employing them have a significant impact on the accuracy and dependability of software tools. Analysis errors may result from incorrect settings or misinterpretations.[19]

2. Hardware tools: Because they don't change the software, hardware tools like write blocks are often regarded as highly dependable.[19]

F. Training and Expertise:

1. Software Tools: Appropriate training and expertise are necessary for effective usage of software tools.[20]
To produce accurate results, cybercrime investigators need a solid understanding of the procedures and instruments available.

2. Hardware equipment: Even if some hardware tools are simple to use, investigators could still need training to ensure correct handling and the best outcomes.[20]

Finally, it should be noted that both hardware and software tools are crucial for cybercrime investigations.

Software solutions are incredibly effective and flexible because they offer considerable automation and analytical capabilities. Hardware tools, on the other hand, are essential for gathering digital evidence without tampering with it.[20]Both of these sorts of techniques are frequently combined in an efficient cybercrime investigation to increase productivity, accuracy, and the investigation's overall success.

VI. Legal and Ethical Considerations

A. Legal Implications:

1. Privacy Concerns: Accessing and analyzing digital data, which may contain sensitive information about people or organizations, is required to use cybercrime investigative tools. While different jurisdictions have different privacy laws and regulations, several issues frequently raised are warrantless searches, data retention, and permission requirements.[21] For instance, when using digital evidence gathered without legal authorization, the Fourth Amendment in the United States can be significant as it protects people from arbitrary searches and seizures.

2. Juridistionay challenges: Cybercrime investigations sometimes span international borders, which makes it difficult to apply uniform legal norms. Data access, sharing, and evidence admissibility regulations in various nations may differ, which could cause disputes and complicate judicial procedures.[21]

3. Data Retention and Destruction: To maintain the integrity and legal admissibility of digital evidence, law enforcement organizations must abide by stringent rules for processing and storing data.[21] To preserve people's rights and avert potential data misuse, data retention procedures must also comply with ethical standards and data protection legislation.

B. Ethical Implications

1. Informed Consent: An essential ethical factor is obtaining the persons whose data is being collected with their informed consent. Although getting consent from suspects may not always be attainable when conducting cybercrime investigations, ethical standards should govern how the data should be used and handled.[22]

2. Data Security and Confidentiality: To avoid unauthorized access and potential leaks, it is crucial to guarantee the security and confidentiality of the data that has been obtained.[22] Strong data encryption, storage, and transfer procedures must be used by ethical professionals to prevent sensitive data from getting into the wrong hands.

3. Transparency and Accountability: The methods and technologies used by law enforcement organizations and cybersecurity experts should be openly disclosed.[22] They must take responsibility for their activities, and any transgressions of moral principles should be investigated and dealt with appropriately.

C. Chain of Custody

1. Evidence Preservation: To protect the integrity and admissibility of digital evidence in court, an uninterrupted chain of custody must be maintained. To prevent objections to the evidence's legitimacy, proper documentation of the evidence-gathering procedure, storage, and handling must be followed.[23]

2. Digital Forensics skills: To ensure correct data capture, processing, and interpretation, handling cybercrime investigation instruments requires specialized digital forensics skills.[23] The incorrect use of these instruments could result in incorrect allegations and erroneous evidence interpretation.

VII. Emerging Trends

Introduction:

The quick development of information and communication technology (ICT) has made the internet an effective instrument for communication, enabling e-commerce, e-learning, and e-banking, among other advantages. However, in addition to these benefits, the usage of cyberspace has also brought about security concerns, which have given rise to cyberattacks or cybercrimes. Effective security measures are required for these crimes, which range from simple email stalking to sophisticated cyber-terrorism. An important instrument to handle cybercrime investigations and manage legal issues in this dynamic field is digital forensics, a relatively new idea.

Digital Forensics: The application of forensic scientific disciplines to electronic-based crime scenes is known as digital forensics. Due to the rising number of publications in recent years, especially in response to the increase in terrorism and cybercrime, it has become a notable area of study. [24]Digital forensics is a critical tool in the fight against cybercrime as cyberspace develops into a lucrative setting for illegal operations.[24] Identification, acquisition, preservation, inspection, analysis, and presentation of electronic evidence are the core tenets of digital forensics.

A. Tools used for Cybercrime Digital Forensics:

Digital forensics tools for cybercrime investigations:

1. MemGator: Automated memory interrogation programme that combines memory analysis tools like Volatility Framework and PTFinder to extract data from memory files and produce an extensive report.[24] Data about memory information, processes, network connections, virus detection, passwords and encryption keys, and the registry may all be retrieved.

2. First on Scene (FoS): A visual basic script that supports forensic investigations by providing an evidence log report using tools like LogonSessions, FPort, PromiscDetect, and FileHasher.[24]

3. Galleta: An effective tool for evaluating cookies associated with browser histories that provides details about websites visited as well as cookie storage locations.[24]

4. Ethereal: A network security tool for sniffing information from incoming and outgoing packets, albeit its performance may be hampered by encryption keys.[24]

5. NMap (Network Mapper): A network security programme that can hide its identity to avoid suspicion while checking remote workstations for open ports.[24]

B. Development of a Cybercrime Investigation Simulator for Immersive Virtual Reality

Recent advancements in computer technology and cell phones have enabled high-quality virtual reality (VR) rendering, expanding VR simulator training into new fields, including crime scene investigation for novice police officers.[25] The project aims to transform the existing Virtual Crime Scene Simulator (VCSS) into an immersive VR experience to enhance training effectiveness.

The current desktop-based VCSS, developed by University College Dublin, received positive feedback but requires improvement to provide a more realistic and immersive scenario. The chosen platform for this transformation is the HTC Vive with built-in support for SteamVR, allowing seamless integration with the existing Unity game engine used in VCSS creation.[25]

C. Windows Forensic Investigations Using PowerForensics Tool

In order to extract, examine, and report digital evidence on Windows operating systems, this article explains how PowerShell can be used in digital forensics. It examines Windows PowerShell's features and its advantages for digital forensic investigators. The PowerForensics programme is highlighted, with the emphasis being on instruments specifically created for forensic investigations.[26] Various Windows forensic artefacts are extracted and identified using PowerForensics, exhibiting both its strengths and weaknesses.

VIII. Challenges and Future Recommendations

A. Software and Hardware Challenges in Cybercrime Investigations:

1. Difficulty: Encryption and anonymity
Technical Definition: Cybercriminals encode their data with encryption techniques, rendering it illegible without the necessary decryption key.[27] They also use anonymity tools, such as virtual private networks (VPNs), to conceal their name and location while engaging in hostile activity.

Example: Assume you have a private diary with a lock that only you know the combination to. Nobody can read what's written within without the key, keeping your secrets hidden. Similarly, hackers utilize encryption to safeguard their data, making it difficult for investigators to access and comprehend the data without the appropriate decryption key.

2. Difficulty: Evolving Cyber Threats
Technical Definition: Cyber-dangers are always evolving and becoming more sophisticated.[27] Hackers create innovative tactics, such as zero-day exploits and polymorphic malware, to avoid detection and circumvent standard security measures.

Example: Consider cyber risks like viruses that change to become more resistant to vaccines. Similarly, hackers develop new attack tactics to circumvent security systems, making it tough for investigators to keep up with the ever-changing cybercrime field.

3. Difficulty: Resource Constraints and Budget Restriction
Technical Definition: Cybercrime investigations necessitate the use of specialised software licences, sophisticated technology, and highly skilled personnel. Organisations and law enforcement agencies may be unable to acquire the most up-to-date tools and technology due to limited resources and financial constraints.[28]

Example: Investigating cybercrime is like to solving a hard puzzle. To solve the enigma, however, expensive tools and professional investigators are required. If the investigators are on a tight budget, they may not be able to afford the most advanced tools, which would slow down the inquiry.

4. Difficulty: Data Overload and Complexity
Technical Definition: Modern cybercrime investigations necessitate the collection of huge amounts of digital data from a variety of sources, including computers, mobile devices, and network records.[29] Analysing such a large and diverse set of data can be time-consuming and difficult.

Example: Consider the following scenario: You have thousands of jigsaw puzzle pieces, each from a distinct puzzle. Putting together puzzle pieces is analogous to analysing diverse digital data throughout an investigation. Identifying the right components and accurately fitting them together can be overwhelming and time-consuming.

5. Difficulties with Standardisation and Interoperability
Technical Explanation: Due to a lack of standardisation and interoperability, different software and hardware tools used in cybercrime investigations may not interact efficiently with one another.[29] This can cause data compatibility concerns and impede investigator collaboration.

Example: In a collaborative project, some team members utilize metric units, while others use imperial units.[29] This lack of standardisation makes it difficult to communicate information and collaborate effectively. Similarly, a lack of standardisation among investigation tools might result in compatibility concerns and a delayed investigation process.

Future Recommendations for Software and Hardware Tools in Cybercrime Investigations:

1. Recommendation: Advancements in AI and machine learning are advised as follow:
Technical explanation: Automate data analysis, anomaly detection, and pattern identification processes by incorporating artificial intelligence (AI) and machine learning (ML) algorithms into cybercrime investigation tools. Investigators can scan massive datasets quickly and proactively identify potential cyber dangers since AI can learn from prior data and ML algorithms can spot aberrant behaviour.[30]

Example: Think of artificial intelligence as a smart assistant that gradually learns your preferences. It can instantly identify strange actions, such as an unexpected guest to your home, when you ask it to look for irregularities in your everyday routine. This helps you remain aware. Similar to this, applying AI and ML to cybercrime investigations enables investigators to spot anomalous patterns in data, including suspect network activity.

2. Recommendation: Information Sharing and Cooperation

Improve communication and information exchange across the many organisations involved in cybercrime investigations, including law

enforcement agencies, cybersecurity companies, and private organisations. [30]Sharing threat intelligence and best practises can enable a collaborative reaction to effectively tackle cybercrime and result in a more thorough understanding of cyber dangers.

Example: Simple Life Example: Assume that you and your neighbours regularly discuss any shady goings-on in your neighbourhood. One neighbour can alert others and encourage increased vigilance if they become aware of a pattern of break-ins. Similar to this, when many authorities and organisations share information on cyber dangers, they can work together to identify and address new threats, lessening the overall impact of cybercrime.

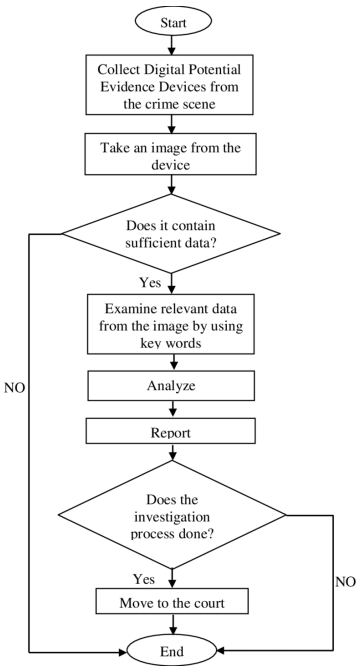
3. Recommendation: Technical explanation for unified cybercrime investigation platforms: Create and put into use systems that seamlessly combine different hardware and software capabilities. These platforms ought to be scalable, adaptable, and interoperable so that investigators may access all required tools from a single interface. This connection improves overall efficiency and streamlines the research process.

Example: Take the field of cybersecurity as an example, where deciphering complex cybercrimes necessitates a combination of hardware, software, and analytical techniques. Imagine a cutting-edge cyber centre that functions like a Swiss Army knife for digital detectives, similar to the technical explanation for unified cybercrime investigation platforms. With a single interface, this hub effortlessly combines various hardware and software capabilities that are built to be scalable, adaptable, and interoperable.

This single cyber platform incorporates features like digital forensics, network analysis, and virus scrutiny, much like the components of a Swiss Army knife gracefully fold into one. By using a single platform, investigators can access a whole set of tools without switching between different programmes. The hub covers all of these tasks, including identifying an attack's origin, examining malicious code, and examining network anomalies.

Similar to how useful the Swiss Army knife is outside, this cybersecurity hub boosts performance. Phases are easily navigated by investigators, speeding up work without software transitions. Scalability of the platform combats changing threats, and interoperability integrates it into current cybersecurity ecosystems, fostering cooperation and information exchange.

This portal changes how cybercrime investigation is conducted by combining skills into a single interface. It simplifies complicated processes, much like the Swiss Army knife, and creates quick and effective solutions to digital dangers.



Recommended Flow chart of Cyber Investigation

Fig 8.1[31]

4. Recommendation: Considerations for Ethics and Data Privacy

Technical justification In all cybercrime investigations, give data privacy and ethical

considerations top priority. To preserve individual rights and uphold the public's trust, make sure that any software or hardware utilised in investigations complies with legal and ethical requirements.[32]

Example: Consider a locksmith who is called to open a locked door as an example from everyday life. It is the locksmith's moral duty to open the door without inflicting any harm and in accordance with the owner's privacy. In a similar way, cybercrime investigators should employ methods and tools that protect individuals' rights while acquiring digital evidence to help solve crimes. These methods and tools should also be compliant with data privacy regulations and ethical standards.

IX. Conclusion

In conclusion, the survey's findings have been beneficial in illuminating the wide range of hardware and software solutions that support the complex field of cybercrime investigations. This newly discovered knowledge emphasises the crucial role that sophisticated and cutting-edge tools play in accelerating the investigative procedure, allowing investigators to expertly extract crucial forensic insights from the digital landscape.

However, the core of a successful cybercrime investigation goes beyond the mere presence of cutting-edge technologies; it hinges on the complex and coordinated coordination between a variety of different software and hardware components. It is impossible to overstate the importance of this thorough integration because it serves as the fundamental engine that drives the discovery and analysis of even the most complex cyberthreats. The landscape of investigation has been greatly enhanced by the seamless and harmonious interoperability of these multifaceted tools, giving investigators the rare ability to manoeuvre through the complex maze of digital footprints with a degree of finesse and mastery that would otherwise be beyond their reach. The true potential of cybercrime investigation is completely realised through this coordinated orchestration, leading to a more comprehensive understanding of the digital realm's complexities and intricacies.

The combination of many instruments, each with a special area of specialty, raises the total effectiveness of cybercrime investigations to previously unheard-of levels. By using a coordinated strategy, dealing with complex challenges becomes a manageable trip in which information from multiple sources and perspectives converges to create an all-encompassing story.

It is crucial to keep on the cutting edge of technology in the vast field of digital security. Because cyber dangers are constantly changing, software and hardware solutions must also advance to stay one step ahead of possible attackers. Furthermore, ethical concerns must continue to take precedence, ensuring that the pursuit of justice is consistently in line with norms of confidentiality and legality.

The need to protect against cyber dangers grows as the digital environment becomes more complex. Using cutting-edge tools and orchestrating their symphonic integration are both required for this. In this endeavour, cybersecurity experts and engineers will work together to strengthen the defences against cybercrime. Cybersecurity measures are in a strong position to provide effective responses to the wide range of growing cyber threats by adhering to four principles: maintaining ethical foundations, keeping up with technological advancements, and utilising software and hardware solutions. Through these coordinated efforts, the war against cybercrime picks up steam, guaranteeing a safer and more secure online environment for everyone.

References:

[1]“Tools and Techniques used to Investigate Cyber Crime,” *www.linkedin.com*. https://www.linkedin.com/pulse/tools-techniques-used-investigate-cyber-crime-amanda-goh.

[2]“EnCase Forensic,” *GetApp*. https://www.getapp.ca/software/2051469/encase-forensic.

[3] CyberSecurityMag, “10 Best Tools for Computer Forensics,” Cyber Security Magazine, Mar. 02, 2019. https://cybersecuritymag.com/computer-forensics-tools/

[4] CYBERVIE, “Introduction To Autopsy | An Open-Source Digital Forensics Tool,” *CYBERVIE*, Sep. 14, 2021. https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/

[5]“Secure, Save and Analyse data with the FRED Workstation - DataExpert EN,” *www.dataexpert.eu*. https://www.dataexpert.eu/products/forensic-hardware-digital-intelligence/fred-workstation/.

[6] CRU, “Write Blockers - CRU,” *CRU*, 2019. https://www.cru-inc.com/data-protection-topics/write-blockers/.

[7] “The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools,” *Sleuthkit.org*, 2019. https://www.sleuthkit.org/index.php

[8] E. Borges, “SecurityTrails | Cyber Crime Investigation Tools and Techniques Explained,” *securitytrails.com*, Aug. 09, 2021. https://securitytrails.com/blog/cyber-crime-investigation

[9] “10 Open-Source Intelligence Tools (That Actually Work With Your Existing Security Software),” *Security Intelligence*. https://securityintelligence.com/articles/10-open-source-intelligence-tools-existing-security-software/

[10]“Steganography - A list of useful tools and resources - 0xRick,” *0xrick.github.io*. https://0xrick.github.io/lists/stego/

[11] A. Cox, J. DeMuro, B. Turner, M. Wycislik-Wilson, C. Ellis, and D. F. 25 June 2020, “Best data recovery software of 2020: Paid and free file recovery solutions,” *TechRadar*. https://www.techradar.com/best/best-data-recovery-software

[12] “5 Best Disk Encryption Software / Tools,” *Comparitech*, Nov. 12, 2018. https://www.comparitech.com/blog/information-security/disk-encryption-software/

[13] “Rekall Forensics,” *www.rekall-forensic.com*. http://www.rekall-forensic.com/

[14]"Forensic Computers | Forensic Hardware | Digital Forensics Workstations", Forensic Computers. [Online]. Available: https://www.forensiccomputers.com/forensic-hardware.

[15] R. Hasan, S. Mahmood, and A. Raghav, "Overview on Computer Forensics tools," *IEEE Xplore*, Sep. 01, 2012. https://ieeexplore.ieee.org/abstract/document/6334663.

[16] E. E.-D. Hemdan and D. H. Manjaiah, "An efficient digital forensic model for cybercrimes investigation in cloud computing," *Multimedia Tools and Applications*, Jan. 2021, doi: https://doi.org/10.1007/s11042-020-10358-x.

[17] Bharadiya, Jasmin. (2023). Cloud Computing Forensics; Challenges and Future Perspectives: A Review. Asian Journal of Computer Science and Information Technology. 16. 1-14. DOI:10.9734/ajrcos/2023/v16i1330

[18] M. Indhumathi, "IJTRD - Paper Detail," *www.ijtrd.com*, Feb. 2020. http://www.ijtrd.com/ViewFullText.aspx?Id=21907.

[19] S. Pawar, C. Bhusari, and S. Vaz, "Survey on Digital Forensics Investigation and their Evidences," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 10, no. 1, pp. 2581–942, 2020, Available: https://ijarsct.co.in/Paper489.pdf

[20] R. V. Mante and R. Khan, "A Survey on Video-based Evidence Analysis and Digital Forensic," *IEEE Xplore*, Mar. 01, 2020. https://ieeexplore.ieee.org/document/9076417.

[21] Landwehr, C., Boneh, D., Mitchell, J.C., Bellovin, S.M., Landau, S. and Lesk, M.E. (2012). Privacy and Cybersecurity: The Next 100 Years. *Proceedings of the IEEE*, 100(Special Centennial Issue), pp.1659–1673. doi:https://doi.org/10.1109/jproc.2012.2189794.

[22] Richter, J. P. (2017). Data Retention: A Critical Analysis of the USA's Data Retention Laws and the Privacy Implications on US Citizens and Non-Citizens. Georgia Journal of International and Comparative Law, 46(1), 1-49.

[23] Casey, E. (2011). *Digital Evidence and Computer Crime Third Edition*. [online] Available at: https://rishikeshpansare.files.wordpress.com/2016/02/digital-evidence-and-computer-crime-third-edition.pdf.

[24] M. Harbawi and A. Varol, "The role of digital forensics in combating cybercrimes," 2016 4th International Symposium on Digital Forensic and Security (ISDFS), Little Rock, AR, USA, 2016, pp. 138-142, doi: 10.1109/ISDFS.2016.7473532.

[25] B. Liu, A. G. Campbell and P. Gladyshev, "Development of a cybercrime investigation simulator for immersive virtual reality," 2017 23rd International Conference on Virtual System & Multimedia (VSMM), Dublin, Ireland, 2017, pp. 1-4, doi: 10.1109/VSMM.2017.8346258.

[26] A. Barakat and A. Hadi, "Windows Forensic Investigations Using PowerForensics Tool," 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2016, pp. 41-47, doi: 10.1109/CCC.2016.18.

[27] A. S. Thakur, “How has cyber security changed in the last decade?,” ZEVENET, Feb. 09, 2022. https://www.zevenet.com/blog/how-has-cyber-security-changed-in-the-last-decade/

[28] “What is Resource-Constrained Scheduling? | Runn,” www.runn.io. https://www.runn.io/blog/resource-constrained-scheduling

[29]“How to Navigate the Lack of Industry Standards & Data Overload | Network Computing,” https://www.networkcomputing.com/network-security/how-navigate-lack-industry-standards-data-overload.

[30]“The Role of Artificial Intelligence in Cybersecurity,” www.boozallen.com. https://www.boozallen.com/s/insight/publication/role-of-artificial-intelligence-in-cyber-security.html

[31] The Flow Chart for a general steps required for the investigation ... Available at: https://www.researchgate.net/figure/The-flow-chart-for-a-general-steps-required-for-the-investigation_fig2_258063968.

[32] B. L. MBA, “Ethical Considerations in AI-Powered Cybersecurity,” Medium, Feb. 15, 2023. https://medium.com/@besniklimaj/ethical-considerations-in-ai-powered-cybersecurity-45cd83db90e0