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* – Because of the rise in cyberattacks brought on by the development of Internet Technology (IT) and the Internet of Things (IoT), cybercrime investigations are crucial for identifying attackers and trends for perception of defence solutions. This paper examines how hardware and software solutions are used in cybercrime investigations for data extraction, recovery, encryption, and analytical purposes. We look at well-known programmes like EnCase, IDA Pro, and Wireshark. The study examines emerging patterns, challenges, ethical and legal concerns, and it makes recommendations for the future. Understanding the benefits and constraints of these tools is more important for improving the efficacy of cybercrime investigations in the face of growing threats.**

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

I. Introduction

The usage of Internet technology (IT) and the Internet of Things (IoT) has raised both the frequency and risk of cyber attacks. However, it is very crucial and difficult to defend against zero-day attacks. Investigation into cybercrime is necessary to pinpoint the attack and the perpetrator. Cybercrime investigations help detect tendencies for possible attacks and create preparations for a defence reply. A cybercrime investigation includes several processes, including investigation, analysis, and recovery of the essential forensic digital evidence from the attacked networks.[1]

For this, a range of forensic instruments that fall within the hardware and software tool categories can be used. The main services provided by hardware tools includes data extraction, data recovery, data encryption, metadata analysis, data carving, link analysis, and virus analysis.

Numerous software applications support techniques like data recovery, encryption-decryption, steganography, virus analysis, memory forensics, log analysis, incident response, open source intelligence (OSINT), and digital forensics. For the survey, we looked at a variety of tools and techniques, including EnCase, IDA Pro, Wireshark, etc.

The majority of the investigations into cybercrime are handled by criminal justice, national security, and private security companies. The comparison of software and hardware tools, legal and ethical concerns, contemporary trends and issues, and future suggestions are among the other topics the essay addresses.

II. Literature Review

Due to the rise in cybercrime, a wide range of software and hardware solutions have been created to aid in the effective ways and thorough

execution of investigations by law enforcement, cybersecurity experts, and experts in digital forensics. We underline the functionality, benefits, and drawbacks of the current software and hardware solutions utilised in cybercrime investigations in this literature review.

A. Digital forensics software tools

The collection, evaluation, and preservation of digital evidence originating from a variety of devices, technology and sources is greatly aided by the use of digital forensic software tools. In this field, many significant tools have emerged:

1. EnCase Forensic: OpenText developed EnCase Forensic as a digital forensic platform to help law enforcement personnel collect, preserve, and decrypt crucial data and evidence from a variety of devices. This solution allows for the discovery of evidence that has been importantly altered, removed, or hidden from a number of sources, such as PCs, social media platforms, cloud services, and IoT/mobile devices.[2] EnCase Forensic goes above and above, accelerating investigations through intelligent automation, by fusing AI-driven procedures with photo analysis.

2. AccessData offers the Forensic ToolKit (FTK), an accessible and reasonably priced forensic software solution with a simple one-touch interface. Based on this programme, AccessData established the ACE certification as a credit; the most recent FTK version is also far more user-friendly. The process is streamlined by the automated complicated searches that FTK has in place. For instance, clicking the Email button instantly retrieves emails. When required, investigators can remain in charge as the FTK report generator successfully generates useful reports inside the software.[3]

3. A user-friendly, open-source software, and cost-free digital forensics tool is Autopsy. It facilitates the use of numerous open-source tools included in The Sleuth Kit. This programme can be used by law enforcement, the military, and business analysts to aid in the investigation of computer-related incidents.Users are able to browse and highlight significant amount of data from forensic searches on computer volumes.[4] In collaboration with nearby programmers, Basis Technology Corp. maintains the tool to a considerable extent.

B. Hardware tools for Digital Forensics

Forensic hardware is mostly used to physically connect a computer's components and collect data for use with forensic software, in contrast to computer forensic software, which concentrates on extracting data logically, practically and within a certain timescale.

1. FRED: FRED, or Forensic Recovery of Evidence Device, is a potent workstation for securely managing, storing, and analysing data from hard discs and other media. The high calibre and scalability of these workstations are well known. In addition to forensic software like EnCase and FTK, FREDs are regularly used. Only FRED systems are equipped with incorporated features such hardware write blocks for IDE, SATA, and SAS drives, USB3, Firewire, and MultiMedia/Memory Card forensic write blockers. [5]

2. Logicube: Logicube provides exceptionally speedy disk-to-disk and disk-to-image transfer solutions, drastically cutting the time required for data capture with speeds of up to 4 gigabytes per minute. To provide a reliable forensic copy, its data capture solution offers real-time integrity checks in addition to securely removing data from a target medium.[3] These gadgets can be customised, include a range of interfaces, and typically feature a convenient term to portable field kit configuration.

3. Write Blockers: Write blockers prevent data from being changed while digital evidence is being captured. Examples include those offered by Tableau and WiebeTech. They protect data integrity while gathering evidence from various storage devices.[6]

The investigation of cybercrime has greatly benefited from the ongoing development of hardware and software solutions. These tools, which vary from network analysis software and digital forensics to specialized means of malware analysis and hardware imaging devices, have made it possible for investigators to gather evidence, catch criminals, and build compelling legal cases. To ensure the success of cybercrime investigation operations, these technologies must advance along with cybercriminals' tactical approaches and maintenance. More research and development are needed to handle the escalating issues and enhance the capabilities of these technologies. to alter things.

III. Software Tools and Cyber Crime Investigation.

In cybercrime investigations, software tools are used to gather and assess evidence, track suspect activities, and monitor network traffic. Important tools include forensic toolkits for data recovery, network analyzers for spotting criminal activity, and encryption programmes for file decryption. These resources are essential for effectively and successfully assisting cybercrime investigators.[8] The exponential growth of cybercrime fuels the continued fight against it, thus making the use of software tools essential for conducting in-depth investigations and identifying offenders. The most common software programmes used in cybercrime investigations are examined in our research.

A. Digital Forensics Software:

1. Autopsy: To find evidence of crimes, retrieve deleted files, and analyse email data, law enforcement and cybersecurity specialists utilise the open-source digital forensics application Autopsy.[8]Additionally, it integrates Sleuth Kit for low level of file system examination.

2. FTK (Forensic Toolkit) is a commercial AccessData tool renowned for its quick and efficient data processing, extensive search capabilities, and compatibility with a wide range of file types.[8] Integral SQLite database for metadata makes storage.

3. EnCase: Industry-recognized commercial software from Guidance Software (now a division of OpenText), which securely collects data from digital devices like PCs, smartphones, and cloud storage while maintaining the integrity of the evidence for admission in court.[7] And access to and decryption of private file systems

4. Sleuth Kit: An open-source forensic toolkit with command-line tools for disc and file analysis that enables thorough investigations and the recovery of deleted or hidden material.[7] An open-source library for analysing file and disc systems.

B. Network Forensics Software:

1. Wireshark: A well-liked open-source network protocol analyzer that enables the detection of shady activities and probable security breaches in real-time network traffic. For the packet capture and protocol analysis, use libpcap.[9]

2. NetworkMiner: A passive network sniffer and packet analysis programme that focuses on extracting images, documents, and executable files exchanged over the network in order to obtain Open Source Intelligence (OSINT),[9] aiding investigators in discovering the hostnames, domain names, and open ports used by cybercriminals. files and metadata from PCAP files by parsing them to it.

C. Malware Analysis Tools:

Investigators must be able to comprehend the characteristics and behaviour of malicious software in order to identify the nature of cyber hazards and develop effective mitigation strategies. A few notable malware detection tools are listed below:

1. IDA Pro: The well-known disassembler and debugger IDA Pro is commonly used by reverse engineers and malware researchers to examine binary files. The interactive and user-friendly interface of malware allows experts to investigate its internal workings and identify potential weaknesses.[11] By understanding the behaviour and programming of malicious software, investigators can develop effective defences and contribute to the creation of antivirus signatures. Interactive disassembler that supports a variety of processors.

2. Cuckoo Sandbox: To automate the inspection of questionable files and URLs in a secure environment, Cuckoo Sandbox was developed as an open-source malware analysis tool. Cuckoo Sandbox tracks network activities and monitors malware behaviour to produce in-depth data on the behaviours of the infection.[11] Thanks to this crucial tool, investigators can quickly identify the type of threat and evaluate its impact on the system. malware analysis that is automated and virtualized.

D. Memory Forensics Tools:

Memory forensics tools are crucial for providing investigators with details on running processes, open network connections, and concealed malware when used to study a system's volatile memory. Well-known memory forensics tools include the following:[13]

1. Volatility: Using the powerful open-source memory forensics toolkit Volatility, investigators can glean valuable information from the volatile memory of operating systems. Traditional disk-based forensics might not be able to fully preserve all of the data, but Volatility can search through RAM dumps for network connections, running programmes, and hidden malware. Because memory forensics frequently offers vital insights into the runtime behaviour of cyber threats, volatility is a crucial investigative approach today.[13] Memory analysis utilising plug-ins for several operating systems.

2. Rekall: Another one is Rekall, formerly known as Volatility Framework 2. It is a well-known memory analysis programme. It offers a variety of tools and plugins to analyse memory dumps and discover significant artefacts for additional investigation.[13] Researchers have the freedom to effectively address a variety of cybercrime scenarios thanks to Rekall's flexibility, which enables them to develop special plugins for particular use cases.Framework for memory analysis with support for Windows.

E. Log Analysis Tools:

The ELK Stack (Elasticsearch, Logstash, and Kibana), three reliable open-source tools for organising and analysing process massive volumes of log data, enables investigators to combine records, identify trends, and swiftly identify security flaws.[12]

Splunk is the greatest commercially available log management and analysis tool. It offers proactive threat detection through machine learning, real-time log monitoring, extensive search options, and data visualisation.[12]

F. Incident Response Platforms:

IBM Resilient: A centralised platform that streamlines incident software response by automating tasks, enhancing teamwork, and using a playbook-driven methodology to lessen the impact of cyber threats.[10]

1. RSA NetWitness: A cutting-edge platform that combines analytics, network visibility, and endpoint visibility to find and analyse complex threats, enabling proactive threat hunting and quick action.

2. Palo Alto Networks Cortex XSOAR: Comprehensive SOAR platform that improves case management, automates repetitive activities, and speeds up incident response by integrating with a variety of security solutions.[10]

G. Tools for encryption and decryption:

1. VeraCrypt is an open-source disc encryption tool that protects sensitive data and ensures the secure retention of evidence during cybercrime investigations by employing powerful encryption techniques like AES and Twofish.[12]

2. BitLocker: This Windows operating system-integrated full-disk encryption technology makes it simple to encrypt whole drives in order to protect data from unauthorised access.[12] When conducting criminal investigations, this technology is essential for safeguarding forensic images and evidence.

H. Open Source Intelligence (OSINT) Tools: Investigators can learn a lot from widely accessible sources by using OSINT tactics, which also helps in the identification of leads and a better knowledge of cyberthreats. The following is a list of a few OSINT tools that are frequently used in cybercrime investigations:

1. Maltego: A powerful OSINT tool that makes it easier to gather and evaluate the actual data on people, groups, and connections, Maltego.[9] In order to identify potential threats and cybercriminal networks, it provides investigators with access to a graphical user interface that enables them to see data and linkages.[9]

2. theHarvester: Information is obtained via the command-line OSINT programme theHarvester from a variety of open sources, including search engines, social networking websites, and DNS databases.[9] TheHarvester is a tool that investigators can use during reconnaissance to gather crucial information that could lead to fruitful leads.

I. Data Recovery Tools:

During cybercrime investigations, data recovery technologies are crucial for assisting investigators in recovering lost or destroyed data from storage media. These tools are essential for recovering crucial evidence that may have been purposefully or accidentally deleted. The following is a list of some popular data recovery tools:[9]

1. Recuva: Recuva is an easy-to-use data recovery tool that assists in restoring erased files from storage media, including hard drives, memory cards, and USB devices.[8] During a cybercrime investigation, vital evidence that may have been accidentally or maliciously deleted can be recovered with Recuva.

2. TestDisk: TestDisk is a powerful data recovery programme that is recognised for its ability to repair corrupt boot the disk sectors and restore missing partitions. 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. The Java-based application Stegsolve offers a variety of visualisation methods and techniques, including colour inversion and bit plane slicing, for the analysis of image data, allowing users to locate and extract hidden information from images.[10]

2. StegDetect is a command-line steganography detection tool that may locate concealed data in

photos/pics and identify steganography telltale indications, alerting investigators to the potential presence of such material for further investigation.[10]

IV. Hardware Tools for Cyber Crime Investigation

As cybercriminals hone their evasion techniques and investigators find it more difficult to navigate 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, there is a case to be made for the adoption of some sophisticated tools that complement their software counterparts.[15]

These technologies are employed along the entire chain, from extraction to validation to analysis, and they are a major aid to law enforcement organisations all over the world. We offer a few examples of these devices, sorted by use case and application domain.

A. Evidence and Data Acquisition:

An investigation will take many more steps after this one. After obtaining a search warrant, officers move on to gather and record all objects and items they determine to be crucial to the investigation.[14] Second, the investigating team needs to have professionals with the knowledge and experience necessary to extract any crucial information from the suspect's gadgets without contaminating them. They make use of a range of technologies, including as Write Blockers, Disc Imagers, Mobile Device extraction, and Network Forensic Devices, to get a complete picture of the state of the suspects' systems.

When write blocking is turned on, forensic imaging software can easily collect a bit-by-bit copy of memory storage, hard drives, SSDs, CPU registers, caches, etc., as well as all file information. 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:

It is crucial to validate the data after carefully collecting all the information required for the investigation. Although we have some tools at our disposal to evaluate and rigorously validate the data, this is typically done with specialised or proprietary software. The hashes of stored forensic data are compared to the original data to remove discrepancies. By ensuring that the data has not been changed or tampered with during the investigative process, this is essential for guaranteeing the integrity and authenticity of digital evidence gathered.[14] Several well-known examples of these devices:

1. Forensic imager Tableau TX1: This hardware equipment computes and validates hash values of gathered photos thanks to built-in hashing and validation capabilities. Because of its user-friendly interface and dependable functioning, it is a recommended tool for guaranteeing the integrity of the evidence.[14]

2. CRU WiebeTech UltraDock v5, is a hardware-based write-blocker with forensic image hashing capabilities.[14]

3. Cellebrite UFED Touch: Can validate evidence by generating hash values of data acquired from mobile devices and verifying their integrity.[14]

C. Storage and Analysis:

After collection, digital evidence and data need to be safely stored in designated devices. This process includes storage device acquisition, handling, transportation, and cloud provisioning. Law enforcement and forensic experts carefully prepare every step of the transportation procedure.[15] This covers the modes of

transportation, the routes taken, the security personnel, and any tools necessary to preserve evidence while it is being transported.

Additionally, a chain of custody is kept that shows when and how the evidence was transferred as well as who handled, examined, and studied it. This is significant because, together with the other evidence, the prosecutor must present it to the judge.[15] To ensure that evidence is moved from the scene to its destination securely, appropriate risk management procedures should be employed.

Finally, to ensure that data is neither altered or purposely destroyed by insiders in order to influence the decision, fault-tolerant, data redundancy, and rigorous access limits must be maintained. Data duplicators offer a secure storage medium in addition to features like encryption, built-in write-blockers, and biometric access. Examples include the Cellebrite UFED Ruggedized Storage, the Voyager M3 Evidence Drying Cabinet, and the CRU WiebeTech Digital Forensic Storage.

After the storage stage, the digital evidence can be duplicated and given to various forensic specialists for study to quicken the vulnerability investigation. Of course, the sharing will be meticulously noted in the chain of custody document and recorded. The analysis phase may comprise the following actions:

1. Data Extraction: After the evidence has been safely saved, the analysis procedure starts. Data extraction from confiscated electronic devices and media is frequently the first step.[15] It is possible to extract intelligence files, emails, pictures, logs, and other important information. Consider Cellebrite UFED.

2. Data recovery: this technique is used to retrieve deleted or concealed data that was not accessible immediately. As an illustration, Magnet AXIOM.[15]

3. Data Decryption: If the suspect's device has advanced countermeasures such as data encryption, tools such as Elcomsoft Phone Breaker can be utilised to obtain encrypted data from mobile devices and cloud services.[15] Among other things, it can decrypt passwords and encrypted backups.

4. Examining Metadata: Metadata such as file timestamps and user activity logs can provide contextual endpoint information. Hardware tools help with information analysis in order to create timelines and user behaviours.[15] Logicube Forensic ComboDock F8, for example, can be used in conjunction with forensic software to inspect data while avoiding inadvertent changes.

5. Data Carving: The process of retrieving lost or damaged secure files by extracting fragmented or unallocated data from the storage medium is known as data carving. The Tableau TD3 Forensic Duplicator, for example, can be used for data carving activities to recover buried or lost data when combined with forensic software.[15]

6. Link Analysis: Link analysis identifies and visualises connections between diverse kinds of data to reveal correlations and patterns. Palantir Gotham, for example, includes link analysis features that allow investigators to connect and examine data pieces in order to find these linkages.[15]

7. Malware Analysis: If the accused infected desktops and laptops with malware as a precautionary measure, 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. During the investigation into the Russian hacking of the Democratic National Committee (DNC) in the run-up to the 2016 U.S. Presidential Election, hardware forensic tools were extensively deployed. Investigators test to used hardware write blocks and forensic imaging techniques to create replicas of hijacked devices.[15] This allowed them to search the servers for malicious code, trace the attack paths, and find evidence linking the intrusion to specific hacker groups.

2. In financial fraud investigations, hardware forensic techniques are used to examine digital material related to insider trading and other financial crimes. By taking forensic pictures of suspects' computers and mobile devices using hardware authentication write blocks, investigators can find evidence of illegal trading operations, communication with accomplices, and covert financial transactions.[15]

3. In the context of the Stuxnet virus, a sophisticated cyberweapon designed to target Iran's nuclear programme, hardware forensic techniques were important in evaluating infected industrial control response systems. Investigators used specialised hardware write blocks and imaging technologies to protect the integrity of hacked machines.[15] By investigating the worm's code and behaviour in a controlled environment, experts were able to pinpoint the worm's origins and find evidence pointing to state-sponsored cyber espionage and sabotage.

4. In cases involving cryptocurrency-related crimes, hardware forensic approaches have been used to recover lost or stolen digital assets. Investigators employed specialised tools to check damaged hard drives, USB devices, and storage media containing 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:

The following comparison of software and hardware tools in cybercrime investigations analyses the benefits and drawbacks of each approach in order to aid law enforcement and cybersecurity specialists in identifying and minimising cyber hazards. Despite the fact that both types of tools are necessary for cybercrime investigations, their purposes and applications are distinct. Let's examine the contrast in more detail:

A. Definitions

1. Software tools are programmes or apps that run on computers or mobile devices to perform certain tasks related to cybercrime investigations. They include, among other things, software for digital forensics, malware scanning, network analysis, and memory analysis.

2. Hardware tools are physical items designed to aid in the investigation of cybercrime.
Frequently security audit used hardware tools include write blocks, hardware-based imaging devices, network traffic analyzers, and others.

B. Functionality:

1. Software tools: Digital forensics software serves as the core of cybercrime investigations. It enables the collection, storage, and analysis of digital evidence from a range of gadgets, including laptops, smartphones, and storage devices.[16]Large data collections can be analysed, repetitive tasks can be automated, and complex data relationships can be visualised using software tools.

2. Hardware instruments are necessary for collecting information from various devices without tampering with the original evidence. For instance, write blocks ensure the accuracy of the source data during acquisition by blocking any changes. Hardware management tools are routinely used to create forensic images at the start of an inquiry.[16]

C. Cost and Accessibility:

1. Compared to physical solutions, software tools are often more accessible and more inexpensive. Because many digital forensics software solutions are available commercially or as open-source, a wide range of clients can afford them.[17]

2. Hardware tools: Hardware tools can be relatively expensive and may require specific training in order to be used effectively. This might make them less reachable, particularly for smaller or less well-funded law enforcement agencies.[17]

D. Automation and Speed:

1. Software tools: Keyword searches, data carving, and hash computations are just a few of the time-consuming tasks that can be automated by software tools.[18] This technology greatly speeds up the investigation process, allowing investigators to efficiently handle more cases.

2. Hardware instruments can be quicker during the data collection phase since they interact directly with the actual storage media. However, the further inquiry with software tools may take longer.[18]

E. Reliability and accuracy:

1. Software tools: The accuracy and dependability of software tools are significantly influenced by the quality of the algorithms and the level of expertise of the investigators using them. Misinterpretations or wrong settings might lead to analysis errors.[19]

2. Hardware tools: Hardware tools like write blocks are frequently thought of as being very dependable because they don't alter the software.[19]

F. Training and Expertise:

1. Software Tools: Appropriate training and experience are required for effective software tool utilisation.[20]

Cybercrime investigators must have a thorough awareness of the techniques and tools available in order to deliver accurate results.

2. Hardware: Even if some hardware tools are simple to use, investigators may require training to ensure proper handling and the best results.[20]

Finally, it should be highlighted that cybercrime investigations require both hardware and software tools.

Because they provide significant automation and analytical capabilities, software solutions are extremely effective and versatile. In contrast, hardware equipment are required for obtaining digital evidence without tampering with it.[20] Both of these strategies are routinely used in an effective cybercrime investigation to boost productivity, accuracy, and the overall success of the investigation.

VI. Legal and Ethical Considerations

A. Legal Implications:

1. Privacy Concerns: Using cybercrime investigative tools for cyber hygiene necessitates accessing and analysing digital data, which may contain sensitive information about individuals or organisations. While different jurisdictions have distinct privacy laws and regulations, unwarranted searches, data retention, and authorization requirements are regularly challenged.[21] When using digital evidence obtained without legal consent, for example, the Fourth Amendment in the United States can be important since it protects persons from arbitrary searches and seizures.

2. Legal issues: Cybercrime investigations frequently cross international borders, making it difficult to apply universal legal standards. Data access, sharing, and evidence admissibility regulations may differ among countries, thereby causing disputes and complicating legal proceedings.[21]

3. Data Retention and Destruction: To ensure the integrity and legal admissibility of digital evidence, law enforcement agencies must follow strict data processing and storage guidelines.[21] Data retention methods must also adhere to ethical standards and data protection legislation in order to protect people's rights and prevent potential data misuse.

B. Ethical Consequences

1. Informed Consent: Obtaining the informed consent of the people whose data is being gathered is a critical ethical aspect. Although obtaining consent from suspects is not always possible when network conducting cybercrime investigations, ethical norms should govern how data is utilised and managed.[22]

2. Data Security and secrecy: To avoid unauthorized access and potential leaks, it is critical to ensure the data's security and secrecy.[22] To prevent sensitive data from falling into the wrong hands, ethical professionals must utilise strong data encryption, storage, and transfer processes.

3. Transparency and Accountability: The methodologies and technologies employed by law enforcement agencies and cybersecurity specialists should be made public.[22] They must accept accountability for their actions, and any violations of moral norms must be examined for threats and dealt with accordingly.

C. Chain of Custody

1. Evidence Preservation: An uninterrupted chain of custody must be maintained in order to ensure the integrity and admissibility of digital evidence in court. To avoid challenges to the evidence's legitimacy, thorough documentation of the evidence-gathering, storage, and handling procedures must be followed.[23]

2. Digital Forensics Skills: Handling cybercrime investigation instruments necessitates specialised digital forensics skills to enable proper data acquisition, processing, and interpretation.[23] improper use of these tools may result in false allegations and improper evidence interpretation.

VII. Emerging Trends

Introduction:

Because of the rapid advancement of information and communication technology (ICT), the internet has become a powerful tool for communication, enabling e-commerce, e-learning, and e-banking, among other benefits. However, in addition to these advantages, the use of cyberspace has raised security issues, giving birth to cyberattacks or cybercrimes. For these crimes, which vary from basic email stalking to sophisticated cyber-terrorism, effective security measures are essential. Digital forensics, a relatively new concept, is a crucial tool for handling cybercrime investigations and managing legal difficulties in this dynamic industry.

Digital Forensics: Digital forensics is the application of forensic science disciplines to electronic-based crime scenes. It has become a prominent topic of study since the number of publications has increased in recent years, particularly in reaction to the surge in terrorism and cybercrime.[24] As cyberspace evolves into a lucrative setting for unlawful operations, digital forensics has become an essential tool in the battle against the cybercrime.[24] The fundamental principles of digital forensics include the identification, acquisition, preservation, inspection, analysis, and presentation of electronic evidence.

A. Tools - Cybercrime Digital Forensics:

Digital forensics tools for cybercrime investigations:

1. MemGator: A memory interrogation programme that integrates memory analysis tools such as Volatility Framework and PTFinder to extract data from memory files and generate a comprehensive report.[24] Memory data, processes, network connections, virus detection, passwords

and encryption keys, and registry information can all be retrieved.

2. First on Scene (FoS): A VB script that aids forensic investigations by generating an evidence log report using tools such as LogonSessions, FPort, PromiscDetect, and FileHasher.[24]

3. Galleta: A useful tool for analysing cookies connected with browser histories, which provides information about websites visited as well as cookie storage locations.[24]

4. Ethereal: A network security tool that affects sniffs data from incoming and outgoing packets, albeit its performance may be limited by encryption keys.[24]

5. NMap (Network Mapper): A network security tool that can conceal its identity while scanning remote workstations for open ports.[24]

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

High-quality virtual reality (VR) rendering is now possible because to recent developments in computer and mobile technology. This has opened up new applications for VR simulator training, including crime scene investigation for new police officers.[25] To improve training efficacy, the project intends to convert the current Virtual Crime Scene Simulator (VCSS) into an immersive VR experience.

The present desktop-based VCSS, created by University College Dublin, has gotten good reviews, but it still has to be improved to offer a more immersive and realistic setting. The HTC Vive, which has built-in support for SteamVR, was selected as the platform for this transformation because it enables easy connection with the Unity game engine already in use for VCSS development.[25]

C. Windows Forensic Investigations Using PowerForensics Tool

This article describes how PowerShell can be used in digital forensics to extract, analyse, and report digital evidence on Windows operating systems. It looks at the benefits of Windows PowerShell for digital forensic investigators. The PowerForensics programme emphasises the, with a focus on tools made especially for forensic investigations.[26] PowerForensics is used to extract and identify various Windows forensic artefacts, showcasing both its advantages and disadvantages.

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, data breach,

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.

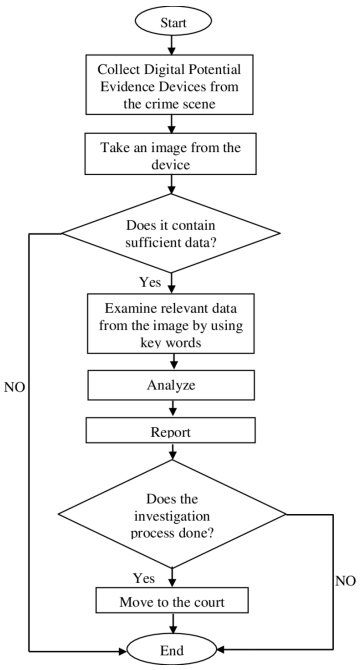
3. Recommendation: Technical explanation for unified cybercrime investigation platforms: Create and put into use systems that seamlessly combine different hardware and software capabilities. These platforms ought security information sharing to be scalable, adaptable, and interoperable so that investigators 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 software 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. 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