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.[1] 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.[1] 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.[2]

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.[3] 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.[3] 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.[3] 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.[4]

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. [4]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: Simple Life Example: Take a look at a Swiss Army knife, which integrates a knife, screwdriver, and bottle opener into one little instrument. A unified cybercrime investigation platform, like the Swiss Army knife, combines several tools, such as digital forensics, network analysis, and malware analysis, into one comprehensive solution, making it simpler for investigators to carry out their duties effectively.

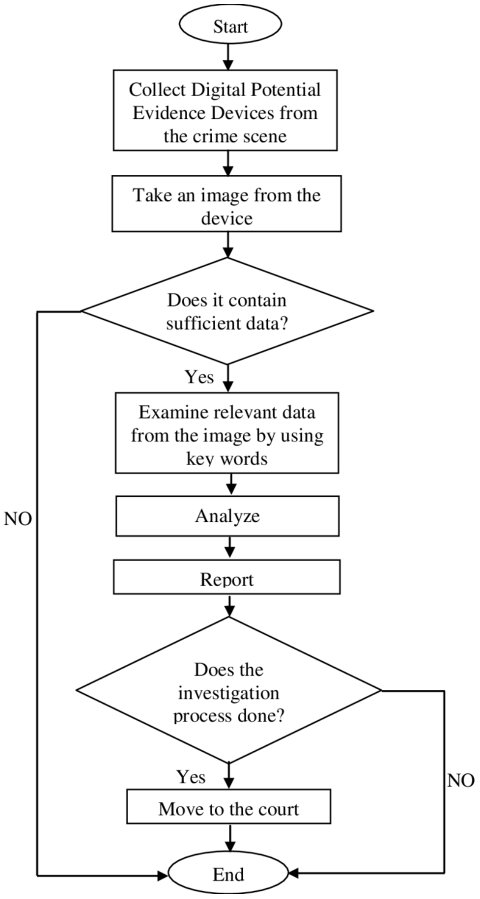
Start
Collect Digital Potential Evidence Devices from the crime scene
Take an image from the device
Does it contain sufficient data?
Yes
NO
Examine relevant data from the image by using key words
Analyze
Report
Does the investigation process done?
Yes
NO
Move to the court
End

Fig 1[5]

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.[6]

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.

Reference:

[1] 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/

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

[3]“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.

[4]“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

[5] *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.

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