Literature Review

The rise in cybercrime has led to the creation of a diverse array of software and hardware solutions, designed to assist law enforcement, cybersecurity experts, and digital forensics specialists in conducting thorough and streamlined investigations. This literature review seeks to offer a comprehensive overview of the current software and hardware tools employed in cybercrime investigations, emphasizing their functionalities, strengths, and drawbacks.

1. 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 by OpenText is a digital forensic platform designed to empower law enforcement personnel in decrypting, amassing, and safeguarding crucial data and evidence from a diverse array of devices. This solution enables the revelation of concealed, erased, or altered evidence across multiple origins, including computers, social media platforms, cloud services, and IoT/mobile devices. EnCase Forensic goes further by incorporating AI-driven workflows and image analysis, streamlining investigations through intelligent automation. [1]

1. Forensic ToolKit (FTK):

AccessData offers a user-friendly forensic software tool with a simple one-touch interface, making it accessible and budget-friendly. The latest FTK version is even more user-friendly, and AccessData has introduced the ACE certification based on this software. FTK has an automated complex search setup, simplifying the process. For example, clicking the Email button instantly retrieves emails. The FTK report generator efficiently creates useful reports within the software, while investigators retain control when needed.[2]

1. Autopsy:

Autopsy is a free and open-source digital forensics platform with a user-friendly interface. It simplifies the utilization of various open-source tools from The Sleuth Kit. This software aids law enforcement, military, and corporate analysts in investigating computer-related incidents. It allows users to examine and highlight relevant data from forensic searches on computer volumes. Basis Technology Corp. primarily maintains the tool, collaborating with community programmers.[3]

1. 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:

FRED, or Forensic Recovery of Evidence Device, is a potent workstation used for securely handling, preserving, and analyzing data from hard drives and other media. These workstations are highly regarded for their scalability and superior quality. FREDs often complement forensic software like EnCase and FTK. Notably, FRED systems are distinct for being the sole forensic workstations with built-in features like hardware write blockers for IDE, SATA, and SAS drives, as well as USB3, Firewire, and MultiMedia/Memory Card forensic write blockers. [4]

1. Logicube:

Logicube provides exceptionally fast disk-to-disk and disk-to-image transfer solutions, with speeds of up to 4 gigabytes per minute, offering significant time savings for data acquisition. Their data capture equipment not only securely retrieves data from a target media but also performs real-time integrity checks to ensure a reliable forensic copy. These devices are versatile, featuring various interfaces, and often come in a convenient portable field kit setup.[2]

1. Write Blockers:

Write blockers, such as those offered by Tableau and WiebeTech, prevent data alteration during the acquisition of digital evidence. They ensure data integrity while acquiring evidence from various storage devices.[5]

The field of cybercrime investigation has greatly benefited from the continuous development of software and hardware tools. These tools, ranging from digital forensics and network analysis software to specialized malware analysis and hardware imaging devices, have enabled investigators to uncover evidence, track down cybercriminals, and build strong cases for legal action. However, as cybercriminals evolve their techniques, these tools must continue to evolve as well to ensure the effectiveness of cybercrime investigation efforts. Further research and development are necessary to address emerging challenges and enhance the capabilities of these tools. paraphrase and change it.

References

1.EnCase Forensic. (n.d.). GetApp. <https://www.getapp.ca/software/2051469/encase-forensic>

2. CyberSecurityMag. (2021). 10 Best Tools for Computer Forensics in 2021. *Cyber Security Magazine*.<https://cybersecuritymag.com/computer-forensics-tools/>

3. Tathagat. (2021). Introduction To Autopsy | An Open-Source Digital Forensics Tool. *CYBERVIE*. <https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/>

4. *Secure, Save and Analyse data with the FRED Workstation - DataExpert EN*. (n.d.). <https://www.dataexpert.eu/products/forensic-hardware-digital-intelligence/fred-workstation/>

5. *Write blockers - CRU*. (2020, December 2). CRU. <https://www.cru-inc.com/data-protection-topics/write-blockers/>