# SURVEY AND COMPARE THE USE OF SOFTWARE AND HARDWARE TOOLS IN CYBERCRIME INVESTIGATIONS

Raghavendran Raghunathan
Information Systems Security
Concordia University, Montreal, Canada
raghavorton21@gmail.com

Arun Prasad Karunanithi
Information Systems Security
Concordia University, Montreal, Canada
karunanithiarunprasad@gmail.com

Hari Krishna Anala
Electrical and Computer Engineering
Concordia University, Montreal, Canada
harikrishnaanala@gmail.com

Sree Satya Vanka
Electrical and Computer Engineering
Concordia University, Montreal, Canada
vankasreesatya@gmail.com

Venkatalaxmi Sai Durga Gadde
Electrical and Computer Engineering
Concordia University, Montreal, Canada
saidurgagadde@gmail.com

Abdul Aziz Midthuru
Electrical and Computer Engineering
Concordia University, Montreal, Canada
abdulazizmidthuru@gmail.com

Nethra Sri Tangootor Balaji
Information Systems Security
Concordia University, Montreal, Canada
tbnethrasri@gmail.com

***Abstract*—With advancement in technology, crime has not been limited to traditional crimes. The 21st century has been characterized by massive innovations that have led to various ways the people interact. Cybercrimes have been growing progressively with development of newer and sophisticated technologies day by day. It has become an escalating concern in today's digital age where effective investigation techniques are required to combat cybercrimes. Digital forensic tools are used to identify and analyze cybercriminals.**

**This report presents a comprehensive survey and comparative analysis of different software and hardware tools used in cybercrime investigations. This study outlines the critical role of software tools like digital forensic software, network forensic tools, memory forensic tools, malware analysis tools and log analysis software. It also explains the significance of hardware tools like write blockers, hardware imagers, network capture hardware and GPS tracking devices. As this field of cybercrime is evolving, the knowledge on effective integration of tools is required to combat digital or cyber threats by cybersecurity professionals and law enforcement agencies. The analysis of various forensic tools mentioned in this report can be used to assist the investigators in selecting the appropriate tool.**

***Index Terms*—Cybercrime, Digital Forensics, Software Tools, Hardware Tools, Cyber Threats, Cybersecurity, Network Forensic Tools.**

## I. INTRODUCTION

Cybercrime refers to many criminal activities that are carried out using computers, networks, mobile phones, and the internet. Cybercriminals use technologies as a tool with the intention of causing harm, disruption, or some kind of financial gain. There are various cybercrimes in which a few of them are hacking,

identity thefts, phishing, online frauds , cyber bullying, data breaches, Denial of service (DoS) attacks and many more. As the technology advances , scope for cybercrime also increases , posing significant challenges to individuals, organizations, and governments worldwide.

Cybercrime investigation is the process of identifying, analysing, and mitigating malicious activities that occur in cyberspace and computer-based crimes. There are a wide variety of specialized tools and techniques which are used by cyber security professionals to investigate different cybercrimes. Cybercrime investigators who investigate the above cybercrimes, are very crucial in ensuring safety and security of digital systems, protecting sensitive information and bringing cybercriminals to justice.

When a cybercrime occurs, the attacker leaves a trace which indicates some kind of significant information such as the date and time of attack or tools used to commit that crime. The cybercrime investigator then needs various tools to match the crime and criminal using the evidence left. These cyber-forensic tools are utilized in recovery of data and investigation of the crime by collecting the evidence from devices such as computers or mobile phones. Digital evidence in which information is stored in digital devices like phones in emails, images can be used in courts. There should be proper precautions taken while handling the digital evidence. Authenticity can be questioned as there is a chance of modifying the data in a digital device.

## II. DIGITAL FORENSICS

Digital Forensics is a branch of forensic science which focuses on investigation of material found in digital devices such as mobile phones, networks, or computers. The digital forensic model is characterized by a process which involves Identification, Preservation, Analysis, Documentation of acquired evidence and Presentation. This procedure is followed by the cybercrime investigator to find the criminal.

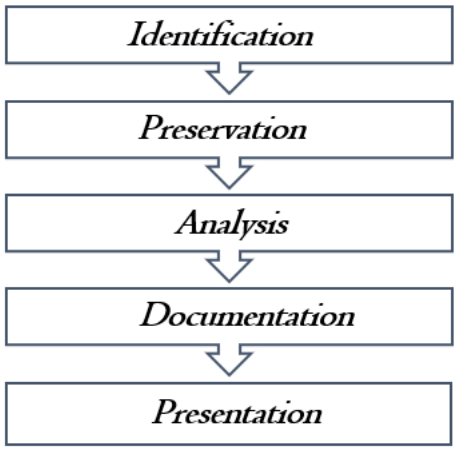


**Fig. 1.** The steps in the process of digital forensics.

1) Identification: This step involves understanding the nature of the case responsibilities are identified. Obtaining legal authorization, such as search warrants and securing the crime scene. Identify the potential sources of digital evidence, such as computers, mobile devices, cloud services, or network logs.

2) Preservation : This step involves Isolating and securing the digital evidence and preventing tampering. Usage of write-blockers or hardware tools to create forensic copies of the original data for analysis.

3) Analysis: This step involves analyzing the forensic copies to identify relevant data. Recovering deleted data using specialized tools and techniques like data carving. Conclusions can be drawn by putting parts of data togethers from the evidence acquired.

4) Documentation: This step involves documenting the entire process thoroughly, including tools and processes used and the results obtained which can be acceptable by courts.

5) Presentation: This step involves summarizing and drawing conclusions. Report is written on the decision made against the person who committed the crime and is saved in the database for future reference.

Digital forensics is a multidisciplinary field that encompasses various branches or subdomains, each specializing in a particular aspect of investigating digital evidence. Some of the key branches of digital forensics include:

### *A. Computer forensics*

This is the most common and well-known branch of digital forensics. It involves the investigation of digital evidence from computers, laptops, servers, and other computing devices. Computer forensics experts analyze data storage media, operating systems, applications, and network logs to identify, preserve, and extract relevant information. It is a specialized field that applies investigative techniques to uncover digital artifacts, traces, and information to support legal proceedings, cybersecurity, incident response, and various investigative tasks. Computer forensics plays a crucial role in identifying, investigating, and preventing cybercrime and other digital offenses.

The major types of computer forensic tools are namely—Encase, CIANE, Digital Forensic framework(DFF) and Forensic Toolkit(FTK).

a. EnCase:

It is a widely used computer forensic tool which was developed by Guidance Software, now part of OpenText. EnCase helps law enforcement agencies and cybercrime investigators by closing cases faster and improving public safety. It is a superior efficient tool with in-depth evidence investigation where the evidence format is court acceptable. With the AI and ML support it can automatically identify images of things used by attackers. Encase helps investigators search and identify evidence from computers and mobile devices.

b. DFF (Digital Forensic Framework):

It is an open-source platform which is used by many organizations, law enforcement agencies, educational institutions to collect, save and disclose the digital evidence in computer forensics. The data will not be modified when collecting and disclosing the evidence. With DFF, there is also a chance of recovering deleted and hidden files and accessing remote devices.

c. CAINE:

It is a LINUX distribution created as a Digital Forensics Project. It offers a computer forensic environment which integrates existing software tools as software modules and provides a user-friendly GUI. It is an open-source tool which can be customized and extended with additional plugins to meet the requirements of cybercrime investigators.

d. FTK:

Forensic Toolkit is a commercial digital investigations solution with a valid license. It is built for speed, stability, and ease of use. It has an intuitive interface, email analysis , processing speeds, and stability which makes it better from the other tools. FTK offers enhanced features like One shared case database, faster searching with a reliable environment and supports multi-threading/multi-core support.

TABLE I
COMPARISION OF COMPUTER FORENSIC TOOLS

| *Features* | *EnCase* | *CAINE* | *DFF* | *FTK* |
|---|---|---|---|---|
| **Developer** | OpenText | CAINE Project | Digital Forensics Framework | AccessData |
| **License** | Commercial | Open-source | Open-source | Commercial |
| **Platform Support** | Windows, Linux, macOS | Windows, Linux (Live CD) | Windows, Linux, macOS | Windows |
| **GUI& Command-Line Interface** | Yes | Yes | Yes | Yes |
| **Third-party Plugins** | Supports limited third-party plugins | No third-party plugin support | Extensive support for third-party tools | Extensive third-party support |
| **File Recovery** | Yes | Yes | Yes | Yes |

### *B. Mobile device forensics*

Mobile device forensics focuses on the examination of smartphones, tablets, and other mobile devices to retrieve data such as call logs, text messages, emails, photos, and application data. As mobile devices become increasingly pervasive, this branch of digital forensics has gained significant importance. The top mobile device forensic tools are mentioned below –

a. Andriller:

It is a popular open source android forensic tool with a powerful set of features used by investigators to extract and analyze digital evidence acquired from android devices. It supports various types of file formats making it a versatile option for cybercrime investigation. Even when the device is locked the investigators can use Andriller to extract the information which becomes an added advantage.

b. Oxygen Forensic Detective:

It is a globally trusted forensic tool used by law enforcement , government agencies, and businesses. This tool helps in extracting data from locked android devices and performing logical and physical extractions to uncover all kinds of evidence including hidden and deleted data. It provides cost effective and powerful analytical solutions compared to other tools

c. MOBILedit:

It is a commercial licensed tool with all-in-one solution for data extraction from mobile phones, smart watches, and cloud. It has an intuitive and user-friendly GUI and supports a wide range of devices. It has extensive features like deleted data recovery, concurrent processing, and stronger security.

d. Autopsy:

It is an open-source mobile device forensic platform which offers faster and easy to use analysis of acquired evidence. It includes a module specifically designed for mobile device forensics. It allows investigators to acquire, analyze and examine the evidence. It is a user-friendly and powerful tool widely used by investigators.

TABLE II
COMPARISION OF MOBILE DEVICE FORENSIC TOOLS

| *Feature* | *Andriller* | *Oxygen Forensic Detective* | *MOBILedit* | *Autopsy* |
|---|---|---|---|---|
| **Developer** | Not specified | Oxygen Forensics | Compelson | Basis Technology Corporation |
| **License** | Commercial | Commercial | Commercial | Open-source |
| **Platform Support** | Windows, Linux (via Wine) | Windows, macOS, Linux | Windows | Windows, Linux, macOS |
| **Deleted Data Recovery** | Yes | Yes | Yes | Yes |
| **Cloud Data Extraction** | No | Yes | Yes | Limited (through plugins) |

### *C. Network forensics*

Network forensics deals with the analysis of network traffic and communication data to identify suspicious activities, intrusions, and cyber-attacks. Investigators use specialized tools to capture and analyze packets to reconstruct network-based events.

a. NetworkMiner:

NetworkMiner is an open-source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files. NetworkMiner can also be used to capture live network traffic by sniffing a network interface. NetworkMiner is primarily designed to run in Windows, but can also be used in Linux.

b. Xplico:

Xplico is an open-source network forensics analysis tool used by cybersecurity professionals to dissect and decode data from captured network traffic. It supports a wide range of protocols, allowing extraction of files, images, videos, and metadata from communication streams. The tool's web-based interface facilitates session reconstruction, metadata analysis, and content extraction, aiding investigators in understanding network activities.

c. NMAP:

It is a free and open-source cybersecurity tool in Cyber that examines IT systems and networks for security

vulnerabilities. It is also known as Network Mapper. Furthermore, it enables professionals to monitor host uptime, map out potential areas of network and service assault, and take major security actions as a result.

d. PyFlag:

FLAG (Forensic and Log Analysis GUI) is an advanced forensic tool for the analysis of large volumes of log files and forensic investigations. PyFlag has a long list of functionality, including the ability to load many different log file types and do forensic analysis on disks and images. PyFlag can also quickly and efficiently analyze network traffic acquired by tcpdump. Because PyFLAG is web-based, it may be deployed on a centralized server and shared with multiple users at the same time. Data is loaded into cases, which separates information.

TABLE III
COMPARISION OF NETWORK FORENSIC TOOLS

| ***Feature*** | ***NetworkMiner*** | ***Xplico*** | ***Nmap*** | ***PyFlag*** |
|---|---|---|---|---|
| **Developer** | Netresec AB | Xplico Team | Gordon Lyon | PyFlag Team |
| **License** | Commercial / Free | Open-source | Open-source | Free and open source |
| **Platform Support** | Windows also works-Linux, macOS | Linux | Cross-platform | Cross-platform |
| **Extracted Content** | Emails, images, files | Files, images | Host information | Network artifact |
| **Offline Analysis** | Yes (PCAP files) | Yes (PCAP files) | No | Yes |
| **Protocol Support** | Extensive | Extensive | Extensive | TCP/IP and others |
| **Malware Detection** | Basic (signature-based) | No | No | No |

*D. Memory forensics*

This branch involves the examination and interpretation of large datasets to identify patterns, anomalies, and evidence related to criminal activities. It is often used in financial crimes and fraud investigations.

The major tools are identified as :

a. Volatility:

It is an open-source memory forensic framework for malware analysis and incident response. It is a very powerful tool written in python which interacts with memory dump files such as viewing the internet history, retrieving commands entered into command prompt and hashed passwords. It can also retrieve SSL keys and certificates.

b. Rekall:

It is an advanced forensic and incident response framework. It is the only free and open-source memory analysis tool which works with windows page files and mapped files. It can be used as a library. With its advanced GUI and plugins, it has been the most powerful memory analysis tool.

c. Memoryze:

Mandiant's Memoryze tool is without question one of the best forensic tools available. It is an incredibly powerful memory analysis suite that should be part of every incident responder's toolkit. It's free, but requires some patience and training to use the tool.

d. Mandiant Redline:

It is a memory forensic tool which is used to analyze memory in the attacker’s system which obtains information about processes and drivers running in memory and collect system metadata, event logs, registry data, network information, all services and running tasks. It provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.

TABLE IV
COMPARISION OF MEMORY FORENSIC TOOLS

| ***Feature*** | ***Volatility*** | ***Rekall*** | ***Memoryze*** | ***Mandiant Redline*** |
|---|---|---|---|---|
| **Developer** | Volatility Team | Rekall Development Team | Guidance Software | FireEye, Inc. |
| **License** | Open-source | Open-source | Open-source | Open-source |
| **Platform Support** | Cross-platform (Windows, macOS, Linux) | Cross-platform (Windows, macOS, Linux) | Windows | Windows |
| **Live Memory Analysis** | Yes (using kernel modules) | Yes (using kernel modules) | No | Yes (using kernel modules) |
| **User-Friendly** | Command-line interface | Command-line and web interface | Graphical interface | Graphical interface |
| **File Carving** | Capable of file carving from memory images | Capable of file carving from memory images | Cannot perform file carving | Capable of file carving from memory images |
| **Community Support** | Active | Active | Limited | Limited |

## III. HARDWARE FORENSIC TOOLS

Hardware tools in forensic analysis refer to specialized devices and equipment used by investigators to acquire,

preserve, and examine digital evidence from hardware devices. There are numerous tools created keeping with forensic analysis in mind such as Forensic Imaging Devices, Write Blockers, Chip-Off Tools, etc...

In this report we showcase the perspective of how legitimate investigators enable the preservation and acquisition of digital evidence while maintaining the integrity of the original data. On the other hand, hackers misuse these same hardware tools for illegal and malicious activities. Hardware tools can be categorized based on their specific functionalities and areas of focus the main categories include Access Control Devices, Password Recovery and Decryption Tools, Metadata Analysis tool, Credit Card fraud devices, Steganography Detection Tools and Digital cameras and Web cameras.

TABLE V
COMPARISION OF HARDWARE FORENSIC TOOLS

| ***Hardware Tool*** | ***Purpose and Functionality*** | ***Usage Information*** | ***Most Used Tool*** |
|---|---|---|---|
| **Forensic Write-Blockers** | Prevents write operations to storage devices, ensuring data integrity during investigation. | Connect between device and analysis system. | Tableau, WiebeTech |
| **Imaging Hardware** | Devices for creating exact copies (forensic images) of digital storage media for analysis. | Requires connecting source and target devices. | Various manufacturers |
| **Tableau TD2u** | Versatile forensic duplicator for disk imaging, drive cloning, and data recovery from various devices. | Offers user-friendly interface for image creation. | Tenable (A part of Guidance Software) |
| **CRU WiebeTech Forensic Field Kit** | Kit with hardware write-blockers and adapters for connecting storage devices to computers for analysis. | Includes write-blockers, cables, and power adapters. | CRU WiebeTech |
| **Logicube Forensic Falcon NEO** | High-speed imaging solution for forensic imaging, cloning, and analysis of digital storage media. | Supports imaging at rapid speeds for efficiency. | Logicube |
| **Cellebrite UFED Touch2** | Mobile forensic tool for extracting and analyzing data from smartphones, tablets, SIM cards, and more. | Requires connecting the device and initiating scan. | Cellebrite |
| **Network Forensics Tools** | Hardware appliances for capturing and analyzing network traffic to detect intrusions and activities. | Deployed within network infrastructure. | Cisco, Plixer (among others) |
| **JTAG/Chip-Off Tools** | Used for physically extracting data from devices by accessing memory chips, bypassing device security. | Requires skilled technicians for chip removal. | Various manufacturers |

## IV. VULNERABILITY TOOLS

The main goal and objective of vulnerability scanning is to identify the potential threats before the hackers try to access the information. Network's security can be maintained by conducting regular scans to have an up-to-date assessment and taking steady approach to enhance the cybersecurity. Moreover, vulnerability scanning helps you meet data protection standards and ensures data processing security.

Vulnerability tools used in cybercrime investigations play a vital role in identifying weaknesses, flaws, and potential entry points within digital systems and networks that malicious actors may exploit. These tools help law enforcement agencies, cybersecurity professionals, and digital investigators uncover vulnerabilities that have been exploited by cybercriminals, gather evidence, and ultimately enhance cybersecurity measures. The scan generates a comprehensive report that outlines all system scans conducted and the vulnerabilities detected, each with a corresponding severity rating. One of the most well-known network vulnerability scanners in the world is Nessus. It enables software that was installed on the PC to be checked for misconfiguration. It also identifies the open ports on the machine and the software version that is currently installed. Additionally, it checks for vulnerabilities that could allow a remote hacker to manipulate or access sensitive data on a system, denial-of-service attacks against the TCP/IP stack,

and PCI DSS evaluations. Acunetix is a program that automatically assesses the security of online applications by searching them for exploitable flaws like SQL Injection and Cross-Site Scripting. Acunetix typically scans any website or online application that may be accessed through a web browser and uses the HTTP/HTTPS protocol.

TABLE VI

COMPARISION OF VULNERABILITY TOOLS

| ***Vulnerability Tool*** | ***Purpose and Functionality*** | ***Major Features*** | ***Platform Support*** | ***License*** |
|---|---|---|---|---|
| **Nessus** | Comprehensive vulnerability assessment tool for identifying security vulnerabilities across systems. | Network, web, and cloud scanning | Cross-platform (Windows, Linux),masOS | Commercial (Free version available), GPL |
| **OpenVAS** | Open-source vulnerability scanner with network and web scanning capabilities. | Network and web scanning | Cross-platform (Windows, Linux) | GNU General Public License (GPL) |
| **Qualys** | Cloud-based platform for vulnerability management, offering real-time assessment and compliance. | Network and web scanning | Cloud-based | Commercial and open source. |
| **Rapid7 Nexpose** | Vulnerability management solution providing insights into security risks and vulnerabilities. | Network, web, and cloud scanning | Cross-platform (Windows, Linux) | Commercial |
| **Acunetix** | Web vulnerability scanner that detects and reports security vulnerabilities in web applications. | Web application scanning | Cross-platform (Windows, Linux) | Commercial |
| **Nikto** | Open-source web server scanner that identifies potential security issues in web servers. | Web server scanning | Cross-platform (Windows, Linux) | Open-source (GNU GPL) |
| **Retina** | Vulnerability management tool for assessing, prioritizing, and remediating security risks. | Network and web scanning | Cross-platform (Windows, Linux) | Commercial |

## V. CONCLUSION

From our survey and research on computer forensic tools, EnCase emerges as a comprehensive solution for evidence acquisition and analysis, empowering investigators to navigate intricate digital landscapes. For network forensics, NetworkMiner stands out with its passive sniffing capabilities, extracting valuable artifacts from captured traffic. In memory forensics, Volatility excels in deep memory analysis, unveiling hidden processes and malware. In the mobile forensics' domain, Oxygen Forensic Detective takes the lead, offering advanced data parsing and decryption features for comprehensive mobile device analysis. These best-in-class tools collectively enable professionals to uncover insights, reconstruct digital incidents, and resolve complex cybercrime investigations with precision and efficacy.

Forensic write-blockers, hardware-based imaging devices, portable forensic workstations, chip-off tools, and JTAG analyzers emerge as the forefront of hardware solutions. These tools collectively ensure impeccable evidence integrity, precise duplication of storage media, on-site investigative capabilities, advanced data extraction from damaged devices, and forensic analysis of embedded systems. Representing the industry's best, these hardware tools empower digital forensics professionals with a robust arsenal to navigate the intricate physical dimensions of investigations, thereby safeguarding evidentiary integrity and elevating the efficacy of cybercrime mitigation strategies.

In the analysis and comparison of vulnerability assessment tools reveal the vital contributions of the industry's top choices. Nessus excels in comprehensive vulnerability scanning across diverse systems, Qualys provides real-time assessment and compliance management for proactive risk mitigation, OpenVAS offers open-source versatility for thorough vulnerability analysis, Burp Suite stands out for advanced web application testing and security assessment, and Nmap's adept network mapping capabilities empower precise identification of potential security gaps. By harnessing the strengths of these tools, cybersecurity professionals can adeptly identify, prioritize, and address vulnerabilities, enhancing their organization's resilience against evolving cyber threats and ensuring the protection of critical assets.

***Github URL for the project:***

https://github.com/sai-durga/INSE6610-2023-Project-Group9.git

## ACKNOWLEDGMENT

We would like express our sincere gratitude to our Professor Dr. Ivan Pustogarov, for giving us this opportunity to research on the tools used by cybercrime investigators. His guidance, suggestions and motivation has inspired us throughout the course. Being able to work and study in this course has been a huge honor and privilege.

## REFERENCES


[1] "OpenText Encase Forensic," OpenText. https://www.opentext.com/products/encase-forensic#features

[2] "PRODUCT OVERVIEW." Available: https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encase-forensic-en.pdf

[3] Caine, "CAINE Live USB/DVD - computer forensics digital forensics," Caine-live.net, 2018. https://www.caine-live.net/

[4] "Digital Forensic Software," Exterro. https://www.exterro.com/ftk-product-downloads (accessed Aug. 03, 2023).

[5] Netresec, "NetworkMiner - The NSM and Network Forensics Analysis Tool ⛏," Netresec, 2019. https://www.netresec.com/?page=networkminer

[6] Nmap, "Nmap," Nmap.org, 2017. https://nmap.org/

[7] "Xplico – About," www.xplico.org. https://www.xplico.org/about

[8] "py4n6/pyflag," GitHub, Feb. 15, 2023. https://github.com/py4n6/pyflag

[9] "Google Code Archive - Long-term storage for Google Code Project Hosting.," code.google.com. https://code.google.com/archive/p/pyflag/ (accessed Aug. 05, 2023).

[10] "How to use Andriller - Forensic Tool [SOLVED] | GoLinuxCloud," www.golinuxcloud.com, Feb. 17, 2023. https://www.golinuxcloud.com/andriller-android-forensic-tool/

[11] "Oxygen Forensic® Detective," Oxygen Forensics. https://oxygenforensics.com/en/products/oxygen-forensic-detective/

[12] "MOBILedit Forensic," MOBILedit. https://www.mobiledit.com/mobiledit-forensic

[13] "Rekall At a Glance - Rekall Forensics," www.rekall-forensic.com. http://www.rekall-forensic.com/documentation-1/rekall-documentation/rekall-at-a-glance (accessed Aug. 02, 2023).

[14] L. Williams, "What is Digital Forensics? History, Process, Types, Challenges," Guru99.com, Oct. 23, 2019. https://www.guru99.com/digital-forensics.html

[15] L. Williams, "What is Cybercrime? Types, Tools, Examples," www.guru99.com, Jun. 30, 2023. https://www.guru99.com/cybercrime-types-tools-examples.html#3 (accessed Aug. 02, 2023).

[16] "Blossom-Hands-on exercises for computer forensics and security." Accessed: Aug. 08, 2023. [Online]. Available: https://www.mmu.ac.uk/media/mmuacuk/content/documents/school-of-computing-mathematics-and-digital-technology/blossom/AutomatedAnalysisExtending-Capabilities.pdf

[17] GeeksforGeeks, "CAINE Forensic Environment," GeeksforGeeks, May 31, 2020. https://www.geeksforgeeks.org/caine-forensic-environment/

[18] "Understanding Digital Forensics: Process, Techniques, and Tools," BlueVoyant. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools#:~:text=The%20main%20types%20of%20digital%20forensics%20tools%20include%20disk%2Fdata

[19] "Part 2: Forensic Hardware Tools | Engineering360," www.globalspec.com. https://www.globalspec.com/reference/31783/203279/part-2-forensic-hardware-tools

[20] A. Saxena, "Top 15 Cybersecurity tools You Must Know in 2023," Sprinto, Mar. 11, 2023. https://sprinto.com/blog/best-cybersecurity-tools/ (accessed Aug. 02, 2023).

[21] "Top 11 Most Powerful CyberSecurity Software Tools In 2019," Softwaretestinghelp.com, Aug. 21, 2019. https://www.softwaretestinghelp.com/cybersecurity-software-tools/

[22] https://www.knowledgehut.com/blog/security/cyber-security-tools

[23] Jai Narayan Goel, B.M. Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, Procedia Computer Science, Volume 57, 2015, Pages 710-715, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.07.458.

[24] Bairwa, Sheetal & Mewara, Bhawna & Gajrani, Jyoti. (2014). Vulnerability Scanners-A Proactive Approach To Assess Web Application Security. International Journal on Computational Science & Applications. 4. 10.5121/ijcsa.2014.4111.

[25] International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014 DOI:10.5121/ijcsa.2014.4111

[26] Alazmi, Suliman & Leon, Daniel. (2022). A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3161522.