Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 06 | June-2026
ISSN (O) 3107-6696

An Open-Source Framework for Windows System Data Acquisition and Forensic Analysis

MAYURI V. K.

Jeppiaar University

Introduction - The rapid growth of digital technologies has significantly transformed modern society, enabling individuals and organizations to store, process, and exchange large amounts of information through computer systems. However, this technological advancement has also increased the risk of cybercrimes such as data theft, malware attacks, unauthorized access, and digital fraud. As cyber threats continue to evolve, the need for effective methods to investigate and analyse digital evidence has become increasingly important. Digital forensics plays a critical role in identifying, collecting, preserving, and analysing electronic data from computer systems to support cyber security investigations and legal proceedings. *(Casey, 2011)*

Digital forensic investigation involves examining digital devices such as computers, storage media, and networks in order to uncover evidence related to cyber incidents. Investigators must follow systematic procedures to ensure that digital evidence is collected in a reliable and legally admissible manner. One of the most important aspects of digital forensics is data acquisition, which refers to the process of capturing and preserving data from a computer system without modifying the original evidence. After acquiring the data, investigators perform forensic analysis to identify system artifacts, recover deleted files, examine user activity, and detect potential malicious behaviour. *(Carrier, 2005)*

Among various operating systems, Microsoft Windows is one of the most widely used platforms in both personal and enterprise environments. Due to its popularity, Windows systems are frequently targeted by cybercriminals who attempt to exploit vulnerabilities, install malware, or gain unauthorized access to sensitive information. As a result, forensic investigators must have effective tools and frameworks to collect and analyse digital evidence from Windows systems. This process often involves creating forensic images of storage devices, analysing file systems such as NTFS and FAT, and examining system artifacts including registry entries, log files, and application data.

Digital forensic investigations typically require specialized software tools to perform tasks such as disk imaging, file recovery, artifact extraction, and system analysis. Many commercial forensic tools provide advanced capabilities but require expensive licenses, which may not be affordable for educational institutions, students, and small organizations. Therefore, open-source and freely available forensic tools have become an important alternative for conducting digital investigations. These tools provide essential forensic capabilities while allowing researchers and investigators to perform analysis without significant financial investment.

This project focuses on developing an open-source framework for Windows system data acquisition and analysis using freely available forensic tools. The framework integrates tools such as FTK Imager for forensic disk imaging and OS Forensics for system artifact analysis. By combining these tools within a structured investigation process, the framework enables investigators to collect digital evidence, analyse system activities, and recover important forensic artifacts from Windows environments. *(Sammons, 2015)*

The primary goal of this research is to demonstrate that open-source and freely available forensic tools can be effectively used to perform digital investigations. The proposed framework provides a cost-effective solution for analysing Windows systems while maintaining the integrity and reliability of digital evidence. This approach is particularly useful for students, researchers, and cyber security professionals who require practical methods for performing digital forensic analysis without relying on expensive commercial software. (Nelson et al., 2019)

REVIEW OF LITERATURE

2.1 A Framework Analysis of the Open-Source Software Development Paradigm in 2000 by Joseph Feller and Brian Fitzgerald. Feller and Fitzgerald (2000) examined the concept of Open-Source Software (OSS) and its impact on modern software development. The study explains that open-source systems allow developers to freely access, modify, and distribute source code, unlike proprietary software where the code is restricted. The authors proposed a framework combining Information Systems Architecture and Soft Systems Methodology to analyse OSS development. Their framework examines aspects such as what the system is, why it is developed, how development occurs, and who contributes to it. The research highlights that OSS projects rely on global collaboration, where developers from different locations work together through internet-based tools. This collaborative model enables continuous improvement through community

contributions and bug fixes. The study also notes that open-source development improves software quality, flexibility, and cost efficiency. Developers participate to gain experience, enhance skills, and build professional reputation. The findings support the idea that open-source approaches can be used to develop cost-effective frameworks for Windows system data acquisition and analysis. (Feller & Fitzgerald, 2000)

2.2 First Steps, Lasting Impact: Platform-Aware Forensics for the Next Generation of Analysts in 2026 by Vinayak Jain, Sneha Sudhakaran, and Saranyan Senthivel. Digital forensics is essential for investigating cybercrimes by collecting and analysing digital evidence from computer systems. Jain, Sudhakaran, and Senthivel studied how forensic evidence acquisition differs between Windows and Linux operating systems. The research explains that factors such as operating system architecture, file systems, encryption methods, and tool compatibility influence forensic investigations. The authors highlight two key methods: disk forensics, which analyses stored data, and memory forensics, which examines volatile data in RAM. Tools such as FTK Imager and Autopsy are commonly used to create disk images and recover deleted files. The study also discusses the role of open-source forensic tools like The Sleuth Kit and Volatility for analysing disk and memory artifacts. Experiments using virtual machines and malware samples showed that system configuration and malware type affect evidence visibility. The research emphasizes the importance of evidence integrity using hash functions such as SHA-256. Overall, the study supports the use of open-source tools to develop efficient frameworks for Windows system data acquisition and forensic analysis. (Jain, Sudhakaran, & Senthivel, 2026)

2.3 The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory in 2014 by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters. Memory forensics is an important technique in digital investigations because many cyber threats operate in volatile memory (RAM) instead of leaving traces on disk. Ligh, Case, Levy, and Walters explain how memory analysis helps investigators detect malicious processes, hidden malware, and suspicious system activities. The study highlights that attackers often use techniques such as rootkits, process injection, and in-memory malware to avoid detection. These threats usually disappear when the system is restarted, making memory acquisition essential. The authors introduce the Volatility framework, an open-source tool used to analyse memory dumps and extract information such as running processes, network connections, and loaded drivers. The research also explains that Volatility uses a modular plugin architecture, allowing investigators to extend its capabilities. Proper memory acquisition methods are necessary to maintain forensic integrity and evidence reliability. The study concludes that combining memory analysis with disk forensics improves cybercrime investigations and supports the development of open-source frameworks for Windows system data acquisition and analysis. (Ligh, Case, Levy, & Walters, 2014)

2.4 A Road Map for Digital Forensic Research in 2001 by Gary Palmer. Gary Palmer introduced an early framework for digital forensic investigations through the Digital Forensic Research Workshop (DFRWS). The study provides a structured approach for conducting reliable digital forensic analysis. The DFRWS model includes six phases: identification, preservation, collection, examination, analysis, and presentation. These stages guide investigators from discovering digital evidence to presenting findings in legal environments. The research emphasizes maintaining evidence integrity during the forensic process to ensure reliable results. Techniques such as hashing are recommended to verify that digital evidence remains unchanged. The study also highlights the role of forensic tools in acquiring disk images and analysing file systems. Over time, the development of open-source forensic tools has made digital investigations more accessible and cost-effective. The DFRWS model has influenced many modern forensic frameworks and supports the development of open-source systems for Windows data acquisition and analysis. (Palmer, 2001)

2.5 Sleuth Kit and Autopsy: Open-Source Digital Forensics Tools in 2001 by Sleuth Kit. Labs. The Sleuth Kit (TSK) and Autopsy are widely used open-source digital forensic tools for analysing computer systems and disk images. The Sleuth Kit functions mainly as a command-line toolset, while Autopsy provides a graphical interface that simplifies the forensic investigation process. These tools support file systems such as NTFS and FAT, which are commonly used in Windows environments. Investigators can analyse file metadata, recover deleted files, and examine directory structures using The Sleuth Kit. Autopsy enhances these capabilities by offering features such as keyword search, timeline analysis, and artifact recovery. These functions help investigators detect suspicious activities and reconstruct digital events. One major advantage of these tools is their open-source nature, allowing researchers to modify and extend their capabilities. They are widely used in academic research and cybersecurity training environments. Overall, these tools support the development of open-source frameworks for Windows system data acquisition and forensic analysis. *(Carrier, 2001)*

2.6 Volatility: Advanced Memory Forensics Framework in 2014 by Volatility Foundation.
Volatility is a widely used **open-source framework for memory forensics** that allows investigators to analyse raw memory dumps from computer systems. It helps cybersecurity professionals and researchers detect **malicious activities and hidden threats** within system memory. The framework focuses on analysing **volatile data in RAM**, such as running processes, network connections, loaded drivers, and encryption keys. Since many cyber threats operate only in memory, analysing RAM is important for identifying hidden malware. Volatility uses a **modular plugin architecture**, enabling investigators to perform tasks such as process analysis, registry examination, and malware detection. It also supports multiple operating systems including **Windows, Linux, and macOS**. The framework is particularly useful in **Windows forensic investigations**, where malware often hides in memory structures. Because Volatility is open-source, researchers can modify it and develop new plugins. Overall, the framework plays an important role in **open-source systems for Windows data acquisition and forensic analysis**. *(Volatility Foundation, 2014)*

2.7 Live Forensics Analysis of LINE App on Proprietary Operating System established by Imam Riadi, Sunarti, Muhammad Erman Syah Rauli in 2019. This study focuses on the application of **live digital forensic techniques** to analyse user activities in the LINE messaging application. The authors explain that live forensics allows investigators to collect data from a system while it is still running. This method is important for obtaining **volatile data such as RAM contents, active processes, and network information**. The researchers used tools like RAM Capturer to capture memory data and analyse communication artifacts. Their work shows that valuable digital evidence such as chat messages and login information can be recovered from system memory. The study also highlights the importance of preserving evidence integrity during acquisition. The research contributes to digital forensic investigations by demonstrating effective techniques for live system analysis. These findings support the need for efficient forensic frameworks capable of acquiring and analysing system data in real time. The approach is relevant for developing **open-source Windows forensic frameworks** for data acquisition and investigation. (Riadi, Sunarti, & Rauli, 2019)

2.8 A Study on Digital Forensic Tools discovered by Kambiz Ghazinour, Deep M. Vakharia, Krishna Chaitanya Kannaji, Rohit Satya Kumar at 2017. This research provides an overview of various **digital forensic tools used in cybercrime investigations**. The authors discuss how forensic tools assist investigators in collecting, preserving, and analysing digital evidence from computer systems. The paper examines different tools used for disk imaging, memory acquisition, and data recovery. It also highlights the importance of maintaining evidence integrity to ensure that collected data remains legally acceptable. The study compares several tools

based on efficiency, reliability, and usability. The authors emphasize that selecting appropriate forensic tools is essential for successful investigations. The research also identifies challenges related to cost and accessibility of commercial forensic software. As a result, the study encourages the use of **open-source forensic solutions** that can provide similar capabilities. This work supports the development of frameworks that allow investigators to perform Windows system data acquisition and analysis using freely available tools. *(Ghazinour et al., 2017)*

2.9 Digital Forensics and Incident Response proposed by Kevin Mandia, Matthew Pepe, Jason Luttgens in 2014. This research explains the importance of **digital forensics and incident response techniques** in identifying and investigating cyber incidents. The authors discuss how digital evidence can be collected from computer systems, network logs, and storage devices. The study highlights different stages of a forensic investigation, including evidence identification, acquisition, analysis, and reporting. It emphasizes the need for proper tools and procedures to maintain the reliability of collected data. The researchers also describe how forensic tools can be used to analyse system activities and detect malicious behaviour. The paper provides insight into handling security incidents in enterprise environments. It stresses the role of systematic investigation methods in identifying attackers and recovering compromised systems. The study contributes to the field by explaining practical approaches for system investigation. These concepts are useful in designing **frameworks for Windows system data acquisition and analysis**. *(Mandia, Pepe, & Luttgens, 2014)*

2.10 Digital Forensic Investigation: Principles and Practices by John Sammons in 2015

This study explains the **fundamental principles of digital forensic investigations** and the processes involved in analysing digital evidence. The author describes the stages of forensic investigation, including evidence identification, collection, preservation, analysis, and documentation. The research highlights the importance of using reliable forensic tools and maintaining proper chain-of-custody procedures. It also discusses methods used to recover deleted or hidden data from computer systems. The study emphasizes the need for structured investigation techniques to ensure accurate results. The author also explores the challenges faced by investigators while handling large volumes of digital data. The research encourages the use of standardized forensic practices during cybercrime investigations. The concepts presented help investigators analyse system activities effectively. These principles support the creation of **open-source frameworks for Windows system data acquisition and analysis.** ***(Mandia, Pepe, & Luttgens, 2014)***

AIM & OBJECTIVES

AIM

The aim of this research is to design and evaluate an open-source framework for efficient and forensically sound acquisition and analysis of data from Windows-based systems, ensuring data integrity and evidentiary reliability.

OBJECTIVES OF THE STUDY

- To develop a structured open-source framework for acquiring volatile and non-volatile data from Windows systems.
- To evaluate the effectiveness of forensic tools such as Autopsy, Volatility, and FTK Imager in extracting digital evidence (Casey, 2011).
- To ensure forensic integrity through hashing, logging, and adherence to chain-of-custody principles (Kent et al., 2006).

METHODOLOGY

4.1 Research Design

This research adopts an experimental and analytical design. The experimental component involves simulating cyber incidents on Windows systems, while the analytical component focuses on interpreting collected forensic artifacts. A controlled environment ensures repeatability and minimizes external interference (Casey, 2011).

4.2 Sample and Sampling Technique

The study employs purposive sampling to select systems configured to generate relevant forensic artifacts.

- **Sample Type:** Windows 10 and Windows 11 systems
- **Sample Size:** 5–10 systems
- **Environment:** Virtual machines and physical systems
- **Sampling Method:** Purposive sampling

Each system is configured with specific scenarios such as normal usage, malware infection, unauthorized access, and data deletion.

4.3 Sample Collection (Data Acquisition)

Data acquisition follows established forensic principles to ensure evidence integrity.

Types of Data Collected

Volatile Data:

- RAM contents
- Running processes
- Network connections

Non-Volatile Data:

- Disk images
- Registry files
- Event logs
- File system metadata

Tools Used

- FTK Imager – disk imaging
- Volatility – memory analysis
- Autopsy – disk analysis

Procedure

1. Isolate the system from networks
2. Acquire volatile data first
3. Capture memory dumps
4. Perform disk imaging using write blockers
5. Generate hash values (MD5, SHA-256)
6. Maintain detailed logs

These steps align with forensic best practices for maintaining data integrity (Kent et al., 2006).

4.4 Data Analysis Techniques

- **Memory Analysis:** Detect hidden processes and malware using Volatility (Ligh et al., 2014)
- **Disk Analysis:** Recover deleted files using Autopsy (Carrier, 2005)
- **Registry Analysis:** Identify persistence mechanisms
- **Log Analysis:** Examine Windows Event Logs
- **Timeline Analysis:** Reconstruct system events

OBSERVATION

Disk Image Acquisition

FTK Imager was used to create a forensic image of the Windows system.

A complete bit-by-bit copy of the storage device was successfully generated.

The acquisition process was performed without altering the original data.

The integrity of the evidence was preserved throughout the imaging process.

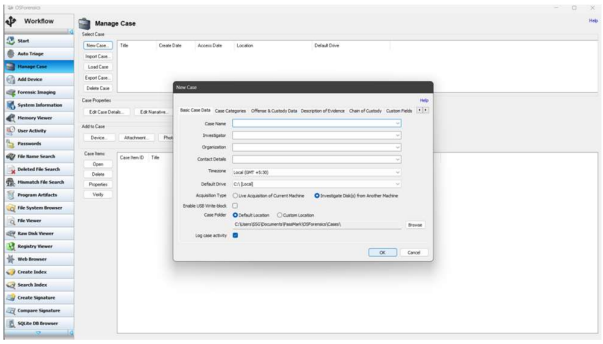

Image: 1 Creating a case.

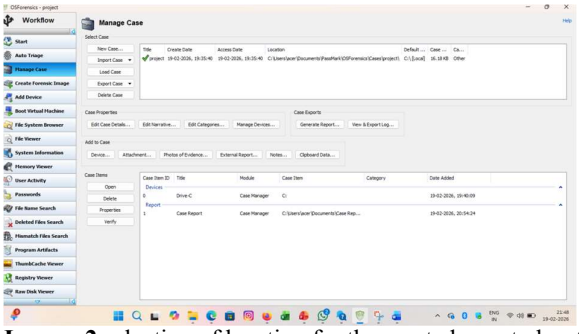

Image: 2 selection of location for the created case to be stored.

File System Structure Analysis

System directories, user folders, and application files were visible.

Both system-generated and user-created files were accessible.

The structure provided insight into how data is organized within the system.

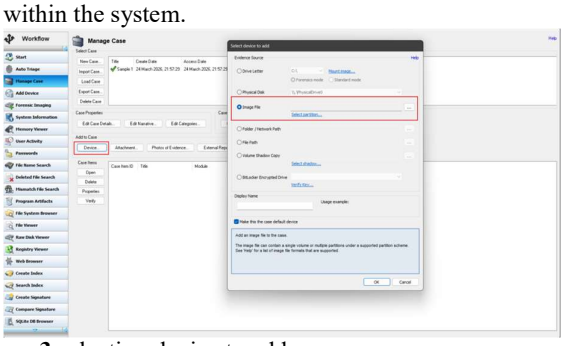

Image: 3 selecting device to add

Analysis of Allocated and Unallocated Space

The tool provided access to both allocated and unallocated disk space.

Unallocated space contained traces of deleted files.

Deleted data was not permanently erased from the storage device.

This allowed recovery and identification of previously removed files.

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 06 | June-2026
ISSN (O) 3107-6696

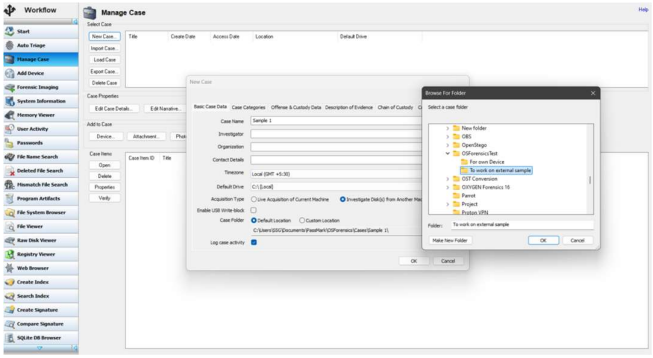

Image: 4 browse for folder

Recovery of Deleted Files

Deleted files were successfully identified and recovered.
Different file types such as documents, images, and temporary files were observed.
Recovery demonstrated that data remnants persist even after deletion.
This is crucial for retrieving hidden or intentionally removed evidence.

File Metadata Examination

File metadata such as timestamps was analysed.
Key timestamps included:

Creation time
Modification time
Last access time

Metadata provided valuable information about user activity.
It helped in understanding file usage patterns and timelines.

Identification of System Artifacts

Various system artifacts were identified.
These included:

- Log files
- Hidden system files
- Application data
- Artifacts provided insights into system operations and user interactions.
- They played an important role in reconstructing system events.

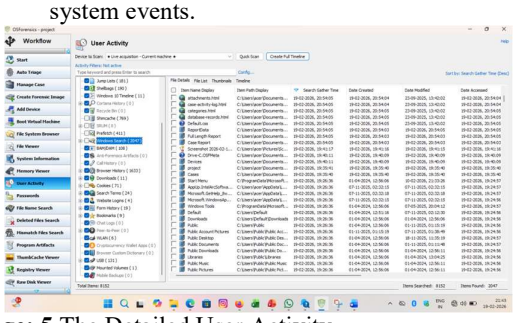

Image: 5 The Detailed User Activity

Evidence Integrity Confirmation

No changes were observed in the forensic image.
This confirmed that the evidence remained intact throughout the investigation.
Ensured that the findings are reliable and admissible.

Summary of Observations

FTK Imager effectively acquired and preserved digital evidence.
Deleted and hidden data could be successfully identified.
System artifacts and metadata provided meaningful insights into system activity.
The overall process confirmed the effectiveness of forensic tools in Windows investigations.

Learned Outvomes

The study produced several key findings:

1. There is a direct relationship between increased digital usage and the rise in cybercrime incidents.
2. Phishing and malware attacks are among the most common types of cyber threats.
3. A significant percentage of users lack basic cybersecurity awareness.
4. Weak authentication methods (such as simple passwords) contribute heavily to security breaches.
5. Organizations with updated security systems experience fewer cyber incidents.
6. Legal provisions exist but are not always effectively implemented due to technical complexities.
7. Awareness programs and training significantly reduce the risk of cyber threats.
8. Data protection measures such as encryption and firewalls improve overall system security.
9. Insider threats and human errors remain a major concern.
10. Preventive strategies are more effective than reactive measures in controlling cybercrime.

These results demonstrate that cybersecurity requires both technological solutions and behavioural changes among users

DISCUSSION

The study highlights the growing dependence on digital technologies and the corresponding rise in cybercrime activities. The findings indicate that increased internet penetration, digital transactions, and cloud-based storage systems have significantly expanded the attack surface for cybercriminals. Various forms of cybercrime such as phishing, malware attacks, identity theft, and unauthorized data access are becoming more sophisticated and frequent.
The analysis reveals that lack of awareness among users, weak password practices, and insufficient cybersecurity infrastructure are major contributing factors. Organizations, especially small and medium enterprises, often lack advanced security mechanisms, making them vulnerable targets. Additionally, legal frameworks, though evolving, still face challenges in enforcement due to jurisdictional issues and rapid technological advancements.

Another important aspect identified is the role of human error in cybersecurity breaches. Even with advanced security systems, negligence and lack of training can lead to significant vulnerabilities. The study also emphasizes the importance of digital literacy and continuous monitoring systems to mitigate risks.

Overall, the discussion shows that cybercrime is not just a technical issue but a socio-economic and legal concern requiring a multi-disciplinary approach involving technology, law enforcement, and public awareness.

CONCLUSION

Cybercrime has become one of the most significant challenges in today's digital world due to the increasing dependence on technology and internet-based services. Although modern technological developments have improved communication, business, education, and daily life, they have also created opportunities for cybercriminals to exploit digital vulnerabilities. Threats such as hacking, phishing, ransomware, identity theft, and online financial fraud continue to increase, affecting individuals, organizations, and governments across the globe. This study highlights the importance of adopting a strong and preventive cybersecurity strategy that includes effective legal measures, advanced security technologies, and increased public awareness. Organizations should strengthen their security infrastructure through tools like encryption, firewalls, and regular system monitoring while also training employees to recognize and respond to cyber threats. At the same time, individuals must practice safe online behavior by protecting personal information, using strong passwords, and remaining cautious while accessing unknown links or websites. The study also emphasizes the importance of cooperation among governments, law enforcement agencies, private sectors, and international organizations in tackling cybercrime effectively, as many cyber threats operate beyond geographical boundaries. In addition, educational institutions and workplaces should promote cybersecurity awareness programs to help people understand digital risks and responsible internet usage. Emerging technologies such as artificial intelligence and machine learning can further improve cyber defence systems by identifying suspicious activities more efficiently. As digital transformation continues to expand into every aspect of society, maintaining cybersecurity will become increasingly essential for protecting privacy, financial stability, and national security. Therefore, a combined effort involving technology, awareness, policy implementation, and international cooperation is necessary to build a safer and more secure digital environment for the future.

REFERENCES

1. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
2. Al-Zour, A., et al. (2016). *Mobile forensic investigations: A guide to evidence collection, analysis, and presentation*. McGraw-Hill Education.
3. Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model*. Makerere University Press.
4. Lessard, J., & Kessler, G. C. (2010). *Android forensics: Investigation, analysis and mobile security for Google Android*. Syngress.
5. Khan, S. U., & Khan, R. (2019). *Handbook of digital forensics and investigation*. Wiley.
6. Hoog, A. (2011). *Android forensics: Investigation, analysis, and mobile security for Google's Android*. Elsevier.
7. Rashid, A., et al. (2020). *Advanced mobile forensics: Deep dive into Android data analysis*. Springer.
8. Zdziarski, J. (2011). *Android forensics: Investigating the Android operating system*. O'Reilly Media.
9. Rogers, M. (2006). *Computer forensics: Principles and practice*. Pearson Education.
10. Engebretson, P. (2013). *The basics of digital forensics*. Syngress.
11. Garfinkel, S. (2010). *Digital forensics: Threatscape and best practices*. Wiley.
12. Anderson, R. (2020). *Security engineering*. Wiley.
13. Whitman, M., & Mattord, H. (2021). *Principles of information security*. Cengage.
14. Kaspersky Lab Reports. (2023). *Cyber threat landscape*.
15. Symantec (Broadcom). (n.d.). *Internet security threat report*.
16. ENISA. (2022). *Threat landscape report*.
17. OECD. (2021). *Digital security risk management*.
18. Cisco. (2023). *Cybersecurity report*.
19. IBM. (2022). *Cost of data breach report*.
20. McAfee. (2023). *Economic impact of cybercrime*.
21. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).
22. ITU. (2022). *Global cybersecurity index*.
23. World Bank. (2021). *Digital development report*.
24. Europol. (2023). *Internet organized crime threat assessment*.
25. Palo Alto Networks. (2023). *Unit 42 threat report*.
26. Check Point Research. (2023). *Cyber attack trends*.

27. Cloudflare. (2022). *Security trends report*.
28. Microsoft. (2023). *Microsoft digital defense report*.
29. Accenture. (2022). *State of cybersecurity resilience*.
30. Deloitte. (2023). *Cyber risk services report*.
31. PwC. (2022). *Global digital trust insights*.