Article

Not peer-reviewed version

Improvements in Cybersecurity: Coupling Python for Digital Forensics

Abbas Abdulazeez Abdulhameed * , Nadia Mahmood Hussien , Yasmin Makki Mohialden , Guillaume Herlem , Isabelle LAJOIE , Réda YAHIAOUI

Posted Date: 25 July 2023

doi: 10.20944/preprints202307.1666.v1

Keywords: cybersecurity; digital forensics; cyber threats; forensic investigator; python

Article

Improvements in Cybersecurity: Coupling Python for Digital Forensics

Nadia Mahmood Hussien [1], Yasmin Makki Mohialden [1], Abbas Abdulhameed [1,*], Guillaume Herlem [2], Isabelle Lajoie [2] and Reda Yahiaoui [2]

[1] Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
[2] Laboratoire de Nanomedicine, Imagerie, Thérapeutique université de Franche comté
* Correspondence: abbasabdulazeez@uomustansiriyah.edu.iq

Abstract: This article delves deeply into digital forensics, covering computer forensics, network forensics, and mobile device forensics. It analyzes the techniques and methodologies used by forensic investigators in various disciplines. It underlines the difficulties investigators encounter and the importance of thorough investigations to combat ever-increasing cyber risks. The paper emphasizes the necessity of leveraging digital forensic tools to improve cybersecurity and provides a thorough list of widely used Python libraries suitable for each investigation strategy, allowing for effective comparison. Furthermore, it emphasizes the availability and suitability of these Python libraries in computer device investigations (PyTSK3, Volatility, Pyregfi, and Pyevtx), mobile device investigations (Pytsk3, Volatility, Pyewf, dfVFS, Androguard, and pyMobileDevice), and network forensics (Scapy, Bro/Zeek, Dpkt, pypcap, and NetworkX). The creation of these libraries recognizes the complexities of digital crimes and the importance of applying modern techniques in forensic investigations. Particularly, digital forensics plays an important role for healthcare providers because modern medical devices produce, store, and transmit large amounts of patient and therapy information, which could provide a forensic investigator with a treasure trove of potential digital evidence.

Keywords: cybersecurity; digital forensics; cyber threats; forensic investigator; python

1. Introduction

Safeguarding networks, systems, devices, and data from unauthorized access and exploitation of personal information is the essence of cybersecurity. Recent research and analysis highlight a significant increase in cyber threats and attacks, emphasizing the need for automation in the realm of digital forensics. However, the exponential growth of data volumes poses a challenge for the field, particularly in terms of data recovery and carving.

A cybersecurity forensics expert investigates past wrongdoing. Depending on the scenario, this requires a variety of tasks. These activities include retrieving and analyzing data from storage devices, including computers, phones, and networks; tracking down cybercriminals; recovering stolen information; tracing computer attacks; and assisting in other computer-related investigations [1,2].

The advent of the digital age has undoubtedly transformed the lives and work of individuals. Nonetheless, the pervasive nature of cybercrimes poses threats to user privacy and data. This alarming increase in cybercrime has become a major concern for cybersecurity professionals. Digital forensics has emerged as a valuable tool for investigating cyberattacks, enabling effective examination and analysis of digital evidence [1,3].

Healthcare apps include serious security flaws, such as the use of insecure authentication systems and a lack of proper security controls. Because of these flaws, they are unprotected and vulnerable to a variety of criminal attacks, putting patients' safety and privacy at risk, especially since these applications manage sensitive medical data and provide life-sustaining tasks. We list unauthorized access to medical records as one of the most common crimes targeting healthcare applications. Such attacks may endanger the victims' privacy by disclosing their medical information, or they may endanger their lives by maliciously altering their medical records to render future medical prescriptions by physicians incorrect. Because of its inherent sensitivity, health information is regarded as one of the most appealing targets for cybercriminals, yet digital investigations of incidents involving health information are sometimes hampered by a lack of the essential infrastructure for forensic readiness [4–6].

Digital forensics is the use of forensic and scientific techniques to legally extract information from digital devices such as computers and smartphones. This legally obtained information can then be used as evidence in court. Computer forensics is a subset of digital forensics that includes network forensics, server forensics, computer forensics, internet forensics, social media forensics, storage forensics, online gaming, data/disk forensics, and VR forensics. Identification, retrieval, investigation, verification, and evidence presentation are all phases in solving digital crimes. However, the ongoing rise in cyber dangers requires the optimization of digital infrastructure for forensic operations. The discipline of digital forensics involves technical, legal, and resource constraints, which are exacerbated by the steady development of malware, which has hampered the efficiency of forensic investigations [7,8].

In summary, digital forensics plays a vital role in today's cybersecurity landscape, particularly in combating cybercrime. Its application helps protect user data and privacy, as well as enabling the effective investigation and presentation of digital evidence in legal proceedings. However, the field faces challenges in keeping up with the exponential growth of data volumes and adapting to evolving cyber threats. Ongoing research and development are crucial to enhancing the efficiency and effectiveness of digital forensic tools and techniques in the ever-changing digital landscape [9–11].

The outline of the paper is as follows: section Digital Forensics Types, Section 3 Case Studies for Cybersecurity Forensics Tasks and discussions, Section 4 Conclusion.

2. Digital Forensics types

2.1. Computer Forensics

Computer forensics is critical in assessing the prevalence of automated data processing systems and acquiring evidence from a variety of sources, including computers, embedded devices, and USB pen drives. It entails searching through system logs and local history for valuable artifacts. Hidden, encrypted, temporary, and password-protected files, critical documents and spreadsheets, file transfer logs, text communication logs, internet browsing histories, and photos, graphics, videos, and music are among the artifacts. In addition, the process comprises evaluating event logs and system logs, as well as looking for illicit, pirated, or legitimate code [12,13].

Table 1 lists some of the most commonly used Python packages in computer forensics, with brief definitions and comparisons.

These packages are open-source and community-maintained. They're easy to integrate into your Python-based digital forensics workflow due to their broad functionality and documentation. Each package has its own learning curve and requires familiarity with appropriate artifacts and data structures. Before employing a package in a forensic investigation, thoroughly read the documentation. The investigation's needs and artifacts determine the package. To cover all areas of computer forensics efficiently, employ many packages.

doi:10.20944/preprints202307.1666.v1

Table 1. lists computer forensics Python packages [14–18].

Name	Specification	Website
PyTSK3	PyTSK3 is a Python library that provides access to the Sleuth Kit (TSK) functionality. It allows you to analyze file systems, extract file metadata, and recover deleted files from disk images or live systems PyTSK3 is a powerful package for low-level file system analysis and data recovery.	https://pypi.org/project/pytsk3/
Volatility	Volatility is a popular open-source framework for memory forensics. It enables you to analyze volatile memory (RAM) to extract valuable information, such as running processes , network connections, loaded DLLs, and artifacts related to malware or system compromise. Volatility supports multiple operating systems and provides a wide range of plugins for comprehensive memory analysis.	https://pypi.org/project/volatility3/
Pyregfi	Pyregfi is a Python library for parsing Windows registry files. It allows you to extract registry keys, values, and data from forensic images or live systems. Pyregfi simplifies the process of analyzing the Windows Registry and enables you to uncover information related to user activity, system configurations, installed software, and more.	https://packages.debian.org/buster/python-pyregfi
Pyevtx	Pyevtx is a Python library for parsing Windows Event Log (EVTX) files. It enables you to extract event records from EVTX files and access their properties and data Pyevtx is useful for investigating security events, system events, application events, and other event logs to gain insights into system activity and potential security incidents.	https://pypi.org/project/evtx/

2.2. Forensics of Mobile Devices

Mobile forensics is the recovery of digital evidence from mobile devices as well as the study of call logs and text messages, including SMS and email conversations. It also gives location information via GPS data or cell site logs. Furthermore, mobile forensics investigates communication services such as BBM, WhatsApp, and WebChat, discovering crucial information. It allows you to examine phone numbers and information about service providers. It also displays the history of incoming and outgoing phone logs, SMS messages, emails, and IRC conversation logs, as well as contact information kept in address books and calendars. Given the nature of the data involved, security issues are crucial in mobile forensics[12,13,19].

Some Python libraries often used in mobile device forensics, with brief descriptions and a comparison: As shown in Table 2 some Python packages commonly used in mobile device Forensics [14–16,20–26]

Table 2. Some Python packages commonly used in mobile device Forensics.

Name	Description	Website
Scapy	is a powerful packet manipulation and network scanning library. It allows you to capture, dissect, and forge network packets. Scapy provides functionality for packet crafting, sniffing, and decoding, making it useful for network forensics tasks such as analyzing network traffic and extracting information from packets.	https://scapy.net/
Bro/Zeek	Originally known as Bro, Zeek is an open-source network analysis framework. It provides a high-level programming language and powerful scripting capabilities for analyzing network traffic. Zeek captures network traffic and generates log files that can be further analyzed for forensic purposes.	https://github.com/bro
Dpkt	A fast and efficient packet parsing library for Python It supports various protocols and allows you to extract information from network packet captures. dpkt provides functionality for dissecting and manipulating packets, making it useful for network forensics analysis.	https://dpkt.readthedocs.io/en/latest/
Pypcap	is a Python wrapper for the libpcap packet capture library. It enables you to capture network packets at the packet level, providing access to the raw packet data. Pypcap allows you to perform network forensics tasks such as packet capture and analysis.	https://pypi.org/project/pypcap/
NetworkX	While not specifically designed for network forensics, NetworkX is a powerful graph analysis library that can be useful in analyzing network structures. It provides functionality for creating, manipulating, and analyzing graphs, which can be utilized for network forensics tasks such as visualizing network connections and identifying patterns.	https://networkx.org/

When evaluating these packages, it is critical to assess their individual features, simplicity of use, community support, and documentation. Each product may have strengths and limitations depending on the specific requirements and circumstances of the investigation. It is recommended that you read the documentation and user feedback for each package before making a decision based on your individual requirements.

2.3. Forensics of networks

The monitoring and analysis of LAN, WAN, and internet traffic, including packet-level investigation, is part of network forensics. It collects and analyzes logs from numerous sources in order to assess the scope of the intrusion and the amount of data collected.

The forensic study of databases and their data is the subject of database forensics. Database content, log files, and in-RAM data are all investigated. For data modification and analysis, specialized software tools with audit recording capabilities are used.

The examination of financial scams and the linkage of findings with financial documents are all part of forensic data analysis. Close coordination with trained fraud examiners is common in this industry.

In conclusion, network forensics investigates network traffic, whereas database forensics investigates databases and their contents. Forensic data analysis focuses on financial fraud investigations and collaboration with professional fraud examiners. These specialist domains are critical in digital forensics, assisting in the discovery of evidence and the facilitation of investigations [12,13,19]. Table 3 displays Python network forensics [27–31].

Table 3. Network Forensics in Python.

Name	Description	Website
Scapy	is a powerful packet manipulation and network scanning library. It allows you to capture, dissect, and forge network packets. Scapy provides functionality for packet crafting, sniffing, and decoding, making it useful for network forensics tasks such as analyzing network traffic and extracting information from packets.	https://scapy.net/
Bro/Zeek	Originally known as Bro, Zeek is an open-source network analysis framework. It provides a high-level programming language and powerful scripting capabilities for analyzing network traffic. Zeek captures network traffic and generates log files that can be further analyzed for forensic purposes.	https://github.com/bro
Dpkt	A fast and efficient packet parsing library for Python It supports various protocols and allows you to extract information from network packet captures. dpkt provides functionality for dissecting and manipulating packets, making it useful for network forensics analysis.	https://dpkt.readthedocs.io/en/latest/
Pypcap	is a Python wrapper for the libpcap packet capture library. It enables you to capture network packets at the packet level, providing access to the raw packet data. Pypcap allows you to perform network forensics tasks such as packet capture and analysis.	https://pypi.org/project/pypcap/
NetworkX	While not specifically designed for network forensics, NetworkX is a powerful graph analysis library that can be useful in analyzing network structures. It provides functionality for creating, manipulating, and analyzing graphs, which can be utilized for network forensics tasks such as visualizing network connections and identifying patterns.	https://networkx.org/

When comparing these packages, evaluate their features, performance, ease of use, community support, and documentation. Depending on the individual requirements and circumstances of the network forensics investigation, each product offers advantages and disadvantages. It is recommended that you read the documentation and user feedback for each package before making an informed decision based on your individual needs.

3. Case studies for Cybersecurity Forensics Tasks and discussion

There is a tow case studies of cybersecurity forensics tasks:

Case Study 1: Unauthorized Data Breach

1. Gathering evidence of cybercrime: In this case, a company suspects that an unauthorized individual gained access to their sensitive data. The digital forensic investigator's tasks include:
   - Analyzing log files: The investigator examines the system log files to identify any suspicious activities, such as unauthorized login attempts or unusual network traffic.
   - Collecting and preserving digital evidence: The investigator uses specialized tools to collect and preserve evidence, including disk images, network traffic captures, and relevant files.
   - Identifying intrusion artifacts: The investigator looks for changes in system code, configurations, or other artifacts that indicate a breach, such as modified files or altered timestamps.
2. Preparing acquired data: Once the evidence is collected, the investigator needs to prepare the acquired data for analysis. This involves:
   - Making duplicates: The investigator makes forensic duplicates of the original evidence to confirm the data's integrity and prevent unintended change. This is usually done with forensic imaging software such as EnCase or FTK Imager.
   - Decrypting seized data: If the investigator encounters encrypted data during the investigation, specialized programs and procedures are used to decrypt the data. For example, if encrypted files are found, the investigator may employ cryptographic analysis techniques or leverage encryption keys obtained during the investigation to decrypt the data.
   - Processing images: Images acquired from the investigation, such as screenshots or memory captures, are processed using appropriate software tools. This may involve analyzing metadata, extracting relevant information, or enhancing image quality for later analysis.

Case Conclusion

In this case study, the digital forensic investigator successfully gathered evidence of the unauthorized data breach by analyzing log files, collecting and preserving digital evidence, and identifying intrusion artifacts. The acquired data was then prepared for analysis by creating duplicates to prevent modification, decrypting any seized encrypted data, and processing images using suitable software tools.

The investigation's findings and the prepared data can be used for further analysis, such as identifying the extent of the data breach, determining the entry point of the attacker, and uncovering any compromised systems or sensitive information.

Case Study 2: Financial Fraud and Cyber Attack

A financial institution experienced a significant cyberattack that led to financial fraud. The digital forensic investigator gathered evidence, including network logs, backups, and transaction records. Their tasks involved:

- Establishing a tracking database to organize evidence systematically.
- Summarizing key findings following reporting procedures.
- Acting as a technical expert and liaison with law enforcement, effectively communicating incident details.
- Ensuring compliance with the chain of custody for digital media according to the Federal Rules of Evidence.
- Authoring and publishing detailed reports, recommendations, and white papers tailored to appropriate audiences.

Case Conclusion

In this case study, the digital forensic investigator effectively reported a cybercrime incident involving financial fraud. By establishing a tracking database, summarizing findings, serving as a technical expert and liaison, ensuring chain of custody compliance, and authoring reports, the investigator contributed to documentation, legal proceedings, and the dissemination of insights. The investigator's reports and recommendations can enhance cybersecurity measures, raise industry awareness, and support law enforcement efforts against cybercrime. Note that specific tasks and procedures may vary depending on jurisdiction, organization, and incident nature.

Digital forensics tools have evolved to address tampering and data corruption challenges. These specialized tools include disk and data capture, file viewers, registry analysis, internet and network analysis, email analysis, mobile device analysis, Mac OS analysis, and database forensics tools. They greatly improve investigators' abilities, ensuring a precise and dependable investigation of digital evidence. Please keep in mind that the preceding case study is merely illustrative, and the actual activities and techniques used in real-world investigations may differ depending on the circumstances and available resources.

3.1. Utilization of Digital Forensics Tools

The tools of the digital forensics are [32,33] :

1. Disk and data capture tools: Investigators use these tools to create a bit-for-bit copy of the compromised system's hard drive, preserving the original evidence without modification. They identify encrypted files and hidden partitions as potential evidence.
2. File viewers and file analysis tools: These tools extract and analyze individual files from the captured disk image, enabling in-depth examination of various file types. Investigators scrutinize metadata and content for indicators of compromise.
3. Registry analysis tools: Investigators extract user and activity information from the compromised Windows system's registry, reconstructing attacker actions and establishing a timeline of events.
4. Internet and network analysis tools: These tools examine network traffic logs and monitor user activity, identifying suspicious IP addresses, unauthorized data transfers, and command-and-control servers.
5. Email analysis tools: Investigators scan email content, attachments, and server logs to uncover communication channels and relevant evidence, including phishing attempts and data leakage.
6. Mobile device analysis tools: For mobile devices involved in the breach, investigators extract data from internal and external memory to identify connections between the breach and the devices used.
7. Mac OS analysis tools: When Mac operating systems are affected, investigators retrieve metadata from Mac devices to examine file timestamps, user accounts, and application usage.
8. Database forensics tools: Investigators analyze and manipulate data within databases, generating reports on unauthorized queries, modifications, and data leakage.

The utilization of digital forensics tools in this case enhances investigators' capabilities, ensuring a thorough and reliable analysis of digital evidence during a cybersecurity breach investigation.

4. Conclusions

The employment of specialist technologies has greatly enhanced digital forensic analysis by efficiently resolving issues about evidence tampering and ensuring accurate outcomes, such as these concerns about a key piece of information in the healthcare system. These tools enable investigators to collect, extract, evaluate, and present evidence more efficiently. Their ongoing progress reflects the complexities of digital crimes, which require new techniques for successful investigations. Investigators can protect the integrity of the evidence and unearth significant insights by using the appropriate tools at each stage. It is critical to continually update and adjust these tools in order to keep up with evolving technologies and emerging threats. Furthermore, future digital forensic tool research and development will improve the accuracy, efficiency, and efficacy of investigations in the ever-changing arena of cybercrime.

The study emphasizes the availability of a variety of Python modules that assist investigators in conducting digital inquiries, retrieving evidence, and performing analysis across multiple domains. These libraries are designed specifically to meet the needs of computer device investigations (PyTSK3, Volatility, Pyregfi, and Pyevtx), mobile device investigations (Pytsk3, Volatility, Pyewf, dfVFS, Androguard, and pyMobileDevice), and network forensics (Scapy, Bro/Zeek, Dpkt, pypcap, and NetworkX). The creation of these libraries recognizes the complexities of cybercrime and the importance of employing modern approaches in investigation operations.

The topic of this article is the advancement of digital forensics technologies. The restricted alternatives first aroused concerns about evidence manipulation. However, the desire for precise analysis led to the development of advanced technologies to solve these challenges.

Disk/data capture, file viewers/analysis, registry analysis, internet/network analysis, email analysis, mobile device analysis, Mac OS analysis, and database forensics tools are some examples of specialized tools.

Each category has a specific function. Drive encryption is extracted using disk and data capture tools. File viewers and analysis programs perform in-depth examinations of files. The Windows registry is used by registry analysis tools to extract user activities. Tools for Internet and network analysis.

Reveal network traffic and user behavior. Email analysis tools look for evidence in email text. Data from memory is extracted by mobile device analysis software. Metadata is retrieved from Mac systems using Mac OS analysis tools. Database forensics software examines and reports on database activities.

Acknowledgments: This work was supported in part by the FEDER "European Regional Development Fund" Project "Reper@ge" (The Reper@ge project is developed at the Nanomedicine, Imaging and Therapeutics Laboratory, Franche-Comté University), and Mustansiriyah University, College of Science, Department Computer Science, Cyber Security lab. Baghdad, Iraq

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alghamdi, M.I. Digital Forensics in Cyber Security-Recent Trends, Threats, and Opportunities. In *Cybersecurity Threats with New Perspectives*; Sarfraz, M., Ed.; IntechOpen: Rijeka, 2021; chapter 1. doi:10.5772/intechopen.94452.
2. Pandey, A.K.; Tripathi, A.K.; Kapil, G.; Singh, V.; Khan, M.W.; Agrawal, A.; Kumar, R.; Khan, R.A. Current challenges of digital forensics in cyber security. *Critical Concepts, Standards, and Techniques in Cyber Forensics* **2020**, pp. 31–46. doi:10.4018/978-1-7998-1558-7.ch003.
3. Paul Joseph, D.; Norman, J. An Analysis of Digital Forensics in Cyber Security. First International Conference on Artificial Intelligence and Cognitive Computing; Bapi, R.S.; Rao, K.S.; Prasad, M.V.N.K., Eds.; Springer Singapore: Singapore, 2019; pp. 701–708. doi:10.1007/978-981-13-1580-0_67.
4. Grispos, G.; Bastola, K. Cyber autopsies: The integration of digital forensics into medical contexts. 2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS). IEEE, 2020, pp. 510–513. doi:10.1109/CBMS49503.2020.00102.
5. Chernyshev, M.; Zeadally, S.; Baig, Z. Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems* **2019**, *43*, 1–12. doi:10.1007/s10916-018-1123-2.
6. Ellouze, N.; Rekhis, S.; Boudriga, N. Forensic investigation of digital crimes in healthcare applications. In *Digital forensics and forensic investigations: Breakthroughs in research and practice*; IGI Global, 2020; pp. 227–258. doi:10.4018/978-1-7998-3025-2.ch017.
7. Sharma, B.K.; Joseph, M.A.; Jacob, B.; Miranda, B. Emerging trends in Digital Forensic and Cyber security- An Overview. 2019 Sixth HCT Information Technology Trends (ITT), 2019, pp. 309–313. doi:10.1109/ITT48889.2019.9075101.

doi:10.20944/preprints202307.1666.v1

8. Ukwen, D.O.; Karabatak, M. Review of NLP-based systems in digital forensics and cybersecurity. 2021 9th International symposium on digital forensics and security (ISDFS). IEEE, 2021, pp. 1–9. doi:10.1109/ISDFS52919.2021.9486354.
9. AlSaad, S.N.; Hussien, N.M. Landmark based shortest path detection in alarm system. *Al-Mustansiriyah Journal of Science* **2018**, *29*, 135–140. doi:10.23851/mjs.v29i2.276.
10. Muhamed, S.J. Detection and Prevention WEB-Service for Fraudulent E-Transaction using APRIORI and SVM. *Al-Mustansiriyah Journal of Science* **2022**, *33*, 72–79. doi:10.23851/mjs.v33i4.1242.
11. Al-Windi, B.K.; Abbas, A.H.; Mahmood, M.S. Using Texture Analyses and Statistical Classification for Detection Plant Leaf Diseases. *Al-Mustansiriyah Journal of Science* **2021**, *32*, 1–4. doi:10.23851/mjs.v32i5.1115.
12. Prasanthi, B. Cyber forensic tools: a review. *International Journal of Engineering Trends and Technology (IJETT)* **2016**, *41*, 266–271. doi:10.14445/22315381/IJETT-V41P249.
13. Fernando, V. Cyber forensics tools: A review on mechanism and emerging challenges. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2021, pp. 1–7. doi:10.1109/NTMS49979.2021.9432641.
14. Du, X.; Scanlon, M. Methodology for the Automated Metadata-Based Classification of Incriminating Digital Forensic Artefacts. Proceedings of the 14th International Conference on Availability, Reliability and Security; Association for Computing Machinery: New York, NY, USA, 2019; ARES '19. doi:10.1145/3339252.3340517.
15. Python, I. Volatility 3: The volatile memory extraction framework. https://pypi.org/project/volatility3/. Accessed: 2023.
16. Singh, D.; Yadav, R. A Comprehensive Study and Implementation of Memory Malware Analysis with Its Application for the Case Study of CRIDEX. In *Intelligent Cyber Physical Systems and Internet of Things: ICoICI 2022*; Hemanth, J.; Pelusi, D.; Chen, J.I.Z., Eds.; pringer International Publishing: Cham, 2023; pp. 31–44. doi:10.1007/978-3-031-18497-0_3.
17. Dutra, A.H. Forensic acquisition of file systems with parallel processing of digital artifacts to generate an early case assessment report. Doctoral dissertation, Instituto Politécnico de Beja, Portugal, 2021.
18. Python, I. pyevtx-rs. https://pypi.org/project/evtx/.
19. Chaturvedi, A.; Awasthi, A.; Shanker, S. Cyber Forensic-A Literature Review. *Trinity Journal of Management, IT & Media* **2020**, *10*, 24–29. doi:10.48165/tjmitm.2019.1002.
20. Python, I. Python bindings module for libewf. https://pypi.org/project/libewf-python/.
21. Altheide, C.; Carvey, H. *Digital forensics with open source tools*; Elsevier, 2011.
22. Python, I. Digital Forensics Virtual File System (dfVFS). https://pypi.org/project/dfvfs/.
23. Groß, T.; Busch, M.; Müller, T. One key to rule them all: Recovering the master key from RAM to break Android's file-based encryption. *Forensic Science International: Digital Investigation* **2021**, *36*, 301113. DFRWS 2021 EU - Selected Papers and Extended Abstracts of the Eighth Annual DFRWS Europe Conference, doi:https://doi.org/10.1016/j.fsidi.2021.301113.
24. Python, I. Androguard is a full python tool to play with Android files. https://pypi.org/project/androguard/.
25. Nikale, S.A.; Purohit, S. Comparative Analysis of Android Application Dissection and Analysis Tools for Identifying Malware Attributes. In *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*; River Publishers, 2023; pp. 87–103.
26. Python, I. python implementation for libimobiledevice library. https://pypi.org/project/pymobiledevice/.
27. Rohith, R.; Moharir, M.; Shobha, G.; others. SCAPY-A powerful interactive packet manipulation program. 2018 international conference on networking, embedded and wireless systems (ICNEWS); IEEE, , 2018; pp. 1–5. doi:10.1109/ICNEWS.2018.8903954.
28. Mudgal, A.; Bhatia, S. Experimental-based comparative study on open-source network intrusion detection system. *International Journal of Internet Technology and Secured Transactions* **2022**, *12*, 462–475. doi:10.1504/IJITST.2022.125781.
29. Chen, J.; Yang, W.; Cui, C.; Zhang, Y. Research and Implementation of Intelligent Detection for Deserialization Attack Traffic. 2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST); IEEE, , 2022; pp. 1206–1211. doi:10.1109/IAECST57965.2022.10061969.

30. Babić, I.; Maksimović, A.; Nedeljković, S.; Jovanović, M.; Čabarkapa, M.; Randjelović, D. Useful Python libraries for creating IDS software. Thematic conference proceedings of international significance. Vol. 2/International scientific conference" Archibald Reiss Days", Belgrade, 6-7 November 2019. Belgrade: University of Criminal Investigation and Police Studies, 2019, pp. 337–347.
31. Hagberg, A.; Conway, D. Networkx: network analysis in python. https://networkx.github.io, 2020.
32. Brunty, J. Validation of forensic tools and methods: A primer for the digital forensics examiner. *Wiley Interdisciplinary Reviews: Forensic Science* **2023**, *5*, e1474. doi:10.1002/wfs2.1474.
33. Saxena, I.; Usha, G.; Vinoth, N.; Veena, S.; Nancy, M. The Future of Artificial Intelligence in Digital Forensics: A Revolutionary Approach. In *Artificial Intelligence and Blockchain in Digital Forensics*; River Publishers, 2023; pp. 133–151.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.