METHODS AND MODELS FOR ENSURING INFORMATION SECURITY DURING THE COLLECTION OF DIGITAL EVIDENCE

Pronin Y. V.[1], Zubok V. Y.[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",*
forensic.ua@gmail.com, vitalii.zubok@pimee.ua

This review explores the current state of research at the intersection of cybersecurity and digital forensics, focusing on methods and models developed to ensure information security during the collection of digital evidence. It categorizes recent contributions on secure acquisition, cryptographic validation, volatile data, cloud and IoT environments, and anti-forensic challenges. Emphasis is placed on standardization, legal compliance, and interdisciplinary collaboration.

Keywords: cybersecurity, information security, digital forensics, digital evidence

Introduction

The digitalization of society and the growth of cybercrime have made secure digital evidence collection critical for investigations. Cybersecurity ensures protection of systems and data, while digital forensics manages acquisition and preservation of digital artifacts. The rise of technologies such as IoT and cloud computing, alongside anti-forensic tactics, complicates admissibility and integrity of digital evidence.

Methods

The study uses a thematic literature review approach to analyze publications from 2015 to 2024. Scopus was used as a primary data source, with queries including: "cybersecurity AND digital forensics", "information security AND digital evidence", and other combinations. Google was used for Ukrainian-language materials to capture regional perspectives.

Inclusion criteria: peer-reviewed journals/conferences, English and Ukrainian sources, content addressing secure

evidence collection. Exclusion: physical-only forensics, non-academic materials, and redundant or methodology-lacking studies. Articles were grouped into five thematic areas: (1) secure acquisition and cryptographic validation, (2) live forensics, (3) cloud/IoT/big data forensics, (4) legal standards, and (5) anti-forensics (Figure 1).

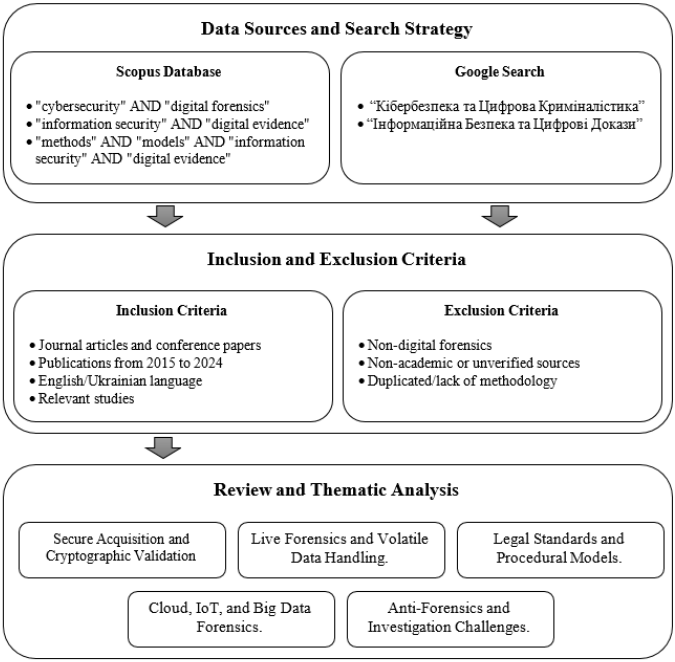

Figure 1. Literature Review Methodology

Results

Thematic analysis reveals the following findings:

– Secure Acquisition: Forensic imaging and hashing ensure evidence authenticity. However, challenges include evidence tampering risks, device diversity, and cross-jurisdictional issues.
– Live Forensics: Volatile data acquisition allows real-

time analysis but risks alteration. Tools minimizing system interference are essential.

- Cloud & IoT: These platforms introduce risks of unauthorized access. Encryption and access control are required. Forensics helps trace intrusions.
- Legal Standards: A lack of harmonized regulations weakens admissibility. GDPR, ECPA, and ISO/IEC guide best practices.
- Anti-Forensics: Obfuscation, deletion, and counterfeiting pose increasing threats. Structured threat modeling is key to mitigation.

Conclusion

The convergence of cybersecurity and forensics is evident but faces practical gaps. Forensic readiness is underdeveloped. Legal inconsistencies challenge international collaboration. Tool validation remains insufficient. Interdisciplinary training is critical to ensure both technical rigor and legal compliance.

Future work should develop standardized frameworks, promote AI-driven evidence collection, address legal ambiguity in cross-border data handling, and institutionalize forensic readiness.

Stronger collaboration between legal, technical, and operational domains is necessary to ensure the security and credibility of digital evidence in modern investigative practice.

References

1. Allah Rakha N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review, 16(2), 23–54. DOI: https://doi.org/10.22201/iij.24485306e.2024.2.18892

2. Belshaw S., Nodeland B. (2022). Digital evidence experts in the law enforcement community: understanding the use of forensics examiners by police agencies. Secur J 35, 248–262. DOI: https://doi.org/10.1057/s41284-020-00276-w

3. Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510-2523 ((1986)). https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

4. Hoelz, B., Maues, M. (2017). Anti-Forensic Threat Modeling. In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIII. DigitalForensics 2017. IFIP Advances in Information and Communication Technology, vol 511. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-67208-3_10

5. International Organization for Standardization. (2022). ISO/IEC 27002:2022(en): Information security, cybersecurity and privacy protection – Information security controls. https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27002:ed-3:v2:en

6. Khakhanovskyi, V., & Hrebenkova, M. (2022). Identification, collection, and investigation of electronic imagery as sources of evidence. Law Journal of the National Academy of Internal Affairs, 12(4), 28-39. DOI: https://doi.org/10.56215/04221204.28

7. Mishra, Alok & Alzoubi, Yehia & Anwar, Memoona J. & Gill, Asif. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security. 120. DOI: https://doi.org/10.1016 /j.cose.2022.102820

8. Benancio, Lizbardo & Canales, Ricardo & Leon, Paolo & Huamani Uriarte, Enrique. (2021). Integrity and Authenticity of Digital Images by Digital Forensic Analysis of Metadata. International Journal of Emerging Technology and Advanced Engineering. 11. 38-45. DOI: https://doi.org/ 10.46338/ijetae0921_05

9. Pathak, M., Mishra, K.N. & Singh, S.P. (2024). Securing data and preserving privacy in cloud IoT-based technologies an analysis of assessing threats and developing effective safeguard. Artif Intell Rev 57, 269. https://doi.org/10.1007/s10462-024-10908-x

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

11. Ritzkal, Hendrawan, A.H., Kurniawan, R., Aprian, A.J., Primasari, D., Subchan, M. (2024). Enhancing cybersecurity through live forensic investigation of Remote Access Trojan attacks using FTK Imager software. International Journal of Safety and Security Engineering, Vol. 14, No. 1, pp. 217-223.

DOI: https://doi.org/10.18280/ijsse.140121

12. Setiawan, Nova & Pratama, Ahmad & Ramadhani, Erika. (2022). Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce. JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia). 7. 1-9. DOI: https://doi.org/10.32528/justindo.v7i1.5356