UDC 004.056:343.98

IMPROVING DIGITAL FORENSICS METHODS IN CYBERCRIME DETECTION

Kariyev Ulugbek Orifjonovich
Master's student, Computer Science and Engineering Technology,
Sharda University Uzbekistan, Republic of Uzbekistan, Andijan
E-mail: ulugbek1986@mail.ru

Abstract. The article examines current problems in applying digital forensics methods to the detection and investigation of cybercrimes. The key factors that reduce the effectiveness of traditional approaches are analyzed: the explosive growth of digital data volumes, ubiquitous encryption, the spread of cloud services, Internet of Things devices and anti-forensic techniques. Based on an analysis of the international standards ISO/IEC 27037 and NIST SP 800-86, an improved six-stage model of digital forensic examination is proposed. The model includes automated prioritization (triage) of evidence sources, priority acquisition of volatile data, cryptographic integrity control with an immutable chain-of-custody log, and timeline correlation analysis supported by machine learning. A weighted model for assessing the priority of digital sources is proposed. It is shown that the proposed approach makes it possible to reduce the time of preliminary analysis and to increase the evidentiary value of digital traces.

Keywords: digital forensics, cybercrime, digital evidence, triage, memory forensics, chain of custody, hash function, machine learning, anti-forensics.

Introduction. The rapid digitalization of all spheres of public life is accompanied by a growing number of crimes committed with the use of information and communication technologies. In the Republic of Uzbekistan, the implementation of the "Digital Uzbekistan – 2030" strategy [9] is actively developing e-government services, remote banking and e-commerce, which at the same time widens the attack surface available to offenders. The adoption of the Law of the Republic of Uzbekistan "On Cybersecurity" [8] laid the legal foundation for protecting the information infrastructure; however, effective counteraction to cybercrime is impossible without reliable methods for detecting, recording and examining digital traces.

Digital forensics is an applied scientific discipline that studies methods for the identification, collection, preservation, analysis and presentation of digital evidence in a form admissible in law enforcement and judicial proceedings [2]. Classical models of digital forensic examination were formed at a time when the main object of examination was a single personal computer with a hard disk of relatively small capacity. The “make a full copy of the storage medium and then examine it” methodology was justified and well formalized [1].

As early as 2010, S. Garfinkel noted that the “golden age” of digital forensics was coming to an end and pointed to a crisis of traditional approaches caused by growing storage capacity, encryption and cloud technologies [5]. Subsequent studies confirmed that the increase in data volume leads to a significant backlog of cases in forensic laboratories [10], and a review of current research identifies cloud forensics, the Internet of Things and the use of artificial intelligence among the key challenges [3].

The aim of the study is to develop an improved model of digital forensic examination that increases the speed and reliability of cybercrime detection under conditions of large volumes and heterogeneity of digital data.

Materials and methods

The methodological basis of the study comprised a systemic and comparative analysis of existing digital forensic process models [4], the international standards ISO/IEC 27037:2012 [7] and NIST SP 800-86 [6] governing the handling of digital evidence, and the RFC 3227 recommendations on the order of data collection according to volatility [11]. Methods of expert assessment and multi-criteria analysis were used to substantiate the prioritization criteria. The traditional and proposed approaches were compared against a set of qualitative criteria: speed, completeness, integrity preservation, resistance to anti-forensics and scalability.

Results and discussion

1. Systematization of the problems of modern digital forensics. The analysis of literature and practice made it possible to identify the main groups of factors that reduce the effectiveness of traditional methods (Table 1).

Table 1. *Factors reducing the effectiveness of traditional digital forensics methods*

Factor	**Manifestation**	**Consequence for the investigation**
Data volume	Terabyte-scale storage, many devices per person	Longer examination times, growing case backlog
Encryption	Full-disk encryption, secure messengers	Data inaccessible once the device is powered off
Cloud services	Data distributed across jurisdictions	Difficult seizure, legal restrictions on access
Internet of Things	Non-standard OS and formats, small memory	Lack of universal tools
Anti-forensics	Data wiping, timestamp tampering, fileless malware	Loss or distortion of traces
Volatile data	Processes, network connections, keys in RAM	Irrecoverable loss if seized incorrectly

As Table 1 shows, a significant part of critical information exists only in volatile memory or in external systems. Consequently, a model focused exclusively on the examination of a powered-off storage medium (dead forensics) does not meet current conditions.

2. Improved model of digital forensic examination. The proposed model includes six interrelated stages, each of which supplements the basic requirements of the standards [6; 7].

Stage 1. Preparation. Development of standard response scenarios by type of cybercrime (fraud, unauthorized access, distribution of malware), preparation of verified software tools and hardware write blockers.

Stage 2. Identification and prioritization (triage). At the scene, a rapid assessment of all potential evidence sources is performed and they are ranked by priority using a weighted model (Formula 1). This makes it possible to examine the most significant objects first instead of imaging every storage medium in full.

Stage 3. Volatility-aware acquisition. Data are collected in decreasing order of volatility [11]: registers and cache, main memory, network state and running processes, temporary files, persistent storage, archival data. A memory dump of a running device

must be acquired before it is powered off, since RAM contains encryption keys, traces of fileless malware and activity history [12].

Stage 4. Preservation and integrity control. A cryptographic hash (SHA-256) is computed for each acquired image, and all examiner actions are recorded in a chain-of-custody log. It is proposed to keep this log in immutable form: each entry contains the hash of the previous entry, which makes any unnoticed alteration of the history impossible and increases the court's confidence in the digital evidence.

Stage 5. Integrated analysis. A unified timeline of events (super-timeline) is built from file system data, operating system logs, network logs and application artifacts. Machine learning methods are used to select relevant objects: file classification, anomaly detection in logs, and matching against databases of known hashes. The results of automated analysis are necessarily verified by an examiner.

Stage 6. Presentation of results. Preparation of an expert report describing the methods and tools used, including their versions, to ensure the reproducibility of the examination.

3. Weighted source prioritization model. For the triage stage, it is proposed to evaluate the priority of the i-th source of digital evidence using the formula:

$$P_i = w_1 \cdot R_i + w_2 \cdot V_i + w_3 \cdot T_i + w_4 \cdot A_i, \quad (1)$$

where R_i is the relevance of the source to the type of crime; V_i is the volatility of the data (risk of loss); T_i is the proximity of the time of last activity to the time of the incident; A_i is the accessibility of the data (absence of encryption or availability of keys); $w_1 \ldots w_4$ are weighting coefficients ($\sum w_k = 1$) determined by expert judgment for each type of crime. All indicators are normalized to the interval [0; 1]. Sources with the highest P_i value are examined first.

For example, when investigating unauthorized access to a banking system, it is advisable to assign the greatest weight to relevance and volatility ($w_1 = 0.35$; $w_2 = 0.30$), which ensures that the server's main memory and network logs are examined first. When investigating fraud via messengers, priority shifts to mobile devices and cloud backups.

4. Comparative assessment of the approaches. A comparison of the traditional and proposed approaches is given in Table 2.

Table 2. *Comparison of the traditional and improved approaches*

Criterion	Traditional approach	Improved approach
Order of examination	Full imaging of all storage media	Triage and ranking of sources using Formula (1)
Volatile data	Often lost during seizure	Priority acquisition of RAM dump and network state
Integrity control	Image hash, paper log	Hash plus immutable linked chain-of-custody log
Analysis	Separate examination of artifacts	Unified timeline and cross-source correlation
Processing large volumes	Manual review	Automated filtering with examiner verification
Resistance to anti-forensics	Low	Increased through memory analysis and timestamp correlation

Applying the proposed model enables a shift from an extensive ("copy everything and review everything") to an intensive, targeted examination. The time of preliminary analysis is reduced because the most significant data are extracted and examined within the first hours after an incident is detected, while lower-priority sources are processed in the background.

At the same time, implementation of the model involves a number of limitations. First, the results of machine learning algorithms must be explainable; otherwise their evidentiary value may be challenged. Second, collecting data from a running system inevitably introduces minimal changes to it, which must be documented. Third, the effectiveness of the model depends directly on the qualifications of specialists, which requires the development of relevant educational programs at technical universities.

Conclusion

1. Traditional digital forensics methods focused on the examination of a powered-off storage medium do not ensure timely detection of cybercrimes under conditions of growing data volumes, encryption, cloud technologies and anti-forensics.

2. A six-stage model of digital forensic examination is proposed that is consistent with the requirements of ISO/IEC 27037 and NIST SP 800-86 and is supplemented with a triage stage, priority acquisition of volatile data, an immutable chain-of-custody log and integrated timeline analysis.

3. A weighted model for prioritizing sources of digital evidence has been developed, taking into account the relevance, volatility, temporal proximity and accessibility of data, which allows the resources of forensic units to be allocated rationally.

4. Promising directions for further research include experimental validation of the model on real cases, development of explainable machine learning algorithms for forensic analysis, and adaptation of the methodology to Internet of Things devices.

References:

1. Carrier B. File System Forensic Analysis. – Boston: Addison-Wesley, 2005. – 569 p.

2. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. – 3rd ed. – Waltham: Academic Press, 2011. – 840 p.

3. Casino F., Dasaklis T.K., Spathoulas G. et al. Research trends, challenges, and emerging topics in digital forensics: A review of reviews // IEEE Access. – 2022. – Vol. 10. – P. 25464–25493.

4. Du X., Le-Khac N.-A., Scanlon M. Evaluation of digital forensic process models with respect to digital forensics as a service // Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017). – Dublin, 2017. – P. 573–581.

5. Garfinkel S.L. Digital forensics research: The next 10 years // Digital Investigation. – 2010. – Vol. 7. – P. S64–S73.

6. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86. – Gaithersburg: NIST, 2006. – 121 p.

7. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. – Geneva: ISO, 2012. – 36 p.

8. Law of the Republic of Uzbekistan “On Cybersecurity” No. ZRU-764 of 15.04.2022 [Electronic resource]. – URL: https://lex.uz (accessed: 27.09.2026).

9. Decree of the President of the Republic of Uzbekistan “On approval of the Digital Uzbekistan – 2030 strategy and measures for its effective implementation” No. UP-6079 of 05.10.2020 [Electronic resource]. – URL: https://lex.uz (accessed: 27.09.2026).

10. Quick D., Choo K.-K.R. Impacts of increasing volume of digital forensic data: A survey and future research challenges // Digital Investigation. – 2014. – Vol. 11, No. 4. – P. 273–294.

11. Brezinski D., Killalea T. Guidelines for Evidence Collection and Archiving: RFC 3227. – IETF, 2002. – 10 p.

12. Ligh M.H., Case A., Levy J., Walters A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. – Indianapolis: Wiley, 2014. – 912 p.