Digitális keretrendszer a bírósági tevékenységekhez

Digital Framework for judicial activity

SEBESTYÉN György, Ioan TICOVAN

Kolozsvári Műszaki Egyetem, Románia

Abstract

In the context of the rapid advancement of Information and Communication Technologies (ICT), digital forensic investigations are increasingly supported by specialized tools. Each phase of an investigation—from secure data acquisition and storage to knowledge extraction and information visualization—requires scalable and robust ICT solutions. This paper proposes an integrated framework specifically designed for judicial investigations, aimed at optimizing the acquisition, processing, and analysis of digital evidence.

The proposed solution introduces an operational workflow that ensures the secure handling of digital artifacts while maintaining the rigor required for legal admissibility. A key component of this framework is the data capture module, which enables selective network traffic interception, multiple simultaneous captures based on different criteria from the same data stream, as well as synchronized multipoint capture from geographically distributed locations. This level of flexibility is particularly valuable in cybercrime investigations.

The second major component of the framework is the secure storage module, developed to protect digital evidence from tampering, loss, or unauthorized access. The proposed architecture implements twelve parallel protection mechanisms to ensure data integrity. To optimize communication across distributed subsystems and reduce data traffic, only metadata is stored in a private blockchain. This approach significantly reduces the volume of data replicated between nodes while preserving traceability and verifiability of the evidence. The solution was validated in closed (air-gapped) infrastructures, demonstrating operational efficiency under high-security constraints.

The third aspect addressed involves the analysis and interpretation of data collected during digital forensic operations. Several methods for automatic evidence extraction were tested, with a particular focus on artificial intelligence (AI)-based techniques. These AI models improve the speed and accuracy of identifying digital evidence by recognizing trained patterns using specialized neural networks.

In conclusion, the proposed framework provides end-to-end support for digital forensic workflows—from intelligent data capture to secure evidence storage and AI-assisted analysis. It enhances the capabilities of judicial and law enforcement institutions in combating cybercrime, while ensuring the integrity and legal admissibility of electronic evidence.

Kivonat

Az információs és kommunikációs technológiák (IKT) gyors fejlődésének köszönhetően a digitális kriminalisztikai vizsgálatokat egyre inkább speciális eszközök támogatják. Egy vizsgálat minden szakasza – az adatok biztonságos megszerzésétől és tárolásától kezdve a tudáskinyerésen és információmegjelenítésen át – skálázható és megbízható IKT-megoldásokat igényel. Jelen tanulmány egy integrált keretrendszert javasol, amelyet kifejezetten bírósági vizsgálatokhoz terveztünk, azzal a céllal, hogy optimalizálja a digitális bizonyítékok megszerzését, feldolgozását és elemzését.

A javasolt megoldás egy olyan működési munkafolyamatot vezet be, amely biztosítja a digitális bizonyítékok biztonságos kezelését, miközben megőrzi a jogi elfogadhatósághoz szükséges szigort. A keretrendszer egyik kulcseleme az adatgyűjtő modul, amely lehetővé teszi a hálózati forgalom szelektív begyűjtését és különböző kritériumok alapján történő tárolását. Ez a rugalmasság különösen értékes a kiberbűnözési vizsgálatok során.

A keretrendszer második fő eleme a biztonságos tárolómodul, amely megakadályozza a digitális bizonyítékokhoz való jogosulatlan hozzáférést. Az architektúra tizenkét védelmi mechanizmust valósít meg az adatintegritás biztosítása érdekében. Ezek a mechanizmusok kriptográfiai módszerekre, blokklánc-technológiára, valamint szigorúan ellenőrzött írási technikákra (például WORM – write once, read many) épülnek. Az elosztott alrendszerek közötti kommunikáció optimalizálása és az adatforgalom csökkentése érdekében csak a digitális bizonyítékokhoz kapcsolódó metaadatokat tároljuk egy privát blokkláncon, így biztosítva az adatok integritását. Ez a megközelítés jelentősen csökkenti a csomópontok között replikált adatok mennyiségét, miközben megőrzi a bizonyítékok nyomon követhetőségét és ellenőrizhetőségét. A megoldást zárt (air-gapped) infrastruktúrákban validáltuk, ahol magas biztonsági követelmények mellett is hatékonyan működött.

A rendszer harmadik eleme az adatok elemzésére és értelmezésére vonatkozik, amelyeket a digitális kriminalisztikai műveletek során gyűjtöttek. Több automatikus bizonyíték-kinyerési módszert is teszteltünk, különös hangsúlyt fektetve a mesterséges intelligencia (MI) alapú technikákra. Ezek az MI-modellek javítják a digitális bizonyítékok azonosításának sebességét és pontosságát, mivel speciális neurális hálózatok segítségével ismerik fel a betanított mintákat.

Összefoglalva, a javasolt keretrendszer teljes körű támogatást nyújt a digitális kriminalisztikai munkafolyamatokhoz – az intelligens adatgyűjtéstől a biztonságos bizonyítéktároláson át az MI-alapú elemzésig. Ezáltal növeli a bírósági és bűnüldöző szervek képességeit a kiberbűnözés elleni küzdelemben, miközben biztosítja az elektronikus bizonyítékok integritását és jogi elfogadhatóságát.

IRODALMI HIVATKOZÁSOK

1. I. V. Țicovan and G. Sebestyen, "Judicial Surveillance of Cyber-Physical Systems," in 2022 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 2022. doi: 10.1109/AQTR55203.2022.9801934.
2. I. V. Țicovan and G. Sebestyen, "Forensic Investigation of Data Storage Systems," in 2024 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 2024, pp. 1–7, doi: 10.1109/AQTR61889.2024.10554109.
3. I. V. Țicovan and G. Sebestyen, "Solutions for enhancing the protection of digital evidence in judicial information systems," Romanian Journal of Information Technology and Automatic Control, vol. 35, no. 2, pp. 19–32, 2025, doi: 10.33436/v35i2y202502. [Online]. Disponibil: https://rria.ici.ro/documents/1368/art._%C8%9Aicovan_Sebestyen.pdf
4. I. V. Ticovan și G. Sebestyen, „Forensic Data Analysis Pipeline," Acta Univ. Sapientiae, Informatica, vol. 17, no. 3, 2025. [Online]. Disponibil: https://doi.org/10.1007/s44427-025-00004-5
5. Radu-Marian Portase, Adrian Coleșa, Gheorghe Sebestyen, Efficient Multi-Stage Detection of Malicious Windows Executable During Execution, 2023 IEEE 19th International Conference on Intelligent Computer Communication and Processing (ICCP)