Volume 3, Issue 8 August 2025 **ISSN (E):** 2938-3757

DEVELOPMENT OF FORENSIC LABORATORIES IN THE FIELD OF DIGITAL FORENSICS IN UZBEKITAN

I. M. Kupriyanova
Chief Expert, Department of Digital Expertises Main Forensic Center,
Ministry of Internal Affairs of the Republic of Uzbekistan
Kupriyanova6420@mail.ru

Abstract
This article examines the current state and key areas of forensic laboratory development, focusing on institutional changes, human resources, logistical equipment, the legal environment, and interdepartmental cooperation.

Keywords: Digital forensics, cybercrime, forensic laboratories.

Introduction

The rapid growth of the digital economy and the penetration of information technologies into all areas of life have radically changed the criminogenic landscape: in Uzbekistan, the share of crimes involving IT technologies in 2024 reached nearly half of the total. In these circumstances, the role of forensic laboratories (FL) specializing in digital forensics is decisive: they ensure the lawful collection, examination, and interpretation of digital evidence, forming the evidentiary basis for investigation and trial.

Statistical indicators confirm that digital forensics is one of the most dynamically developing areas of forensic expertise. According to the Ministry of Internal Affairs (MIA), in 2024, 58,800 cybercrimes were registered across the country — 68 times more than in 2019 (863 cases). Between 2021 and 2024, the total financial damage to citizens amounted to about 1.909 trillion UZS, while the recovery of stolen funds remained minimal — about 4%. The most widespread crimes include thefts using bank cards and social engineering; almost every second crime involved IT technologies.

On August 1, 2024, a Research Institute of Digital Forensics was established within the structure of the Academy of Law Enforcement Agencies to provide scientific and methodological support, conduct examinations, and train specialists. In parallel, international initiatives are being implemented to build capacity: OSCE programs on electronic evidence, practical courses on mobile forensics within BOMCA-10, and joint activities with international partners. A foundation is being laid for unifying approaches to the collection, storage, and exchange of electronic evidence, as well as for scaling the network of forensic laboratories.

Currently, training in digital forensics at the Academy of the MIA is carried out by the Department of Forensic Examinations. This department is responsible for forming professional

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

competencies in forensic activities, including the study of theoretical foundations, methods, and technologies of evidence analysis.

The curriculum of the department includes the subject "Fundamentals of Digital Forensics", which covers issues of seizure, analysis, and interpretation of electronic evidence, as well as the use of specialized hardware and software tools for examining digital media. In addition, related disciplines are taught, such as forensics, forensic support of investigations, forensic medicine and psychiatry, and financial forensics.

From July 1, 2025, the Academy of the MIA plans to establish a new structural unit — the Faculty of Cybersecurity and Digital Forensics. It will include specialized departments focused on training personnel in cyber law, information security, and digital technologies. This will expand the academic and research base, introduce modern standards and methodologies of digital forensics, and strengthen cooperation with international partners within cybersecurity programs.

Thus, the development of the Department of Digital Forensics and the creation of a dedicated faculty at the Academy of the MIA of the Republic of Uzbekistan reflect the strategic course towards strengthening the country's human and scientific-technical potential in combating cybercrime.

Core Competencies of Forensic Laboratories in Digital Forensics

The core competencies of FLs in digital forensics include:

1.Lawful seizure and preservation of digital media.

2.Recovery of deleted data and decoding of information arrays.

3.Extraction of data from mobile devices, cloud services, and messengers.

4.Analysis of network events, logs, browser and application artifacts.

5.Preparation of expert conclusions and participation in court proceedings.

An important focus is the development of national methodologies and quality standards adapted to the local legal system.

Infrastructure and Equipment

The effectiveness of FLs directly depends on modern hardware-software complexes and secure data infrastructures. The basic toolkit includes solutions for mobile forensics (UFED, XRY, Magnet AXIOM, Belkasoft, etc.), workstations for storage and file systems (APFS, ext4, NTFS), cryptanalysis and password-recovery systems, as well as server storage with integrity control (WORM/immutable policies), redundancy, and access segmentation.

Other essential components include secure workstations with "clean environment" policies, autonomous networks for malware analysis (sandboxes), tools for working with network dumps and IoT, calibration and validation of tools, regular interlaboratory comparisons, and documentation of the chain of custody.

Human Resources

The shortage of qualified personnel is the main constraint to development. To minimize risks, a multi-level model is proposed:

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

- Basic training — operational skills in seizure and initial documentation.
- Advanced training — analysis of OS, mobile platforms, cloud services, and cryptographic data.
- Specialized training — reverse engineering, malware analysis, crypto-assets, network investigations.

It is important to implement a unified competency framework in digital forensics linked to positions and levels of responsibility, provide academic tracks (Master's, PhD), internships, and interdepartmental mentoring. International courses and certifications should be combined with local training programs based on specialized institutions.

Legal Framework and International Cooperation

The development of FLs is impossible without updating procedural norms governing work with electronic evidence, including cross-border requests. Practice shows the need to unify requirements for seizure protocols, digital signatures, and integrity verification, as well as to create interdepartmental registers of expert methodologies.

At the international level, mechanisms for the rapid exchange of data are in demand, while ensuring human rights and data protection requirements. It is recommended to deploy national guidelines for cooperation with foreign service providers, considering MLAT and other procedures.

Systemic Challenges

Systemic problems include:

1.Rapid obsolescence of tools and methodologies.
2. An imbalance between high demand for personnel and limited supply.
3.Fragmentation of departmental knowledge bases.
4.Technological and licensing restrictions on access to the best global solutions.
5.Insufficient maturity of information security processes among other participants in criminal proceedings.

Another risk is dependence on a small number of specialists and bottlenecks in infrastructure (servers, licenses, key methodologies), which requires redundancy and documentation.

Proposed Roadmap for FL Development

1. Laboratory networking — creation of a unified departmental network of FLs with a competence catalog, request queues, unified registers of methodologies and reporting, and mechanisms for mutual resource backup.
2. Technological modernization — equipment renewal plans (3–4-year cycles), implementation of secure immutable storage and automated case management systems.
3. Methodological core — national standards of digital forensics, validation procedures, interlaboratory comparisons; regular control tests and quality audits.
4. Human resources — competency model, modular training programs, mentoring, internships, and academic tracks; support for research projects and applied R&D.
5. Law and international cooperation — updated procedural regulations, guidelines for cross-border electronic evidence requests, participation in OSCE/EU/UN and bilateral projects.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

6. Communication and prevention — cooperation with banks, payment systems, and the IT sector; digital hygiene programs for the population with a focus on countering social engineering.

Conclusion

The current surge in cybercrime is not a temporary phenomenon but a consequence of the digital transformation of the economy and social practices. The response to this challenge is the systemic development of forensic infrastructure — from institutional frameworks and unified standards to personnel policies and technological platforms.

The establishment of the Research Institute of Digital Forensics, the expansion of international training programs, and the modernization of forensic laboratories form the basis for sustainable counteraction to cyber threats and for improving the quality of investigations. Without investment in personnel, methodologies, and secure infrastructures, breakthroughs are impossible; with them, digital forensics can become a cornerstone of trust in justice in the digital age.

References:

[1] Kun.uz. Uzbekistan sees 68-fold surge in cybercrime: Nearly 2 trillion UZS stolen in five years. May 29, 2025.

[2] Gazeta.uz. Cybercrimes in Uzbekistan increase 68-fold in five years. May 31, 2025.

[3] Cyber University of Uzbekistan. Cyber University – A New Era Begins in Uzbekistan's Higher Education (MIA cybercrime data, 2024).

[4] UzDaily. Uzbekistan establishes Research Institute of Digital Forensics (Academy of Law Enforcement Agencies). June 25, 2024.

[5] OSCE. Expert-level meeting on requesting electronic evidence across borders (Tashkent, 4 December 2024). December 12, 2024.

[6] OSCE. Workshop in Uzbekistan supports development of national competency framework and training strategy on cybercrime and electronic evidence. June 3, 2025.

[7] BOMCA-10. EU strengthens digital forensics capacity in Uzbekistan (National workshop, June 3–5, 2025). June 5, 2025.

[8] Yuz.uz. In Uzbekistan, the number of cybercrimes has increased 68 times over the past five years. 2025.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4