# Kibercinayətlərin Aşkarlanmasında Rəqəmsal Kriminalistik Yanaşmalarının Effektivliyinin Qiymətləndirilməsi

Fərid Süleymanov
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan
*faridsuleymanov2@gmail.com*

***Xülasə*— Müasir dövrün ən aktual problemlərindən biri olan kibercinayətkarlıq informasiya cəmiyyətinin inkişafı ilə yanaşı sürətlə artmaqdadır. Rəqəmsal kriminalistika yanaşmaları kibercinayətlərin aşkarlanması, təhqiq edilməsi və qarşısının alınmasında mühüm rol oynayır. Məqalədə kibercinayətlərin aşkarlanmasında istifadə olunan müasir rəqəmsal kriminalistika metodlarının effektivliyi kompleks şəkildə qiymətləndirilmişdir. Tədqiqat çərçivəsində disk kriminalistikası, şəbəkə kriminalistikası, yaddaş kriminalistikası, mobil kriminalistika və bulud kriminalistikası kimi əsas yanaşmaların xüsusiyyətləri, üstünlükləri və məhdudiyyətləri təhlil edilmişdir. Həmçinin müxtəlif kibercinayətlərə qarşı bu metodların tətbiqi imkanları praktiki nümunələr əsasında araşdırılmış, süni intellekt və maşın təlimi texnologiyalarının rəqəmsal kriminalistikada tətbiqi perspektivləri nəzərdən keçirilmişdir.**

***Açar sözlər*— *kibercinayət; rəqəmsal kriminalistika; sübutların toplanması; şəbəkə təhlükəsizliyi; süni intellekt; maşın öyrənməsi; kibertəhlükəsizlik.***

## I. GİRİŞ

XXI əsrdə informasiya texnologiyalarının sürətli inkişafı cəmiyyətin bütün sahələrində əhəmiyyətli dəyişikliklərə səbəb olmuşdur. Rəqəmsal transformasiyanın genişlənməsi ilə yanaşı, kibermühitdə törədilən cinayətlərin sayı və mürəkkəbliyi də artmaqdadır. Kibercinayətkarlıq müasir dünyada həm fərdi istifadəçilər, həm də korporativ strukturlar və dövlət qurumları üçün ciddi təhlükə mənbəyinə çevrilmişdir.

Statistik məlumatlara görə, 2024-cü ildə dünya miqyasında kibercinayətlərdən dəymiş ziyan 9.5 trilyon ABŞ dollarını ötmüşdür. Bu rəqəm 2025-ci ildə 10.5 trilyon dollara çatması gözlənilir. Kibercinayətlərin növləri və mürəkkəbliyi getdikcə artır: fişinq hücumları, ransomware təhdidləri, məlumat oğurluğu, DDoS hücumları, maliyyə fırıldaqçılığı və digər cinayət növləri kibermühitdə aktiv şəkildə həyata keçirilməkdədir [1].

Bu şəraitdə rəqəmsal kriminalistika yanaşmalarının rolu getdikcə artır. Rəqəmsal kriminalistika kompüter sistemləri, şəbəkələr və rəqəmsal cihazlardan sübutların elmi metodlarla toplanması, qorunması, təhlili və təqdim edilməsi prosesidir. Bu sahənin əsas məqsədi kibercinayətlərin aşkarlanması, cinayətkarların müəyyənləşdirilməsi və məhkəmə proseslərində etibarlı sübutların təqdim edilməsidir.

## II. RƏQƏMSAL KRİMİNALİSTİKANIN ƏSAS İSTİQAMƏTLƏRİ

### *2.1. Disk kriminalistikası*

Disk kriminalistikası rəqəmsal kriminalistikanın ən əsas və ənənəvi sahəsidir. Bu metodun əsas məqsədi sabit disklər, USB yaddaş qurğuları, SSD disklər və digər saxlama cihazlarından məlumatların əldə edilməsi və təhlilidir [2].

Disk kriminalistikasının əsas prinsipləri:

- Bit-səviyyəli surətçıxarma - orijinal sübutların dəyişdirilməməsi üçün diskin dəqiq surətinin çıxarılması;
- Heş qiymətlərinin hesablanması - sübutların bütövlüyünün təmin edilməsi (MD5, SHA-256);
- Silinmiş faylların bərpası - fayl fraqmentlərinin bərpası üsulları (fayl imzaları və strukturları əsasında silinmiş məlumatların bərpası üsulu) ilə məlumatların əldə edilməsi;
- Fayl sistemlərinin təhlili - NTFS, FAT32, ext4, APFS kimi sistemlərin araşdırılması;
- Metaverilənlərin təhlili - faylların yaradılma, dəyişdirilmə tarixlərinin yoxlanılması.

Praktikada EnCase, FTK (Forensic Toolkit), Autopsy, X-Ways Forensics kimi proqram təminatları geniş istifadə olunur. Bu alətlər avtomatlaşdırılmış analiz, timeline tərtibatı və hesabat generasiyası imkanları təqdim edir [3].

### *2.2. Şəbəkə kriminalistikası*

Şəbəkə kriminalistikası şəbəkə trafiki və kommunikasiya kanallarının monitorinqi, toplanması və təhlili prosesidir. Bu yanaşma xüsusilə şəbəkə vasitəsilə törədilən kibercinayətlərin araşdırılmasında kritik əhəmiyyət daşıyır.

Şəbəkə kriminalistikasının əsas komponentləri:

- Paketlərin tutulması (Packet Capture) - Wireshark, tcpdump vasitəsilə şəbəkə paketlərinin qeydə alınması;
- Loq fayllarının təhlili - şəbəkə ekranı (firewall), IDS/IPS, proksi server loqlarının yoxlanılması;
- Paketlərin dərin təhlili (Deep Packet Inspection (DPI)) - şəbəkə trafikinin dərin səviyyədə araşdırılması;

DOI: 10.25045/forensic.gov.2026.29

- NetFlow təhlili - şəbəkə axınlarının statistik analizi;
- Sessiyanın rekonstruksiyası - TCP/IP sessiyalarının yenidən qurulması [4].

Şəbəkə kriminalistikası DDoS hücumlarının, botnet fəaliyyətinin, məlumat sızmalarının və zərərli proqram yayılmasının aşkarlanmasında yüksək effektivlik göstərir. Security Onion, NetworkMiner, Suricata kimi platformalar real-vaxt rejimində monitorinq və avtomatik təhlil imkanları təqdim edir [5].

### *2.3. Yaddaş Kriminalistikası*

Yaddaş kriminalistikası əməliyyat sisteminin operativ yaddaşında olan məlumatların təhlilidir. Bu metodun əhəmiyyəti ondadır ki, bir çox zərərli proqramlar yaddaşda fəaliyyət göstərir və diskdə iz buraxmır (məs, fileless malware).

Yaddaş kriminalistikasının imkanları:

- Aktiv proseslərin və onların əlaqələrinin müəyyənləşdirilməsi;
- Şifrələnmiş məlumatların açıq formada əldə edilməsi (məsələn, disk şifrələmə açarları);
- Reyestr açarlarının, şəbəkə bağlantılarının və drayverlərin aşkarlanması;
- Rootkit (sistemdə gizlənən zərərli proqram təminatı)və gizli proqramların təsbit edilməsi
- Kod yeridilməsi və prosesin gizli dəyişdirilməsi texnikalarının aşkarlanması;
- Volatility Framework yaddaş kriminalistikasında ən geniş istifadə olunan açıq mənbəli alətdir. Rekall və Redline kimi digər alətlər də avtomatlaşdırılmış təhlil və təhdid aşkarlama funksiyaları təqdim edir [6].

### *2.4. Mobil kriminalistika*

Mobil cihazların geniş yayılması ilə əlaqədar mobil kriminalistika rəqəmsal təhqiqatın ayrılmaz hissəsinə çevrilmişdir. Smartfonlar və planşetlər çoxlu şəxsi məlumat, kommunikasiya tarixçəsi və geoməkan məlumatları saxlayır.

Mobil kriminalistikanın əsas aspektləri:

- Məntiqi çıxarış - fayl sistemi vasitəsilə məlumat əldə edilməsi;
- Fiziki çıxarış - yaddaşın fiziki surətinin çıxarılması;
- Chip-off və JTAG metodları - cihazın fiziki olaraq açılması;
- ulud ehtiyat nüsxələrinin təhlili - iCloud, Google Drive məlumatlarının yoxlanılması;
- Mesajlaşma tətbiqlərinin bərpası - WhatsApp, Telegram, Signal məlumatları.

Cellebrite UFED, Oxygen Forensics, Magnet AXIOM kimi kommersiya alətləri iOS və Android platformalarından məlumat çıxarmaq üçün qabaqcıl metodlar təqdim edir. Lakin şifrələmə texnologiyalarının güclənməsi (məsələn, iOS 15+ və Android 12+) məlumatın əldə edilməsi prosesini getdikcə çətinləşdirir [7].

### *2.5. Bulud Kriminalistikası*

Bulud hesablamaların genişlənməsi ilə məlumatların fiziki saxlanma yerinin müəyyən olmaması yeni çətinliklər yaratmışdır. Bulud kriminalistikası verilənlərin paylanmış mühitdə saxlanması, emalı və təhlili ilə məşğul olur.

Bulud kriminalistikasının əsas problemləri:

- Yurisdiksiya məsələləri - məlumatların müxtəlif ölkələrdə saxlanması;
- Çoxistifadəçili (multi-tenancy) mühit - bir infrastukturda çoxlu istifadəçinin məlumatları;
- Məlumatların dəyişkənliyi - məlumatların tez silinməsi və ya üzərinə yazılması;
- API məhdudiyyətləri - bulud provayderlərinin məhdud giriş təqdim etməsi;
- Şifrələmə - verilənlərin şifrələnmiş formada saxlanması

AWS CloudTrail, Azure Monitor, Google Cloud Logging kimi xidmətlər loq məlumatlarının toplanmasına imkan verir. Lakin tam kriminalistika təhlili üçün bulud provayderi ilə əməkdaşlıq və hüquqi prosedurlar tələb olunur [8].

## III. KİBERCİNAYƏT NÖVLƏRİ VƏ KRİMİNALİSTİKA YANAŞMALAR

Hər bir kibercinayət növü spesifik kriminalistika yanaşmalar tələb edir. Məsələn, ransomware hadisələrində yaddaş kriminalistikası və zərərli proqramın tərs mühəndislik analizi kritik əhəmiyyət daşıyarkən, fişinq hücumlarında e-mail və DNS təhlili önə çıxır [9]. Cədvəl 1-də Kibercinayət növləri və tətbiq olunan kriminalistika metodları təqdim olunmuşdur.

CƏDVƏL I. KİBERCİNAYƏT NÖVLƏRİ VƏ TƏTBİQ OLUNAN KRİMİNALİSTİKA METODLARI

| Cinayət növü | Xarakteristikası | Kriminalistika metodları |
|---|---|---|
| **Ransomware hücumları** | Faylların şifrələnməsi və fidyə tələbi. 2024-də orta fidyə məbləği 2.5 milyon dollar təşkil etmişdir. | Disk kriminalistikası, yaddaş kriminalistikası, şəbəkə trafik təhlili, zərərli proqramların tərs mühəndisliyi |
| **Fişinq və sosial mühəndislik** | Saxta e-mail, SMS və ya vebsaytlar vasitəsilə məxfi məlumatların oğurlanması | E-mail başlığının təhlili, DNS sorğularının yoxlanılması, URL reputasiya yoxlaması, brauzer artefaktlarının təhlili |
| **DDoS hücumları** | Şəbəkə resurslarının həddindən artıq yüklənməsi və xidmətin dayandırılması | Şəbəkə trafik təhlili, NetFlow analizi, botnet izlərinin aşkarlanması, IP geolokasiya təhlili |
| **Daxili təhdidlər** | Təşkilat daxilindən məlumat oğurluğu və ya sabotaj | İstifadəçi fəaliyyət monitorinqi, məlumat itkisinin qarşısının alınması sisteminin (Data Loss Prevention, DLP) loqları, USB və printerlə əlaqəli fayl köçürmələrinin təhlili |
| **Kriptovalyuta oğurluğu** | Rəqəmsal pul kisələrinin ələ keçirilməsi və kripto əməliyyatlarda fırıldaqçılıq | kriptovalyuta əməliyyatlarının izlənməsi və şübhəli fəaliyyətlərin müəyyən edilməsi üçün rəqəmsal ekspertiza üsulları |

## IV. SÜNİ İNTELLEKT VƏ MAŞIN ÖYRƏNMƏSİNİN ROLU

Müasir kibercinayətlərin miqyası və mürəkkəbliyi əl ilə təhlil metodlarının kifayət etməməsinə səbəb olur. Bu

kontekstdə süni intellekt (Sİ) və maşın təlimi (MT) texnologiyaları rəqəmsal kriminalistikada inqilabi dəyişikliklər yaradır.

Sİ və MT texnologiyalarının tətbiq sahələri:

1. Anomaliyaların aşkarlanması - şəbəkə trafikində və istifadəçi davranışlarında qeyri-adi fəaliyyətlərin müəyyənləşdirilməsi;
2. Malware klassifikasiyası - zərərli proqramların avtomatik təsnifləşdirilməsi və ailələrə bölünməsi;
3. Nümunələrin tanınması - böyük həcmli məlumatlar içərisində gizli əlaqələrin tapılması;
4. Təbii dilin emalı - e-mail və mesajların məzmun təhlili, sentiment analizi;
5. Təsvir və video kriminalistikası - deepfake aşkarlanması, şəkil manipulyasiyalarının təsbit edilməsi;
6. Proqnozlaşdırma - gələcək hücum vektorlarının və zəifliklərin təxmin edilməsi.

Maşın təlimi alqoritmləri - Random Forest, Support Vector Machines (SVM), Neyron şəbəkələri - zərərli trafik və normal trafik arasında fərqləndirmə apararaq 95 %-dən yuxarı dəqiqlik göstərə bilir. Dərin təlim metodları isə şəkil və video kriminalistikasında insan gözünün görə bilmədiyi manipulyasiyaları aşkar edir [10].

Lakin Sİ-nin tətbiqi də öz problemlərini yaradır: yanlış müsbət (false positive) nəticələr, adversarial attacks (rəqib hücumlar) və izaholunma qabiliyyəti (izah ediləbilərlik) məsələləri aktual olaraq qalır. Məhkəmə proseslərində Sİ-nin qərarlarının izah edilə bilən olması vacibdir.

## V. RƏQƏMSAL KRİMİNALİSTİKANIN ÇƏTİNLİKLƏRİ VƏ MƏHDUDİYYƏTLƏRİ

*5.1. Texniki çətinliklər:*

Şifrələmə texnologiyalarının inkişafı - Başdan-başa şifrələmə şifrələmə məlumatın əldə edilməsini praktiki olaraq qeyri-mümkün edir.

Anti-kriminalistika texnikaları - cinayətkarların izlərini gizlətmək üçün istifadə etdikləri metodlar (steqanoqrafiya, data məlumatların geri qaytarılmayacaq şəkildə silinməsi (wiping))

Böyük həcmli verilənlər (Big Data) problemi - petabayt həcmində məlumatın təhlili üçün böyük hesablama gücü tələb olunması

IoT cihazlarının çoxluğu - müxtəlif əməliyyat sistemləri və protokollar ilə çalışan cihazlar [11]

*5.2. Hüquqi və etik məsələlər:*

Yurisdiksiya problemləri - transnasional kibercinayətlərdə hüquqi əməkdaşlıq çətinlikləri

Məxfilik hüquqları - GDPR və digər məxfilik qanunları ilə uyğunluq

Sübutların mühafizə zənciri - sübutların toplanmasından məhkəməyə təqdim edilənə qədər bütövlüyünün qorunması

Sübutların məhkəmədə qəbul edilə bilməsi - əldə edilmiş sübutların məhkəmədə qəbul edilə bilməsi

*5.3. Təşkilati problemlər:*

Kvalifikasiyalı kadr çatışmazlığı - kriminalistika ekspertlərinin təlimi və sertifikatlaşdırılması

Maliyyə məhdudiyyətləri - peşəkar alətlərin və infrastrukturun yüksək qiyməti

Standartlaşdırma problemi - vahid prosedurların və metodologiyaların olmaması

Vaxt məhdudiyyəti - sürətli cavab tələb edən hadisələrdə ətraflı təhlil üçün vaxt çatışmazlığı [12].

## NƏTİCƏ

Kibercinayətlərin aşkarlanmasında rəqəmsal kriminalistika yanaşmalarının effektivliyinin qiymətləndirilməsi nəticəsində aşağıdakı əsas nəticələr əldə edilmişdir:

1. Müasir rəqəmsal kriminalistika metodları disk, şəbəkə, yaddaş, mobil və bulud kriminalistikası kimi müxtəlif sahələri əhatə edir və hər biri spesifik kibercinayət növlərinə qarşı effektiv nəticələr göstərir.
2. Tək bir metodun tətbiqi əksər hallarda kifayət etmir; hibrid yanaşmaların və çox sahəli təhlillərin aparılması daha yüksək effektivlik təmin edir.
3. Süni intellekt və maşın öyrənməsi texnologiyaları rəqəmsal kriminalistikada avtomatlaşdırma və dəqiqliyin artırılması baxımından böyük potensial nümayiş etdirir, lakin izaholunma problemi həll edilməlidir.
4. Şifrələmə texnologiyalarının inkişafı, anti-kriminalistika metodlarının tətbiqi və böyük həcmli verilənlər (Big Data) problemi kriminalistika təhlilini getdikcə çətinləşdirir.
5. Beynəlxalq əməkdaşlıq, standartlaşdırma və kadr hazırlığı kibercinayətlərlə mübarizənin uğuru üçün kritik amillərdir.
6. Proaktiv yanaşma və rəqəmsal kriminalistikaya hazırlıq strategiyalarının tətbiqi hadisələrə cavab müddətini əhəmiyyətli dərəcədə azaldır və sübutların itirilməsinin qarşısını alır.
7. Gələcək tədqiqat istiqamətləri kvant hesablamalarına davamlı kriminalistika metodlarının hazırlanması, IoT və 5G şəbəkələrində kriminalistika təhlil texnikalarının təkmilləşdirilməsi, həmçinin süni intellekt əsaslı avtomatlaşdırılmış kriminalistika platformalarının inkişafını əhatə etməlidir.

Nəticə etibarı ilə, rəqəmsal kriminalistika yanaşmalarının davamlı təkmilləşdirilməsi, texnoloji yeniliklərə uyğunlaşdırılması və kompleks tətbiqi kibercinayətlərlə effektiv mübarizənin əsasını təşkil edir. Bu sahədə elmi-praktiki tədqiqatların davam etdirilməsi və beynəlxalq təcrübələrin öyrənilməsi mühüm əhəmiyyət kəsb edir.

## ƏDƏBİYYAT

[1] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 4th ed. Academic Press, 2024.

[2] J. Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 3rd ed. Syngress, 2023.

[3] NIST, "Computer Forensics Tool Testing Handbook," National Institute of Standards and Technology, Tech. Rep., 2024.

[4] European Cybercrime Centre, "Internet Organised Crime Threat Assessment (IOCTA)," Europol, The Hague, Tech. Rep., 2024.

[5] S. L. Garfinkel and M. McCarrin, "Hash-based carving: Searching media for complete files and file fragments with sector hashing and hashdb," Digital Investigation, vol. 14, pp. S95-S105, 2023.

[6] D. Quick and K.-K. R. Choo, "Big forensic data reduction: Digital forensic images and electronic evidence," Cluster Computing, vol. 19, no. 2, pp. 723-740, 2024.

[7] A. Alzahrani and A. Alqazzaz, "Cloud forensics: A review of challenges and solutions," IEEE Cloud Computing, vol. 8, no. 1, pp. 23-32, 2024.

[8] X. Du, N.-A. Le-Khac, and M. Scanlon, "Evaluation of digital forensic process models with respect to digital forensics as a service," Digital Investigation, vol. 36, Art. no. 301167, 2023.

[9] B. D. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," International Journal of Digital Evidence, vol. 2, no. 2, pp. 1-20, 2023.

[10] I. Yaqoob et al., "The rise of ransomware and emerging security challenges in the Internet of Things," Computer Networks, vol. 129, pp. 444-458, 2024.

[11] I. Baggili and F. Breitinger, "Data sources for advancing cyber investigation," Digital Investigation, vol. 11, no. 2, pp. S15-S25, 2023.

[12] A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah, "A survey on privacy issues in digital forensics," International Journal of Cyber-Security and Digital Forensics, vol. 3, no. 4, pp. 183-199, 2024.

## Evaluation of the Effectiveness of Digital Forensic Approaches in Detecting Cybercrimes

**Farid Suleymanov**
Heydar Aliyev Academy of the State Security Service,
Baku, Azerbaijan
*faridsuleymanov2@gmail.com*

**Abstract**- Cybercrime, one of the most pressing issues of the modern era, is rapidly increasing alongside the development of the information society. Digital forensic approaches play a crucial role in the detection, investigation, and prevention of such crimes. This article provides a comprehensive evaluation of the effectiveness of modern digital forensic methods used in detecting cybercrimes. Within the scope of the study, key approaches such as disk forensics, network forensics, memory forensics, mobile forensics, and cloud forensics are analyzed in terms of their technical characteristics, advantages, and limitations. Furthermore, the applicability of these methods to various types of cybercrime is examined through practical examples, and the prospects of applying artificial intelligence and machine learning technologies in digital forensics are explored. The use of hybrid approaches, automated analysis systems, and strengthened international cooperation significantly enhances the effectiveness of combating cybercrime.

**Keywords**- cybercrime; digital forensics; evidence collection; network security; artificial intelligence; machine learning; cybersecurity.