Rəqəmsal Sübutların Bütövlüyünün Təmin Edilməsi: Kriptoqrafik və Kriminalistik Mexanizmlər

Akif Orucəliyev[1], Fərid Süleymanov[2], Vüqar Hüseynli[3]
[1,2,3]Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası
[1]*akiforuceliyev@gmail.com*, [2]*faridsuleymanov2@gmail.com*, [3]*huseynlivq@gmail.com*

***Xülasə*— Rəqəmsal sübutların bütövlüyünün qorunması müasir məhkəmə-hüquq sistemində mühüm rol oynayır və ədalətli qərarların verilməsində əsas amillərdən biri hesab olunur. Bu məqalədə sübutların toplanması, saxlanması və təqdim edilməsi mərhələlərində onların etibarlılığını və hüquqi qəbuledilənliyini .təmin edən əsas mexanizmlər təhlil olunur. Xüsusilə heş funksiyaları, rəqəmsal imzalar və zəncirvari nəzarət (chain of custody) kimi kriptoqrafik və kriminalistik üsulların tətbiqi araşdırılır. Bununla yanaşı, sübutların dəyişdirilməsinin qarşısının alınması, onların orijinallığının qorunması və məhkəmə prosesində düzgün təqdim edilməsi üçün istifadə olunan metodların əhəmiyyəti vurğulanır. Bu yanaşmalar rəqəmsal kriminalistik ekspertizanın etibarlılığını artırır və hüquqi proseslərin şəffaflığını təmin edir.**

Açar sözlər— rəqəmsal sübutlar; kriptoqrafiya; kriminalistika; heş funksiyası; rəqəmsal imza; zəncirvari nəzarət.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı ilə cinayətlərin törədilməsi və araşdırılması üsulları da əsaslı şəkildə dəyişmişdir. Müasir dövrdə cinayətlərin əksəriyyəti rəqəmsal izlər buraxır və ya tamamilə virtual mühitdə baş verir. Bu kontekstdə rəqəmsal sübutların düzgün toplanması, saxlanması və məhkəməyə təqdim edilməsi mühüm əhəmiyyət kəsb edir.

Rəqəmsal sübutların ən kritik xüsusiyyətlərindən biri onların asanlıqla dəyişdirilə bilməsidir. Fiziki sübutlardan fərqli olaraq, rəqəmsal məlumatlar iz buraxılmadan dəyişiklik edilə bilər. Bu səbəbdən rəqəmsal sübutların bütövlüyünün təmin edilməsi üçün xüsusi kriptoqrafik və texniki mexanizmlərdən istifadə olunur [1].

Məqalənin məqsədi rəqəmsal sübutların bütövlüyünün təmin edilməsində istifadə olunan müasir kriptoqrafik və kriminalistik metodların təhlili, onların praktiki tətbiqi və mövcud problemlərin müəyyənləşdirilməsidir.

II. RƏQƏMSAL SÜBUTLARIN BÖTÜVLÜYÜ KONSEPSİYASI VƏ KRİPTOQRAFİK MEXANİZMLƏR

2.1. Bütövlüyün Tərifi və Əhəmiyyəti

Rəqəmsal sübutların bütövlüyü dedikdə, məlumatın toplanma anından məhkəmədə təqdim olunmasına qədər olan bütün mərhələlərdə onun orijinal halının qorunması başa düşülür. Bütövlük üç əsas komponenti əhatə edir:

- Məlumat bütövlüyü (Data Integrity) – sübutun məzmununun dəyişməz qalması;
- Autentiklik (Authenticity) – sübutun həqiqətən iddia edilən mənbədən gəlməsi;
- Zəncirvari nəzarət (Chain of Custody) – sübutun hər bir hərəkətinin sənədləşdirilməsi.

2.2. Bütövlüyə Təhdidlər

Rəqəmsal sübutların bütövlüyünə bir sıra təhlükələr mövcuddur:

- Qəsdən dəyişdirilmə – zərərli niyyətlə sübutların manipulyasiyası;
- Təsadüfi zədələnmə – texniki səhvlər və ya qeyri-peşəkar işlənmə nəticəsində pozulmalar;
- Metadata dəyişikliyi – fayl yaranma tarixi, dəyişdirilmə tarixi kimi məlumatların modifikasiyası;
- Anti-kriminalistik texnikalar – izlərin silinməsi və ya çaşdırıcı məlumatların əlavə edilməsi [2].

Kriptoqrafik mexanizmlər

1) Heş Funksiyaları

Heş funksiyaları rəqəmsal sübutların bütövlüyünün təmin edilməsinin təməl daşıdır. Bu funksiyalar istənilən həcmdə məlumata sabit uzunluqda unikal rəqəmsal "barmaq izi" (heş qiyməti) yaradır. Cədvəl I-də rəqəmsal kriminalistikada geniş istifadə olunan heş alqoritmlər təqdim edilmişdir.

CƏDVƏL I. RƏQƏMSAL KRİMİNALİSTİKADA GENİŞ İSTİFADƏ OLUNAN HEŞ ALQORİTMLƏRİ

Alqoritm	Heş qiyməti (bitlərlə)	Təsvir
MD5	128	Köhnəlmiş, kolliziyalara həssas (hazırda istifadədən çıxarılmış)
SHA-1	160	2017-ci ildən etibarən təhlükəsiz hesab edilmir, tədricən istifadədən çıxarılır
SHA-256	256	Hazırda ən çox istifadə edilən standart, yüksək təhlükəsizlik səviyyəsi
SHA-512	512	Maksimum təhlükəsizlik tələb edən hallarda istifadə olunur
SHA-3	224-512	Ən son NIST standartı, fərqli arxitektura (Keccak), gələcək perspektivli

Heş funksiyasının əsas xassələri:

DOI: 10.25045/forensic.gov.2026.40

- Determinizm – eyni məlumata həmişə eyni heş qiymət verir;
- Tez hesablana bilmə – böyük fayllar üçün də sürətli işləyir;
- Tərs hesablanma çətinliyi – heş (qiymətindən) orijinal məlumata qayıtmaq qeyri-mümkündür - məlum heş qiymətinə görə orijinal məlumatın bərpası praktik həll edilməyən məsələdir.

Kolliziyaya dözümlülük – iki fərqli məlumat üçün eyni heş dəyəri (qiyməti) əldə etmək praktiki həll edilməyən məsələdir.

2) Rəqəmsal İmzalar

Rəqəmsal imzalar sübutun autentikliyini və mənbəyini təsdiq etməyə imkan verir. PKI (Public Key Infrastructure) əsasında işləyən bu mexanizm aşağıdakı funksiyaları təmin edir [3]:

- Autentifikasiya – sübutun mənbəyinin təsdiqi (doğrulanması);
- Bütövlük – məlumatın dəyişməz qalmasının təsdiqi;
- İmtinanın qeyri-mümkünlüyü – əməliyyatın sonradan inkar edilə bilinməməsi.

Rəqəmsal imzanın işləmə prinsipi:

1. Sübut faylının heş qiyməti hesablanır.
2. Hesablanmış heş qiyməti faylı hazırlayanın məxfi açarı ilə şifrələnir (imza yaranır) və sübut faylı ilə birlikdə göndərilir.
3. Doğrulama zamanı alınmış sübut faylının cari heş qiyməti hesablanır, rəqəmsal imza isə göndərənin açıq açarı ilə deşifrə edilir.
4. Deşifrə edilmiş heş qiyməti cari heş qiyməti ilə müqayisə edilir. Heş qiymətləri üst-üstə düşərsə, imza etibarlı, sübut isə dəyişdirilməmiş hesab olunur. Əks halda, imza etibarsız, məlumat isə təhrif olunmuş hesab edilir [4].

III. KRİMİNALİSTİK MEXANİZMLƏR, PROSEDURLAR VƏ ONLARIN MÜASİR TƏTBİQ SAHƏLƏRİ

1) Kriminalistik təsvirin yaradılması (Forensic Imaging)

Rəqəmsal sübutların toplanmasının ilk və ən kritik addımı kriminalistik surətləmədir. Bu proses orijinal sübutun bit-for-bit dəqiq nüsxəsinin yaradılmasını əhatə edir.

Kriminalistik təsvirin yaradılması üsulları:

- Write-blocking cihazlarından istifadə – orijinal sübuta yazma əməliyyatlarının qarşısının alınması;
- DD (Data Dump) – Linux əsaslı bit-səviyyə kopyalama;
- FTK Imager, EnCase, X-Ways – peşəkar kriminalistik alətlər;
- E01, AFF formatları – sıxılmış və heş dəyəri olan kriminalistik təsvir formatları.

2) Zəncirvari Nəzarət (Chain of Custody)

Zəncirvari nəzarət sübutun toplanma anından məhkəmədə təqdim olunmasına qədər keçdiyi bütün mərhələlərin sənədləşdirilməsidir. Bu proses sübutun etibarlılığının təmin edilməsində həlledici rol oynayır [5].

Zəncirvari nəzarət sənədində qeyd edilməli məlumatlar:

- Sübutun təsviri və identifikasiya nömrəsi;
- Toplama tarixi, saatı və yeri;
- Toplayan şəxsin adı, imzası və təşkilatı;
- Sübutla hər bir əlaqə (kim, nə zaman, hansı məqsədlə);
- Saxlama şəraiti və yeri;
- Hər mərhələdə hesablanmış heş dəyərləri.

3) Yazmadan mühafizə (Write Protection) və Fiziki Təhlükəsizlik

Orijinal sübutların qorunması üçün bir sıra fiziki və proqram təminatı tədbirləri tətbiq edilir:

- Aparat səviyyəli write-blocker qurğuları – Tableau, WiebeTech kimi cihazlar;
- Faraday çantaları – mobil cihazlar üçün siqnal izolyasiyası;
- Anti-statik qablaşdırma – elektromaqnit zədələnmələrdən mühafizə;
- İqlim nəzarətli saxlama otaqları – təhlükəsiz uzunmüddətli saxlama [6].

Müasir tətbiq sahələri və texnologiyalar

1) Blokçeyn Texnologiyası

Blokçeyn texnologiyası rəqəmsal sübutların bütövlüyünün təmin edilməsində yeni imkanlar açır. Dəyişdirilməz, paylanmış reyestr sistemi sayəsində sübutların tarixçəsinin manipulyasiyasız saxlanması mümkündür.

Blokçeynin kriminalistik tətbiqləri:

- Sübutların heş dəyərlərinin blokçeyndə saxlanması;
- Zəncirvari nəzarət qeydlərinin avtomatlaşdırılması;
- Smart contracts vasitəsilə sübutlara giriş nəzarəti;
- Beynəlxalq təhqiqatlarda məlumat mübadiləsinin təhlükəsizliyi.

2) Bulud Kriminalistikası

Bulud xidmətlərinin geniş yayılması rəqəmsal sübutların toplanması və saxlanması üçün yeni çətinliklər yaradır. Multi-tenant arxitektura, jurisdiksiya məsələləri və fiziki məkandan asılılıq əlavə mürəkkəblik gətirir.

Bulud mühitində bütövlüyün təmin edilməsi mexanizmləri:

- API əsaslı sübut toplama – provayder interfeysləri vasitəsilə məlumat toplanması;
- Ani vəziyyət surəti (snapshot) və loq fayllarının

təhlükəsiz ixracı;

- Kriptoqrafik attestasiya – provayderin verdiyi sübutların təsdiqi;
- Volatil yaddaşın analizi – vyaddaş sübutlarının toplanması [7].

3) Süni İntellekt və Maşın Öyrənməsi

Süni intellekt texnologiyaları rəqəmsal sübutların təhlilində və bütövlüyünün yoxlanılmasında getdikcə daha çox istifadə olunur:

- Anomaliyaların aşkarlanması – sübutlarda qeyri-adi dəyişikliklərin müəyyənləşdirilməsi;
- Deepfake aşkarlanması – manipulyasiya olunmuş media fayllarının təsdiqi;
- Metaverilənlərin analizi – zaman nişanları və fayl atributlarında uyğunsuzluqların tapılması;
- Avtomatlaşdırılmış heş yoxlama – böyük həcmli sübutların effektiv doğrulanması.

IV. PRAKTİK TƏTBİQ, TÖVSİYƏLƏR, ÜMUMİ ÇƏTİNLİKLƏR VƏ MƏHDUDİYYƏTLƏR

1) Standart Kriminalistik Prosedur

Rəqəmsal sübutların bütövlüyünün təmin edilməsi üçün aşağıdakı addımlar tövsiyə olunur:

1. İdentifikasiya – sübutun növünün, harada yerləşdiyinin və əhəmiyyətinin müəyyənləşdirilməsi;
2. Qorunma – sübutun dəyişdirilməsinin və fraqmentlərinin yox edilməsinin qarşısının alınması;
3. Toplama – kriminalistik alətlərlə bit-bit (bit-for-bit) surətin yaradılması;
4. Heş hesablama – SHA-256/SHA-3 ilə bütövlük dəyərinin əldə edilməsi;
5. Sənədləşdirmə – zəncirvari nəzarət formalarının doldurulması;
6. Saxlama – təhlükəsiz və iqlim nəzarətli mühitdə qorunma;
7. Təhlil – iş nüsxələri üzərində araşdırmaların aparılması;
8. Təqdimetmə – məhkəmədə sübutun etibarlılığının nümayişi [8].

2) Beynəlxalq Standartlar və Sertifikatlaşdırma

Rəqəmsal kriminalistik təcrübələr bir sıra beynəlxalq standartlara uyğun aparılmalıdır (Cədvəl 2) [9].

CƏDVƏL II. BEYNƏLXALQ STANDARTLAR

Standart	Təsvir
ISO/IEC 27037	Rəqəmsal sübutların identifikasiyası, toplanması və saxlanması üzrə təlimatlar
ISO/IEC 27041	Təhqiqat metodları üzrə təminat və peşəkarlıq
NIST SP 800-86	Kriminalistik texnikaların insident response-a inteqrasiyası

3) Alətlər və Proqram Təminatı

Bütövlüyün təmin edilməsi üçün istifadə olunan əsas proqram təminatları (Cədvəl 3.

CƏDVƏL III. ƏSAS PROQRAM TƏMINATLARI

Alət	Növ	Əsas funksiyalar
EnCase Forensic	Kommersiya	Disk surətləmə, məlumat bərpası, təhlil, hesabat
FTK (Forensic Toolkit)	Kommersiya	Sürətli indeksləmə, e-poçt təhlili, şifrə sındırma
Autopsy	Açıq mənbə	Qrafik interfeys, zaman xətti analizi, fayl sistemi baxışı
Volatility	Açıq mənbə	Yaddaş kriminalistikası, zərərli proqram təminatının analizi, proses təhlili
X-Ways Forensics	Kommersiya	Sürətli onaltılıq redaktor (hex editor), disk klonlama, RAID dəstəyi
Cellebrite UFED	Kommersiya	Mobil cihaz kriminalistikası, app məlumatları, buludla sinxronizasiya

Çətinliklər və məhdudiyyətlər

1) Texniki Çətinliklər

- Şifrələnmiş sübutlar – hesablanmış heş qiymətinin hesablanmasında istifadə olunan məxfi açarın əldə edilməsinin çətinliyi;
- Anti-kriminalistik texnikalar – izlərin silinməsi, steqanoqrafiya, məlumatın qəsdən anlaşılmazlaşdırılması (data obfuscation);
- Böyük həcmli məlumatlar – terabayt səviyyəsində sübutların işlənməsi.
- Volatil sübutlar – yaddaş, şəbəkə trafiki kimi tez dəyişən məlumatlar [10].

2) Hüquqi və Prosedur Çətinlikləri

- Yurisdiksiya problemləri – beynəlxalq təhqiqatlarda qanunvericilik fərqləri;
- Məxfilik hüquqları – GDPR, KVKK (Türkiyənin "Kişisel Verilerin Korunması Kanunu") kimi qanunlarla tarazlıq;
- Rəqəmsal sübutların qəbulediciliyi – məhkəmələrdə etibarlılığın sübut edilməsi;
- Ekspert şəhadətinin keyfiyyəti – müvafiq sertifikatlaşdırılmış mütəxəssislərin çatışmazlığı.

NƏTİCƏ

Rəqəmsal sübutların bütövlüyünün təmin edilməsi müasir məhkəmə-hüquq sisteminin əsas tərkib hissəsidir. Kriptoqrafik mexanizmlər – heş funksiyaları, rəqəmsal imzalar və zaman nişanları – texniki baxımdan sübutların dəyişməz qalmasını təmin edir. Kriminalistik prosedurlar isə bu sübutların peşəkar və qanuni şəkildə toplanması, saxlanması və təqdim edilməsini mümkün edir.

Blokçeyn, süni intellekt və bulud texnologiyalarının inkişafı rəqəmsal kriminalistika sahəsində yeni imkanlar açır, eyni

zamanda yeni çətinliklər yaradır. Şifrələnmə, anti-kriminalistik texnikalar və beynəlxalq jurisdiksiya məsələləri daimi yeniləşməni və metodoloji təkmilləşdirməni tələb edir.

Gələcək perspektivlər:

- Post-kvant kriptoqrafiya – kvant kompüterlərinə davamlı heş və şifrələmə alqoritmləri;
- Avtomatlaşdırılmış zəncirvari nəzarət – IoT və blokçeyn inteqrasiyası;
- Beynəlxalq standartlaşdırma – vahid kriminalistik protokolların qəbul edilməsi;
- AI-əsaslı təhlil sistemləri – daha sürətli və dəqiq sübut qiymətləndirməsi.

Rəqəmsal sübutların bütövlüyünün təmin edilməsi təkcə texniki məsələ deyil, eyni zamanda hüquqi, etik və prosedur aspektləri əhatə edən kompleks sahədir. Bu sahədə uğur yalnız texnologiya, hüquq və təhqiqat orqanlarının sıx əməkdaşlığı ilə əldə edilə bilər.

ƏDƏBİYYAT

[1] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.

[2] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[3] Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO/IEC 27037:2012.

[4] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64-S73, 2010.

[5] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence, vol. 2, no. 2, 2003.

[6] V. Roussev and G. G. Richard, "Breaking the Performance Wall: The Case for Distributed Digital Forensics," in Digital Forensic Research Workshop, 2004.

[7] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics," arXiv preprint arXiv:1807.10359, 2018.

[8] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability," Journal of Digital Forensics, Security and Law, vol. 8, no. 2, pp. 34-47, 2013.

[9] M. Kohn, M. Eloff, and M. Olivier, "Framework for a Digital Forensic Investigation," in Information Security for South Africa, 2013.

[10] M. M. Pollitt, "An Ad Hoc Review of Digital Forensic Models," in 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2007.

Ensuring the Integrity of Digital Evidence: Cryptographic and Forensic Mechanisms

Akif Orucaliyev[1], Farid Suleymanov[2], Vugar Huseynli[3]
[1,2,3]Heydar Aliyev Academy of the State Security Service, Baku, Azerbaijan
[1]*akiforuceliyev@gmail.com*,[2]*faridsuleymanov2@gmail.com*, [3]*huseynlivq@gmail.com*

Abstract - Ensuring the integrity of digital evidence plays a crucial role in modern judicial systems and is considered one of the key factors in delivering fair decisions. This article provides a comprehensive analysis of the main mechanisms that ensure the reliability and legal admissibility of evidence during its collection, storage, and presentation stages. In particular, the application of cryptographic and forensic methods such as hash functions, digital signatures, and chain of custody is examined. Additionally, the importance of methods used to prevent tampering, preserve the originality of evidence, and ensure its proper presentation in legal proceedings is emphasized. These approaches enhance the reliability of digital forensics and ensure transparency in legal processes.

Keywords - digital evidence; cryptography; forensics; hash function; digital signature; chain of custody.