AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 9.918 IMPACT FACTOR
Volume-3| Issue-4| 2025 Published: |30-04-2025|

ZAMONAVIY RAQAMLI TERGOVLARDA TEXNOLOGIK MOSLASHUV VA TEXNIK EHTIYOJLAR

https://doi.org/10.5281/zenodo.15176244

G‘ulomov Sherzod Radjaboyevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani, dotsent, tel:+998909708464
Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti, tel:+998997481489
Zoirov Diyorbek Dilshod o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU talabasi, tel:+998994123320
Abdumutalov Behruzbek Ma’rufjonovich
Muxammad al – Xorazmiy nomidagi TATU talabasi, tel:+998979979938

Annotatsiya

Ushbu maqolada zamonaviy raqamli tergov jarayonlarida yuzaga keladigan texnologik moslashuv ehtiyoji, raqamli kriminalistika vositalarining texnik talablari, apparat va dasturiy ta’minotga qo‘yiladigan mezonlar haqida fikr yuritiladi. Shuningdek, turli operatsion tizimlar, mobil qurilmalar va bulutli texnologiyalar bilan ishlashda yuzaga keladigan dolzarb muammolar va ularni hal etish yo‘llari tahlil qilinadi.

Kalit so‘zlar

raqamli kriminalistika, texnik moslashuv, apparat ta’minoti, operatsion tizimlar, dasturiy vositalar, mobil qurilmalar

Axborot texnologiyalari jadal rivojlanayotgan davrda raqamli jinoyatlar ko‘lami kengayib bormoqda. Jinoyatchilar tomonidan turli xil qurilmalar va platformalardan foydalanilayotgani tergovchilardan zamonaviy texnik vositalar va dasturiy ta’minotlar bilan ishlashni, shuningdek, har doim yangilanib turuvchi texnologiyalarga moslashishni talab qiladi. Shu bois, raqamli kriminalistika laboratoriyalari texnologik moslashuvchanlik, apparat resurslar va turli xil tizimlarga ishlov berish bo‘yicha yuqori darajada tayyor bo‘lishi zarur.

Texnologik moslashuv zarurati. Zamonaviy tergov jarayonlarida faqat kompyuterlar emas, balki smartfonlar, planshetlar, tarmoqqa ulangan qurilmalar, bulutli saqlash tizimlari, IoT (Internet of Things) qurilmalari va hatto avtomobillar ham dalil manbai sifatida paydo bo‘lmoqda. Ushbu qurilmalar orasidagi texnologik farqlar ularni tahlil qilishda o‘ziga xos yondashuvlarni talab etadi. Misol uchun,

iOS va Android tizimlaridagi fayl tuzilmalari, ma'lumotlarni shifrlash usullari, xavfsizlik siyosatlari o'zaro farqlanadi.

Tergovchilarning texnologik muhitdagi doimiy o'zgarishlarga tezkor moslasha olishi, yangi formatlar va fayl tizimlarini tushunishi, yangi chiqqan qurilmalar bilan ishlay olish qobiliyati raqamli tergovning aniqligi va samaradorligini belgilaydi. Shu sababli, laboratoriyalar yangilanadigan uskunalar, foydalanuvchi qulay interfeyslar, kengaytiriladigan tizimlar bilan ta'minlanishi kerak.

Apparat va dasturiy ta'minot mezonlari. Raqamli kriminalistika laboratoriyalari uchun apparat va dasturiy ta'minot tanlashda aniqlik, samaradorlik va texnologik moslashuv kabi mezonlar asosiy ahamiyat kasb etadi. Laboratoriyada tahlil qilinadigan dalillarning soni, sifati va murakkabligi ortib borayotgan hozirgi davrda, ish stansiyalarining texnik imkoniyatlari tergov sifati va tezligiga bevosita ta'sir ko'rsatadi.

Avvalo, apparat vositalarni tanlashda quyidagi mezonlarga qat'iy rioya qilinishi lozim:

— ***Protsessor (CPU):*** Kriminalistik tahlillar uchun ko'p yadroli va yuqori chastotali protsessorlar zarur. Ayniqsa, parol buzish, shifrlangan fayllarni ochish, fayl tizimlarini indekslash kabi jarayonlarda ko'p yadroli arxitekturali CPU'lar ish unumdorligini sezilarli darajada oshiradi.

— ***Operativ xotira (RAM):*** Zamonaviy tahlil vositalari ko'plab ma'lumotlar bilan ishlaydi, shuning uchun RAM hajmi kamida 32 GB yoki undan ortiq bo'lishi tavsiya etiladi. Ayrim holatlarda 64 GB va hatto 128 GB xotira talab qilinadi.

— ***Saqlash tizimlari (HDD/SSD):*** SSD drayvlar yuqori tezlikda ma'lumot o'qish va yozishni ta'minlaydi, bu esa tahlil jarayonlarini sezilarli darajada tezlashtiradi. Disk tasvirlari va dalillarni saqlash uchun esa keng hajmli HDD'lar (10 TB va undan ortiq) kerak bo'ladi.

— ***Grafik protsessor (GPU):*** Hashing va password cracking kabi jarayonlarda grafik protsessorlardan foydalanish sezilarli tezlik beradi. Shuningdek, video, tasvir va media fayllarni tahlil qilishda GPU'lar samarali yechim hisoblanadi.

Shuningdek, zamonaviy laboratoriyalar turli tashqi qurilmalarni ulash va ularni tahlil qilish imkonini beruvchi interfeyslarga ega bo'lishi kerak. Masalan:

— USB 3.0/3.1/Type-C portlari,
— SD-karta o'quvchilar,
— Disk yurituvchilar (CD/DVD/Blu-ray),
— Mobil qurilma ulash modullari,
— SATA/IDE adapterlar va write-blocker qurilmalari.

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 9.918 IMPACT FACTOR
Volume-3| Issue-4| 2025 Published: |30-04-2025|

Dasturiy ta'minot tanlashda esa ko‘p platformalilik, keng formatlarni qo‘llab-quvvatlash, avtomatlashtirilgan tahlil funksiyalari kabi mezonlar muhim hisoblanadi. Quyidagi yirik dasturiy vositalar keng qo‘llaniladi:

— FTK (Forensic Toolkit): Dalillarni indekslash, tahlil qilish va hisobot tayyorlashda qulay interfeysga ega.

— EnCase: Disk nusxalarini olish, sud uchun maqbul hujjatlar tayyorlashda keng tarqalgan professional vosita.

— X-Ways Forensics: Resurslarni kam talab qiladi, lekin juda keng imkoniyatlarga ega.

— Autopsy: Ochiq kodli platforma bo‘lib, kengaytirilgan plaginlar orqali funksionalligini kengaytirish mumkin.

— Cellebrite: Asosan mobil qurilmalarni tahlil qilishda, jumladan iOS va Android operatsion tizimlarida kuchli imkoniyatlarga ega.

— Magnet AXIOM: Tarmoqlar, disklar, mobil qurilmalar va bulut xizmatlaridan dalillar yig‘ish, tahlil qilish va vizualizatsiya qilish imkonini beradi.

Ushbu dasturlar har xil operatsion tizimlar va fayl tizimlari bilan ishlay olishi zarur. Chunki zamonaviy qurilmalarda quyidagi fayl tizimlar uchrashi mumkin:

— NTFS, FAT32, exFAT (Windows)

— HFS+, APFS (macOS)

— ext3, ext4 (Linux)

— ReFS (Windows Server)

—FATX (Xbox), YAFFS (Android NAND) kabi kamroq tarqalgan tizimlar.

Bundan tashqari, barcha dasturiy vositalar ma’lumot yaxlitligini buzmasdan o‘qiy olish, dalilga zarar yetkazmasdan ko‘rish va huquqiy jihatdan maqbul hisobotlar tayyorlash imkonini berishi kerak. Shu maqsadda, dasturlar tomonidan yaratilgan har bir hisobot auditga ochiq bo‘lishi, “chain of custody” talablariga mos bo‘lishi kerak.

Yakuniy jihat — texnik va dasturiy vositalarning doimiy yangilanishi. Chunki yangi fayl formatlari, qurilmalar va hujum turlari paydo bo‘lmoqda. Laboratoriya bular bilan ishlay olish uchun yangilanib boruvchi lisenziyalarga ega bo‘lishi va xodimlar uchun muntazam treninglar o‘tkazilishi kerak.

Dasturiy ta'minot. Raqamli kriminalistika laboratoriyalari uchun dasturiy ta’minot tanlashda funksional imkoniyatlar, ko‘p platformalilik, format va fayl tizimlarining xilma-xilligini qo‘llab-quvvatlash, ma’lumot xavfsizligini saqlash imkoniyati kabi bir qator mezonlar asosiy ahamiyatga ega. Laboratoriya nafaqat klassik kompyuter tizimlari, balki mobil qurilmalar, tarmoqli qurilmalar, virtual muhitlar va bulutli platformalar bilan ham ishlay oladigan tizimlar bilan jihozlanishi lozim.

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 9.918 IMPACT FACTOR
Volume-3| Issue-4| 2025 Published: |30-04-2025|

Masalan, FTK (Forensic Toolkit) dalillarni indekslash va tahlil qilishda tezkorligi bilan ajralib turadi; EnCase esa sudga taqdim etiladigan hisobotlarni tayyorlashda keng qo‘llaniladi. X-Ways Forensics resurslarni kam talab qilsa-da, samaradorlik darajasi yuqori bo‘lgan platformadir. Autopsy esa ochiq kodli va kengaytiriluvchi arxitekturaga ega bo‘lib, byudjet cheklovlari mavjud laboratoriyalar uchun mos keladi.

Cellebrite — ayniqsa mobil qurilmalarni, ya’ni iOS va Android tizimlarida ishlovchi smartfonlarni chuqur tahlil qilishga mo‘ljallangan; Magnet AXIOM esa turli platformalarda, shu jumladan bulut xizmatlaridan ham dalillarni olish imkonini beradi. Bu vositalar mobil telefonlar, planshetlar, USB qurilmalar, tarmoq disklaridan ma’lumot yig‘ish va ularni sud uchun tayyorlashda keng foydalaniladi.

Yuqoridagi dasturlar turli xil fayl tizimlarini ham to‘liq qo‘llab-quvvatlashi kerak. Chunki zamonaviy qurilmalarda quyidagi fayl tizimlar uchraydi:

— NTFS, exFAT, FAT32 (Windows)
— HFS+, APFS (macOS)
— ext3, ext4, Btrfs (Linux)
— ReFS (Windows Server)
— FATX, YAFFS, YAFFS2, UFS, F2FS (mobil va maxsus qurilmalar)

Aynan kam uchraydigan fayl tizimlari bilan ishlay olish imkoniyati laboratoriyaning texnologik moslashuvchanligini oshiradi. Shu bilan birga, har bir dasturiy ta’minot xalqaro standartlarga mos hisobot yaratish, dalil zanjiri (chain of custody)ni buzmagan holda ma’lumotni saqlash va eksport qilish imkoniyatiga ega bo‘lishi kerak.

Mobil qurilmalar va bulutli texnologiyalar bilan ishlash. Bugungi kunda mobil qurilmalar — smartfonlar, planshetlar va boshqa portativ gadjetlar — raqamli jinoyatlarda ishtirok etuvchi asosiy vositalardan biriga aylangan. Ular orqali muloqotlar, moliyaviy tranzaksiyalar, hujjat aylanishi, joylashuv ma’lumotlari va boshqa ko‘plab dolzarb axborotlar amalga oshiriladi. Shunday ekan, mobil qurilmalardan dalillarni to‘g‘ri va ishonchli tarzda olish, saqlash va tahlil qilish tergovchilarning asosiy vazifalaridan biridir.

Mobil qurilmalar bilan ishlashda turli xil operatsion tizimlar (Android, iOS, HarmonyOS va boshqalar), ishlab chiqaruvchi modellar va xavfsizlik siyosatlari hisobga olinadi. Shu sababli laboratoriyalar quyidagilarga ega bo‘lishi zarur:

— Universal adapterlar va kabel to‘plamlari;
— OT-versiyalariga mos keluvchi sinxronlash modullari;
— Jailbreak yoki Root huquqlari orqali chuqur tizimga kirish imkoniyati;
— Shifrlangan bo‘lgan qurilmalardan ma’lumot olish texnologiyalari.

Mobil qurilmalarda dalil sifatida quyidagilar aniqlanishi mumkin: SMS va chat yozishmalari, geolokatsiya tarixi, fotosuratlar, audio, ilova faoliyati, bulutga sinxronlash loglari va hatto qurilmaning energiya sarfi asosidagi foydalanish profili.

Bundan tashqari, ***bulutli texnologiyalar*** ham kriminalistik tahlil doirasiga kiradi. Hozirda ko‘plab foydalanuvchilar fayllarni saqlash, hujjat almashish va aloqa qilish uchun bulutli xizmatlardan foydalanadi: Google Drive, iCloud, OneDrive, Dropbox kabi platformalar bular jumlasidandir. Shu sababli, tergovchilar:

— Bulutdagi akkauntlarga kirish (sud ruxsati asosida),

— Bulutga yuklangan fayllarning metama’lumotlarini aniqlash,

— Sinxronlangan qurilmalarni aniqlash va bog‘liq faoliyatni tahlil qilish kabi imkoniyatlarga ega bo‘lishi kerak.

Bulutli texnologiyalar bilan ishlashda autentifikatsiya, ikki bosqichli himoya (2FA), shifrlash usullari va log fayllar tahlili muhim o‘rin tutadi. Ko‘p hollarda bulutda saqlanayotgan ma’lumotlar real qurilmada mavjud bo‘lmasligi mumkin, shuning uchun tergovchilar bulut resurslari bilan ishlash tajribasiga ega bo‘lishi shart.

XULOSA.

Zamonaviy raqamli jinoyatlarni tergov qilish jarayonida texnologik moslashuv va texnik ehtiyojlarga e’tibor berish tergovning ishonchliligi va samaradorligini belgilovchi asosiy omillardan biridir. Maqolada ko‘rib chiqilganidek, apparat va dasturiy ta’minot mezonlari, mobil qurilmalar va bulutli texnologiyalar bilan ishlashdagi o‘ziga xosliklar tergovchilardan yuqori texnik tayyorgarlikni talab qiladi. Tergovchilarning zamonaviy qurilmalarga tez moslasha olishi, turli fayl tizimlari va operatsion tizimlar bilan ishlash tajribasi raqamli dalillarning aniqligi va qonuniyligini ta’minlaydi. Kelgusida raqamli kriminalistika laboratoriyalarining samaradorligini oshirish uchun ularni doimiy yangilanadigan texnologiyalar bilan jihozlash, ko‘p platformali yondashuvni kengaytirish va malakali mutaxassislar tayyorlash muhim vazifalardan biri bo‘lib qolmoqda.

ADABIYOTLAR:

1. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. Cengage Learning, 2018.
2. Garfinkel S. L. Digital forensics research: The next 10 years. Digital Investigation, Vol. 7, 2010.

3. Casey E. Digital Evidence and Computer Crime. Academic Press, 2011.
4. Cellebrite – www.cellebrite.com
5. AccessData FTK – www.exterro.com/ftk
6. Magnet AXIOM – www.magnetforensics.com
7. ISC2 – Certified Cyber Forensics Professional (CCFP). www.isc2.org
8. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni. 11.12.2003 y.