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|

MA'LUMOTLARNI OLISHDA ZAMONAVIY OPERATSION TIZIMLAR VA DASTURIY VOSITALARNING O'RNI

https://doi.org/10.5281/zenodo.15176231

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 raqamli kriminalistika sohasida ma'lumotlarni qo'lga kiritishda operatsion tizimlarning roli, ularning imkoniyatlari va dasturiy vositalar bilan uyg'un ishlashi tahlil qilinadi. Windows va Linux muhitlarida dalillarni yig'ish usullari, RAID tizimlar bilan ishlash, Live CD va Mini-WinFE kabi muqobil muhitlar, shuningdek, ma'lumotni tiklash va shifrlashdan chiqarishdagi ilg'or vositalar yoritiladi.

Kalit so'zlar

raqamli kriminalistika, Windows, Linux, Live CD, Mini-WinFE, RAID, deshifrlash, forensik tahlil

Raqamli jinoyatlar sonining ortib borishi raqamli kriminalistika sohasida yangi yondashuv va vositalarga bo'lgan ehtiyojni oshirmoqda. Dalillarni tezkor, aniq va qonuniy asosda yig'ish uchun tergovchilarga turli operatsion tizimlarda ishlay oladigan platformalararo vositalar zarur bo'lmoqda. Har bir operatsion tizim ma'lumotlarni olishda o'ziga xos imkoniyat va cheklovlarga ega. Maqolada zamonaviy tizimlar, vositalar va texnologiyalar tahlil qilinadi.

Windows tizimida dalil yig'ish va Mini-WinFE muhitidan foydalanish. Windows operatsion tizimi dunyo bo'yicha eng keng tarqalgan ish stoli platformasi bo'lib, ko'pchilik foydalanuvchilar tomonidan qo'llaniladi. Shu sababli, raqamli jinoyatlar yoki tergov jarayonlarida duch kelinadigan dalillar katta ehtimol bilan Windows muhitiga bog'liq bo'ladi. Windows tizimining o'ziga xosligi shundaki, u tarkibida murakkab fayl tizimlari (NTFS, ReFS), yashirin fayllar, sistem jarayonlar,

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|

avtomatik yuklanadigan komponentlar, reyestr yozuvlari va foydalanuvchi faoliyati loglarini saqlovchi strukturaviy bo‘linmalarga ega.

Windows tizimidan faol holatda ma’lumot yig‘ish, ya’ni ishlayotgan kompyuterda tahlil olib borish, dalilga zarar yetkazish xavfini tug‘diradi. Har qanday tergov harakati, masalan, papkani ochish, diskka murojaat qilish yoki ilova ishga tushirish — tizimda yangi yozuvlar paydo bo‘lishiga olib keladi. Bu esa sudda dalil yaroqliligini so‘roq ostiga qo‘yishi mumkin.

Shu bois, maxsus forensik muhitlar — xususan, Mini-WinFE (Windows Forensic Environment) — ishlab chiqilgan. Mini-WinFE bu Windows PE (Preinstallation Environment) asosida yaratilgan yengil muqobil tizim bo‘lib, kompyuterni yuklash va disk bilan o‘zaro aloqani “read-only” (o‘qish rejimi) asosida amalga oshirish imkonini beradi. Bu esa dalil qurilmasiga hech qanday yozuv kiritmasdan ma’lumotlarni olishga imkon beradi.

Mini-WinFE (Windows Forensic Environment) forensik tahlil uchun mo‘ljallangan yengil operatsion tizim bo‘lib, u Windows PE asosida yaratilgan va dalil qurilmasiga hech qanday o‘zgartirish kiritmasdan, faqat o‘qish rejimida ishlash imkonini beradi. Ushbu muhit orqali operatsion tizim yuklanmasdan turib disk tasvirini olish mumkin, shuningdek, avtomatik tarzda “write blocker” funksiyasi yoqiladi va bu diskdagi har qanday yozuvlarning oldini oladi. BitLocker shifrlangan disklar bo‘yicha esa RAMda saqlanayotgan parollar yoki kalit fayllar aniqlanib, deshifrlash jarayoni amalga oshiriladi. Mini-WinFE muhitiga o‘rnatilgan skriptlar va avtomatlashtirilgan vositalar yordamida tergovchi ma’lumot yig‘ish jarayonini sezilarli darajada tezlashtirishi mumkin. Ushbu tizim orqali fayl tizimlarini ko‘rish, ularni nusxalash va hash qiymatlarini yaratish ham mumkin. Mini-WinFE odatda Live CD yoki USB orqali yuklanadi va uni FTK Imager, OSFClone kabi forensik vositalar bilan integratsiya qilish mumkin. Bu yondashuv forensik tozalik tamoyillariga mos keladi va dalillarning sud oldida qonuniy yaroqliligini ta’minlashda muhim o‘rin tutadi.

Linux distributivlarida kriminalistik tahlil. Linux asosidagi maxsus distributivlar ham raqamli kriminalistika sohasida keng qo‘llaniladi. Bu distributivlar asosan ochiq kodli bo‘lib, turli modullarga ega va zamonaviy tahlil vositalari bilan boyitilgan. Ular odatda Live CD/USB shaklida ishlaydi va hech qanday o‘rnatishni talab qilmaydi, bu esa diskdagi mavjud fayllarga yozuv kiritmasdan tahlil o‘tkazish imkonini beradi.

Eng mashhur Linux distributivlari:

- ***CAINE*** (Computer Aided Investigative Environment): to‘liq forensik vositalar majmuasi bo‘lib, grafik interfeys va terminal orqali ishlash imkoniyatini

beradi. Unda Autopsy, Sleuth Kit, Guymager, RegRipper kabi ko‘plab tahlil vositalari mavjud.

- ***Kali Linux***: asosan xavfsizlik tahlili, penetratsion test va zaiflik aniqlash uchun ishlatiladi, lekin unda ham forensik modullar (DC3DD, Binwalk, Volatility) mavjud.

- ***DEFT Linux:*** tarmoq tahlili, virtual muhitlar va bulutli saqlash tizimlari bilan ishlash imkoniyatlariga ega. Sudga taqdim etilishi mumkin bo‘lgan hujjatlarni avtomatik yaratish imkoniyati mavjud.

- ***Sleuth Kit/Autopsy:*** bu to‘plam ochiq kodli forensik tahlil vositalaridan iborat bo‘lib, har qanday Linux distributivida mustaqil ishlatilishi mumkin.

Linux distributivlari quyidagi imkoniyatlarni taqdim etadi:

- Disklarning to‘liq sektorma-sektor nusxasini olish (bit-to-bit imaging);
- Ma’lumotlarning hash (xesh) qiymatini hisoblash (MD5, SHA-1, SHA-256);
- Fayl tizimi tahlili (NTFS, FAT32, ext4, HFS+);
- O‘chirilgan fayllarni tiklash, log fayllar va reyestr yozuvlarini tahlil qilish;
- RAID va LVM (Logical Volume Management) tizimlarida ma’lumot yig‘ish;
- Virtual muhitlar (VMware, VirtualBox) ichidagi disklarni ochish va tahlil qilish;
- Bulut saqlashlarga sinxronlangan fayllarni aniqlash.

Linux tizimlarining yana bir muhim afzalligi — ularni to‘liq avtomatlashtirilgan skriptlar bilan sozlash va dalillarni standart shaklda eksport qilish imkonidir. Bu esa ko‘p miqdordagi qurilmalar ustida ishlayotgan tergovchilar uchun vaqt va resurs tejaydi.

RAID tizimlar bilan ishlash. RAID (Redundant Array of Independent Disks) texnologiyasi ko‘p hollarda korporativ muhitda ishlatiladi. Kriminalistik tahlil uchun RAID tizimlardan ma’lumot yig‘ish murakkabroq, chunki ma’lumotlar bir nechta disklar orasida bo‘linadi yoki zaxira qilinadi.

RAID 0, 1, 5, 6 va 10 arxitekturalarining har biri turlicha konfiguratsiyani nazarda tutadi. Forensik tahlil uchun eng ko‘p duch kelinadigan holatlar RAID 0 (stripping) va RAID 5 (stripping with parity) tizimlaridir. Bu tizimlar bilan ishlashda tergovchi quyidagilarga tayyor bo‘lishi kerak:

- Har bir diskni alohida o‘qib olish;
- Tizim konfiguratsiyasini aniqlash va rekonstruksiya qilish;
- XOR asosidagi paritet ma’lumotlar yordamida to‘liq disk holatini tiklash.

Guymager va OSFClone kabi vositalar RAID tuzilmalarni aniqlash va tasvir olishda qo‘llaniladi. Shuningdek, RAID Recon va R-Studio kabi pullik vositalar murakkab konfiguratsiyalar bilan ishlashga mo‘ljallangan.

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|

Shifrlangan disklar va deshifrlash usullari. Shifrlangan disklar va fayllar bilan ishlash raqamli kriminalistika sohasida eng katta muammolardan biri sanaladi. Windowsda keng qo‘llaniladigan BitLocker, yoki Linuxda LUKS (Linux Unified Key Setup) tizimlari orqali shifrlangan disklar maxfiylikni ta’minlaydi.

- Shifrlashni ochish uchun quyidagi yondashuvlar mavjud:
- RAM tahlili orqali parolni aniqlash (dinamik holatda);
- Soxta tizim orqali foydalanuvchini parol kiritishga undash (social engineering);
- TPM (Trusted Platform Module) asosida ishga tushirilgan disklar uchun TPM ma’lumotlarini olish;
- Brute-force va dictionary attacks — vaqt va resurs talab etadi.

Cellebrite, ElcomSoft, Passware Kit Forensic kabi dasturlar shifrlangan ma’lumotlar bilan ishlashda keng qo‘llaniladi.

XULOSA.

Raqamli kriminalistikada dalillarni ishonchli, tezkor va qonuniy asosda yig‘ish uchun zamonaviy operatsion tizimlar va ularning muqobil muhitlaridan samarali foydalanish zarur. Windows tizimi uchun Mini-WinFE kabi forensik muhitlar yordamida dalillar o‘zgarmasdan nusxalanadi. Linux distributivlari esa ochiq kodli va kengaytirilgan tahlil imkoniyatlari bilan ajralib turadi. RAID tizimlar bilan ishlashda esa disk arxitekturasini tahlil qilish va to‘g‘ri rekonstruksiya qilish katta tajriba talab qiladi. Shifrlangan disklar bilan ishlash esa ma’lumotni deshifrlash bo‘yicha ilg‘or vositalarni qo‘llashni talab etadi. Xulosa qilib aytganda, tergovchilarning zamonaviy operatsion tizimlar va tahlil vositalaridan xabardorligi — raqamli dalilning sud oldida yaroqliligini ta’minlovchi asosiy omillardan biridir.

ADABIYOTLAR:

1. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. Cengage Learning, 2018.
2. Carrier B. File System Forensic Analysis. Addison-Wesley, 2005.
3. Garfinkel S. L. Digital Forensics Research: The Next 10 Years. Digital Investigation, Vol. 7, 2010.
4. Kali Linux – www.kali.org
5. CAINE Linux – www.caine-live.net
6. Passware Kit Forensic – www.passware.com/kit-forensic/
7. ElcomSoft Forensic Tools – www.elcomsoft.com
8. Cellebrite – www.cellebrite.com