RAQAMLI KRIMINALISTIKADA QO‘LLANILADIGAN ZAMONAVIY DASTURIY VOSITALARNING TAHLILI

Raxmanova Mohidil Egamberdiyevna
O’zbekiston respublikasi ichki ishlar vazirligi Akademiya
Kriminalistik ekspertizalar kafedrasi katta o’qituvchi
mohidil.rahmonova88gmail.com Tel: 971100203
https://doi.org/10.5281/zenodo.18722873

ARTICLE INFO

Qabul qilindi: 15- fevral 2026 yil
Ma’qullandi: 18- fevral 2026 yil
Nashr qilindi: 21- fevral 2026 yil

KEY WORDS

Kalit so‘zlar: raqamli kriminalistika, dalil tahlili, DumpIt, FTK Imager, WinPmem, Magnet Ram Capturer, Autopsy, Open Stego, Volatility, Wireshark.

ABSTRACT

Ushbu maqolada raqamli kriminalistika sohasida ochiq kodli dasturlarning roli, afzalliklari va qo‘llanilish imkoniyatlari tahlil qilinadi. Ochiq kodli vositalar – asosan budjet tejamkorligi, kengaytiriluvchanlik va jamoaviy rivojlantirish imkoniyatlari bilan ajralib turadi. Ushbu maqolada raqamli kriminalistikada keng qo‘llaniladigan zamonaviy dasturiy vositalar DumpIt, FTK Imager, WinPmem, Magnet Ram Capturer, Autopsy va Open stego dasturlari tizimlari tahlil qilinadi. Maqolada har bir vositaning funksional imkoniyatlari, afzalliklari, cheklovlari va ularning amaliyotdagi o‘rni solishtirilib, samaradorlik darajasi baholanadi. Tadqiqot natijalari raqamli dalillarni yig‘ish, tahlil qilish va saqlashda dasturiy yechimlarning muhim ahamiyatga ega ekanligini ko‘rsatadi.. Yakuniy qismda esa, ochiq kodli kriminalistik vositalarning istiqbollari, ulardan yanada samarali foydalanish bo‘yicha tavsiyalar beriladi.

Axborot va raqamli texnologiyalar asrida raqamli jinoyatlar ko‘lami tobora kengayib, murakkablashib bormoqda. Jahonning turli mamlakatlarida jinoyatchilikka qarshi kurashish yo‘nalishidagi tadqiqotlar natijalari yangicha rivojlanish bosqichlari jinoyatlarning yangi ko‘rinishlari shakllanishiga turtki bo‘layotganini ko‘rsatmoqda. Xususan, raqamlashtirishning yuqori sur’atlarda rivojlanishi ta’sirida jinoyatlar shakllari va uni sodir etish usullari zamonaviylashib, axborot texnologiyalari shaxsga va uning mulkiga tajovuz qilishga qaratilgan huquqbuzarliklar, shuningdek, kiberjinoyatchilikning sodir etilishida asosiy omil bo‘lmoqda.

Shu sababli hozirgi vaqtda butun dunyoda kiberjinoyatchilikka qarshi kurashishga huquqni muhofaza qiluvchi organlar faoliyatidagi eng dolzarb muammolardan biri sifatida qaralmoqda. Kiberjinoyatlarning turlari va ushbu jinoyatni sodir etayotgan shaxslar soni ortib borayotgani yangi tahdidlar yuzaga kelishi bilan izohlanmoqda. Raqamli jinoyatlar qatoriga kiberhujumlar, shaxsiy ma’lumotlarning o’g’irlanishi, firibgarlik va zararli dasturlarning tarqatilishi kiradi.

Tahlillar va statistik ma’lumotlarga ko‘ra, 2024 yilda kiberjinoyatlar ortidan keladigan yillik global zarar 11,4 trillion dollarga teng bo‘lgan, 2026 yilda 120 foiz o‘sib, 25,8 trillion dollarga yetishi bashorat qilinmoqda. Ayrim manbalarda ta’kidlanishicha, 2026 yilga kelib kiberjinoyatlar global transmilliy jinoyatlarning umumiy sonidan ko‘ra 5 baravar ko‘proq sodir etilishi kutilmoqda.

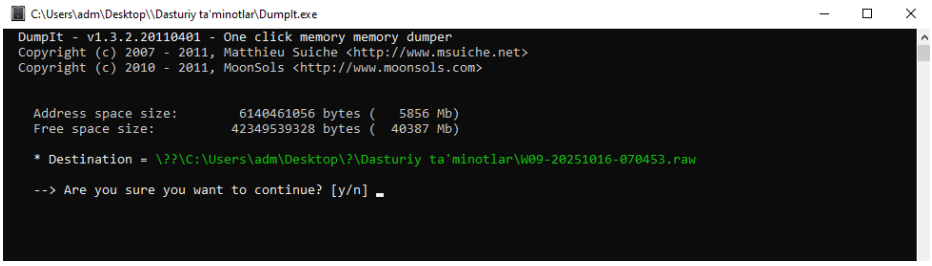
Raqamli kriminalistika — bu raqamli qurilmalardan olingan ma’lumotlarni tahlil qilish orqali jinoyatlarni aniqlash va tergov qilishga yo‘naltirilgan ilmiy soha bo‘lib, u zamonaviy jinoyatchilikka qarshi kurashda muhim rol o‘ynaydi. An’anaviy raqamli kriminalistika vositalari ko‘pincha yopiq kodli va qimmatbaho bo‘lib, ularni sotib olish va yangilab borish kichik byudjetli tashkilotlar uchun qiyinchilik tug‘diradi. Masalan, EnCase dasturining bir foydalanuvchi uchun litsenziyasi $8,284 atrofida, FTK esa $12,114 dan yuqori turadi . Bu holat ochiq kodli (open-source) dasturlarga bo‘lgan ehtiyojni oshirmoqda, chunki ular ko‘pincha bepul yoki arzon bo‘lib, keng jamoaviy qo‘llab-quvvatlashga ega. [1] Ochiq kodli raqamli kriminalistika vositalari orasida Autopsy, The Sleuth Kit (TSK), Volatility, Wireshark va CAINE Linux kabi dasturlar ajralib turadi. Masalan, Autopsy dasturi fayl tizimlarini tahlil qilish, fayllarni tiklash va tarmoq faoliyatini kuzatish imkoniyatlarini taqdim etadi . Volatility esa xotira (RAM) tahlilini amalga oshirishda foydalidir, bu esa zararli dasturlarni aniqlashda muhim ahamiyatga ega . Statistik ma’lumotlarga ko‘ra, ochiq kodli raqamli kriminalistika vositalari bozori 2023-yilda $1.4 milliardga baholangan bo‘lib, 2032-yilgacha bu ko‘rsatkich $3.2 milliardga yetishi kutilmoqda . Bu esa ushbu vositalarga bo‘lgan talabning ortib borayotganini ko‘rsatadi. O'sishning asosiy omillaridan biri butun dunyo bo'ylab kiberjinoyatlarning ko'payishi bo'lib, bu samarali tergov va hal etish uchun ilg'or raqamli kriminalistika vositalarini talab qiladi. Buzg'unchilik, ma'lumotlarning buzilishi va noqonuniy onlayn faoliyat kabi kiber tahdidlarning o'sishi murakkab va tejamkor raqamli kriminalistika vositalariga talabni oshirdi. Moslashuvchan va tejamkor bo'lgan ochiq manbali raqamli kriminalistika vositalari kiberxavfsizlik choralarini kuchaytirmoqchi bo'lgan tashkilotlar orasida katta qiziqish uyg'otdi. Bundan tashqari, turli sohalarda raqamli ma'lumotlarning o'sib borayotgan hajmi muhim ma'lumotlarni samarali tahlil qiladigan va chiqarib oladigan raqamli kriminalistika vositalariga bo'lgan ehtiyojni kuchaytirmoqda va shu bilan bozor o'sishini rag'batlantirmoqda. Ushbu maqolada ochiq kodli raqamli kriminalistika vositalarining imkoniyatlari, ularning afzalliklari va cheklovlari, shuningdek, ularni amaliyotda qo‘llash tajribalari muhokama qilinadi. Maqola, shuningdek, ushbu vositalarning kelajakdagi rivojlanish istiqbollarini ham yoritilgan.

Adabiyotlar tahlili va metodlar

Ochiq kodli raqamli kriminalistika vositalari jinoyat tergovlari va kiberxavfsizlik sohasida muhim rol o‘ynaydi. Ular orasida DumpIt, FTK Imager, WinPmem, Magnet Ram Capturer, Autopsy, Open Stego, Volatility, **Wireshark** kabi dasturlar ajralib turadi.[2]

DumpIt — bu Windows operatsion tizimlaridan xotira tasvirlarini olish uchun raqamli sud ekspertizasida keng qo‘llaniladigan samarali vosita hisoblanadi. U joriy holatda tez va oson ishga tushirilishi, shuningdek sud-tibbiy tasvir (forensic image) olish jarayonida foydalanilishi uchun mo‘ljallangan yengil va qulay dasturdir. DumpIt o‘zining oddiy interfeysi va mustaqil ishlashi tufayli xotira olish ishlarini soddalashtiradi, bu esa tergov jarayonini tezlashtirishda muhim ahamiyat kasb etadi. DumpIt vositasi buyruq satridan mustaqil bajariluvchi (portable executable) fayl shaklida taqdim etiladi. U 32-bit va 64-bit arxitekturadagi Windows tizimlarida

muammosiz ishlaydi hamda hech qanday qo‘shimcha o‘rnatishni talab qilmaydi. Shu sababli, uni USB flesh-disk yoki boshqa tashqi saqlash qurilmasiga ko‘chirib olib, kerakli paytda istalgan kompyuterda darhol ishga tushirish mumkin. Xotira tasvirini olish jarayoni juda sodda va foydalanuvchi uchun oson dastur hisoblanadi.

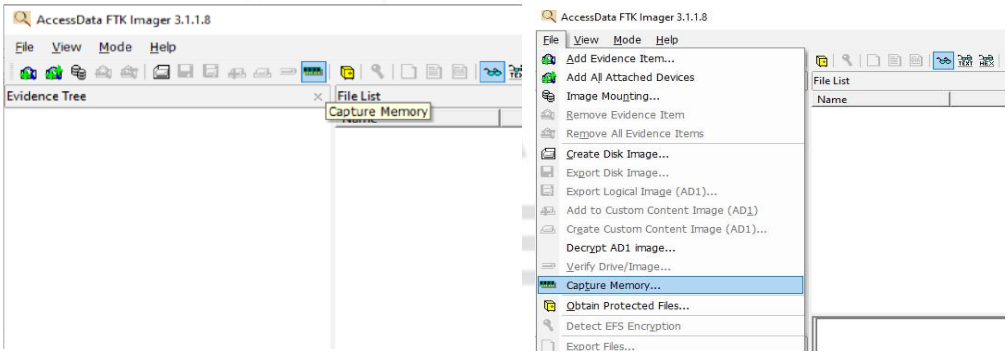


DumpIt jarayoni (ishlayotgan holati)

FTK Imager — bu AccessData kompaniyasi tomonidan ishlab chiqilgan raqamli dalillarni (digital evidence) olish, tahlil qilish va saqlash uchun mo‘ljallangan bepul forensik dasturdir.

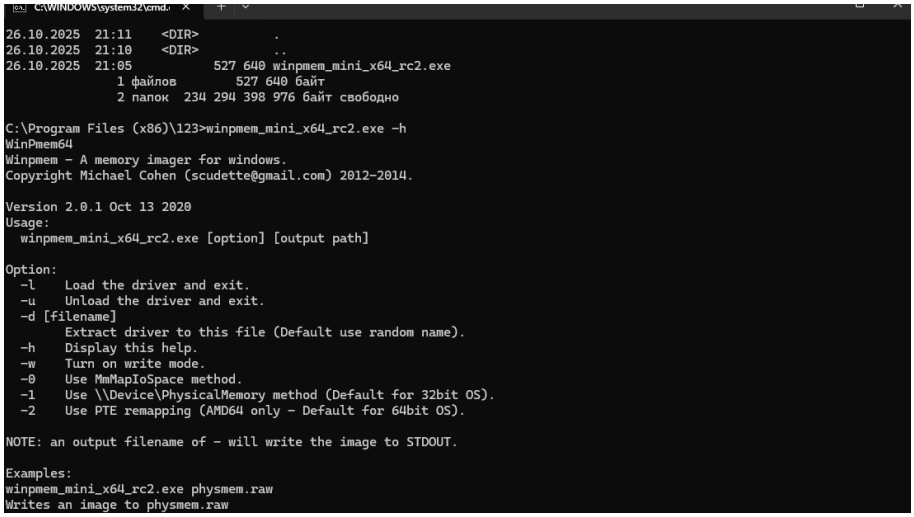
Uning asosiy vazifalari:

- Disk / fleshkadan imaging (to‘liq nusxa olish)
- Hash qiymatlar (MD5, SHA1, SHA256) hisoblash
- Fayllarni ko‘rish, deleted (o‘chirilgan) fayllarni tiklash
- Disk, partition, RAM, yoki fayl tizimlarini preview qilish (ko‘rish)
- Dalilni eksport qilish yoki E01 (EnCase image) fayl sifatida saqlash



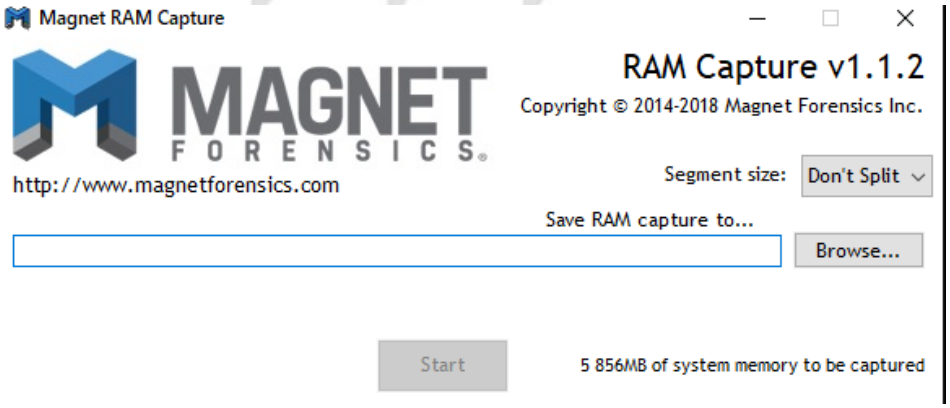
FTK-Imager interfeysi

WinPmem - bu bepul va ochiq manbali xotirani olish vositasi bo‘lib, undan Windows tizimidan xotirani tushirish uchun foydalanish mumkin. Yaroqli va ishonchli xotira tasviri bilan sud tahlilchilari shubhali hodisa haqida qimmatli ma’lumotlarga ega bo‘lishlari mumkin.



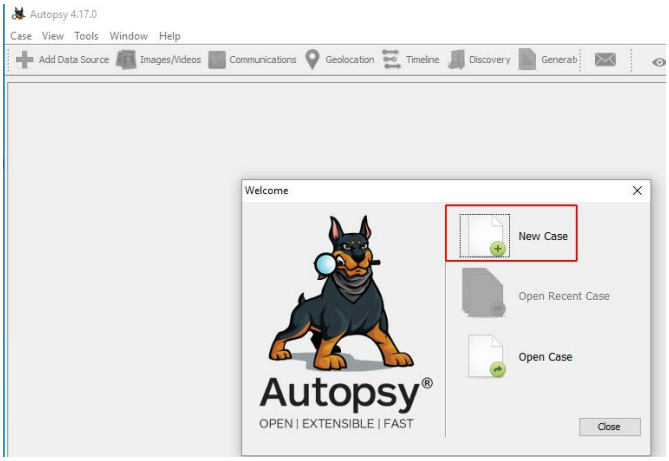
WinPmem ro‘yxati

MAGNET RAM Capture — bu Windows operatsion tizimining joriy ish holatidagi operativ xotirasini saqlab olish uchun mo‘ljallangan maxsus vositadir. Ushbu dastur, ayniqsa, sud-tergov jarayonlarida foydalanish uchun ishlab chiqilgan bo‘lib, u ishlayotgan tizimdagi o‘zgaruvchan (volatile) ma’lumotlarni saqlab olib, keyinchalik oflayn holatda tahlil qilish imkonini beradi.



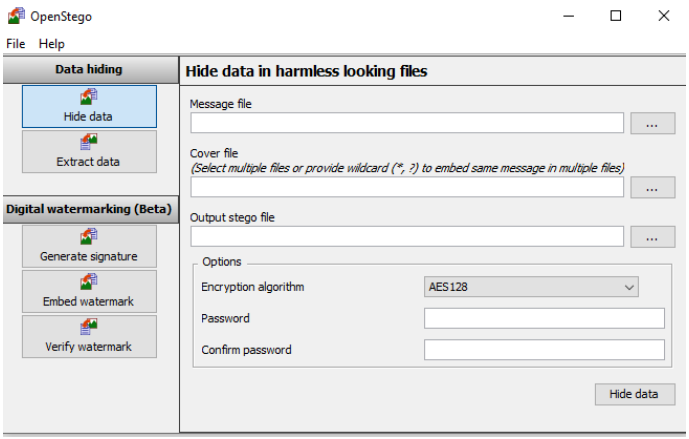
Magnet RAM Capture interfeysi

Autopsy - bu smartfonlar va qattiq disklarni samarali tahlil qiladigan raqamli raqamli kriminalistika platformasi. U butun dunyo bo'ylab ko'plab foydalanuvchilar, jumladan huquqni muhofaza qilish idoralari, harbiylar va korporatsiyalar tomonidan kompyuter tizimida tekshiruvlar o'tkazish uchun ishlatiladi. U qulay interfeysga ega, ma’lumotlarni tez qayta ishlaydi va tejamkor. Bu dastur grafik interfeysga ega bo‘lib, fayl tizimlarini tahlil qilish, o‘chirilgan fayllarni tiklash, veb-artifaktlarni ajratib olish, xesh filtrlash va kalit so‘zlar bo‘yicha qidiruv kabi funksiyalarni taqdim etadi[3].



Autopsy interfeysi

Steganografiya — bu axborotni yashirin shaklda uzatish san'ati bo'lib, uning asosiy maqsadi xabar mavjudligini yashirishdir. Steganografiya so'zi yunon tilidan olingan bo'lib, "steganos" – yashiringan, "graphein" – yozmoq degan ma'nolarni bildiradi. Steganografiyaning o'ziga xos jihati shundaki, u kriptografiyadan farqli ravishda xabarni shifrlamaydi, balki xabar borligini butunlay ko'zdan yashiradi. Masalan, kriptografiyada xabar maxsus kalit bilan shifrlanadi va o'qib bo'lmaydigan shaklga keltiriladi, steganografiyada esa xabar oddiy ko'rinadigan fayl – rasm, audio, video yoki hujjat ichiga singdirib yuboriladi. Shu sababli steganografiya bilan yaratilgan fayl tashqi tomondan hech qanday o'zgarishsiz ko'rinadi, ammo uning ichida yashirin ma'lumot mavjud bo'ladi. Bu fayllarni ochish va berkitishda **Open Stego** dasturidan foydalaniladi.



Open Stego interfeysi

Volatility: Bu dastur xotira (RAM) tahlilini amalga oshirishda foydalidir, bu esa zararli dasturlarni aniqlashda muhim ahamiyatga ega .

Wireshark: Tarmoq trafikini real vaqt rejimida tahlil qilish imkonini beruvchi vosita bo'lib, u HTTP, FTP, DNS kabi protokollarni qo'llab-quvvatlaydi[8]

Muhokama va natijalar.

Ochiq kodli dasturlarning afzalliklari bepul yoki arzon bo'lib, kichik byudjetli tashkilotlar uchun qulay hisoblanadi. Ochiq kodli dasturlarda dastur kodini o'zgartirish ya'ni dastur yoki tizimga qo'shimcha funksiyalarni qo'shish, uni o'zgartirish yoki boshqa tizimlar bilan integratsiya qilish imkoniyati mavjud. **Ochiq kodli vositalar**da foydalanuvchilar kodga

bevosita kirish huquqiga ega bo‘lganliklari sababli, dasturni yangi modullar bilan boyitilishi mumkin, maxsus ehtiyojlarga moslab o‘zgartirilishi mumkin va turli platforma yoki tizimlarga moslashtirilishi osonroq bo‘ladi. Shuningdek, j**amoaviy rivojlantirish imkoniyatlari ham mavjud. Chunki b**u ochiq kodli loyihalar ko‘pincha butun dunyo bo‘ylab dasturchilar hamjamiyati tomonidan birgalikda ishlab chiqiladi. Bu ko‘plab dasturchilar bir vaqtning o‘zida ishlashi t**ezroq rivojlanishiga, sabab bo’lishi** mumkin, ko‘proq odamlar kodni ko‘rib chiqadi va fikr bildiradi bu esa **xatoliklarni tez aniqlash va tuzatish**ga, har xil tajribaga ega ishtirokchilar yangi yechimlar taklif qiladi, bu esa **yangi g‘oyalar va takliflar kiritilishiga** jamoa tomonidan muntazam tarzda yangilanib turishiga sabab bo’ladi. Shuning uchun ochiq kodli vositalar kengaytirishga qulay va jamoaviy ishlash imkonini bergani uchun ham foydalanuvchilar orasida mashhurdir. Ochiq kodli dasturlar ba’zi hollarda rasmiy texnik yordam mavjud emasligi, sudda dalil sifatida qabul qilinishi uchun dastur vositalarining ishonchliligi va dalil zanjiri (chain of custody)ni ta’minlash zarurligi va ochiq kodli dasturlar xavfsizlik nuqtai nazaridan ba’zi zaifliklarga ega bo‘lganligini uning kamchiliklari deb qarash mumkin.[7]

Tadqiqot natijalari shuni ko‘rsatadiki, ochiq kodli va bepul tarqatiladigan dasturiy vositalar raqamli kriminalistikada katta amaliy ahamiyatga ega. Ular yirik tijoriy dasturlarga nisbatan ham samarali, ham moslashuvchan bo‘lib, ekspertlar uchun keng imkoniyatlar yaratadi. Quyida tahlil qilingan vositalarning asosiy natijalari keltiriladi:

DumpIt — operativ xotira (RAM) dan ma’lumotlarni tez va to‘liq olish imkonini beradi. Uning afzalligi — foydalanish soddaligi va minimal tizim resurslarini talab qilishi. Kamchiligi — tahlil qismi mavjud emas, faqat xotirani nusxalashni amalga oshiradi.

WinPmem — xotira nusxasini olishda yuqori aniqlikni ta’minlaydi va tizim yadrosi darajasida ishlaydi. Bu vosita dalil yaxlitligini buzmasdan ma’lumotlarni olish imkonini beradi, biroq ba’zi antiviruslar tomonidan bloklanishi mumkin.

Magnet RAM Capturer — turli Windows versiyalarida samarali ishlaydi, xotira bo‘yicha avtomatik hisobot hosil qiladi. U ilg‘or xesh tekshiruvi orqali dalilning yaxlitligini kafolatlaydi.

Autopsy — ochiq manbali eng mashhur tahlil platformalaridan biri. U fayl tizimi, metama’lumotlar, brauzer tarixi va log fayllarni chuqur tahlil qilish imkonini beradi. Shuningdek, Autopsy modulli tuzilishga ega bo‘lib, foydalanuvchilar yangi plaginlar yaratish orqali tizimni kengaytirishlari mumkin.

OpenStego — steganografik tahlil vositasi bo‘lib, fayllar ichida yashirilgan ma’lumotlarni aniqlash va dekodlash imkonini beradi. Bu vosita raqamli jinoyatlarda yashirin axborot almashinuvini aniqlashda muhim rol o‘ynaydi.

Natijalar ko‘rsatdiki, ochiq kodli vositalar raqamli dalillar bilan ishlashda **yengil, tezkor va ishonchli** natija beradi. Ularning kombinatsion qo‘llanilishi (masalan, WinPmem + Autopsy) kompleks tahlilni amalga oshirish imkonini yaratadi.

Xulosa va takliflar

O‘tkazilgan tadqiqot natijalari shuni ko‘rsatadiki, raqamli kriminalistikada qo‘llaniladigan zamonaviy ochiq kodli dasturiy vositalar dalillarni to‘plash, tahlil qilish va saqlash jarayonlarida muhim o‘rin tutadi. DumpIt, WinPmem va Magnet RAM Capturer vositalari xotira tahlilida, Autopsy esa fayl tizimi va log ma’lumotlarini tahlil qilishda yuqori samaradorlik ko‘rsatadi. OpenStego esa raqamli fayllarda yashirin ma’lumotlarni aniqlashda va steganografik faoliyatni ochishda qo‘llaniladigan muhim vosita sifatida baholandi.

Ochiq kodli vositalarning asosiy afzalliklari erkin foydalanish imkoniyati, kengaytiriluvchanlik, shaffoflik va platformalararo moslik hisoblanadi. Ular pulli dasturlarga nisbatan qulayroq, ayniqsa ta’lim muassasalari va ilmiy-tadqiqot laboratoriyalari uchun samarali yechimdir.

Biroq, bu dasturlarda ayrim kamchiliklar ham mavjud:

- Rasmiy texnik qo‘llab-quvvatlashning yo‘qligi;
- Sud-huquq amaliyotida sertifikatlanmaganlik;
- Barqarorlik va xavfsizlik bo‘yicha kafolatlarning yetishmasligi.
- Shu bilan birga, bu vositalar o‘zining ochiqligi, jamoaviy rivojlantirilishi va tezkor yangilanishi bilan raqamli kriminalistikani yangi bosqichga olib chiqmoqda. Ularni ilmiy izlanishlar, tajriba-sinov ishlari hamda amaliy ekspertiza jarayonlariga keng tatbiq etish raqamli dalillar bilan ishlashning sifatini va ishonchliligini oshiradi.

Kelajakda ochiq kodli dasturlarni sun’iy intellekt texnologiyalari bilan integratsiya qilish, bulutli tahlil platformalarida qo‘llash va yuridik sertifikatsiya tizimini takomillashtirish raqamli kriminalistikaning istiqbolli yo‘nalishlari sifatida ko‘rilmoqda. Bu texnologiyalar yanada aniqroq va tezkor natijalar beradi, masalan, yuzni tanib olish, giyohvand moddalarni tahlil qilish yoki elektron dalillarni avtomatik tahlil qilish mumkin. Aqlli uy qurilmalari, kameralar va sensorlar jinoyat dalillarini yig‘ishda muhim manba bo‘lishi mumkin. Ochiq kodli dasturlar IoT qurilmalarini tergov qilishda yordam beradi. **Virtual reallik va simulyatsiyalar yordamida j**inoyat joyini 3D rekonstruksiya qilish sud jarayonlarida dalillarni aniqroq taqdim etish imkonini beradi.

Bu esa raqamli kriminalistika sohasida yanada chuqurroq tahlil va tezkor tergov imkoniyatlarini taqdim etadi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Joakim Kävrestad, Marcus Birath, Nathan Clarke - Fundamentals of Digital Forensics_ A Guide to Theory, Research and Applications-Springer (2024) 4-bet
2. A. Bhardwaj, K. Kaushik - Practical Digital Forensics. Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD, and Memory (2023)
3. Adam Tilmar Jakobsen - Practical Cyber Intelligence_ A Hands-on Guide to Digital Forensics-John Wiley & Sons (2024)
4. M. Mason, Congressional Testimony, Statement before the House Judiciary Committee, Federal Bureau of Investigation, Washington, DC (www.fbi.gov/congress/congress07/mason101707.htm), 2007.
5. ASTM International, ASTM E2678-09 Standard Guide for Education and
6. Training in Computer Forensics, West Conshohocken, Pennsylvania (www.astm.org/Standards/E2678.htm), 2009.

7. Isa Ismail (Pharmacy Enforcement Division), Khairul Akram Zainol Ariffin (Center for Cyber Security, Universiti Kebangsaan Malaysia), Received 2024.02.14
8. Muhibullah. Mohammed - Windows Forensics Analyst Field Guide_ Engage in proactive cyber defense using digital forensics techniques-Packt (2023)
9. Shukurov K., Ochilov M., Khasanov U., Kholdorov S., Rakhmanova M. Advanced Speaker Diarization Techniques for Analyzing Uzbek Speech Signals, in: Proceedings of IEMTRONICS 2025, in: P. G. Bradford, S. K. Koul, S. A. Gadsden, K. P. Ghatak (eds), Lecture Notes in Electrical Engineering, vol. 1468, Springer, Singapore, pp. 615–629, Jan. 02 2026, DOI: https://doi.org/10.1007/978-981-95-0433-6_42