ISNN 3030-3907

2026/4
VOLUME 5

# DEVELOPMENT OF SCIENCE

## ILMIY JURNAL



# Development of science

## Ilmiy jurnal

*2026/4 VOLUME 5*

*ISSN 3030 -3907*

***Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.***

**BOSH MUHARRIR:**
***Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.***
**TAHRIRIYAT KENGASH RAISI:**
***Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor***
***TAHRIRIYAT KENGASH A’ZOLARI***

**TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ**

***Bozorov G‘ayrat Rashidovich***
*Buxoro Davlat Texnika Universiteti, professor*
***Abdurahmonov Olim Rustamovich***
*Buxoro Davlat Texnika Universiteti, professor*
***Adizov Bobur Zamirovich***
*O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor*
***Hayitov Ruslan Rustamjonovich***
*Buxoro Davlat Texnika Universiteti, professor*
***Jumayev Qayum Karimovich***
*Buxoro Davlat Texnika Universiteti, professor.*
***Berdiyev Dorob Murodovich***
*Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor*
***Maxmudov Rafiq Amonovich***
*Buxoro Davlat Texnika Universiteti, professor.*
***Tilloyev Lochin Ismatilloyevich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Raxmonov Qahramon Sanakulovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Barakayev Nusratullo Rajabovich***
*Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.*
***Jo‘rayev Xayrullo Fayziyevich***
*Buxoro Davlat Texnika Universiteti, professor.*
***Panoyev Erali Rajabboyevich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Ataullayev Sherzod Nabiullyevich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Murodov Malik Negmurodovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Axmedova Ozoda Bahronovna***
*Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.*
***Safarov Bahri Jumayevich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Xaydarov Axtam Amonovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Safarov Jasur Alijon o‘g‘li***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Асадова Раъно Дилмуратовна***
*Тошкент Давлат техника университети доценти*

**KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ**

***Axmedov Voxid Nizomovich***
*Buxoro Davlat Texnika Universiteti, professor*
***Umarov Baqo Bafoyevich***
*Buxoro Davlat Universiteti, professor*
***Kodirov Abduaxad Abduraximovich***
*Qarshi davlat Universiteti, professor*
***Qurbonov Mingniqul Jumagulovich***
*Qarshi davlat Universiteti, dotsent*
***Turemuratov Sharibay Naurizbaevich***
*O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor*
***Tursunov Kaxor Shonazarovich***
*Qarshi davlat Universiteti, professor*
***Do‘stov Hamro***
*Buxoro Davlat Texnika Universiteti, professor*
***Panoyev Nodir Shavkatovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Olimov Bobur Bahodir o‘g‘li***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Kasimov Sherzod Abduazimovich***
*Termiz Davlat Universiteti, professor.*
***Aliqulov Rustam Valiyevich***
*Termiz Davlat Universiteti, professor*
***Tropov Xamza Tursunovich***
*Samarqand Davlat Universiteti, professor*

**IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ**

***Nizamov Aslitdin Badreddinovich***
*Buxoro Davlat Texnika Universiteti, professor.*
***Boboyev Akmal Choriyevich***
*Buxoro Davlat Texnika Universiteti, professor.*
***Ergashxojayeva Shaxnoza Djasurovna***
*Toshkent davlat iqtisodiyot universiteti, professor*
***Saidaxmedova Nodira Ilxomovna***
*Toshkent davlat iqtisodiyot universiteti, professor*
***Muxsinov Bekzod Toxirovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Shakarov Qulmat Ashirovich***
*Renessans ta'lim universiteti,dotsent.*
***Jumaeva Zulfiya Qayumovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Norova Salomat Yusupovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Avezova Shaxnoza Maxmudjonovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Jalilov Jamshid G‘anijonovich***
*Toshkent davlat iqtisodiyot universiteti, dotsent*
***Xasanova Gulruh Djumanazarovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*

**PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ**

***Siddiqova Sadoqat G‘afforovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Zoyirov Erkin Xalilovich***
*Buxoro Davlat Texnika Universiteti, DSc, professor*
***Gaffarov Feruz Hasanovich***
Puchon Universiteti, *professor*
***Ruziyev Davron Yuldashevich***
*Buxoro Davlat Universiteti, professor*
***Muradova Firuza Rashidovna***
*Buxoro Davlat Texnika Universiteti, professor.*
***Yunusova Gulandon Samiyevna***
*Buxoro Davlat Texnika Universiteti, professor.*
***To‘xtayeva Zebo Sharifovna***
*Buxoro Davlat Texnika Universiteti, professor.*
***Navro‘zova Gulchixra Nigmatovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Uzoqova Laylo Polvonovna***
*Buxoro muhandislik – texnologiya instituti, dotsent.*
***To‘raqulova Marjona Qiyom qizi***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Muradova Zarina Rashidovna***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Murodov Sanjar Aslonovich***
*Buxoro Davlat Texnika Universiteti, dotsent.*
***Shodiyev Jahongir Jo‘raqulovich***
*Buxoro Davlat Texnika Universiteti, dotsent*
***Gaffarov Laziz Hasanovich***
*Buxoro muhandislik – texnologiya instituti, dotsent.*

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.



ISSN 3030-3907

**Development of science** ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.



ISSN 3030-3907

# RAQAMLI KRIMINALISTIKADA MA'LUMOTLARNI ISHLOV BERISH VA FAYL CARVING USULI ASOSIDA DALILLARNI QAYTA TIKLASH ALGORITMLARI

**Orif Allanov Menglimuratovich**
*Dotsent, PhD, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O'zbekiston*
*E-mail: allanov@tuit.uz*
**Dildora Makhkamova Begaliyevna**
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti assistent Toshkent, O'zbekiston*
*E-mail: d.maxkamova@tuit.uz*
**Ibragimov Saddambek Oybek o'g'li**
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, magistr, Toshkent, O'zbekiston*
*E-mail: saddamibragimov0804@gmail.com*
**Quyliyev Behro'z Sherzod o'g'li**
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, talaba, Toshkent, O'zbekiston*
*E-mail: behruzquyliyev06@gmail.com*

**Annotatsiya.** Ushbu maqolada zamonaviy raqamli kriminalistika vositalarining imkoniyatlari va ularga bo'lgan ehtiyojlarni baholash masalalari yoritilgan. Tadqiqot davomida apparat va dasturiy ta'minotga asoslangan kriminalistika vositalarining turlari, ularning operatsion tizimlar hamda fayl tizimlari bilan ishlash samaradorligi tahlil qilingan. Maqolaning asosiy qismi ma'lumotlarni olish, tasdiqlash va ekstraktsiya qilish jarayonlariga bag'ishlangan bo'lib, bunda o'chirilgan ma'lumotlarni qayta tiklashda fayl carving (salvaging) usulining ahamiyati ochib berilgan. Shuningdek, fayl sarlavhalarini o'n oltilik (hex) tahlil qilish orqali yashirilgan ma'lumotlarni aniqlash metodikasi WinHex va OSForensics dasturlari misolida ko'rsatib o'tilgan. Natijalar raqamli dalillar sifatini ta'minlash va tergov jarayonlarini avtomatlashtirish bo'yicha amaliy tavsiyalar beradi.

**Kalit so'zlar.** Raqamli kriminalistika, ma'lumotlarni olish (acquisition), fayl carving, ma'lumotlarni ekstraktsiya qilish, xesh qiymati, o'n oltilik tahrirlovchi (hex editor), raqamli dalil, ma'lumotlarni qayta tiklash.

**Аннотация.** В данной статье рассматриваются возможности современных инструментов цифровой криминалистики и вопросы оценки необходимости их использования. В исследовании проанализированы типы аппаратных и программных средств криминалистики, их эффективность в работе с



ISSN 3030-3907

операционными системами и файловыми системами. Основная часть статьи посвящена процессам сбора, проверки и извлечения данных, а также раскрывается важность метода восстановления удаленных данных (восстановления файлов). Кроме того, демонстрируется методология идентификации скрытых данных посредством шестнадцатеричного анализа заголовков файлов с использованием программ WinHex и OSForensics. Результаты содержат практические рекомендации по обеспечению качества цифровых доказательств и автоматизации процессов расследования.

**Ключевые слова:** цифровая криминалистика, сбор данных, восстановление файлов, извлечение данных, хеш-значение, шестнадцатеричный редактор (hex-редактор), цифровые доказательства, восстановление данных.

**Abstract.** This article discusses the capabilities of modern digital forensics tools and the issues of assessing the needs for them. The research analyzed the types of hardware and software-based forensics tools, their efficiency in working with operating systems and file systems. The main part of the article is devoted to the processes of data acquisition, verification and extraction, and the importance of the file carving (salvaging) method in recovering deleted data is revealed. Also, the methodology for identifying hidden data through hexadecimal (hex) analysis of file headers is demonstrated using the WinHex and OSForensics programs. The results provide practical recommendations for ensuring the quality of digital evidence and automating investigative processes.

**Keywords.** Digital forensics, data acquisition, file carving, data extraction, hash value, hexadecimal editor (hex editor), digital evidence, data recovery.

**KIRISH**.

Raqamli davrda texnologiyalarning keng tarqalishi natijasida ma’lumotlar hajmining misli ko‘rilmagan darajada oshishi natijasida raqamli kriminalistika ishlarida qayta ishlanishi kerak bo‘lgan ma’lumotlar miqdori tez sur’atlarda ortib borayotgani ushbu soha uchun ko‘p yillardan beri dolzarb muammo bo‘lib kelmoqda[1,2]. Biroq, muammo haligacha qoniqarli tarzda hal etilmagan. Mazkur ishdagi taklif qilinayotgan yechimda har bir yangi saqlash vositasi tasodifiy tarqalgan ma’lumotlarni o'z ichiga olgan “qora quti” deb o‘ylashdan ko'ra, biror narsani topish ehtimoli katta bo'lgan joylarda qidirish qoidasini qo’llashni ta’kidlaydi. Raqamli ma'lumotlarning o'lchami, tezligi va o'tkinchi xususiyati xavfsizlik choralari va sud ekspertizasi uchun muammolarni keltirib chiqaradi. Shu sababli, raqamli kriminalistika jinoiy tergovda ajralmas vosita hisoblanadi, shuning uchun keng qamrovli ma'lumotlar to'plamini qayta ishlash va tahlil qilishning samarali usullari zarurligini ta’kidlaydi[3]. An’anaviy xeshlash usullari va qo‘lda tekshirish yondashuvlari tasvirlar hajmining keskin oshib borishi hamda yanada



ISSN 3030-3907

murakkab manipulyatsiya va anti-forensik usullarning paydo bo‘lishi tufayli sezilarli bosim ostida qolmoqda[4.5]; bu holat ayniqsa fayl tizimi mavjud bo‘lmagan sharoitlarda amalga oshiriladigan file carving va xeshga asoslangan carving kabi raqamli kriminalistika yo‘nalishlarida yaqqol ko‘rinadi, chunki bu jarayonlar faqat saqlangan ma’lumotlarning o‘z xususiyatlariga tayanib ishlaydi[6,7]. Har qanday kriminalistik tadqiqotning muvaffaqiyati foydalanilayotgan vositalarning ishonchliligi va ma’lumotlarni tiklash jarayonidagi vaqt samaradorligiga bog‘liqdir. Tergov jarayonida duch kelinadigan eng katta muammolardan biri bu — shubhali qurilmalardagi ma’lumotlarning butunligini saqlagan holda nusxa olish va o‘chirilgan yoki yashirilgan fayllarni qayta tiklashdir.

Xususan, ma’lumotlarni ekstraktsiya qilish bosqichida qo‘llaniladigan “carving” (fayl bo‘laklarini yig‘ish) usuli raqamli ekspertizaning eng murakkab va muhim qismlaridan biri hisoblanadi. Ushbu jarayon nafaqat o‘chirilgan fayllarni topish, balki fayl sarlavhalarini (file headers) tahlil qilish orqali ataylab o‘zgartirilgan ma’lumotlarni aniqlash imkonini ham beradi.

**ADABIYOTLAR TAHLILI VA METODOLOGIYA.** Raqamli kriminalistika sohasidagi tadqiqotlar nafaqat texnik algoritmlarni, balki olingan dalillarning huquqiy maqomini belgilovchi me’yoriy asoslarni ham qamrab oladi. Xususan, raqamli dalillarni sudda tan olish masalalari Federal Evidence Review (2014) va mashhur “Frye v. U.S” kabi huquqiy pretsedentlar orqali asoslanadi. Ushbu manbalar ekspertiza natijalarining ilmiy asoslanganligi va mutaxassis xulosalarining ishonchlilik mezonlarini belgilab beradi[8,9].

Tadqiqotning texnik asosi sifatida turli xil fayl tizimlarining ishlash prinsiplarini o‘rganish muhim ahamiyatga ega. Microsoft TechNet ma’lumotlariga ko‘ra, FAT va NTFS fayl tizimlarida ma’lumotlarning joylashishi va o‘chirilgan fayllarni qayta tiklash imkoniyatlari turlicha[10,11]. Ayniqsa, yangi avlod fayl tizimi hisoblangan ReFS (Resilient File System) ning joriy etilishi ma’lumotlar butunligini ta’minlashda yangi bosqichni boshlab berdi[12,13], biroq kriminalistik nuqtai nazardan o‘chirilgan ma’lumotlarni carving qilish jarayonini biroz murakkablashtirdi.

Operatsion tizimlar ichki tuzilishini tushunish, raqamli kriminalistga tizim xotirasidagi va registrlaridagi izlarni tahlil qilish imkonini beradi[14,15]. Russinovich va Solomon (2012) kabi olimlarning tadqiqotlari Windows tizimining yadrosi va fayl vaqtlari bilan ishlash mexanizmlarini chuqur yoritib bergan bo‘lib, bu “carving” jarayonida fayllarning yaratilish va o‘zgartirilish sanalarini aniqlashda asosiy manba bo‘lib xizmat qiladi.



ISSN 3030-3907

Shuningdek, zamonaviy kriminalistikada mobil qurilmalar ekspertizasi alohida o‘rin egallaydi. Epifani va Stirparo (2015) ning iOS tizimlari bo‘yicha hamda Tamma va Tindall (2015)ning Android platformalari bo‘yicha olib borgan tadqiqotlari smartfonlardan ma’lumotlarni olish (acquisition) va tahlil qilishning amaliy metodikasini ko‘rsatib beradi[18]. Mobil qurilmalarda ma’lumotlar ko‘pincha SQLite bazalarida saqlanishi, ulardan o‘chirilgan yozuvlarni tiklashda an’anaviy fayl carving usullariga qo‘shimcha ravishda ma’lumotlar bazasi tahlilini ham talab etadi.

Zararli dasturlarni tahlil qilish borasida Sikorski va Honig (2012) tomonidan taklif etilgan “Practical Malware Analysis” metodikasi tizimga hujum uyushtirilganidan so‘ng qolgan raqamli izlarni o‘rganishda dolzarbdir. Bu usullar kiberjinoyat sodir etilgan muhitda qanday turdagi kriminalistik vositalarga ehtiyoj borligini belgilashga yordam beradi[19].

Xulosa qilib aytganda, tahlil qilingan adabiyotlar raqamli kriminalistikaning nazariy asoslaridan tortib, mobil va server platformalaridagi amaliy yechimlarigacha bo‘lgan masalalarni qamrab oladi. Bu esa raqamli dalillarni tiklash algoritmlarini ishlab chiqishda fundamental asos bo‘lib xizmat qiladi.

Raqamli kriminalistika vositalari doimiy ravishda ishlab chiqarilmoqda, yangilanmoqda. Shuning uchun yangi funksiyalar va o‘zgarishlar uchun yetkazib beruvchilarning veb-saytlarini muntazam ravishda kuzatib turish muhimdir. Ushbu yangilanishlar hozirgi kunda duch kelayotgan muammolarni hal qilishda yordam berishi mumkin.

Har qanday kriminalistika vositasini sotib olishdan oldin, vosita tergov davomida vaqt tejashini va buning tiklangan ma’lumotlarning ishonchliligiga ta’siri ko‘rib chiqiladi. Ko‘plab grafik interfeysga ega raqamli kriminalistika vositalari ko‘p resurs, xotira va tezkor protsessorlarga ega kompyuterlarni talab qiladi. Ba’zan ular ortiqcha resurslarga ega bo‘lishi mumkin, chunki boshqa dasturlar, masalan, antivirus dasturlari, fon rejimida ishlaydi. Ushbu fon rejimidagi dasturlar raqamli kriminalistika dasturi bilan resurslar uchun joy talashadi. Natijada raqamli kriminalistika dasturi yoki operatsion tizim to‘xtashi ya’ni “qaytib qolishi” mumkin, bu esa tekshiruvlardagi kechikishlarga olib keladi.

Raqamli kriminalistika vositalariga ehtiyojlarni baholash. Raqamli kriminalistika apparat va dasturiy ta’minotni xarid qilishni asoslash uchun biznes rejasini ishlab chiqish kerak. Variantlarni o‘rganayotganda, ba’zan texnik yordamni o‘z ichiga oladigan ochiq manba vositalarini ko‘rib chiqish mumkin. Maqsad imkon qadar ko‘proq funksiyalar uchun eng yaxshi narxdagi vositani topishdir. Vositalarni tanlashda quyidagilarni inobatda olish kerak:



ISSN 3030-3907

– Raqamli kriminalistika vositasi qaysi operatsion tizimda ishlaydi? Vosita bir nechta operatsion tizimlarda ishlay oladimi?

– Raqamli kriminalistika vositasi ko‘p funksiyalimi? Masalan, u Windows va Linuxda yoki macOS da ishlaydimi?

– Raqamli kriminalistika vositasi FAT, NTFS va Ext4 kabi bir nechta fayl tizimlarini tahlil qila oladimi?

– Raqamli kriminalistika vositasi takroriy vazifalarni va ishlarni avtomatlashtirish uchun skript tili bilan ishlatilishi mumkinmi?

– Raqamli kriminalistika vositasi ma’lumotlarni tahlil qilish uchun zarur bo‘lgan vaqtni kamaytirishga yordam beradigan avtomatlashtirilgan funksiyalarga egami?

– Yetkazib beruvchining mahsulot yordam berish bo‘yicha obro‘si qanday? Ochiq manba vositalari uchun, yordam berish forumlari qanday?

Raqamli kriminalistika vositalarining turlari. Raqamli kriminalistika vositalari ikki katta toifaga bo‘linadi:

apparat;

dasturiy ta’minot.

**Apparat turidagi raqamli kriminalistika vositalari**. Apparat turidagi raqamli kriminalistika vositalari oddiy, bitta maqsadli komponentlardan to‘liq kompyuter tizimlari va serverlargacha bo‘lishi mumkin. Masalan, Tableau T35es-R2 SATA/IDE eSATA ko‘prigi bitta qurilma yordamida SATA yoki IDE diskiga kirishni ta’minlaydigan bitta maqsadli komponentdir. Ba’zi to‘liq tizimlar ya’ni, Digital Intelligence F.R.E.D tizimlari, DIBS Advanced Forensic Workstations, Forensic Computers’ Forensic Examination Stations va portable units, Ace Laboratory tizimlari bo‘lib, zararlangan disklar ma’lumotlarini tiklash uchun mo‘ljallangan.

**Dasturiy kriminalistika vositalari**. Dasturiy kriminalistika vositalari buyruq satri dasturlari va grafik interfeysga ega dasturlar sifatida guruhlanadi. Ba’zi vositalar bitta vazifani bajarish uchun ixtisoslashgan. Masalan, New Technologies, Inc. (NTI) tomonidan ishlab chiqilgan SafeBack buyruq satri diskni olish vositasi sifatida mo‘ljallangan. U asosiy vosita sifatida emas, balki barcha narsalar muvaffaqiyatsiz bo‘lganda ishonchli zaxira sifatida ishlatiladi. Boshqa vositalar ko‘plab har xil vazifalarni bajarish uchun mo‘ljallangan. Masalan, PassMark Software OSForensics, X-Ways Forensics, Guidance Software EnCase, Magnet Forensics AXIOM va AccessData FTK grafik interfeysga ega vositalar bo‘lib, ko‘plab kriminalistika olish va tahlil funksiyalarini bajarishga mo‘ljallangan.



ISSN 3030-3907

Dasturiy kriminalistika vositalari odatda shubhali qurilmadan ma’lumotlarni tasvir fayliga nusxalash uchun ishlatiladi. Ko‘plab grafik interfeysli (GUI) acquisition vositalari tasvir faylida barcha tuzilmalarni asl disk kabi o‘qish va tasvir fayllarini tahlil qilish qobiliyatiga ega.

**Raqamli kriminalistika vositalarining vazifalari**. Barcha raqamli kriminalistika vositalari, apparat va dasturiy ta’minot, aniq funksiyalarni bajaradi. Yangi vositalarni sinab ko‘rayotganda, NIST tashkilotining Kompyuter kriminalistika vositalarini sinovdan o‘tkazish (CFTT) dasturi, ASTM International (ilgari Amerika Sinov va Materiallar Jamiyati) ning E2678 standartidan va Kompyuter Dalilari Xalqaro Tashkilotidan (IOCE) kelgan ko‘rsatmalarga rioya qilish foydali bo‘ladi. Shuningdek, ISO standarti 27037 (www.iso.org/standard/44381.html) raqamli dalil birinchi javobgarlarini (DEFR) tasdiqlangan vositalardan foydalanishni tavsiya etadi. Quyidagi funksiyalar toifalari raqamli kriminalistika vositalarini baholash uchun ko‘rsatmalar sifatida xizmat qiladi, ular ma’lumotlarni tahlil qilish va tiklash shuningdek, ma’lumotlar sifatini ta’minlash uchun qo‘shimcha funksiyalarni o‘z ichiga oladi:

– Ma’lumotlarni olish;
– Tasdiqlash va tekshirish;
– Ekstraktsiya;
– Qayta qurish;
– Hisobot berish.

NIST tashkilotining kompyuter kriminalistika vositalarini sinovdan o‘tkazish (CFTT) va boshqa guruhlarning qo‘shimcha funksiyalarni, masalan, ma’lumotlarni olish, mobil qurilmalardan ma’lumotlarni chiqarish, faylni qayta qurish va satr qidirish kabi funksiyalarni o‘z ichiga oladi.

**Ma’lumotlarni olish**. Ma’lumotlarni olish raqamli kriminalistika tergovlaridagi birinchi vazifa bo‘lib, asl diskning nusxasini tayyorlashdir. Ushbu protsedura asl diskni saqlashni ta’minlaydi, shunda u buzilmaydi va raqamli dalilga zarar yetmaydi. Ma’lumotlarni olish toifasidagi qo‘shimcha funksiyalar quyidagilarni o‘z ichiga oladi:

– Jismoniy ma’lumot nusxasi;
– Mantiqiy ma’lumot nusxasi;
– Ma’lumot olish formati;
– Buyruq satrida olish;
– GUI orqali olish;
– Masofadan turib fizik nusxa olish.

ISO standarti 27037 ma’lumot olishdagi eng muhim omillardan biri DEFR ning kompetensiyasi hisoblanadi va tasdiqlangan vositalardan foydalanish mumkin


ISSN 3030-3907

ekanligini ta’kidlaydi. U turli vaziyatlarda qanday qilib ma’lumot olishni yondashish bo‘yicha ko’rsatmalarni o‘z ichiga oladi. Eng muhimi, nima qilinganini va nega qilinganini hujjatlashtirishdir. Masalan, agar xavfli materiallar mavjud bo‘lgan joyda ma’lumot olib qolinsa, tezlik muhim ahamiyatga ega. Shuning uchun tezkor xotirani olishni e’tiborsiz qoldirib, qurilmalarni to‘plashga e’tibor qaratish mumkin. Shuningdek, butun jismoniy diskni nusxalash yoki faqat bir partition yoki papkaga e’tibor berish haqida qaror qabul qilish uchun oqim diagrammalarini topish kerak.

Ba’zi raqamli kriminalistika dasturiy paketlari, masalan, AccessData FTK, tasvir olish uchun alohida vositalarga ega. Masalan, Magnet AXIOM kriminalistik tasvirni olish va uni bir vaqtda qayta ishlashga imkon beradi. Biroq, ba’zi tadqiqotchilar tasvir olish uchun Tableau TD2, Logicube Talon, VOOM HardCopy 3P yoki Intelligent Computer Solutions, Inc. dan Image MASSter Solo-4 kabi raqamli kriminalistikaning apparat qurilmalaridan foydalanishni afzal ko‘radilar. Ushbu apparat qurilmalari ma’lumot olish uchun o‘rnatilgan dasturiy ta’minotga ega. Diskni nusxalash uchun boshqa qurilma yoki dastur kerak emas, ammo, ma’lumotlarni tahlil qilish uchun raqamli kriminalistika dasturiy ta’minoti kerak bo‘ladi.

Boshqa ma’lumot olish vositalari diskni olish uchun apparat qurilmalari va dasturiy vositalarni birlashtirishni talab qiladi. Masalan, ko‘plab dasturiy vositalar disklarni faqat o‘qish rejimida o‘rnatadi va boshqalari jismoniy yozuvni blokirovka qilish uskunasini talab qilishi mumkin. Har qanday vosita ichida o‘rnatilgan dasturiy ta’minotni blokirovka qilish vositasi mavjud bo‘lsa, dalilning o‘zgartirilmaganligini ta’minlash uchun uni tasdiqlash kerak.

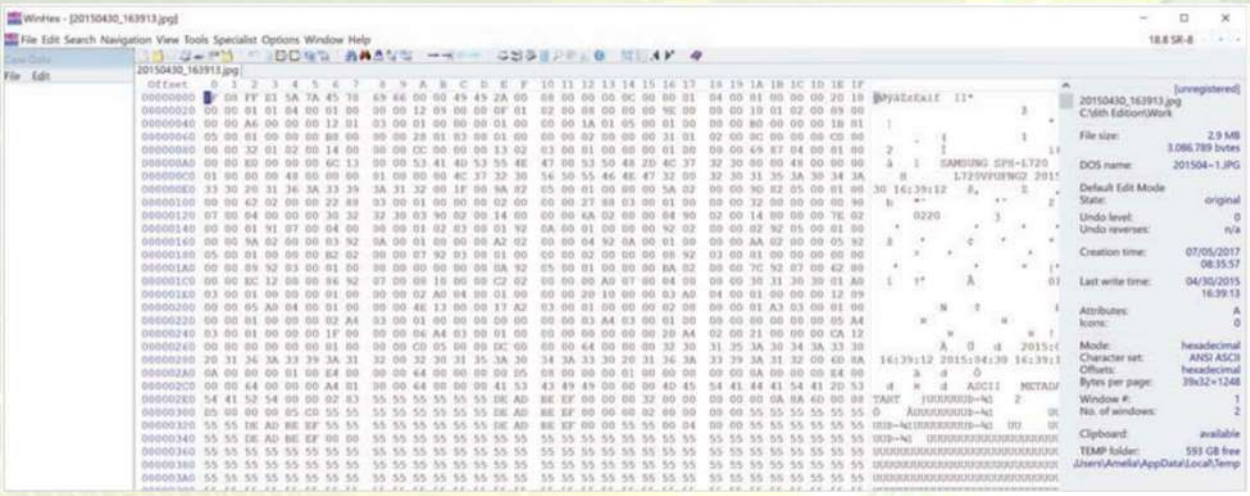
Dasturiy ta’minot orqali nusxa olishning ikkita usuli mavjud bo‘lib, ular diskning butun qismini jismoniy nusxalash va diskning partitsiyasini mantiqiy nusxalashdir. Ko‘pgina dasturiy ta’minot orqali nusxa olish vositalari butun jismoniy diskni yoki faqat mantiqiy partitsiyani tasvirlash imkoniyatini o‘z ichiga oladi. Odatda, vaziyat jismoniy yoki mantiqiy nusxa olishni tanlashni belgilaydi. Mantiqiy nusxa olishni tanlashning bir sababi disk shifrlanishidir.

Diskdan nusxa olish formatlari asl ma’lumotdan yetkazib beruvchi maxsus egoriyalargacha farq qiladi. Asl ma’lumot formati, odatda, Linux dd buyruqi yordamida yaratiladigan, ma’lumot faylining, disk partitsiyasining yoki butun diskning oddiy *“bit-for-bit”* nusxasidir. Asl formatli tasvir olish vositasi ma’lumotlarni bir diskdan boshqasiga yoki bo‘lingan fayllarga nusxalash imkoniyatini beradi. Bu haqiqiy o‘zgartirilmagan nusxa bo‘lgani uchun, asl tasvir faylida mavjud bo‘lgan ma’lumotni har qanday o‘n oltilik ko‘rinishga ega tahrirlovchi bilan ko‘rish mumkin, masalan, Hex Workshop yoki WinHex misol



ISSN 3030-3907

qilsa bo‘ladi. Ushbu vositalar ma’lumotlarning o‘n oltilik ko‘rinishini (1-rasmga qarang) yoki ochiq matnli ko‘rinishini beradi.



**1-rasm. WinHex dasturida ma’lumotlarni ko‘rish**

Kichik segmentlangan fayllarni yaratish, ishlab chiqaruvchi sotib olish vositalarida odatiy xususiyatdir. Ularning maqsadi, olingan ma’lumotlarni kichik media, masalan, CD va USB disklariga saqlashni osonlashtirishdir.

Katta tashkilotlarda fayllardan masofadan nusxa olish keng tarqalgan. Korporativ darajadagi kompaniyalar geografik jihatdan xilma-xil bo‘lganligi sababli, tergovchilar tizimlarga jismoniy kirish uchun uzoq masofalar o‘tishi kerak bo‘lishi mumkin. AccessData va EnCase kabi mashhur vositalar tarmoqda disk tasvirlarini masofadan olish imkoniyatiga ega va bu olish jarayoni “*dd”* buyrug‘i yordamida ham amalga oshirilishi mumkin.

**Tasdiqlash va tekshirish**. Tasdiqlash va tekshirish funksiyalari bir-biri bilan chambarchas bog‘liq.

*Tasdiqlash* vositaning maqsadga muvofiq ishlayotganini tasdiqlash usuli.

*Tekshirish* ikkita ma’lumot to‘plami bir xil ekanligini tasdiqlovchi jarayondir. Bu esa xesh qiymatlarini hisoblash yoki boshqa shunga o‘xshash usullar yordamida amalga oshiriladi. Boshqa bog‘liq jarayon filtratsiya, bu esa tergov natijalarini saralash va qidirish orqali yaxshi ma’lumotlarni va shubhali ma’lumotlarni ajratishni o‘z ichiga oladi. Vositalarni tasdiqlash va ma’lumotlarni tekshirish filtratsiyani amalga oshirish imkonini beradi.

Vositani tasdiqlash uchun, kompyuter va mobil qurilmalar uchun yaratilgan kriminalistik tasvirlardan foydalanish mumkin. Bu fayllar NIST tashkilotining CFTT yoki raqamli dalil bo‘yicha ilmiy ishchi guruh (SWGDE) kabi veb-saytlarda joylashtirilgan bo‘lib, ushbu vosita diskda dalil sifatida nima topishi kerakligini ko‘rsatadi. Ular natijalar chegaralarini berishi mumkin. Masalan, vosita Linux tasvirlarini olishda yaxshi ishlashini, ammo eski Windows versiyalari bilan muammolarga duch kelishini aniqlay oladi. Ushbu guruhlar, shuningdek, apparat



ISSN 3030-3907

nusxa olish vositalarini sinovdan o‘tkazish natijalarini ham chop etadi. Vositani tasdiqlagandan so‘ng, hamma kriminalistik nusxalarning bir xil xesh qiymatiga ega ekanligini ta’minlash zarur.

Barcha kriminalistika sotib olish vositalarida ma’lumot nusxalash jarayonini tekshirish usuli mavjud bo‘lib, u asl diskni tasvir bilan taqqoslaydi. Masalan, EnCase olingan ma’lumotlarning MD5 xesh qiymatini hisoblashni taklif qiladi va FTK ma’lumotlarni olish jarayonida MD5 va SHA-1 hash to‘plarini tasdiqlaydi. Image MASSter Solo-4 kabi apparat nusxa olish vositalari ma’lumot olish jarayonida bir vaqtning o‘zida MD5 va CRC-32 xeshlashni amalga oshira oladi.

Filtratsiyani amalga oshirganda, yaxshi ma’lumotlarni shubhali ma’lumotlardan ajratish kerak. Yaxshi ma’lumotlar ma’lum fayllardan iborat bo‘lib, ular operatsion tizim fayllari, umumiy dasturlar (masalan, Microsoft Word) va kompaniyaning kundalik ishlarida ishlatiladigan standart fayllarni o‘z ichiga oladi. Shuningdek, operatsion tizimning yangi o‘rnatilishi, barcha dasturlar va ma’lum yaxshi tasvirlar va hujjatlar (jadval fayllari, matn fayllari va boshqalar) uchun yaxshi xesh qiymatlari ro‘yxatini yaratish uchun ishlatish mumkin. Ushbu ma’lumotlar bilan tergovchi barcha ma’lumotlarni tanlangan yaxshi ro‘yxatga kiritmasdan, boshqa fayllarga e’tibor qaratishi mumkin. Filtratsiya shuningdek, jinoyat tergovlarida dalil uchun ma’lumotlarni topish yoki xodimni ishdan bo‘shatish, ishni qurish uchun ham qo‘llanilishi mumkin.

Bir nechta raqamli kriminalistika vositalari ma’lum orginal fayl xesh to‘plarini integratsiyalash va shubhali diskdan olingan fayl xesh qiymatlarini solishtirish imkoniyatiga ega. Ushbu jarayon bilan katta miqdordagi ma’lumotlarni tezda chiqarib tashlash mumkin, shunda dalil tahliliga e’tiborni qaratish mumkin. Shuningdek, o‘z xesh to‘plarini yaratishni boshlash mumkin. Yana bir muhim xususiyat ma’lumot sektorlarini xeshlash va solishtirishdadir. Bu, qisman o‘zgartirilgan bo‘lishi mumkin bo‘lgan disk joyidagi ma’lumotlar bo‘laklarini aniqlashda foydalidir.

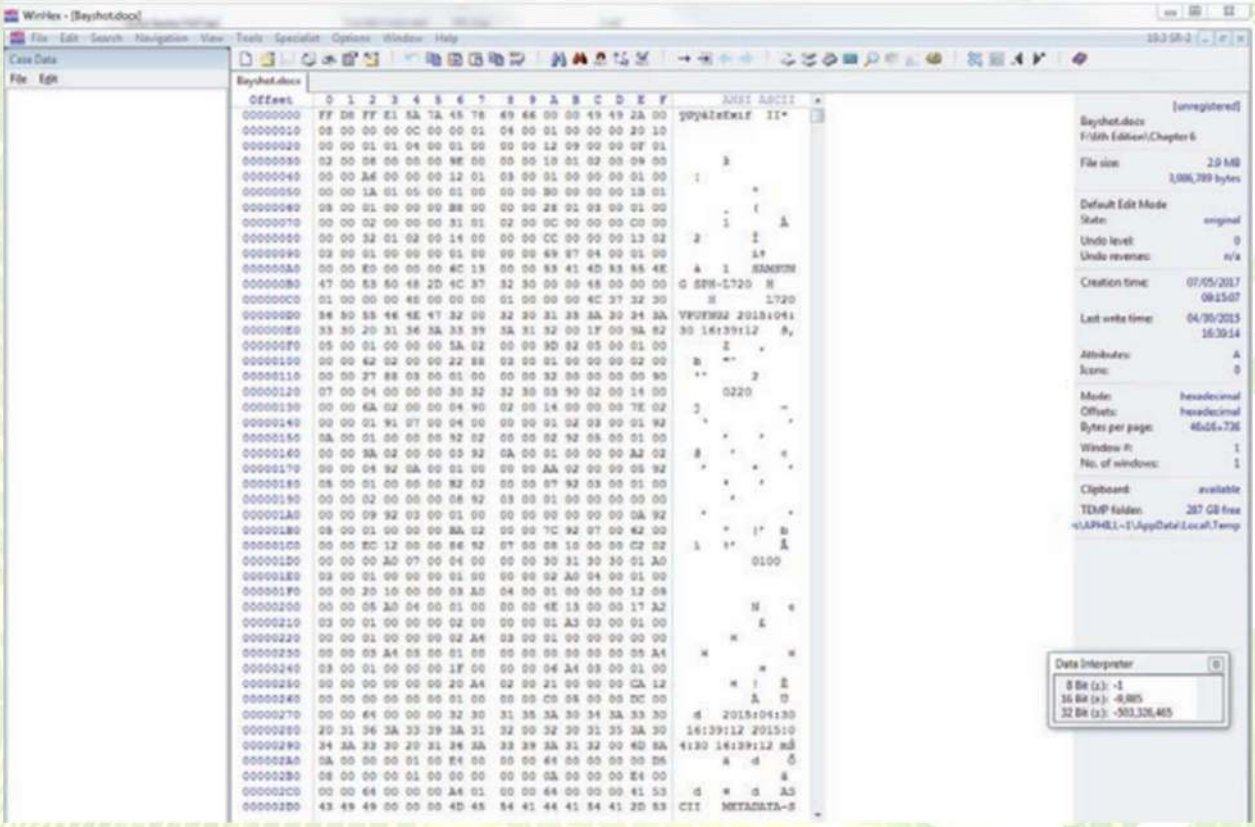
Ma’lumotlarni filtratsiya qilishning yana bir usuli ma’lum fayl turlari uchun sarlavha qiymatlarini tahlil qilish va tasdiqlashdir. Har bir fayl turining fayl kengaytmasi bilan bog‘liq sarlavha qiymati mavjud bo‘lib, ko‘plab raqamli kriminalistika vositalari umumiy fayl sarlavhalarining ro‘yxatini o‘z ichiga oladi. Ushbu fayl sarlavhalarini ko‘rish uchun o‘n oltilik tahrirlovchisini ishlatish mumkin, bu esa fayl kengaytmasining fayl turiga mos kelmasligini aniqlash imkonini beradi. Fayl kengaytmasini o‘zgartirish ko‘pincha ma’lumotlarni yashirish yoki o‘zgartirish uchun amalga oshiriladi va agar fayl sarlavhalari tekshirilimasa, muhim ma’lumotlarni o‘tkazib yuborish mumkin. Grafik fayllar



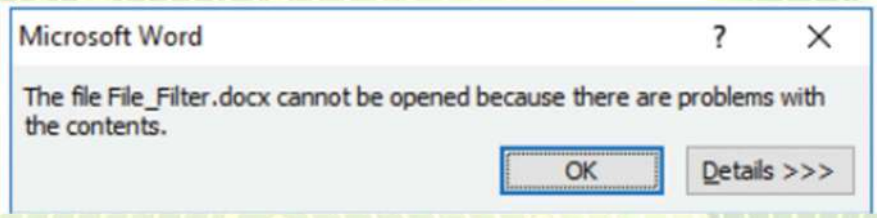
ISSN 3030-3907

uchun standart ko‘rsatkich — “FF D8” o‘n olti lik qiymati, bu esa 2-rasmda ko‘rsatilgan *“Bayshot.docx”* faylining birinchi qatorida ko‘rinadi.

Bayshot.docx faylida sarlavhada “FF D8” borligi sababli, bu *.docx fayli emas *.jpeg tasviridir. Agar ushbu faylni Microsoft Word dasturida ochishga harakat qilinsa, agar Windows 7 yoki 8.1 dan foydalanilsa 3-rasmda ko‘rsatilgan xato xabarini ko‘rish mumkin. Biroq, Windows 10 avtomatik ravishda faylni JPEG sifatida aniqlaydi va to‘g‘ri kengaytmani qo‘shadi.



**2-rasm. Fayl sarlavhasi *.jpeg faylini bildiradi**



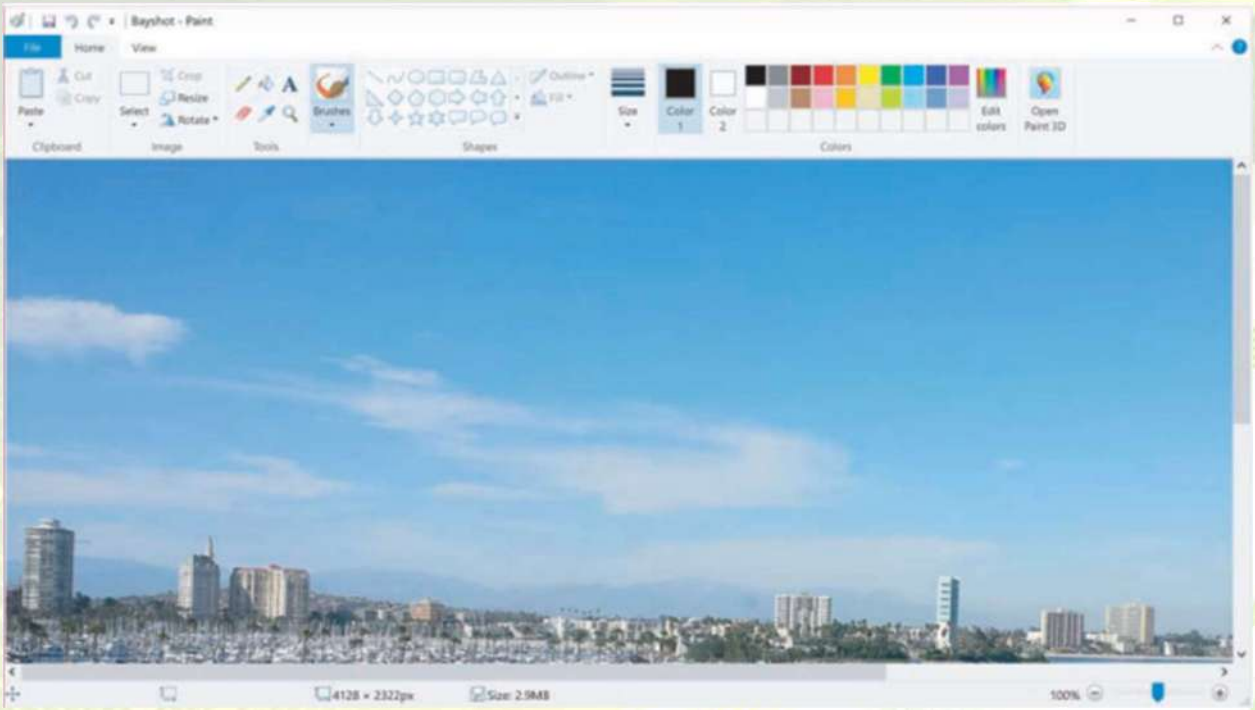

**3-rasm. Word dasturida *.jpeg faylni ochishga urinayotganda xato xabari**

Agar fayl Microsoft Paint kabi tasvirni ko‘rish dasturi bilan ochilsa, 4-rasmda ko‘rsatilgan rasmni ko‘rish mumkin.

Fayl kengaytmalari o‘rniga fayl sarlavhalarini qidirish va solishtirish filtrlashni yaxshilaydi. Ushbu xususiyat yordamida ataylab o‘zgartirilgan fayllarni topish mumkin.



ISSN 3030-3907



**4-rasm Paint dasturida “Bayshot.docx” fayli ko‘rinishi**

**Ekstraktsiya**. Ekstraktsiya funksiyasi raqamli tergovlarda ma’lumotlarni tiklash vazifasini bajaradi va bu barcha vazifalardan eng murakkabi hisoblanadi. Ma’lumotlarni tiklash tergov ma’lumotlarini tahlil qilishda birinchi qadamdir. Ekstraktsiya jarayonida ishlatiladigan quyidagi qo‘shimcha funksiyalar mavjud:

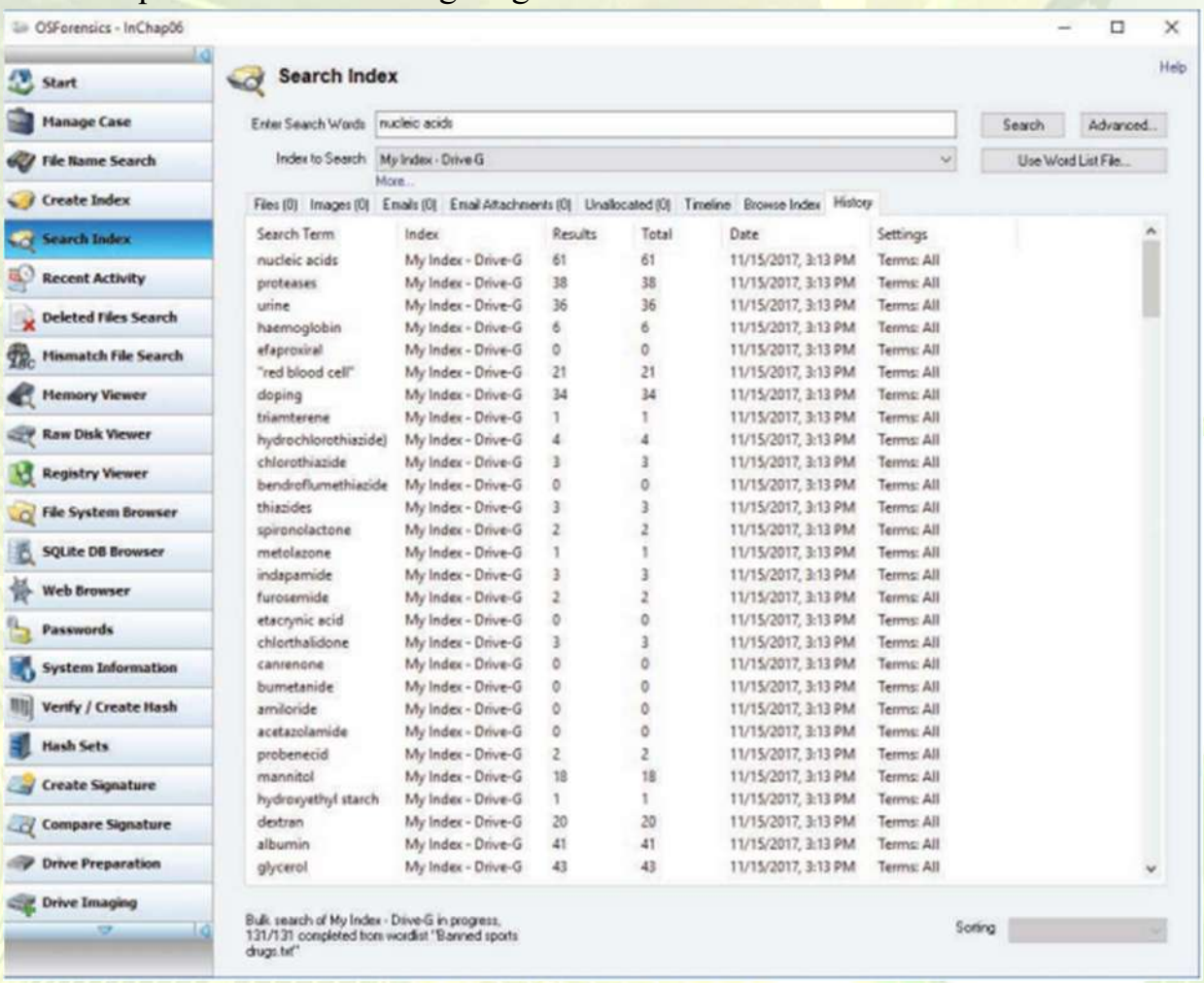
– Ma’lumotlarni ko‘rish;
– Kalit so‘zlarni qidirish;
– Siqilgan fayllarni ochish;
– Qayta tiklash (carving);
– Shifrlarni ochish;
– Belgilash.

Ko‘plab raqamli kriminalistika vositalari raqamli dalillar uchun ma’lumotlarni ko‘rish mexanizmini o‘z ichiga oladi va ma’lumotlarni ko‘rishning bir necha usullarini taklif etadi. Jumladan, papkalar va fayllar kabi mantiqiy disk tuzilmalarini. Ushbu vositalar, shuningdek, ajratilgan fayl ma’lumotlarini va ajratilmagan disk joylarini maxsus fayl va disk ko‘rish vositalari bilan ko‘rsatadi. Ushbu ma’lumotlarni odatiy shaklda ko‘rish, tergov uchun izlarni tahlil qilish va yig‘ish jarayonini osonlashtiradi.

Raqamli tergovlarda keng tarqalgan vazifa muhim ma’lumotlarni qidirish va tiklashdir. Raqamli kriminalistika vositalarida tergovga qiziqish bildiruvchi kalit so‘zlarni qidirish funksiyalari mavjud. Agar to‘g‘ri ishlatilsa, kalit so‘z qidiruvi tahlil jarayonini tezlashtiradi, ammo, kalit so‘zlarni noto‘g‘ri tanlash juda ko‘p ma’lumotlarni keltirib chiqaradi. Qidiruv masshtabini qisqartirishning yana bir


ISSN 3030-3907

usuli muayyan holat uchun yaratilgan so‘z ro‘yxatlaridan foydalanishdir. Quyidagi 5-rasmda OSForensics dasturida *“banned sports drugs”* deb nomlangan o‘rnatilgan fayl ko‘rsatilgan bo‘lib, u qattiq diskdan *“nucleic acids”* kalit so‘zini indeksli qidiruv uchun ishlatilganligini ko‘rish mumkin.




**5-rasm. OSForensics dastuirida qidirish uchun so‘zlar ro‘yxatidan foydalanish**

Ba’zi vositalar bilan qidiriladigan fayl turlarini tanlash uchun filtrlarni o‘rnatish mumkin, masalan, faqat PDF fayllarini qidirish. Ba’zi raqamli kriminalistika vositalarida, masalan, X-Ways Forensics va OSForensics, diskdagi barcha so‘zlarni indekslash funksiyasi mavjud. Ushbu funktsiyalar kalit so‘z qidiruvlarini tezlashtiradi, bu esa tahlilni ham tezlashtiradi.

Ekstraktsiya uchun yana bir muhim xususiyat raqamli kriminalistika vositasining o‘qiy oladigan formatlaridir. Masalan, OSForensics Microsoft .pst va .ost fayllaridan ma’lumotlarni o‘qish va indekslash funksiyasiga ega. EnCase esa Microsoft .pst fayllarini indekslash va tahlil qilish uchun uchinchi tomon qo‘shimchasiga ega. Shuningdek, EnCase va X-Ways Forensics ma’lumotlarni ekstraktsiya qilish uchun skriptlar yaratishga imkon beradi, ammo FTK dasturining eski versiyalarida bu xususiyat mavjud emas. Odatda, raqamli qurilmalardan



ISSN 3030-3907

dalillarni aniq olish va hisobot berish uchun vositalarning kombinatsiyasidan foydalanish kerak.

Tergov jarayoni shuningdek, shubhali diskdan o‘chirilgan fayllarning bo‘laklarini qayta tiklashni ham o‘z ichiga oladi. Amerikada bu qayta tiklash *“carving”* deb ataladi; Yevropada esa *“salvaging”* deb ataladi. Tergovchilar ko‘pincha ajratilgan disk joyidan ma’lumotlarni olishlari kerak. Fayl sarlavha ma’lumotlarini aniqlash, “tasdiqlash va tekshirish”da aytib o‘tilganidek, ma’lumotni carving qilish uchun ishonchli usuldir. Ko‘pgina raqamli kriminalistika vositalari disk yoki tasvirning ajratilgan joylarini tahlil qilish va *carving* qilish va yangi qayta tiklangan faylga nusxalash mumkin bo‘lgan bo‘laklar yoki to‘liq fayl tuzilmalarini aniqlaydi. Ba’zi tergovchilar bo‘laklangan ma’lumotlarni qo‘lda buyruq satri vositasi yordamida carving qilishni afzal ko‘rishadi, ammo o‘rnatilgan carving funksiyalariga ega ilg‘or GUI vositalari hozirda ko‘proq tarqalgan. Yuqoridagi 5-rasmda OSForensics dasturidagi ma’lumot carving qilish xususiyati ko‘rsatilgan.

Ba’zi vositalar, masalan, Simple Carver Suite (www.simplecarver.com) va DataLifter, eksport qilingan ajratilgan disk joyidan ma’lum ma’lumot turlarini carving qilish uchun maxsus ishlab chiqilgan. DataLifter boshqa sarlavha qiymatlarini qo‘shish imkoniyatini taqdim etadi.

Ko‘plab siqish yoki zip utilitalari, masalan, WinZip, 7Zip va pzip mavjud. Agar raqamli kriminalistika vositasi siqilgan fayl yoki zip arxivini kriminalistik tasvir sifatida uchratadigan bo‘lsa, u fayllarni ochish uchun to‘g‘ri algoritmni qo‘llaydi. Masalan, Windows fayllarini ochish Lempel-Ziv algoritmi, Lz32.dll yordamida amalga oshiriladi. Boshqa operatsion tizimlar va siqish utilitalari boshqa algoritmlardan foydalanadi.



ISSN 3030-3907




**6-rasm.OS raqamli kriminalistikada ma’lumotlarni tiklash variantlari**

Raqamli tergovlarda asosiy muammo shifrlangan fayllardan yoki tizimlardan ma’lumotlarni tahlil qilish, tiklash va shifrlanishni ochishdir. Shifrlash diskda, disk partitsiyasida yoki faylda qo‘llanilishi mumkin. Ko‘plab elektron pochta xizmatlari, masalan, Microsoft Outlook, .pst papkalari va xabarlar uchun shifrlash himoyasini taqdim etadi. Shifrlash platformaga xos bo‘lishi mumkin, masalan, Windows Shifrlash fayl tizimi (EFS) va BitLocker yoki uchinchi tomon vositalari, masalan, Pretty Good Privacy (PGP) va GnuPG yordamida amalga oshirilishi mumkin.

Tergov nuqtai nazaridan, shifrlangan fayllar va tizimlar muammoli hisoblanadi. Ko‘plab parolni tiklash vositalari parol lug‘at hujumlari uchun potentsial parol ro‘yxatlarini yaratish imkoniyatiga ega. Parollar odatda to‘g‘ridan-to‘g‘ri matn shaklida emas, balki xesh qiymatlari sifatida saqlanadi va bir tomonlama qiymatlar sifatida mo‘ljallangan, ya’ni ularni buzish uchun algoritmni qo‘llash mumkin emas. Parol ro‘yxatlari parollarni taxmin qilish uchun boshlang‘ich nuqtani beradi[17].

Shuningdek, shubhali shaxsning kasbi va qiziqishlariga oid so‘zlarni sinab ko‘rish mumkin. Ba’zan parollar vaqtincha faylga yoki tizim fayliga, masalan, pagefile.sys ga yoziladi. Shuning uchun ushbu fayllarni tekshirish foydali texnika hisoblanadi. OSForensics, ko‘plab raqamli kriminalistika vositalari kabi, o‘rnatilgan parolni buzuvchi funksiyasiga ega. Dastlab, fizik tizim tekshirilayotgan bo‘lsa u brauzer va operatsion tizim parollarini olishga harakat qiladi. Keyin, u rainbow jadvallarini (parol xesh qiymatlarini o‘z ichiga oluvchi fayllar) yaratadi va



ISSN 3030-3907

xesh qiymatlarini taqqoslaydi, parol bilan mos kelishini aniqlashga harakat qiladi. Agar muvaffaqiyatga erishmasa, keyingi qadam shifrlangan faylga nisbatan kuchli hujum o‘tkazishdir. OSForensics, masalan, Windows tizimida saqlangan login parollarni tiklashga harakat qiladi va brauzer parollarini tiklash kabi qo‘shimcha funksiyalarga ega. Mobil qurilmalarni kengaytirish bilan, parollarga kirish imkoniyati foydalanuvchilarning parollarining xavfsizligiga bog‘liq.

Dalilni topgandan so‘ng, keyingi vazifa uni belgilash yoki saqlashdir. Ko‘plab raqamli kriminalistika vositalari belgilardan foydalanib, raqamli dalilni hisobga olish generatoriga kiritadi, bu esa tekshirish natijalarining HTML yoki RTF formatida texnik hisobotini ishlab chiqaradi. Hisobot generatori ishga tushirilganda, belgilangan joylar hisobotga yuklanadi.

*Qayta tiklash.* Kriminalistika vositasida qayta tiklash funksiyasining maqsadi shubhali diskni qayta yaratishdir, bu esa jinoyat yoki hodisa paytida nima bo‘lganini ko‘rsatadi. Shubhali diskni nusxalashning yana bir sababi, boshqa raqamli tergovchilar uchun to‘liq funktsional nusxani yaratishdir. Ular dalillarni o‘zlariga olishlari, test va tahlil qilishlari mumkin. Agar disk zarar ko‘rgan bo‘lsa, qayta tiklash ham amalga oshiriladi. Qayta tiklash usullari quyidagilar:

– Diskdan-diskga nusxa olish
– Partitsiyadan-partitsiyaga nusxa olish
– Tasvirdan-diskga nusxa olish
– Tasvirdan-partitsiyaga nusxa olish
– Diskdan-tasvirga nusxa olish

Ma’lumotlarga ishlov berish va carving qilish orqali fayllarni qayta tiklash.

Shubhali diskning tasvirini qayta yaratishning bir necha usullari mavjud. O‘n yillar oldin, ideal usul shubhali disk bilan bir xil marka va model diskdan foydalanish edi, ammo diskdan-diskga nusxalar hozirda kam qo‘llaniladi. Odatda, tasvir boshqa joyga, masalan, partitsiya, jismoniy disk yoki virtual mashinaga nusxalanadi. Diskni nusxalashning eng oddiy usuli shubhali diskdan maqsadli joyga to‘g‘ridan-to‘g‘ri diskdan-tasvirga nusxa olishni amalga oshiradigan vositadan foydalanishdir. Ko‘plab vositalar ushbu vazifani bajarishi mumkin. Bitta bepul vosita — Linux “*dd”* buyrug‘i, ammo uning katta kamchiligi bor, u manba disk bilan bir xil o‘lchamdagi tekis, siqilmagan faylni ishlab chiqaradi.

Ba’zi vositalar o‘zlarining maxsus formatlariga ega bo‘lib, ularni faqat ular yaratgan dastur yordamida tiklash mumkin. Masalan, ProDiscover tasviri (.eve format) faqat ProDiscover yordamida tiklanishi mumkin. Ammo, ko‘plab vositalar fayllarni .E01 yoki .001 formatiga aylantira oladi, shunda turli vositalarda ulardan foydalanish mumkin.



ISSN 3030-3907

Raqamli kriminalistika tahlili ko‘pincha vaqt bilan bog‘liq vaziyatlar, masalan, o‘g‘rilik yoki qotillik bilan bog‘liq ishlar bilan murakkablashadi, ammo disklarni soya qilish bunday vaziyatlarda foydali texnika hisoblanadi[16]. Bu shubhali diskni o‘qish uchun o‘qishdan bosh tortadigan IDE portiga va yozish uchun *“shollow disc”* deb ataladigan portga ulanishi kerak bo‘lgan apparat qurilmasini talab qiladi. Masalan, Voom Technologies Shadow Drive. Voom qurilmasi kompyuterga ulanganida, shubhali diskda dasturlar ishga tushishi va ulardan foydalanish mumkin. Odatda shubhali diskda yozilishi kerak bo‘lgan barcha ma’lumotlar soyali diskka yo‘naltiriladi.

**Hisobot tayyorlash.** Kriminalistik disk tahlilini va tekshirishni amalga oshirish uchun hisobot yaratish kerak. Windows raqamli kriminalistika vositalari mavjud bo‘lmaganda, bu jarayon shubhali diskdan ma’lumotlarni nusxalash va raqamli dalilni qo‘lda olishni talab qilar edi. Tergovchi keyin dalilni alohida dasturga, masalan, matn tahrirlovchisiga nusxalab, hisobot yaratardi. Matn tahrirlovchisida o‘qib bo‘lmaydigan fayl ma’lumotlari ma’lumotlar bazalari, jadval fayllari va grafiklar kabi hisobotga chop etilmaydigan belgilar, masalan, binar ma’lumotlarni kiritishni qiyinlashtirardi. Odatda, bu hisobotlar elektron ravishda saqlanmasdi, chunki tergovchilar barcha narsalarni bitta katta qog‘oz hisobotga birlashtirish uchun bir nechta turli ilovalar bo‘yicha chop etilgan nusxalarni to‘plashlari kerak edi.

Yangi raqamli kriminalistika vositalari elektron hisobotlarni turli formatlarda ishlab chiqarishi mumkin, masalan, matn tahrirlovchi hujjatlar, HTML veb-sahifalar va Acrobat PDF fayllari. Hisobot funksiyasining qo‘shimcha funksiyalari quyidagilarni o‘z ichiga oladi:

– Belgilash yoki saqlash;
– Log hisobotlari;
– Vaqt chizmalari;
– Hisobot generatori.

Tasdiqlash jarayonining bir qismi sifatida, ko‘pincha shubhali diskdan ma’lumotlarni olish jarayonida amalga oshirgan qadamlarga hujjat tayyorlash kerak. Ko‘plab raqamli kriminalistika vositalari tergovchining faoliyatlarini qayd etuvchi *log* hisobotini ishlab chiqarishi va ekstraktsiya jarayonida belgilangan yoki taglangan dalillarni o‘z ichiga olishi mumkin. Shundan so‘ng, turli formatlarda hisobot yaratish uchun o‘rnatilgan hisobot generatori ishlatiladi. Belgilangan dalillarni ko‘rsatadigan hisobot generatorlariga ega va ular EnCase, FTK, OSForensics, ILookIX va X-Ways Forensics dasturlaridir.

Log hisobotini oxirgi hisobotga qo‘shish mumkin, bu esa tekshirish jarayonida amalga oshirgan qadamlarni hujjatlashtirish uchun foydali bo‘ladi. Peer



ISSN 3030-3907

nazoratini talab qiladigan holatlar uchun, log hisobotlari qaysi faoliyatlar amalga oshirilganini va asl tahlil va tekshirishda qanday natijalar topilganini tasdiqlaydi. Raqamli kriminalistika vositalari tomonidan ishlab chiqarilgan hisobotlar tergovchining hisobotini o‘rnini bosmaydi, shuning uchun tergovchilar o‘z qarorlarini va natijalarni vosita ishlab chiqaradigan hisobotdan ko‘ra batafsilroq tushuntira olishlari kerak.

**Vositalarni taqqoslash**. Qaysi kriminalistika vositasini sotib olishni aniqlashda yordam berish uchun funksiyalar, qo‘shimcha funksiyalar va ishlab chiqaruvchilar mahsulotlari taqqoslash jadvali foydali bo‘ladi. Funksiyalar va qo‘shimcha funksiyalarni ishlab chiqaruvchilar mahsulotlari bilan kesishish, ehtiyojlarga eng mos keladigan raqamli kriminalistika vositasini aniqlashni osonlashtiradi.

**Olingan natijalar va tahlillar.**

Tadqiqot davomida raqamli kriminalistika vositalarining amaliy imkoniyatlari va ularni ishlatish bo‘yicha bir qator aniq natijalar olindi:

1. Dasturiy va apparat vositalarni taqqoslaganda, ko‘p funksiyali grafik interfeysli dasturlar ancha ustun chiqdi. Masalan, EnCase, FTK, OSForensics va X-Ways Forensics komandali satrga qaraganda samaraliroq ishlaydi. Lekin, bu dasturlar kuchli kompyuter va ko‘p resurs talab qiladi. Imkoni past qurilmada yoki fon jarayonlari ko‘p bo‘lsa, tergov jarayonlari anchagina sekinlashadi.

2. Ma’lumotlar butunligini aniqlashda MD5, SHA-1 va CRC-32 kabi xesh algoritmlarining ishonchliligi amalda tasdiqlandi. Jismoniy va mantiqiy nusxa olishni solishtirganda, ayniqsa, shifrlangan disklar ustida mantiqiy nusxa olish samaraliroq bo‘ladi. Uzoqdan nusxa olish uchun maxsus vositalar (masalan, EnCase yoki AccessData) yirik tashkilotlar uchun vaqt va resursni ancha tejaydi.

3. Fayl carvingda fayl sarlavhasini hex orqali tahlil qilish yashirin yoki noto‘g‘ri nomlangan fayllarni aniqlashda yordam berdi. Masalan, WinHex yordamida Bayshot.docx faylini topilganda, aslida u JPEG rasm bo‘lib chiqqani bunday tahlilning ahamiyatini ko‘rsatdi. Fayl kengaytmasi o‘zgartirilgan fayllarni ham sarlavhasi orqali oson aniqlash mumkin.

4. Ma’lumotlarni ajratib olish va tiklashda OSForensics’da indeksli so‘z bo‘yicha izlash yoki carving funksiyasi yordamida o‘chirilgan fayllarni topish mumkin bo‘ldi. Simple Carver Suite va DataLifter dasturlari esa murakkab va bir-biriga kirishib ketgan ma’lumotlarni qayta tiklashda yaxshi natija berdi. ZIP va RAR arxiv fayllari ustida esa Lempel-Ziv algoritmlari samaraliroq ekani ko‘rindi.

5. Shifrlangan fayllarni o‘rganishda Rainbow jadvallari va lug‘at (dictionary) hujumlari orqali parollarni aniqlash ancha osonlashdi. Shu bilan birga,



ISSN 3030-3907

vaqtincha parollar tizim fayllarida saqlanib qolishi mumkinligi tergovchilar uchun muhim ahamiyatga ega bo‘ldi.

6. Hisobot tayyorlashda zamonaviy kriminalistika vositalari avtomatik tarzda HTML, RTF, PDF formatda hisobotlar tuzish imkonini beradi. Log hisobotlari esa sud va tekshiruv jarayonlarida dalil ishonchliligini ko‘rsatish uchun juda zarur ekanini tajriba davomida aniq ko‘rsatdi.

**XULOSA.**

Ushbu tadqiqot raqamli kriminalistika sohasidagi zamonaviy vositalar, metodlar va algoritmlarning keng qamrovli tahlilini amalga oshirdi. Quyidagi asosiy xulosalar shakllantirildi:

Birinchidan, raqamli kriminalistika jarayonining muvaffaqiyati ko'p jihatdan to‘g‘ri vositani tanlash va uni to‘g‘ri qo‘llashga bog‘liq. Hech bir yagona vosita barcha kriminalistik vazifalarni to‘liq qamrab ola olmaydi — shuning uchun kompleks yondashuv, ya’ni bir nechta vositalarni birgalikda qo‘llash tavsiya etiladi.

Ikkinchidan, fayl carving usuli o‘chirilgan yoki ataylab yashirilgan ma'lumotlarni tiklashda kriminalistik tergovning eng muhim va murakkab bosqichi hisoblanadi. Fayl sarlavhalarini hex tahlil qilish — fayl kengaytmasi o‘zgartirilgan hollarda ham haqiqiy fayl turini aniqlash imkonini beruvchi ishonchli metodika ekanligi isbotlandi.

Uchinchidan, raqamli dalillarning huquqiy kuchga ega bo‘lishi uchun xesh qiymatlari orqali ma’lumot butunligini tasdiqlash, barcha tergov qadamlarini log hisobotida hujjatlashtirish va ISO 27037 hamda NIST CFTT standartlariga rioya qilish majburiy shart hisoblanadi.

To‘rtinchidan, fayl tizimlari (FAT, NTFS, ReFS, Ext4) va operatsion tizimlarning ichki tuzilishini chuqur tushunish kriminalistik mutaxassis uchun zaruriy fundamental bilim bo'lib, bu bilim carving jarayonining sifati va samaradorligini bevosita belgilaydi.

Beshinchidan, raqamli ma'lumotlar hajmining tez sur'atlarda ortib borishi, antiforensik usullarning murakkablashuvi va shifrlash texnologiyalarining keng tarqalishi — zamonaviy kriminalistika vositalarini doimiy yangilab borish va sun’iy intellektga asoslangan avtomatlashtirilgan tahlil algoritmlarini ishlab chiqishni dolzarb vazifaga aylantirmoqda.

Xulosa qilib aytganda, raqamli kriminalistika — faqat texnik soha bo‘lib qolmasdan, huquqiy, axloqiy va protsessual talablarni ham qamrab oluvchi murakkab interdissiplinar yo'nalish sifatida rivojlanib bormoqda. Kelajakdagi tadqiqotlar sun’iy intellekt yordamida fayl carving algoritmlarini avtomatlashtirish, bulutli muhitlarda kriminalistik tahlil metodikasini ishlab chiqish va mobil



ISSN 3030-3907

qurilmalar ekspertizasini takomillashtirish yo'nalishlarida olib borilishi maqsadga muvofiqdir.

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Brunty J. Validation of forensic tools and methods: a primer for the digital forensics examiner. WIREs For Sci. 2023;5(2):-1474. https://doi.org/10.1002/wfs2.1474.
2. Gladyshev, P., James, J., 2017. Decision-theoretic file carving. Digit. Invest. 22 (Suppl. C), 46-61
3. Rana MS, Hasan MM, Moneruzzaman M. An introduction to digital forensics (cyber forensics). Int J Res Public Rev. 2023. htt ps://doi.org/10.55248/gengpi.4.1223.123427
4. Ding K, Meng F, Liu Y, Xu N, Chen W. Perceptual hashing based forensics scheme for the integrity authentication of high resolution remote sensing image. Information. 2018;9(9):229. https://doi.org/10.3390/info9090229.
5. Rani D, Gill NS, Gulia P. A forensic framework to improve digital image evidence administration in iiot. J Ind Inf Integr. 2024;38:100568. https://doi.org/10.1016/j.jii.2024.100568
6. Poisel, R., Tjoa, S., 2013. A comprehensive literature review of file carving. In: 2013 International Conference on Availability, Reliability and Security, pp. 475-484.
7. Pal, A., Memon, N., 2009. The evolution of file carving. IEEE Signal Process. Mag. 26 (2), 59-71.
8. Federal Evidence Review, 2014. Federal rules of evidence. Available from: http://federalevidence.com/rules-of-evidence (accessed 22.05.2014).
9. Frye v. U.S| Casebriefs, n.d. Casebriefs. Available from: http://www.casebriefs.com/blog/law/evidence/evidence-keyed-to-fisher/lay-opinions-and-expert-testimony/frye-v-u-s/ (accessed 24.05.2014).
10. File Systems, n.d. Microsoft TechNet. Available from: http://technet.microsoft.com/en-us/library/cc938949.aspx (accessed 25.06.2014).
11. How FAT Works, 2003. Local File Systems. Available from: http://technet.microsoft.com/en-us/library/cc776720(v=ws.10).aspx (accessed 24.06.2014).
12. Lucas, M., 2013. Windows Server 2012: Does ReFS replace NTFS? When should I use it? Available from: http://blogs.technet.com/b/askpfeplat /archive/2013/01/02/windows-server-2012-does-refs-replace-ntfs-when-should-i-use-it.aspx (accessed 29.06.2014).



ISSN 3030-3907

13. Sinofsky, S., n.d. Building the next generation file system for Windows: ReFS. Available from: https://blogs.msdn.com/b/b8/archive/2012/01/16/building-the-next-generation-file-system-for-windows-refs.aspx (accessed 29.06.2014).
14. Registry, n.d. Windows. Available from: http://msdn.microsoft.com/en-us/library/windows/desktop/ms724871(v=vs.85).aspx (accessed 11.09.2014).
15. Russinovich, M.E., Solomon, D.A., 2012. Windows Internals, sixth ed. Microsoft Press, Redmond, Washington.
16. Drinkwater, R., 2010. Forensics from the sausage factory: Volume shadow copy forensics cannot see the wood for the trees? Available from: http://forensicsfromthesausagefactory.blogspot.com/2010/02/volume-shadow-copy-forensics-cannot-see.html (accessed 10.08.2014).
17. Matloff, N., Salzman, P., 2008. The Art of Debugging with GDB, DDD, and Eclipse. No Starch Press, San Francisco.
18. Epifani, M., Stirparo, P., 2015. Learning iOS Forensics: A Practical Hands-on Guide to Acquire and Analyze iOS Devices with the Latest Forensic Techniques and Tools. Packt Publishing, Birmingham, UK.
19. Sikorski, M., Honig, A., 2012. Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software. No Starch Press, San Francisco.



ISSN 3030-3907