"JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN" JURNALI
VOLUME 04, ISSUE 04, 2026. APRIL
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

ELEKTRON MA'LUMOTLARNI BELGILAYDIGAN TEXNOLOGIK XUSUSIYATLAR VA POTENSIAL DALIL MANBALARI

B.Z.Karimov
TDYU Kriminalistika va sud ekspertizasi shubasi katta o'qituvchisi

Annotatsiya. *Mazkur maqolada elektron ma'lumotlarning kriminalistik ahamiyati, ularning texnologik xususiyatlari hamda potensial dalil manbalari sifatida tutgan o'rni tahlil etilgan. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi sharoitida elektron dalillar jinoyatlarni sodir etish, yashirish va fosh etishda muhim rol o'ynayotgani asoslab berilgan. Tadqiqotda elektron ma'lumotlarning an'anaviy moddiy dalillardan farqli jihatlari, ularni to'plash, saqlash, tekshirish va baholash jarayonlarida yuzaga keladigan muammolar ko'rib chiqilgan. Xususan, elektron qurilmalarning asosiy komponentlari — markaziy protsessor (CPU), dasturiy ta'minot, tizim soati, xotira va saqlash vositalarining elektron dalillar shakllanishiga ta'siri ilmiy asosda yoritilgan. Shuningdek, vaqt belgilarining (time stamp) kriminalistik ahamiyati, ularning aniqligi va noto'g'ri sozlanishining tergov xulosalariga ta'siri tahlil qilingan. Elektron dalillarni aniqlash, tiklash va baholash jarayonida yuzaga keladigan texnik va protsessual muammolar, jumladan yo'qolgan ma'lumotlarni qayta tiklash hamda ularning ishonchliligini baholash masalalari yoritilgan. Tadqiqot natijasida elektron dalillarni baholashda texnologik xususiyatlarni chuqur tahlil qilish zarurligi, shuningdek, tergov amaliyotida maxsus bilim va yondashuvlardan foydalanish muhimligi asoslab berilgan.*

Kalit so'zlar: *elektron dalillar, raqamli kriminalistika, virtual izlar, elektron qurilma, markaziy protsessor (CPU), dasturiy ta'minot, operatsion tizim, vaqt belgisi (time stamp), metama'lumotlar, xotira (RAM, ROM), saqlash vositalari, bulut texnologiyalari, fayl tizimi, raqamli izlar, dalillarni baholash.*

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jinoyat sodir etish, uni yashirish va fosh etish jarayonlarida elektron ma'lumotlar alohida ahamiyat kasb etmoqda. Elektron ma'lumotlar an'anaviy moddiy izlardan tubdan farq qiluvchi texnologik xususiyatlarga ega bo'lib, ularni to'plash, saqlash, tekshirish va baholashda maxsus ilmiy-texnik yondashuvlarni talab etadi. Shu bois

elektron ma’lumotlarning mavjudligi va huquqiy ahamiyatini belgilovchi texnologik talablarni aniqlash dolzarb ilmiy masala hisoblanadi.

Turli xil qurilmalar elektron ma’lumotlarni yaratish va saqlashga qodir va bunday ma’lumotlar dalil sifatida xizmat qilishi mumkin [1]. Ushbu maqolada elektron dalillarni belgilaydigan umumiy texnologik xususiyatlar bilan tanishtirishdir. Albatta, bu yerda texnik masalalarni tahlil qilishdan asosiy maqsad, elektron ma’lumotlar (virtual izlar)ni tergovchi tomonidan huquqiy baholash, ular bilan ishlash mobaynida mutaxassis (ekspert) duch keladigan muammolar muhokama qilinadi.

Elektron dalillar an’anaviy moddiy dalillardan farqli ravishda, murakkab texnologik muhitda shakllanadi, saqlanadi va o‘zgaradi. Elektron qurilmaning apparat va dasturiy komponentlari elektron ma’lumotlarning paydo bo‘lishi, modifikatsiyalanishi hamda ularning tergov jarayonida aniqlanishiga bevosita ta’sir ko‘rsatadi. Shu bois elektron dalillarni kriminalistik jihatdan baholashda qurilmaning asosiy texnologik xususiyatlarini tahlil qilish muhim ahamiyat kasb etadi.

Quyida biz elektron ishlov berish tizimlarida (elektron qurilmalar) asosiy komponentlarning rolini batafsil bayon qilamiz.

Avvalo, elektron qurilma o’zi nima degan savol to’xtalib o’tishni maqsadga muvofiq deb hisbolaymiz. Elektron qurilma deb e’tirof etish uchun u bir qancha funksiyalarga ega bo’lishi lozim. Jumladan, u axborotni yarata olishi, qayta ishlashi, saqlashi yoki uzatish qobiliyatiga ega bo’lish bilan birga elektr energiya oqimini nazorat qilish orqali ma’lum bir tizimni boshqarishi lozim. Demak, “**elektron qurilma – ma’lumotni yaratish, qayta ishlash, saqlash hamda uzatish qobiliyatiga ega bo’lgan va energiya oqimini nazorat qilish orqali tizimni boshqaradigan apparatdir**”.

Biroq, oddiy tashuvchi bilan elektron qurilmani farqlash lozim bo’ladi. Elektron tashuvning asosiy vazifasi elektron axborotni muayyan muddatda saqlashdan iborat hisoblanadi. Shunda, “**elektron tashuvchi – elektron axborotni faqat saqlash uchun mo’ljallangan, ikkilamchi vosita**” deb ta’riflashimiz mumkin.

Endi elektron qurilmaning asosiy komponentlarini ko’rib chiqamiz:

Markaziy protsessor (CPU) deb ataladigan, har qanday elektron qurilmaning funksional asosiy tarkibiy qismi bo’lib, o’zi ham bir qancha tarkibiy qismlardan

iborat yadro. Bu qismlar birgalikda ma’lumotlarni qabul qiladi, mantiqiy yoki arifmetik amallarni bajaradi va natijalarni chiqaradi. Natijalar mahalliy saqlash moslamasiga yoki displey blokiga uzatiladi yoki boshqa qurilmaga tarmoq orqali yuboriladi. Har qanday elektron dalil (fayl, log, yozuv) CPU faoliyati natijasida shakllanadi. Agar protsessor ishlamasa – elektron ma’lumot hosil bo‘lmaydi.

Carrier elektron dalillarni “tizim tomonidan bajarilgan operatsiyalarning izlari” sifatida talqin qilib, ushbu operatsiyalarning markazida CPU turishini ko‘rsatadi. Protsessor foydalanuvchi buyruqlarini fayl tizimi darajasida real o‘zgarishlarga aylantiradi [9].

Demak, protsessor barcha hisbolash jarayonlarini bajaradi, foydalanuvchi buyruqlarini real amallar (harakat)ga aylantiradi. Ya’ni u fayllarni ochish, tahrirlash va o’chirish jarayonida metama’lumotlarni avtomatik yangilaydi. Tanenbaum operatsion tizimlar nazariyasida protsessorni axborotning mavjud bo‘lishi va harakatga kelishining asosiy sharti sifatida ko‘rsatadi. Uning fikricha, dasturiy va ma’lumotlar faqat CPU faoliyati orqali “real holat” kasb etadi [10]. Kriminalistik ahamiyati shundaki, hatto foydalanuvchi “faqat ko’rdim xolos” degan taqdirda ham kirish vaqti (Accessed time) o’zgarib qoladi. Casey ta’kidlashicha, “...har qanday virtual iz yoki elektron dalil kompyuter tizimida markaziy protsessor tomonidan bajarilgan hisoblash amallari natijasida yuzaga keladi. CPU axborotni qayta ishlamas ekan, virtual muhitda axborot (dalil) shakllanishi mumkin emas” [8]. Bundan tashqari protsessor faoliyati tergovda elektron dalillarni to’plash yoki tahlil qilishga ham ta’sir qilishi mumkin. Masalan, jonli tekshiruvlar protsessor (CPU) faoliyati tezkor xotira (RAM)dagi ma’lumotlarni o’zgartiradi.

Dasturiy ta’minot elektron qurilmaga ko’rsatmalar beruvchi dasturlardan iborat. Dasturiy ta’minot – kompyuter algoritmlari, ko‘rsatmalar va ma’lumotlar majmuasi bo‘lib, u kompyuter tizimi funksiyalarini boshqaradi va bajaradi; aynan shu jihat uni apparat (hardware) komponentidan ajratib turadi [10]. Dasturiy ta’minotning ikkita asosiy toifasi mavjud: tizim dasturiy ta’minoti va ilova (amaliy) dasturiy ta’minot.

Nomidan ko’rinib turibdiki, qurilmaning asosiy ishlashi uchun tizim dasturiy ta’minoti talab qilinadi. Elektron qurilmaning asosiy ishini boshqaradigan dasturiy ta’minotlar majmuasi operatsion tizim deb ataladi. Casey elektron dalil mazmuni va tuzilishi uni yaratgan dasturiy muhitga bog‘liq ekanini, aynan dastur fayl formatini va log mexanizmini belgilashini ko‘rsatadi [11]. Operatsion tizim ma’lumotlar

oqimini boshqarish, xotira ajratish va qurilmaning har qanday apparat komponentlarini, masalan, displey, kiritish qurilma (lar), tarmoqning o’zaro ta’siri va boshqalarni nazorat qiladi va boshqaradi. Shuningdek, Casey dasturiy muhit aniqlanmas ekan, elektron dalil noto‘g‘ri talqin qilinishi mumkinligini ko‘rsatadi. Carrier dasturiy ta’minotni “fayl tizimi va foydalanuvchi o‘rtasidagi vositachi” sifatida baholab, elektron izlar aynan shu qatlamda shakllanishini asoslaydi [12]. Operatsion tizim, shuningdek, foydalanuvchiga apparat va ilova (amaliy) dasturiy ta’minot o’rtasida interfeys vazifasini bajaradi. Keng ma’noda, statsionar kompyuterlar, noutbuklar va planshetlar kabi an’anaviy hisoblash qurilmalari uchun amaliy dasturiy ta’minot tizimning foydalanuvchiga aloqador tomonini ta’minlaydi. Bu foydalanuvchiga kompyuterda muayyan turdagi vazifalarni bajarishga imkon beruvchi “maxsus maqsadli” dasturiy ta’minot hisoblanadi. Bularga matnni qayta ishlash, chop etish, veb-sahifalarni ko’rish, elektron pochtani boshqarish, ijtimoiy tarmoqlar, taqdimotlarni tayyorlash va taqdim etish, raqamli hisoblarning murakkab to’plamlarini bajarish va shunga o’xshashlar ishlar kiradi. Ilova (amaliy) dasturlarga Microsoft Word, Internet Brauzerlar, PowerPoint, Excel va LibreOffice kabilarni misol qilib keltirish mumkin. Ushbu va boshqa amaliy dasturlar ko’pchilikning kompyuterlardan foydalanishining asosiy sabablarini ifodalaydi (ya’ni, kompyuter va uning amaliy dasturlari yordamida soddalashtirilgan aniq vazifalarni bajarish uchun). Garfinkel brauzerlar va messenjerlar kabi dasturlar maxsus ikkilamchi izlar (artifacts) hosil qilishini ta’kidlaydi [13]. Demak, dasturiy ta’minot fayl formatini belgilaydi, ma’lumotlarni qanday yozishni aniqlaydi hamda jurnal (log) va virtual izlar hosil qiladi. Masalan, Brauzer (kukki, kesh, tarix) yoki Messenger (chat jurnallari, media metama’lumotlari va h.k.) kabi ikkilamchi izlarni qoldiradi. Dasturiy ta’minotning yana bir jihati avtomatik yangilanish, fon yoki fon osti jarayonlari va jurnal aylanmasi elektron dalillarni o’z-o’zidan o’rgartirishi yoki yo’q qilishi mumkin. Lekin, ba’zi elektron dalillar foydalanuvchi harakatisiz ham o’zgaradi. Tergovchi (mutaxassis, ekspert) qaysi dastur ma’lumotni yaratganini, uning versiyasini va sozlamalarini aniqlamasdan turib to’g’ri xulosa bera olmaydi.

Vaqt belgilari. Elektron qurilmalarning ishlashi bilan bog’liq yana bir komponentni muhokama qilish kerak: Bu soat. Soat elektron qurilmada ikkita funksiyani bajaradi:

1) Voqealar sinxronlashtirilishi va oldindan aytib bo’ladigan tartibda sodir bo’lishini ta’minlash uchun vaqt impulslarini ishlab chiqaradigan qurilma

hisoblanadi. Olimlar energiya uzatish samaradorligi uchun “rezonans sharoitlar” kerakligini ko‘rsatadi (ya’ni, spektral moslik zarur) [14]. Ya’ni energiya o’tishi uchun chastota (tebranish) bir xil bo’lishi kerak. Qurilmada aynan mana shu vazifani soat bajaradi. Soat protsessorning barcha komponentlarini muvofiqlashtiradi. Har qanday operatsiyaning har bir bosqichi ketma-ketlikda bajarilishi kerak va ba’zi operatsiyalar har xil tezlikda ishlaydi. Tizim operatsiyalari elektron soatning impulslari bilan sinxronlashtiriladi [16]. Impulslarning chastotasi faza yopiq sikli (Phase Locked Loop) tomonidan boshqariladi, bu esa o’z navbatida kvarts kristali bilan tartibga solinadi. Kristalning tebranish tezligi, siklni oshirish nisbati va har bir ko’rsatma talab qiladigan qadamlar soni kompyuterning ishlash tezligini aniqlaydi.

2) Soat odamlar orasida ko’pincha kun va sana vaqtini saqlashga xizmat qiladigan qurilma sifatida qaraladi. Elektron qurilma (kompyuter) tizimlari o’z soatlarini Internetda mavjud bo’lgan ishonchli vaqt manbai bilan sinxronlashtiradi, masalan, Tarmoq vaqt protokoli kabi tizim interfeysi. Bu Internetga ulangan qurilmalarga vaqt sozlamalarini sinxronlashtirish imkonini beradi (geografik joylashuv va vaqt zonalarini hisobga olgan holda). Vaqtni sinxronlashtirishni ta’minlashning ikkita muhim maqsadi bor. Birinchi maqsad - hodisalarning o’z vaqtida va to’g’ri ketma-ketlikda sodir bo’lishini ta’minlash [17]. Ikkinchi maqsad - odamga o’tmishdagi voqealar haqida ma’lumot olish, shu jumladan voqealar qachon sodir bo’lganligi va ular sodir bo’lgan ketma-ketlikni aniqlash imkonini berishdir [17]. Bu faqat aniq vaqt belgilari mavjud bo’lganda mumkin hisoblanadi. Misol uchun autentifikatsiya qilish, elektron imzolar va tizim hodisalari jurnallarida qayd etilgan nosozliklar diagnostikasi uchun vaqt tamg’asi mexanizmini o’z ichiga olishi mumkin.

Ko’pgina ilovalarda o’rnatilgan soat batareyadan quvvat oladi va hatto qurilma o’chirilgan bo’lsa ham uzluksiz ishlaydi. Uzoq vaqt davomida qurilma yoqilmasa, yoqish tugmasi bosilganda ham yoqilmasligi mumkin, chunki batareya quvvati tugagan bo’ladi va qayta zaryadlash yoki almashtirishni talab qilishi mumkin. Odatda, soatni qo’lda sozlash (hatto noto’g’ri o’rnatish ham) mumkin. Bu mahalliy mintaqadagi haqiqiy vaqtga nisbatan tizim soatining biroz noto’g’ri bo’lishiga olib keladi. Bunday noaniqlik yuqorida ko’rsatilgan soatning ikkala maqsadda ishlatilishiga, ya’ni hodisalarni rejalashtirish va jurnalga ta’sir qilishi mumkin, chunki ikkala jihat ham tizim soatidan olingan vaqtga bog’liq bo’ladi. Vaqtning aniqligi muhim bo’lgan hollarda, vaqtni yaxshiroq mos yozuvlar manbalariga

(masalan, Internet-vaqt serverlari) moslashtirish uchun soat odatda vaqti-vaqti bilan sozlashni talab qiladi. Bu juda muhim masala, chunki soatning to’g’riligi yoki boshqachaligi haqidagi so’roqsiz va konteksdan tashqari taxminlar noto’g’ri xulosaga olib kelishi mumkin.

Vaqt belgilari eng muhim elementlardan biri hisoblanadi. Casey vaqt belgilari operatsion tizim, protsessor va tizim soati o‘zaro hamkorligi natijasida avtomatik ravishda shakllanishini ta’kidlaydi. Ushbu jarayon foydalanuvchi nazoratidan tashqarida bo‘lib, elektron dalillarning xronologik mazmunini belgilaydi [18]. Elektron dalillar nuqtai nazaridan, tizim soati ko’pincha vaqtni belgilashda muhim rol o’ynaydi. Masalan, operatsion tizim faylni yaratish yoki o’zgartirish kabi voqealarni qayd etish uchun sana va vaqt sozlamalaridan foydalanadi. Kompyuterlarda bunday ma’lumotlar ko’pincha fayl “metama’lumotlari” (asosiy ma’lumotlarni tavsiflovchi yoki sharhlovchi ma’lumotlar) deb ataladi, chunki sana va vaqt ma’lumotlari fayl bilan bog’langan, lekin fayldagi ma’lumotlar yoki foydalanuvchi to’g’ridan-to’g’ri nazorat qiladigan ma’lumotlarning bir qismi emas. Carrier fayl tizimi darajasida vaqt belgilari tizim soatiga to‘liq bog‘liqligini va agar tizim vaqti noto‘g‘ri sozlangan bo‘lsa, barcha elektron dalillar noto‘g‘ri vaqt kontekstida shakllanishini ko‘rsatadi [19]. Vaqt belgilari, shuningdek, foydalanuvchi loginlari, parolni o’zgartirish kabi tizim hodisalariga va qurilmaning maqsadiga qarab, foydalanuvchi tomonidan bosib o’tilgan qadamlar soni kabi sensor tomonidan qayd etilgan hodisalarga nisbatan qayd etiladi. Tanenbaum tizim vaqtini operatsion tizimning fundamental resurslaridan biri sifatida baholab, noto‘g‘ri vaqt sozlamalari butun tizimdagi ma’lumotlar mantig’iga salbiy ta’sir ko‘rsatishini ilmiy asoslaydi [19]. Bunday hodisalar bilan bog’liq bo’lgan vaqt va sana ma’lumotlari tizim jurnali fayllarida (hodisalar jurnallari) qayd etiladi. Bunday jurnallar ko’pincha voqealar ketma-ketligi to’g’risidagi ma’lumotlarning muhim manbai bo’lib, foydalanuvchining aniq faoliyati haqida ma’lumot beradi.

Demak, Markazi protsessor (CPU), operatsion tizim (OS) va tizim soati uchligi hamkorligida vaqt belgilari (time stamp) yaratiladi. Noto’g’ri vaqt sozlamasi – noto’g’ri xulosa demakdir. Axborotni saqlash va tahlil qilish yuzasidan turli fayl tizimlari (NTFS, FAT) turlicha vaqt aniqligiga ega. Bulut muhitida server va foydalanuvchi vaqti ham farqlanadi. Bundan shunday xulosa kelib chiqadiki, kriminalistik jihatdan vaqt belgisi mutlaq haqiqat emas, balki tahlil ob’ekti bo’lib xizmat qiladi. Masalan, elektron dalillarni baholashda, agar vaqt belgilari boshqa

dalillar bilan mos kelsa, ishonchlilik ortadi, zid bo'lsa, manipulyatsiya ehtimoli paydo bo'ladi. Vaqt tafovutlari sudda dalilni rad etish uchun asos bo'lishi mumkinligini ko'rsatadi. Chunki, elektron dalillar nuqtai nazaridan vaqt belgilari diagnostik emas, balki yuqori aniqligi sababli identifikatsion masala hisoblanadi.

Xotira va saqlash. Dasturlar, chiqish natijalari va dasturlar ishlaydigan boshqa ma'lumotlarni saqlash uchun elektron qurilmalar xotiraga tayanadi. Umuman olganda, saqlashning ikkita shakli mavjud: birlamchi saqlash va ikkilamchi saqlash. Birlamchi (asosiy) xotira protsessor tomonidan to'g'ridan-to'g'ri kirish mumkin bo'lgan xotiradir. Odatda yarimo'tkazgich xotirasi shaklini oladi, masalan:

1) Tasodifiy kirish xotirasi (RAM) deb nomlanuvchi ichki xotira [20]. Ushbu chip qayta-qayta saqlash (yozish) va saqlangan ma'lumotlarni olish (o'qish) qobiliyatiga ega.

2) Ma'lumotlarni bir marta saqlashga qodir, lekin ma'lumotlarni qayta yozishga imkon bermaydigan ichki xotira sanaladi. Ma'lumotlar kiritilgandan so'ng, bu turdagi xotira faqat ma'lumotlarni o'qish imkonini beradi. Bu faqat o'qish uchun mo'ljallangan xotira (ROM) deb ataladi.

3) Ma'lumotlarni saqlaydigan va normal ishlashi davomida o'zini ROM sifatida tutadigan, lekin ma'lumotlarni o'chirish va almashtirishga ruxsat beruvchi ichki xotira. Qurilmaning bu shakli o'chiriladigan, dasturlashtiriladigan faqat o'qish uchun xotira (EPROM - *erasable programmable read-only memory*) deb nomlanadi [21]. Flesh ROM EPROMning bir turidir.

Ikkilamchi xotira protsessor tomonidan bevosita foydalana olmaydigan xotiradir. Agar u saqlanadigan ma'lumotlar kerak bo'lsa, protsessor ikkilamchi xotiraga kirish va kerakli ma'lumotlarni asosiy xotiraga o'tkazish uchun kirish/chiqish kanallaridan foydalanadi. Birlamchi xotiradan farqli o'laroq, ikkilamchi xotira o'zgaruvchan emas. Saqlash vositalari (elektron tashuvchi) sifatida qattiq disklar (HDD, SSD) va USB xotira ikkilamchi saqlashning odatiy shakllaridir. Ular kompyuterga doimiy ravishda biriktirilishi mumkin (ichki xotira) yoki kerak bo'lganda biriktirilishi mumkin (tashqi xotira). Tashqi xotiraning boshqa shakllari kompyuterga kamroq proksimal bo'lishi mumkin, masalan, tarmoqqa biriktirilgan xotira (NAS - Network-attached storage) [21], tarmoq drayverlari yoki "bulut saqlash" xotirasi. Ikkilamchi xotira o'zgaruvchan bo'lmaganligi sababli, qattiq disk va u bilan bog'liq oflayn saqlash vositalari qurilma uchun elektron dalillarning muhim manbai hisoblanadi. Ammo birlamchi xotiraning o'zgaruvchanligi uning

ma’lumotlarini qaytarib bo’lmaydi degani emas. Fizik jihatdan olish va boshqa kompyuterga o’tkazishdan oldin RAM xotirasini “muzlatish” bo’yicha tajriba, ishlov berilgan chiplardan operativ xotira ma’lumotlarini tiklash mumkin bo’lgan g’ayrioddiy konteksni aniqladi [21].

Ma’lumotlarni saqlash vositalari

Elektron ma’lumotlarni saqlashning yoki saqlash kontekslarining xilma-xilligi tegishli ma’lumotlarni istiqbolli dalil sifatida topish oddiy masala emasligini anglatadi. Ma’lumotlar qattiq disklar, DVD yoki kompakt disklar, flesh-xotiralar, xotira kartalari yoki mikro xotira qurilmalari (odatda smartfonlarda bo’lgani kabi) saqlash qurilmalarida lokal holatda (periferik emas) saqlanishi mumkin. Ammo ma’lumotlar tarmoqqa ulangan saqlash, masofaviy tarmoqlar yoki “bulut” saqlash qurilmalari kabi masofadan ham saqlanishi mumkin. Soha tergovchilarini tashvishga soladigan narsa – bu shaxsning kompyuteridan masofadan turib saqlanadigan ma’lumotlarni topish va ularga qonuniy ruxsat olish bilan bog’liq qiyinchiliklardir. Ma’lumotlarni saqlash kontekslari turlicha bo’lishi mumkin (5-ilova).

Yo’qolgan ma’lumotlar

Elektron dalillar bo’yicha mutaxassis qattiq diskdagi yoki boshqa saqlash vositalaridagi bir qator “yo’qolgan” ma’lumotlarni aniqlay oladi:

1) Agar foydalanuvchi qasddan qattiq disk qismlarini “yaroqsiz” deb belgilasa, u tegishli disk diagnostikasi yoki tekshirish vositasidan foydalanmasdan ko’rish mumkin bo’lmagan katta hajmdagi ma’lumotlarni yashirishi mumkin. (Chunki operatsion tizim avtomatik ravishda ushbu “yaroqsiz sektorlar”dan foydalanishdan qochadi).

2) Foydalanuvchi ma’lumotlarni o’chirib tashlaganida, eski fayl yangi ma’lumotlar bilan yozilguncha diskda qoladi. Faqat fayl tizimidagi tizim ko’rsatkichlari (pointer) o’chiriladi. Agar faylning bir qismi qayta yozilgan bo’lsa ham, asl faylni o’z ichiga olgan disk bloklarining butun to’plami to’liq qayta yozilmagan bo’lsa, o’chirilgan faylning bir qismini tiklash mumkin bo’ladi.

Biroq, tiklangan ma’lumotlar faqat topilganligi sababli haqiqiy yoki ishonchli dalil ekanligini anglatmaydi. Ma’lumotlar yo’qolishi yoki shikastlanishi mumkin bo’lgan ko’plab kontekslar mavjud va bu qayta tiklanadigan har qanday natijada olingan ma’lumotlarning ishonchliligiga ta’sir qiladi [22]. Masalan, dasturdagi xatolar natijasida ma’lumotlarning buzilishi yoki yo’qolishi, tashqi manbalardan olingan ma’lumotlarga aralashishi mumkin [22].

Bundan tashqari, shuni ta’kidlash kerakki, dalillarning ishonchliligiga nisbatan elektron dalillar bo’yicha mutaxassis tekshiruv o’tkazishi va ma’lumotlarni qayta tiklash usuli ham ta’sir qilishi mumkin. Agar tergov jarayoni dalillarga ta’sir qilsa, uning ishonchliligi talbiiy ravishda pasayadi.

Elektron ma’lumotlar ikkilik (binar) ma’lumotlarga keng tasniflanadi, bunda ma’lumotlar ikkilik shaklda taqdim etiladi, ya’ni matnli ma’lumotlar, shu jumladan alfa, raqamlar va tinish belgilaridan iborat. Aslida bu foydalanuvchiga matn va raqamlarni o’qish, tasvirlarni ko’rish yoki ovozni eshitish imkonini berish uchun ma’lumotlarning ikkilik shakliga o’zgartirish deganidir. Elektron axborotni to’g’ridan to’g’ri ikkilik (2 baza) sanoq sistemasi yordamida ifodalash mumkin, lekin xozirda sakkizlik (8 baza) yoki, eng ko‘p qo’llaniladigan, o‘n oltilik (16 baza) bilan ifodalash keng tarqalgan [23].

Matnli ma’lumotlar uchun bir qator kodlar mavjud. Umumiy foydalaniladigan ba’zi kodlar Unicode [2], Axborot almashinuvi uchun Amerika standart kodi (ASCII) [3], Kengaytirilgan ikkilik kodli o’nlik almashish kodi (EBCDIC) [3], va Unicode Transformation Format-8 (UTF-8)[4], deb nomlanadi. Bu Internetda ishlatiladigan standart belgilar kodi bo’lib, barcha mumkin bo’lgan belgilarni kodlash imkoniyatiga ega. Ko’pgina kompyuterlar xozirda Unicode va ASCII dan foydalanadilar. Tergovchida odatda elektron qurilma foydalanuvchisiga ko’rinmaydigan xususiyatlarni ko’rish imkonini berish uchun ishlatiladigan ikkilik ma’lumotlarni ko’rsatishga mo’ljallangan dasturiy ta’minotlar mavjud bo’lishi kerak. Masalan, Microsoft Word formatida saqlangan hujjatlar odatda ko’rinmaydigan dastur metama’lumotlarini o’z ichiga oladi. Muayyan turdagi dasturiy ta’minot (EXIF)ni qo’llash orqali tergovchi ma’lumotlarning barcha jihatlarini ko’rishi va bu tergovga yordam beradigan muhim ma’lumotlarni ochib berishi mumkin.

Kompyuterni ishga tushirish. Elektron qurilma har safar yoqilganda, uning ishlashi uchun turli komponentlar bir-biri bilan o’zaro ta’sirga kirishadi. Bu ishga tushirish jarayoni yoki tizimni “yuklash” (booting) deb ataladi. Ko’pgina qurilmalarda faqat o’qish uchun mo’ljallangan xotirada turli xil “boot loader”, “boot process”, “boot strap” yoki “initial program load” deb ataladigan dasturlar mavjud bo’ladi. Aynan shu dastur tizimni ishga tushirishga imkon beradi. Umuman olganda, u shunday ishlaydi:

1) Tizim yoqilganda, boshqaruv birinchi navbatda asosiy kirish va chiqish tizimiga (BIOS) [5], qurilmaning ROM xotirasida doimiy joylashgan dasturga o’tkaziladi.

2) BIOS tizimning turli komponentlarini sinab ko’radi, ularning faol va ishlayotganligini tekshiradi. U amalga oshiradigan turli testlarning natijalari tizim chiqishida ko’rinishi mumkin. Yuklash jarayoni, shuningdek, barcha oldingi (eski) ma’lumotlar va metama’lumotlarning mahalliy birlamchi xotirasini tozalashi mumkin. BIOS birinchi (yoki standart) ikkilamchi saqlash qurilmasini topadi, saqlash qurilmasida operatsion tizimni qidiradi va boshqaruvni operatsion tizimning yuklash yozuvi (boot record)ga o’tkazadi.

3) Yuklash yozuvi tizimni nazorat qiladi. Ushbu dastur shuningdek, yuklash jarayonini o’z ichiga oladi, u o’z navbatida operatsion tizimni yuklashdan oldin konfiguratsiyani yuklaydi va sinovdan o’tkazadi.

4) Nihoyat, operatsion tizim har qanday ishga tushirish dialogini (masalan, mobil telefon xizmati provayderining identifikatori) ko’rsatadi. Agar foydalanuvchi avtorizatsiya qilingan bo’lsa (masalan, kodni taqdim etish orqali), ilova (amaliy) darajasidagi dasturlarga kirish huquqini beradi va foydalanuvchi ilova orqali qurilmani boshqarishi mumkin bo’ladi.

Xulosa o’rnida shuni aytish mumkinki, elektron qurilmalarning keng tarqalganligi va ularga deyarli to’liq ishonishimizni hisobga oladigan bo’lsak, ushbu paragrafda ko’rsatilgandek, tergov jarayonida to’planishi, tekshirilishi va baholanishi mumkin bo’lgan elektron dalillar doirasi juda kengdir. Elektron audio, video va foto tasvirlardan tortib, Internetga ulangan kompyuterning murakkab xatti-harakatlarigacha belgilash mumkin. Elektron dalillarni baholash tergovchi (sudya, advokat) ishining asosiy qismiga aylandi. Har bir tergovchi (mutaxassis) bunday elektron dalillarni tekshirish, izohlash, qabul qilinishi va ko’rib chiqish bo’yicha tegishli maslahatlar berishga tayyor bo’lishi kerak. Bu masalalarning barchasi keyingi paragraflarda tegishli tarzda ko’rib chiqiladi.

Foydalanilgan adabiyotlar ro’yxati:

1. Mason, S., & Seng, D. (Eds.). (2017). Electronic Evidence (4th ed.). University of London Press. p. 1 http://www.jstor.org/stable/j.ctv512x65

2. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

3. Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems (4th ed.). Pearson.

4. Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.

5. David Anderson, Janet Delve, Milena Dobreva. (2025). The Preservation of Complex Objects. Volume 1. Visualisations and Simulations. Published by The University of Portsmouth.

6. Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.

7. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

8. Garfinkel, S. (2015). Digital media triage with bulk data analysis. Digital Investigation, 14, S49–S59.

9. Andrews, D. L., Bradshaw, D. S., & Scholes, G. D. (2015). Resonance energy transfer. In Photonics: Scientific Foundations, Technology and Applications (Vol. IV). John Wiley & Sons.

10. Hosmer, Chet. (2002). Proving the Integrity of Digital Evidence with Time.. IJDE. 1.

11. Chris Boyd, Pete Forster, Time and date issues in forensic computing - a case study, Digital Investigation, Volume 1, Issue 1, 2004, Pages 18-23, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2004.01.002.

12. Malcolm W. Stevens, Unification of relative time frames for digital forensics, Digital Investigation, Volume 1, Issue 3, 2004, Pages 225-239, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2004.07.003.

13. Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.

14. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

15. Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems (4th ed.). Pearson.

16. https://en.wikipedia.org/wiki/Random-access_memory

17. https://en.wikipedia.org/wiki/EPROM

18. https://en.wikipedia.org/wiki/Network-attached_storage

19. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. 2009. Lest we remember: cold-boot attacks on encryption keys. Commun. ACM 52, 5 (May 2009), 91–98. https://doi.org/10.1145/1506409.1506429

20. Sommer, Peter. (1997). Downloads, Logs and Captures: Evidence from Cyberspace. Journal of Financial Crime. 5. 138-151. 10.1108/eb025826.

21. Casey, Eoghan. (2002). Error, Uncertainty and Loss in Digital Evidence.. IJDE. 1.

22. https://en.wikipedia.org/wiki/Numeral_system

23. J.Klensin and Michael Padlipsky, "Unicode format for Network Interchange" (2008) RFC 5198 <https://tools.ietf.org/html/rfc5198>

24. Vinton Cerf, "RFC 20 – ASCII format for Network Interchange" (1969) RFC 20 <https://tools.ietf.org/html/rfc20>.

25. R.T.Braden, "EBCDIC/ASCII mapping for Network RJE" (1972) RFC 338 <https://tools.ietf.org/html/rfc338>.

26. F.Yergeau, "UTF-8, a transformation format of ISO 10646" (2003) RFC 3629 <https://tools.ietf.org/html/rfc3629>.

27. https://en.wikipedia.org/wiki/BIOS