RAQAMLI KRIMINALISTIKA VOSITALARIGA EHTIYOJLARNI BAHOLASH

Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika”
Ergashbekov Nurbek Avazbek o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU

Annotatsiya: Ushbu maqolada raqamli kriminalistika jarayonida raqamli dalillarni tekshirish, tasdiqlash, tiklash va tahlil qilishning zamonaviy usullari yoritiladi. Tergov jarayonining maqsad va doirasini aniqlash, qidiruv orderlari yoki sud qarorlarining rolini tushuntirish bilan birga, xususiy sektor tergovlari, jinoyat ishlari va fuqarolik ishlari o‘rtasidagi farqlar tahlil qilinadi. Raqamli dalillarni yig‘ish jarayonida qo‘llaniladigan xeshlash, o‘n oltilik tahrirlovchilar yordamida tasdiqlash, yashirin bo‘limlarni aniqlash, yomon klasterlarni belgilash, bitlarni o‘zgartirish kabi texnikalar batafsil ko‘rib chiqiladi. Shuningdek, steganografiya, shifrlash va parolni buzish bo‘yicha amaliy hujum usullari hamda ularni aniqlash yo‘llari yoritilgan. Maqola raqamli kriminalistik tekshiruvlarda Autopsy, WinHex va boshqa kriminalistika vositalaridan foydalanish imkoniyatlariga ham alohida e’tibor qaratadi. Tadqiqotda tergov jarayonida scope creep (doiraning kengayishi) hodisasining ahamiyati va tergov rejasini moslashtirish zarurati asoslab beriladi.

Kalit so‘zlar: Raqamli kriminalistika, raqamli dalillar, xeshlash, Autopsy, WinHex, steganografiya, shifrlash, parol tiklash, brute-force hujumi, dictionary attack, rainbow table, yashirin bo‘limlar, disk tahlili, kriminalistik tasvir, dalil integriteti, bit-level analysis.

Raqamli dalillarni tekshirish va tahlil qilish tergovning xususiyatiga hamda qayta ishlanishi kerak bo‘lgan ma’lumotlar hajmiga bog‘liq. Jinoyat tergovlari odatda qidiruv orderida belgilangan ma’lumotlarni topish bilan cheklansa, fuqarolik tergovlari sud tomonidan belgilangan hujjatlarni oshkor qilish talablariga bo‘ysunadi. Xususiy sektordagi tergovchilar esa ko‘pincha kompaniya siyosatining buzilganligini aniqlash uchun faqatgina muayyan elementlarni, masalan, elektron pochta xabarlarini tekshirishlari mumkin. Shu sababli, tergov odatda bir nechta aniq ma’lumotlarni topish va tiklash bilan cheklanadi, bu esa jarayonni soddalashtirib, tezlashtiradi.

Biroq, xususiy sektor muhitida, ayniqsa, sud jarayoni mavjud yoki kutilayotgan bo‘lsa, kompaniyaning yuristi tergovchini iloji boricha ko‘proq ma’lumotni tiklashga yo‘naltirishi mumkin. Ushbu talabni qondirish esa ko‘p soatlik mashaqqatli ishni talab qiladi. Bundan tashqari, bunday tergovlarda ***kengayib boruvchi doira*** (scope creep) hodisasi yuzaga keladi. Ya’ni, tergov davomida kutilmagan dalillar topilgani sababli, yurist qo‘shimcha ma’lumotlarni ham tahlil qilishni so‘rashi mumkin. Natijada tergovning hajmi dastlabki rejalardan chiqib ketib, dalillarni ajratish, tahlil qilish va taqdim etish uchun zarur bo‘lgan vaqt va resurslar ortadi. Shuning uchun, agar tergov rejalashtirilganidan uzoq davom etsa yoki uning doirasi kengaysa, tergovchidan bu holatni tushuntirish talab

qilinadi. Shunday vaziyatlarga duch kelganda, qo‘shimcha tergov talablarini hujjatlashtirish juda muhim.

Scope creep*ning* ko‘payishiga sabab bo‘luvchi omillardan biri jinoyat tergovlari sud jarayonidan oldin dalillarni yanada batafsil tekshirishni talab qiladi. Bu prokurorlarga himoyachi advokatlarning e’torozlarini qaytarishga yordam beradi. Chunki himoyachi advokatlar odatda mijozlariga qarshi ishlatiladigan raqamli dalillarni to‘liq oshkor qilish huquqiga ega bo‘ladilar. Natijada, tergov jarayonida yangi dalillar paydo bo‘lishi mumkin. Ammo bu yangi dalillar ko‘pincha prokurorga oshkor qilinmaydi, aksincha, ayblanuvchini himoya qilish uchun ishlatiladi. Shu sababli, prokuror jamoasi sudga qadar barcha dalillarni to‘liq va puxta tahlil qilganiga ishonch hosil qilishi kerak.

Raqamli kriminalistika ishlariga yondashish. Bu rejada tergovning maqsadi va doirasi, kerakli materiallar hamda bajarilishi lozim bo‘lgan vazifalar aniqlanadi. Raqamli kriminalistika ishlarining aksariyatida qo‘llaniladigan umumiy tamoyillar mavjud bo‘lsada, har bir holatda yondashuv tergov qilinayotgan ish turiga bog‘liq.

Masalan, elektron pochta orqali tahdid qilish bilan bog‘liq dalillarni to‘plash faqat tarmoq jurnallariga va elektron pochta serverining zaxira nusxalariga kirish orqali maxsus xabarlarni topish bilan cheklanib qolishi mumkin. Biroq, bu jarayon ishning ichki tashkilot tergovi, fuqarolik tergovi yoki huquq-tartibot idoralari olib borayotgan jinoyat tergovi ekaniga bog‘liq holda o‘zgaradi. Ichki tergovlarda dalillarni to‘plash nisbatan oson, chunki xususiy sektor tergovchilari odatda kerakli yozuv va fayllarga to‘g‘ridan-to‘g‘ri kirish imkoniyatiga ega bo‘ladilar. Ammo kiber-ta’qib (cyberstalking) jinoyati tergovida internet xizmat provayderi (ISP) va elektron pochta xizmatini taqdim etuvchi kompaniyalar bilan bog‘lanish talab qilinadi. Ayrim kompaniyalar bunday tergovlarni qo‘llab-quvvatlash tizimlariga ega bo‘lsada, ko‘plab tashkilotlar elektron pochta xabarlarini atigi 90 kun yoki undan ham qisqa muddat saqlaydi, keyin o‘chirib yuboradi.

Sanoat josusligida gumon qilingan xodimni tergov qilish esa eng ko‘p ish talab qiladi. Bunday tergovni boshlashdan oldin, tashkilot xoh u xususiy kompaniya, xoh davlat idorasi bo‘lsin foydalanish qoidalari va shaxsiy daxlsizlik huquqlari chegaralarini aniq belgilaganligiga ishonch hosil qilish kerak. Bunday tergovlarda:

- Ofisda kuzatuv kamerasi o‘rnatish va xodimning harakatlarini nazorat qilish talab qilinadi;
- Dasturiy yoki apparat keylogger (masofadan bosilgan tugmalarni qayd etuvchi vosita) joylashtirilishi lozim;
- Tarmoq administratorining yordami bilan internet va tarmoq faoliyati monitoringi amalga oshirilishi kerak;
- Masofaviy ma’lumot olish (remote acquisition) orqali xodimning kompyuterida saqlanayotgan ma’lumotlar olinishi va keyinchalik turli vositalar yordamida u qanday tashqi qurilmalardan foydalanganligi aniqlanishi mumkin.

Har bir ish turi o‘ziga xos yondashuvni talab qiladi, shuning uchun tergov oldidan aniq strategiya ishlab chiqish muhimdir.

Raqamli kriminalistika tergovlari uchun standart amaliyot bosqichlari. Barcha raqamli kriminalistika tergovlari uchun quyidagi asosiy bosqichlarga amal qilish tavsiya etiladi:

1. Maqsadli disklarga ishlov berish

– IACIS (International Association of Computer Investigative Specialists) tashkiloyning tavsiya qilinishicha, tergov uchun ishlatiladigan maqsadli disklarda oldindan tozalangan, qayta formatlangan va viruslardan tekshirilgan saqlash vositalar ishlatilishi kerak;

– Hech bo‘lmaganda, ishlatiladigan saqlash vositalari zararli dasturlardan tozalangan bo ‘lishi lozim;

– Tarmoq saqlash vositalariga kirish imkonini beruvchi ilg‘or raqamli kriminalistika vositalari ishlatilganda, tarmoq xavfsizligi choralari, masalan, kirish nazorati ro‘yxati (ACL), xavfsiz sozlangan yo‘naltiruvchi (router) va xavfsizlik devori (firewall) qo‘llanilishi kerak;

– Diskdan diskka nusxa olishda, asl disk maqsadli diskni xuddi shunday konfiguratsiya bilan formatlaydi;

– Agar saqlash vositalarini butunlay tozalash kerak bo ‘lsa, X-Ways Security, Digital Intelligence PDWipe yoki WhiteCanyon SecureClean kabi vositalardan foydalanish kerak.

2. Gumondorning kompyuteridagi apparat vositalarni inventarizatsiya qilish

– Kompyuter musodara qilingan paytdagi holatini qayd etish;

– Tergov dalillarini to‘plash jarayonining bir qismi sifatida barcha jismoniy apparat qismlarini hujjatlashtirish.

3. Statik nusxa olish

– Asl diskni kompyuterdan olib tashlash kerak

– Tizimning *CMOS* (Complementary Metal-Oxide Semiconductor) soat va sana qiymatlarini tekshirish.

4. Ma’lumotlarni olish usulini qayd etish

– Ma’lumotlarni qanday usulda olganini hujjatlashtirish;

– Masalan, bit-stream tasvir yaratish va qaysi vosita ishlatilganini yozib qo‘yish;

– Tasvirni tasdiqlash uchun MD5 yoki SHA-1 hash qiymatlari yaratganligingizni qayd etish.

5. Disk tasviri ma’lumotlarini tizimli va mantiqiy tahlil qilish

6. Barcha papkalar va fayllarning ro‘yxatini tuzish

– *Autopsy* kabi raqamli kriminalistika vositalari yordamida barcha fayllar va papkalar ro‘yxatini yaratish;

– Ro‘yxatlarni Excel, HTML yoki boshqa formatlarda eksport qilish;

– Aniq dalillar qayerdan topilganini qayd etish va ularning tergovga qanday bog‘liq ekanini ko‘rsatish.

7. Barcha ma’lumot fayllarini tekshirish

– Iloji bo‘lsa, barcha fayllarni va papkalarni tekshirish, bu jarayonni disk hajmining asosiy katalogi (root directory) dan boshlash;

– Agar qidiruv orderi yoki hujjatlarni oshkor qilish talabi bo‘lsa, faqat ruxsat etilgan hujjatlar tekshirilishi kerak.

8. Parol bilan himoyalangan fayllarni ochish

– Tergovga tegishli bo‘lgan parol bilan himoyalangan fayllarning ichidagi ma’lumotlarni tiklashga harakat qilinadi;

– OSForensics Password Recovery, AccessData Password Recovery Toolkit (PRTK) yoki Passware Kit Enterprise kabi vositalardan foydalaniladi.

9. Barcha bajariluvchi (binary yoki .exe) fayllarni tekshirish

– Agar bajariluvchi fayl ma’lum xesh qiymatlariga mos kelmasa, uning vazifasini aniqlash kerak;

– System32 kabi tizim papkalari tarkibidagi o‘z joyida bo‘lmagan fayllarni qayd etish kerak;

– Disk muharriri orqali bajariluvchi fayl haqida ma’lumot topilmasa, uning qanday ishlashini va nimalarga ta’sir qilishini tekshirish kerak.

10. Dalillarni nazorat qilish va hujjatlashtirish uchun:

– Tergov davomida barcha dalillarni nazorat qilish;

– Har bir bosqichni aniq hujjatlashtirish va tergov davomida to‘plangan natijalarni qayd etib borish zarur.

Tekshiruv rejasini takomillashtirish va o‘zgartirish. Fuqarolik va jinoiy ishlar bo‘yicha tergovlarning doirasi odatda qidiruv orderlari yoki chaqiruv qog‘ozlari bilan belgilanadi. Bu esa qaysi ma’lumotlarni tiklash mumkinligini aniq ko‘rsatib beradi. Biroq, xususiy sektordagi ishlar, masalan, xodimlarning qoidabuzarliklarini tekshirish, ma’lumotlarni tiklashda qat’iy cheklovlarga ega bo‘lmasligi mumkin. Bunday hollarda, tergov rejasi iloji boricha aniq va puxta ishlab chiqilishi lozim. Umuman olganda, tergov doirasi barcha tegishli dalillarni o‘z ichiga olishi kerak, lekin ayni paytda ortiqcha vaqt va resurslarni behuda sarflashga sabab bo‘ladigan ma’lumotlarni tahlil qilmaslik kerak. Masalan, agar xodim ish vaqtida kompaniya resurslaridan foydalangan holda onlayn biznes yuritishda ayblansa, tergovni ushbu vaqt oralig‘iga yo‘naltirish orqali qidiruv doirasi qisqartirish mumkin. Ruxsatsiz internetdan foydalanish bo‘yicha dalillarni izlash uchun asosiy e’tibor vaqtinchalik internet fayllari, internet tarixlari va elektron pochta xabarlari tahliliga qaratiladi.

Tergov boshida qanday ma’lumotlarni izlayotganda aniq bilish vaqtdan samarali foydalanishga yordam beradi, hamda juda keng qamrovli qidiruv olib borishning oldini oladi. Biroq, tergov jarayonida ish bilan bog‘liq elektron pochta xabarlari ichida onlayn biznesga tegishli moliyaviy ma’lumotlar saqlangan jadval yoki Word hujjatlariga havolalar topilishi mumkin. Bunday holatda, tergov doirasini kengaytirib, ushbu turdagi fayllarni ham qamrab olish maqsadga muvofiq bo‘ladi. Demak, muhim jihat aniq reja asosida boshlash, ammo yangi dalillar yuzaga kelganda moslashuvchanlikni saqlashdir.

Autopsy yordamida ma’lumotlarni tasdiqlash

Quyidagi fayl tizimlarida raqamli kriminalistik tahlil o‘tkazishi mumkin:

– Microsoft: FAT, NTFS, ExFAT, UFS1 va UFS2;
– ISO 9660 va YAFFS2;
– Mac: HFS+ va HFSX;
– Linux: Ext2fs, Ext3fs va Ext4fs.

Bundan tashqari, *Autopsy* turli manbalardan, jumladan, boshqa dasturiy ta’minot ishlab chiqaruvchilarining tasvir fayllarini tahlil qila oladi. U quyidagi formatlarni qo‘llab-quvvatlaydi:

- Raw (xom ma’lumotlar);
- Expert Witness;
- Virtual mashina tasvir fayllari (.vdi va .vhd).

Autopsy ma’lum operatsion tizim va dasturiy ta’minot fayllarini aniqlash va chiqarib tashlashni yaxshilash uchun NIST National Software Reference Library (NSRL) MD5 xeshlarining indekslangan versiyasiga ega. Bundan tashqari, NSRL ma’lumotlar bazasini *Autopsy* dasturiga import qilish mumkin.

1.1. Raqamli kriminalistika ma’lumotlarini tasdiqlash

Raqamli kriminalistikaning eng muhim jihatlaridan biri raqamli dalillarni tasdiqlashdir, chunki yig‘ilgan ma’lumotlarning yaxlitligini ta’minlash sudda dalil sifatida taqdim etish uchun juda muhimdir. Ko‘pgina raqamli kriminalistik vositalari nusxa fayllari uchun xeshlash funksiyasini taklif qiladi. Biroq, raqamli kriminalistika vositalarida xeshlashni bajarishda ayrim cheklovlar mavjud. Shuning uchun ma’lumotlar yaxlitligini ta’minlash uchun o‘n oltilik tahrirlovchilarni ishlatish zarur.

O‘n oltilik muharrirlovchi bilan tekshirish. Ilg‘or o‘n oltilik tahrirlovchilar raqamli kriminalistika vositalarida mavjud bo‘lmagan ko‘plab funksiyalarga ega. Masalan, ma’lum fayllar yoki sektorlarni xeshlash. Ushbu vositalardan foydalanishni o‘rganish juda muhim, ayniqsa, ma’lum bir faylni, masalan, noqonuniy tasvirni topish zarur bo‘lganda. Xesh qiymatiga ega bo‘lish orqali raqamli kriminalistika vositasidan shubhali faylni izlash uchun foydalanish mumkin. Fayl nomi o‘zgartirilgan bo‘lsa ham, u aslida zararli fayl bo‘lishi mumkin. To‘liq funksiyali o‘n oltilik tahrirlovchi bilan xesh qiymatlarini olish raqamli kriminalistika vositalariga qaraganda tezroq va osonroq bo‘ladi. WinHex MD5 va SHA-1 kabi bir nechta xeshlash algoritmlarini qo‘llab quvvatlaydi. Ba’zida ma’lum fayllar yoki sektorlarning xesh qiymati kerak bo‘ladi, masalan, ma’lumotlar yoki fragmentlarning (sektorlarning) ma’lum bir fayl tarkibiga mos kelishini tekshirish yoki siyrak (sparse) akvizatsiyadan keyin ma’lumotlarni zudlik bilan tasdiqlash uchun.

Operatsion tizim yordamida fayllarni yashirish. Ma’lumotlarni yashirishning ilk texnikalaridan biri fayl kengaytmasini o‘zgartirish hisoblanadi. Agar gumonlanuvchi ichida ayblovchi dalillar saqlangan *Excel faylini yashirmoqchi* bo‘lsa, uning kengaytmasini *“.xlsx → .jpg”* qilib o‘zgartirishi mumkin. Bunday holatda tergovchi faylni Excelda ochishga harakat qilganda xatolik yuzaga keladi. Lekin zamonaviy raqamli kriminalistika vositalari fayl sarlavhalarini tekshiradi va uning haqiqiy turini kengaytma bilan solishtirib

ko‘radi. Agar nomuvofiqlik aniqlansa, fayl shubhali fayl sifatida belgilab, qo‘shimcha tahlil qilishni talab qiladi.

Yana bir yashirish usuli fayl xususiyatlarida (Properties) “Hidden” atributini tanlash. Bunday holatda, agar tergovchi *File Explorer* orqali fayllarni ko‘rmoqchi bo‘lsa, u *yashirin fayllarni ko‘rsatish (Show Hidden Files, Folders, and Drives)* opsiyasini yoqishi kerak. Lekin raqamli kriminalistika vositalari yashirin fayllarni aniqlab, tergovchilarga ularni oshkor qilish imkonini beradi.

Bo‘limlarni (partitions) yashirish usuli. Bo‘limlarni yashirishning bir usuli Windows disklarni bo‘limlash vositasi, ya’ni diskpartition yordamida amalga oshiriladi. *PowerShell*da quyidagi buyruqlarni kiritib, bo‘limni yashirish mumkin:

– Powershell;
– CopyEdit;
– Diskpart;
– remove letter=E.

Bu bo‘limning harfini olib tashlaydi va uni File Explorerda ko‘rinmas holga keltiradi.

Bo‘limni yana ko‘rinadigan qilish uchun quyidagi buyruq ishlatiladi:

– powershell;
– CopyEdit;
– Diskpart;
– assign letter=E.

Undan tashqari boshqa disk boshqarish vositalari ham mavjud:

– IM-Magic;
– EaseUS Partition Master;
– Linux GRUB (Grand Unified Bootloader).

Yashirin bo‘limlarni aniqlash. Agar gumonlanuvchi diskpartition yoki boshqa usullar yordamida bo‘limni yashirgan bo‘lsa, uni disk maydoni tahlili orqali aniqlash mumkin.

Tekshirish bosqichlari quyidagilardan iborat:

1. *Disk maydonini hisobga olish.* Dalil drayvni tekshirishda barcha disk joylarini hisobga olish kerak. Agar izohsiz bo‘sh joy mavjud bo‘lsa, u yashirilgan bo‘lishi mumkin;
2. *Bo‘sh joylarni tahlil qilish*. Diskdagi aniqlanmagan joylarni tahlil qilib, ular qo‘shimcha dalillarni o‘z ichiga olishini tekshirish lozim;
3. *Kriminalistik vositalardan foydalanishi.* Raqamli kriminalistika vositalari yoki o‘n oltilik tahrirlovchilar yordamida bo‘sh joylarni skanerlash kerak.
4. *Normal bo‘lmagan tafovutlarni aniqlash.* Windows Vista va undan keyingi versiyalarda bo‘limlar orasidagi bo‘sh joy odatda 128 baytni tashkil qiladi. Agar bo‘shliq bundan katta bo‘lsa, u yashirin bo‘lish ehtimoli bor.
5. *Dalillarni to ‘plash va tasdiqlash.* Agar yashirin bo‘lim aniqlansa, uni to‘liq skanerlash va undagi ma ‘lumotlarni tahlil qilish kerak.

Xulosa

Raqamli kriminalistika zamonaviy tergov jarayonining muhim tarkibiy qismi bo‘lib, unda dalillarning to‘liqligi, ishonchliligi va yuridik kuchga ega bo‘lishi uchun qat’iy metodologiyalar qo‘llaniladi. Tergov jarayonining muvaffaqiyatli kechishi maqsad va doiraning aniq belgilanishi, tegishli vositalardan foydalanish, dalillarni to‘g‘ri ajratish, tasdiqlash va hujjatlashtirishga bog‘liq. Raqamli dalillar ko‘pincha yashirilgan, shifrlangan yoki manipulyatsiya qilingan bo‘lishi mumkinligi sababli, tergovchi o‘n oltilik tahlil, xeshlash, yashirin bo‘limlarni topish, steganaliz va parolni buzish kabi texnik jihatlardan xabardor bo‘lishi zarur.

ADABIYOTLAR:

1. NIST — Computer Forensics Tool Testing (CFTT) Program.
2. ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition and preservation of digital evidence.
3. IOCE — International Organization on Computer Evidence.
4. Guidance Software — EnCase Forensic Documentation.
5. AccessData — FTK User Guide.
6. X-Ways Forensics Official Documentation.
7. Magnet Forensics — AXIOM User Manual.
8. PassMark — OSForensics Technical Specifications.
9. Brian Carrier. *File System Forensic Analysis.* Addison-Wesley.
10. Nelson, Phillips, Steuart. *Guide to Computer Forensics and Investigations.*