LINUX OPERATSION TIZIMI FAYL TIZIMINING TUZILISHI VA KRIMINALISTIK AHAMIYATI

Shukurov Orziqul Pardayevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani muovin
itel:+99899996636990
Zoirov Diyorbek Dilshod o‘g‘li
Saidov Yaxshimurodbek Umidjonovich
Jalilov Muhammad Hasan og‘li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada Linux operatsion tizimi fayl tizimining asosiy tuzilmalari, inode bloklari, fayllarning joylashuvi va kriminalistik tahlil uchun foydali bo‘lgan muhim jihatlar yoritiladi. Shuningdek, Linuxda kriminologik tekshiruvlarda qo‘llaniladigan asosiy vositalar (Sleuth Kit, Autopsy) haqida so‘z yuritiladi.*

Kalit so‘zlar: *Linux, fayl tizimi, inode, Ext4, kriminalistika, Sleuth Kit, Autopsy.*

Linux operatsion tizimi UNIX asosida yaratilgan bo‘lib, ochiq kodli va xavfsiz tuzilishga ega. Unga asoslangan fayl tizimlar, ayniqsa Ext4, axborot xavfsizligi va kriminalistik tekshiruvlar uchun katta ahamiyat kasb etadi. Fayl tizimi – bu operatsion tizimga diskdagi fayllarni qanday tashkil qilish, saqlash va ularga murojaat qilishni belgilovchi asosiy tizimdir.

Linux fayl tizimi strukturasi boshqa operatsion tizimlarga nisbatan yanada soddalashtirilgan, biroq u kuchli va moslashuvchan imkoniyatlarga ega. Linuxda barcha narsalar — fayllar, kataloglar, qurilmalar va hatto protsesslar ham fayl sifatida ko‘riladi. Bu yondashuv tizimni universal va kengaytiriladigan qiladi. Operatsion tizim resurslarini bir xil interfeys orqali boshqarish imkonini beradi. Masalan, tarmoq interfeyslari, apparat qurilmalari va foydalanuvchi bilan muloqot qiluvchi fayllar ham alohida fayl sifatida qaraladi, bu esa modullik va muvofiqlikni ta'minlaydi.

Fayllar kataloglar ko‘rinishida saqlanadi va har bir katalog ham o‘zi alohida fayl sifatida belgilanadi. Har bir katalog ichida boshqa fayllar yoki kataloglar joylashgan bo‘lishi mumkin, bu esa Linux fayl tizimiga daraxtsimon tuzilmani beradi. Bu tuzilma orqali har qanday obyektga yagona ildiz katalog (/) orqali kirish mumkin. Masalan, foydalanuvchi fayllari /home ostida, tizim konfiguratsiyalari /etc ostida, qurilmalar esa /dev katalogida joylashadi.

Linuxning asosiy fayl tizimlari orasida Ext2, Ext3 va ayniqsa hozirgi kunda keng tarqalgan Ext4 tizimi alohida o‘rin egallaydi. Ular orasida Ext4 eng so‘nggi versiya bo‘lib, barqarorlik, tezkorlik va ishonchlilik jihatidan sezilarli ustunliklarga ega. Bu tizim keng doiradagi qurilmalarda, jumladan serverlar, ish stantsiyalari, hattoki mobil qurilmalarda ham ishlatiladi.

Ext4 — Fourth Extended File System — zamonaviy fayl tizimi bo‘lib, u quyidagi afzalliklarga ega:

- 16 TB dan ortiq bo‘limlarni qo‘llab-quvvatlashi: Bu juda katta hajmdagi ma’lumotlarni boshqarish imkonini beradi va katta xotiraga ega zamonaviy qurilmalar bilan mos keladi;

- Jurnallash (journaling) tizimi orqali fayllarni tiklash imkoniyati mavjud. Bu tizim fayl tizimida yuzaga kelgan nosozliklar yoki to‘satdan elektr ta'minotining uzilishi holatlarida fayl tizimining yaxlitligini saqlab qoladi. Jurnallar orqali oxirgi operatsiyalar qayta tiklanadi;

- Fayl joylashuvini optimallashtirish mexanizmlari mavjud bo‘lib, fayllar diskda iloji boricha ketma-ket joylashtiriladi. Bu esa o‘qish/yozish tezligini oshiradi va umumiy tizim samaradorligini yaxshilaydi;

- Fayllar ustida parallel operatsiyalarni bajara olish, ayniqsa server tizimlarida bir vaqtning o‘zida ko‘plab foydalanuvchi murojaatlari amalga oshirilganda juda muhimdir. Bu Ext4 fayl tizimini yuqori yuklama sharoitlarida barqaror ishlashga moslashtiradi.

Linuxda har bir fayl yoki katalogga inode deb nomlanuvchi maxsus tuzilma biriktirilgan bo‘ladi. Inode — bu fayl tizimidagi har bir fayl yoki katalog uchun saqlanadigan metama’lumotlar to‘plamidir. Inode faylning o‘zida emas, balki uning atributlari, ya’ni fayl haqida ma’lumotlarni saqlaydi. Bu tuzilma fayl tizimining ichki ishlash prinsiplarini belgilaydi va uni boshqa tizimlardan ajratib turadi.

Inode quyidagi muhim ma’lumotlarni o‘z ichiga oladi:

- Faylning turi (oddiy fayl, katalog, havola (link), qurilma fayli va boshqalar). Bu ma’lumot orqali tizim fayl bilan qanday munosabatda bo‘lishi kerakligini aniqlaydi;

- Faylga oid ruxsatlar, ya’ni kim faylni o‘qishi, yozishi yoki bajara olishini belgilovchi o‘quv, yozuv va bajaruv huquqlari. Bu Linuxdagi xavfsizlik siyosatining asosiy elementlaridan biri hisoblanadi;

- Foydalanuvchi identifikatori (UID) va guruh identifikatori (GID) — fayl egasi va u mansub bo‘lgan guruhni aniqlaydi;

- Fayl hajmi — baytlarda ko‘rsatiladi, bu foydalanuvchi interfeysida fayl hajmini aniqlash imkonini beradi;

- Yaratilgan vaqti, oxirgi bor o‘zgartirilgan va o‘qilgan vaqti — bu vaqt belgilaridan fayl ustida kim va qachon ish olib borganini aniqlash mumkin;

- Faylning diskdagi joylashuvi, ya’ni fayl ma’lumotlari saqlanadigan data block manzillari. Inode ushbu bloklarga yo‘naltiruvchi ko‘rsatkichlar (pointerlar) orqali bog‘lanadi. Agar fayl juda katta bo‘lsa, ko‘p darajali (indirekt) pointerlar yordamida faylning qolgan qismi joylashtirilgan bo‘sh bloklar bilan bog‘lanadi.

Inode tuzilmasining yana bir afzalligi — u fayl nomini saqlamaydi. Fayl nomi va u tegishli bo‘lgan inode raqami katalog fayllarida alohida saqlanadi. Bu orqali bir nechta fayl nomlari bitta inode'ga havola qilishi mumkin (qattiq havolalar — hard links).

Inode pointerlari orqali fayllar fizik disk bloklariga bog‘lanadi. Har bir inode tuzilmasi odatda 12 yoki 13 pointerni o‘z ichiga oladi. Fayl kichik bo‘lsa (masalan, matnli

hujjat, konfiguratsion fayl yoki skript), unda to‘g‘ridan-to‘g‘ri pointerlar (direct pointers) orqali faylning ma’lumotlari bevosita diskdagi ma’lum bloklarga bog‘lanadi. Bunday pointerlar odatda 10 tagacha bo‘lib, har biri bir blok manzilini ko‘rsatadi. Bu pointerlar orqali to‘g‘ridan-to‘g‘ri faylning ma’lumotlarini tezkor o‘qish mumkin.

Fayl hajmi oshgani sari, ushbu to‘g‘ridan-to‘g‘ri pointerlar yetarli bo‘lmaydi va bu holatda 1-darajali indirekt pointer ishga tushadi. Bu pointer bir blokdagi ko‘plab yangi pointerlar ro‘yxatini o‘z ichiga oladi — masalan, bir blokda 128 ta manzil bo‘lishi mumkin. Fayl hajmi yana ortsa, 2-darajali (double indirekt) pointer va undan keyin 3-darajali (triple indirekt) pointerlar ketma-ketlikda faol bo‘ladi. Ushbu indirekt pointerlar orqali fayl juda katta bo‘lsa ham (masalan, bir necha gigabayt yoki terabayt), uni bo‘lib-bo‘lib saqlash va boshqarish imkoniyati yaratiladi.

Bu mexanizm, ayniqsa katta hajmli, murakkab strukturalarga ega ma’lumotlar bilan ishlovchi tizimlar uchun qulaydir. Masalan:

- HD yoki 4K video fayllar;
- ISO obrazlar, arxivlar va disk tasvirlari;
- Blockchain ma’lumotlari (kriptovalyutalar bilan bog‘liq);
- Serverdagi log fayllari va zaxira nusxalar.

Bunday fayllar bir necha minglab bloklardan iborat bo‘lishi mumkin va bu bloklarning izchil boshqarilishi inode va uning pointerlari orqali amalga oshiriladi.

Raqamli kriminalistika nuqtai nazaridan, Linux tizimi axborot izlarini saqlash borasida ancha qulay platforma hisoblanadi. Fayl tizimlarida fayl o‘chirilganda u darhol diskdan yo‘q qilinmaydi. Inode yozuvining mos flaglari (belgilari) o‘zgartiriladi va fayl “o‘chirilgan” deb belgilanadi. Ammo uning haqiqiy ma’lumotlari (bloklardagi kontent) hali diskda mavjud bo‘ladi, to u ustiga yangi fayl yozilmaguncha. Bu esa kriminalistik tahlilchilar uchun muhim imkoniyat — o‘chirilgan fayllarni tiklash ehtimoli mavjud.

Quyidagi Linux buyruqlari kriminologik tekshiruvlar uchun amaliy jihatdan foydalidir:

- badblocks — diskdagi yomon sektorlarni aniqlab, ularni ro‘yxatga olish imkonini beradi. Yomon sektorlar jinoyatchilar tomonidan maxfiy ma’lumotlarni yashirish uchun foydalanilishi mumkin

- e2fsck — fayl tizimining yaxlitligini tekshirib, xatoliklar yoki nomuvofiqliklarni aniqlaydi. Bu vosita diskdagi tuzilmalarni tahlil qilishda muhim vositadir;

- ls -ia — fayllarning inode raqamlarini va ularga tegishli havola (link) sonini ko‘rsatadi. Bu orqali bir faylga nechta havola mavjudligini aniqlab, ma’lumotni yashirish yoki nusxalash holatlarini topish mumkin;

- ln va ln -s — mos ravishda qattiq havolalar (hard links) va ramziy havolalar (symbolic links) yaratish uchun ishlatiladi. Havolalar orqali jinoyatchilar o‘chirilgan ko‘rinishdagi, ammo hali mavjud bo‘lgan fayllarga kirishni davom ettirishlari mumkin.

Qattiq havolalar bir xil inode raqamiga ega bo‘lib, faylning asl nusxasidan ajralmaydi. Ya’ni, birinchi nusxa o‘chirilsa ham, boshqa havola orqali unga kirish mumkin. Bu jihat raqamli jinoyatlarda dalillarni yashirish yoki ko‘paytirish uchun

ishlatilishi mumkin. Ramziy havolalar esa mustaqil inodega ega bo‘lgan yo‘naltiruvchi fayllardir, ular boshqa kataloglar, hatto boshqa disk bo‘limlariga ham ishora qilishi mumkin.

Linuxda qo‘llaniladigan raqamli kriminalistika vositalari:

Sleuth Kit — bu komandali qator interfeysda ishlovchi kuchli vositalar to‘plami bo‘lib, tsk_recover, fls, icat, ils kabi buyruqlardan iborat. Ular diskdagi fayl tizim tuzilmalari, inode yozuvlari, fayl bloklarini chuqur tahlil qilish imkonini beradi. Ayniqsa, o‘chirilgan fayllarni tiklash va kim tomonidan yaratilganini aniqlash uchun qo‘llaniladi.

Autopsy — Sleuth Kit asosida ishlaydigan grafikli (GUI) interfeysga ega vosita. Foydalanuvchiga disk tasvirlarini ko‘rish, jurnallarni tahlil qilish, so‘z bo‘yicha qidiruvlar olib borish, skrinshotlar olish, va dalil sifatida fayllarni saqlash imkonini beradi. Sud-tergov jarayonlari uchun mos va yuridik jihatdan qabul qilinadigan natijalarni yaratadi.

Foremost — bu fayllarni header va footer imzolari asosida aniqlab, RAW tasvirlardan ularni ajratib olish imkonini beruvchi kuchli data carving vositasi. U ko‘plab fayl formatlarini tanib oladi va o‘chirilgan ma’lumotlarni tiklashda foydali.

TestDisk va PhotoRec — diskni tiklash, partitsiyalarni qayta aniqlash va media fayllarni qirib olish (carving) uchun ishlatiladi. Ayniqsa, fleshkalar va SD kartalardan fayl tiklash uchun juda foydali.

- Bu vositalar orqali kriminalistika mutaxassislari quyidagilarni amalga oshirishlari mumkin:

- Disk tasvirlarini yaratish va tahlil qilish (read-only holatda);

- Fayl tizim tuzilishini tekshirish, xususan inode orqali;

- O‘chirilgan fayllarni qidirish, tiklash va ularning yaratilgan, o‘zgartirilgan vaqtlarini aniqlash;

- Fayllar, kataloglar, havolalar va jurnal yozuvlari asosida foydalanuvchi faoliyatini tiklash;

- Jinoyatga oid dalillarni aniqlash va hujjatlashtirish.

Xususan, inode raqamlarining o‘zgarishini yoki noto‘g‘ri ko‘rsatilgan havolalar sonini aniqlash orqali, kim faylga oxirgi bor murojaat qilganini, qanday o‘zgarishlar kiritganini, qachon fayl o‘chirilganini va bu kimga tegishli bo‘lishi mumkinligini aniqlash mumkin. Bu esa raqamli tergov jarayonining eng muhim bosqichlaridan biridir.

XULOSA.

Linux operatsion tizimining fayl tizimi, ayniqsa Ext4, zamonaviy raqamli infratuzilmalarda yuqori ishonchlilik va barqarorlikni ta’minlaydi. Fayllarning inode tizimi orqali boshqarilishi, disk bloklarining aniq va izchil tashkil etilishi, jurnallash imkoniyatlari va ko‘p darajali pointerlar kabi texnik xususiyatlari uni raqamli kriminalistika sohasida ham samarali platformaga aylantiradi.

Fayl o‘chirilganidan so‘ng uning haqiqiy ma’lumotlari ma’lum vaqtgacha diskda saqlanib qoladi, bu esa kriminalistik tahlilchilar uchun dalillarni tiklash va tekshirish imkonini beradi. Bunda badblocks, e2fsck, ls -ia, ln, ln -s kabi buyruqlar, shuningdek, Sleuth Kit, Autopsy va Foremost kabi maxsus tahlil vositalari katta yordam beradi.

Shu bois, axborot xavfsizligi, sud-tergov jarayonlari va kriminalistika yo‘nalishlarida ishlovchi mutaxassislar Linux fayl tizimi tuzilmasi va uning ichki mexanizmlarini chuqur o‘rganishlari zarur. Bu nafaqat o‘chirilgan yoki yashirilgan fayllarni aniqlashda, balki axborotning ishonchliligini baholashda ham muhim ahamiyatga ega.

ADABIYOTLAR:

1. The Sleuth Kit and Autopsy. Rasmiy sayt: www.sleuthkit.org
2. Foremost — Open Source Forensics Tool. Rasmiy manba: http://foremost.sourceforge.net
3. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 3rd Edition.
4. Carrier, Brian. File System Forensic Analysis. Addison-Wesley, 2005.
5. Tanenbaum, A. S. & Bos, H. Modern Operating Systems. 4th Edition, Pearson.
6. Бабаян, В. М., Linux. Основы администрирования. СПб: Питер, 2021.
7. Андрей Юдин, Linux глазами хакера. СПб: БХВ-Петербург, 2020.
8. Stallings, William. Operating Systems: Internals and Design Principles. 9th Edition, Pearson, 2017.
9. O‘zbekiston Respublikasi «Axborotlashtirish to‘g‘risida»gi Qonuni, 2003 yil