

Qilichev E.J

Muhammad al-Xorazmiy nomidagi TATU 2-bosqich magistranti

Ilmiy rahbar: Gafurov A.A

Anatatsiya: *Ushbu ishda zararlangan fayllar, ularning aniqlash vositalari va zararlanish yo'llaridan himoya qilish algoritmlarini ishlab chiqish keltirib o'tilgan.*

Kalit so'zlar: *Zararlangan fayllar.*

Zarargan fayl – ma'lumotlarning xususiyati va tuzilishida o'zgarish sodir bo'lgan fayl. Bunday o'zgarishlar natijasida fayl yaroqsiz yoki foydalanish uchun qoniqarsiz bo'lib qoladi.

Zarar turlicha bo'lishi mumkin, agar foydalanuvchi ma'lumotlarga kirish huquqini to'liq yoki qisman yo'qotilganda. Ma'lumotlarning faqat bir qismi yo'qolsa, qolgan qismiga shikas yetmasa zarar etkazilmagan ma'lumotlarning qolgan qismiga kirish imkoni bo'ladi.

Fayl buzilishining asosiy sabablari

- Diskdagi ma'lumotlar o'chirilgandan so'ng fayllarni tiklash;
- Disk bo'ladigan xatolar;
- Virus yoki antiviruslarning faylga ta'siri;
- Ilovadagi kuzatiladigan xatolar;
- Foydalanuvchi harakati;

Ushbu buzilishlarning birin - ketin ko'rib chiqsak.

Diskdagi ma'lumotlar o'chirilgandan so'ng fayllarni tiklash;

Diskdagi keraksiz ma'lumotlarni o'chirganingizdan so'ng, keraksiz malumotlar bilan birga muhim ma'lumotlar ham o'chib ketganligiga duch kelasiz. Bunday hollarda, o'chirilgan ma'lumotlarni qayta tiklash uchun yordamchi dasturlarga muhtojlik sezasiz. Ushbu ilovalar to'g'ridan-to'g'ri fayl tizimi bilan ishlaydi. Agar fayl haqidagi ma'lumotlar tizimdan to'liq o'chirilmagan bo'lsa ularning faylni katta yoki kamroq darajada tiklash imkoni bor.

Birinchidan, agar siz fayllarni o'chirib tashlaganingizdan so'ng disk bilan faol ishlagan bo'lsangiz, tasodifan o'chirilgan fayl joyiga yangi ma'lumotlar yozilishi mumkin. Buning sababi quydagicha, tizim yangi ma'lumotlar o'chirish jarayonida bo'shatilgan joyga yozadi.

Yana bir keng tarqalgan holat - o'chirilgan faylning bloklash ketma-ketligini to'liq tiklash mumkin emas. Bunday holda, ilovalar ichki algoritmlardan foydalangan holda fayllar bilan bog'liq kutilgan bloklarni olishga harakat qiladi, bu har doim ham kutilgan natijani keltirmaydi.

O'chirilgandan keyin fayllarni tiklashda mumkin bo'lgan zararni umumlashtirib, biz quyidagi odatiy muammolarni ajratib ko'rsatishimiz mumkin:

Faylning bir qismi yangi ma'lumotlar bilan qayta yoziladi.

Asl faylning bir qismini qayta tiklash mumkin edi, lekin shu bilan birga, faylga unga aloqador bo'lmagan bloklar noto'g'ri tayinlangan.

Disk xatosi

Ko'pincha tashuvchining o'zi ishlashida muammolar paydo bo'lgan holatlar mavjud. Disk - bu ma'lumotlarni saqlash uchun bloklar to'plami (ushbu maqolada biz aniqroq "sektor", "klaster", "trek" va boshqalar o'rniga mavhum "blok" atamasidan foydalanamiz). Vaqt o'tishi bilan, ommaviy axborot vositalaridan foydalanganda, ba'zi bloklar yaroqsiz bo'lib qolgan va nosozlikdan oldin mavjud bo'lgan ma'lumotlarga kirish imkoni bo'lmagan holatlar yuzaga keladi. Muhim fayllarga tegishli ma'lumotlar buzilgan bloklarda saqlangan bo'lsa, bu ayniqsa yoqimsiz. Bunday holda, o'qishga harakat qilishda ham, yozishga harakat qilishda ham xatolar yuzaga keladi. U quyidagicha namoyon bo'ladi: aytaylik, Word hujjatingizning bir qismi shikastlangan blokda saqlangan. Microsoft Word faylni ochishga harakat qilganda, diskdan ushbu qismni o'qishga harakat qiladi, tizimdan operatsiyaning mumkin emasligi haqida xatolik oladi, natijada matn protsessor faylni ochishning mumkin emasligi haqida xabar beradi.

Zararlangan diskdan faylni tiklash

Agar disk qismlarga bo'lingan bo'lsa, ba'zi fayllar undan zararsiz o'qilishi mumkin.

Yomon bloklarga yozish uchun etarlicha zararli bo'lgan fayllar maxsus dasturlari yordamida chiqarilishi kerak va ular keyingi davolanishni talab qiladi.

Virus yoki antivirusning ta'siri

Ma'lumotlarning buzilishining mumkin bo'lgan sabablari viruslarning ta'siri va antiviruslarning noto'g'ri ishlashi ham bo'lishi mumkin.

Viruslar va ularning turlarining batafsil tavsifi ushbu maqola doirasidan tashqarida. Ammo shuni ta'kidlash kerakki, viruslarning ba'zi turlari zarar etkazish uchun foydalanuvchi fayllarini keraksiz ma'lumotlar bilan ataylab yozishi mumkin. Ko'pgina viruslar buni o'zlarining "replikatsiya" jarayonida ham amalga oshiradilar, fayllarning bir qismini foydalanuvchi kompyuterida va boshqa mashinalarda tarqatish bilan birga yozadilar, shuningdek niqoblash uchun.

Agar ta'rifga ko'ra, biz virusdan yaxshi narsa kutmasak, qanday qilib zarar manbai antivirus bo'ladi? Umuman olganda, antivirusning ishlash printsiplari fayl mazmunini o'qish va unga ma'lum bo'lgan viruslarga xos bo'lgan zanjirlarni ("imzolar") baytlar ketma-ketligida qidirishdan iborat. Xavfsizlikni ta'minlash uchun foydalanuvchi ma'lumotlarini virus zanjiri sifatida noto'g'ri talqin qilish va faylni kesib tashlash mumkin bo'lgan holatlar istisno qilinmaydi. So'nggi paytlarda antivirus algoritmlari sezilarli darajada yaxshilangan bo'lsa-da, bunday holatlar vaqti-vaqti bilan bo'lib turishi mumkin. Zarar zonalarini diskdagi bloklarning chegaralariga to'g'ri kelmaydi, lekin bloklardan kichikroq yoki kattaroq bo'lishi mumkin.

Ilovadagi xatolar

Foydalanuvchi ma'lumotlarining buzilishining keng tarqalgan omili - bu fayllarni ko'rish va tahrirlash uchun ishlatiladigan dasturdagi xato. Bu omil mustaqil ravishda ham, boshqa omillar bilan ham muammolarni keltirib chiqarishi mumkin (elektr quvvatining uzilishi, dasturga antivirus ta'siri, RAM etarli emas). Deyarli har doim faylga o'zgarishlarni saqlash vaqtida muammolar paydo bo'ladi. Photoshopda uch o'lchamli tasvir tahrirlangan, sezilarli o'zgarishlar amalga oshirilgan, keyin o'zgarishlarni saqlashga urinayotganda, dastur bazi sabablarga ko'ra ishdan chiqadi. Fayl qisman yozilgan va shuning uchun shikastlangan ko'rinadi. Saqlangan tasvirni yana ochishga harakat qilganingizda, dastur bunga dosh bera olmaydi, chunki ichki tuzilma izchil emas. Bu dastur ishdan chiqishining mumkin bo'lgan sabablaridan faqat bir misol. Zararning "klinik ko'rinishi" viruslar, antiviruslar tomonidan zararlanganda ko'rish mumkin bo'lgan narsaga yaqin. Agar zarar ishi bitta bo'lsa, unda buzilish sababini tushunish deyarli mumkin emas. Juda ko'p omillar va ularning kombinatsiyasi xatoga olib kelishi mumkin. Profilaktik chora sifatida ma'lumotlaringizning e'lon qilinmagan zaxira nusxasini oling.

Agar zarar muntazam ravishda sodir bo'lsa, unda ular yuzaga kelgan sharoitlarni ko'rib chiqishga arziydi. Muammodan xalos bo'lish uchun siz bir necha yo'nalishga qarashingiz kerak. Qidiruv tizimiga olingan xato xabarlarini kiriting, ko'pincha xato tavsifi bilan birga siz uning echimini topasiz. Fayllarni buzadigan dasturni yangilang. Operatsion tizim yangilanishlarini o'rnating. Zararlangan fayllarni maxsus dasturlar yordamida tiklash mumkin.

Foydalanuvchi harakati

Foydalanuvchi harakatlari ham faylning buzilishiga olib kelishi mumkin. Yorqin misol - barcha to'plangan o'zgarishlar unga yozilmagan bir vaqtda flesh-diskni kompyuterdan uzib qo'yish. Buzilgan hujjatlar, shikastlangan fotosuratlar shu tarzda olinadi.

Foydalanuvchilar uchun bir nechta oddiy maslahatlar: Iloji bo'lsa, mediada joylashgan fayllarni hech qachon tahrirlamang.

ADABIYOTLAR RO'YXATI:

1. S.K.G'aniev, M.M. Karimov, K.A. Toshev «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi», «Aloqachi» 2008 yil
2. Эдель Д.А., Гуфан К.Ю. Способ автоматического выявления вредоносных вложений на основе использования скрытых марковских моделей // Материалы Седьмой Всероссийской научно-практической конференции "Перспективные системы и задачи управления". - Таганрог: Изд-во ТТИ ЮФУ, 2012. - 343 с.

3. Михайлов А. В. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. – М.: Диалог-МИФИ, 2012. – 148 с.
4. Партыка Т. Л. Информационная безопасность учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ, 2011. – 432 с.