MA'LUMOTLARNI YASHIRISHDA ZAMONAVIY FAYL TIZIMLARINING VAQT BELGILARIGA ASOSLANGAN STEGANOGRAFIYANI QO'LLASH

Nuriddin Akbarovich Jabbarov
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, o'qituvchi-stajyor
nuriddinjabbarov2696@gmail.com

Ilyos Hamidulla o'g'li Vaydullayev
Geologiya fanlari universiteti, o'qituvchi
vaydullayevi@gmail.com

ANNOTATSIYA

Ushbu tadqiqod ishida raqamli steganografiyaning so'nggi yutuqlari orasida turli xil fayl tizimlarining tuzilishidagi imkoniyatlarni hisobga olgan holda ma'lumotlarni yashirish usullari alohida tahlil qilib o'tilgan. Bu usullar ma'lumotlarni saqlash vositalari xususiyatlari bilan bevosita bog'langan. Tadqiqotimizning asosiy maqsadi - klasterli fayl tizimlarida ma'lumotlarni yashirish usullarining tahlilini o'tkazish, ularning imkoniyatlarini tadqiq qilish va ma'lumotlarni steganografik himoya qilishning samarali mexanizmlarini yaratishdan iborat. Ushbu ishimizda asosiy e'tibor steganografiya sohasining kiberxavfsizlik muammolarini yechishdagi ahamiyatiga qaratilgan.

Kalit so'zlar: *Steganografiya, NTFS, FAT va ext4 fayl tizimlari*, TOMS tizimi, MFT yozuvlari.

ABSTRACT

In this research paper, among the latest advances in digital steganography, data hiding methods are analyzed separately, taking into account the possibilities in the structure of various file systems. These methods are directly related to data storage media. The main purpose of this study is to analyze the methods of data concealment in cluster file systems, to study their capabilities and to create effective mechanisms for steganographic data protection. In this paper, we focus on the role of steganography in solving cybersecurity problems.

Keywords: *Steganography, NTFS, FAT and ext4 file systems, TOMS system, MFT records.*

KIRISH

Fayllarning vaqt belgilarini steganografik kanal sifatida ishlatib maxfiy axborotlarni fayl tizimining qismlariga yashirish mumkin. Yuqori aniqlikka ega taymerlarga asoslangan zamonaviy operatsion tizimlarining vaqt belgilari saqlanish va ishlatilish jarayonlarida informatsion uzilishlar vujudga keladi. Shu jarayonlarni hisobga olib ma'lumotlarning maxfiyligini, ishonchligini va foydalanuvchanligini ta'minlovchi ko'p sathli steganografik tizimni shakllantirishni amalga oshirsa bo'ladi. Quyida taqdim etilgan usul turli xil fayl to'plamlaridan iborat millionlab fayllarga ega NTFS fayl tizimi yordamida nazariy va amaliy tahlillarga ko'ra baholanadi. Fayl tizimidan oddiy foydalanish jarayonida ushbu usuldan foydalanib yashiringan ma'lumotlarning aniqlab olish deyarli imkonsiz. Qolaversa, taqdim etilgan usul raqamli kriminalistika sohasida ham ma'lumotlarni yashirish va ularni mavjudligini fosh etishda qo'llanilishi mumkin.

ASOSIY QISM

Fayl tizimi asosida ma'lumotlarni yashirish uchun "fishy" tizimi natijalari yordamida hozirgi kunda eng ommabop fayl tizimlari bo'lgan NTFS, FAT va ext4 fayl tizimlari uchun ma'lumotlarni yashirish usullarini tahlil qilish mumkin. Tahlil natijalari 1-jadvalda berilgan. Jadvalda ✓ belgisi bilan belgilangan maydonlar tekshirish o'tkazilgan usullarni, ✗belgisi bilan belgilangan maydonlar hali o'rganish jarayoni kechayotganini va - belgisi bilan bu usul boshqa fayl tizimlarida mavjud emasligini bildirish uchun ishlatilgan. Bundan tashqari jadvalda ma'lumotni yashirish usullarning yashirin axborot hajmi, bardoshliligi va aniqlanish ehtimolliklari ham baholangan.

Fayl tizimining texnik xususiyatlari ma'lumotlarni tavsiflash uchun qo'shimcha ma'lumotlar tuzilmalarining (ya'ni "metama'lumotlar") asl nusxasi kabi kirish huquqlari va muhim fayl voqealari sodir bo'lgan sana va vaqtni aniqlaydi.

1-jadval. Fayl tizimi maydonlarida ma'lumotni yashirish usullari haqida umumiy ma'lumot

Usul nomi	Ta'rif	Yashirilishi mumkin bo'lgan ma'lumot hajmi	Aniqlanish ehtimolligi	Bardoshliligi	Fayl tizimi		
					FAT	NTFS	EXT4
fileslack	File Slack dan foydalanish	yuqori	o'rtacha	past	✓	✓	✓
Mftslack	MFT Slack dan foydalanish	yuqori	yuqori	past	-	✓	-
Ads	AltDS ni qo'llash	yuqori	yuqori	o'rtacha	-	✓	-
Addcluster	Qo'shimcha klaster/Blok joylash	yuqori	o'rtacha	past	✓	✓	✓
Badcluster	Nosoz klasterlar/ Blok joylash	yuqori	o'rtacha	yuqori	✓	✓	✓
Reserved gdt blocks	Zahira GDT bloklardan foydalanish	yuqori	yuqori	o'rtacha	-	-	✓
Superblock slack	Superblok maydonidan foydalanish	o'rtacha	yuqori	yuqori	-	-	✓
superblock reserved	Zahira superblok maydonidan foydalanish	past	o'rtacha	yuqori	-	-	✓
superblock backups	Superblock zahira nusxalaridan foydalanish	o'rtacha	o'rtacha	yuqori	-	-	✓
osd2	Foydalanilmagan osd2 inod maydonidan foydalanish	past	o'rtacha	yuqori	-	-	✓
obso faddr	Foydalanilmagan Obso_faddr inod maydonidan foydalanish	past	o'rtacha	yuqori	-	-	✓
Bootsector	Yuklovchi sektor maydonidan foydalanish	past	yuqori	yuqori	✓	✓	✓
null_dir_entries	Nulli dir yozuv maydonidan foydalanish	yuqori	o'rtacha	past	-	-	✓
gdt_slack	Gdt yozuvlari katalogidan foydalanish	o'rtacha	yuqori	o'rtacha	-	-	✓
groupdescr_reserved	Group-desc dagi zahira maydonidan foydalanish	past	o'rtacha	yuqori	-	-	✓
gdt backups	Gdt zahira nusxalaridan foydalanish	yuqori	o'rtacha	o'rtacha	-	-	✓
blockbitmap slack	Block Bitmap zahira maydonidan foydalanish	past	yuqori	yuqori	-	-	✓
inodebitmap slack	Inode Bitmap zahira maydonidan foydalanish	past	yuqori	yuqori	-	-	✓

inode slack	Indekslangan inode zahiralaridan foydalanish	yuqori	o‘rtacha	o‘rtacha	-	-	✓
inode reserved	Inode tuzilmasida zahira maydondan foydalanish	yuqori	o‘rtacha	yuqori	-	-	✓
uninit data structure	Uninitialized Block Groups maydonidan foydalanish	yuqori	o‘rtacha	past	-	-	✓

Umumiy metama’lumotlar ham faylning ishlash davrini tavsiflovchi vaqtinchalik ma’lumotlar kabi foydalanuvchi harakatlariga va operatsion tizimning o‘ziga juda sezgir bo‘lishadi. Masalan fayllar hodisalarining ma’lum vaqt belgilarini istalgan vaqtda fayl tizimidan normal usulda yozib olinishi mumkin. Bunga faylning oxirgi modifikatsiyasi va oxirgi kirish vaqt belgisi kirishi mumkin. Bizning ma’lumotimizga ko‘ra vaqtinchalik ma’lumotlarning nozikligi vaqt belgilarining hali ham steganografik vosita sifatida o‘rganilmaganiga sabab bo‘lishi mumkin.

Zamonaviy fayl tizimidagi vaqt belgilari. Zamonaviy fayl tizimlari vaqt belgilarini qanday ishlatishini quyidagi bo‘limda tahlil qilinadi. Olg‘a surmoqchi bo‘lgan taxmin shuni anglatadiki vaqt belgilarida foydalanilmagan (ortiqcha) bo‘shliqlar mavjud bo‘lib, ular steganografik quvvatga ega bo‘lgan mantiqiy kanalni yaratish uchun yetarli. Ko‘pgina zamonaviy fayl tizimlari vaqt belgilari sifatida 64 bitli qiymatlardan foydalanganligi va ikkinchi soniyali bo‘laklash usulini taklif qilishini 1-jadval yordamida aniqlashimiz mumkin. Ushbu jadval ma’lumotlari bugungi kunda iste’molchilarning asosiy foydalanadigan operatsion tizimlari yoki unga kiradigan barcha fayl tizimlarini qamrab oladi (masalan, Apple OS X, Google Android, GNU/Linux va Microsoft Windows). *Vaqt belgilarini yaratish noyob hodisa hisoblanib ma’lumotning katta statik qismi hisoblanadi [1]. Har safar faylga murajaat qilinganda yoki unga o‘zgartirish kiritilganda vaqt belgilarining kirish va o‘zgartirish qismlari ham yangilanadi. Vaqt belgilari qismlariga ma’lumot yashirishning ikkita yangi vositasi mavjud. Timestamp-Magic tizimi ext4 fayl tizimining bir necha vaqt belgilari indeks ro‘yxatining nanosekund qismiga ma’lumotlarni yashirish imkoniyatiga ega [2]. TOMS tizimi esa aynan shu usulni NTFS fayl tizimining MFT yozuvlarining filename atributiga ma’lumotlarni yashiradi. Quidagi jadvalda eng keng tarqalgan fayl tizimlarining vaqt belgilari haqidagi ma’lumotlar keltirilgan.*

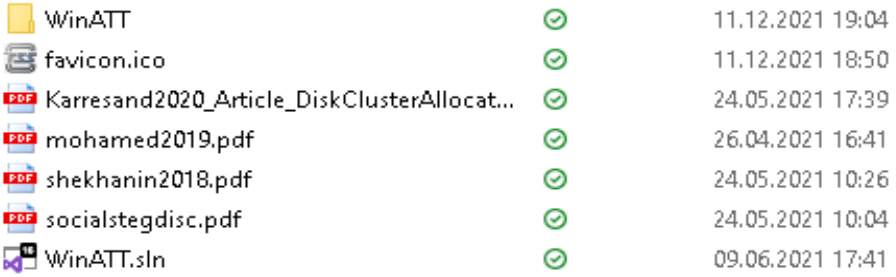
2-jadval. Eng keng tarqalgan fayl tizimlarining vaqt belgilari

Fayl tizimi	Fayl vaqt belgisi	Hajmi	Vaqt bo‘laklari
NTFS	Yaratish	64 bit	100 nsek
	Kirish	64 bit	100 nsek
	O‘zgartirish	64 bit	100 nsek
	MFT yozuvini o‘zgartirish	64 bit	100 nsek
ext4	Yaratish	64 bit	1 nsek
	Kirish	64 bit	1 nsek
	O‘zgartirish	64 bit	1 nsek
	O‘zgartirish atributi	64 bit	1 nsek
Btrfs	Yaratish	64 bit	1 nsek
	Kirish	64 bit	1 nsek
	O‘zgartirish	64 bit	1 nsek
	O‘zgartirish atributi	64 bit	1 nsek
ZFS	Yaratish	64 bit	1 nsek
	Kirish	64 bit	1 nsek
	O‘zgartirish	64 bit	1 nsek
	O‘zgartirish atributi	64 bit	1 nsek
FAT32	Yaratish	32 bit	2 sek
	Kirish	16 bit	1 kun
	O‘zgartirish	32 bit	2 sek
HFS+	Yaratish	32 bit	1 sek
	Kirish	32 bit	1 sek
	O‘zgartirish	32 bit	1 sek
	O‘zgartirish atributi	32 bit	1 sek
	Zahira nusxalash	32 bit	1 sek
ext3	Kirish	32 bit	1 sek
	O‘zgartirish	32 bit	1 sek
	O‘zgartirish atributi	32 bit	1 sek

Jadvaldagi ma’lumotlarga asosan tahlil qilingan barcha faly tizimlari quyidagi 3 ta vaqt belgisini qo‘llab quvvatlaydi. Bular yaratish, kirish va o‘zgartirish. Uchala vaqt belgilari ham sana va vaqt bilan bog‘liq bo‘lgan ma’lumotlarni sekund aniqligida saqlaydi.

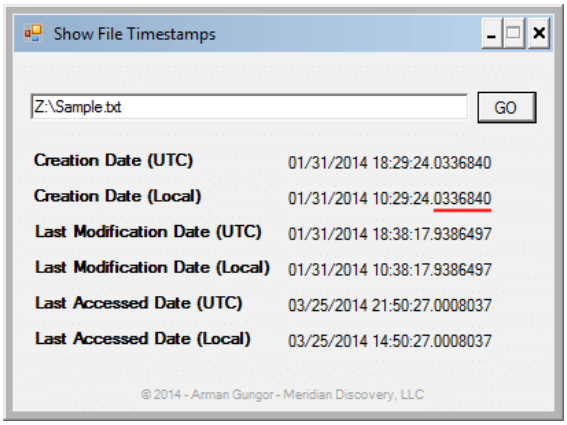
MUHOKAMA VA NATIJA

Fayllarni nusxalash, ularga o‘zgartirish kiritish kabi operatsion tizimning standart yangilanishlaridan tashqari fayl tizimining vaqt belgilari oddiy foydalanuvchilar tomonidan manipulyatsiya qilinishga operatsion tizim tomonidan cheklab qo‘yilgan. Ammo buzg‘unchi shaxslar turli xil usullarni qo‘llab ushbu vaqt belgilarini o‘zgartirishlari mumkin. Bunga eng keng tarqalgan usul sifatida fayl tizimi vaqt belgilarini o‘zgartiruvchi dasturiy vositalar misol bo‘la oladi.



1-rasm. Windows 10 opertsion tizimida minut aniqligidagi vaqt belgilarining ko‘rinishi

Nanosaniyadagi aniqlik fayl tizimiga kiradigan oxirgi foydalanuvchilarga aniq yoki bilvosita yetkazilmaydi. Ular 1-rasmda tasvirlanganidek, sekund aniqligidagi bo‘laklashga erishadigan fayl vaqt belgisi ma’lumotlari sifatida taqdim etilmoqda. Shunday qilib, vaqt belgilari qanday saqlanishi va ulardan foydalanish o‘rtasida axborot uzilishi mavjud bo‘lishi mumkin.



2-rasm. NTFS fayl tizimida vaqt belgilarining 100 nanosekund aniqlikdagi ko‘rinishi

Demak, Windows operatsion tizimi barcha vaqt belgilarini $MFT ya’ni fayllarning asosiy jadvalida saqlaydi. Har bir NTFS fayl tizimli mantiqiy disk o‘zining $MFT fayliga ega va bu fayl joriy mantiqiy diskning maxsus MFT maydonida saqlanadi. NTFS fayl tizimi vaqt belgilari 64 bitli butun sonlar ko‘rinishidagi baytlar ketma-ketligi sifatida saqlandi.Vaqt belgilarining kengaytmasi 100 nanosekund bo‘lib,

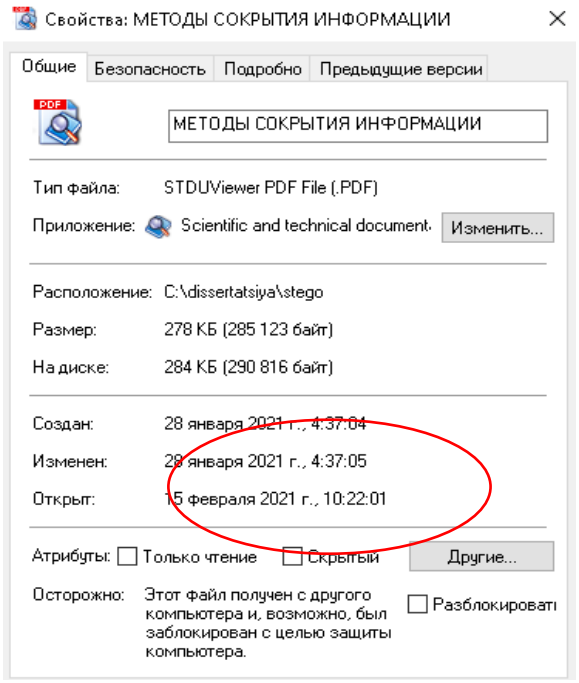
u 1601 yil 1-yanvardan boshlab UTC (Coordinated Universal Time-muvofiqlashtirilgan universal vaqt) vaqti bilan hisoblanadi. Vaqt belgilarining bunday aniqlikdagi kengaytmasi jarayonlarni osonlik bilan farqlash va ularni tartibga solish imkonini beradi. FAT tizimidan farqli ravishda NTFS tizimidagi vaqt belgilarining aniqlik darajasining yuqoriligi ularni tartiblash bilan bog‘liq muammolarni keltirib chiqaradi.

NTFS fayl tizimi vaqt belgilari ikki xil atributda $STANDARD_INFORMATION va $FILE_NAME atributlarida saqlanadi. Bu atributlar turli metama’lumotlarni o‘zida saqlaydi va yozuv uchun faqat bitta $STANDARD_INFORMATION atributi mavjud bo‘lsada, fayl uchun bir nechta $FILE_NAME atributi mavjud bo‘lishi mumkin. Vaziyatga qarab bir nechta $FILE_NAME atributlari mavjud bo‘lishi mumkin, chunki to‘rtta nom maydoni mavjud bo‘lib, ular DOS 8.3 nomlari, Windows nomlari, POSIX nomlari hamda DOS va Windows bilan mos keladigan fayl nomlari uchun umumiy nomlar maydonlaridan iborat bo‘lishi mumkin. Shunday qilib, yozuv bir vaqtning o‘zida uchta $FILE_NAME atributiga ega bo‘la oladi.

Muhim farqlardan biri shundaki, $STANDARD_INFORMATION atributi foydalanuvchi darajasidagi jarayonlar tomonidan o‘zgartirilishi mumkin, shuning uchun vaqt belgisini boshqarish vositalarining aksariyati faqat ushbu qiymatni o‘zgartiradi. $FILE_NAME atributi esa faqat tizim yadrosi tomonidan o‘zgartirilishi mumkin. Ma’lumotlarga ko‘ra, hali birorta antikriminalistik dasturiy vosita $FILE_NAME qiymatlarini o‘zgartira olmaydi. Lekin buni $MFT fayliga to‘g‘ridan-to‘g‘ri kirish orqali amalga oshirish mumkin [3].

Demak, uchta fayl vaqt belgisi ya’ni yaratish, kirish va o‘zgartirish deyarli barcha tahlil qilingan fayl tizimlari tomonidan qo‘llab-quvvatlanadi. Uchala vaqt belgilari sana va vaqtni ikkinchi darajali granularlik (bir yoki 100 ns) bilan saqlaydi. Vaqt belgilarining nanosekund aniqlikdagi qiymatlari fayl tizimi foydalanuvchilari bevosita taqdim etilmaydi. Lekin maxsus dasturlar yordamida NTFS fayl tizimi uchun vaqt belgilarining 0,1mikrosekund aniqlikdagi qiymatlarini olishimiz mumkin. Yuqoridagi 2-rasmda vaqt belgilarining nanosekund darajasi ko‘rinishidagi qiymatlar bilan taqdim etiladi. Microsoft Windows operatsion tizimi foydalanuvchilari fayl vaqt belgilarini quidagi 3-rasmda aks ettirilgandek ko‘rishadi.

Yaratish (create) vaqt belgisi faylning yaratilishi bilan bog‘liq unikal jarayon bo‘lganligi uchun statik ma’lumot turiga tegishlidir. Kirish (access) va o‘zgartirish (modification) vaqt belgilari esa har safar faylga murojaat qilinganda yoki unga o‘zgartirish kiritilganda yangilanadi.



3-rasm. Windows foydalanuvchilarida vaqt belgilarining namoyon bo‘lishi.

Zamonaviy operatsion tizimlari yuqori samaradorlikni ta’minlash maqsadida ma’lumotlarni saqlash qurilmalari texnologiyalaridagi so‘nggi yutuqlardan harajatlarni kamaytirish bilan bir qatorda ishonchlilik va bardoshlilikni ta’minlash uchun ham foydalanmoqda. Buni SSD va flesh xotira qurilamalari misolida ko‘rishimiz mumkin. Bu qurilmalarda vaqt belgilariga xizmat ko‘rsatishda fayl tizimlarining unumdorligini oshirish sozlamalarining borligi bunga yaqqol namuna bo‘ladi. Bu sozlamalar yordamida faylga oxirgi kirish yoki unga o‘zgartirish kiritish vaqt belgilarini o‘chirib qo‘yish mumkin. Bunday yondashuv ma’lumotlarni saqlash qurilmasining ish unumdorligini va albatta hayot davrini ham oshirish imkonini beradi. Shunga qaramay, ko‘pchilik foydalanuvchi darajasidagi holatlarda faqatgina kirish vaqt belgisi sozlamalari o‘zgarishsiz qoladi.

XULOSA

Yuqoridagi tahlil natijalari fayl tizimi vaqt belgilarilarini steganografik kanal sifatida ishlatilishi mumkin degan taxminimizni to‘laligicha oqladi. Fayl tizimi vaqt belgilari filtrlarida foydalanilmaydigan yoki ortiqcha maydonlarning mavjudligi ushbu usuldan foydalanib ma’lumotlarni yetarlicha hajmlarda yashirish imkoniyatini yaratib beradi. Fayl tizimi turiga va foydalanish senariysiga qarab bu sig‘im har bir fayl uchun birdan to‘qqiz baytgacha bo‘lgan hajmlarda bo‘lishi mumkin. Hozirgi kunda yuzlab, minglab va hattoki millionlab fayllarga ega zamonaviy fayl tizimlari har bir kompyuterimizda borligi hech kimga sir emas. Albatta bu maydonlarga bir necha megabayt qo‘shimcha ma’lumotlarni xavfsiz yashirish va ulardan kerakli paytga qiyinchiliksiz foydalanish imkoniyati ushbu tadqiqod ishining asosiy maqsadidir.

FOYDALANILGAN ADABIYOTLAR

1. Gyu-Sang Cho, 2016. Data Hiding in NTFS Timestamps for Anti-Forensics. International Journal of Internet, Broadcasting and Communication Vol.8 No.3 31-40
2. Göbel, T. and Baier, H., 2018. Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding. Digital Investigation, 24, pp.S111-S120.
3. Neuner, S., Voyiatzis, A., Schmiedecker, M., Brunthaler, S., Katzenbeisser, S. and Weippl, E., 2016. Time is on my side: Steganography in filesystem metadata. Digital Investigation, 18, pp.S76-S86.