

FIIT STU

Voľne šíriteľné nástroje na obnovu zmazaných súborov

Princípy Informačnej Bezpečnosti

Norbert Matuška
10-8-2024

Contents

Analýza súborových systémov.....	1
FAT32	1
Stručné vlastnosti FAT32.....	1
Mazanie súborov vo FAT32	1
Obnova zmazaných súborov vo FAT32	2
Obmedzenia FAT32	2
Záver	2
NTFS.....	3
Stručné vlastnosti NTFS.....	3
Mazanie súborov v NTFS	3
Obnova zmazaných súborov v NTFS	3
Obmedzenia NTFS	4
Záver	4
EXT4	4
Stručné vlastnosti EXT4	4
Mazanie súborov v EXT4.....	4
Obnova zmazaných súborov v EXT4	5
Obmedzenia EXT4	5
Záver	5
Analýza voľne dostupných nástrojov na obnovu údajov	6
Testdisk	6
Hlavné funkcie Testdisku	6
Ako Testdisk funguje pri obnove zmazaných dát.....	7
Recuva	7
Hlavné funkcie Recuvy	7
Ako Recuva funguje pri obnove zmazaných dát.....	8
Photorec	8
Hlavné funkcie Photorecu	8

Ako Photorec funguje pri obnove zmazaných dát	9
Testovanie	10
Predpríprava testovania	10
Testovanie v súborovom systéme FAT32	11
Náhodne mazanie súborov	11
Korupcia súborov	12
Formátovanie disku	12
Prepisovanie dát na disku	13
Zhrnutie pre súborový systém FAT32	13
Testovanie v súborovom systéme NTFS	13
Náhodné mazanie súborov	13
Korupcia súborov	14
Formátovanie disku	14
Prepisovanie dát na disku	15
Zhrnutie pre súborový systém NTFS	15
Testovanie v súborovom systéme EXT4	15
Náhodne mazanie súborov	16
Korupcia súborov	16
Formátovanie disku	17
Zhrnutie pre súborový systém EXT4	17
Záver a hodnotenie	19
Súborové systémy	19
Nástroje na obnovu dát	19
Celkové hodnotenie	20
Prílohy	21
Zdroje	24

Figures

Figure 1Súborový systém použitý na testovanie	11
Figure 2Používateľské rozhranie Recuvy, po úspešnej obnove zmazaných súborov.....	21
Figure 3Používateľské rozhranie PhotoRec	22
Figure 4Používateľské rozhranie TestDisku	22
Figure 5Neúspešná obnova formátovaných súborov v TestDisku.....	23
Figure 6Používateľské rozhranie DiskGenius.....	23

Analýza súborových systémov

Súborový systém je základnou zložkou každého operačného systému, ktorá určuje spôsob, akým sú organizované, ukladané a načítané údaje. V tomto projekte sa zameriam na najpoužívanejšie súborové systémy, ako sú:

- FAT32: Starší súborový systém, ktorý sa stále používa najmä na vymeniteľné médiá ako USB kľúče.
- NTFS: Hlavný súborový systém pre operačné systémy Windows, ktorý poskytuje vysokú úroveň zabezpečenia a obnovy.
- EXT4: Súborový systém, ktorý sa používa na Linuxe, poskytuje pokročilé funkcie v správe súborov a údajov.

FAT32

FAT32 (File Allocation Table, 32-bit) je jeden z najstarších a stále používaných súborových systémov. Vznikol ako rozšírenie predchádzajúcich verzií (FAT12 a FAT16) a umožnil používanie väčších diskov a súborov. Je navrhnutý tak, aby bol čo najjednoduchší a najkompatibilnejší, a to je dôvod, prečo sa používa najmä na prenosné úložiská ako USB kľúče, pamäťové karty a externé disky.

Stručné vlastnosti FAT32

Maximálna veľkosť súboru je 4 GB, to znamená, že žiadny súbor väčší ako 4 GB nemôže byť uložený na zariadení formátovanom systémom FAT32. Maximálna veľkosť oddielu: 8 TB ale to je v závislosti od operačného systému. Kompatibilita: FAT32 podporujú takmer všetky operačné systémy vrátane Windows, macOS, Linuxu a dokonca aj niektoré herné konzoly a televízory.

Mazanie súborov vo FAT32

Keď v súborovom systéme FAT32 zmažete súbor, systém nevymaže samotné dáta. Namiesto toho iba "označí" priestor, kde bol súbor uložený, ako voľný pre ďalšie použitie. Tento proces funguje tak, že sa v tabuľke alokácie súborov (FAT) vymaže záznam o danom súbore, ale dáta zostanú fyzicky na disku, až kým sa tento priestor neprepíše novými dátami.

Tabuľka FAT je v podstate zoznam odkazov na bloky (klastre) na disku, kde sú uložené dáta jednotlivých súborov. Keď sa súbor zmaže, operačný systém vymaže iba tento odkaz v tabuľke, ale skutočné dáta sú stále prítomné v klastroch. To znamená, že ak došlo k zmazaniu omylom, existuje veľká šanca, že sa súbor dá obnoviť, ak ešte nedošlo k jeho prepísaniu inými dátami.

Obnova zmazaných súborov vo FAT32

Vďaka tomu, ako FAT32 spracováva zmazané súbory, je možné použiť rôzne nástroje na obnovu dát, ktoré dokážu „prečítať“ a obnoviť obsah klastrov, ktoré sú stále na disku, ale už nemajú odkaz v tabuľke FAT. Tento proces funguje nasledovne:

Nájdenie zmazaných súborov: Nástroje na obnovu, ako napríklad TestDisk alebo Recuva, prehľadávajú úložisko a snažia sa identifikovať súbory, ktoré už nemajú odkazy v tabuľke FAT, ale ich dáta sú stále na disku. Tieto nástroje dokážu nájsť fyzické klastre, kde sú uložené dáta, a „rekonštruovať“ súbor.

Obnovenie súboru: Ak nástroj dokáže nájsť a identifikovať celý súbor, môže ho obnoviť tak, že znovu vytvorí odkaz v tabuľke FAT a umožní prístup k dátam.

Úspešnosť obnovy: Úspešnosť obnovy závisí na tom, či boli klastre so zmazanými dátami medzitým prepísané inými súbormi. Ak bol disk po zmazaní súborov stále aktívne používaný, je pravdepodobné, že niektoré alebo všetky klastre súboru boli prepísané, čo znemožňuje úplnú obnovu.

Obmedzenia FAT32

FAT32 nie je veľmi efektívny v správe fragmentovaných súborov. Keď sa súbor ukladá v niekoľkých nesúvislých častiach na rôznych miestach disku, jeho obnova môže byť zložitejšia, pretože nástroj na obnovu musí nájsť a správne pospájať všetky časti súboru. Ak po zmazaní dôjde k uloženiu nových dát na disk, môžu byť pôvodné dáta nenávratne stratené. Preto je kľúčové zastaviť akékoľvek ďalšie operácie zápisu na disk, ak si všimnete, že došlo k zmazaniu dôležitých súborov. FAT32 taktiež neposkytuje žiadne pokročilé mechanizmy na ochranu dát. V porovnaní s modernými súborovými systémami, ako je NTFS, neponúka žiadne zabudované funkcie pre šifrovanie alebo oprávnenia. To znamená, že každý, kto má prístup k úložisku, sa môže pokúsiť obnoviť zmazané súbory, čo môže predstavovať bezpečnostné riziko.

Záver

FAT32 je síce starší súborový systém, ale stále nachádza uplatnenie v mnohých zariadeniach kvôli svojej širokej kompatibilite. Z hľadiska obnovy dát je to však dvojsečná zbraň – na jednej strane je obnova relatívne jednoduchá, pokiaľ sú dáta ešte fyzicky na disku. Na druhej strane, jeho neschopnosť efektívne zvládať fragmentáciu a bezpečnostné riziká z neho robia systém menej vhodný na citlivé alebo kritické dáta.

NTFS

NTFS (New Technology File System) je moderný súborový systém, ktorý bol vyvinutý spoločnosťou Microsoft a prvýkrát predstavený v roku 1993 s príchodom systému Windows NT. Dnes je to primárny súborový systém pre Windows a nahradil staršie systémy ako FAT32 vďaka svojim pokročilým funkciám pre správu dát, bezpečnosť a výkon.

Stručné vlastnosti NTFS

Maximálna veľkosť súboru je prakticky neobmedzená (16×1024^6 bytes) v praxi limitovaná na 16 TB v závislosti od systému. Maximálna veľkosť oddielu siaha až do 256 TB, čo robí NTFS vhodným pre veľké úložné systémy. NTFS taktiež umožňuje definovanie prístupových práv k súborom a adresárom, ako aj šifrovanie dát, čo zvyšuje bezpečnosť.

Záznam o zmene dát (journaling): NTFS používa systém denníka, ktorý umožňuje zaznamenávať všetky zmeny súborov, čo zlepšuje spoľahlivosť a umožňuje rýchlejšie zotavenie po zlyhaní systému.

Mazanie súborov v NTFS

Rovnako ako pri FAT32, aj pri NTFS, keď zmažete súbor, operačný systém nevymaže fyzické dáta zo zariadenia okamžite. Súbor je „označený“ ako zmazaný a miesto, kde bol uložený, je pripravené na prepis novými dátami. Avšak NTFS je sofistikovanejší v spôsobe, akým spravuje súbory, aj vďaka Master File Table (MFT). NTFS používa štruktúru nazvanú MFT, ktorá uchováva informácie o každom súbore a adresári. Pri zmazaní súboru sa záznam o súbore v MFT nevymaže, ale označí sa ako „nepoužitý.“ Samotné dáta súboru však stále zostávajú na disku, kým nie sú prepísané novými dátami. Taktiež používa Data Streams - NTFS umožňuje priradiť k súboru viacero dátových tokov (streams). Pri zmazaní hlavného dátového toku môžu niektoré iné časti súboru zostať prítomné na disku, čo môže komplikovať úplné odstránenie alebo obnovu.

Obnova zmazaných súborov v NTFS

Vďaka tomu, že NTFS je pokročilejší súborový systém, je obnova dát o niečo zložitejšia, ale zároveň spoľahlivejšia v porovnaní s FAT32. Obnovovacie nástroje využívajú MFT na hľadanie záznamov o zmazaných súboroch a pokúšajú sa obnoviť dáta, ak ešte neboli prepísané. MFT obsahuje informácie o všetkých súboroch, vrátane tých, ktoré boli zmazané. Nástroje na obnovu dokážu využiť tieto informácie na identifikáciu a obnovu zmazaných súborov. Ak záznam o súbore stále existuje v MFT a nebol prepísaný, obnovenie súboru je relatívne jednoduché. NTFS taktiež spravuje fragmentované súbory oveľa lepšie ako FAT32. Vďaka svojej štruktúre je NTFS schopný efektívnejšie spravovať roztrúsené časti súborov po disku, čo znamená, že nástroje na obnovu dát majú vyššiu šancu úspešne obnoviť aj

fragmentované súbory. Vďaka systému denníkovania, systém môže automaticky obnoviť neuložené alebo čiastočne zmazané súbory z denníka, ak dôjde k neočakávanému zlyhaniu (napríklad výpadok elektriny). To zvyšuje spoľahlivosť obnovy dát.

Obmedzenia NTFS

Rovnako ako pri FAT32, ak sa zmazaný súbor medzičasom prepíše inými dátami, jeho obnova je nemožná. Preto je dôležité zastaviť ďalšie operácie na disku, ak sa omylom zmaže dôležitý súbor. NTFS má aj pokročilé funkcie, ako sú data streams a kompresia, čo môže sťažiť obnovu súborov. Nástroje na obnovu musia byť kompatibilné s týmito funkciami, aby mohli správne obnoviť dáta.

Ak bol súbor chránený oprávneniami alebo šifrovaný pomocou EFS (Encrypting File System), jeho obnova môže byť zložitejšia alebo dokonca nemožná bez správneho dešifrovacieho kľúča alebo oprávnenia.

Záver

NTFS je robustný a moderný súborový systém, ktorý ponúka pokročilé funkcie na správu dát a ich ochranu. Z pohľadu obnovy zmazaných súborov poskytuje viacero možností vďaka denníkovaniu a záznamom v MFT. Hoci je obnova dát často úspešná, nástroje na obnovu musia byť kompatibilné s pokročilými funkciami NTFS, ako sú šifrovanie a data streams, aby bola obnoviteľnosť súborov čo najúčinnnejšia.

EXT4

EXT4 (Fourth Extended File System) je moderný súborový systém používaný hlavne na Linuxových distribúciách. Predstavený bol v roku 2008 ako vylepšenie svojho predchodcu EXT3. EXT4 sa stal veľmi obľúbeným vďaka svojej spoľahlivosti, výkonu a schopnosti spravovať veľké objemy dát, čo ho robí ideálnym pre moderné pevné disky a SSD.

Stručné vlastnosti EXT4

Maximálna veľkosť súboru je 16 TB. Maximálna veľkosť oddielu je 1 EB (exabajt), čo je extrémne veľké množstvo dát. EXT4 používa funkciu extents, ktorá znižuje fragmentáciu tým, že alokuje súbory v súvislých blokoch. Podobne ako NTFS, aj EXT4 používa systém denníkovania, aby minimalizoval riziko straty dát pri neočakávanom vypnutí alebo zlyhaní systému. EXT4 je taktiež spätne kompatibilný s EXT2 a EXT3, čo znamená, že ich oddiely možno prečítať a upravovať bez konverzie.

Mazanie súborov v EXT4

Keď v systéme EXT4 zmažete súbor, jeho dáta nie sú okamžite odstránené. Namiesto toho je záznam o súbore zmazaný z adresára a bloky, ktoré tento súbor používali, sú označené ako

„voľné“, čo znamená, že môžu byť prepísané inými dátami. Táto metóda umožňuje obnovu zmazaných dát, pokiaľ ešte nedošlo k ich prepísaniu.

EXT4 používa systém s názvom extents, ktorý alokuje dáta vo väčších blokoch (rozšíreniach) namiesto jednotlivých blokov. To znižuje fragmentáciu, ale môže mierne skomplikovať proces obnovy, pretože bloky súborov sú uložené vo väčších a menej fragmentovaných sekvenciách.

EXT4 obsahuje aj funkciu delayed allocation, ktorá môže oneskoriť fyzický zápis dát na disk, aby zlepšila výkon. To však znamená, že pri náhlom výpadku systému môžu byť niektoré zmeny neuložené, aj keď boli logicky zmazané.

Obnova zmazaných súborov v EXT4

Obnova dát v EXT4 je založená na vyhľadávaní neprepísaných blokov, kde sú stále uložené dáta súborov. Nástroje na obnovu dát, ako napríklad extundelete a TestDisk, využívajú informácie z denníka a záznamov súborového systému na rekonštrukciu súborov. EXT4 uchováva denník, v ktorom sú zaznamenávané zmeny na disku. Nástroje na obnovu môžu použiť tieto záznamy na získanie nedávno zmazaných dát, najmä ak bol súbor nedávno odstránený a jeho dáta ešte neboli prepísané. Hoci extents znižujú fragmentáciu, môžu skomplikovať obnovu, pretože alokované bloky sú väčšie. Nástroje musia byť schopné interpretovať tieto extents, aby správne našli všetky časti súboru a vrátili ich na miesto. Taktiež funkcia delayed allocation môže spôsobiť, že niektoré dáta nebudú uložené, ak došlo k náhlému výpadku napájania alebo systému. To môže zhoršiť úspešnosť obnovy, pretože nie všetky operácie, ktoré sa v pamäti „odohrali“, boli fyzicky zapísané na disk.

Obmedzenia EXT4

Ako pri každom súborovom systéme, kľúčovým faktorom pri obnove dát je, či boli dáta medzičasom prepísané inými. Ak sa bloky, ktoré boli označené ako voľné, už použili na nové dáta, obnovenie pôvodného súboru je skôr nemožné. Hoci extents pomáhajú znížiť fragmentáciu, pre obnovu to znamená, že nástroje musia byť schopné správne spracovať tieto rozsahy. Ak dôjde k poškodeniu rozsahov, môže byť obnova dát dosť zložitá. Zápis do denníka v EXT4 zabezpečuje, že sú dáta bezpečné aj pri náhlých výpadkoch, ale denník sa používa hlavne na metadáta, nie na samotné dáta. To znamená, že ak došlo k zmazaniu alebo poškodeniu súboru, denník nemusí vždy obsahovať informácie potrebné na úplnú obnovu.

Záver

EXT4 je moderný a vysoko výkonný súborový systém, ktorý ponúka lepšiu správu dát a nižšiu fragmentáciu v porovnaní s predchádzajúcimi verziami EXT. Jeho funkcie ako extents a

delayed allocation zlepšujú výkon, ale môžu komplikovať proces obnovy dát. Avšak nástroje špecifické pre EXT4, ako extundelete, poskytujú výkonné možnosti na obnovenie zmazaných dát, pokiaľ ešte neboli prepísané novými informáciami. Celkovo je EXT4 spoľahlivý súborový systém, ktorý poskytuje solídne možnosti obnovy dát, ale úspešnosť závisí od konkrétnych podmienok, ako je prepísanie a spôsob alokácie súborov.

Analýza voľne dostupných nástrojov na obnovu údajov

Voľne šíriteľné nástroje na obnovu zmazaných súborov predstavujú efektívne a často cenovo dostupné riešenie pre používateľov, ktorí potrebujú obnoviť stratené údaje. V rámci tohto projektu sa budem zaoberať analýzou hlavne nasledujúcich nástrojov: TestDisk, ktorý je open-source nástroj na obnovu stratených diskových oddielov a opravu zavádzacieho sektora. Recuva je jednoduchý nástroj na obnovu zmazaných súborov z rôznych úložísk. Ale aj ďalšie ako napríklad Photorec, Foremost, Scalpel, Ultimate Boot CD, SafeCopy.

Testdisk

TestDisk je open-source nástroj na obnovu dát, ktorý bol pôvodne vyvinutý na obnovu stratených partícií a opravu bootovacích sektorov diskov. Postupom času sa stal výkonným nástrojom na obnovu dát, ktorý zvláda rôzne typy úloh vrátane obnovy zmazaných súborov z rôznych súborových systémov. Jeho hlavnou výhodou je univerzálnosť a to, že je bezplatný a dostupný na viacerých platformách (Windows, macOS, Linux).

Hlavné funkcie Testdisku

TestDisk dokáže vyhľadať a obnoviť stratené alebo poškodené partície. To je užitočné v prípadoch, keď sa partícia stratí kvôli chybám vo formátovaní alebo iným softvérovým problémom. Tento nástroj podporuje obnovu z viacerých typov partičných tabuliek, vrátane MBR (Master Boot Record), GPT (GUID Partition Table), a ďalších.

TestDisk môže opraviť poškodené bootovacie sektory, čo umožňuje systémom opäť zaviesť operačný systém alebo získať prístup k dátam. Dokáže prepisovať chybné bootovacie sektory zálohami alebo vytvoriť nový bootovací sektor, ak záloha neexistuje.

TestDisk je schopný obnoviť zmazané súbory z viacerých súborových systémov vrátane FAT32, NTFS, EXT2/EXT3/EXT4 a HFS+ (macOS). Pri tomto procese prehľadáva disky, aby identifikoval súbory, ktoré boli zmazané, ale ešte neboli prepísané novými dátami.

Ako Testdisk funguje pri obnove zmazaných dát

Keď TestDisk začína proces obnovy, prvým krokom je skenovanie celého disku alebo partície. Nástroj hľadá neporušené časti súborových systémov, záznamy o súboroch v súborových tabuľkách a nezmazané klastre, ktoré by mohli obsahovať dáta.

Ak je cieľom obnoviť stratené partície, TestDisk analyzuje disk na základe štruktúry partičných tabuliek a porovnáva ich so záložnými kópiami. Dokáže automaticky zistiť stratené partície a obnoviť ich do pôvodného stavu, čím sa používateľ dostane k svojim dátam.

Pri obnove súborov TestDisk skenuje záznamy o zmazaných súboroch, ktoré sú stále dostupné v súborovej tabuľke (napr. MFT v NTFS alebo FAT tabuľka vo FAT32). Tieto záznamy obsahujú informácie o tom, kde sú súbory fyzicky umiestnené na disku. Ak tieto bloky neboli prepísané, TestDisk dokáže súbory obnoviť do ich pôvodného stavu.

V prípade, že záznamy sú poškodené alebo neúplné, TestDisk využíva „deep scan“ (hlbkové skenovanie), ktoré prehľadáva celý disk po zmazaných blokoch dát a pokúša sa zrekonštruovať súbory na základe vzorov a metadát.

Recuva

Recuva je bezplatný nástroj na obnovu zmazaných súborov, vyvinutý spoločnosťou Piriform, ktorá je známa aj ďalšími populárnymi programami ako CCleaner. Recuva je navrhnutá ako užívateľsky prívetivý nástroj, ktorý umožňuje jednoduchú obnovu zmazaných dát z rôznych úložných médií. Je dostupná pre operačný systém Windows a podporuje viacero súborových systémov.

Hlavné funkcie Recuvy

Hlavnou funkciou Recuvy je schopnosť obnoviť zmazané súbory z pevných diskov, USB kľúčov, pamäťových kariet, externých diskov a ďalších zariadení. Nástroj podporuje širokú škálu súborových formátov, vrátane dokumentov, obrázkov, hudobných súborov, videí a e-mailov.

Recuva podporuje obnovu dát z rôznych typov úložných médií a súborových systémov:

- NTFS, FAT32, exFAT pre Windows systémy.
- Schopnosť pracovať s úložnými zariadeniami, ktoré boli formátované alebo inak poškodené.

Recuva obsahuje funkciu Deep Scan, ktorá je schopná vykonávať hlbkovú analýzu úložného zariadenia a nájsť súbory, ktoré už boli zmazané pred dlhším časom alebo ktoré boli ťažšie

identifikovateľné pri rýchlom skenovaní. Tento režim prehľadáva disk sektor po sektore, aby našiel dáta, ktoré ešte neboli prepísané.

Okrem obnovy dát Recuva poskytuje aj funkciu secure delete (bezpečné mazanie), čo znamená, že môže bezpečne odstrániť súbory tak, že ich nie je možné znovu obnoviť. Táto funkcia využíva viaceré prepisy diskového priestoru, aby sa zabezpečilo, že pôvodné dáta sú nenávratne zničené.

Ako Recuva funguje pri obnove zmazaných dát

Keď je v Recuvy spustený proces obnovy, nástroj najskôr vykoná rýchle skenovanie, pri ktorom prehľadá záznamy v súborovom systéme (napríklad NTFS MFT alebo FAT tabuľky). Ak sú v týchto tabuľkách stále prítomné informácie o zmazaných súboroch, Recuva dokáže získať späť celý súbor vrátane jeho názvu, cesty a obsahu.

Ak rýchle skenovanie neodhalí žiadané súbory, Recuva prejde na hĺbkové skenovanie. Tento proces prehľadáva disk sektor po sektore, hľadá fragmenty dát, ktoré sú stále prítomné na úložnom zariadení. Hoci tento proces trvá dlhšie, má vyššiu úspešnosť pri obnove dát, ktoré boli zmazané už pred dlhšou dobou alebo po čiastočnom formátovaní disku.

Po dokončení skenovania Recuva zobrazí zoznam nájdených súborov spolu s informáciou o ich stave (teda či sú súbory v dobrom stave na obnovu, čiastočne poškodené alebo úplne prepísané). Používateľ si potom môže vybrať, ktoré súbory chce obnoviť, a Recuva ich obnoví do vybranej destinácie.

Recuva umožňuje používateľovi zamerať sa na konkrétne oblasti disku alebo priečinky, kde sa súbory pravdepodobne nachádzajú, čo šetrí čas pri skenovaní a zvyšuje šancu na úspešnú obnovu.

Photorec

PhotoRec je open-source softvér určený na obnovu zmazaných súborov, primárne multimediálnych, ako sú fotografie, videá a ďalšie typy súborov, z rôznych úložných zariadení. Vyvinutý bol spolu s nástrojom TestDisk spoločnosťou CGSecurity, a hoci sa primárne zameriava na obnovu fotografií, zvláda obnovu rôznych typov súborov z pevných diskov, USB kľúčov, pamäťových kariet a CD/DVD. Je známy svojou schopnosťou pracovať aj s poškodenými súborovými systémami a ponúka širokú podporu naprieč platformami.

Hlavné funkcie Photorecu

PhotoRec používa metódu obnovy založenú na signatúrach súborov, čo znamená, že nepracuje priamo s tabuľkami súborového systému, ale prehľadáva celé médium po

sektoroch a hľadá známe signatúry súborov. Tento prístup umožňuje obnovu súborov aj v prípadoch, keď je súborový systém poškodený alebo nečitateľný.

Aj keď je nástroj pomenovaný po obnove fotografií, podporuje viac ako 480 formátov súborov, vrátane obrázkov (JPEG, PNG, TIFF), videí (AVI, MP4, MOV), dokumentov (DOC, PDF), archívov (ZIP, RAR) a mnoho ďalších.

PhotoRec podporuje širokú škálu súborových systémov, vrátane FAT32, NTFS, ext2/ext3/ext4, HFS+, exFAT a mnoho ďalších. To znamená, že je schopný obnovovať súbory z rôznych typov zariadení a systémov.

Nástroj je špeciálne navrhnutý na prácu so súborovými systémami, ktoré sú poškodené alebo nečitateľné. Vďaka tomu je užitočný pri obnove dát z poškodených diskov alebo zariadení, ktoré operačný systém už nedokáže prečítať.

PhotoRec je navrhnutý tak, aby nikdy nezapisoval na disk, z ktorého obnovuje dáta. Všetky obnovené súbory sú ukladané na iné médium, čím sa minimalizuje riziko prepísania pôvodných dát.

Ako Photorec funguje pri obnove zmazaných dát

Na rozdiel od iných nástrojov, ktoré sa spoliehajú na súborové tabuľky (ako MFT v NTFS alebo FAT tabuľka), PhotoRec používa prístup na báze signatúr. To znamená, že nástroj prehľadáva disk sektor po sektore a hľadá známe signatúry súborov. Keď PhotoRec nájde známu signatúru, pokúsi sa obnoviť celý súbor. Tento prístup umožňuje obnovu dát aj v prípade, že je súborový systém úplne poškodený alebo stratený.

Ak bol disk formátovaný alebo súborový systém poškodený, PhotoRec môže stále obnoviť dáta, pretože nevyužíva informácie zo súborového systému. Tento prístup je veľmi užitočný pri náhlych formátovaniach alebo mechanickom poškodení disku.

PhotoRec obnovuje dáta tým, že ich ukladá na iné úložné médium (napr. iný disk alebo oddiel). Tento spôsob obnovy zabraňuje prepísaniu pôvodných dát, čo by mohlo znížiť šance na úspešnú obnovu ďalších súborov.

Testovanie

Predpríprava testovania

Pre účely testovania obnovy zmazaných súborov som pripravil komplexné testovacie prostredie zahŕňajúce rôzne scenáre, ktoré simulujú bežné situácie straty dát. Na začiatku som definoval základné testovacie podmienky a metodiku. Využil som voľne dostupnú stránku <https://file-examples.com/>, ktorá ponúka široké spektrum súborov rôznych formátov. Tieto súbory som použil na simuláciu konkrétnych prípadov, ako sú náhodné mazanie, korupcia súborov, formátovanie disku a prepisovanie dát.

Po stiahnutí testovacích súborov som ich umiestnil na testovací disk, ktorý bol následne pripravený na jednotlivé scenáre. Každý scenár som starostlivo naplánoval a zdokumentoval, aby som zaistil konzistentnosť a porovnateľnosť výsledkov.

Na testovanie som si stanovil štyri základné scenáre:

1. **Náhodné mazanie súborov** – simuloval som bežnú situáciu, keď sú súbory z disku neúmyselne odstránené. Tento scenár slúžil na overenie schopnosti nástrojov obnoviť dáta, ktoré sú fyzicky stále prítomné na disku, ale ich odkazy boli zmazané.
2. **Korupcia súborov** – v tomto scenári som zámerne poškodil vybrané súbory, aby som otestoval, či a do akej miery nástroje dokážu obnoviť dáta z neúplných alebo chybových záznamov.
3. **Formátovanie disku** – simuloval som rýchle aj plné formátovanie testovacieho disku, aby som zistil, ako nástroje reagujú na situácie, keď sú súborové tabuľky odstránené alebo prepísané.
4. **Prepisovanie dát na disku** – tento scenár predstavoval najnáročnejšiu situáciu, keď som po zmazaní súborov zámerne zapísal nové dáta na disk, aby som simuloval reálne používanie zariadenia po strate dát. Tento test mal overiť, do akej miery dokážu nástroje obnoviť pôvodné súbory aj po čiastočnom prepísaní dát.

Každý test som vykonával samostatne pre súborové systémy FAT32, NTFS a EXT4, aby som pokryl široké spektrum platforiem a spôsobov ukladania dát. Počas testovania som dôsledne zaznamenával všetky kroky a výsledky, vrátane úspešnosti obnovy, rýchlosti nástroja a jeho schopnosti detegovať jednotlivé typy problémov. Týmto som vytvoril pevný základ pre hodnotenie testovacích nástrojov v ďalších fázach projektu.

Name	Date modified	Type	Size
Audio	13/11/2024 02:18	File folder	
Dokumenty	13/11/2024 02:18	File folder	
Obrázky	13/11/2024 04:50	File folder	
Videa	13/11/2024 02:18	File folder	

Figure 1 Súborový systém použitý na testovanie

Testovanie v súborovom systéme FAT32

V rámci testovania som sa sústredil na súborový systém FAT32, ktorý patrí medzi najstaršie a stále široko používané súborové systémy. FAT32 je známy svojou jednoduchosťou, avšak má aj isté obmedzenia, najmä v správe fragmentovaných súborov a zabezpečení dát. Testovanie prebiehalo v štyroch scenároch – náhodné mazanie súborov, korupcia súborov, formátovanie disku a prepisovanie dát. Pri každom scenári som použil tri vybrané nástroje: Recuva, PhotoRec a TestDisk. Cieľom bolo vyhodnotiť, ako tieto nástroje zvládajú obnovu dát v rôznych podmienkach.

Náhodne mazanie súborov

V tomto scenári som odstránil niekoľko súborov rôznych formátov (.docx, .jpg, .txt) z testovacieho disku, pričom súbory neboli fyzicky prepísané. Cieľom bolo zistiť, ako jednotlivé nástroje zvládajú obnovu dát, ktoré sú stále fyzicky prítomné na disku, ale ich odkazy v súborovej tabuľke boli odstránené.

- **Recuva:** Tento nástroj bol veľmi úspešný pri obnove všetkých zmazaných súborov. Používateľsky prívetivé rozhranie umožnilo jednoduché nastavenie a rýchle skenovanie. Všetky obnovené súbory boli v perfektnom stave, bez akýchkoľvek chýb alebo poškodení. Okrem toho Recuva poskytuje možnosť hĺbkového skenovania (Deep Scan), ktoré som použil na overenie, či nejaké súbory neboli prehliadnuté. Táto funkcia potvrdila úplnú obnovu dát a ukázala, že nástroj je výborne optimalizovaný pre scenáre náhodného mazania.
- **PhotoRec:** PhotoRec takisto obnovil všetky zmazané súbory. Vzhľadom na to, že pracuje na báze signatúr súborov, nástroj dokázal nájsť aj niektoré súbory, ktoré neboli súčasťou aktuálneho testovania, ale predtým boli zmazané. Tento prístup je užitočný, ak používateľ potrebuje obnoviť staršie dáta. Obnova však nebola taká intuitívna ako pri Recuve, pretože PhotoRec nezachováva pôvodné názvy súborov ani ich adresárovú štruktúru, čo môže sťažiť identifikáciu obnovených dát.

- **TestDisk:** TestDisk exceloval v rýchlosti a precízności obnovy. Dokázal identifikovať všetky zmazané súbory a obnoviť ich do pôvodného stavu. Navyše, TestDisk identifikoval aj skryté a systémové súbory, ktoré iné nástroje prehliadli. Tento nástroj je mimoriadne výkonný a zároveň ponúka možnosti hĺbkového skenovania, ktoré odhalili aj staršie zmazané dáta. Jeho konzolové rozhranie však môže byť pre bežných používateľov menej intuitívne.

Korupcia súborov

Pre tento scenár som poškodil 30 % obsahu niekoľkých súborov, aby som simuloval častý problém, akým je poškodenie dát pri prenose alebo výpadku systému. Zameral som sa na obnovu formátov .docx a .jpg, pričom som sledoval, či sú nástroje schopné tieto dáta aspoň čiastočne rekonštruovať.

- **Recuva:** Recuva identifikovala poškodené súbory, ale nedokázala ich obnoviť. Aj pri použití hĺbkového skenovania nástroj nenašiel funkčné verzie poškodených súborov. Táto neschopnosť obnovy naznačuje, že Recuva nie je vhodná na obnovu dát z poškodených súborov.
- **PhotoRec:** PhotoRec rovnako nedokázal obnoviť poškodené súbory. Jeho signatúrny prístup našiel fragmenty súborov, ale výsledkom boli prázdne alebo nečitateľné súbory. Tento nástroj je navrhnutý primárne na obnovu stratených, nie poškodených dát.
- **TestDisk:** Podobne ako ostatné nástroje, aj TestDisk zlyhal pri obnove poškodených dát. Dokázal detegovať poškodené súbory, ale nedisponuje funkciami na opravu alebo rekonštrukciu poškodeného obsahu. Tento výsledok podčiarkuje obmedzenia FAT32 v prípade korupcie dát.

Formátovanie disku

Testoval som obnovu dát po rýchlom aj úplnom formátovaní disku. Rýchly formát vymazal súborovú tabuľku, no dátové klastre zostali fyzicky na disku, zatiaľ čo úplný formát ich prepísal nulami.

- **Recuva:** Pri rýchlom formáte Recuva obnovila všetky dáta bez akýchkoľvek problémov. Po úplnom formáte však nástroj nedokázal nájsť žiadne použiteľné dáta. To naznačuje, že Recuva je efektívna pri povrchových úpravách, ale nie pri hlbšej strate dát.
- **PhotoRec:** PhotoRec úspešne obnovil všetky súbory po rýchlom formáte. Pri úplnom formáte dokázal identifikovať niektoré fragmenty súborov, ale väčšina obnovených dát bola nečitateľná alebo nepoužiteľná. Tento výsledok naznačuje, že PhotoRec je lepší pri hlbšej analýze dát v porovnaní s Recuvou.

- **TestDisk:** Po rýchlom formáte TestDisk nielenže obnovil všetky dáta, ale identifikoval aj niektoré staršie súbory, ktoré neboli súčasťou aktuálneho testu. Po úplnom formáte však, podobne ako ostatné nástroje, nedokázal nájsť žiadne použiteľné dáta.

Prepisovanie dát na disku

V tomto scenári som po zmazaní súborov zámerne zapísal nové dáta na disk, aby som simuloval najnáročnejšiu situáciu obnovy dát.

- **Recuva:** Recuva dokázala obnoviť niektoré časti starších súborov, avšak väčšina dát bola poškodená alebo neúplná. Tento nástroj sa ukázal ako menej efektívny pri rekonštrukcii dát po ich prepísaní.
- **PhotoRec:** PhotoRec identifikoval niekoľko fragmentov starších súborov, ale obnovené dáta boli nekonzistentné a väčšina z nich bola nepoužiteľná. Jeho signatúrny prístup je v takýchto prípadoch obmedzený.
- **TestDisk:** TestDisk bol najúspešnejší pri identifikácii starších dát, ale ich obnova bola len čiastočná. Prepisovanie dát na disku značne komplikovalo proces obnovy, čo zdôrazňuje limity nástrojov aj systému FAT32.

Zhrnutie pre súborový systém FAT32

Testovanie ukázalo, že všetky tri nástroje majú svoje silné a slabé stránky. Recuva vynikla jednoduchosťou a rýchlosťou pri bežných scenároch, no zlyhala pri komplexnejších situáciách. PhotoRec sa osvedčil pri hĺbkovej analýze, ale jeho výsledky sú menej organizované. TestDisk ponúkol najväčší rozsah funkcií a najlepšiu obnovu dát, avšak vyžaduje pokročilejšie znalosti na použitie. Systém FAT32 ukázal svoje limity najmä pri poškodených a prepísaných dátach, kde bola obnova takmer nemožná.

Testovanie v súborovom systéme NTFS

Súborový systém NTFS (New Technology File System) je moderný a široko používaný, najmä v operačných systémoch Windows. V porovnaní s FAT32 ponúka pokročilé funkcie ako journaling, šifrovanie a lepšie zvládanie fragmentácie súborov, čo má priamy vplyv na proces obnovy dát. V rámci testovania som použil štyri rovnaké scenáre – náhodné mazanie, korupcia súborov, formátovanie disku a prepisovanie dát – pričom som sa zameral na efektivitu troch nástrojov: Recuva, PhotoRec a TestDisk.

Náhodné mazanie súborov

Pri tomto teste som odstránil viacero súborov rôznych formátov (.docx, .jpg, .txt) bez toho, aby boli fyzicky prepísané. V NTFS systém uchováva záznamy o súboroch v Master File Table (MFT), čo zjednodušuje ich identifikáciu.

- **Recuva:** Recuva dokázala obnoviť všetky zmazané súbory v neporušenom stave. Nástroj využil informácie z MFT na presné identifikovanie pôvodného miesta súborov, čo viedlo k rýchlej a presnej obnove. Používateľské rozhranie bolo opäť veľmi intuitívne a hĺbkové skenovanie preukázalo vynikajúce výsledky.
- **PhotoRec:** Tento nástroj pracoval opäť so svojím signatúrnym prístupom a dokázal obnoviť všetky zmazané súbory. Výhodou bolo, že PhotoRec našiel aj staršie dáta, ktoré neboli zahrnuté v aktuálnom testovaní, no nevýhodou bolo, že neobnovil pôvodné názvy ani adresárovú štruktúru súborov. Tento nedostatok môže byť problematický, ak je potrebné obnoviť veľký počet súborov.
- **TestDisk:** TestDisk bol najrýchlejší zo všetkých testovaných nástrojov. Využil údaje z MFT na presnú obnovu súborov, vrátane ich názvov a pôvodných adresárov. Okrem toho dokázal identifikovať aj skryté súbory a systémové dáta, ktoré ostatné nástroje prehliadli. Výsledky boli výborné, aj keď používanie nástroja vyžaduje určité znalosti o práci so súborovým systémom.

Korupcia súborov

Pri tomto scenári som poškodil 30 % obsahu vybraných súborov, aby som simuloval situácie, keď sú dáta čiastočne nečitateľné alebo chybné. Sledoval som, či nástroje dokážu takéto dáta obnoviť.

- **Recuva:** Recuva nedokázala obnoviť žiadne poškodené súbory. Aj keď nástroj identifikoval ich prítomnosť na disku, pokusy o obnovu viedli len k vytvoreniu prázdnych alebo nefunkčných súborov.
- **PhotoRec:** PhotoRec podobne zlyhal pri obnove poškodených súborov. Vzhľadom na svoj prístup založený na signatúrach dokázal nájsť len neúplné fragmenty dát, ktoré nebolo možné spojiť do funkčných súborov.
- **TestDisk:** Hoci TestDisk exceluje pri obnove zmazaných súborov, pri korupcii dát bol rovnako neúspešný. Nástroj nedokázal opraviť ani rekonštruovať poškodené časti súborov.

Formátovanie disku

V tomto teste som formátoval disk dvoma spôsobmi: rýchlym a úplným formátovaním. Pri rýchlom formáte zostávajú dáta na disku, avšak súborová tabuľka MFT je vymazaná. Úplný formát prepíše všetky dáta nulami.

- **Recuva:** Pri rýchlom formáte dokázala Recuva obnoviť všetky dáta v pôvodnom stave, čo potvrdzuje jej efektivitu pri prístupe k údajom uloženým v neporušených klastroch. Po úplnom formáte však nástroj nebol schopný obnoviť žiadne dáta.

- **PhotoRec:** PhotoRec obnovil všetky súbory po rýchlom formáte, pričom našiel aj niektoré fragmenty dát po úplnom formáte. Tieto fragmenty však boli nekompletné a nečitateľné. Nástroj ukázal vyššiu flexibilitu pri obnove dát ako Recuva, ale výsledky boli stále obmedzené.
- **TestDisk:** Pri rýchlom formáte TestDisk obnovil všetky dáta vrátane pôvodnej štruktúry adresárov. Po úplnom formáte bol rovnako neúspešný ako ostatné nástroje, pretože všetky dáta boli prepísané nulami. Jeho výkon pri rýchlom formáte však bol vynikajúci a preukázal schopnosť obnoviť aj dáta, ktoré iné nástroje nezistili.

Prepisovanie dát na disku

V poslednom scenári som po zmazaní súborov zapísal nové dáta na disk, aby som simuloval situáciu, keď sú pôvodné klastre prepísané novými údajmi. Tento scenár bol najnáročnejší.

- **Recuva:** Recuva dokázala obnoviť niekoľko fragmentov pôvodných dát, ale väčšina obnovených súborov bola neúplná alebo nečitateľná. Nástroj sa ukázal ako menej efektívny v prípadoch, keď došlo k prepisovaniu.
- **PhotoRec:** PhotoRec identifikoval niekoľko fragmentov starších dát, ktoré boli uložené mimo prepísaných klastrov, no väčšina obnovených súborov bola nepoužiteľná. Výsledky boli nekonzistentné a často zmätočné.
- **TestDisk:** TestDisk preukázal najvyššiu úspešnosť pri identifikácii starších dát. Napriek tomu, že mnoho dát bolo nenávratne stratených, nástroj dokázal obnoviť niektoré funkčné časti súborov, čo naznačuje jeho vyššiu schopnosť pracovať s fragmentovanými údajmi.

Zhrnutie pre súborový systém NTFS

Testovanie v NTFS potvrdilo, že tento súborový systém ponúka vynikajúce možnosti obnovy dát, pokiaľ nedôjde k ich fyzickému prepísaniu. Recuva bola efektívna pri jednoduchých scenároch, ale mala problémy pri komplexnejších prípadoch. PhotoRec vynikol svojím signatúrnym prístupom a schopnosťou nájsť staršie dáta, avšak nezachovával názvy ani štruktúru súborov. TestDisk sa ukázal ako najflexibilnejší a najvýkonnejší nástroj, schopný obnoviť dáta aj v náročných podmienkach. NTFS vynikal pri rýchlom formátovaní a náhodnom mazaní, no obnovu koruptovaných alebo prepísaných dát nezvládal o nič lepšie ako FAT32.

Testovanie v súborovom systéme EXT4

EXT4 (Fourth Extended File System) je moderný súborový systém, používaný predovšetkým na Linuxových platformách. Ponúka pokročilé funkcie ako extents, ktoré znižujú fragmentáciu, a delayed allocation, ktorá zlepšuje výkon. Keďže Windows natívne

nepodporuje prácu so súborovým systémom EXT4, musel som nainštalovať nástroj *DiskGenius*, ktorý mi umožnil formátovať a manipulovať so súbormi na disku v EXT4 prostredí. Testovanie v EXT4 zahŕňalo štyri scenáre: náhodné mazanie, korupcia súborov, formátovanie disku a prepisovanie dát, pričom som opäť použil nástroje Recuva, PhotoRec a TestDisk.

Náhodne mazanie súborov

Pri tomto scenári som vymazal niekoľko testovacích súborov rôznych formátov. EXT4 uchováva dáta v blokoch nazývaných extents, čo teoreticky znižuje fragmentáciu a zjednodušuje proces obnovy.

- **Recuva:** Recuva dokázala identifikovať niektoré zmazané súbory, avšak výsledky neboli konzistentné. Zmazané súbory často obsahovali duplicitné záznamy alebo mali nezvyčajné veľkosti a dátumy úprav. Tento nástroj očividne nie je optimalizovaný na prácu so systémom EXT4, čo limitovalo jeho efektivitu.
- **PhotoRec:** PhotoRec exceloval pri identifikácii a obnove zmazaných súborov. Všetky zmazané dáta boli obnovené, pričom nástroj dokázal nájsť aj súbory, ktoré boli zmazané pred začiatkom aktuálneho testovania. Nevýhodou však bolo, že obnovené súbory nemali pôvodné názvy ani adresárovú štruktúru.
- **TestDisk:** TestDisk si počínal výborne, obnovil všetky zmazané súbory vrátane ich pôvodných názvov a štruktúry adresárov. Nástroj bol rýchly a precízny, čo zdôrazňuje jeho silné stránky pri práci so systémom EXT4.

Korupcia súborov

Pre tento test som poškodil 30 % obsahu vybraných súborov, aby som overil schopnosti nástrojov obnoviť poškodené dáta. EXT4 má robustné mechanizmy pre prácu s metadátami, no to, či pomáhajú pri obnove koruptovaných dát, bolo predmetom testovania.

- **Recuva:** Nástroj nedokázal obnoviť žiadne poškodené súbory. Aj keď ich identifikoval, všetky pokusy o obnovu viedli k prázdny alebo nefunkčným súborom.
- **PhotoRec:** PhotoRec rovnako nepreukázal schopnosť obnovy poškodených dát. Identifikoval len fragmenty, ktoré však boli nečitateľné alebo neúplné.
- **TestDisk:** Hoci TestDisk vykonal dôkladnú analýzu, nebol schopný obnoviť poškodené dáta. Korupcia 30 % súborov sa ukázala ako príliš veľká pre všetky testované nástroje, čo naznačuje obmedzené možnosti obnovy poškodených dát v EXT4.

Formátovanie disku

V tomto scenári som testoval rýchle aj úplné formátovanie disku. Rýchly formát vymazal metadáta, zatiaľ čo úplný formát zničil všetky dáta na disku.

- **Recuva:** Po rýchlom formáte nástroj našiel viacero duplicitných súborov a niektoré z nich obnovil do pôvodného stavu. Po úplnom formáte však nebol schopný nájsť žiadne použiteľné dáta. Táto obmedzená efektivita naznačuje, že Recuva nie je ideálna na obnovu v EXT4.
- **PhotoRec:** PhotoRec úspešne obnovil všetky dáta po rýchlom formáte. Dokázal identifikovať aj niektoré fragmenty dát po úplnom formáte, ale tieto neboli použiteľné. Jeho schopnosť pracovať na nízkej úrovni mu poskytuje výhodu v situáciách, keď sú dáta ešte fyzicky prítomné na disku.
- **TestDisk:** TestDisk dokázal obnoviť všetky súbory po rýchlom formáte vrátane ich názvov a štruktúry adresárov. Po úplnom formáte však, podobne ako ostatné nástroje, nedokázal obnoviť žiadne dáta. Tento výsledok zdôrazňuje, že EXT4 má obmedzené možnosti obnovy po úplnom vymazaní.

Prepisovanie dát na disku

Pre tento test som zámerne zapísal nové dáta na disk po vymazaní pôvodných súborov, aby som simuloval najnáročnejší scenár.

- **Recuva:** Nástroj našiel niekoľko fragmentov starších dát, ale výsledky boli nekonzistentné. Väčšina obnovených súborov bola poškodená alebo neúplná.
- **PhotoRec:** PhotoRec identifikoval niekoľko fragmentov starších dát, ktoré neboli prepísané novými údajmi. Väčšina obnovených súborov však bola nepoužiteľná, čo poukazuje na limity tohto nástroja pri prepisovaní dát.
- **TestDisk:** TestDisk bol opäť najefektívnejší pri identifikácii starších dát, ale aj jeho schopnosti boli obmedzené. Prepisovanie dát na disku značne komplikovalo obnovu a väčšina dát bola nenávratne stratená.

Zhrnutie pre súborový systém EXT4

Testovanie v EXT4 ukázalo, že tento súborový systém poskytuje pokročilé možnosti správy dát, avšak obnova dát po poškodení alebo prepisovaní zostáva náročná.

- Recuva bola najúčinnnejšia pri jednoduchších scenároch, ako je náhodné mazanie a rýchly formát, ale jej výkon bol obmedzený v zložitejších prípadoch.
- PhotoRec exceloval pri hĺbkových analýzách a našiel staršie dáta, no obnovené súbory nemali názvy ani adresárovú štruktúru.

- TestDisk sa ukázal ako najlepší nástroj na prácu v EXT4, najmä pri obnove dát po náhodnom mazaní a rýchlom formáte. Jeho schopnosť zachovať pôvodné názvy a štruktúru súborov z neho robí ideálny nástroj pre tento súborový systém.

Nainštalovanie nástroja *DiskGenius* bolo nevyhnutné na manipuláciu s EXT4 v prostredí Windows, pretože tento systém nie je natívne podporovaný. Tento krok umožnil úspešnú realizáciu testovania, aj keď práca s EXT4 na Windows platforme je o niečo náročnejšia než s inými súborovými systémami.

Záver a hodnotenie

V rámci projektu som analyzoval a testoval tri najčastejšie používané súborové systémy – FAT32, NTFS a EXT4 – a vyhodnotil schopnosti troch nástrojov na obnovu dát: Recuva, PhotoRec a TestDisk. Každý z týchto systémov a nástrojov má svoje výhody, nevýhody a špecifické prípady použitia, pričom výsledky testovania ponúkajú jasný obraz o ich efektívnosti v rôznych situáciách.

Súborové systémy

FAT32 je jednoduchý a široko kompatibilný, no trpí obmedzeniami pri práci s veľkými súbormi a fragmentáciou. Obnova dát je v tomto systéme pomerne jednoduchá, pokiaľ nedošlo k ich prepísaniu, avšak prepis a korupcia dát robia obnovu takmer nemožnou.

NTFS je pokročilý systém s robustnými funkciami ako journaling a efektívnejšou správou fragmentovaných dát. Obnova je často úspešná, najmä v scenároch náhodného mazania alebo rýchleho formátovania, ale pri poškodení alebo prepisovaní dát sú výsledky porovnateľné s FAT32.

EXT4 je moderný a výkonný systém, ktorý sa používa najmä v Linuxových prostrediach. Napriek výhodám, ako je zníženie fragmentácie vďaka extents, obnova dát zostáva výzvou v prípade poškodenia alebo prepísania. Na Windows platforme bolo potrebné použiť nástroj DiskGenius na prácu s týmto systémom.

Nástroje na obnovu dát

Recuva je užívateľsky najprívetivejší nástroj s veľmi dobrými výsledkami pri jednoduchších scenároch, ako je náhodné mazanie alebo rýchly formát. Jeho výkon sa však zhoršuje pri zložitejších situáciách, ako je korupcia alebo prepisovanie dát, a nebol optimalizovaný na prácu s EXT4.

PhotoRec zase vyniká svojím signatúrnym prístupom, ktorý umožňuje obnovu aj zo zničených súborových systémov. Jeho nevýhodou je však nedostatok organizácie v obnovených dátach, pretože nezachováva názvy ani štruktúru priečinkov. Ukázal dobré výsledky najmä pri náročných testoch s FAT32 a EXT4.

TestDisk je ale najflexibilnejší a najrýchlejší nástroj v testovaní. Jeho schopnosť obnoviť dáta vrátane pôvodnej štruktúry priečinkov a názvov súborov ho robí ideálnym pre pokročilých používateľov. Najlepšie si počíнал v scenároch s náhodným mazáním a rýchlym formátovaním vo všetkých súborových systémoch.

Celkové hodnotenie

Každý z testovaných nástrojov má svoje špecifické silné stránky:

- Recuva je najvhodnejšia pre bežných používateľov v jednoduchších situáciách.
- PhotoRec je ideálny na hlbšiu analýzu a obnovu z poškodených alebo nepodporovaných systémov.
- TestDisk je výborný pre pokročilé prípady obnovy a tam, kde je potrebná rekonštrukcia štruktúry súborov.

Kritérium	Recuva	PhotoRec	TestDisk
Úspešnosť	Vysoká pri základných scenároch, obmedzená pri zložitejších prípadoch	Veľmi vysoká pri hĺbkovom skenovaní, chýba štruktúra	Najvyššia zo všetkých nástrojov
Rýchlosť	Rýchla pri základnej obnove, pomalšia pri hĺbkovom skenovaní	Stredná, závisí od veľkosti dát	Rýchla pri štruktúrovanej obnove
Užívateľská skúsenosť	Užívateľsky prívetivé rozhranie	Základné, konzolové rozhranie	Pokročilé, menej intuitívne
Dostupnosť funkcií	Stredná, chýbajú pokročilé možnosti obnovy	Rozsiahla podpora formátov	Komplexné možnosti obnovy
Prehľadnosť	Veľmi prehľadné používateľské rozhranie	Stredná, bez zachovania štruktúry súborov	Dobré pre pokročilých používateľov
Jednoduchosť použitia	Extrémne jednoduché použitie	Náročné pre začiatočníkov	Vyžaduje technické znalosti

Table 1 Hodnotenie nástrojov

Prílohy

Príkladám obrázky z testovania, ktoré sa nehodili na priame použitie v texte, ale považujem ich za dôležité a chcem ich dodatočne prezentovať.

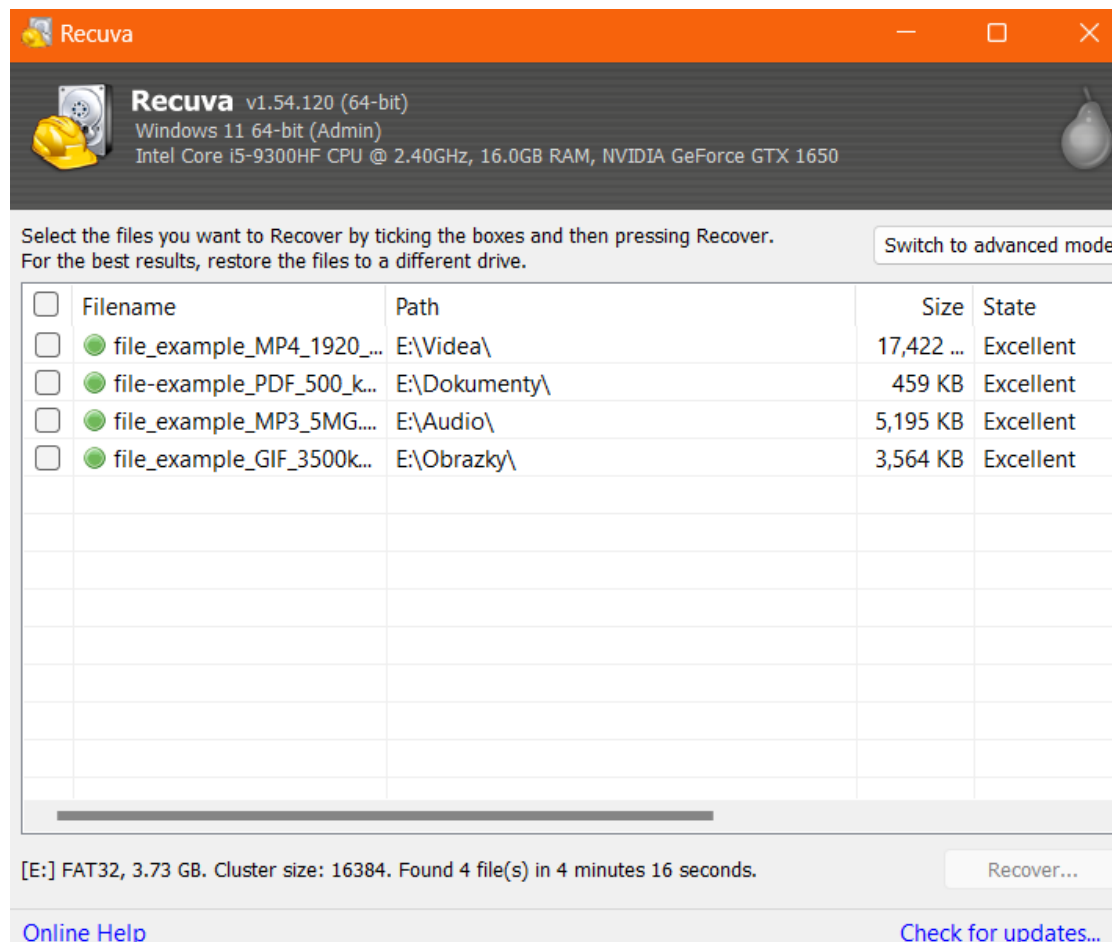
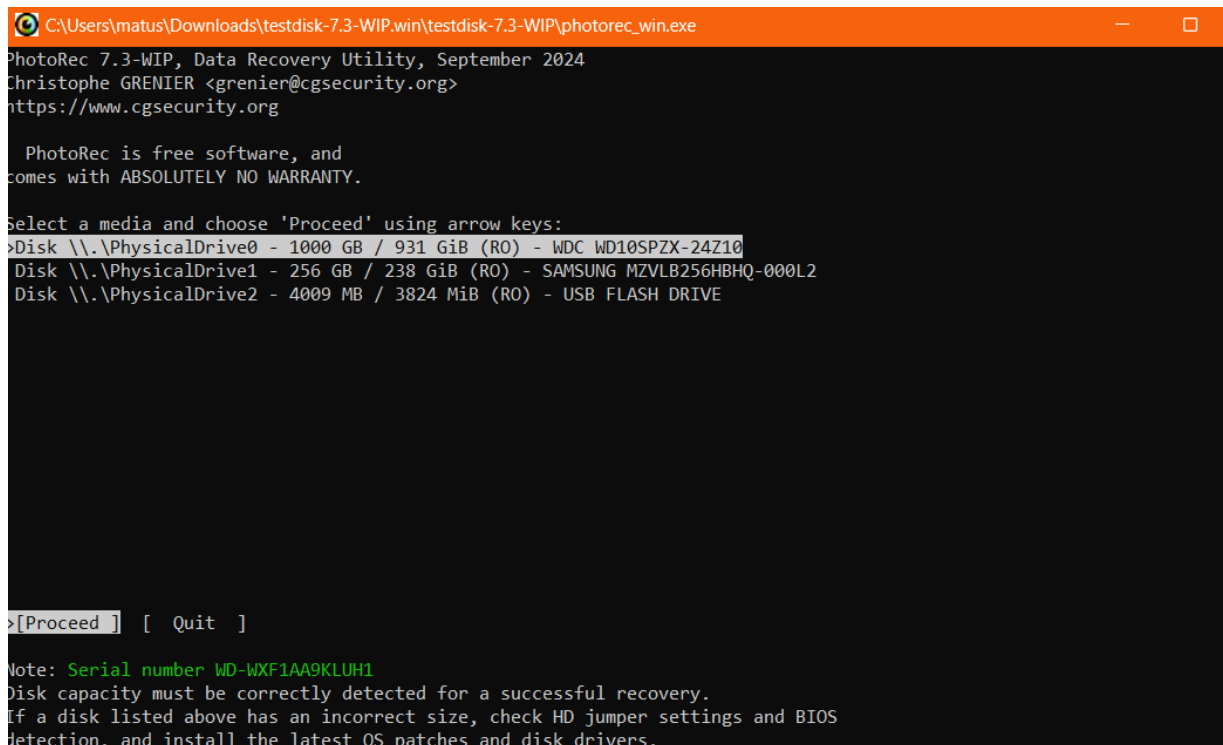


Figure 2 Používateľské rozhranie Recuvy, po úspešnej obnove zmazaných súborov



```
C:\Users\matus\Downloads\testdisk-7.3-WIP.win\testdisk-7.3-WIP\photorec_win.exe
PhotoRec 7.3-WIP, Data Recovery Utility, September 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

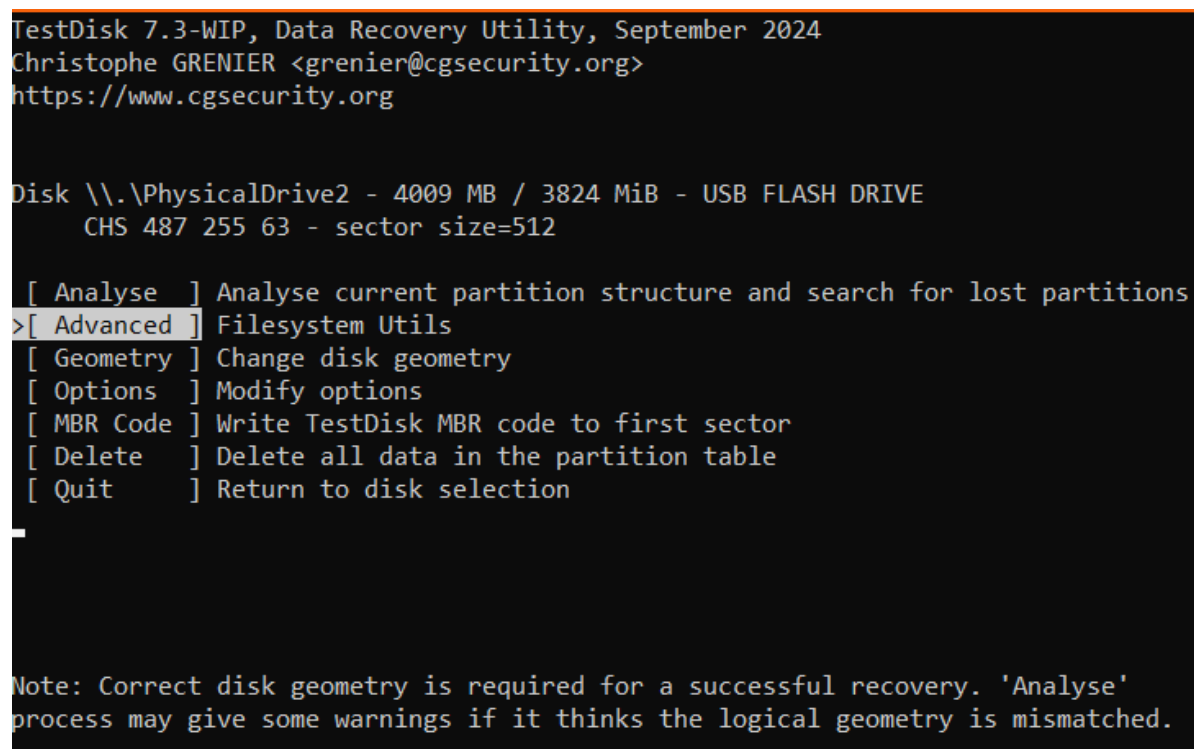
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:
>Disk \\.\PhysicalDrive0 - 1000 GB / 931 GiB (R0) - WDC WD10SPZX-24Z10
Disk \\.\PhysicalDrive1 - 256 GB / 238 GiB (R0) - SAMSUNG MZVLB256HBHQ-000L2
Disk \\.\PhysicalDrive2 - 4009 MB / 3824 MiB (R0) - USB FLASH DRIVE

>[Proceed] [Quit]

Note: Serial number WD-WXF1AA9KLUH1
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

Figure 3 Používateľské rozhranie PhotoRec



```
TestDisk 7.3-WIP, Data Recovery Utility, September 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive2 - 4009 MB / 3824 MiB - USB FLASH DRIVE
CHS 487 255 63 - sector size=512

[Analyse] Analyse current partition structure and search for lost partitions
>[Advanced] Filesystem Utils
[Geometry] Change disk geometry
[Options] Modify options
[MBR Code] Write TestDisk MBR code to first sector
[Delete] Delete all data in the partition table
[Quit] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Figure 4 Používateľské rozhranie TestDisku

```

TestDisk 7.3-WIP, Data Recovery Utility, September 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
 1 P HPFS - NTFS          0 128 1 487 125 22 7823488 [USB DISK]
Deleted files

No deleted file found.

Use q to quit

```

Figure 5 Neúspešná obnova formátovaných súborov v TestDisku

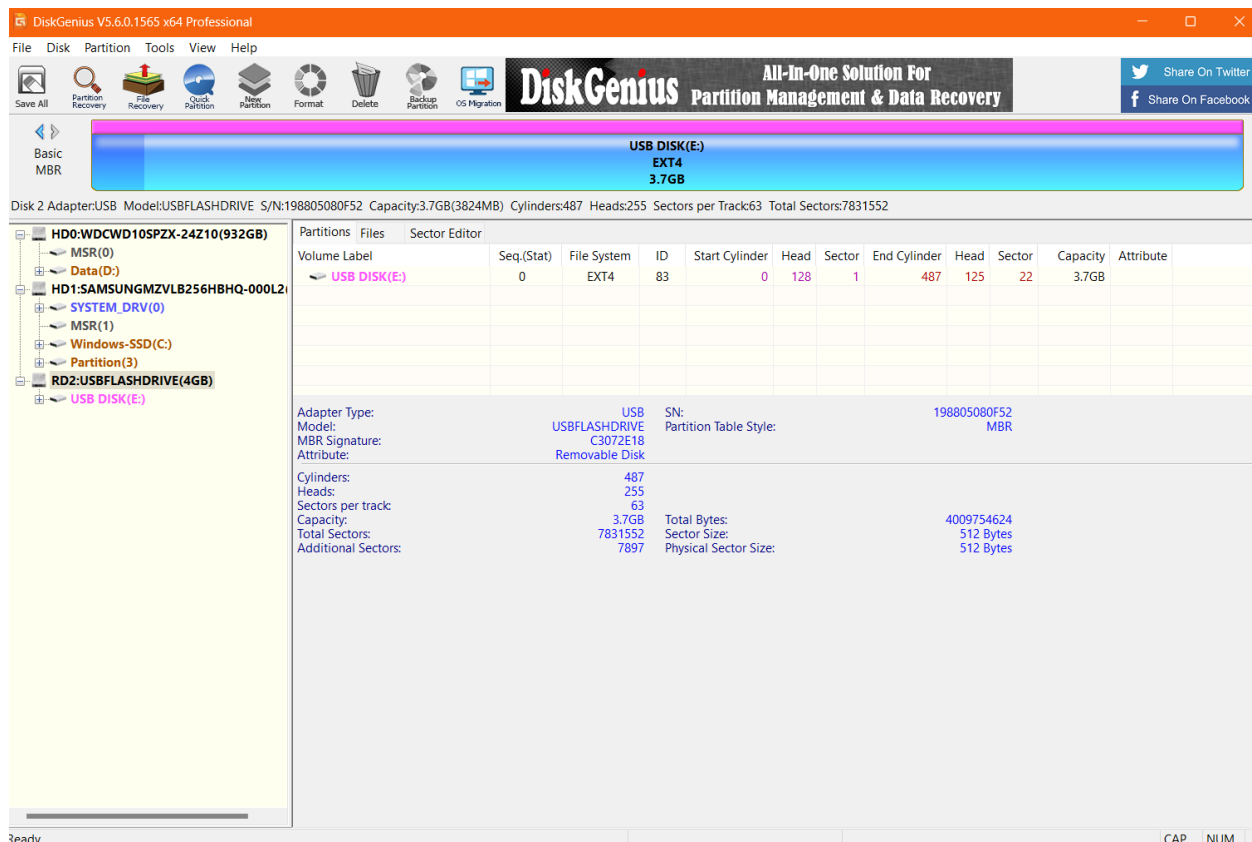


Figure 6 Používateľské rozhranie DiskGenius

Zdroje

<https://answers.microsoft.com/en-us/windows/forum/all/what-is-the-maximum-file-size-fat-fat32-ntfs-file/1663db6b-490e-4021-9e36-f7a6976ac0c0>

https://en.wikipedia.org/wiki/File_Allocation_Table

<https://www.file-recovery.com/recovery-NTFS-data-recoverability-and-integrity.htm>

<https://en.wikipedia.org/wiki/NTFS>

<https://wiki.archlinux.org/title/Ext4>

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/storage_administration_guide/ch-ext4#ext4creating

<https://en.wikipedia.org/wiki/TestDisk>

<https://www.cgsecurity.org/wiki/TestDisk>

<https://en.wikipedia.org/wiki/Recuva>

https://support.ccleaner.com/s/article/how-does-recuva-works?language=en_US

<https://en.wikipedia.org/wiki/PhotoRec>

<https://superuser.com/questions/1193468/how-the-photorec-works-internally-and-how-to-use-it-in-ubuntu14-04>

<https://file-examples.com/>

<https://www.diskgenius.com/>