

Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

Volne šíritelné nástroje na obnovu zmazaných súborov

PRINCÍPY INFORMAČNEJ BEZPEČNOSTI

Marek Čederle

`cederlem@stuba.sk`

Obsah

1 Specifikácia projektu	2
1.1 Progress report č.1	3
1.2 Progress report č.2	3
1.3 Ciele projektu	3
2 Súborové systémy	3
2.1 FAT - File Allocation Table	3
2.1.1 FAT32	4
2.1.2 Štruktúra FAT a FAT32	4
2.1.3 exFAT - Extensible File Allocation Table	5
2.1.4 Štruktúra exFAT	5
2.1.5 Výhody a nevýhody FAT32 a exFAT	7
2.2 NTFS - New Technology File System	7
2.2.1 Štruktúra NTFS	8
2.2.2 Bezpečnosť NTFS	9
2.2.3 Výhody a nevýhody NTFS	9
2.3 ext - Extended File System	9
2.3.1 ext4	10
2.3.2 Štruktúra ext4	10
2.3.3 Výhody a nevýhody ext4	12
3 Nástroje na obnovu údajov	12
3.1 Testdisk	13
4 Experimentovanie s nástrojom testdisk	13
4.1 Zmazanie a obnova súborov	15
4.2 Zapísanie na miesto zmazaného súboru	22
4.3 Zmazanie a obnova partície	23
5 Výsledky experimentov	25
5.1 Zmazanie súborov	25
5.2 Prepísanie zmazaných súborov	26
5.3 Zmazanie partície	26

6	Správne zmažanie dát a formátovanie disku	27
7	Záver	27
8	Poznatky zapracovať	27

1 Špecifikácia projektu

V mojom projekte sa budem venovať analýze súborových systémov pre operačné systémy Windows a GNU+Linux. Bude sa jednať o súborové systémy typu NTFS a ext ale spomeniem aj dodnes veľmi používané FAT32 a exFAT ktoré sa používajú na prenosných médiách. Každý súborový systém by som chcel opísť s tým, že uvediem jeho výhody a nevýhody prípadné porovnanie s ďalšími spomenutými súborovými systémami.

Budem sa zaoberať aj tým, ako správne naformátovať disk (prepísať ho náhodnými dátami alebo samými nulami) aby pri jeho predaji sa z bezpečnostných dôvodov nedalo zistiť čo sa na ňom pred tým nachádzalo. Je to z dôvodu že pri mazaní dát z disku sa vlastne tieto dátá reálne nemažú. Dáta na disku zostanú, len sa z tabuľky záznamov zahodí záznam kde sa súbor nachádza a potom keď sa zapisuje na disk tak operačný systém vie, že môže na toto miesto zapisovať.

Taktiež sa budem zaoberať analýzou nástroja na obnovu zmazených súborov s názvom testdisk. Vysvetlím, prečo som si vybral práve tento nástroj. S týmto nástrojom budem následne experimentovať. Experimenty budú spočívať v tom, že si naformátujem disk a vytvorím na ňom nejaké partície podľa typu daného súborového systému. Následne naň uložím rôzne typy súborov. Budú sa tam nachádzať fotky, textové súbory, archívy, atď. Potom vymažem nejaké z týchto súborov, ale na disk ďalej nič nezapíšem, aby sa nezačali prepisovať dané miesta na disku inými súbormi. Následne vyskúšam nástroj na obnovu zmazených súborov (testdisk) či zvládne tieto súbory obnoviť. Tento experiment zopakujem s tým, že po zmazení ďalších súborov zapíšem na disk zase nové súbory a vyskúšam použiť nástroj na obnovu či dokáže aj po takejto akcii obnoviť súbory. Ďalší experiment bude spočívať v zmazení celej partície a jej následnej obnove týmto nástrojom. V neposlednom rade ukážem, že po správnom formátovaní disku sa nebudú dať dátá obnoviť. Na záver budem prezentovať výsledky experimentov.

1.1 Progress report č.1

V prvom progress reporte vypracujem teoretickú časť, ktorú som na začiatku uviedol. To znamená popísanie rôznych typov súborových systémov a nástrojov na obnovu súborov. V neposlednom rade uvediem ako z bezpečnostného hľadiska správne “zmazať” súbory na disku respektíve ako ho naformátovať tak, aby sa z neho minulé dátá nedali prečítať.

1.2 Progress report č.2

V tomto progress reporte sa budem zameriavať na praktickú/experimentálnu časť. To znamená, že sa pokúsim vykonať všetky vyššie spomenuté experimenty. Na záver budem pracovať na celkovej úprave finálneho dokumentu.

1.3 Ciele projektu

Cieľom tohto projektu je získať informácie z oblasti súborových systémov a vykonať rôzne experimenty s nástrojmi na obnovu údajov. Keďže sa jedná o predmet Princípy informačnej bezpečnosti, tak cieľom je poukázať na dopady neformátovania respektíve neefektívneho “ničenia” súborov na bezpečnosť.

2 Súborové systémy

Súborový systém je metóda a dátová štruktúra, ktorú operačný systém používa na riadenie spôsobu ukladania a načítavania dát. Bez súborového systému by dátá umiestnené na pamäťovom médiu boli jedným veľkým zväzkom dát bez možnosti určiť, kde končí jeden súbor a začína ďalší, alebo kde sa nachádza, keď je potrebné ho načítať. Rozdelením dát na časti a pomenovaním každej časti sa dátá ľahko izolujú a identifikujú. Každá skupina dát sa nazýva súbor.

2.1 FAT - File Allocation Table

FAT je súborový systém vyvinutý pre osobné počítače. Pôvodne vyvinutý v roku 1977 na použitie na disketách, neskôr bol prispôsobený na použitie na pevných diskoch a iných zariadeniach. Často je z dôvodov kompatibility podporovaný súčasnými operačnými systémami pre osobné počítače a mnohými mobilnými zariadeniami a “embed” systémami. FAT ako taký je už v

dnešnej dobe nepoužívaný, ale jeho odnože (FAT32, exFAT) sa doteraz používajú napríklad v prenosných médiách ako USB kľúče, SD karty a podobne.

2.1.1 FAT32

Najpokročilejšia verzia súborového systému FAT je FAT32. S FAT32 sa Microsoft snažil prekonáť obmedzenia FAT16 a prispôsobiť sa väčším možným partíciám. Existuje už od Windowsu 95 a naďalej zostáva populárny, pretože je vysoko kompatibilný s väčšinou operačných systémov (GNU+Linux, MAC) a prenosných zariadení. FAT32 podporuje súbory do 4 GB a partície s maximálnou veľkosťou 2 TB. Používa sa prevažne pre EFI partície a prenosné médiá s kapacitou do 32GB.

2.1.2 Štruktúra FAT a FAT32

Novo naformátovaný disk s FAT vyzerá nasledovne:



FAT File System Structure



FAT32 File System Structure

EaseUS®
Make your life easy!

Obr. 1: Štruktúra súborového systému FAT a FAT32
Zdroj: <https://www.easeus.com/diskmanager/file-system.html>

- Reserved Area
 - Obsahuje boot sector, BPB (BIOS Parameter Block) a celkovo informácie potrebné pre bootovanie a súborový systém.
- 1st FAT Area
 - FAT tabuľka obsahujúca informácie o súboroch a ich umiestnení na disku.
- 2nd FAT Area
 - Obsahuje kópiu FAT tabuľky.
- Boot Directory
 - Niekoľko súborov, ktoré sú súčasťou súborového systému, aležia v rámci adresára.
 - Niekedy sa nazýva aj Root Directory. Používa sa iba v derivátoch FAT12 a FAT16.
 - Obsahuje informácie o súboroch, ktoré sa nachádzajú priamo v koreňovom adresári.
- Data Area
 - Obsahuje samotné dátumy súborov.

2.1.3 exFAT - Extensible File Allocation Table

exFAT je súborový systém predstavený spoločnosťou Microsoft v roku 2006 a optimalizovaný pre flash pamäte, ako sú USB flash disky a SD karty. exFAT bol proprietárny do 28. augusta 2019, kedy Microsoft zverejnil jeho špecifikáciu. Microsoft však stále vlastní patenty na niekoľko častí svojho dizajnu. To spôsobilo rozšírenie jeho podpory medzi rôzne operačné systémy.

exFAT možno použiť tam, kde NTFS nie je vhodným riešením (kvôli vysokej rézii¹), ale kde je potrebná podpora súborov väčších ako 4 GB. Podporuje rádovo väčšiu veľkosť súborov ako FAT32 (ExaByty).

exFAT bol prijatý SD Association ako predvolený súborový systém pre karty SDXC väčšie ako 32 GB.

Windows 8 a novšie verzie natívne podporujú bootovanie z exFAT.

2.1.4 Štruktúra exFAT

Novo naformátovaný disk s exFAT vyzerá nasledovne:

¹angl. overhead



exFAT File System Structure

EaseUS®
Make your life easy!

Obr. 2: Štruktúra súborového systému exFAT
Zdroj: <https://www.easeus.com/diskmanager/file-system.html>

- Boot Region
 - Main Boot Region
 - * Informácie potrebné pre bootovanie.
 - Backup Boot Region
 - * Záloha Main Boot Region.
- FAT Region
 - FAT Alignment
 - * FAT offset a veľkosť.
 - 1st FAT
 - * FAT tabuľka obsahujúca informácie o súboroch a ich umiestnení na disku.
 - 2nd FAT
 - * Záloha FAT tabuľky.
- Data Region
 - Cluster Heap Alignment
 - * Cluster heap offset a veľkosť.
 - Cluster Heap
 - * Obsahuje samotné dátá súborov.
 - Excess Space
 - * Zvyšok priestoru na disku.

2.1.5 Výhody a nevýhody FAT32 a exFAT

FAT32	
Výhody	Nevýhody
Vysoko kompatibilný s rôznymi operačnými systémami.	Nedokáže uložiť súbor, ktorý je väčší ako 4GB.
Je kompatibilný s väčšinou prenosných úložných zariadení.	Nemá natívne šifrovanie súborov a chýbajú mu prístupové povolenia prítomné v moderných súborových systémoch.
	FAT32 je pomalší na čítanie a zápis dát v porovnaní s modernými súborovými systémami.

Tabuľka 1: Výhody a nevýhody súborového systému FAT32

Zdroj: <https://superops.com/ntfs-vs-fat32>

exFAT	
Výhody	Nevýhody
Podporuje súbory väčšie ako 4GB.	Absencia žurnálovania a kompresie dát.
Je predvoleným systémom na SD kartách s vysokou kapacitou	Nemá podporu pre staršie operačné systémy bez špeciálnych ovladačov.
Veľkosť partície je v podstate neobmedzená.	Nemá natívnu podporu pre šifrovanie dát.
Efektívnejší ako FAT32.	Nie je efektívnejší ako NTFS alebo ext.
Podpora všetkých majoritných operačných systémov.	Nie je vhodný pre viac-používateľské aplikácie z dôvodu vyšej fragmentácie.

Tabuľka 2: Výhody a nevýhody súborového systému exFAT

Zdroj: <https://www.profolus.com/topics/exfat-advantages-disadvantages-extensible-fat/>

2.2 NTFS - New Technology File System

NTFS je proprietárny súborový systém vytvorený spoločnosťou Microsoft. Bol uvedený s vtedy novým operačným systémom Windows NT² v roku 1993. Vtedy nahradil dovtedy veľmi používaný súborový systém FAT. NTFS je predovšetkým určený pre pevné disky HDD³ a neskôr aj pre SSD⁴. Je však možné ho použiť aj na prenosové média typu USB kľúč a podobne.

Súborový systém NTFS prináša kombináciu vyšej rýchlosťi, väčšej spoľahlivosti a kompatibility oproti súborovému systému FAT, ktorý bol jeho predchodom v ére operačného systému MS DOS. Natívne podporuje šifrovanie a kompresiu súborov. Podporuje aj veľmi veľké súbory a partície.

Ide o žurnálový súborový systém, čo znamená, že všetky zmeny na disku sú zaznamenané v tzv. žurnáli. V prípade výpadku napájania alebo zlyhania systému je možné rýchlo obnoviť

²New Technology

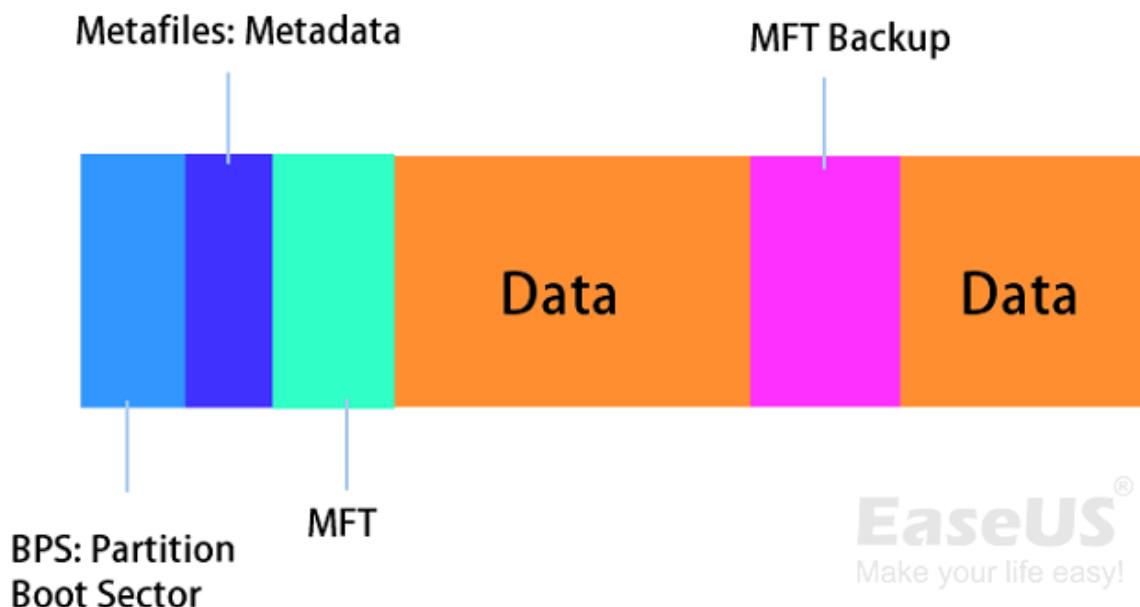
³Hard Disk Drive

⁴Solid State Drive

dáta na disku.

2.2.1 Štruktúra NTFS

Novo naformátovaný disk s NTFS vyzerá nasledovne:



Obr. 3: Štruktúra súborového systému NTFS
Zdroj: <https://www.easeus.com/diskmanager/file-system.html>

- Partition Boot Sector
 - Obsahuje informácie potrebné pre bootovanie. Primárne sa jedná o BootStrap čo je vlastne malý program, ktorý ma za úlohu načítať operačný systém do pamäte.
- Metadata
 - Pomáhajú definovať a organizovať súborový systém, zálohovať kritické údaje súborového systému.
- Master File Table (MFT)
 - Obsahuje záznamy o všetkých súboroch a adresároch na disku. Je to v podstate ekvivalent FAT tabuľky.
- Data
 - Obsahuje samotné dáta súborov.
- MFT Backup
 - Obsahuje zálohu MFT tabuľky.

2.2.2 Bezpečnosť NTFS

Ako som vyššie spomenul tak NTFS natívne podporuje šifrovanie súborov, priečinkov ale aj celých partícii. Súborový systém NTFS umožňuje nastaviť povolenia na prístup k niektorým lokálnym súborom a priečinkom. Inými slovami, dôverný súbor môžete nastaviť tak, aby bol pre niektorých iných používateľov nedostupný. Táto metóda sa nazýva riadenie úrovne prístupu (ACL).

2.2.3 Výhody a nevýhody NTFS

Výhody	Nevýhody
Podporuje veľmi veľké súbory a nemá takmer žiadne reálne obmedzenie veľkosti oddielu.	Má uzatvorený zdrojový kód.
Poskytuje vylepšené zabezpečenie údajov pomocou funkcií riadenia úrovne prístupu a náhľadu šifrovania.	Mac OS dokáže čítať jednotky naformátované v systéme NTFS, ale na systém NTFS je možné zapisovať iba prostredníctvom softvéru tretej strany.
Podporuje automatickú kompresiu súborov, čo umožňuje rýchlejší prenos súborov a väčší úložný priestor na disku.	Prenosné zariadenia, ako sú smartfóny so systémom Android a digitálne fotoaparáty, ho nepodporujú.
Umožňuje diskové kvóty, ktoré firmám poskytujú väčšiu kontrolu nad úložným priestorom.	Kompatibilita so systémami založenými na GNU+Linux súčasne existuje ale iba kvôli vôlej softvérových inžinierov urobiť ovladače vďaka reverznému inžinierstvu.
Umožňuje používateľom sledovať pridané, upravené alebo odstránené súbory na disku.	
Zameriava na konzistenciu súborového systému, takže v prípade výpadku napájania alebo zlyhania systému môžete rýchlo obnoviť svoje údaje.	

Tabuľka 3: Výhody a nevýhody súborového systému NTFS

Zdroj: <https://superops.com/ntfs-vs-fat32>

2.3 ext - Extended File System

ext bol implementovaný v apríli 1992 ako prvý súborový systém vytvorený špeciálne pre jadro Linuxu. Má štruktúru metadát inšpirovanú tradičnými princípmi súborového systému Unix a navrhla ho Rémy Card, aby prekonal určité obmedzenia súborového systému MINIX. Bola to prvá implementácia, ktorá využívala virtuálny súborový systém (VFS⁵), ktorého podpora bola pridaná do jadra Linuxu vo verzii 0.96c, a dokázala spracovať súborové systémy s veľkosťou až 2 GB.

⁵Virtual File System

ext bol prvým z radu rozšírených súborových systémov. V roku 1993 ho nahradili systémy ext2 a Xiafs, ktoré si istý čas konkurovali, ale ext2 zvíťazil vďaka svojej dlhodobej životaschopnosti: ext2 odstránil problémy ext, ako napríklad nemennosť inódov a fragmentáciu.

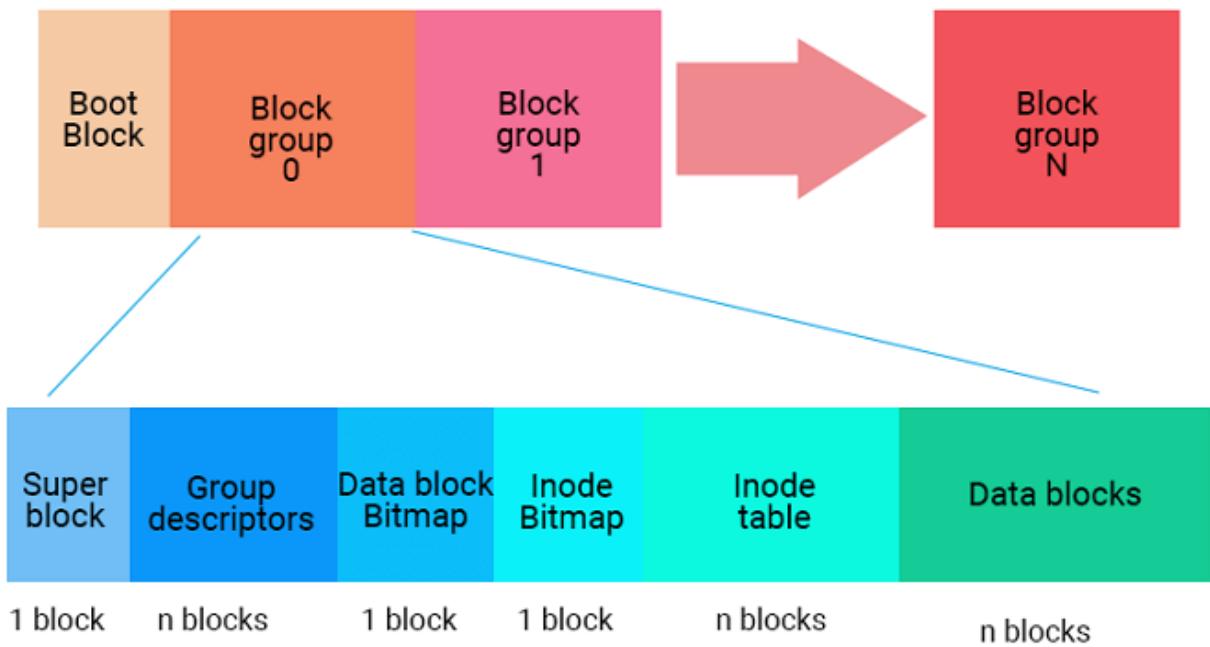
Ďalej sa tento súborový systém rozširoval a aktualizoval. Z tohto vznikli novšie verzie ext3 a ext4.

2.3.1 ext4

Podobne ako pri NTFS aj ext4 je tzv. žurnálový súborový systém. Je veľmi abstraktný čo je výhodou pre software pretože sa software developery nemusia zaoberať priveľa súborovým systémom a ich program by mal fungovať na každom rovnako. Abstrakcia znamená že všetok hardware (disky, a pod.) sú v ext4 reprezentované ako súbor. Má až takú úroveň abstrakcia že vlastne všetko je v podstate súbor. Používa sa ako predvolený súborový systém pre disky na distribúciách založených na Debian a Ubuntu. Taktiež je späťne kompatibilný s ext3.

2.3.2 Štruktúra ext4

Novo naformátovaný disk s ext4 vyzerá nasledovne:



EXT File System Structure

EaseUS
Make your life easy!

Obr. 4: Štruktúra súborového systému ext4

Zdroj: <https://www.easeus.com/diskmanager/file-system.html>

- Boot Block
 - Informácie o bootovaní
- Block group
 - Super block
 - * Superblok sa nachádza na začiatku súborového systému a obsahuje metadáta o súborovom systéme vrátane jeho veľkosti, veľkosti bloku, počtu inódov a ďalších parametrov. Slúži ako hlavný riadiaci blok pre súborový systém
 - Group descriptors
 - * Skupinové deskriptory obsahujú metadáta pre danú skupinu
 - Data block Bitmap
 - * Sleduje status blokov pre danú skupinu
 - Inode Bitmap
 - * Sleduje status inódov pre danú skupinu
 - Inode Table
 - * Obsahujú metadáta a atribúty, čo sa týka oprávnení a ďalších informácií pre každý súbor a adresár v danej skupine
 - Data blocks
 - * Obsahujú dané dátá

2.3.3 Výhody a nevýhody ext4

Výhody	Nevýhody
Podporuje najväčšiu individuálnu veľkosť súboru a veľkosť zväzku súborového systému.	Neposkytuje zabezpečenie dát.
Podporuje všetky znaky okrem NULL a '/.'	Tažké vytvoriť snapshot na inom zväzku.
Môžete previesť súborový systém Ext3 na Ext4.	Využíva viacaj miesta na disku.
Zahŕňa pokročilé funkcie ako rozšírenie, indexovanie adresárov, oneskorenú alokáciu a defragmentáciu.	
Podporuje neobmedzený počet podadresárov.	
Používa timestamp v nanosekundách.	
Podporuje predalokácia pre rozsiahle súbory.	
Podporuje viacnásobnú alokáciu blokov.	

Tabuľka 4: Výhody a nevýhody súborového systému Ext4

Zdroj: <https://www.easeus.com/partition-master/ext2-ext3-ext4-file-system-format-and-difference.html>

3 Nástroje na obnovu údajov

Existuje mnoho nástrojov na obnovu údajov. Či už ide o špecializované nástroje pre obnovu fotiek alebo multimediálnych súborov, alebo o univerzálné nástroje, ktoré dokážu obnoviť akékoľvek súbory. V tejto kapitole sa pozrieme na niektoré z nich.

- Recuva
 - Široko používaný a ľahko ovládateľný nástroj s pokročilými možnosťami skenovania pre rôzne typy súborov. Dostupný pre platofrmu Windows.
- PhotoRec
 - Špecializovaný na obnovenie stratených obrázkov a multimediálnych súborov z rôznych úložných zariadení. Dostupný pre Windows, MacOS, Linux a ďalšie.
- Testdisk
 - Je od rovnakého vývojára ako PhotoRec. Dokáže obnoviť rôzne druhy súborov. Je univerzálny. Nielen obnovuje vymazané súbory, ale tiež pomáha opraviť tabuľku oddielov a boot sektory. Dostupný pre Windows, MacOS, Linux a ďalšie.
- Disk Drill
 - Veľmi podobný nástroj ako Recuva. Narozený od Recuvy, ktorá sa zaobrá skorej funkcionalitou, Disk Drill sa zameriava na používateľský zážitok (UX⁶). Dostupný pre Windows, MacOS.

⁶User Experience



Obr. 5:
Recuva



Obr. 6:
PhotoRec



Obr. 7:
Testdisk



Obr. 8: Disk
Drill

3.1 Testdisk

Prečo som si vybral práve testdisk? Pretože je univerzálny, dokáže obnoviť rôzne druhy súborov. Taktiež vie opraviť tabuľku oddielov a boot sektory. Je crossplatform⁷ a zároveň je FOSS⁸. Podporuje viacero typov partition table (MBR⁹, GPT¹⁰). Zároveň podporuje viacero súborových systémov či už ide o FAT32, exFAT ale aj NTFS a ext. Má jednoduché rozhranie a nie je náročný na systém.

4 Experimentovanie s nástrojom testdisk

Najskôr bolo potrebné si pripraviť testovacie prostredie. Uvažoval som aj nad testovaním na fyzickom disku, ale keďže na mojom počítači mám operačný systém Windows a ten nedokáže pracovať s diskami, ktoré sú naformátované na ext, tak som sa rozhodol, že budem pracovať na virtuálnom stroji (VM¹¹). Použil som program VirtualBox, ktorý je zadarmo. Na VM som nainštaloval vtedy najnovšiu verziu distribúcie Arch. Najprv som si nastavil prostredie aby sa mi lepšie pracovalo. Následne som si stiahol potrebné nástroje a dependencies. Potom som vytvoril virtuálne disky, ktorý som najskôr naformátoval a neskôr pripojil (mountol) do systému. Po tomto sa mohlo začať s experimentovaním.

Najprv som testoval tak, že som mal jeden disk o veľkosti 1 GB a mal 4 partície pre každý súborový systém, ktorému som sa chcel venovať (FAT32, exFAT, NTFS, ext4). Každá partícia mala veľkosť 200 MB. Neskôr kvôli komplikáciám s ext4 som skúsil aj samostatne jeden disk pre každý súborový systém.

Stiahol som si testovací súbor dostatočne veľký na to, aby pokrýval nadpolovičnú väčšinu z partície. Na toto som využil obrázok od NASA JWST¹², ktorý mal veľkosť 130MB.

⁷Podporuje viacero operačných systémov

⁸Free & Open Source Software — zadarmo s voľne šíriteľným zdrojovým kódom

⁹Master Boot Record

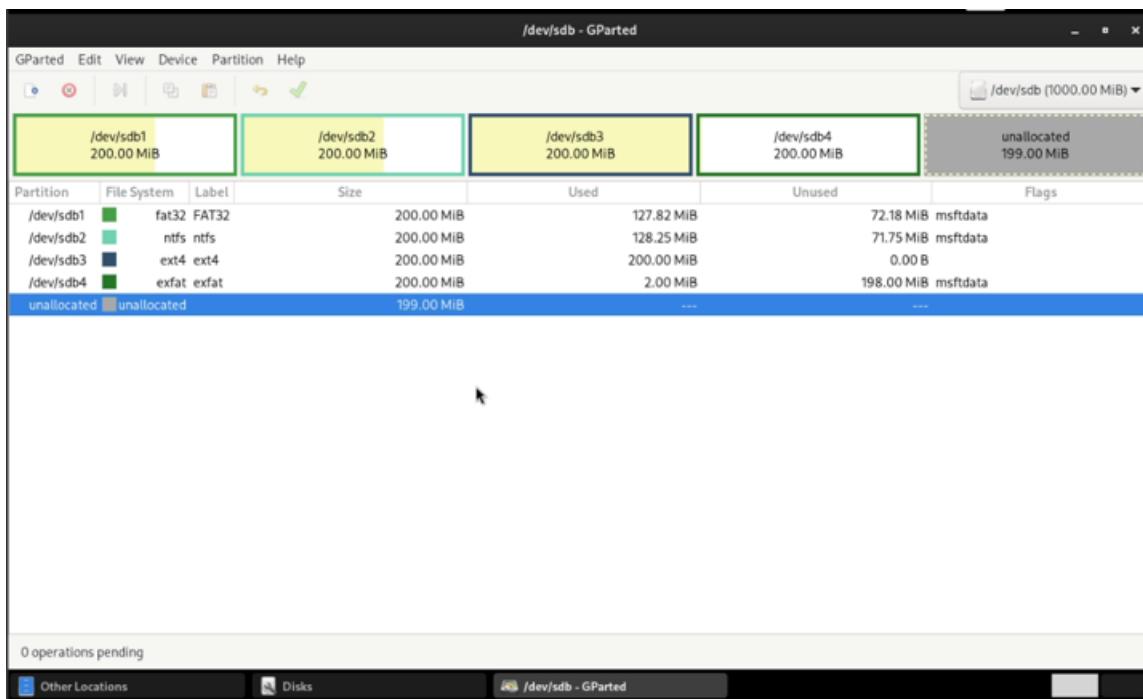
¹⁰GUID Partition Table

¹¹Virtual Machine

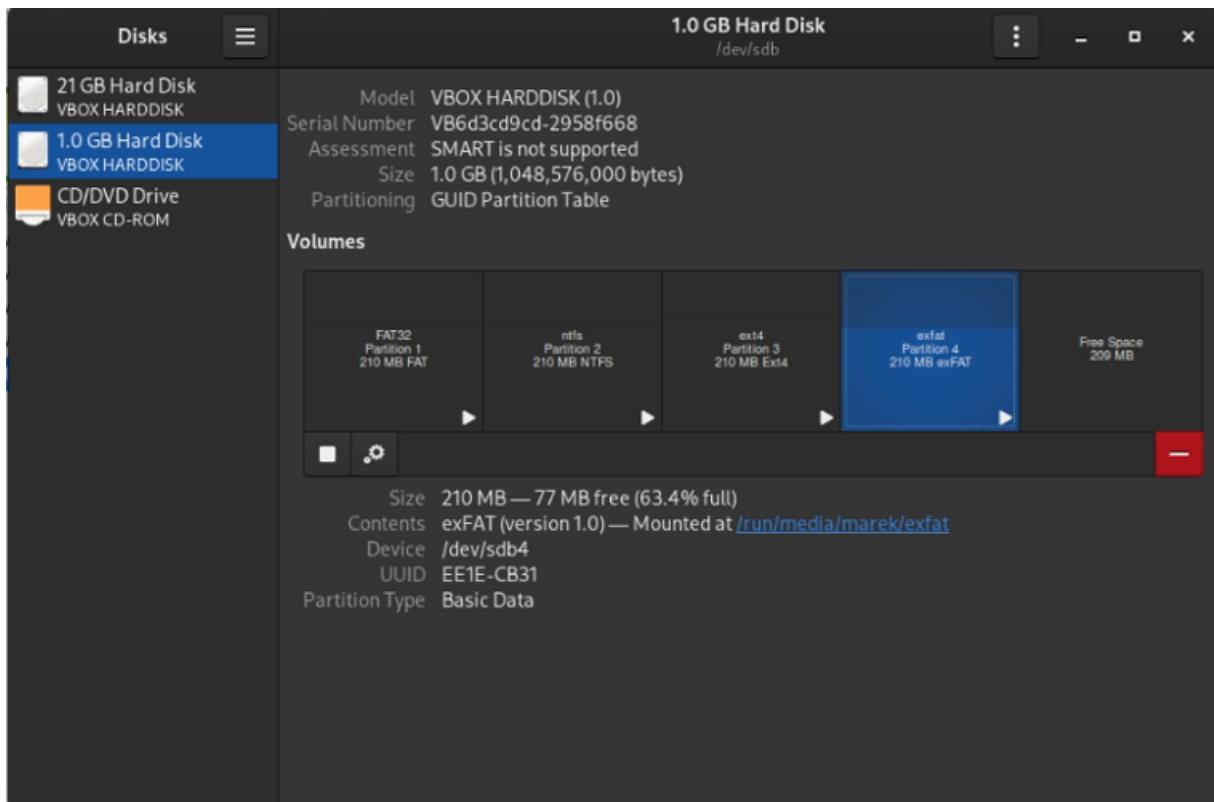
¹²James Webb Space Telescope



Obr. 9: Testovací obrázok



Obr. 10: Gparted — úvodné nastavenie diskov



Obr. 11: Mountnutie diskov/partícií pomocou Gnome Disks

4.1 Zmazanie a obnova súborov

Najskôr som naplnil všetky partície súborom.

```
marek@arch-vm:~
```

NAME	FSTYPE	FSVER	LABEL	UUID	FSAVAIL	FSUSE%	MOUNTPOINTS
sda	vfat	FAT32		A6B2-E230	128.2M	36%	/boot
sda	ext4	1.0		4530810b-b7bb-44c8-b2a4-d9dda09d5f1a	10.5G	40%	/
sdb	vfat	FAT32	FAT32	B27A-80D2	72.2M	63%	/run/media/marek/FAT32
sdb	ntfs		ntfs	7F9207311EDFCAD8	71.7M	64%	/run/media/marek/ntfs
sdb	ext4	1.0	ext4	b71fa0ba-9703-4dd1-90e8-a6b59dc1d68f	43.2M	69%	/run/media/marek/ext4
sdb	exfat	1.0	exfat	EE1E-CB31	73.3M	63%	/run/media/marek/exfat
sr0							[SWAP]
zram0							

Obr. 12: Zobrazenie naplnených partícií — lsblk

```

marek 🐫 on arch-vm ~ 28% | 0% took 76ms
bsh > ls /run/media/marek/ -R
Permissions Size User Date Modified Name
drwxr-xr-x  - marek 10 Apr 19:54 exfat
drwxr-xr-x  - marek 10 Apr 19:35 ext4
drwxr-xr-x  - marek 1 Jan 1970 FAT32
drwxrwxrwx  - marek 10 Apr 19:26 ntfs

/run/media/marek/exfat:
Permissions Size User Date Modified Name
.rw xr-xr-x  131M marek 10 Apr 16:03 lexfat.png

/run/media/marek/ext4:
Permissions Size User Date Modified Name
drwx-----  - marek 10 Apr 19:23 lost+found
.rw-r--r--  131M marek 10 Apr 16:03 lext4.png

/run/media/marek/ext4/lost+found:

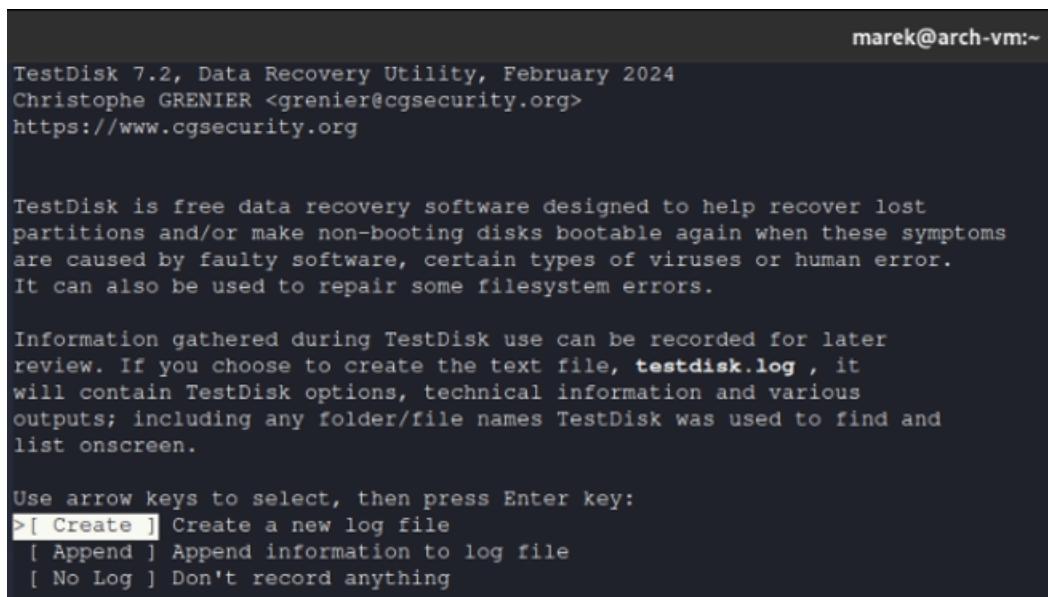
/run/media/marek/FAT32:
Permissions Size User Date Modified Name
.rw-r--r--  131M marek 10 Apr 16:03 lfat32.png

/run/media/marek/ntfs:
Permissions Size User Date Modified Name
.rw-r--r--@ 131M marek 10 Apr 16:03 intfs.png

```

Obr. 13: Zobrazenie naplnených partícíí — ls

Následne som spustil nástroj testdisk v terminály.



Obr. 14: Testdisk — UI

Po vybratí typu logovania sa nám zobrazí obrazovka, kde si môžeme vybrať disk, s ktorým chceme pracovať.

- /dev/sda — systémový disk
- /dev/sdb — disk, ktorý som vytvoril pre testovanie

```
marek@arch-vm:~  
TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
https://www.cgsecurity.org  
  
TestDisk is free software, and  
comes with ABSOLUTELY NO WARRANTY.  
  
Select a media and choose 'Proceed' using arrow keys:  
Disk /dev/sda - 21 GB / 20 GiB - VBOX HARDDISK  
>Disk /dev/sdb - 1048 MB / 1000 MiB - VBOX HARDDISK  
  
  
>[Proceed] [ Quit ]  
  
Note:  
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.
```

Obr. 15: Testdisk — výber disku

Následne nám nástroj automaticky zistí typ partition table. V prípade že nástroj zistí typ chybne, môžeme ho sami vybrať. Náš disk má partition table typu GPT, takže nástroj ho zistil správne a my sme možnosť potvrdili.

```
marek@arch-vm:~  
TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
https://www.cgsecurity.org  
  
Disk /dev/sdb - 1048 MB / 1000 MiB - VBOX HARDDISK  
  
Please select the partition table type, press Enter when done.  
[Intel] Intel/PC partition  
> [EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)  
[Humax] Humax partition table  
[Mac] Apple partition map (legacy)  
[None] Non partitioned media  
[Sun] Sun Solaris partition  
[XBox] XBox partition  
[Return] Return to disk selection  
  
Hint: EFI GPT partition table type has been detected.  
Note: Do NOT select 'None' for media with only a single partition. It's very  
rare for a disk to be 'Non-partitioned'.
```

Obr. 16: Testdisk — výber partition table

Po jeho vybratí sa nám zobrazilo menu na prácu s diskom. Pre nás podstatné budú možnosti “Analyse” a “Advanced”.

- Analyse
 - Táto možnosť nám umožní analyzovať disk a nájsť chyby súborového systému. Tiež slúži na obnovu partícii.
- Advanced
 - Táto možnosť nám zobrazí zistené partície na disku. S ktorými budeme môcť ďalej pracovať.

Po vybratí možnosti “Advanced” nám nástroj zobrazí zistené partície na disku. Najskôr si vyberieme partíciu, s ktorou chceme pracovať a v dolnom menu si vyberieme čo chceme s danou partíciou robiť.

```
marek@arch-vm:~  
TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
https://www.cgsecurity.org  
  
Disk /dev/sdb - 1048 MB / 1000 MiB - CHS 127 255 63  
  
Partition Start End Size in sectors  
> 1 P MS Data 2048 411647 409600 [FAT32]  
2 P MS Data 411648 821247 409600 [ntfs]  
3 P Linux filesystem. data 821248 1230847 409600  
4 P MS Data 1230848 1640447 409600  
  
[ Type ] [ Boot ] >[Undelete] [Image Creation] [ Quit ]  
File undelete
```

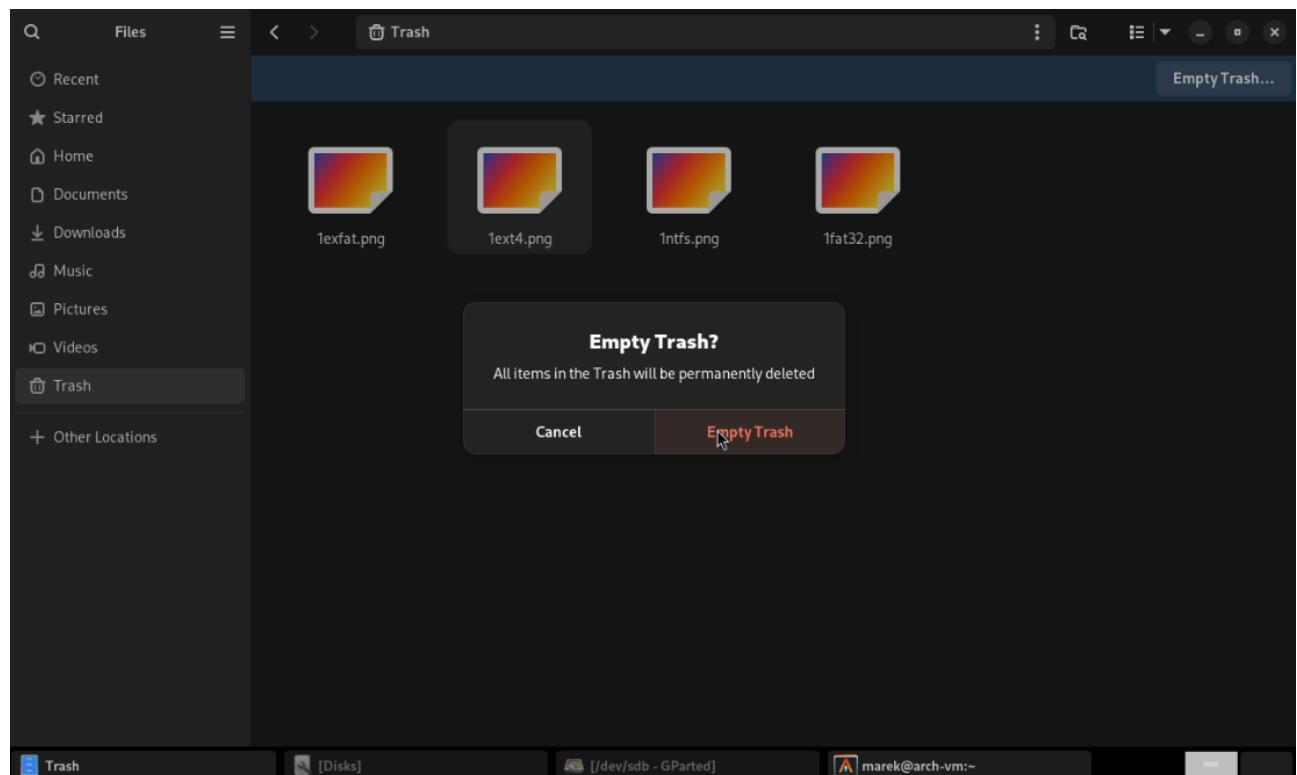
Obr. 17: Testdisk — výber partície

V našom prípade použijeme možnosť “undelete”, ktorá umožnuje obnoviť zmazané súbory. Kedže sme zatial nič nevymazali, tak nám zobrazí súbory a priečinky, ktoré sa tam nachádzajú podobne ako pri “ls” alebo “dir”.

```
marek@arch-vm:~  
TestDisk 7.2, Data Recovery Utility, February 2024  
Christophe GRENIER <grenier@cgsecurity.org>  
https://www.cgsecurity.org  
1 P MS Data 2048 411647 409600 [FAT32]  
Directory /  
-rwxr-xr-x 0 0 130764157 10-Apr-2024 14:03 lfat32.png  
Next  
Use Right to change directory, 'b' to hide deleted files  
'q' to quit, ':' to select the current file, 'a' to select all files  
'c' to copy the selected files, 'e' to copy the current file  
[OtherLocations] [Disks] [/dev/sdb - GParted] marek@arch-vm:~
```

Obr. 18: Testdisk — zobrazenie súborov

Následne vypneme nástroj a zmažeme súbor z každej partície s tým, že zároveň ich vymazeme aj z koša.



Obr. 19: Vymazanie súborov

Potom si opäť spustíme nástroj testdisk s tým že urobíme rovnaké kroky ako boli pred

chvíľou spomenuté. Následne si vyberieme možnosť “undelete” a nástroj nám zobrazí zmazaný súbor. Všimnime si, že teraz je súbor označený červenou farbou. Následne si ho zvolíme a stlačíme malé “c” na jeho skopírovanie.



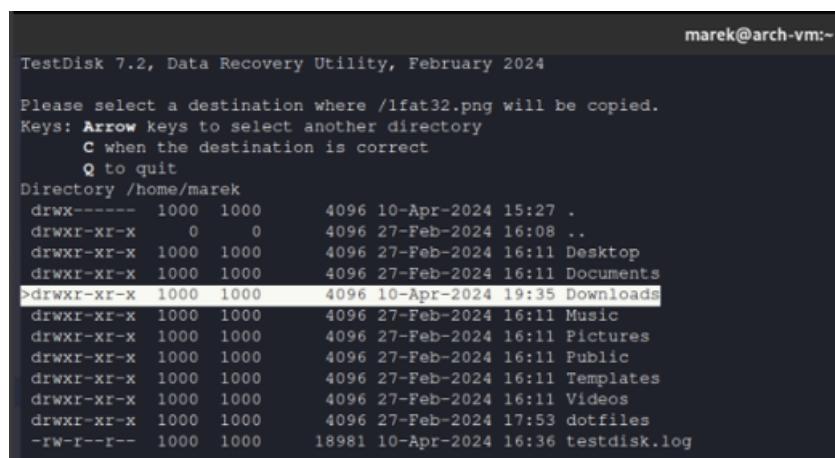
marek@arch-vm:~
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
<https://www.cgsecurity.org>
1 P MS Data 2048 411647 409600 [FAT32]
Directory /

-rwxr-xr-x 0 0 130764157 10-Apr-2024 14:03 lfat32.png
>drwxr-xr-x 0 0 0 10-Apr-2024 17:58 .Trash-1000

Next
Use Right to change directory, 'h' to hide deleted files
'q' to quit, '::' to select the current file, 'a' to select all files
'C' to copy the selected files, 'c' to copy the current file

Obr. 20: Testdisk — obnova zmazaných súborov

Ďalej nám nástroj zobrazí možnosť kam chceme súbor skopírovať. Vyberieme si cestu a stlačíme veľké “C”. Potom nám nástroj zobrazí informáciu o tom, či bol súbor úspešne skopírovaný.



marek@arch-vm:~
TestDisk 7.2, Data Recovery Utility, February 2024

Please select a destination where /lfat32.png will be copied.
Keys: Arrow Keys to select another directory
C when the destination is correct
Q to quit
Directory /home/marek
drwx----- 1000 1000 4096 10-Apr-2024 15:27 .
drwxr-xr-x 0 0 4096 27-Feb-2024 16:08 ..
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Desktop
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Documents
>drwxr-xr-x 1000 1000 4096 10-Apr-2024 19:35 Downloads
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Music
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Pictures
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Public
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Templates
drwxr-xr-x 1000 1000 4096 27-Feb-2024 16:11 Videos
drwxr-xr-x 1000 1000 4096 27-Feb-2024 17:53 dotfiles
-rw-r--r-- 1000 1000 18981 10-Apr-2024 16:36 testdisk.log

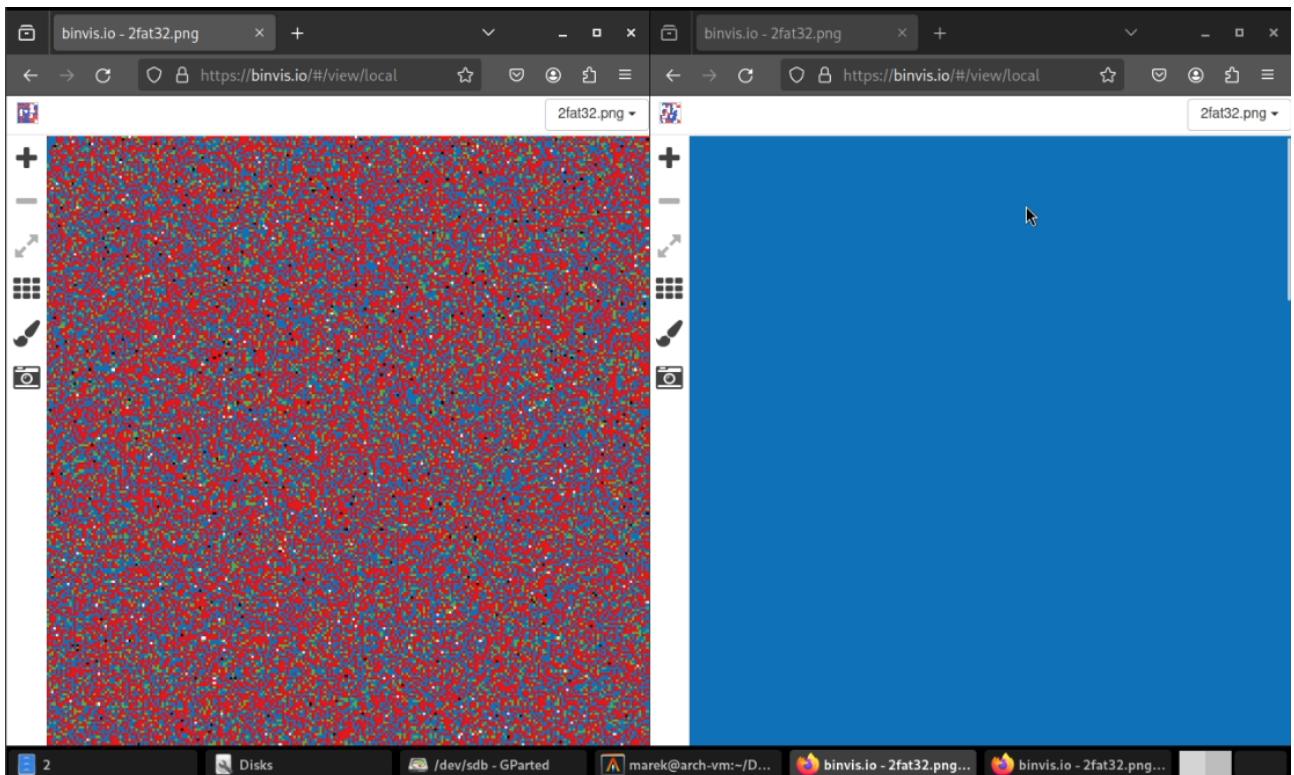
Obr. 21: Testdisk — kopírovanie zmazaného súboru

Tento proces zopakujeme na všetkých partíciah nášho testovacieho disku.

4.2 Zapísanie na miesto zmazaného súboru

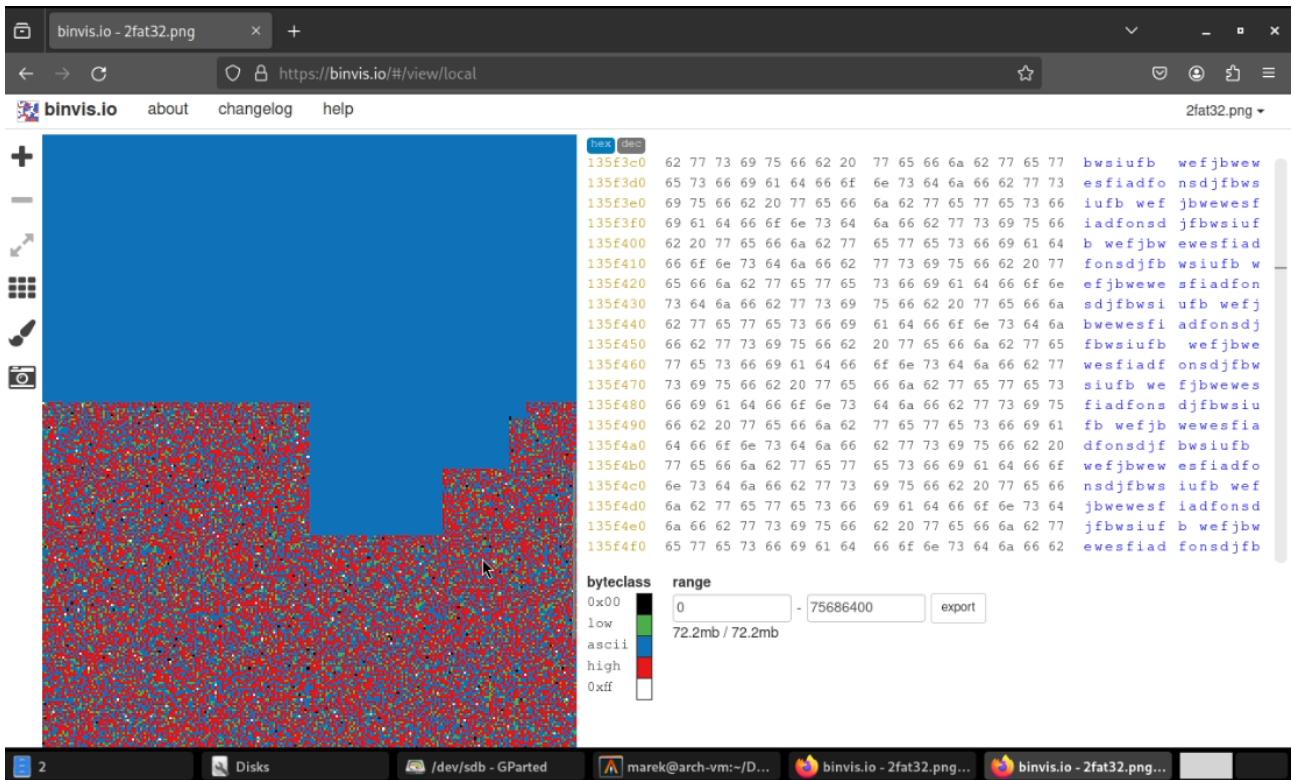
Po predošлом experimentovaní som stiahol iný obrázok z NASA JWST, ktorý mal veľkosť 172 MB. Uložil som ho na každú partíciu. Následne som ho vymazal, ale potom som na partícii nahral ešte textový súbor, ktorý mal 150 MB aby prepísal pozostaté dátá o obrázku. Keď som sa pokúsil obnoviť obrázok, tak som síce našiel jeho záznam, ale keď som ho obnovil, tak jeho začiatok bol prepísaný textovým súborom. Týmto sme o dátá z obrázka prišli, pretože sa po obnovení nedal prezerat.

Tento proces som vizualizoval pomocou webu <https://binvis.io/>. Na obrázku je vidieť nepoškodený súbor vľavo a potom z polovice prepísaný súbor vpravo.



Obr. 22: Vizualizácia pomocou binvis.io

Na druhej vizualizácii je vidieť kde už pokračujú pozostatky dát z obrázku, pretože neboli prepísaný celý, keďže bol väčší ako textový súbor.

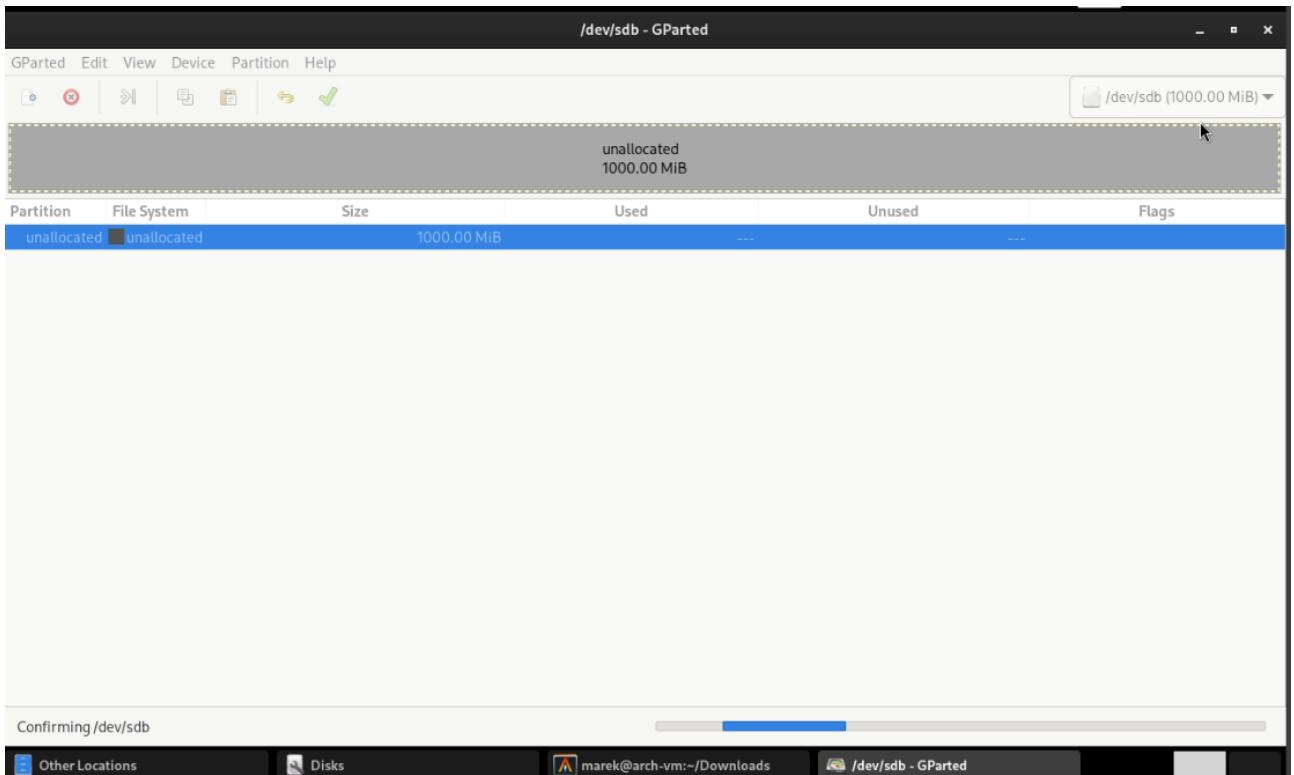


Obr. 23: Vizualizácia pomocou binvis.io — pozostatky dát

Táto skutočnosť nastáva z dôvodu, že pri mazaní súborov z disku sa vymaže iba záznam o súbore a nie sám súbor. V skutočnosti sa ani sám záznam priamo nevymaže ale iba sa označí že na miesto, ktoré mal disk alokovaný pre seba je teraz možné znova zapisovať. Preto je možné dátá z diskov obnoviť ale iba v prípade, že nebudeme zapisovať na daný disk. Keď sa však na miesto zmazaného súboru zapíše iný súbor, tak sa dátá pôvodného súboru prepíšu a týmto sa stane neobnoviteľným.

4.3 Zmazanie a obnova partície

Po predošлом experimentovaní som na záver pomocou programu Gparted vymazal všetky partície.



Obr. 24: GParted — Vymazanie partícíí

Opäť som spustil nástroj testdisk a postupoval podobne ako pri obnove súborov, avšak tentoraz som vybral možnosť “Analyse” a nástroj mi zobrazil všetky zmazané partície. Môžeme si všimnúť, že posledná partícia bola označená ako NTFS aj keď bola naformátovaná na exFAT. Testdisk pravdepodobne iba chybne určil typ jej súborového systému. Následne som potvrdil aby sa partície obnovili. Chyba určenia typu pri exFAT nakoniec ničomu nevadila, pretože aplikácia GNOME Disks vedela že ide o exFAT.

```

marek@arch-vm:~/Downloads
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 1048 MB / 1000 MiB - CHS 127 255 63
  Partition      Start      End    Size in sectors
P FAT32          0  32 33    25 159  6    409600 [FAT32]
P HPFS - NTFS    25 159  7    51 30 43    409600 [ntfs]
P Linux           51 30 44    76 157 17    409600 [ext4]
>P HPFS - NTFS   76 157 18   102 28 54    409600

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
exFAT, blocksize=4096, 209 MB / 200 MiB

```

The screenshot shows the TestDisk 7.2 interface. At the top, it displays the command `marek@arch-vm:~/Downloads` and the software version. Below that is the copyright information for Christophe GRENIER and the website https://www.cgsecurity.org. The main part of the screen shows a table of disk partitions. The table has columns for Partition, Start, End, and Size in sectors. There are four partitions listed: a primary FAT32 partition at offset 0, a primary NTFS partition at offset 25, a logical Linux ext4 partition at offset 51, and a new primary NTFS partition at offset 76. The new partition at offset 76 is highlighted with a green border. At the bottom of the screen, there is a status message: "Structure: Ok. Use Up/Down Arrow keys to select partition." followed by instructions for using the arrow keys to change partition characteristics and other keyboard shortcuts like A, L, T, P, and Enter.

Obr. 25: Testdisk — obnova zmazaných partícií

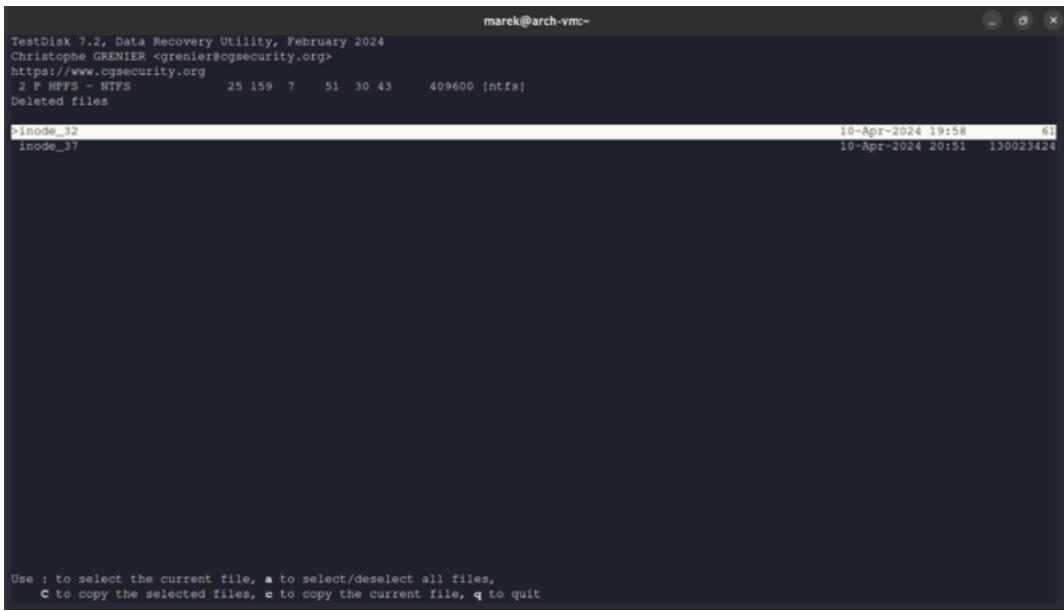
5 Výsledky experimentov

5.1 Zmazanie súborov

Pri práci s FAT32 a exFAT neboli problémy a súbor sa mi podarilo v poriadku obnoviť.

V prípado NTFS nastali komplikácie. Testdisk hlásil, že súborový systém je poškodený. Vtedy som zvolil možnosť “Analyse”, ktorá ho opravila a potom po reštarte VM a spustení testdisku som mohol pokračovať v obnove zmazaných súborov. Pri NTFS sa to riešilo cez inodes a pri obnove bolo treba premenovať súbor aj s koncovkou a nastaviť nad ním vlastníctvo¹³. Táto komplikácia bola pravdepodobne spôsobená tým, že som pracoval na virtuálnom stroji a nie na fyzickom disku. Prípadne preto, že som pracoval na Linuxe a nie na Windows.

¹³ownership



The screenshot shows the TestDisk 7.2 Data Recovery Utility interface. The title bar reads "marek@arch-vm:~" and the window title is "TestDisk 7.2, Data Recovery Utility, February 2024". The main text area displays the following information:

```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
2 F HFS - NTFS      25 159 7    51 30 43    409600 [ntfs]
Deleted files
>inode_32          10-Apr-2024 19:58   61
inode_37          10-Apr-2024 20:51  130023424
```

At the bottom of the screen, there is a message: "Use : to select the current file, **a** to select/deselect all files, **c** to copy the selected files, **c** to copy the current file, **q** to quit".

Obr. 26: Testdisk — obnova zmazaných súborov — NTFS

Zo súborového systému ext4 sa mi nepodarilo obnoviť súbor pretože ho testdisk nezobrazoval. Neskôr som sa v dokumentácii dočítal, že testdisk podporuje ext2 čo mi však prišlo zváštne. Každopádne som tento proces skúsil na disku, kde bola jedna partícia naformátovaná na ext2 avšak aj v tomto prípade mi zmazaný súbor nezobrazovalo. Pravdepodobne to bolo spôsobené tým, že som pracoval vo virtuálnom prostredí.

5.2 Prepísanie zmazaných súborov

Z tohto experimentu nám vyplýva, že ak sa nám niekedy náhodou stane že sme vymazali niečo čo sme nechceli, tak je treba čo najskôr prestaviť zapisovať na disk. To môžeme docieľiť kompletným vypnutím počítača. Ak sa nám podarí zastaviť zápis na disk, tak je veľká šanca že sa nám podarí obnoviť zmazané súbory. Ak však začneme zapisovať na disk, tak je šanca že sa nám nepodarí obnoviť súbory, pretože sa dátá prepíšu.

5.3 Zmazanie partície

Pri obnove zmazaných partícii som nemal žiadne problémy. Testdisk ich zobrazil a následne som ich mohol obnoviť. V prípade, že by som mal dátá na týchto partíciách, tak by som ich mohol obnoviť. Tento proces by bol podobný ako pri obnove zmazaných súborov.

6 Správne zmazanie dát a formátovanie disku

Prikaz shred, funguje vsak iba na HDD lebo SSD pouzivaju TRIM (da sa asi vypnút ?) ktorý vlastne robi wear and tear mechanizmus aby sa disk opotreboval rovnomerne a preto sa data ukladajú náhodne na rôzne bunky a nie sekvenčne ako na HDD aby to bolo rýchlejšie lebo pri ssd na tom nezalezi

sem napisat: ak spravne naformatueme disk tak ze ho pomocou nejakeho nastroja prepiseme cez viacej krat nahodnymi datami tak je mozne ho predat bez obavy ze sa z neho daju obnovit data ktore tam boli pred tym, je to preto lebo pri vymazavani sa v "mazu" v podstate iba zaznameni o danych suboroch repsketive sa oznamia ze tam je teraz volne miesto a moze sa tam zapisovat

7 Záver

ak sa nam stalo ze sme omylom vymazali particiu alebo subory ktore sme nechceli tak treba hned prestat zapisovat na disk a je velka sanca ze data vieme zachranit avsak ak zacneme robit zmeny na disku a nasledne nan zapisovat tak je v podstate jedno aky suborovy system pouzivame v kazdom pripade prepiseme data ktore tam boli

8 Poznatky zapracovat

pri SSD diskoch je treba mat vypnutu funkciu TRIM, ktorá je zodpovedna za rovnomerne opotrebovanie disku a preto neukladá dátá sekvenčne ako HDD aby bolo rýchlejšie ale ukladá náhodne na rôzne bunky.

Literatúra

- [1] Christophe GRENIER. Testdisk - cgsecurity, 2016 - 2023. URL https://www.cgsecurity.org/testdisk_doc/. [Online; accessed 28-February-2024].
- [2] Richard Russen, Yuval Fledel. NTFS Documentation - Linux Reverse Engineered, 2000. URL <https://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf>. [Online; accessed 28-February-2024].
- [3] NTFS Documentation. URL <https://www.ntfs.com/>. [Online; accessed 12-March-2024].

- [4] Tracy King. What Is NTFS File System and Do I Need It? URL <https://www.easeus.com/partition-manager-software/ntfs-file-system.html>. [Online; accessed 13-March-2024].
- [5] Microsoft Corporation. FAT: General Overview of On-Disk Format, 2000. URL <https://dubeyko.com/development/FileSystems/FAT/FAT%20Specs%201.03.pdf>. [Online; accessed 28-February-2024].
- [6] The kernel development community. ext4 Filesystem. URL <https://www.kernel.org/doc/html/v4.19/filesystems/ext4/index.html>. [Online; accessed 28-February-2024].
- [7] Wikipedia contributors. Extended file system — Wikipedia, the free encyclopedia, 2024. URL https://en.wikipedia.org/w/index.php?title=Extended_file_system&oldid=1214102216. [Online; accessed April-2024].
- [8] Tracy King. File System Comparison: NTFS, FAT32, exFAT, and EXT, Which File System Should I Use, 2023. URL <https://www.easeus.com/diskmanager/file-system.html>. [Online; accessed March-2024].
- [9] Wikipedia contributors. File system — Wikipedia, the free encyclopedia, 2024. URL https://en.wikipedia.org/w/index.php?title=File_system&oldid=1220996793. [Online; accessed April-2024].
- [10] Comparing NTFS and FAT32 File Systems: Features, Pros and Cons. URL <https://superops.com/ntfs-vs-fat32>. [Online; accessed March-2024].
- [11] Kristoffer Bonheur. exFAT: Advantages and Disadvantages of Extensible FAT, 2023. URL <https://www.profolus.com/topics/exfat-advantages-disadvantages-extensible-fat/>. [Online; accessed April-2024].
- [12] Wikipedia contributors. Exfat — Wikipedia, the free encyclopedia, 2024. URL <https://en.wikipedia.org/w/index.php?title=ExFAT&oldid=1214486967>. [Online; accessed April-2024].
- [13] Gabriel Ramuglia. Using shred — The Linux Command for Secure File Deletion, 2023. URL <https://ioflood.com/blog/shred-linux-command/>. [Online; accessed April-2024].
- [14] Free Software Foundation, Inc. GNU Coreutils, 1994-2024. URL <https://www.gnu.org/software/coreutils/manual/coreutils.html>. [Online; accessed April-2024].