Princípy informačnej bezpečnosti

Voľné šíriteľné nástroje na obnovu zmazaných súborov

(Progress report č.2 – Praktická časť – Experimentovanie s nástrojom testdisk)

Autor: Marek Čederle

Obsah

- Nástroje na obnovu súborov
- Nástroj testdisk
- Experimentovanie s nástrojom testdisk
  - Obnova zmazaných súborov
  - Obnova zmazaných partícií
- Záver

Nástroje na obnovu súborov

- Recuva
- PhotoRec
- TestDisk
- Disk Drill

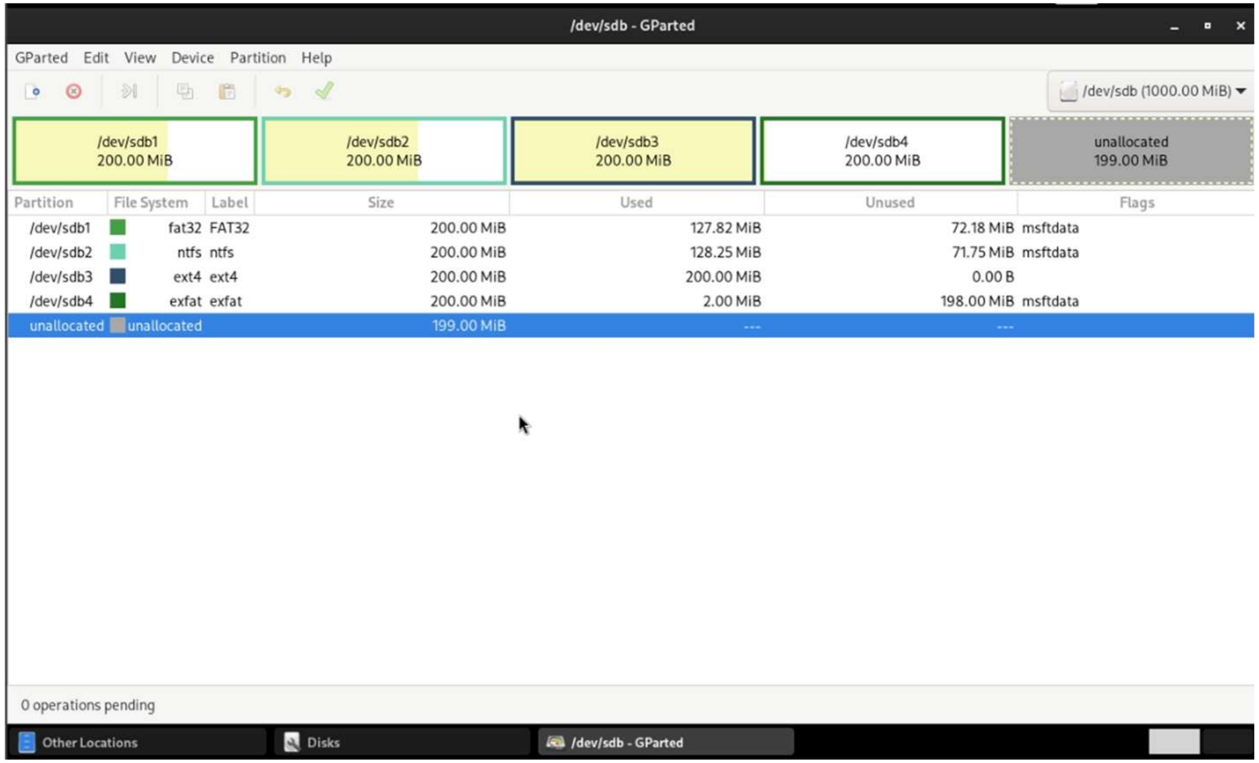
Nástroj testdisk

- FOSS (Free & Open Source)
- Crossplatform
- Podpora viacero typov partition table
- Podpora viacero súborových systémov
- Obnovenie súborov
- Obnovenie partícií
- Jednoduchá a lightweight CLI aplikácia

Experimentovanie s nástrojom testdisk

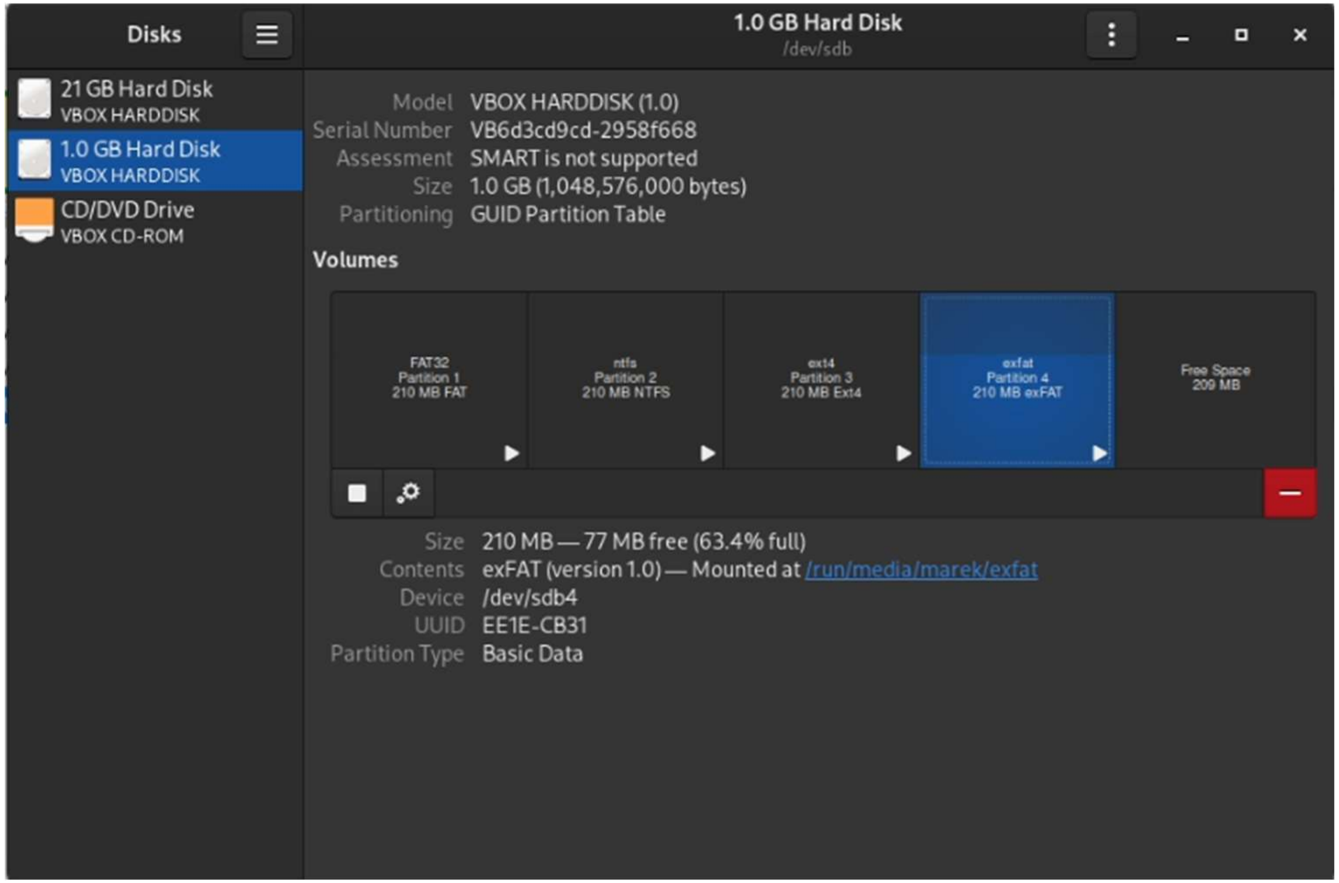
- Predpríprava na experimentovanie:
  - Vytvorenie virtuálneho stroja s Arch Linux
  - Nastavenie prostredia
  - Stiahnutie nástrojov a dependencies
  - Vytvorenie virtuálnych diskov
  - Naformátovanie diskov
  - Mountnutie diskov do systému
- Začiatok experimentovania

- Testovací obrázok – veľkosť: 130MB (Zdroj: NASA JWST)
- Veľkosť partícií: 200MB



Partition	File System	Label	Size	Used	Unused	Flags
/dev/sdb1	🟩 fat32	FAT32	200.00 MiB	127.82 MiB	72.18 MiB	msftdata
/dev/sdb2	🟩 ntfs	ntfs	200.00 MiB	128.25 MiB	71.75 MiB	msftdata
/dev/sdb3	🟦 ext4	ext4	200.00 MiB	200.00 MiB	0.00 B	
/dev/sdb4	🟩 exfat	exfat	200.00 MiB	2.00 MiB	198.00 MiB	msftdata
unallocated	⬜ unallocated		199.00 MiB	---	---	

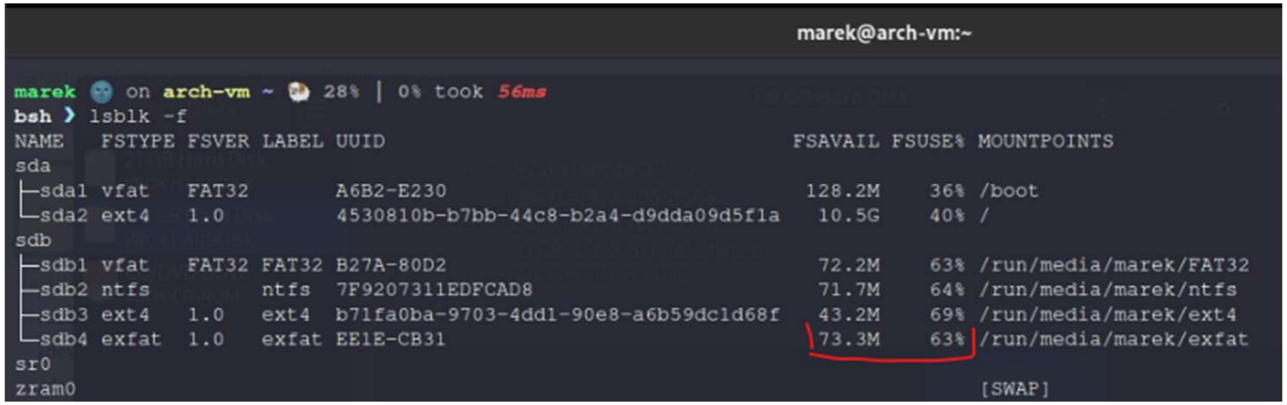
0 operations pending



Model VBOX HARDDISK (1.0)
Serial Number VB6d3cd9cd-2958f668
Assessment SMART is not supported
Size 1.0 GB (1,048,576,000 bytes)
Partitioning GUID Partition Table

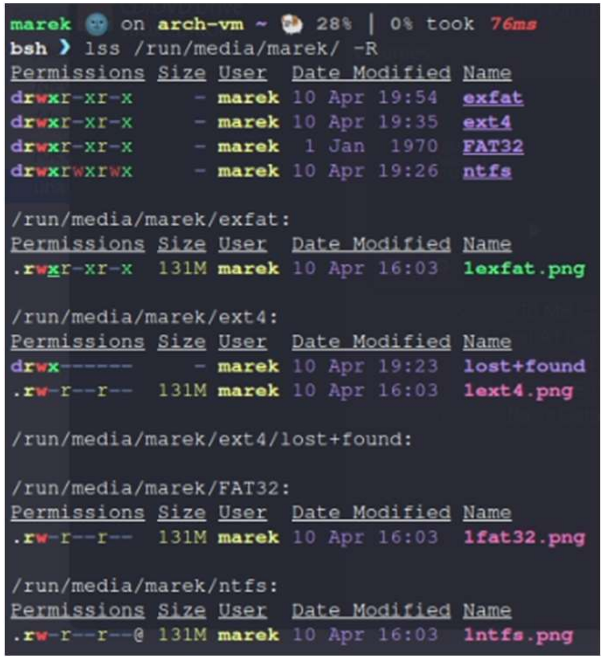
Volumes

Size 210 MB — 77 MB free (63.4% full)
Contents exFAT (version 1.0) — Mounted at /run/media/marek/exfat
Device /dev/sdb4
UUID EE1E-CB31
Partition Type Basic Data

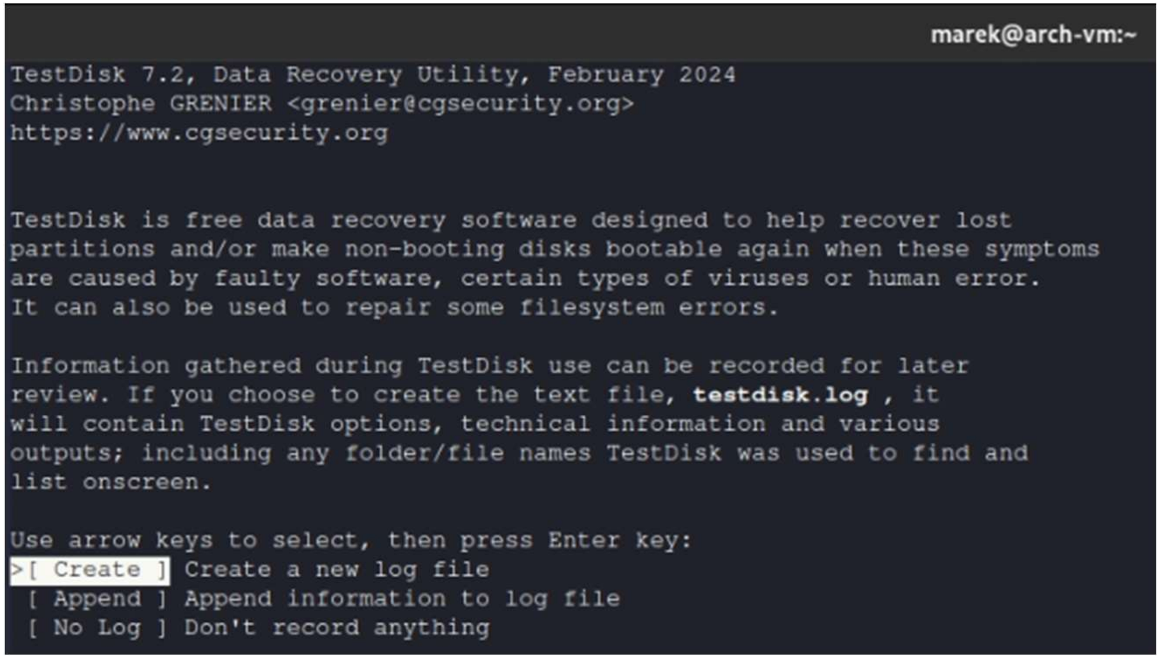


marek@arch-vm:~

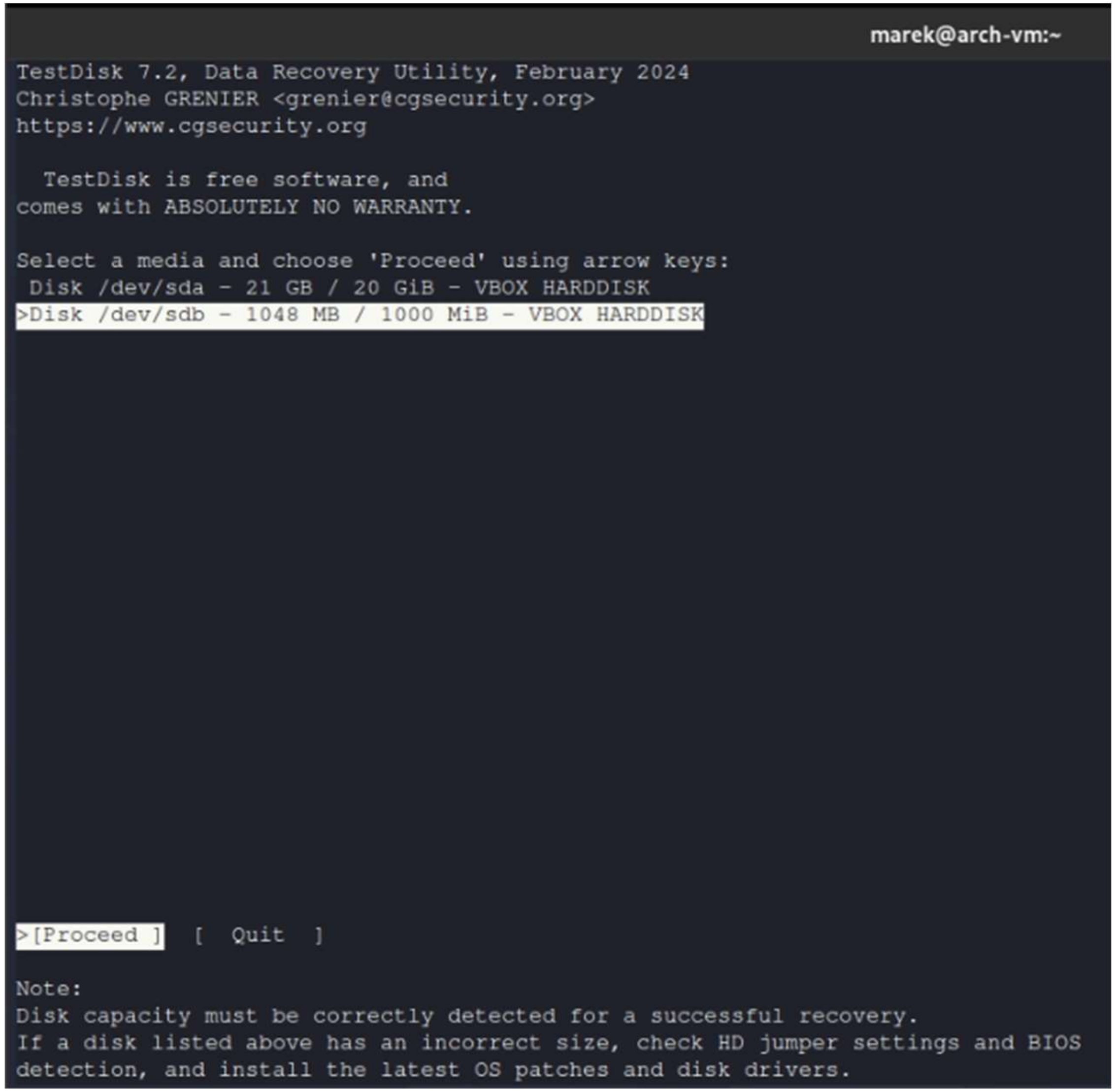
```
marek 🌚 on arch-vm ~ 🐹 28% | 0% took 56ms
bsh ❯ lsblk -f
NAME   FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINTS
sda
├─sda1 vfat   FAT32       A6B2-E230                             128.2M    36% /boot
└─sda2 ext4   1.0         4530810b-b7bb-44c8-b2a4-d9dda09d5f1a   10.5G    40% /
sdb
├─sdb1 vfat   FAT32 FAT32 B27A-80D2                              72.2M    63% /run/media/marek/FAT32
├─sdb2 ntfs         ntfs  7F9207311EDFCAD8                       71.7M    64% /run/media/marek/ntfs
├─sdb3 ext4   1.0   ext4  b71fa0ba-9703-4dd1-90e8-a6b59dc1d68f   43.2M    69% /run/media/marek/ext4
└─sdb4 exfat  1.0   exfat EE1E-CB31                              73.3M    63% /run/media/marek/exfat
sr0
zram0                                                                         [SWAP]
```



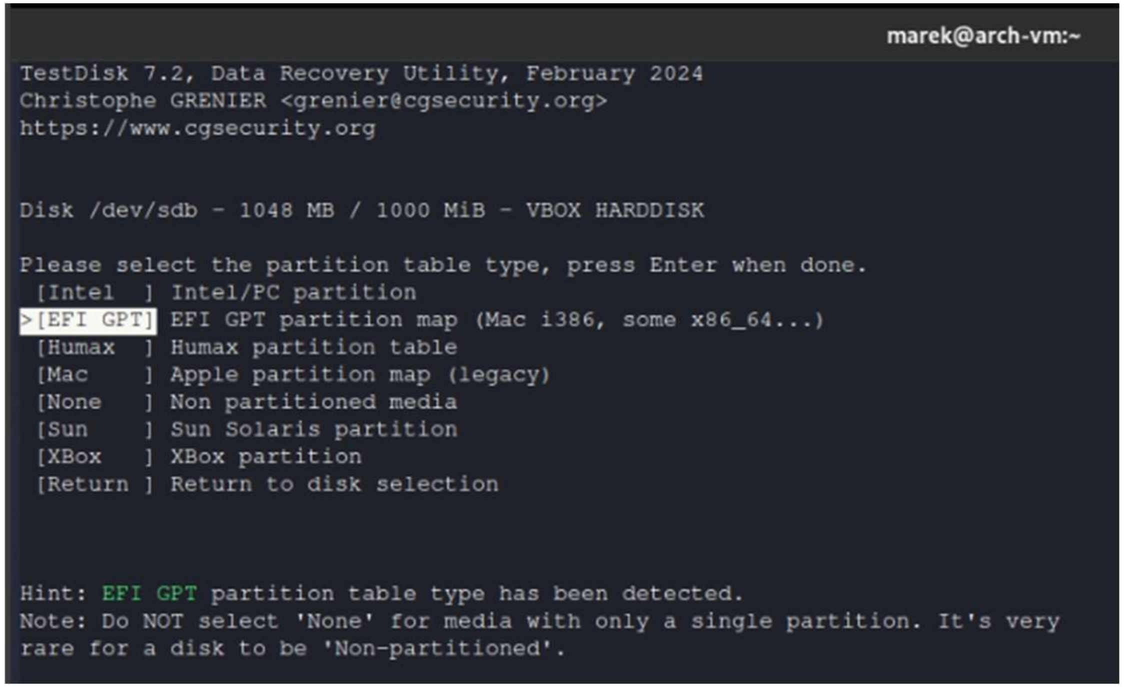
```
marek 🌚 on arch-vm ~ 🐹 28% | 0% took 76ms
bsh ❯ lss /run/media/marek/ -R
Permissions Size User  Date Modified Name
drwxr-xr-x     - marek 10 Apr 19:54  exfat
drwxr-xr-x     - marek 10 Apr 19:35  ext4
drwxr-xr-x     - marek  1 Jan  1970  FAT32
drwxrwxrwx     - marek 10 Apr 19:26  ntfs

/run/media/marek/exfat:
Permissions Size User  Date Modified Name
.rwxr-xr-x  131M marek 10 Apr 16:03  1exfat.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  1ext4.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  1fat32.png

/run/media/marek/ntfs:
Permissions Size User  Date Modified Name
.rw-r--r--@ 131M marek 10 Apr 16:03  1ntfs.png
```



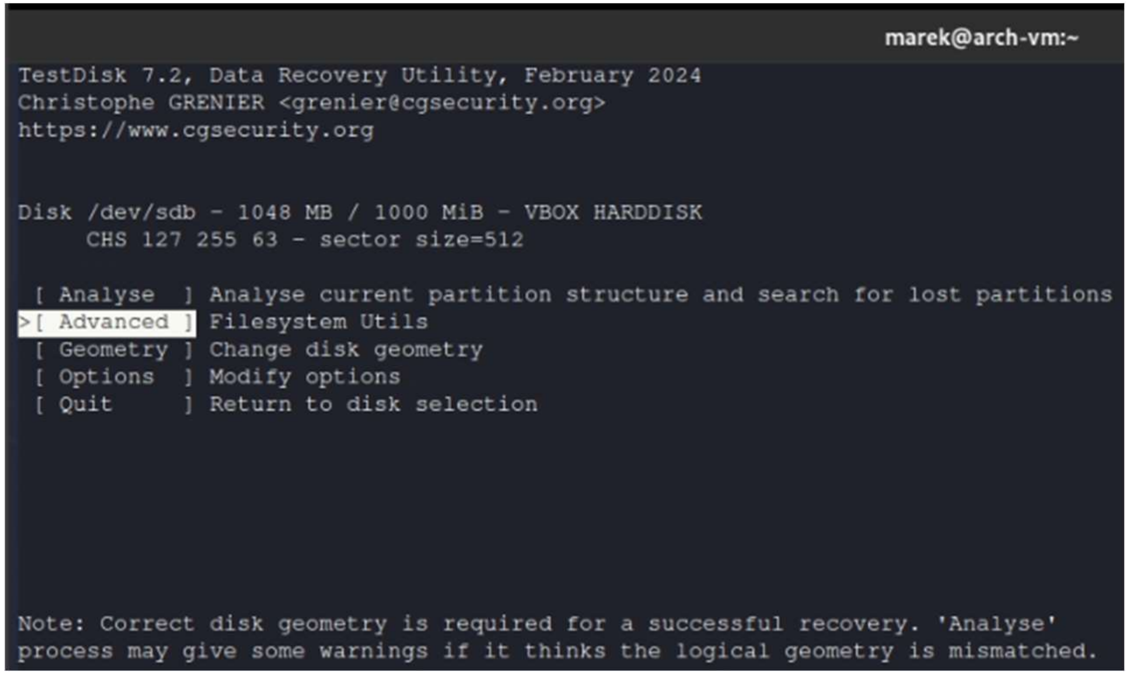
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
 [ Append ] Append information to log file
 [ No Log ] Don't record anything
```



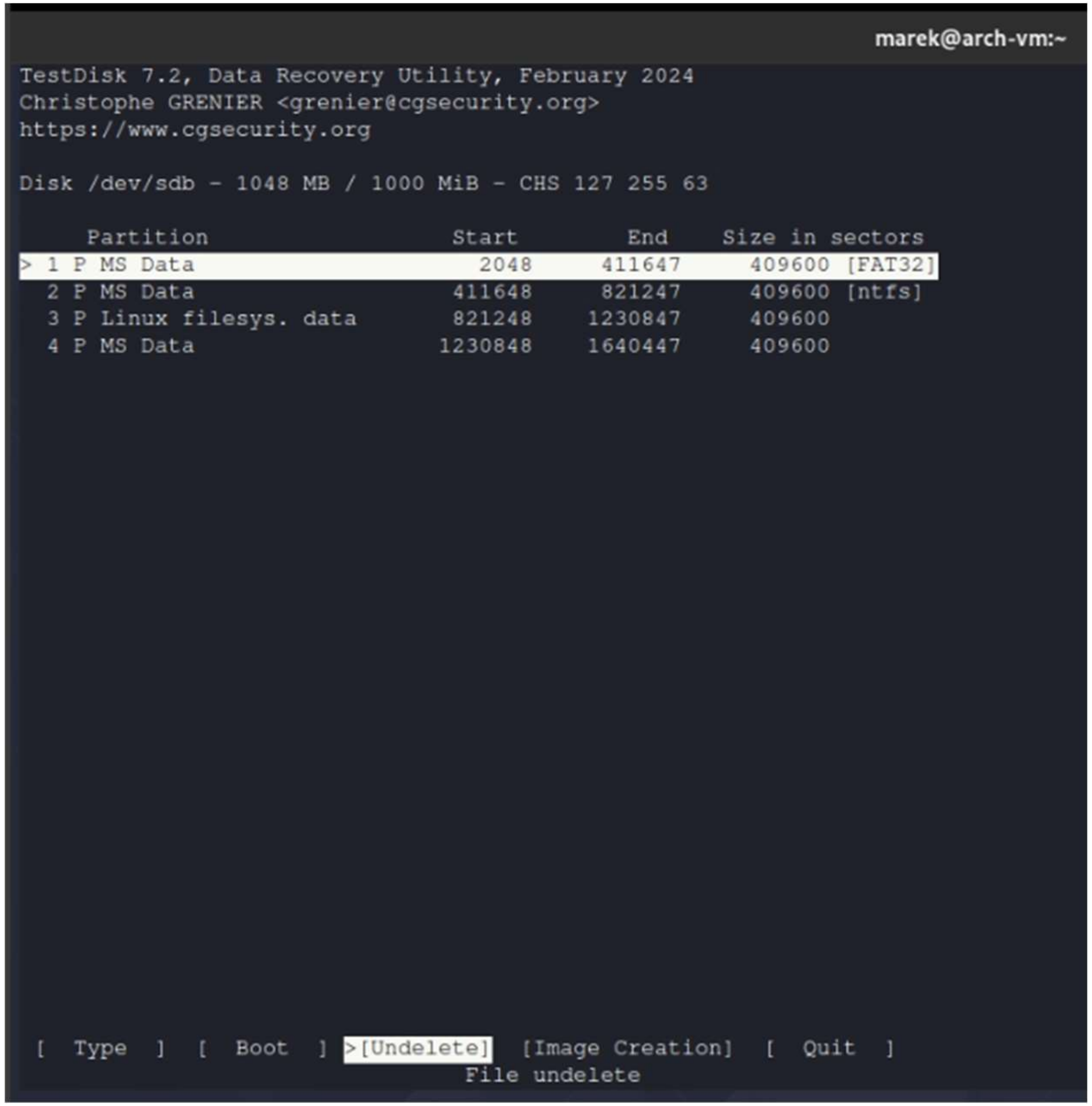
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  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.
```



```
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'.
```

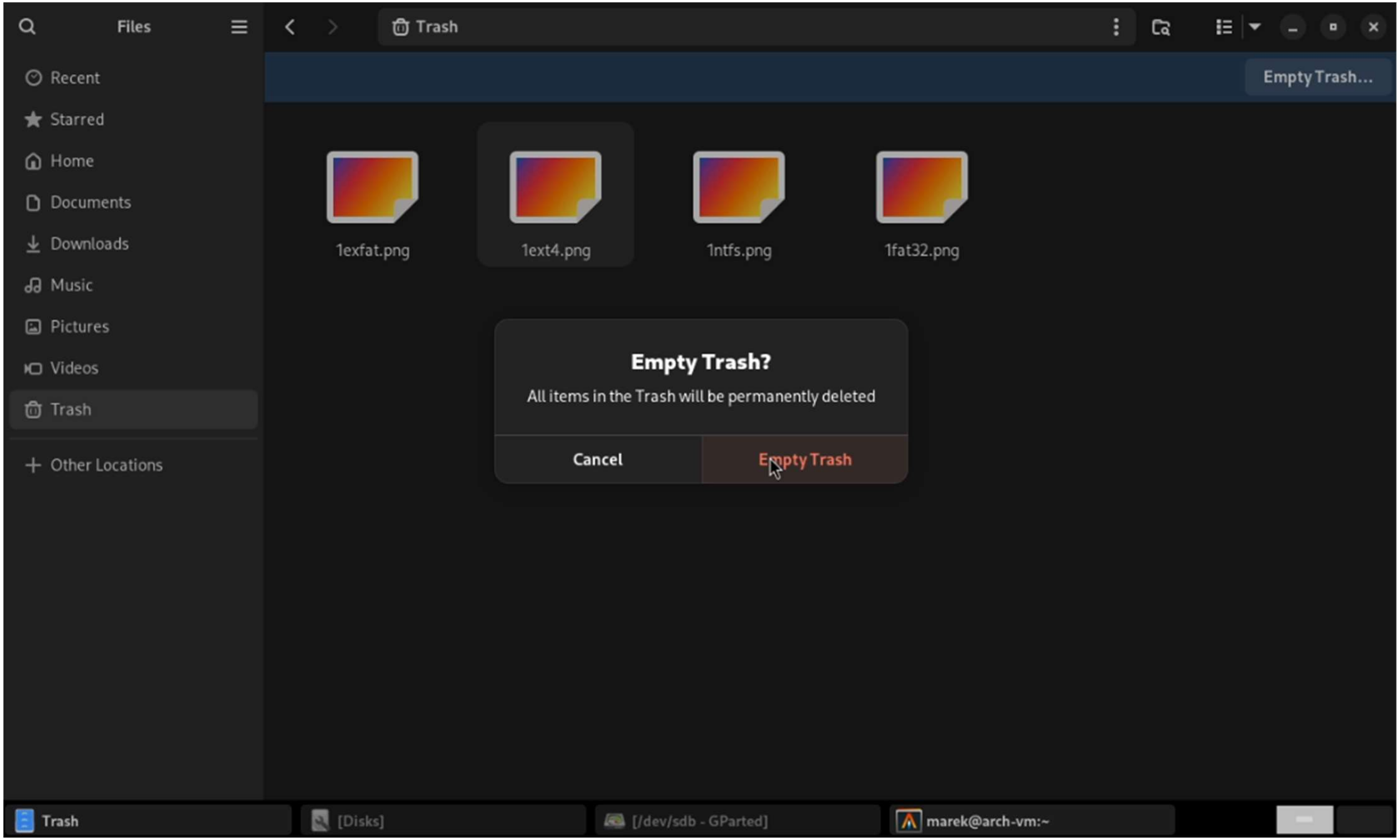


```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk /dev/sdb - 1048 MB / 1000 MiB - VBOX HARDDISK
     CHS 127 255 63 - sector size=512

 [ Analyse  ] Analyse current partition structure and search for lost partitions
>[ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ 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.
```



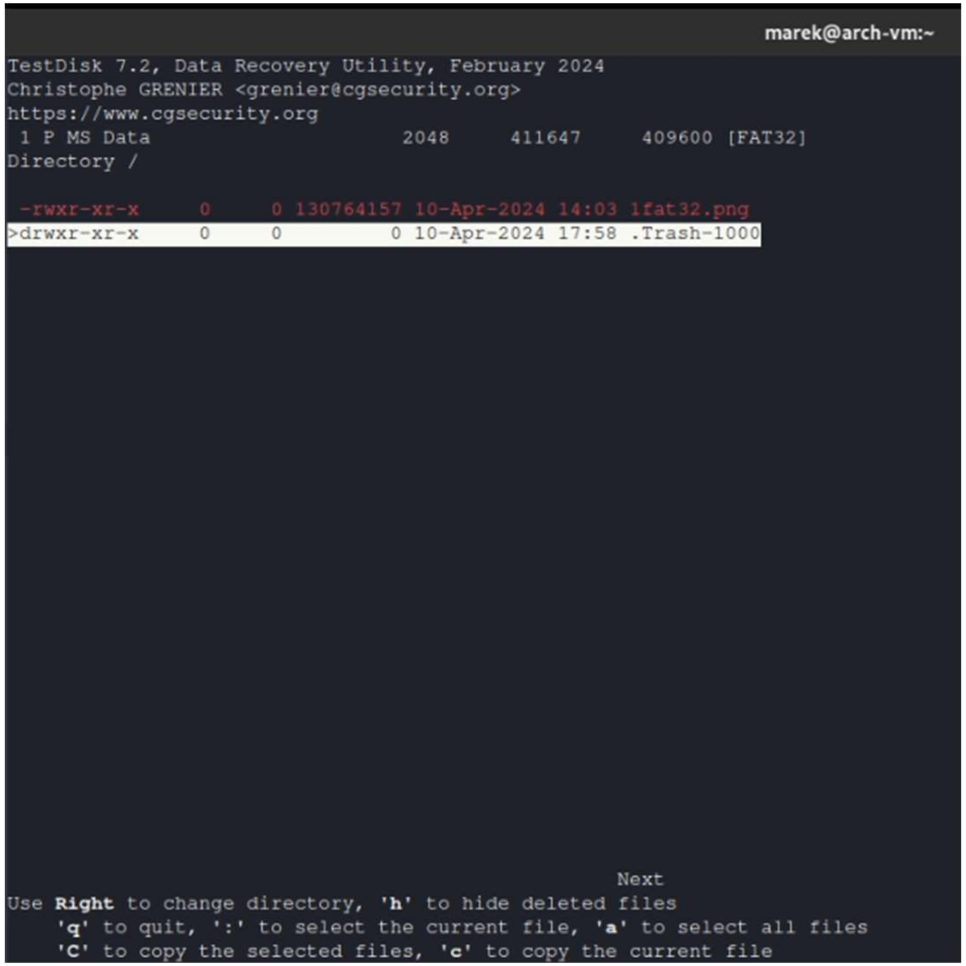
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

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 filesys. data      821248    1230847     409600
  4 P MS Data                 1230848    1640447     409600
```

[Type] [Boot] >[Undelete] [Image Creation] [Quit]
File undelete

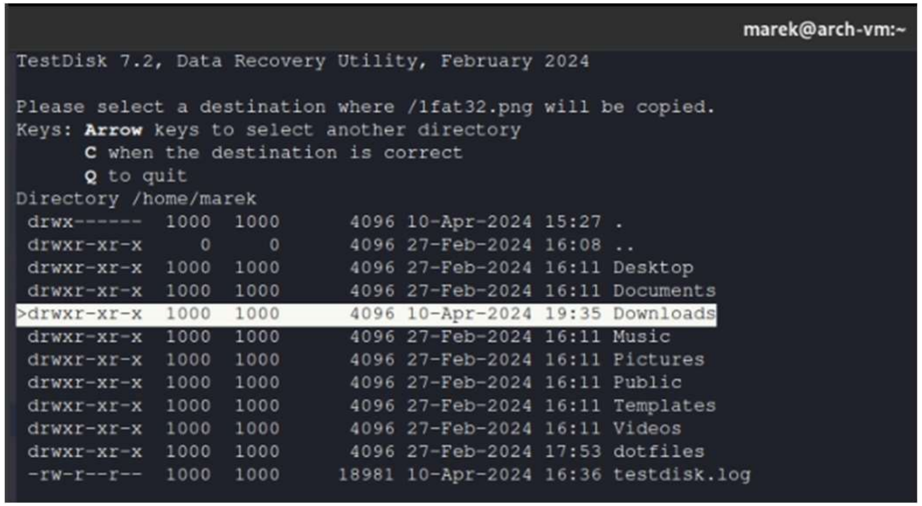


Empty Trash?

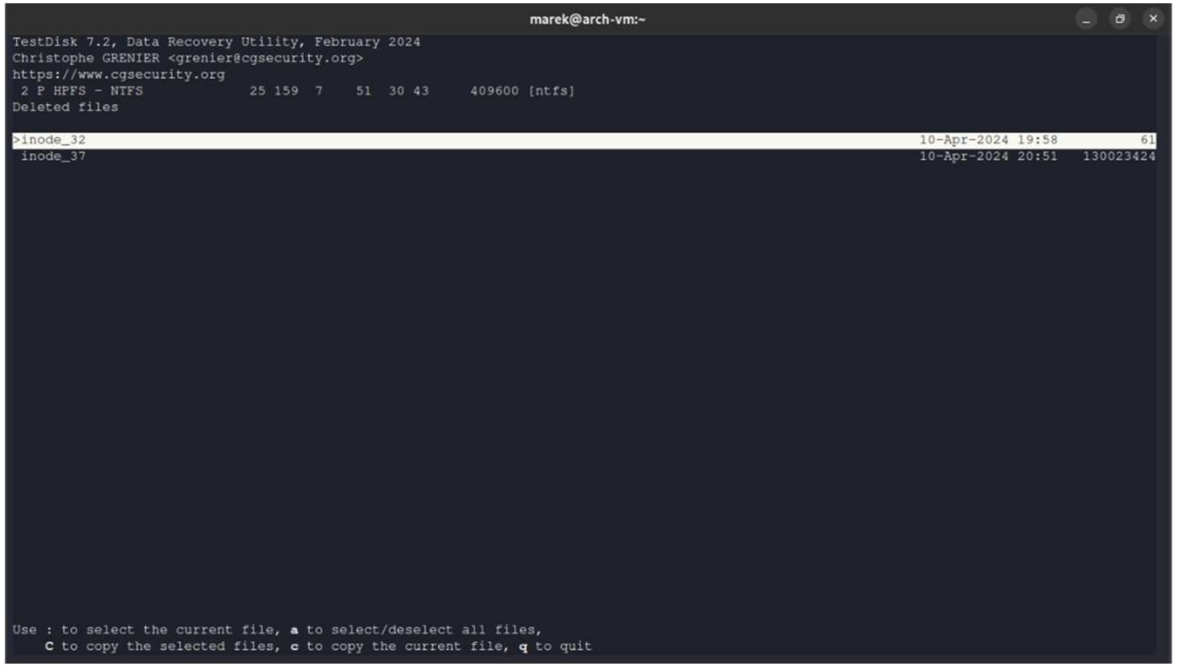
All items in the Trash will be permanently deleted



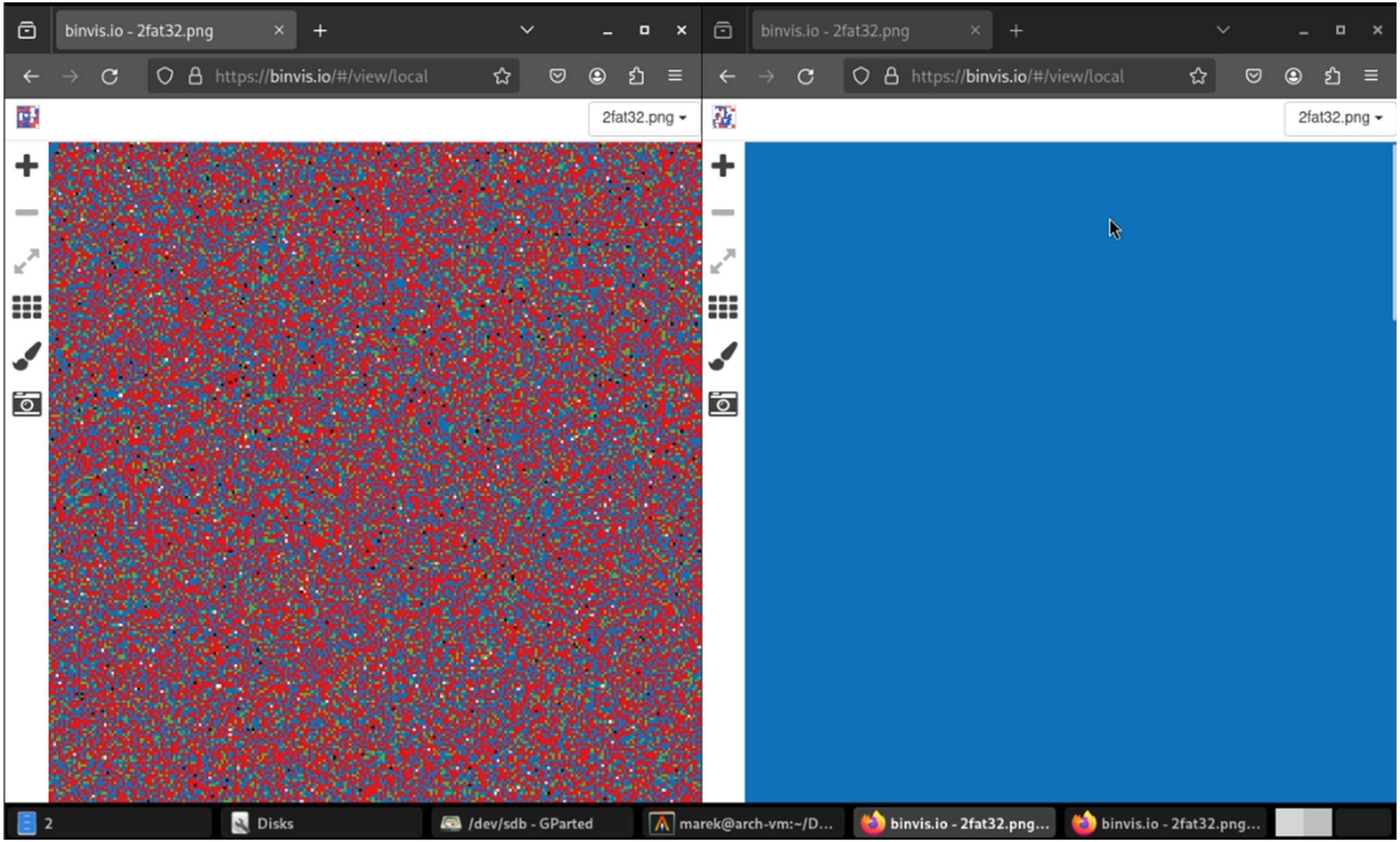
```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
 1 P MS Data                     2048     411647     409600 [FAT32]
Directory /

 -rwxr-xr-x     0     0 130764157 10-Apr-2024 14:03 1fat32.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
```

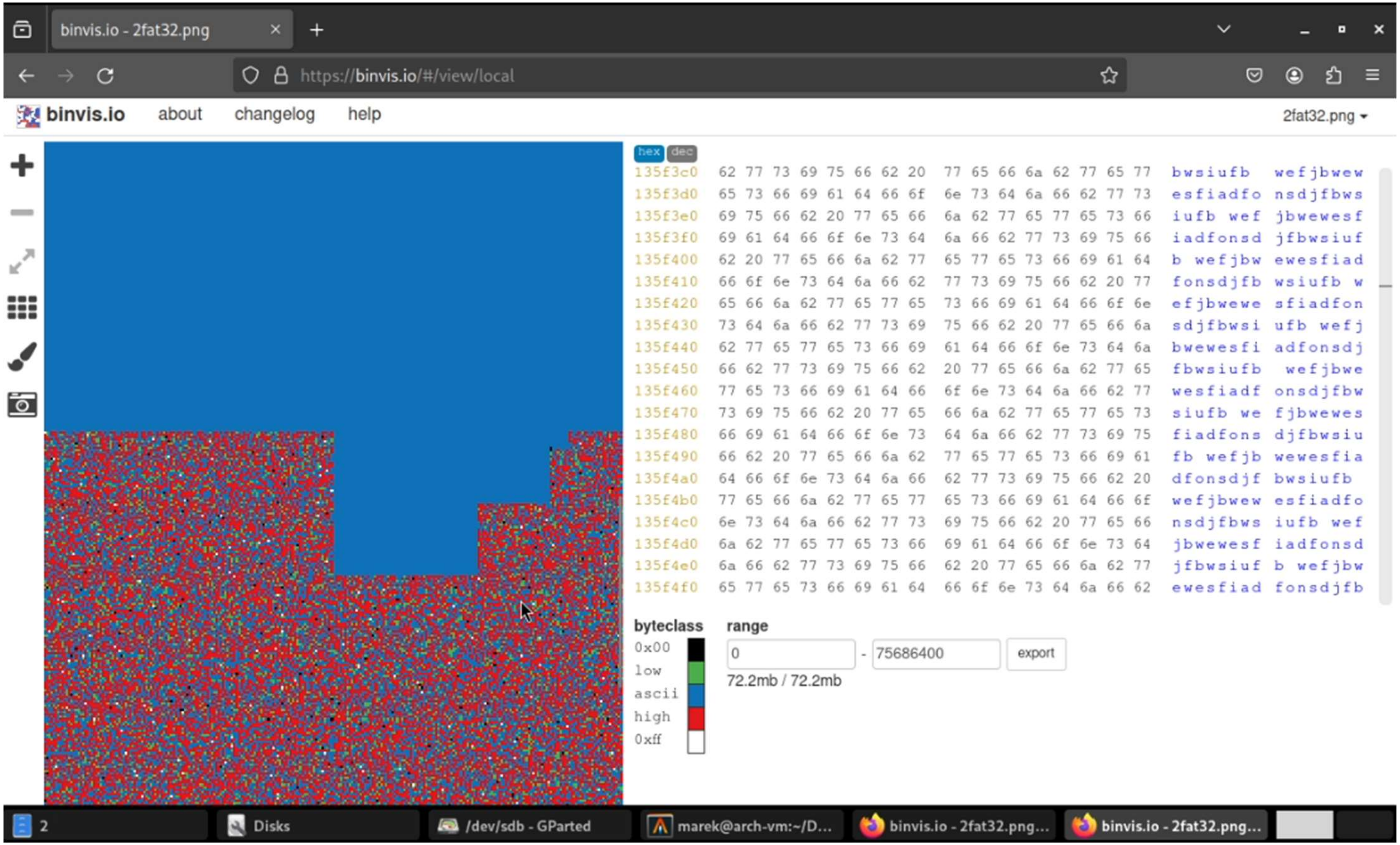


```
TestDisk 7.2, Data Recovery Utility, February 2024

Please select a destination where /1fat32.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
```



```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
 2 P HPFS - 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




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
```


binvis.io - 2fat32.png
https://binvis.io/#/view/local
2fat32.png
binvis.io - 2fat32.png
https://binvis.io/#/view/local
2fat32.png
2
Disks
/dev/sdb - GParted
marek@arch-vm:~/D...
binvis.io - 2fat32.png...
binvis.io - 2fat32.png...



```
135f3c0  62 77 73 69 75 66 62 20  77 65 66 6a 62 77 65 77  bwsiufb  wefjbwew
135f3d0  65 73 66 69 61 64 66 6f  6e 73 64 6a 66 62 77 73  esfiadfo nsdjfbws
135f3e0  69 75 66 62 20 77 65 66  6a 62 77 65 77 65 73 66  iufb wef jbwewesf
135f3f0  69 61 64 66 6f 6e 73 64  6a 66 62 77 73 69 75 66  iadfonsd jfbwsiuf
135f400  62 20 77 65 66 6a 62 77  65 77 65 73 66 69 61 64  b wefjbw ewesfiad
135f410  66 6f 6e 73 64 6a 66 62  77 73 69 75 66 62 20 77  fonsdjfb wsiufb w
135f420  65 66 6a 62 77 65 77 65  73 66 69 61 64 66 6f 6e  efjbwewe sfiadfon
135f430  73 64 6a 66 62 77 73 69  75 66 62 20 77 65 66 6a  sdjfbwsi ufb wefj
135f440  62 77 65 77 65 73 66 69  61 64 66 6f 6e 73 64 6a  bwewesfi adfonsdj
135f450  66 62 77 73 69 75 66 62  20 77 65 66 6a 62 77 65  fbwsiufb  wefjbwe
135f460  77 65 73 66 69 61 64 66  6f 6e 73 64 6a 66 62 77  wesfiadf onsdjfbw
135f470  73 69 75 66 62 20 77 65  66 6a 62 77 65 77 65 73  siufb we fjbwewes
135f480  66 69 61 64 66 6f 6e 73  64 6a 66 62 77 73 69 75  fiadfons djfbwsiu
135f490  66 62 20 77 65 66 6a 62  77 65 77 65 73 66 69 61  fb wefjb wewesfia
135f4a0  64 66 6f 6e 73 64 6a 66  62 77 73 69 75 66 62 20  dfonsdjf bwsiufb 
135f4b0  77 65 66 6a 62 77 65 77  65 73 66 69 61 64 66 6f  wefjbwew esfiadfo
135f4c0  6e 73 64 6a 66 62 77 73  69 75 66 62 20 77 65 66  nsdjfbws iufb wef
135f4d0  6a 62 77 65 77 65 73 66  69 61 64 66 6f 6e 73 64  jbwewesf iadfonsd
135f4e0  6a 66 62 77 73 69 75 66  62 20 77 65 66 6a 62 77  jfbwsiuf b wefjbw
135f4f0  65 77 65 73 66 69 61 64  66 6f 6e 73 64 6a 66 62  ewesfiad fonsdjfb
```

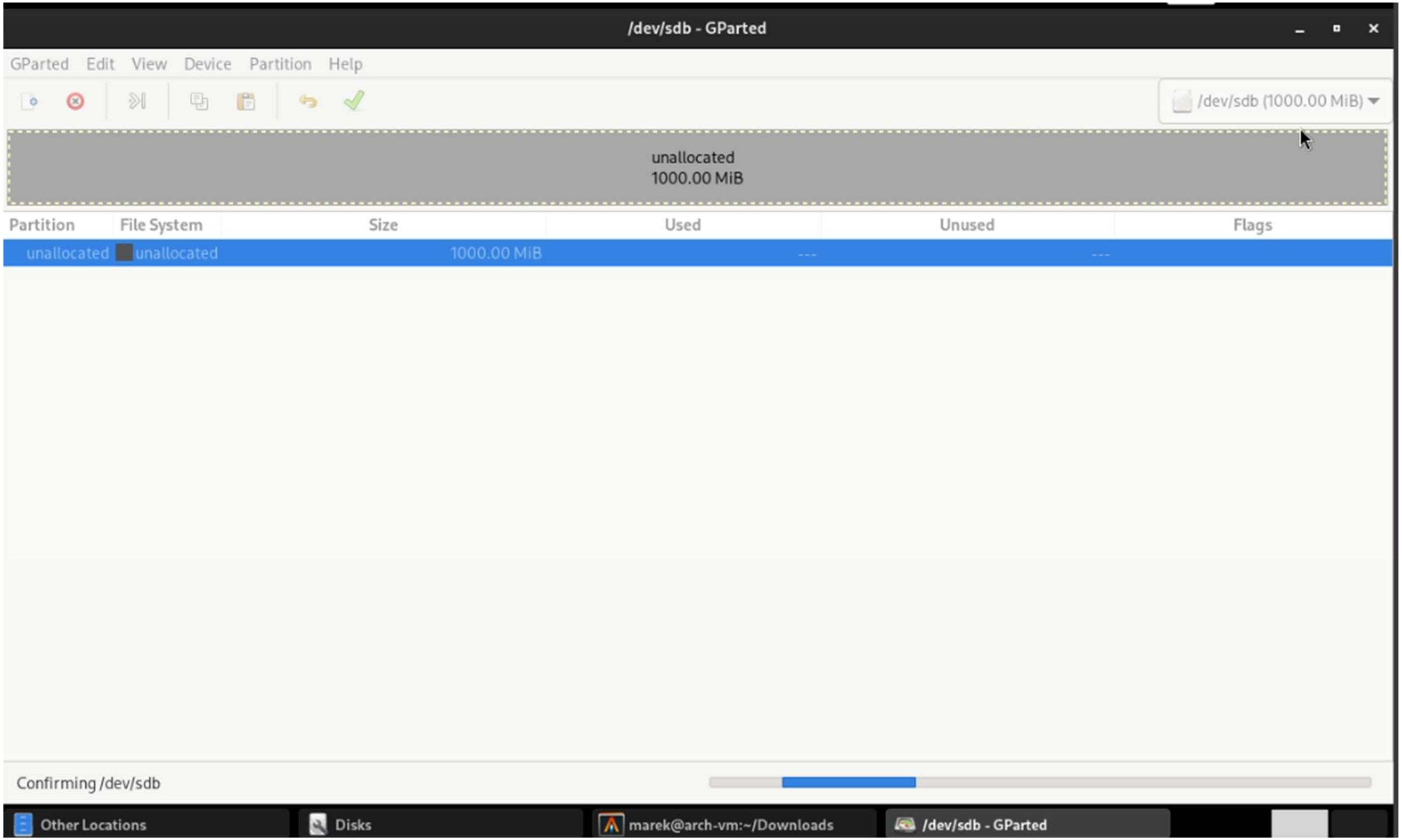
byteclass

0x00	■
low	🟩
ascii	🟦
high	🟥
0xff	□

range

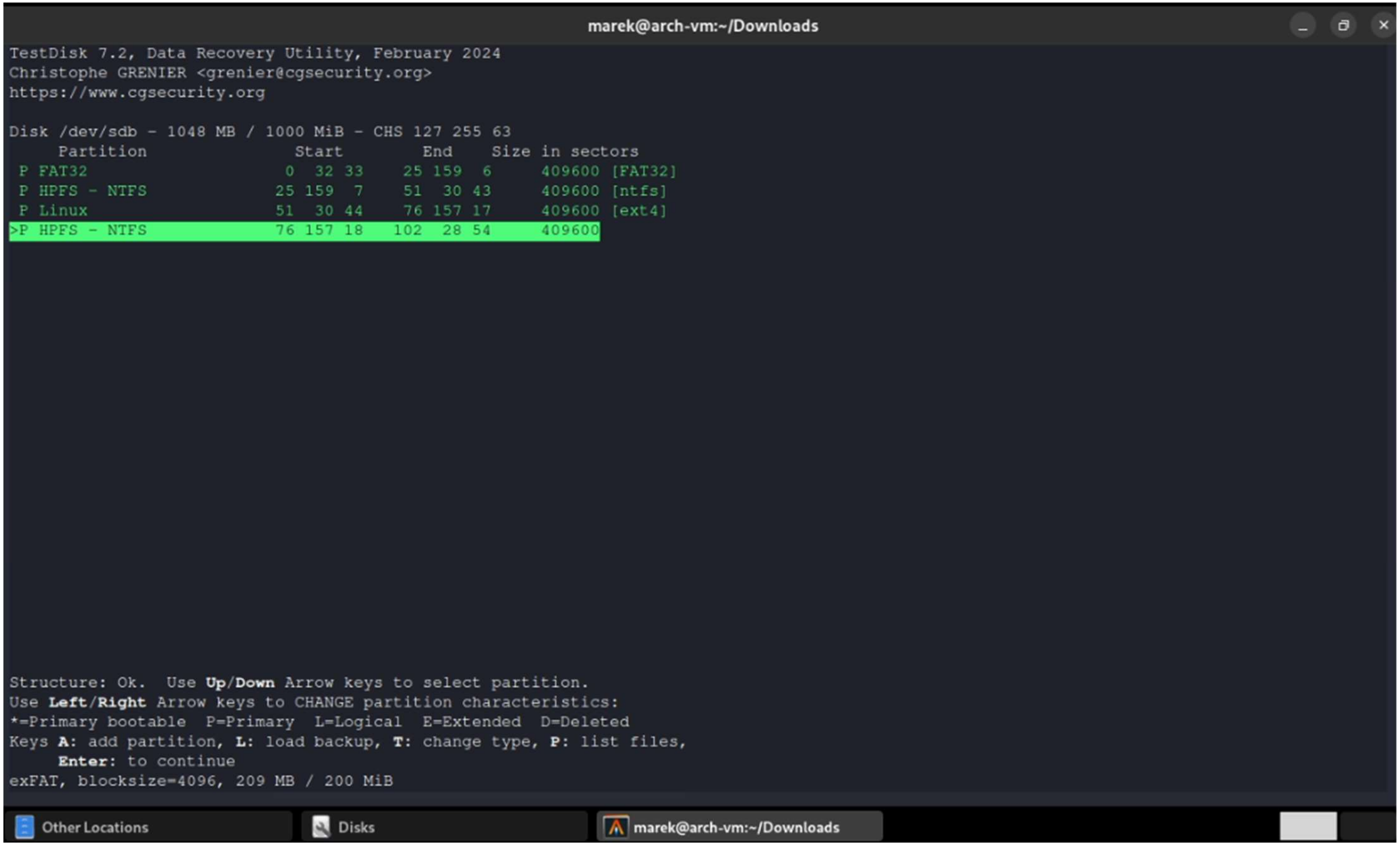
0 - 75686400

72.2mb / 72.2mb



Partition	File System	Size	Used	Unused	Flags
unallocated	■ unallocated	1000.00 MiB	---	---	

Confirming /dev/sdb



```
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
```

Záver

- Podarilo sa mi obnoviť súbory z FAT32, exFAT, NTFS
- Podarilo sa mi obnoviť partície pre všetky súborové systémy

- Nepodarilo sa mi obnoviť súbory z ext4

Ďakujem za pozornosť

Zdroje

- https://www.cgsecurity.org/testdisk_doc/index.html
- https://github.com/cgsecurity/testdisk
- https://www.techradar.com/best/best-data-recovery-software
- Vizualizácia:
- https://binvis.io/#/