

# File-System assignment

## Verifying hashes

Before starting, let's verify the SHA256 hashes of the uncompressed images.

Note: I'm using macOS .

```
shasum -a 256 *.dd

7f9ef6a650c3eda6d6272efaf37bb9d87c234caf27ef1095d89bab93dba44a611 console.dd
44261edf3d078ade9529e995aeeec4614b637bde53c9acb9a0ba070fb13c4b994 corrupted.dd
a1ee435924f28e95807824ae8cb4e8595ffde8539c04b1c6ac68cc0059d207b strange.dd
```

```
shasum -a 256 -c *.sha256

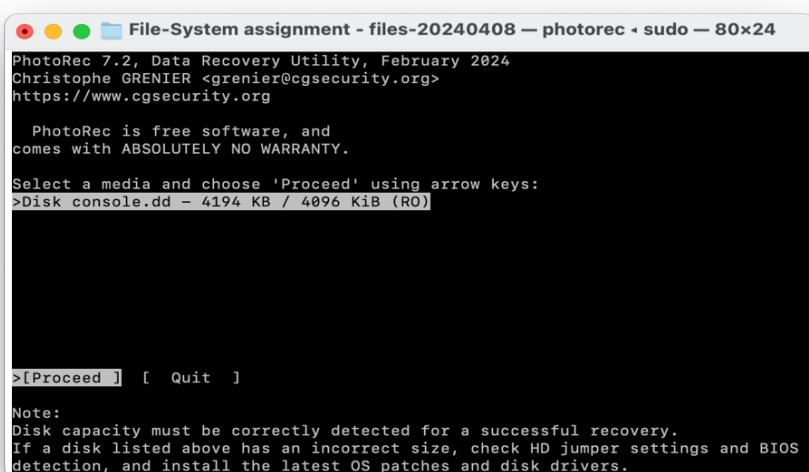
console.dd: OK
corrupted.dd: OK
strange.dd: OK
```

## console.dd

I used [PhotoRec](#) which is a file data recovery software designed to recover lost pictures from digital camera memory or even hard disks.

```
sudo testdisk-7.2/photorec console.dd
```

you shoud run the command as a root user. now we select the .dd image file.



then we choose the whole disk.

```
File-System assignment - files-20240408 — photorec • sudo — 80x24
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk console.dd - 4194 KB / 4096 KiB (R0)

      Partition          Start          End    Size in sectors
>  Unknown              0    0   1    127   1 32        8192 [Whole disk]
     P  FAT12              0    0   1    127   1 32        8192 [NO NAME]

>[ Search ]  [Options]  [File Opt]  [ Quit ]
                                         Start file recovery
```

select other as we know it was in fat format.

```
File-System assignment - files-20240408 — photorec • sudo — 80x24
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

      Unknown          0    0   1    127   1 32        8192 [Whole disk]

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
  [ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other      ] FAT/NTFS/HFS+/ReiserFS/...
```

go to the directory you want to save the found images and click 'c' button on your keyboard to save them.

```
File-System assignment - files-20240408 — photorec • sudo — 80x24
PhotoRec 7.2, Data Recovery Utility, February 2024

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /Users/e/Desktop/UNIGE/Digital Forensics/File-System assignment - files-20240408
>drwx----- 501 20 576 2-May-2024 09:26 .
drwxr-xr-x 501 20 224 8-Apr-2024 20:55 ..
drwxr-xr-x 0 20 96 2-May-2024 09:22 recuper_dir.1
drwxr-xr-x 0 20 160 2-May-2024 09:22 recuper_dir.2
drwxr-xr-x 501 20 640 2-May-2024 09:14 testdisk-7.2
-rw-rw-r-- 501 20 4194304 30-Apr-2024 18:33 console.dd
-rw-rw-r-- 501 20 77 3-Apr-2024 19:10 console.dd.sha256
-rw-rw-r-- 501 20 1476608 30-Apr-2024 18:35 corrupted.dd
-rw-rw-r-- 501 20 79 3-Apr-2024 19:10 corrupted.dd.sha256
-rw-r--r-- 501 20 377263 2-May-2024 09:19 image-1.png
-rw-r--r-- 501 20 333796 2-May-2024 09:26 image-2.png
-rw-r--r-- 501 20 339680 2-May-2024 09:25 image.png
-rw-r--r-- 0 20 40960 2-May-2024 09:23 photorec.se2
-rw-r--r-- 501 20 2367 3-Apr-2024 19:10 readme.txt
Next
```

```
File-System assignment - files-20240408 — photorec • sudo — 80x24
PhotoRec 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk console.dd - 4194 KB / 4096 KiB (R0)
  Partition          Start          End    Size in sectors
  Unknown            0            127    1 32        8192 [Whole disk]

2 files saved in /Users/e/Desktop/UNIGE/Digital Forensics/File-System assignment
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

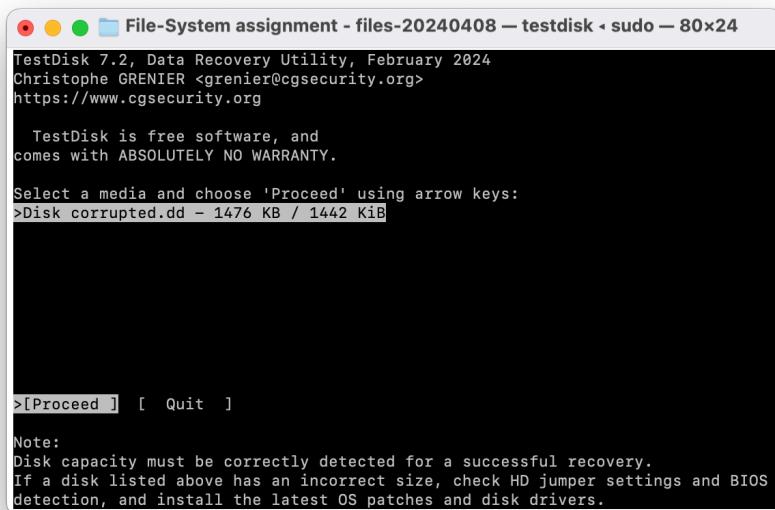
We found two images:



## corrupted.dd

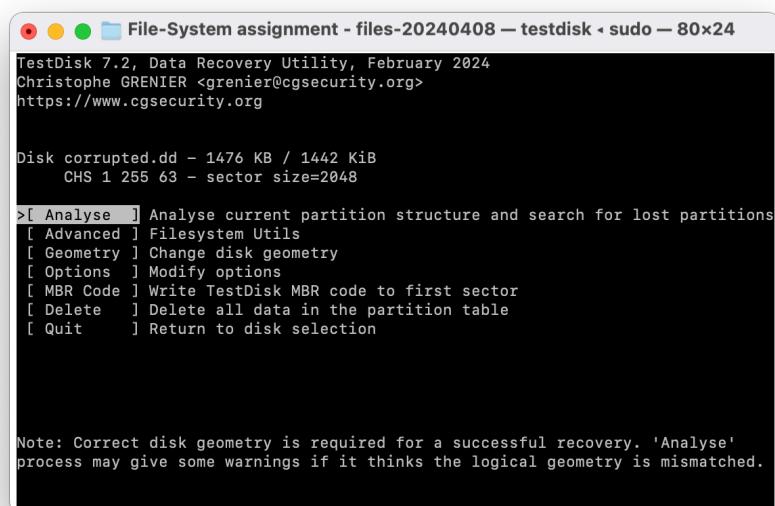
We use [TestDisk](#) to open this file. TestDisk checks the partition and boot sectors of your disks. It is very useful in recovering lost partitions.

**Command:** sudo testdisk-7.2/testdisk corrupted.dd



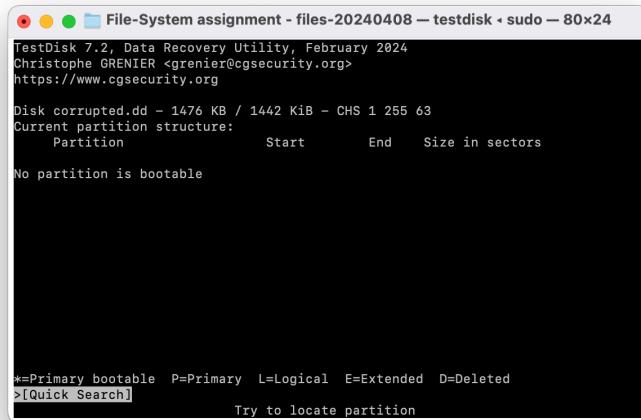
The screenshot shows the TestDisk 7.2 interface. At the top, it displays the version information: "TestDisk 7.2, Data Recovery Utility, February 2024" and the author's name: "Christophe GRENIER <cgrenier@cgsecurity.org>". Below this, a URL is provided: "https://www.cgsecurity.org". A note follows: "TestDisk is free software, and comes with ABSOLUTELY NO WARRANTY." The main menu prompt is "Select a media and choose 'Proceed' using arrow keys:". The current selection is highlighted: ">Disk corrupted.dd - 1476 KB / 1442 KiB". At the bottom of the screen, there are two options: "[Proceed]" and "[Quit]". A note at the bottom states: "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."

Proceed with the disk, select Intel and then select Analyse:



The screenshot shows the TestDisk 7.2 interface after selecting the disk. It displays the disk information: "Disk corrupted.dd - 1476 KB / 1442 KiB" and "CHS 1 255 63 - sector size=2048". Below this, the "Analys" command is selected, and the menu options are listed: "[Analyse]", "[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]", and "[Quit]". A note at the bottom states: "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 will show if there are any partitions.



The screenshot shows the TestDisk 7.2 interface. The title bar reads "File-System assignment - files-20240408 — testdisk « sudo — 80x24". The main window displays the following text:

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

Disk corrupted.dd - 1476 KB / 1442 KiB - CHS 1 255 63
Current partition structure:
  Partition          Start          End    Size in sectors
No partition is bootable

*=Primary bootable  P=Primary  L=Logical  E=Extended  D=Deleted
>[Quick Search]      Try to locate partition
```

There is no partition found. Now for a detailed analysis of the FAT file system, we use [The Sleuth Kit \(TSK\)](#). It does not require mounting the disk image and works directly with the disk data, which can also prevent accidental writes or changes.

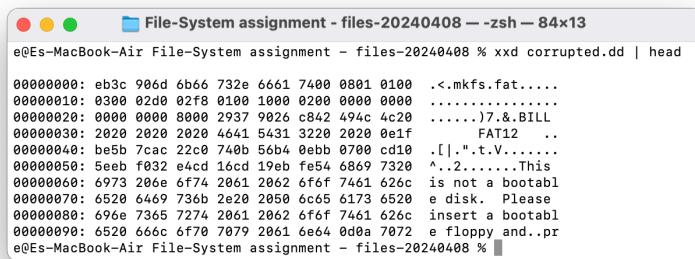
**Command:** mmls corrupted.dd

This command lists the partition layout of the disk image.

However, we don't get any results. This suggests that either the disk image doesn't contain any partitions or the partition table itself may be damaged.

Let's investigate our file some more:

**Command:** xxd corrupted.dd | head



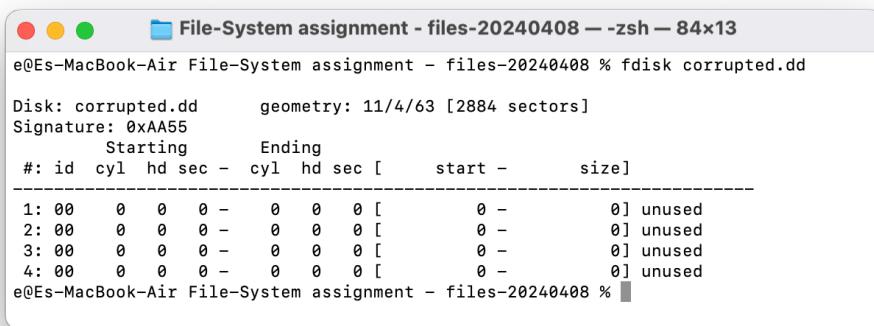
The terminal window title is "File-System assignment - files-20240408 — zsh — 84x13". The command run is "e@Es-MacBook-Air File-System assignment - files-20240408 % xxd corrupted.dd | head". The output shows the raw hex dump of the file, with the last few lines being:

```
00000060: 6973 2066 6774 2061 2061 2062 6f6f 7461 626c is not a bootabl
00000068: 6520 6469 736b 2e20 2050 6c65 6173 6520 e disk. Please
00000070: 696e 7365 7274 2061 2062 6f6f 7461 626c insert a bootabl
00000078: 6520 666c 6f70 7079 2061 6e64 0d0a 7072 e floppy and..pr
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

We used **xxd** to view the first few bytes of the image and found some clues!

1. **Volume Name:** The text "....7.8.BILL" might be part of the volume label. Volume labels can be up to 11 characters long in FAT file systems and typically start at byte offset 43 in the boot sector.
  2. **File System Type:** The string "FAT12" is indicating that the file system type of the disk image is FAT12.
  3. **Non-Executable Warning:** The message "This is not a bootable disk. Please insert a bootable floppy and press any key to try again." is common in disk images that are formatted but not made bootable.
- 

**Command:** fdisk corrupted.dd



```
File-System assignment - files-20240408 --zsh -- 84x13
e@Es-MacBook-Air File-System assignment - files-20240408 % fdisk corrupted.dd

Disk: corrupted.dd      geometry: 11/4/63 [2884 sectors]
Signature: 0xAA55
          Starting     Ending
 #: id  cyl  hd sec [-] cyl  hd sec [      start -      size]
 * 1: 00    0    0   0 -    0    0   0 [           0 -           0] unused
   2: 00    0    0   0 -    0    0   0 [           0 -           0] unused
   3: 00    0    0   0 -    0    0   0 [           0 -           0] unused
   4: 00    0    0   0 -    0    0   0 [           0 -           0] unused
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

---

Looks like the file is damaged so let's try and fix it using TestDisk.

Select None in the picture below.

File-System assignment - files-20240408 - testdisk - sudo - 102x29

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

Disk corrupted.dd - 1476 KB / 1442 KiB

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

Note: Do NOT select 'None' for media with only a single partition. It's very rare for a disk to be 'Non-partitioned'.

And then press enter on your screen to move on:

File-System assignment - files-20240408 - testdisk - sudo - 102x29

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

Disk corrupted.dd - 1476 KB / 1442 KiB - CHS 23 2 16

Partition	Start	End	Size in sectors
> P Unknown	0	1	22 1 1 721

>[ Type ] [Image Creation] [ Quit ]  
Change type, this setting will not be saved on disk

Choose FAT12 and proceed:

File-System assignment - files-20240408 - testdisk - sudo - 102x29

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

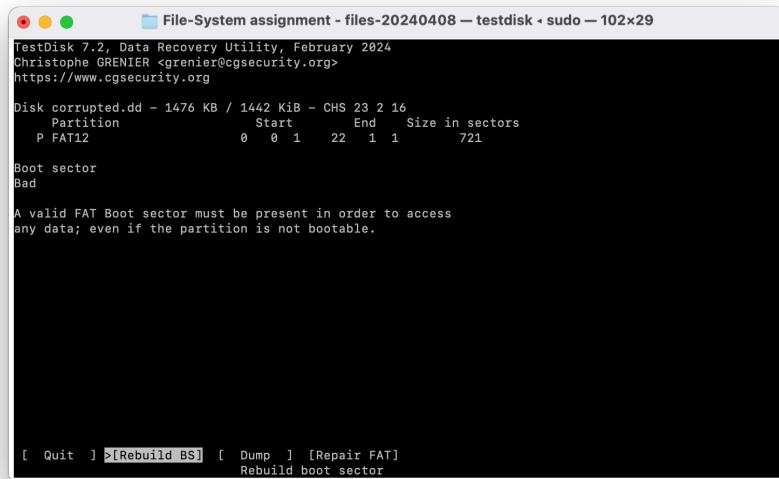
P Unknown 0 0 1 22 1 1 721

Please choose the partition type, press Enter when done.

Unknown	HFS	Linux md 1.x RAID
APFS	HFS+	Netware
BeFS	HFSX	NTFS
btrfs	HFS+	OpenBSD
CramFS	ISO	OS2 Multiboot
ext2	JFS	ReFS
ext3	Linux SWAP	ReiserFS 3.5
ext4	Linux SWAP 2	ReiserFS 3.6
>FAT12	Linux SWAP	ReiserFS 3.x
FAT16	Linux SWAP 2	Sun
FAT32	Linux LUKS	SysV 4
FreeBSD	Linux LVM	UFS
f2fs	Linux LVM2	UFS 2
GFS2	Linux md 0.9 RAID	UFS – Little Endian

[ Proceed ]

We tried repairing FAT and rebuilding BS but didn't get any result.



File-System assignment - files-20240408 - testdisk - sudo - 102x29

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

Disk corrupted.dd - 1476 KB / 1442 KiB - CHS 23 2 16

Partition	Start	End	Size in sectors
P FAT12	0	1	22
	1	1	721

Boot sector  
Bad

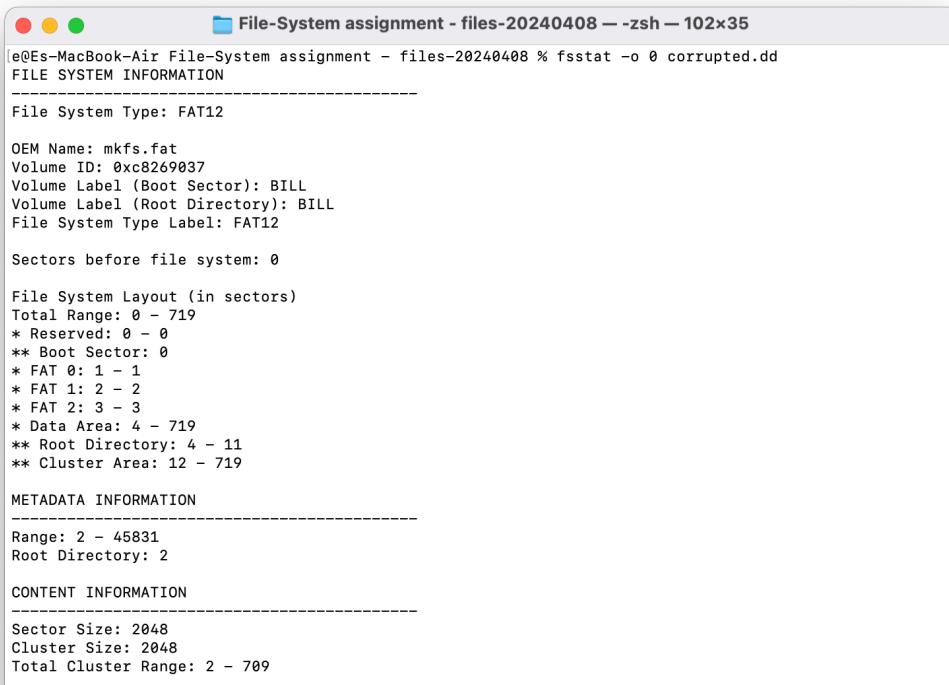
A valid FAT Boot sector must be present in order to access any data; even if the partition is not bootable.

[ Quit ] >[Rebuild BS] [ Dump ] [Repair FAT]  
Rebuild boot sector

---

We use another command called **fsstat**. This will display the details associated with a file system.

**Command:** fsstat -o 0 corrupted.dd



```
e@Es-MacBook-Air:~/File-System assignment - files-20240408 % fsstat -o 0 corrupted.dd
```

FILE SYSTEM INFORMATION

---

File System Type: FAT12

OEM Name: mkfs.fat  
Volume ID: 0xc8269037  
Volume Label (Boot Sector): BILL  
Volume Label (Root Directory): BILL  
File System Type Label: FAT12

Sectors before file system: 0

File System Layout (in sectors)  
Total Range: 0 - 719  
\* Reserved: 0 - 0  
\*\* Boot Sector: 0  
\* FAT 0: 1 - 1  
\* FAT 1: 2 - 2  
\* FAT 2: 3 - 3  
\* Data Area: 4 - 719  
\*\* Root Directory: 4 - 11  
\*\* Cluster Area: 12 - 719

METADATA INFORMATION

---

Range: 2 - 45831  
Root Directory: 2

CONTENT INFORMATION

---

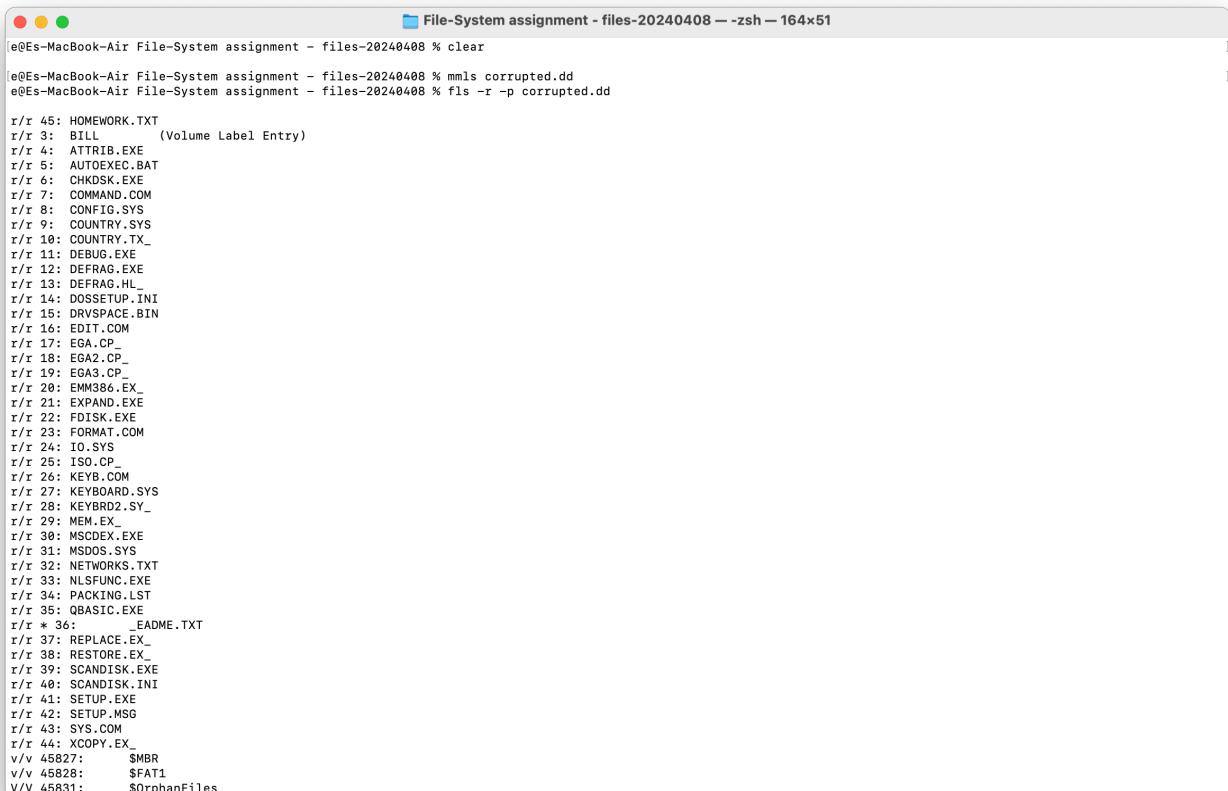
Sector Size: 2048  
Cluster Size: 2048  
Total Cluster Range: 2 - 709

So we finally have some answers:

1. **What is the volume label?** The volume label is **BILL** in the Boot Sector and the Root Directory.
  2. **What is the sector size?** The sector size is **2048 bytes**.
  3. **What is the cluster size?** The cluster size is also **2048 bytes**.
  4. **How many FAT tables are present?** There are **3 FAT tables** present (FAT 0, FAT 1, and FAT 2)
- 

**Command:** fls -r -p corrupted.dd

This command recursively lists files and paths, including deleted files (-r for recursive, -p to display full path).



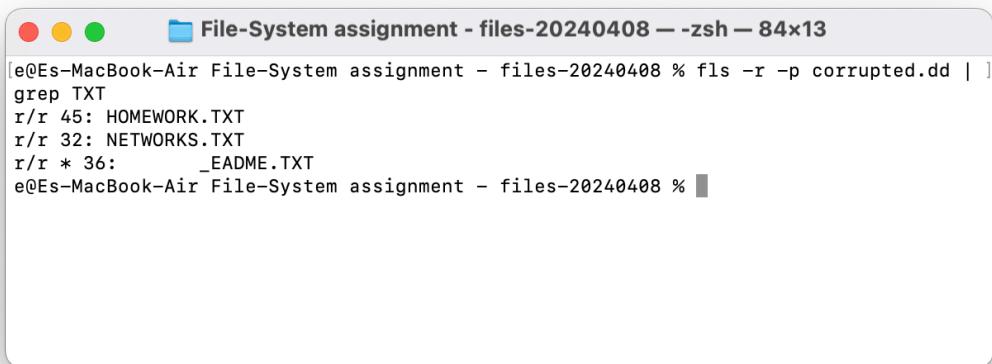
The screenshot shows a terminal window titled "File-System assignment - files-20240408 --zsh -- 164x51". The terminal output is as follows:

```
File-System assignment - files-20240408 --zsh -- 164x51
e0Es-MacBook-Air File-System assignment - files-20240408 % clear
e0Es-MacBook-Air File-System assignment - files-20240408 % mmls corrupted.dd
e0Es-MacBook-Air File-System assignment - files-20240408 % fls -r -p corrupted.dd

r/r 45: HOMEWORK.TXT
r/r 3: BILL          (Volume Label Entry)
r/r 4: ATTRIB.EXE
r/r 5: AUTOEXEC.BAT
r/r 6: CHDKSK.EXE
r/r 7: COMMAND.COM
r/r 8: CONFIG.SYS
r/r 9: COUNTRY.SYS
r/r 10: COUNTRY.TX_
r/r 11: DEBUG.EXE
r/r 12: DEFRAG.EXE
r/r 13: DEFrag.HL_
r/r 14: DOSSETUP.INI
r/r 15: DRVSPACE.BIN
r/r 16: EDIT.COM
r/r 17: EGA.CP_
r/r 18: EGA2.CP_
r/r 19: EGAG.CP_
r/r 20: EMM386.EX_
r/r 21: EXPAND.EXE
r/r 22: FDISK.EXE
r/r 23: FORMAT.COM
r/r 24: IO.SYS
r/r 25: ISO.CP_
r/r 26: KEYB.COM
r/r 27: KEYBOARD.SYS
r/r 28: KEYBRD2.SY_
r/r 29: MEM.EX_
r/r 30: MSCDEX.EXE
r/r 31: MSDOS.SYS
r/r 32: NETWORKS.TXT
r/r 33: NLSFUNC.EXE
r/r 34: PACKING.LST
r/r 35: QBASIC.EXE
r/r * 36: _EADME.TXT
r/r 37: REPLACE.EX_
r/r 38: RESTORE.EX_
r/r 39: SCANDISK.EXE
r/r 40: SCANDISK.INI
r/r 41: SETUP.EXE
r/r 42: SETUP.MSG
r/r 43: SYS.COM
r/r 44: XCOPY.EX_
v/v 45827:      $MBR
v/v 45828:      $FAT1
V/V 45831:      $OrphanFiles
```

We use grep to only get the files with .txt extention.

**Command:** fls -r -p corrupted.dd | grep TXT



```
[e@Es-MacBook-Air File-System assignment - files-20240408 % fls -r -p corrupted.dd | ]
grep TXT
r/r 45: HOMEWORK.TXT
r/r 32: NETWORKS.TXT
r/r * 36: _EADME.TXT
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

**Extracting HOMEWORK.TXT:**

**Command:** icat -o 0 corrupted.dd 45 > HOMEWORK.TXT

This command extracts the file with inode number 45 and redirects the output to a file named HOMEWORK.TXT.

This file contains 'zxgio' string!

**Extracting NETWORKS.TXT:**

**Command:** icat -o 0 corrupted.dd 32 > NETWORKS.TXT

**Extracting \_EADME.TXT (Deleted File):**

Command: icat -o 0 corrupted.dd 36 > \_EADME.TXT

## Finding 'zxgio' String Occurrences

we can use the **grep** command to search for strings within the disk image:

**Command:** grep -ao 'zxgio' corrupted.dd

- **-a** treats the binary file as text.
- **-o** shows only the matched parts.
- **-b** outputs the byte offset.



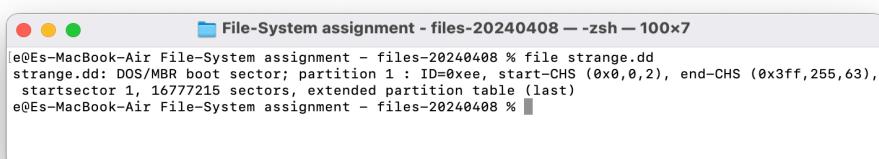
```
File-System assignment - files-20240408 -- zsh -- 90x6
[e@Es-MacBook-Air File-System assignment - files-20240408 % grep -ao 'zxgio' corrupted.dd ]
724025:zxgio
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

For each occurrence, use **istat** in TSK to determine if the byte offset falls within a file, unused space, or slack space.

## strange.dd

**Partition Scheme:**

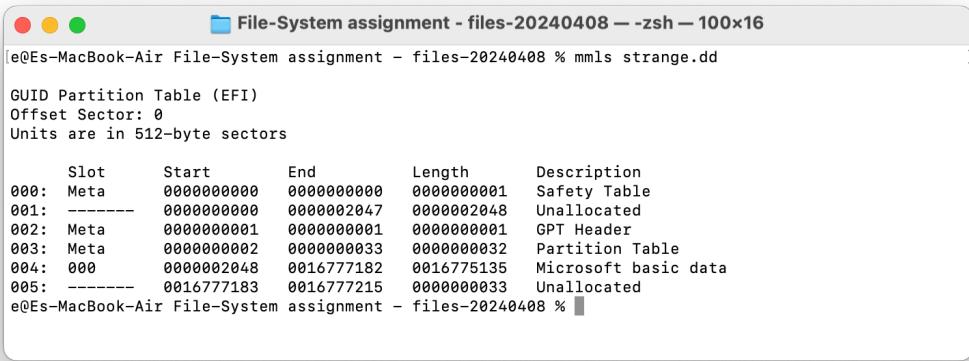
**Command:** file strange.dd



```
File-System assignment - files-20240408 -- zsh -- 100x7
[e@Es-MacBook-Air File-System assignment - files-20240408 % file strange.dd ]
strange.dd: DOS/MBR boot sector; partition 1 : ID=0xee, start-CHS (0x0,0,2), end-CHS (0x3ff,255,63),
startsector 1, 16777215 sectors, extended partition table (last)
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

Using **file** command, we notice the MBR boot sector.

**Command:** mmls strange.dd



```
File-System assignment - files-20240408 --zsh -- 100x16
e@Es-MacBook-Air File-System assignment - files-20240408 % mmls strange.dd

GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

Slot Start End Length Description
000: Meta 0000000000 0000000000 0000000001 Safety Table
001: ----- 0000000000 0000002047 0000002048 Unallocated
002: Meta 0000000001 0000000001 0000000001 GPT Header
003: Meta 0000000002 0000000033 0000000032 Partition Table
004: 000 0000002048 0016777182 0016775135 Microsoft basic data
005: ----- 0016777183 0016777215 0000000033 Unallocated
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

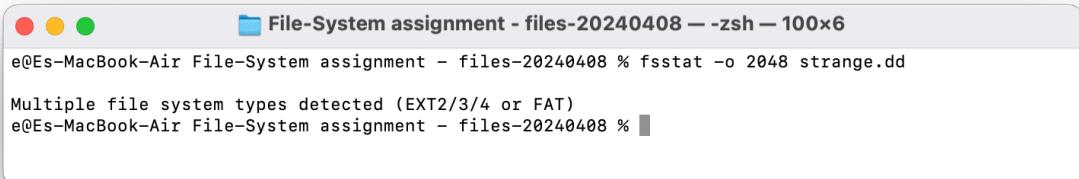
The output indicates that the disk image uses a **GUID Partition Table (GPT)**.

Also, Slot 4 is the First Real Partition. From the **mmls** output, it appears that slot 4 is the first partition designated for storing user data, formatted with a file system recognizable by Windows ("Microsoft basic data").

**Identify the file system type:**

**Command:** fsstat -o 2048 strange.dd

**Note:** The starting sector for slot 4 is 2048 which is why we set it in our command.



```
File-System assignment - files-20240408 --zsh -- 100x6
e@Es-MacBook-Air File-System assignment - files-20240408 % fsstat -o 2048 strange.dd

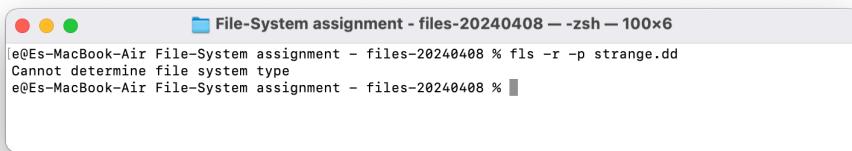
Multiple file system types detected (EXT2/3/4 or FAT)
e@Es-MacBook-Air File-System assignment - files-20240408 %
```

## What is Strange About This Image?

- Large blocks of unallocated space before the start and after the GPT table entries and between defined partitions can be intriguing. This could be wasted space or could contain hidden data.
- The mix of a DOS/MBR boot sector signature along with a GPT partition table can be considered unusual. Typically, GPT does not use a boot sector like MBR.
- Multiple file system types are detected which is strange!

We try to list all the files inside the partition:

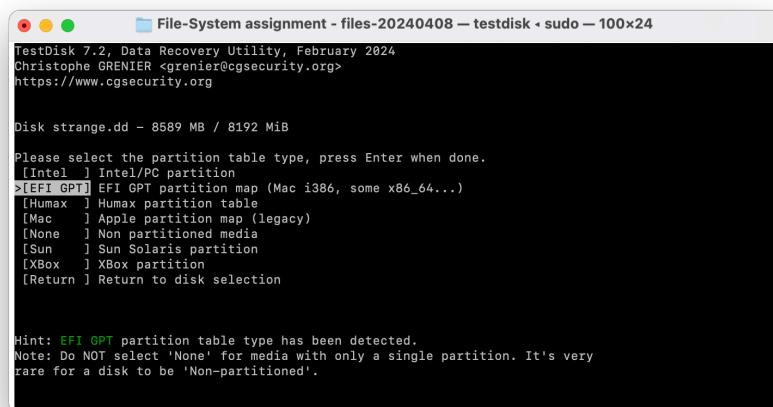
**Command:** `fls -r -p strange.dd`



```
File-System assignment - files-20240408 -- zsh -- 100x6
[e@Es-MacBook-Air File-System assignment - files-20240408 % fls -r -p strange.dd
Cannot determine file system type
e@Es-MacBook-Air File-System assignment - files-20240408 % ]
```

Having multiple types is strange and we can't extract files using previous commands such as **fls** and **icat**. So let's try a different method and open the image using **TestDisk**.

**Command:** `sudo ./testdisk-7.2/testdisk strange.dd`



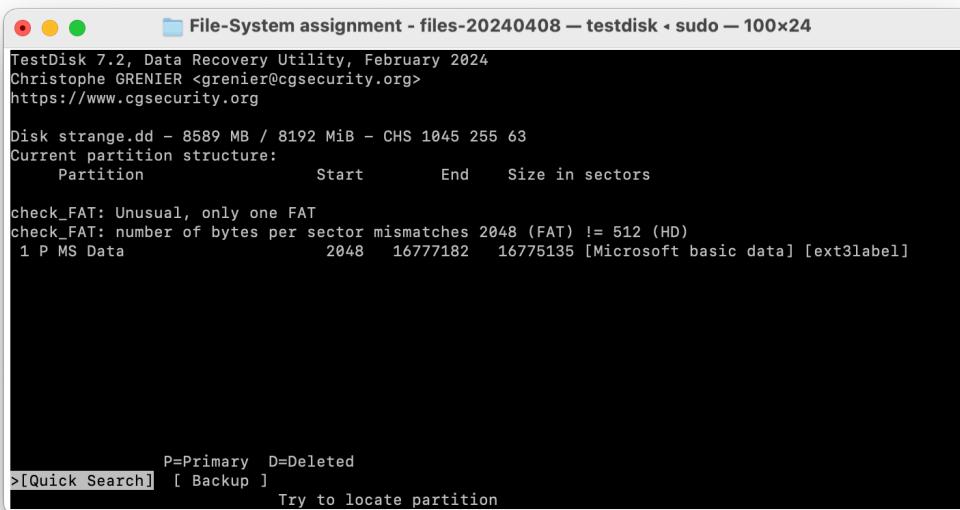
```
File-System assignment - files-20240408 -- testdisk - sudo - 100x24
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk strange.dd - 8589 MB / 8192 MiB

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...)
[Human] Human 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'.
```

Choose GPT and then Analyse.

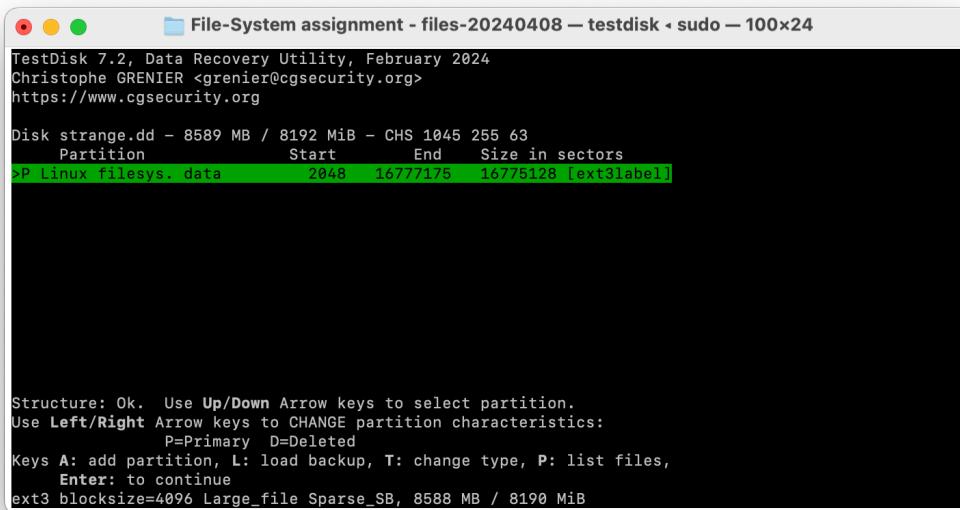


```
File-System assignment - files-20240408 — testdisk — sudo — 100x24
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <cgsecurity.org>
https://www.cgsecurity.org

Disk strange.dd - 8589 MB / 8192 MiB - CHS 1045 255 63
Current partition structure:
  Partition          Start        End    Size in sectors
check_FAT: Unusual, only one FAT
check_FAT: number of bytes per sector mismatches 2048 (FAT) != 512 (HD)
  1 P MS Data           2048   16777182   16775135 [Microsoft basic data] [ext3label]

P=Primary  D=Deleted
>[Quick Search]  [ Backup ]
Try to locate partition
```

Select Quick Search and press **Enter**. it recognizes only one partition:



```
File-System assignment - files-20240408 — testdisk — sudo — 100x24
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <cgsecurity.org>
https://www.cgsecurity.org

Disk strange.dd - 8589 MB / 8192 MiB - CHS 1045 255 63
  Partition          Start        End    Size in sectors
>P Linux file sys. data     2048   16777175   16775128 [ext3label]

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
  P=Primary  D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
      Enter: to continue
ext3 blocksize=4096 Large_file Sparse_SB, 8588 MB / 8190 MiB
```

press P button to see the files:

```
File-System assignment - files-20240408 — testdisk • sudo — 100x24
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <cgrenier@cgsecurity.org>
https://www.cgsecurity.org
P Linux filesystems. data      2048  16777175  16775128 [ext3label]
Directory /

>drwxr-xr-x    0    0      4096 28-Jan-2022 09:42 .
drwxr-xr-x    0    0      4096 28-Jan-2022 09:42 ..
drwx-----    0    0     16384 28-Jan-2022 08:26 lost+found
-rw-r--r--    0    0     314898 28-Jan-2022 09:42 ext3_nashorn_1.jpg
-rw-r--r--    0    0     332534 28-Jan-2022 09:42 ext3_nashorn_2.jpg
-rw-r--r--    0    0     307152 28-Jan-2022 09:42 ext3_nashorn_3.jpg

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
```

We found 3 images. Let's extract them!



