

POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 8	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 28.04.2025	
Data oddania sprawozdania: 29.04.2025	

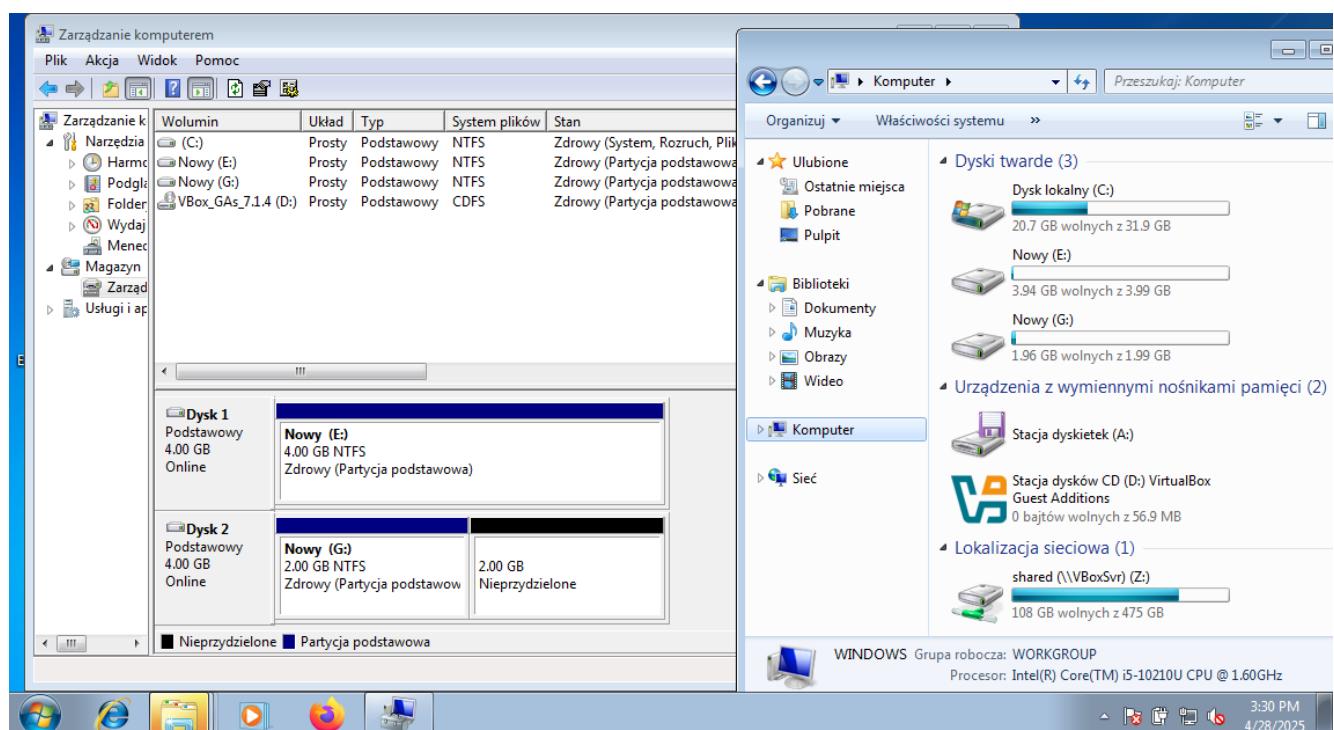
1. Cel ćwiczenia

Zapoznanie się z metodami odzyskiwania skasowanych i uszkodzonych danych.

2. Realizacja zadań laboratoryjnych

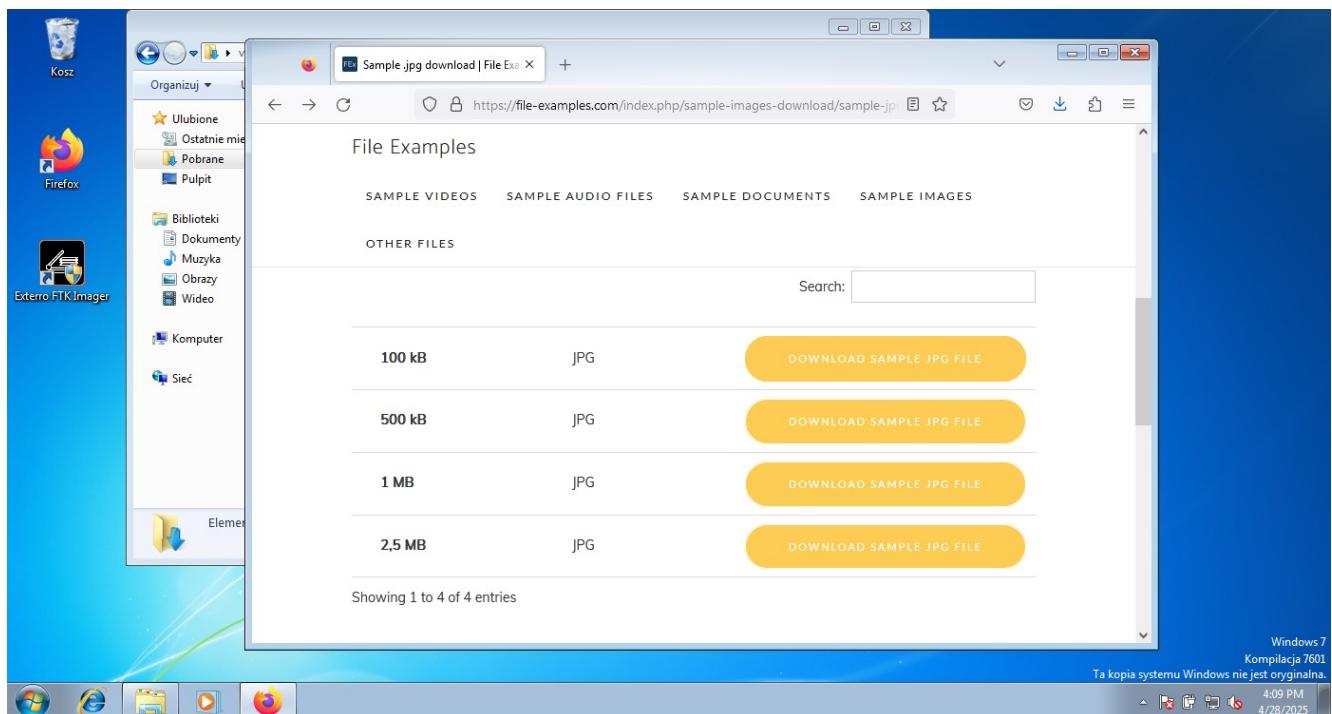
Zadanie 1:

Na systemie wirtualnym Windows wydziel 2 partycje i na jednej z nich utwórz folder z różnymi typami plików (np. .jpg, .txt .mp4 .docx). Następnie usuń kilka z plików (bez przenoszenia do kosza) i użyj wybranego darmowego narzędzia do odzyskiwania danych (np. Recuva, PhotoRec), aby spróbować go przywrócić. Odzyskane dane zapisuj na drugiej partycji. (Zamiast partycji można skorzystać z pendrive)

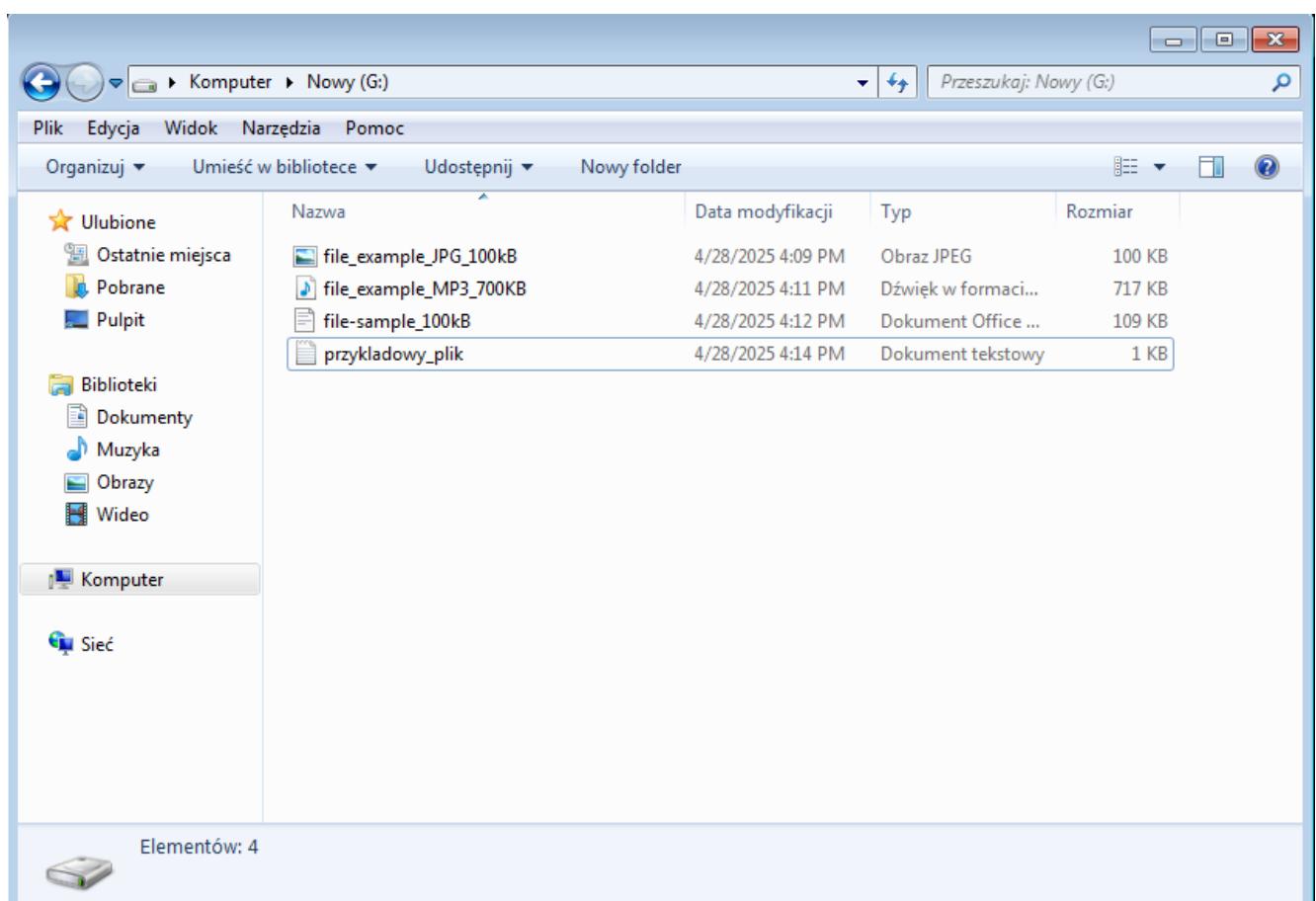


Rysunek 1: zimportowanie dwóch dysków do systemów

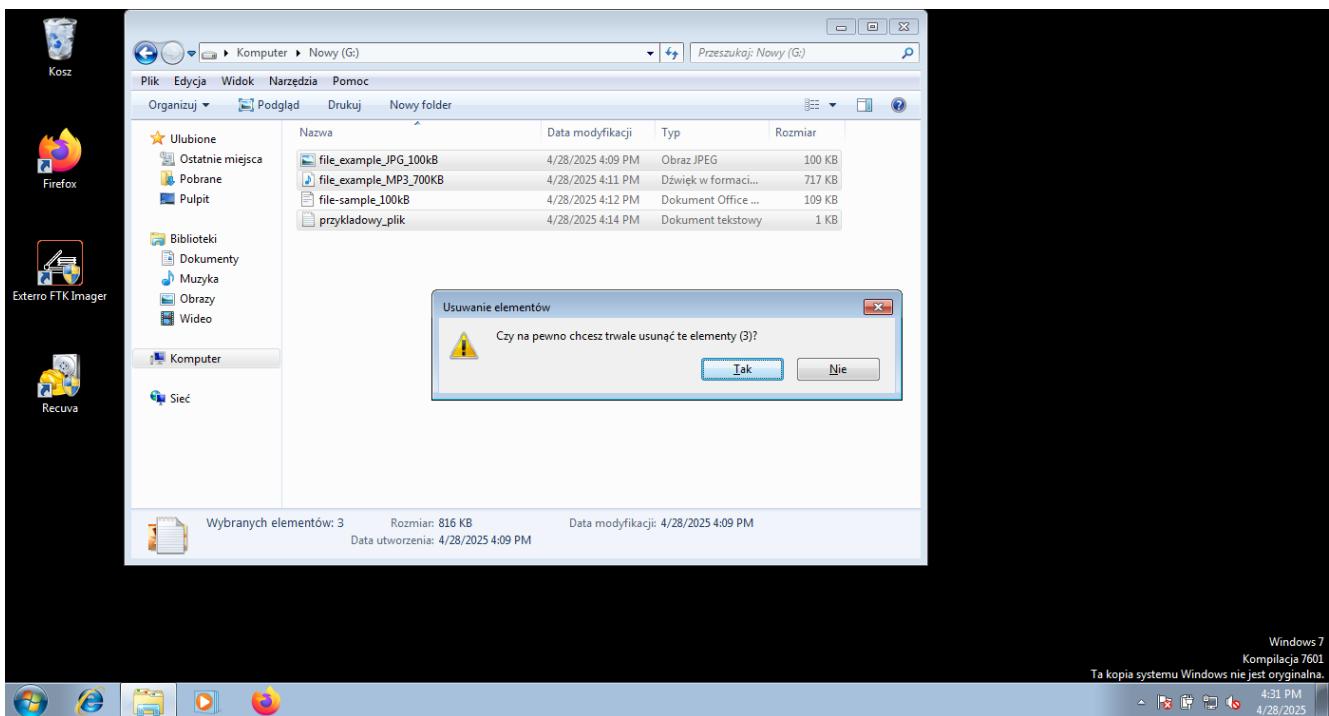
Komentarz: na drugim dysku stworzona została partycja 2GB a nie 4, z powodu komunikatu o braku miejsca: nie będzie miało to znaczenia przy wykonywaniu zadań.



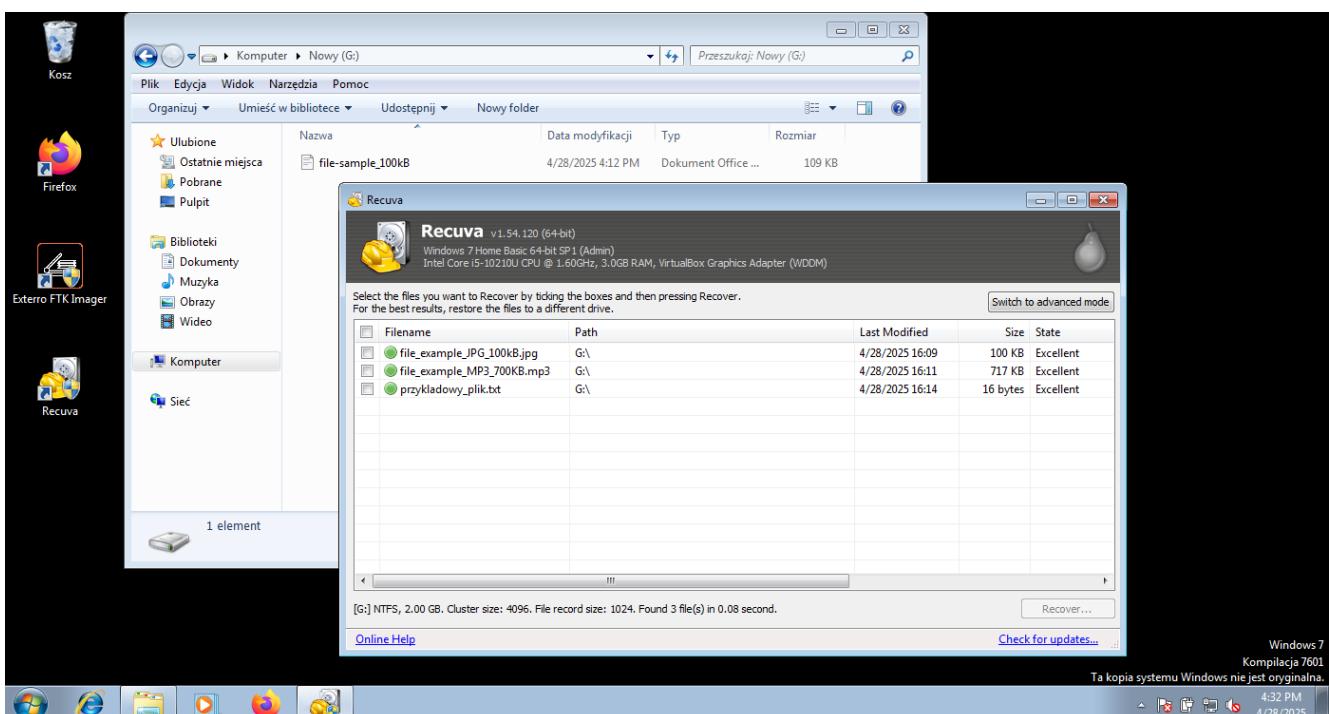
Rysunek 2: pobranie przykładowych plików różnego typu; file-examples.com



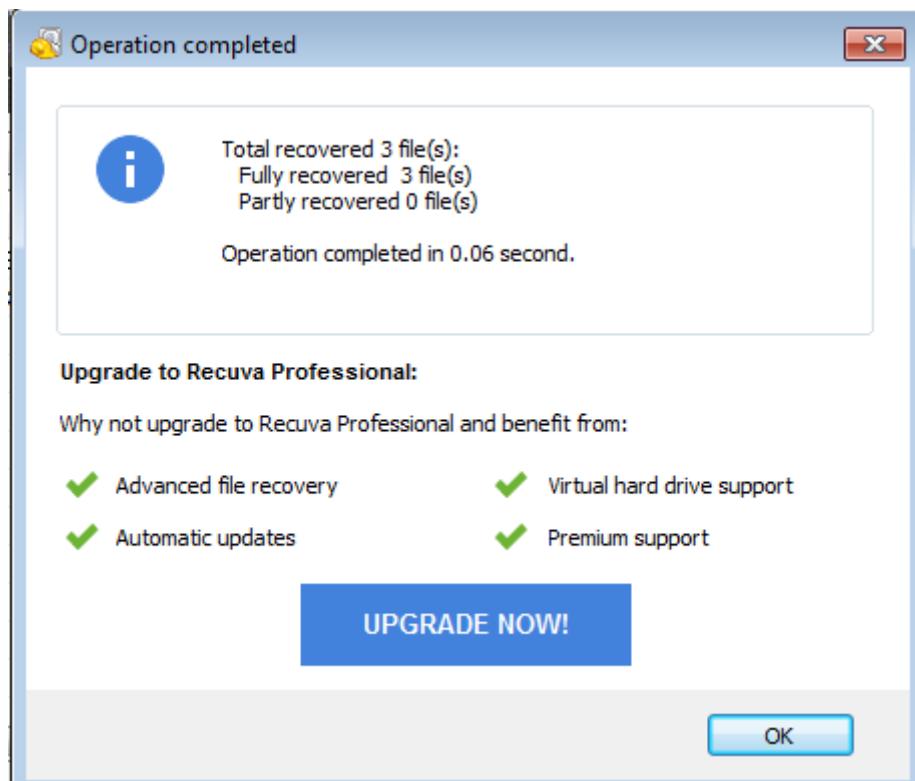
Rysunek 3: pliki na dysku G:



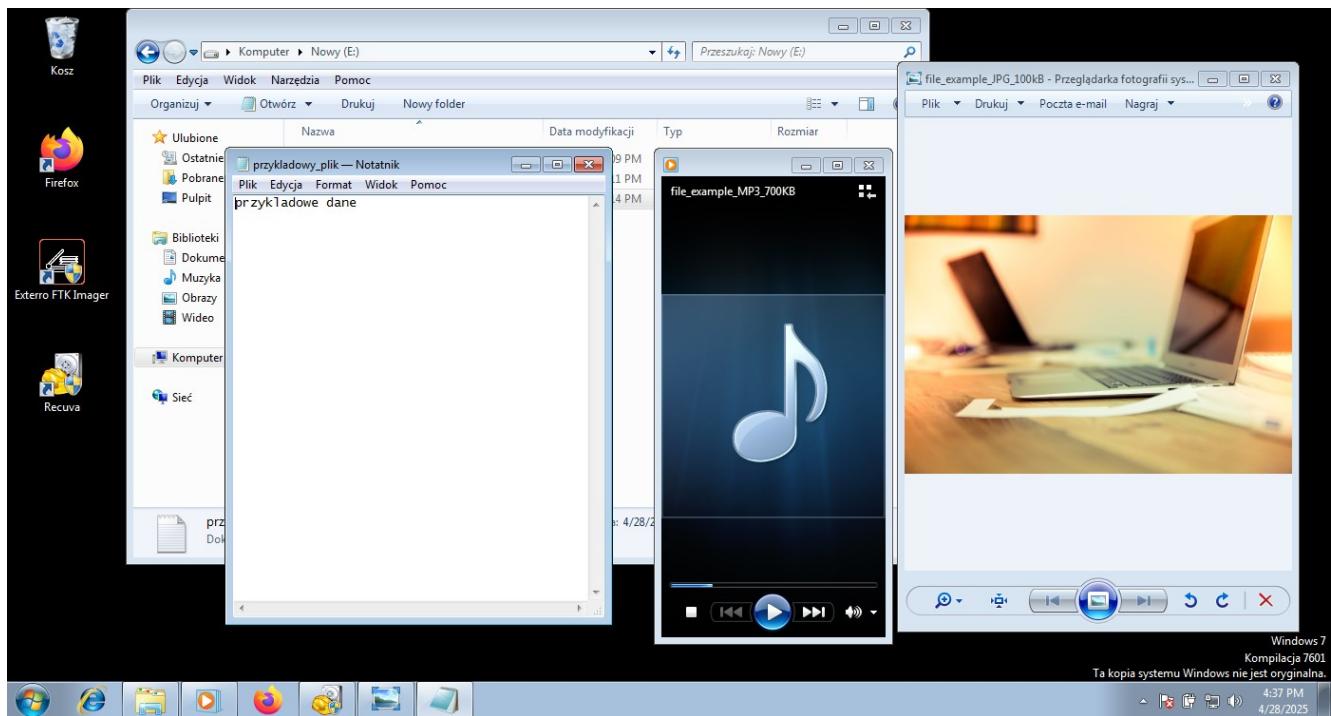
Rysunek 4: trwałe usuwanie wybranych plików



Rysunek 5: odzyskiwanie plików; program recuva



Rysunek 6: pop-up po zakończeniu odzyskiwania



Rysunek 7: test poprawności plików

Komentarz: pliki otwierają się poprawnie i zawierają dobre, nie zniszczone dane.

Pliki zostały odzyskane na dysk E.

Czy udało się odzyskać cały plik?

Tak, wszystkie trzy usunięte wcześniej pliki zostały odzyskane.

Czy odzyskany plik był sprawny (otwierał się poprawnie)?

Tak.

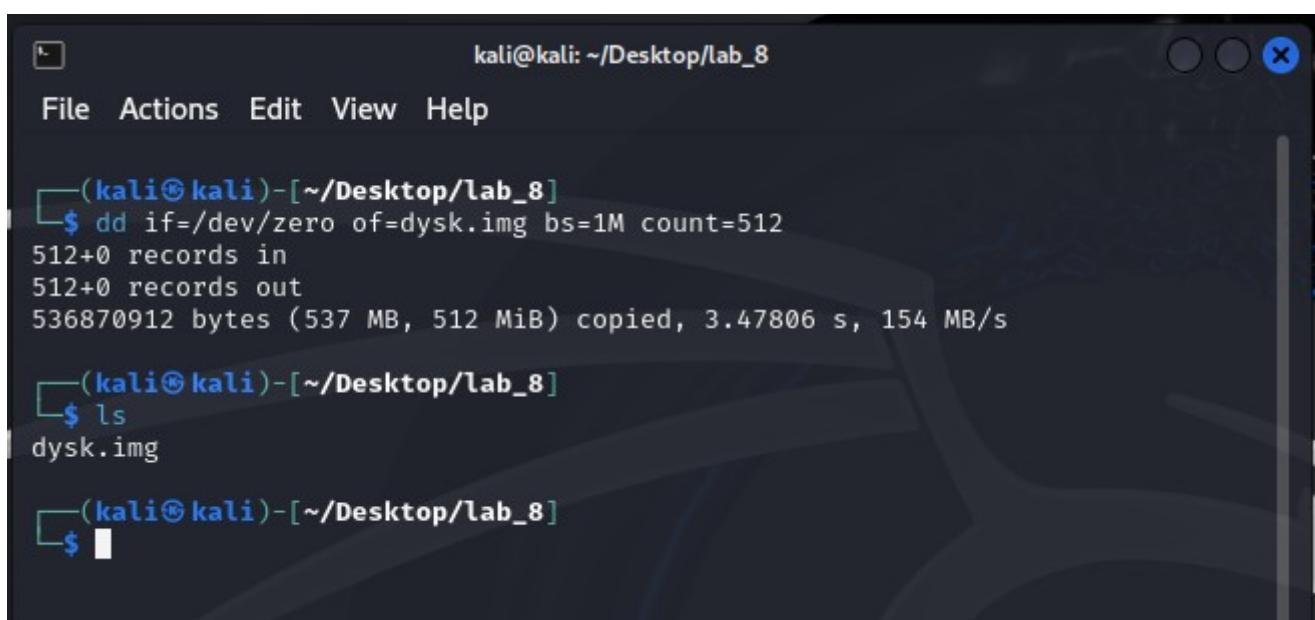
Jakie pliki narzędzie znalazło oprócz skasowanego?

Narzędzie odnalazło tylko 3 skasowane wcześniej pliki.

Zadanie 2:

Odzyskiwanie danych z uszkodzonego obrazu dysku.

**1. Na systemie Linux utwórz nowy plik obrazu korzystając z narzędzia dd
kali**



The screenshot shows a terminal window titled 'kali@kali: ~/Desktop/lab_8'. The terminal content is as follows:

```
(kali㉿kali)-[~/Desktop/lab_8]
$ dd if=/dev/zero of=dysk.img bs=1M count=512
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 3.47806 s, 154 MB/s

(kali㉿kali)-[~/Desktop/lab_8]
$ ls
dysk.img

(kali㉿kali)-[~/Desktop/lab_8]
$
```

Rysunek 8: tworzenie obrazu dysku

2. Następnie sformatuj go jako dysk i dodaj partycję.

The screenshot shows a terminal window with a dark background. At the top, it displays the command line prompt: `kali@kali: ~/Desktop/lab_8`. Below the prompt, the terminal shows the following sequence of commands and output:

```
(kali㉿kali)-[~/Desktop/lab_8]
$ sudo losetup -fP dysk.img
[sudo] password for kali:
(kali㉿kali)-[~/Desktop/lab_8]
$ losetup -a
/dev/loop0: [/]: (/home/kali/Desktop/lab_8/dysk.img)
(kali㉿kali)-[~/Desktop/lab_8]
$ 
```

Rysunek 9: podłączenie pliku do urządzenia loop

kali@kali: ~/Desktop/lab_8

File Actions Edit View Help

```
(kali㉿kali)-[~/Desktop/lab_8]
$ sudo fdisk /dev/loop0

Welcome to fdisk (util-linux 2.40.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS (MBR) disklabel with disk identifier 0x6a62f089.

Command (m for help): n
Partition type
  p  primary (0 primary, 0 extended, 4 free)
  e  extended (container for logical partitions)
Select (default p):

Using default response p.
Partition number (1-4, default 1):
First sector (2048-1048575, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-1048575, default 1048575)
:

Created a new partition 1 of type 'Linux' and of size 511 MiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

(kali㉿kali)-[~/Desktop/lab_8]
$
```

Rysunek 10: tworzenie partycji

```
kali㉿kali: ~/Desktop/lab_8
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop/lab_8]
└─$ sudo mkfs.ext4 /dev/loop0p1
mke2fs 1.47.1 (20-May-2024)
Discarding device blocks: done
Creating filesystem with 523264 1k blocks and 130560 inodes
Filesystem UUID: effe0525-5605-41b3-91ea-52e9c257928c
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729, 204801, 221185, 401409

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

└─(kali㉿kali)-[~/Desktop/lab_8]
└─$ sudo partprobe /dev/loop0
└─(kali㉿kali)-[~/Desktop/lab_8]
└─$
```

Rysunek 11: formatowanie i aktualizacja informacji

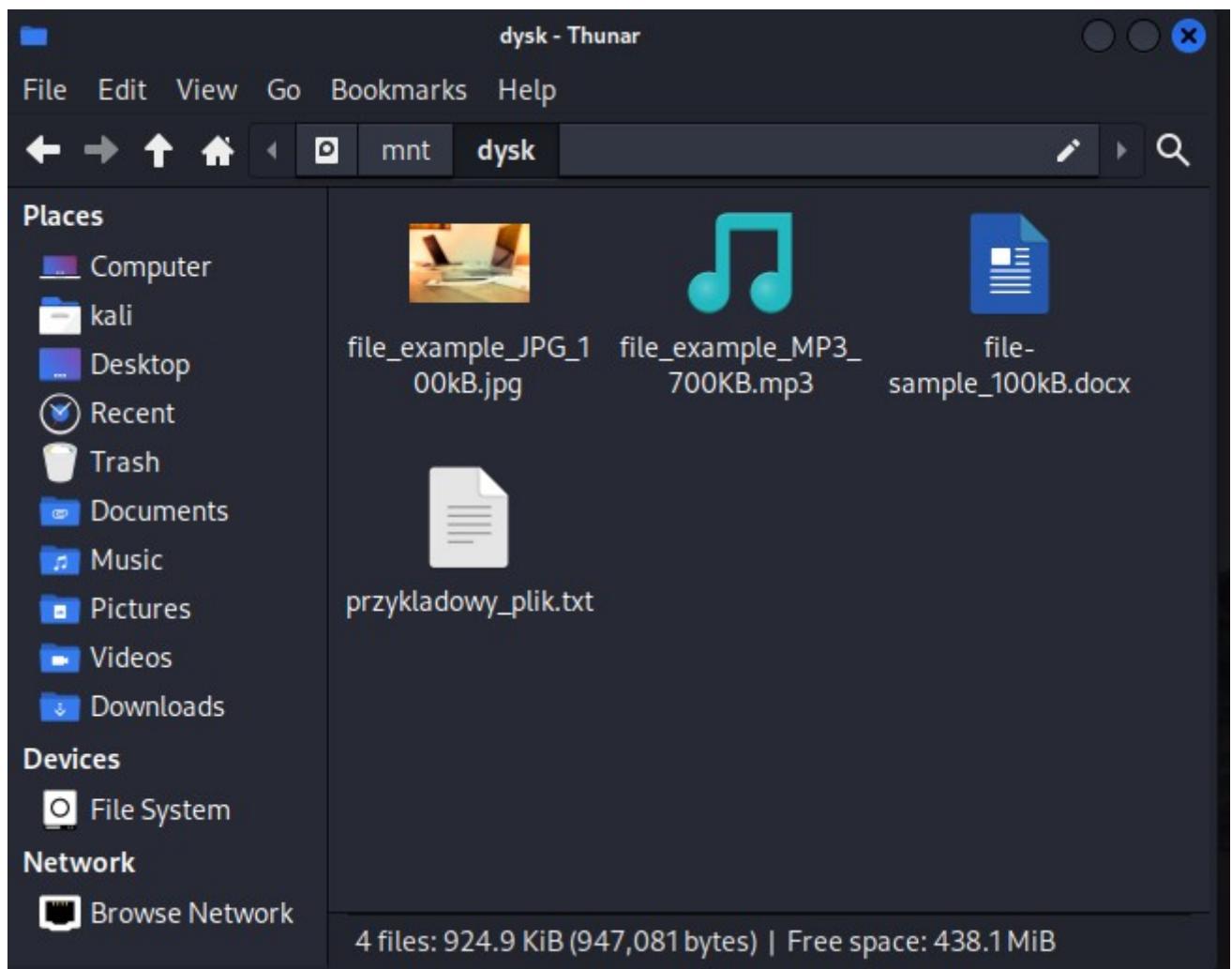
```
└─(kali㉿kali)-[~/Desktop/lab_8]
└─$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0      7:0    0  512M  0 loop
└─loop0p1  259:0   0  511M  0 part
sda       8:0    0 80.1G  0 disk
└─sda1     8:1    0 80.1G  0 part /
sr0       11:0   1 1024M  0 rom
```

Rysunek 12: pokazanie dysku

3. Zamontuj i utwórz kilka katalogów i wrzuć dowolne dane (pliki tekstowe, graficzne itp.)

```
kali@kali: ~/Desktop/lab_8
File Actions Edit View Help
└─(kali㉿kali)-[~/Desktop/lab_8]
$ sudo mkdir /mnt/dysk
└─(kali㉿kali)-[~/Desktop/lab_8]
$ sudo mount /dev/loop0p1 /mnt/dysk
└─(kali㉿kali)-[~/Desktop/lab_8]
$ sudo chmod 777 /mnt/dysk
└─(kali㉿kali)-[~/Desktop/lab_8]
$
```

Rysunek 13: montowanie i zmiana uprawnień



Rysunek 14: dodanie plików

4. Zasymuluj uszkodzenie tablicy partycji: dd if=/dev/zero of=/dev/loop0 bs=512 count=1

The screenshot shows a terminal window titled "kali@kali: ~/Desktop/lab_8". The terminal history includes:

- \$ sudo umount /mnt/dysk
- \$ sudo dd if=/dev/zero of=/dev/loop0 bs=512 count=1
1+0 records in
1+0 records out
512 bytes copied, 0.00118754 s, 431 kB/s
- \$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 512M 0 loop
sda 8:0 0 80.1G 0 disk
└─sda1 8:1 0 80.1G 0 part /
sr0 11:0 1 1024M 0 rom
- \$

Rysunek 15: odmontowanie i uszkodzenie tablicy partycji

5. Korzystając z narzędzia TestDisk spróbuj odzyskać dane z uszkodzonego obrazu dysku.

The screenshot shows a terminal window titled "kali@kali: ~/Desktop/lab_8". The window contains the following text:

```
File Actions Edit View Help
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/loop0 - 536 MB / 512 MiB

>[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 BI
detection, and install the latest OS patches and disk drivers.
```

Rysunek 16: odzyskiwanie danych; TestDisk

A screenshot of a terminal window titled "kali@kali: ~/Desktop/lab_8". The window contains the TestDisk 7.2 Data Recovery Utility. The text output includes:

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

Disk /dev/loop0 - 536 MB / 512 MiB
    1048576 sectors - 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.
```

Rysunek 17: odzyskiwanie danych

kali@kali: ~/Desktop/lab_8

File Actions Edit View Help

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

Disk /dev/loop0 - 536 MB / 512 MiB - 1048576 sectors

Partition	Start	End	Size in sectors
>* Linux	2048	1048575	1046528

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
ext4 blocksize=1024 Large_file Sparse_SB, 535 MB / 511 MiB

Rysunek 18: odzyskiwanie danych

kali@kali: ~/Desktop/lab_8

File Actions Edit View Help

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

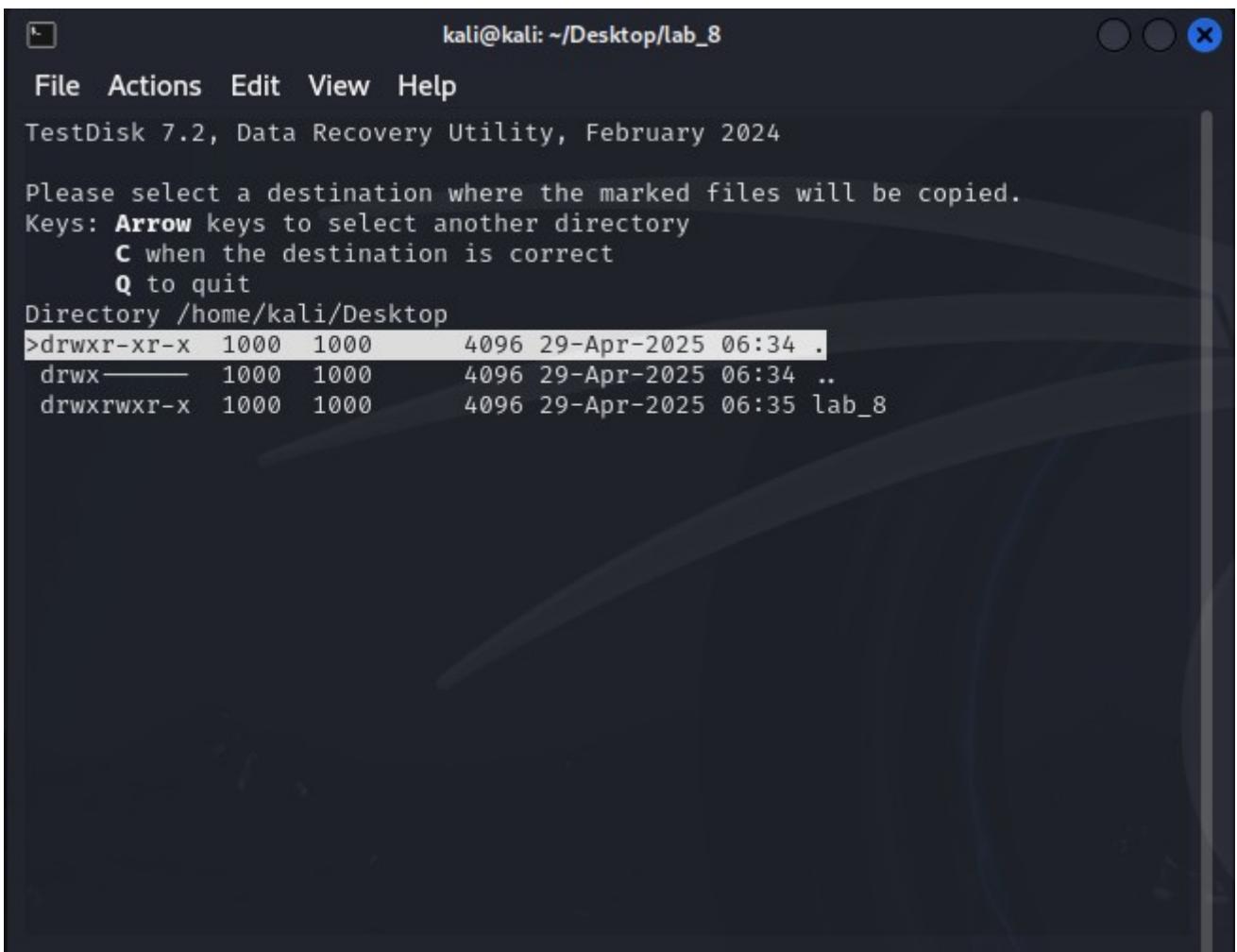
* Linux 2048 1048575 1046528

Directory /

	Size	Modif.	Name
drwxrwxrwx	0	1024 29-Apr-2025 06:38	.
drwxrwxrwx	0	1024 29-Apr-2025 06:38	..
drwx---	0	12288 29-Apr-2025 06:37	lost+found
*-rwxrwx--	1000	102117 28-Apr-2025 10:09	file_example_JPG_100kB.jpg
*-rwxrwx--	1000	733645 28-Apr-2025 10:11	file_example_MP3_700KB.mp3
*-rwxrwx--	1000	111303 28-Apr-2025 10:12	file-sample_100kB.docx
>-rwxrwx--	1000	16 28-Apr-2025 10:14	przykladowy_plik.txt

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

Rysunek 19: kopiowanie odzyskanych danych



kali@kali: ~/Desktop/lab_8

File Actions Edit View Help

TestDisk 7.2, Data Recovery Utility, February 2024

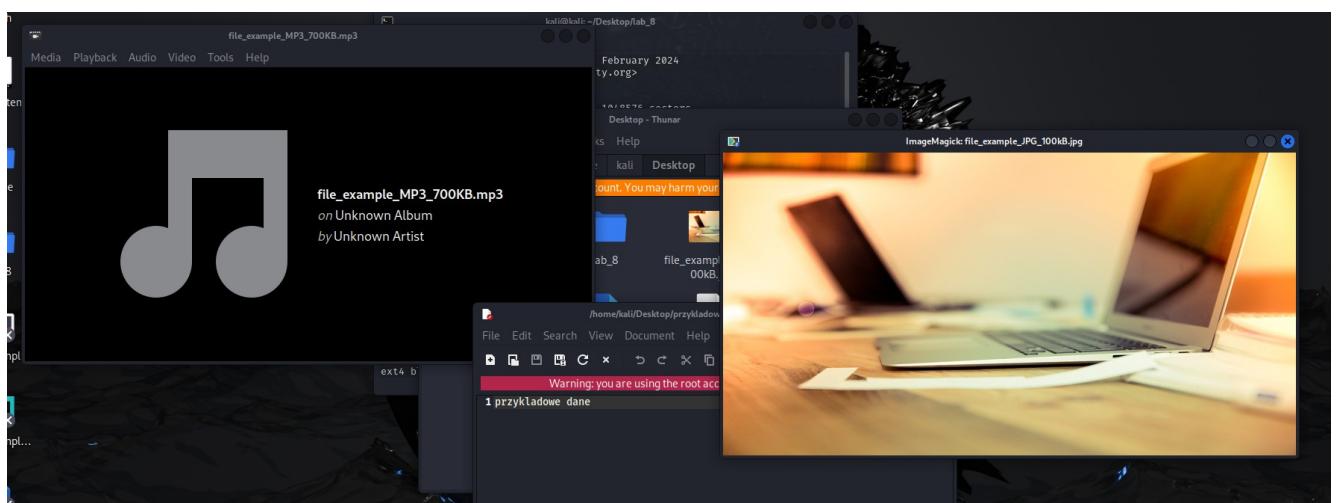
Please select a destination where the marked files will be copied.

Keys: Arrow keys to select another directory
C when the destination is correct
Q to quit

Directory /home/kali/Desktop

```
>drwxr-xr-x 1000 1000 4096 29-Apr-2025 06:34 .
drwx----- 1000 1000 4096 29-Apr-2025 06:34 ..
drwxrwxr-x 1000 1000 4096 29-Apr-2025 06:35 lab_8
```

Rysunek 20: kopiowanie odzyskanych danych



Rysunek 21: prezentacja odzyskanych danych

6. Spróbuj za pomocą TestDisk przywrócić strukturę danych uszkodzonego obrazu dysku.

kali@kali: ~/Desktop/lab_8

File Actions Edit View Help

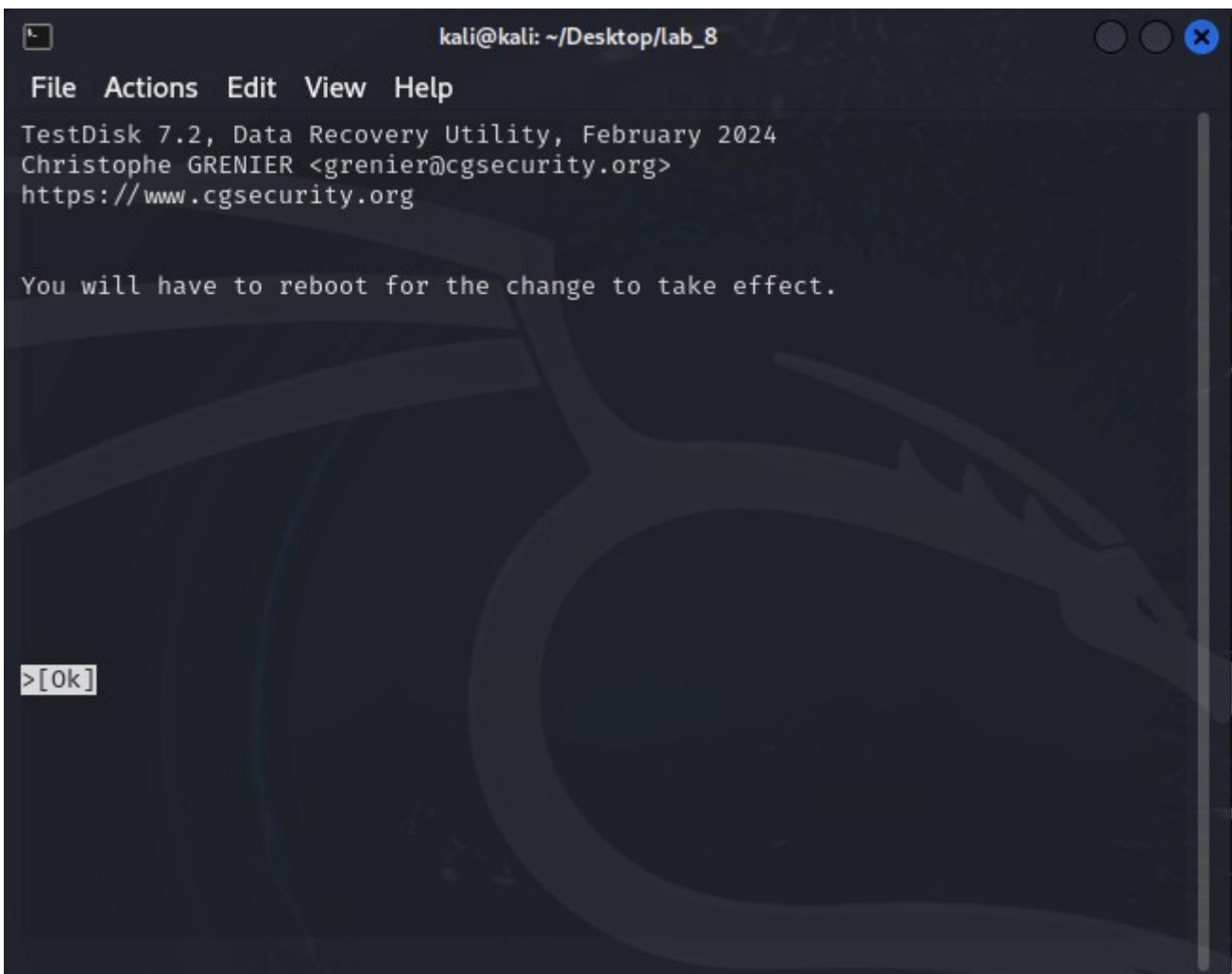
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
<https://www.cgsecurity.org>

Disk /dev/loop0 - 536 MB / 512 MiB - 1048576 sectors

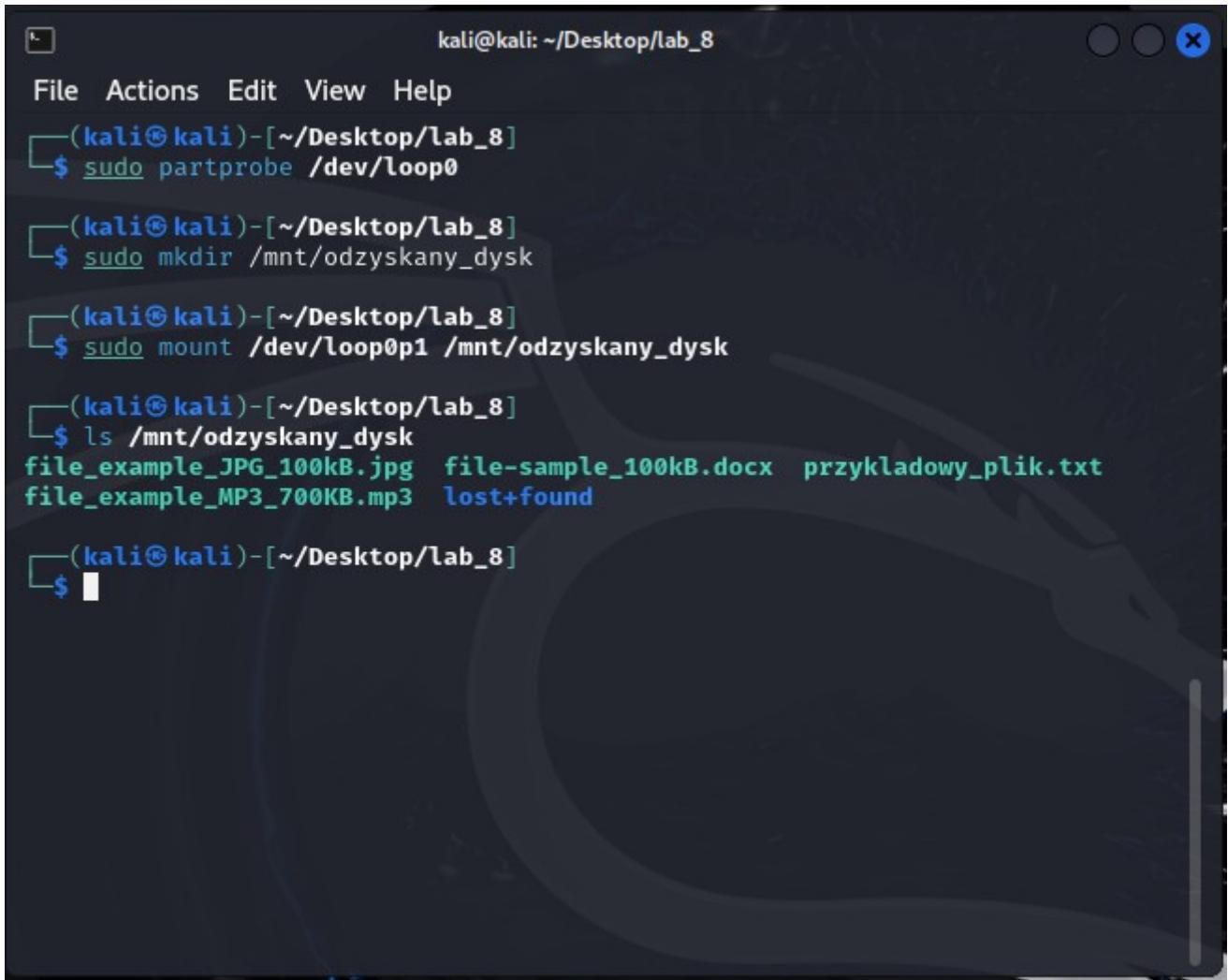
Partition	Start	End	Size in sectors
1 * Linux	2048	1048575	1046528

[Quit] [Return] [Deeper Search] >[Write]
Write partition structure to disk

Rysunek 22: przywracanie struktury danych uszkodzonego dysku



Rysunek 23: przywracanie struktury danych uszkodzonego dysku



The screenshot shows a terminal window titled "kali@kali: ~/Desktop/lab_8". The terminal history is as follows:

```
(kali㉿kali)-[~/Desktop/lab_8]
$ sudo partprobe /dev/loop0
(kali㉿kali)-[~/Desktop/lab_8]
$ sudo mkdir /mnt/odzyskany_dysk
(kali㉿kali)-[~/Desktop/lab_8]
$ sudo mount /dev/loop0p1 /mnt/odzyskany_dysk
(kali㉿kali)-[~/Desktop/lab_8]
$ ls /mnt/odzyskany_dysk
file_example_JPG_100kB.jpg  file-sample_100kB.docx  przykładowy_plik.txt
file_example_MP3_700KB.mp3  lost+found
```

Rysunek 24: prezentacja odzyskanej struktury

Czy udało się zrekonstruować partycję?

Tak.

Jakie były największe trudności?

Proces przebiegł bez większych trudności

3. Wnioski

Nawet jeśli pliki, partycje czy dyski są uszkadzane to za pomocą odpowiednich narzędzi jesteśmy w stanie je odtwarzać.