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 9

Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 05.05.2025	
Data oddania sprawozdania: 11.05.2025	

1. Cel ćwiczenia

- Symulacja procesu bezpiecznego usuwania danych w systemie Linux (VM).

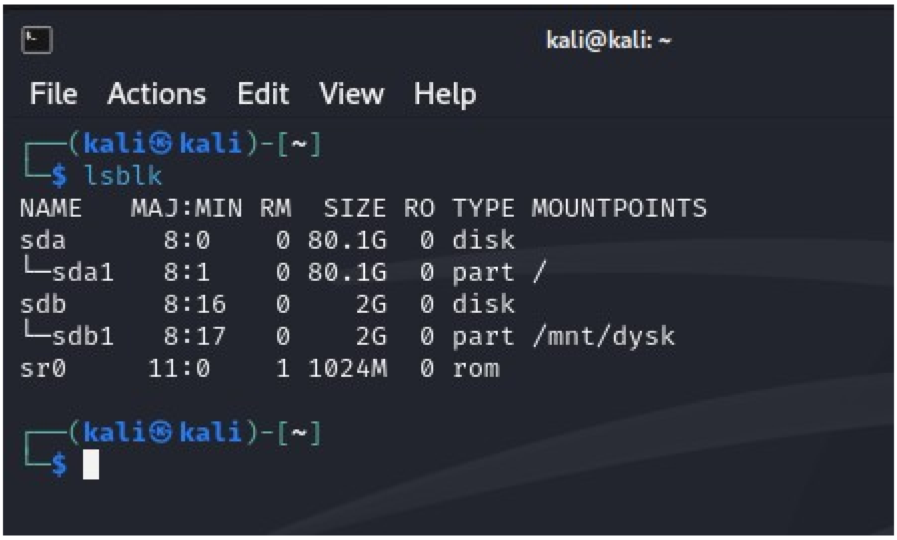
- Przetestowanie narzędzi do logicznego wymazywania danych i ocena ich skuteczności w środowisku testowym.

2. Realizacja zadań laboratoryjnych

Zadanie 1:

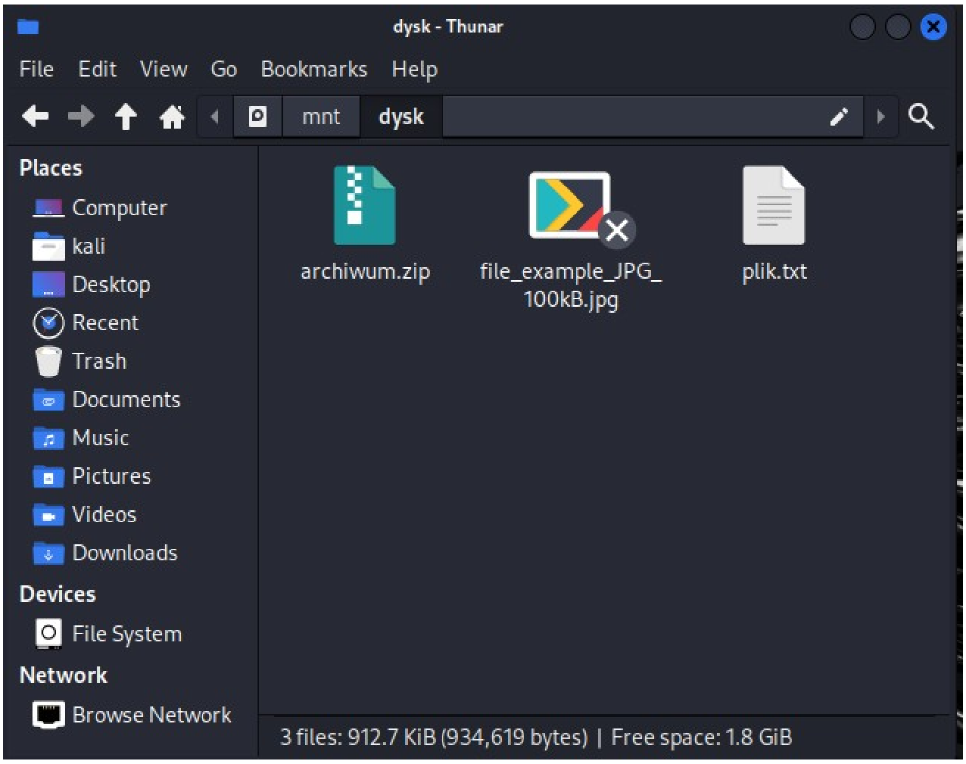
Utwórz testowe pliki (np. .txt, .jpg, .zip) na drugiej mniejszej partycji lub nośniku.

Komentarz: Dysk wykorzystany do tego ćwiczenia to 2GB VHD sformatowany do ext4 i zamontowany tak jak pokazano poniżej.



```
┌──(kali㉿kali)-[~]
└─$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 80.1G  0 disk
└─sda1   8:1    0 80.1G  0 part /
sdb      8:16   0    2G  0 disk
└─sdb1   8:17   0    2G  0 part /mnt/dysk
sr0     11:0    1 1024M  0 rom

┌──(kali㉿kali)-[~]
└─$ 
```

Rysunek 1: zamontowana partycja dysku

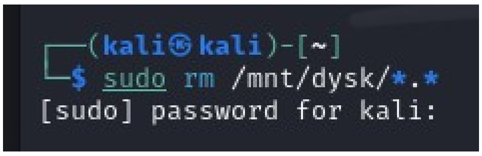


3 files: 912.7 KiB (934,619 bytes) | Free space: 1.8 GiB

Rysunek 2: przykładowe pliki na dysku

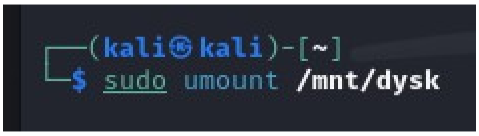
Zadanie 2:

Usuń pliki przy pomocy rm i sprawdź w hexedytorze czy plik jest widoczny



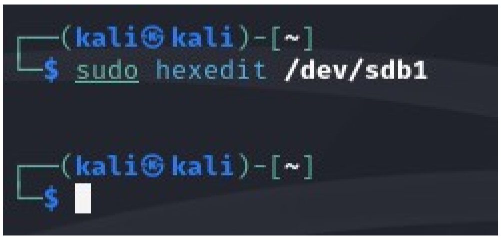
```
┌──(kali㉿kali)-[~]
└─$ sudo rm /mnt/dysk/*.*
[sudo] password for kali:
```

Rysunek 3: usunięcie wszystkich plików



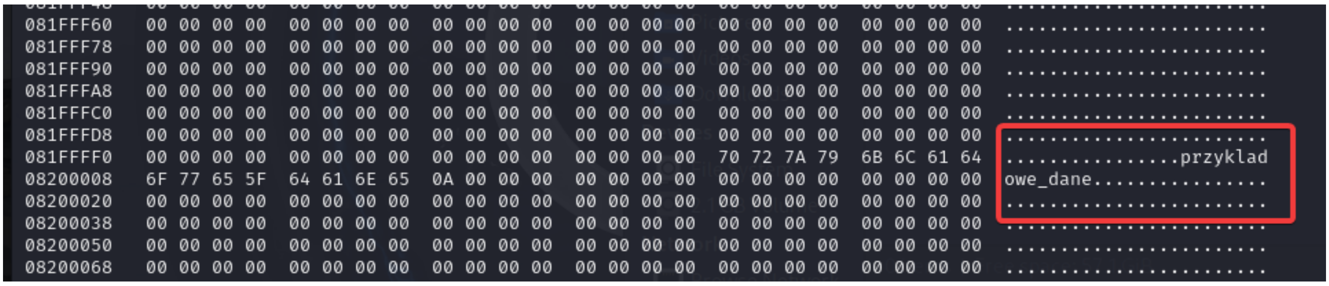
```
┌──(kali㉿kali)-[~]
└─$ sudo umount /mnt/dysk
```

Rysunek 4: odmontowanie dysku



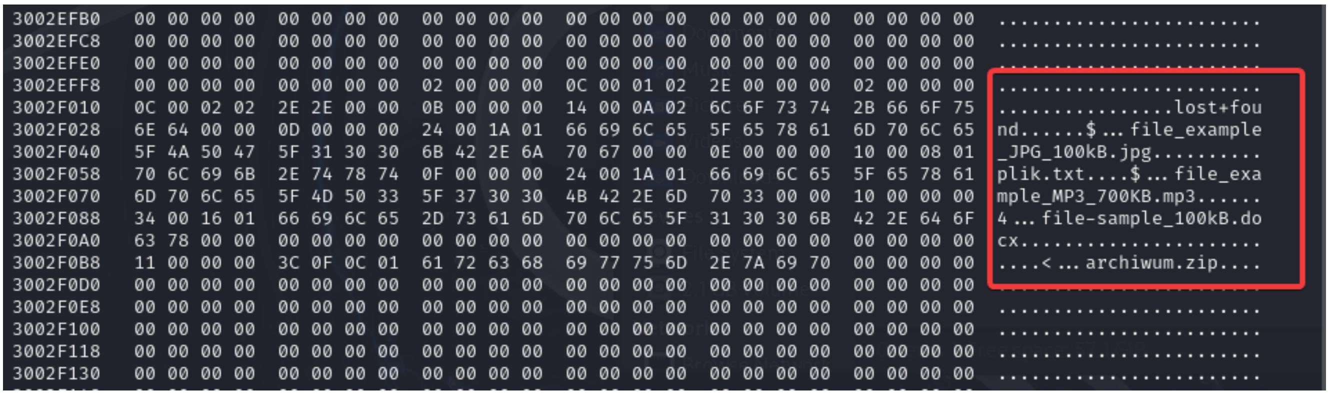
```
┌──(kali㉿kali)-[~]
└─$ sudo hexedit /dev/sdb1

┌──(kali㉿kali)-[~]
└─$ █
```

Rysunek 5: uruchomienie hexedytora; hexedit



```
081FFF60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFF78   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFF90   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFFA8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFFC0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFFD8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
081FFFF0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  70 72 7A 79  6B 6C 61 64  ................przyklad
08200008   6F 77 65 5F  64 61 6E 65  0A 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  owe_dane................
08200020   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
08200038   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
08200050   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
08200068   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
```

Rysunek 6: odnaleziona zawartość pliku .txt



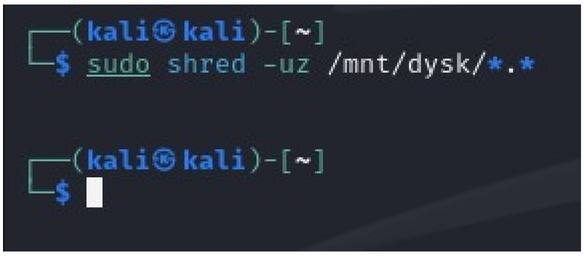
```
3002EFB0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002EFC8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002EFE0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002EFF8   00 00 00 00  00 00 00 00  02 00 00 00  0C 00 01 02  2E 00 00 00  02 00 00 00  ........................
3002F010   0C 00 02 02  2E 2E 00 00  0B 00 00 00  14 00 0A 02  6C 6F 73 74  2B 66 6F 75  ................lost+fou
3002F028   6E 64 00 00  0D 00 00 00  24 00 1A 01  66 69 6C 65  5F 65 78 61  6D 70 6C 65  nd......$...file_example
3002F040   5F 4A 50 47  5F 31 30 30  6B 42 2E 6A  70 67 00 00  0E 00 00 00  10 00 08 01  _JPG_100kB.jpg..........
3002F058   70 6C 69 6B  2E 74 78 74  0F 00 00 00  24 00 1A 01  66 69 6C 65  5F 65 78 61  plik.txt....$...file_exa
3002F070   6D 70 6C 65  5F 4D 50 33  5F 37 30 30  4B 42 2E 6D  70 33 00 00  10 00 00 00  mple_MP3_700KB.mp3......
3002F088   34 00 16 01  66 69 6C 65  2D 73 61 6D  70 6C 65 5F  31 30 30 6B  42 2E 64 6F  4...file-sample_100kB.do
3002F0A0   63 78 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  cx......................
3002F0B8   11 00 00 00  3C 0F 0C 01  61 72 63 68  69 77 75 6D  2E 7A 69 70  00 00 00 00  ....<...archiwum.zip....
3002F0D0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002F0E8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002F100   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002F118   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
3002F130   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
```

Rysunek 7: odnalezione nazwy plików

Zadanie 3:

Przetestuj narzędzia shred, wipe, dd, aby usunąć pliki z nadpisywaniem.

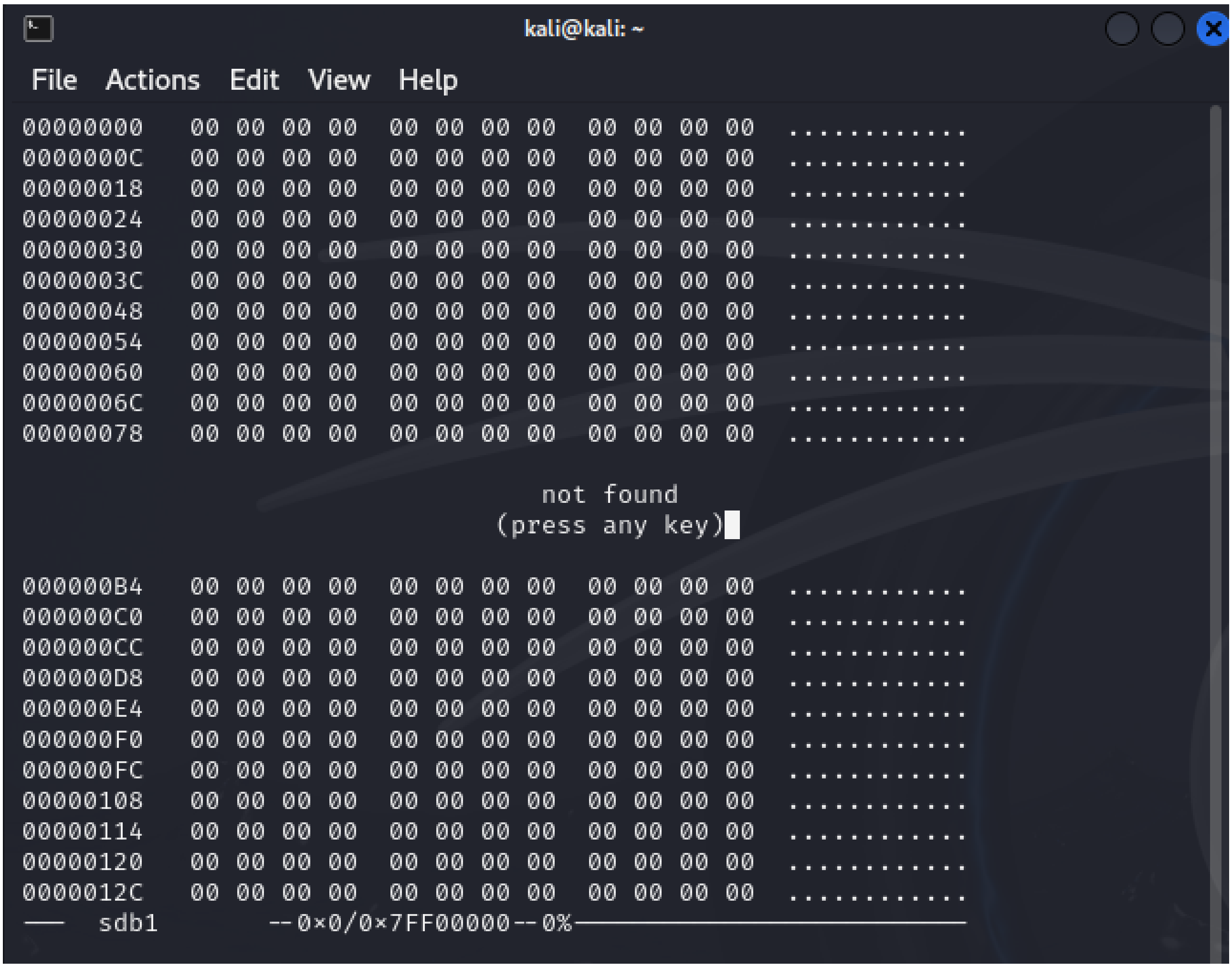
shred:



```
┌──(kali㉿kali)-[~]
└─$ sudo shred -uz /mnt/dysk/*.*

┌──(kali㉿kali)-[~]
└─$ 
```

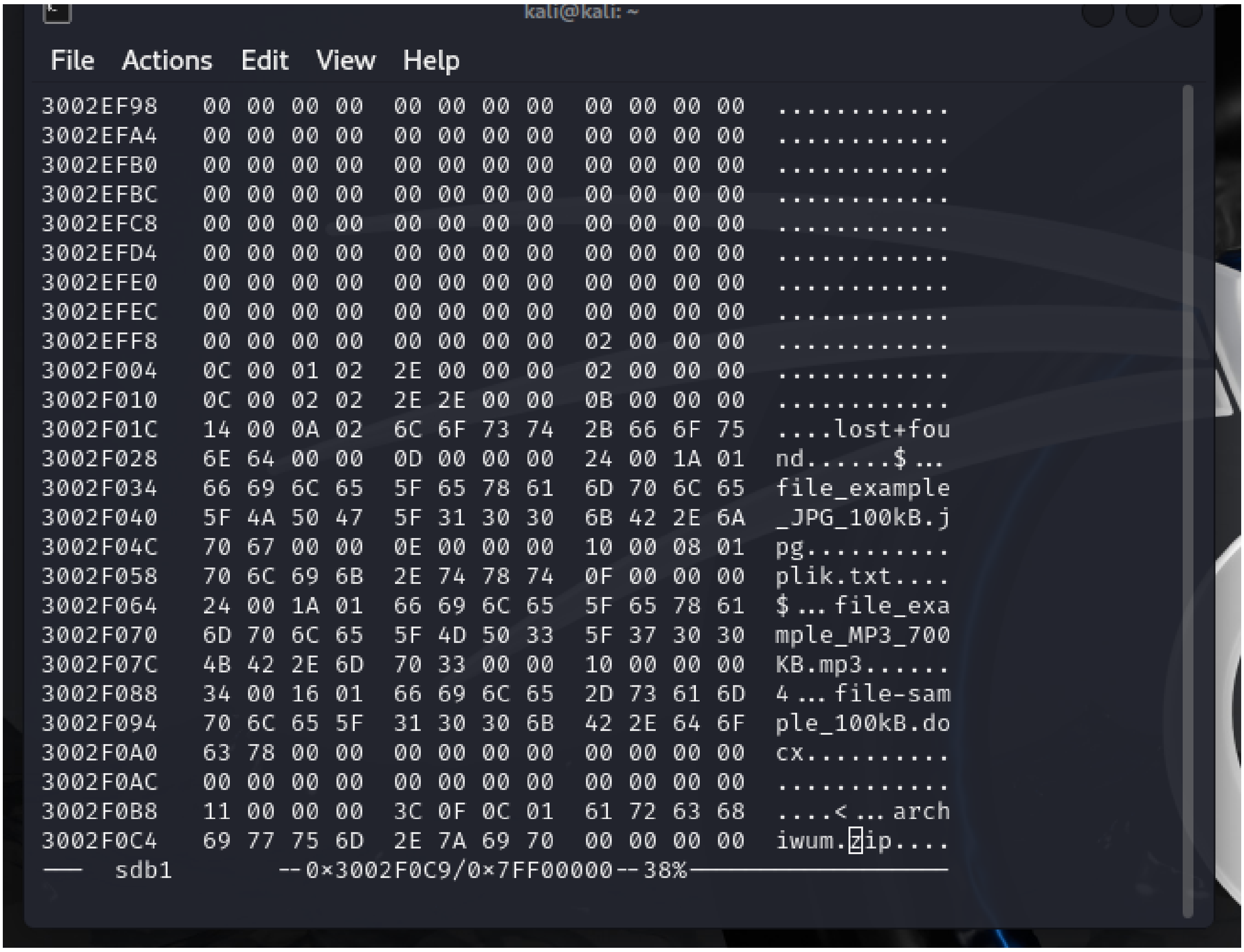
Rysunek 8: usuwanie danych; shred

hexedit:



```
00000000   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000000C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000018   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000024   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000030   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000003C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000048   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000054   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000060   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000006C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000078   00 00 00 00  00 00 00 00  00 00 00 00  ............

                        not found
                     (press any key)

000000B4   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000C0   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000CC   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000D8   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000E4   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000F0   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000FC   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000108   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000114   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000120   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000012C   00 00 00 00  00 00 00 00  00 00 00 00  ............
——  sdb1       --0x0/0x7FF00000--0%──────────────────────────
```

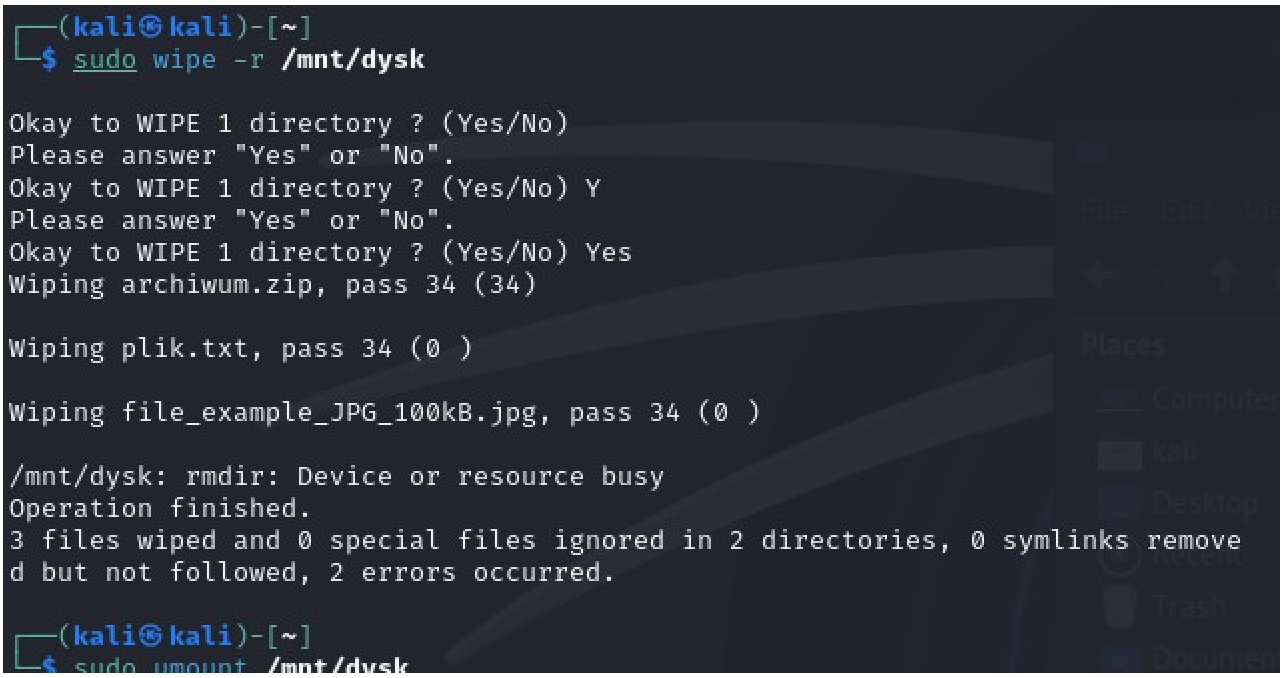
Rysunek 9: wynik przeszukania dla zawartości pliku .txt



```
3002EF98   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFA4   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFB0   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFBC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFC8   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFD4   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFE0   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFEC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFF8   00 00 00 00  00 00 00 00  02 00 00 00  ............
3002F004   0C 00 01 02  2E 00 00 00  02 00 00 00  ............
3002F010   0C 00 02 02  2E 2E 00 00  0B 00 00 00  ............
3002F01C   14 00 0A 02  6C 6F 73 74  2B 66 6F 75  ....lost+fou
3002F028   6E 64 00 00  0D 00 00 00  24 00 1A 01  nd......$...
3002F034   66 69 6C 65  5F 65 78 61  6D 70 6C 65  file_example
3002F040   5F 4A 50 47  5F 31 30 30  6B 42 2E 6A  _JPG_100kB.j
3002F04C   70 67 00 00  0E 00 00 00  10 00 08 01  pg..........
3002F058   70 6C 69 6B  2E 74 78 74  0F 00 00 00  plik.txt....
3002F064   24 00 1A 01  66 69 6C 65  5F 65 78 61  $...file_exa
3002F070   6D 70 6C 65  5F 4D 50 33  5F 37 30 30  mple_MP3_700
3002F07C   4B 42 2E 6D  70 33 00 00  10 00 00 00  KB.mp3......
3002F088   34 00 16 01  66 69 6C 65  2D 73 61 6D  4...file-sam
3002F094   70 6C 65 5F  31 30 30 6B  42 2E 64 6F  ple_100kB.do
3002F0A0   63 78 00 00  00 00 00 00  00 00 00 00  cx..........
3002F0AC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002F0B8   11 00 00 00  3C 0F 0C 01  61 72 63 68  ....<...arch
3002F0C4   69 77 75 6D  2E 7A 69 70  00 00 00 00  iwum.zip....
───  sdb1       --0×3002F0C9/0×7FF00000--38%────────────────
```

Rysunek 10: wynik dla wyszukania „zip”

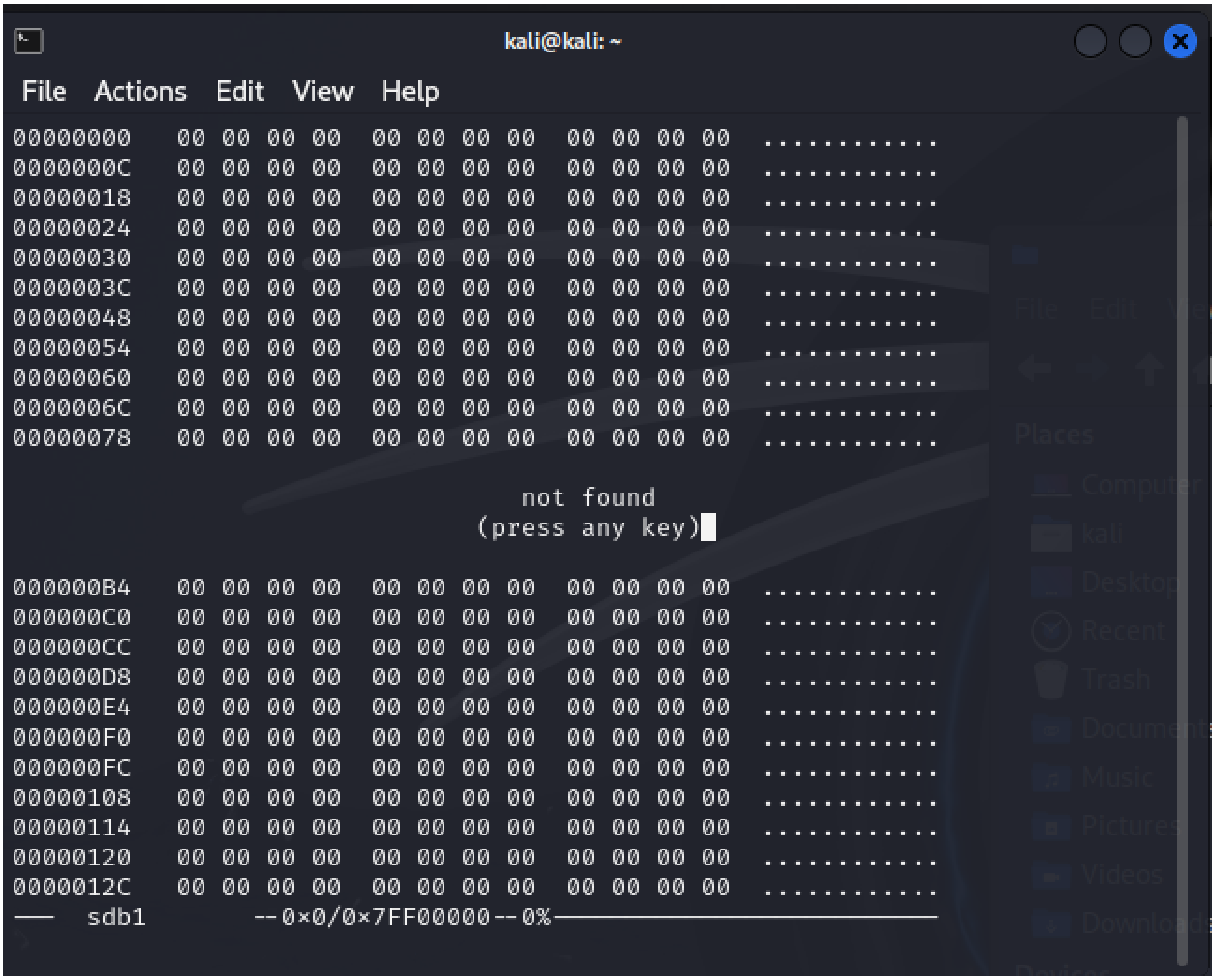
wipe:



```
┌──(kali㉿kali)-[~]
└─$ sudo wipe -r /mnt/dysk

Okay to WIPE 1 directory ? (Yes/No)
Please answer "Yes" or "No".
Okay to WIPE 1 directory ? (Yes/No) Y
Please answer "Yes" or "No".
Okay to WIPE 1 directory ? (Yes/No) Yes
Wiping archiwum.zip, pass 34 (34)

Wiping plik.txt, pass 34 (0 )

Wiping file_example_JPG_100kB.jpg, pass 34 (0 )

/mnt/dysk: rmdir: Device or resource busy
Operation finished.
3 files wiped and 0 special files ignored in 2 directories, 0 symlinks remove
d but not followed, 2 errors occurred.

┌──(kali㉿kali)-[~]
└─$ sudo umount /mnt/dysk
```

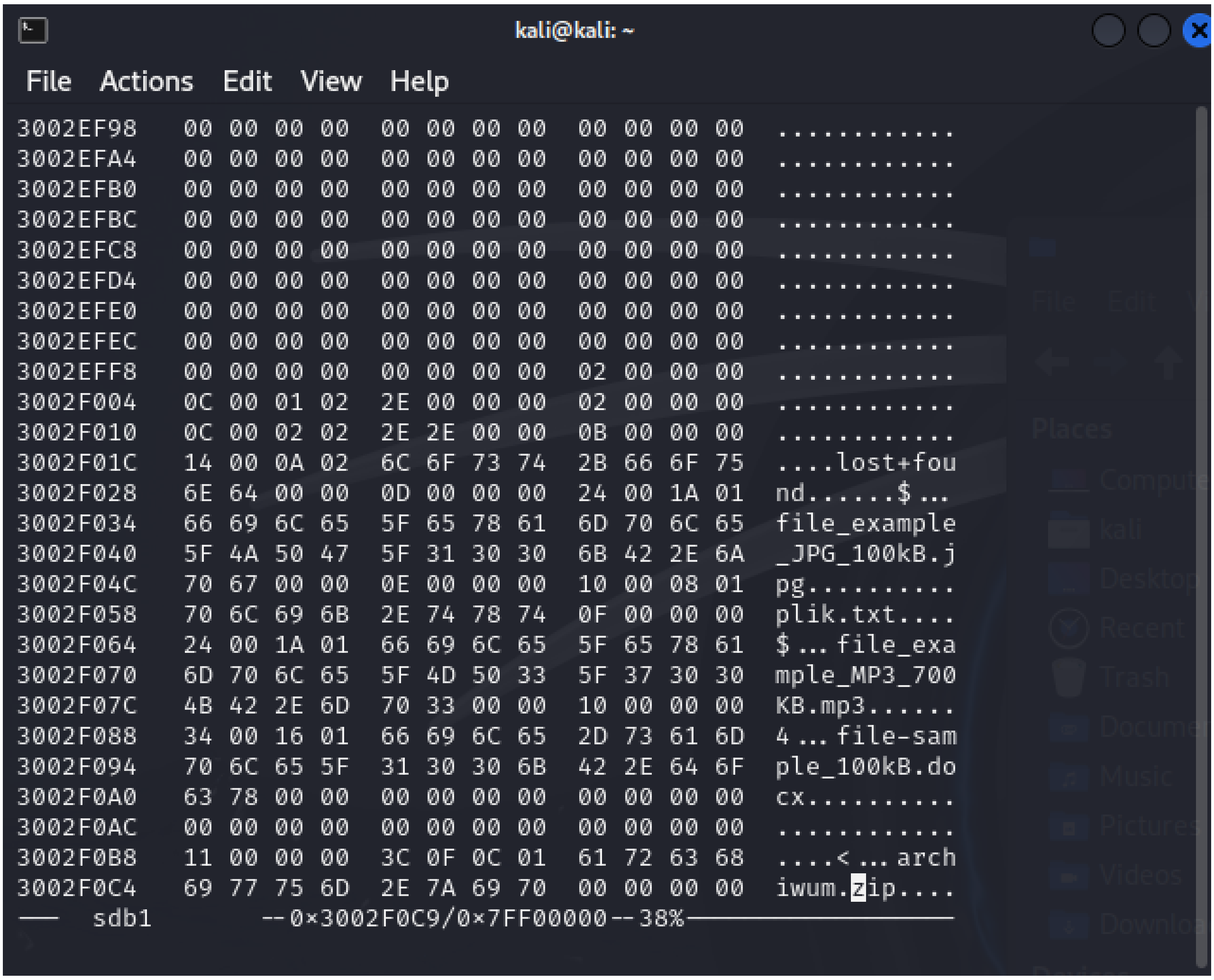
Rysunek 11: usuwanie danych; wipe

hexedit:



```
00000000   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000000C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000018   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000024   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000030   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000003C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000048   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000054   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000060   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000006C   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000078   00 00 00 00  00 00 00 00  00 00 00 00  ............

                                not found
                             (press any key)

000000B4   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000C0   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000CC   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000D8   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000E4   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000F0   00 00 00 00  00 00 00 00  00 00 00 00  ............
000000FC   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000108   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000114   00 00 00 00  00 00 00 00  00 00 00 00  ............
00000120   00 00 00 00  00 00 00 00  00 00 00 00  ............
0000012C   00 00 00 00  00 00 00 00  00 00 00 00  ............
───  sdb1       --0×0/0×7FF00000--0%──────────────────────────
```

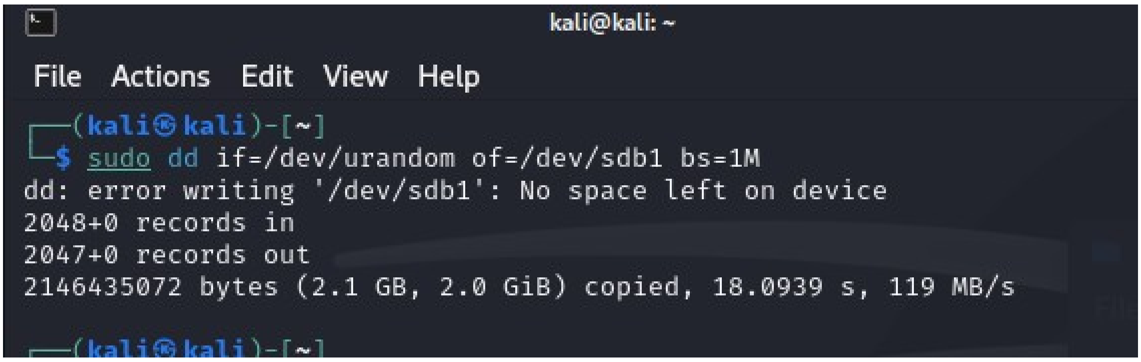
Rysunek 12: wynik przeszukania dla zawartości pliku .txt



```
3002EF98   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFA4   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFB0   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFBC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFC8   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFD4   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFE0   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFEC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002EFF8   00 00 00 00  00 00 00 00  02 00 00 00  ............
3002F004   0C 00 01 02  2E 00 00 00  02 00 00 00  ............
3002F010   0C 00 02 02  2E 2E 00 00  0B 00 00 00  ............
3002F01C   14 00 0A 02  6C 6F 73 74  2B 66 6F 75  ....lost+fou
3002F028   6E 64 00 00  0D 00 00 00  24 00 1A 01  nd......$...
3002F034   66 69 6C 65  5F 65 78 61  6D 70 6C 65  file_example
3002F040   5F 4A 50 47  5F 31 30 30  6B 42 2E 6A  _JPG_100kB.j
3002F04C   70 67 00 00  0E 00 00 00  10 00 08 01  pg..........
3002F058   70 6C 69 6B  2E 74 78 74  0F 00 00 00  plik.txt....
3002F064   24 00 1A 01  66 69 6C 65  5F 65 78 61  $...file_exa
3002F070   6D 70 6C 65  5F 4D 50 33  5F 37 30 30  mple_MP3_700
3002F07C   4B 42 2E 6D  70 33 00 00  10 00 00 00  KB.mp3......
3002F088   34 00 16 01  66 69 6C 65  2D 73 61 6D  4...file-sam
3002F094   70 6C 65 5F  31 30 30 6B  42 2E 64 6F  ple_100kB.do
3002F0A0   63 78 00 00  00 00 00 00  00 00 00 00  cx..........
3002F0AC   00 00 00 00  00 00 00 00  00 00 00 00  ............
3002F0B8   11 00 00 00  3C 0F 0C 01  61 72 63 68  ....<...arch
3002F0C4   69 77 75 6D  2E 7A 69 70  00 00 00 00  iwum.zip....
───  sdb1       --0×3002F0C9/0×7FF00000--38%──────────────────
```

Rysunek 13: wynik dla wyszukania „zip”

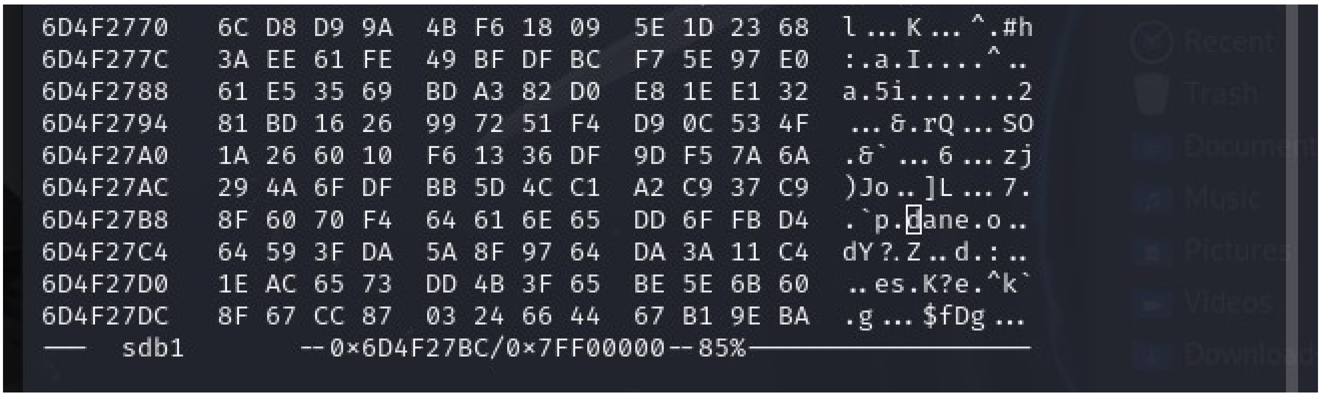
dd:



```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=/dev/urandom of=/dev/sdb1 bs=1M
dd: error writing '/dev/sdb1': No space left on device
2048+0 records in
2047+0 records out
2146435072 bytes (2.1 GB, 2.0 GiB) copied, 18.0939 s, 119 MB/s

┌──(kali㉿kali)-[~]
```

Rysunek 14: nadpisanie partycji; dd

hexedit:



```
6D4F2770   6C D8 D9 9A  4B F6 18 09  5E 1D 23 68  l...K...^.#h
6D4F277C   3A EE 61 FE  49 BF DF BC  F7 5E 97 E0  :.a.I....^..
6D4F2788   61 E5 35 69  BD A3 82 D0  E8 1E E1 32  a.5i.......2
6D4F2794   81 BD 16 26  99 72 51 F4  D9 0C 53 4F  ...&.rQ...SO
6D4F27A0   1A 26 60 10  F6 13 36 DF  9D F5 7A 6A  .&`...6...zj
6D4F27AC   29 4A 6F DF  BB 5D 4C C1  A2 C9 37 C9  )Jo..]L...7.
6D4F27B8   8F 60 70 F4  64 61 6E 65  DD 6F FB D4  .`p.dane.o..
6D4F27C4   64 59 3F DA  5A 8F 97 64  DA 3A 11 C4  dY?.Z..d.:..
6D4F27D0   1E AC 65 73  DD 4B 3F 65  BE 5E 6B 60  ..es.K?e.^k`
6D4F27DC   8F 67 CC 87  03 24 66 44  67 B1 9E BA  .g...$fDg...
──   sdb1       --0×6D4F27BC/0×7FF00000--85%──────────────────
```

Rysunek 15: wynik przeszukania dla zawartości pliku .txt

Komentarz: wydaję mi się, że jest to przypadkowy zbieg okoliczności powstały w wyniku nadpisywania losowymi danymi. Pełna zawartość pliku to: „przykladowe_dane”.

Przeszukanie po pełnej zawartości pliku nie daje wyniku.

Podobna sytuacja zaszła po wyszukaniu „zip” – to wyrażenie zostało znalezione ale najpewniej jest to element losowego ciągu. Wyszukanie „archiwum” nie zwraca nic.

Zadanie 4.

Sprawdź w hexedytorze czy pliki są widoczne

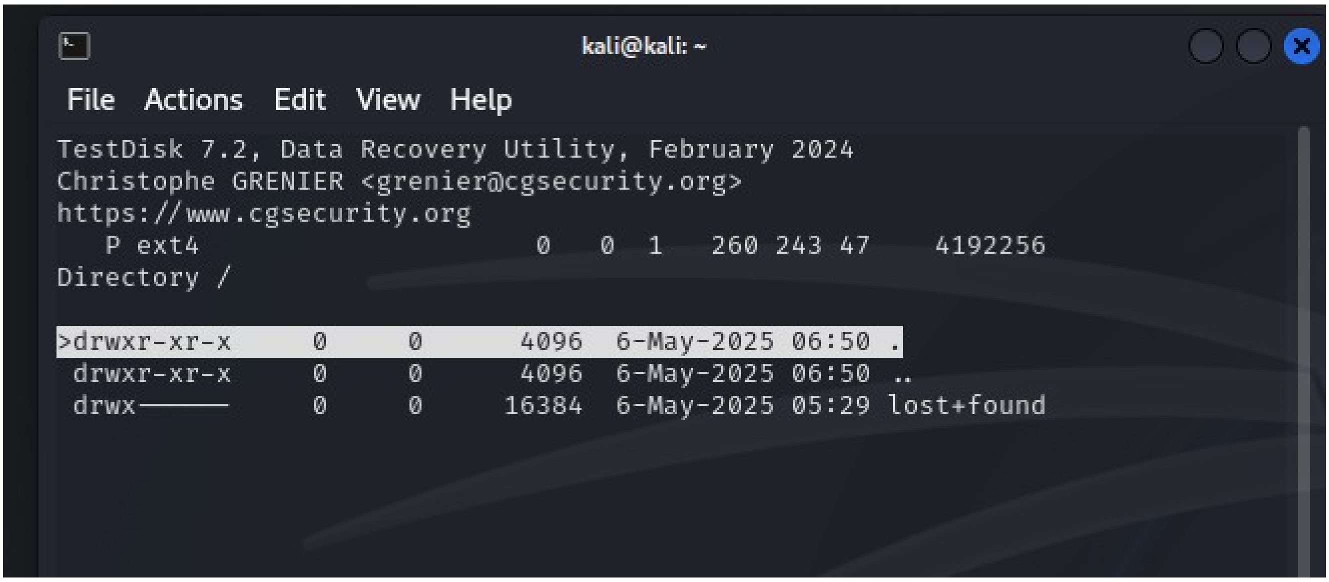
Zadanie zostało wykonane podczas wykonywania zadania 3.

Zadanie 5.

Spróbuj odzyskać pliki za pomocą jednego z programów: testdisk, photorec lub extundelete.

Komentarz: do zadania wykorzystany zostanie program testdisk: będzie wykorzystany na migawce z plikami usuniętymi *shred* oraz na migawce z dyskiem nadpisanym przez *dd.*

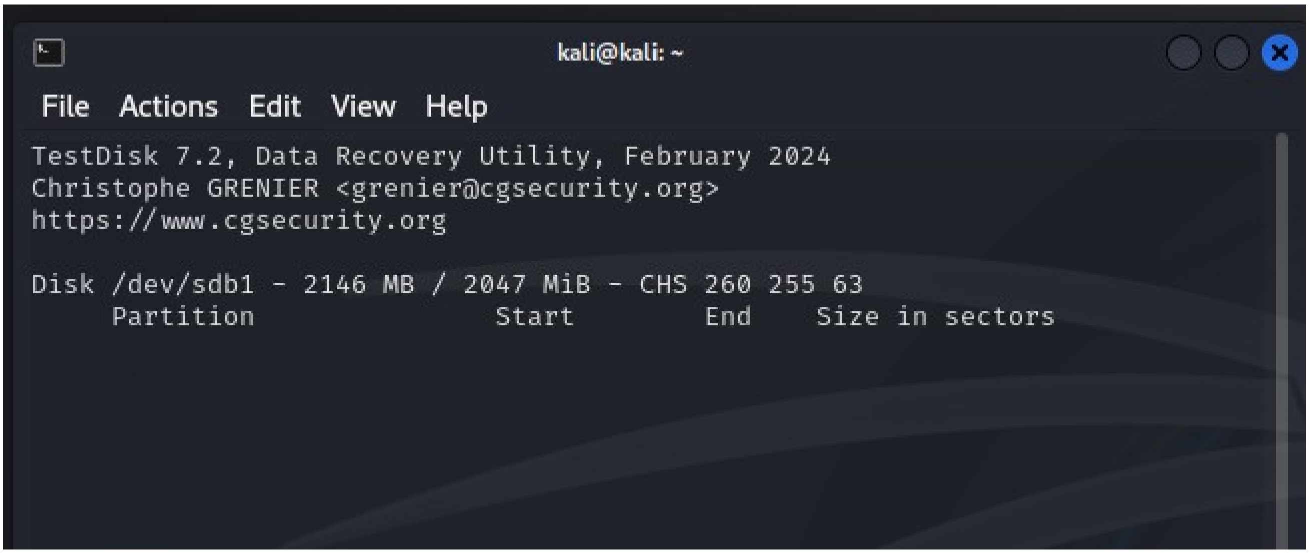
testdisk po shred:



```
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
   P ext4                     0   0  1   260 243 47    4192256
Directory /

>drwxr-xr-x     0     0      4096  6-May-2025 06:50 .
 drwxr-xr-x     0     0      4096  6-May-2025 06:50 ..
 drwx------     0     0     16384  6-May-2025 05:29 lost+found
```

Rysunek 16: próba odzyskania plików; testdisk

testdisk po dd:



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

Disk /dev/sdb1 - 2146 MB / 2047 MiB - CHS 260 255 63
     Partition               Start        End    Size in sectors
```

Rysunek 17: próba odzyskania plików; testdisk

3. Wnioski

Ze wszystkich (innych niż rm) zastosowanych metod wszystkie zdają się usunąć zawartość plików, które chcemy trwale usunąć. *Shred* oraz *wipe* nie usunęły natomiast informacji o nazwach plików, które można było zobaczyć po analizie hexedytorem. Mimo to, przynajmniej w przypadku *shred* dane i tak pozostają nie do odzyskania. Najbardziej przekonującym narzędziem okazało się dd, ponieważ całkowicie zatarł informacje o jakichkolwiek plikach na dysku.