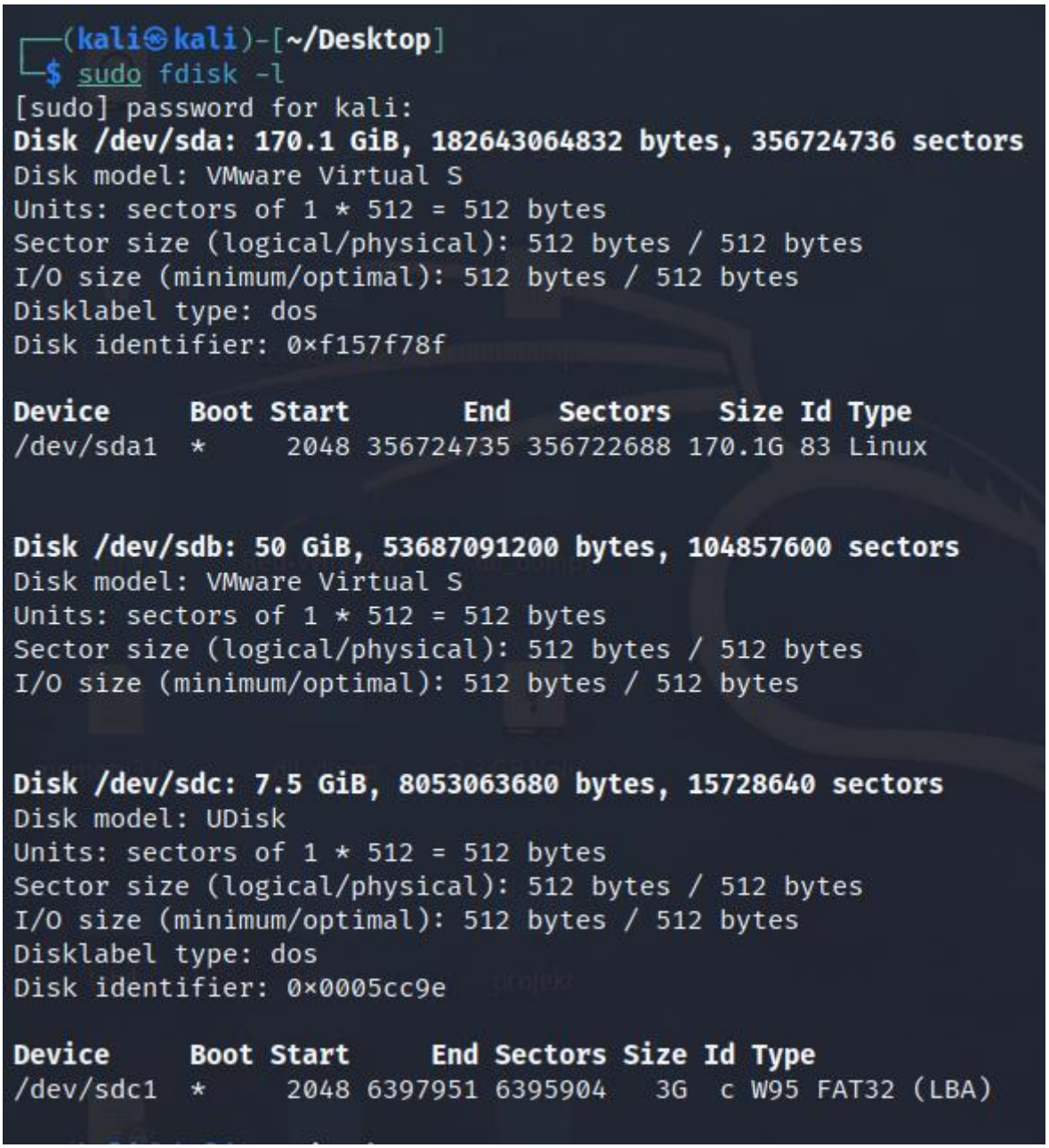
Odzyskiwanie straconych danych przy pomocy odpowiednich narzędzi – Szymon Szkarłat

Celem zadania 3 projektu jest odzyskanie utraconych danych przy pomocy odpowiednich narzędzi. Nośnik, z którego korzystałem podczas tego etapu projektu zawiera dane, które wcześniej odpowiednio przygotowałem.

Sprawdzenie podpiętych urządzeń przy pomocy polecenia sudo fdisk -l

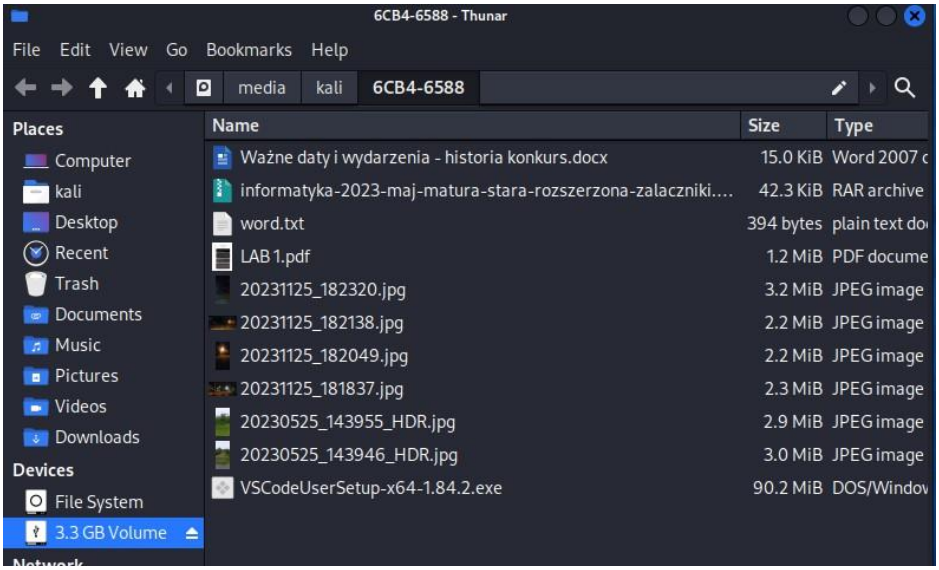


Nasz pendrive jest podpięty.

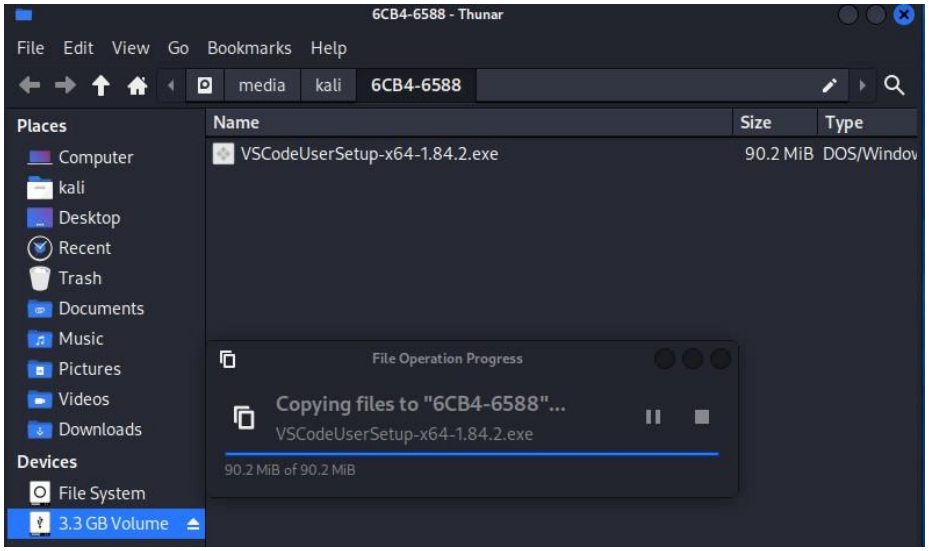
Następnie czyścimy zawartość pendrive'a

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo dc3dd wipe=/dev/sdc1

dc3dd 7.2.646 started at 2023-12-29 12:48:04 -0500
compiled options:
command line dc3dd wipe=/dev/sdc1
device size: 6395904 sectors (probed),    3,274,702,848 bytes
sector size: 512 bytes (probed)
  283639808 bytes ( 270 M ) copied (  9% ),    4 s, 62 M/s
```

Kopiujemy dane na czysty pendrive, a następnie usuwamy je



Następnie umieszczam plik – jest to instalka VSCode



Oczywiście wykonuję kopię binarną, używając do tego celu polecenia dc3dd

```
┌──(kali㉿kali)-[/media/kali]
└─$ sudo dc3dd if=/dev/sdb1 hof=/home/kali/Desktop/lab4/usb-image.dd hash=md5
 log=/home/kali/Desktop/file-log

dc3dd 7.2.646 started at 2023-11-25 13:09:45 -0500
compiled options:
command line dc3dd if=/dev/sdb1 hof=/home/kali/Desktop/lab4/usb-image.dd hash
=md5 log=/home/kali/Desktop/file-log
device size: 6395904 sectors (probed),    3,274,702,848 bytes
sector size: 512 bytes (probed)
```

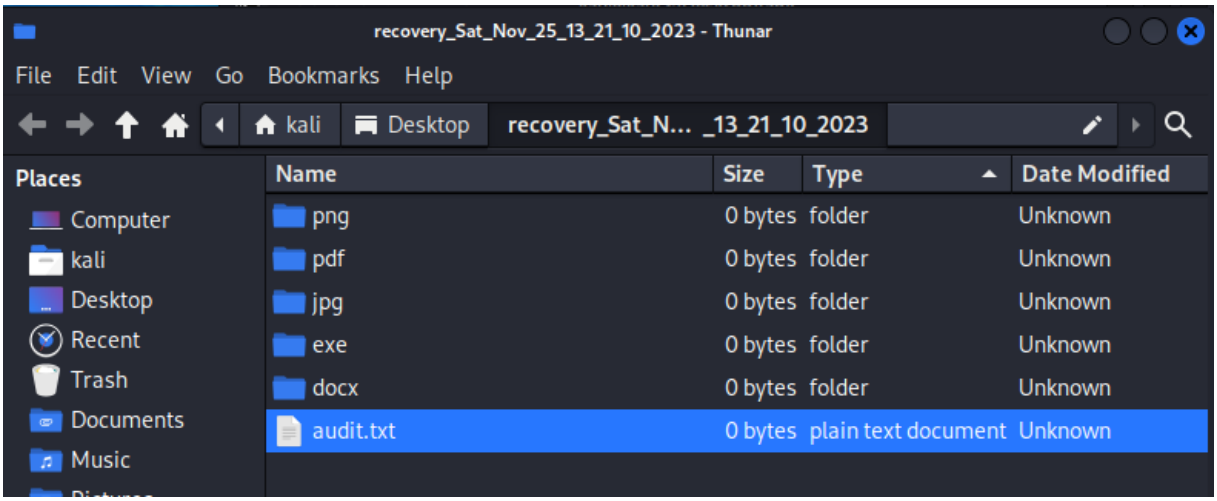
Ukończenie kopii binarnej

```
  3274702848 bytes ( 3 G ) copied ( 100% ),  285 s, 11 M/s

  3274702848 bytes ( 3 G ) hashed ( 100% ),    5 s, 597 M/s

input results for device `/dev/sdb1':
   6395904 sectors in
   0 bad sectors replaced by zeros
   d7710490ae4087a4cad26ab572e57667 (md5)

output results for file `/home/kali/Desktop/lab4/usb-image.dd':
   6395904 sectors out
   [ok] d7710490ae4087a4cad26ab572e57667 (md5)

dc3dd completed at 2023-11-25 13:14:30 -0500
```

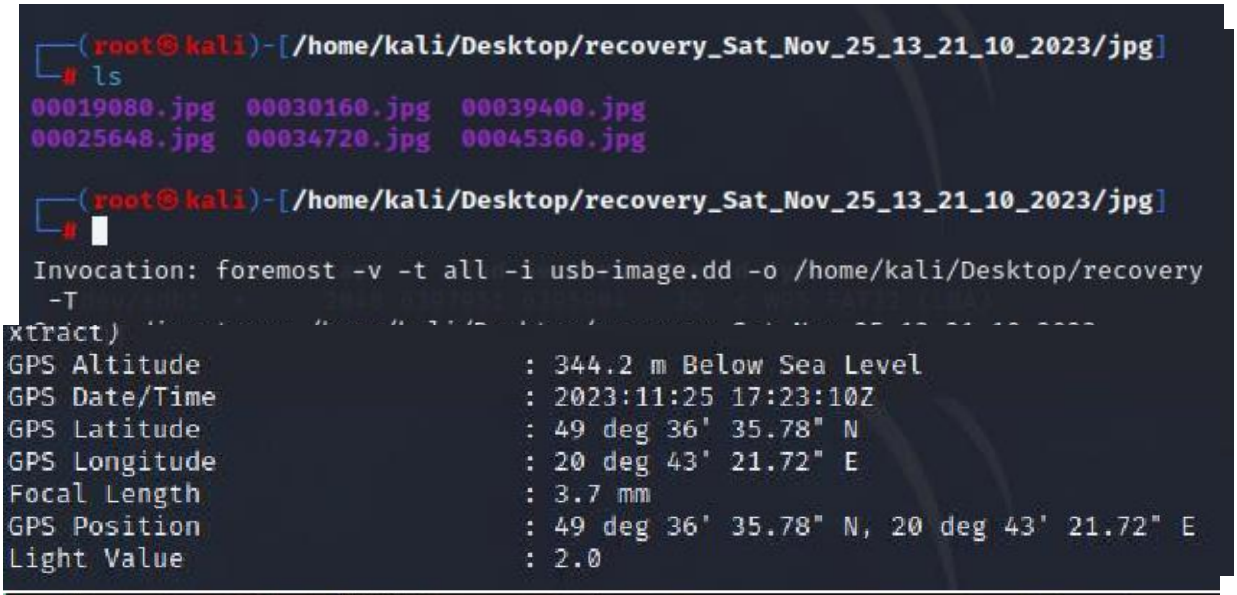
Odzyskanie danych przy pomocy narzędzia Formost

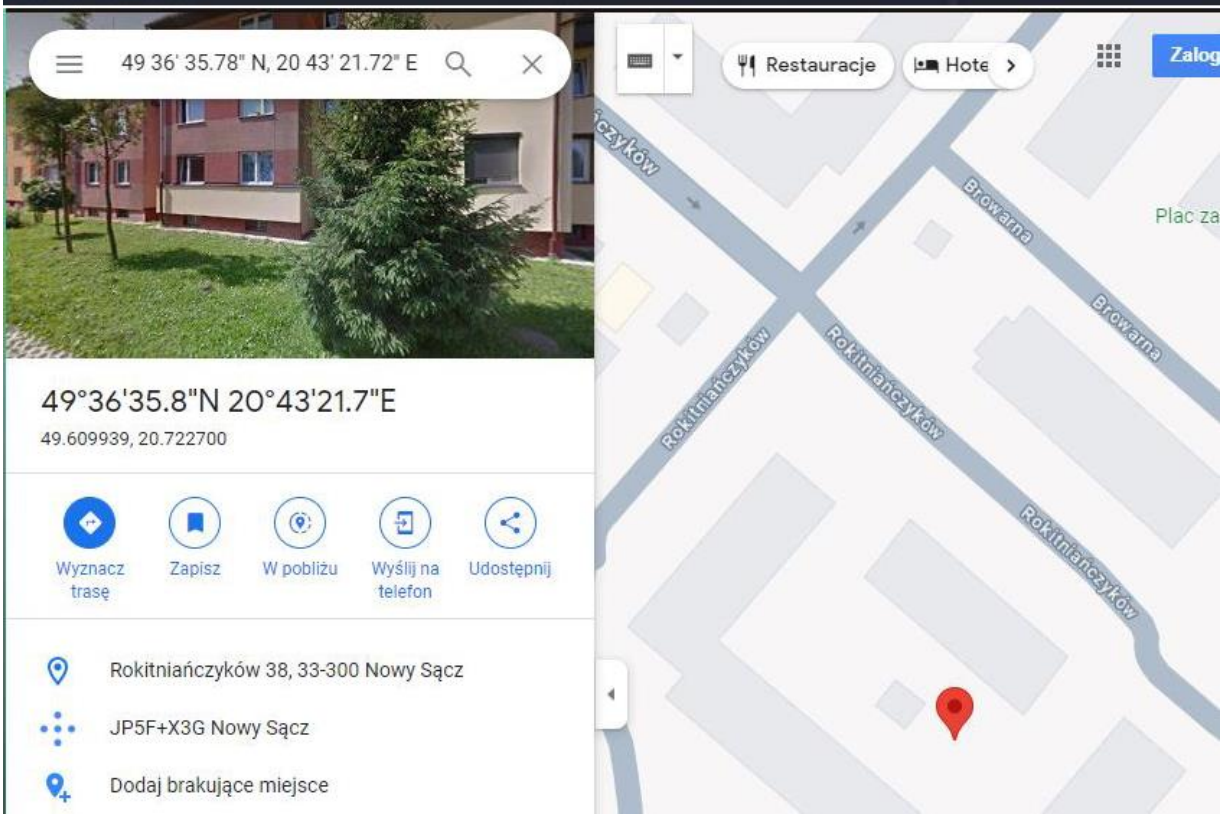
Po zainstalowaniu, odzyskiwanie danych za pomocą narzędzia Foremost

Udało się odzyskać dane



Wyświetlenie zwartości katalogu recovery jako root. Znajdują się tutaj odzyskane dane w formacie jpg





Użycie exiftool na przykładowym zdjęciu

```
┌──(root㉿kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023/jpg]
└─# exiftool 00019080.jpg
ExifTool Version Number         : 12.65
File Name                       : 00019080.jpg
Directory                       : .
File Size                       : 3.4 MB
File Modification Date/Time     : 2023:11:25 13:21:10-05:00
File Access Date/Time           : 2023:11:25 13:21:10-05:00
File Inode Change Date/Time     : 2023:11:25 13:21:10-05:00
File Permissions                : -rw-r--r--
```

Pozyskane metadane zdjęcia

Nie udało mi się odzyskać pliku w formacie rar. Odzyskano natomiast pozostałe pliki

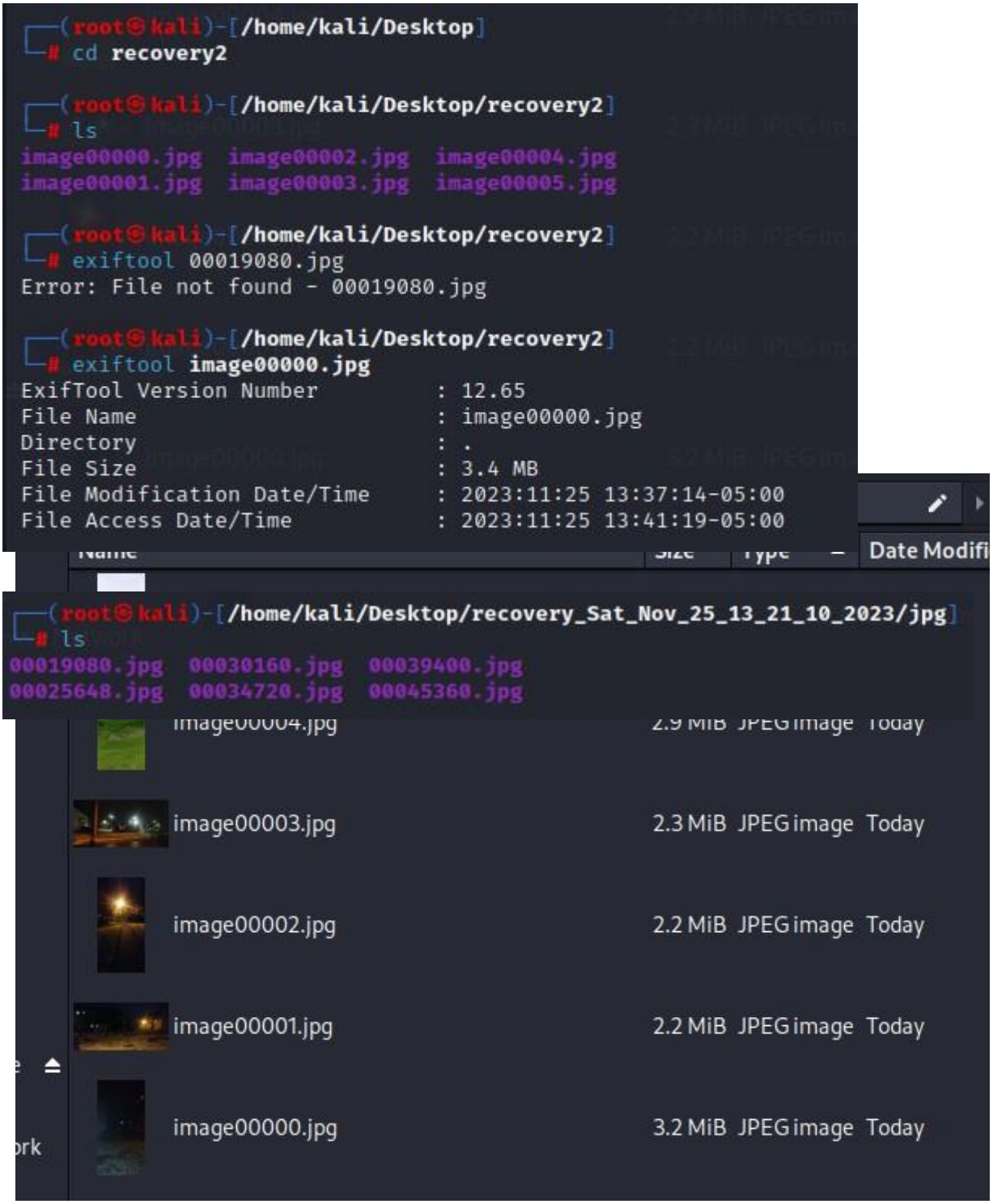
```
┌──(root㉿kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023]
└─# ls
audit.txt  docx  exe  jpg  pdf  png
```

Innym narzędziem, które wykorzytsałem do odzyskiwania danych jest Recoverjpeg

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# recoverjpeg -o recovery2 /dev/sdb1
Restored 6 pictures

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

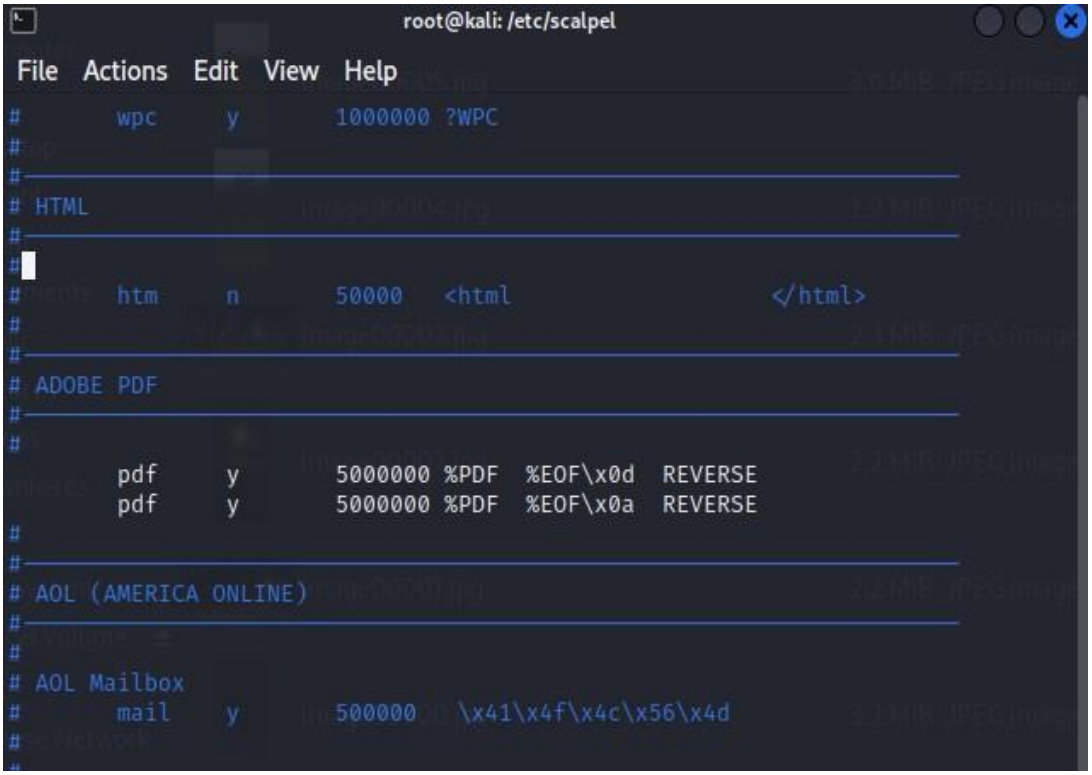
Odzyskałem wszystkie zdjęcia, było dokładnie 6.

Zaleta tego narzędzia jest możliwość podejrzenia i zobaczenia co znajduje się na zdjęciach. W przypadku

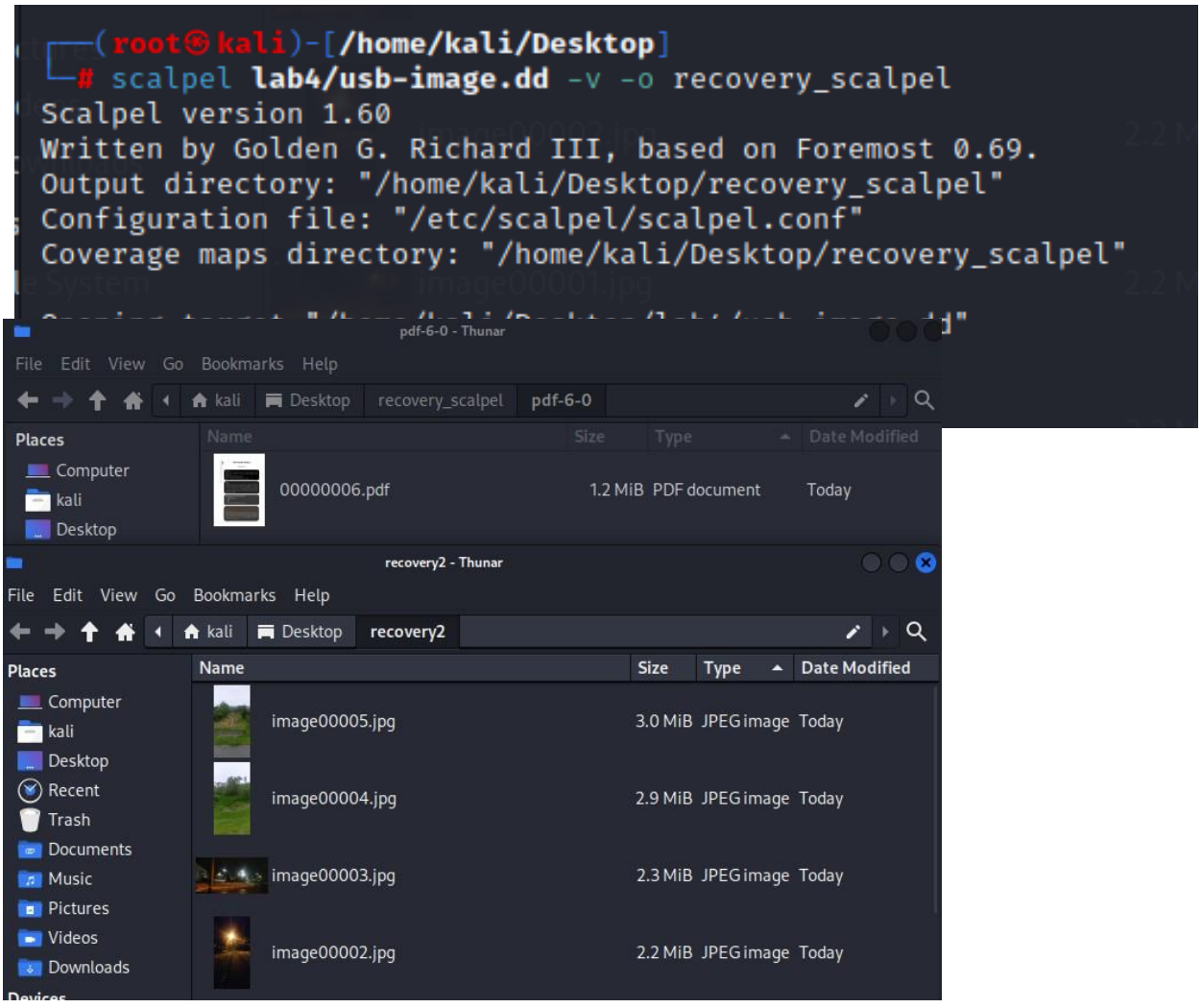


narzędzia Formost nie było to możlwie.
W przypadku Foremost tak wygląda folder z odzyskanymi danymi

Narzędzie Scalpel – jest to narzędzie dostępne domyślnie
Wprowadziłem modyfikację w pliku konfiguracyjnym

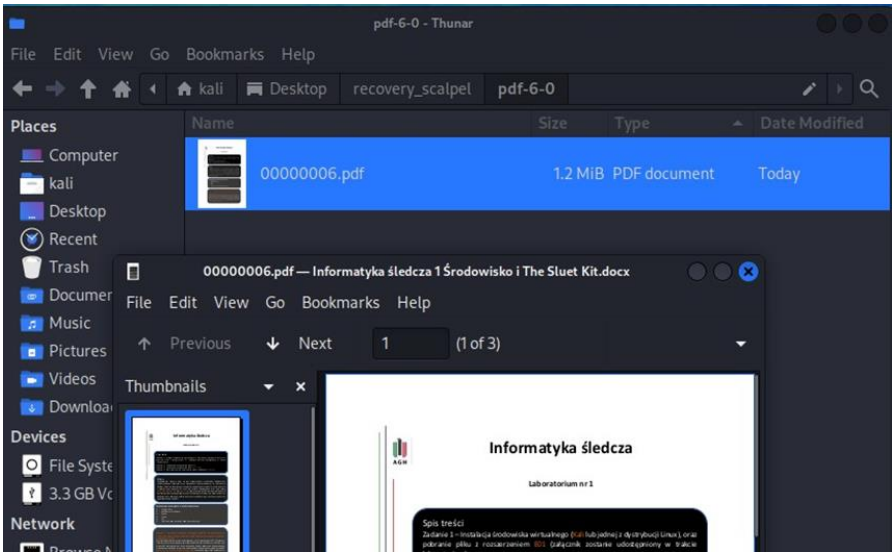


Uruchomienie narzędzia Scalpel
Scalpel odzyskał jedynie pliki w formacie pdf oraz zdjęcia wraz z metadanymi. W przeciwieństwie do innych narzędzi nie odzyskał np. pliku word oraz exe. Pomimo tego, że opcje te zostały odznaczone w pliku konfiguracyjnym.



```
# MICROSOFT OFFICE
#----------------------------------------------------------
#
# Word documents
#
#
        doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \x
d0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 NEXT
        doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
#       pst     y       500000000       \x21\x42\x4e\xa5\x6f\xb5\xa6
#       ost     y       500000000       \x21\x42\x44\x4e
#
# Outlook Express
#       dbx     y       10000000        \xcf\xad\x12\xfe\xc5\xfd\x74\x6f
```

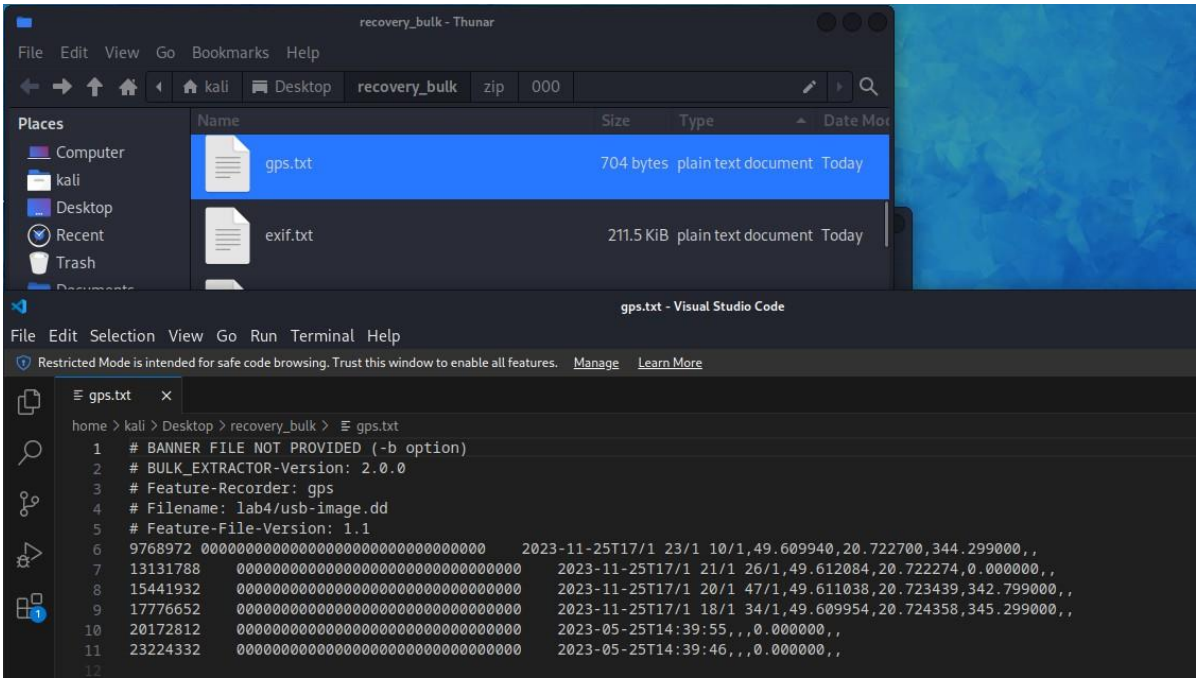
Tylko to udało się odzyskać, przy pomocy narzędzia scalpel. Nie udało się odzyskać plików exe oraz rar. Nazwy plików również zostały zmienione. Dodatkową opcją jest niewątpliwie możliwość podejrzenia pliku pdf.



Uruchomienie Bulk_Extractora. Bulk_Extractor okazał się narzędziem, który przechwycił najwięcej danych, dokonał tego w szczegółowy sposób. Z pewnością przy pomocy tego narzędzia można dowiedzieć się bardzo wielu informacji o odzyskanych danych (np. metadane zdjęć).

```
┌──(kali㉿kali)-[~/Desktop]
└─$ bulk_extractor -o recovery_bulk lab4/usb-image.dd
mkdir "recovery_bulk"
bulk_extractor version: 2.0.0
Input file: "lab4/usb-image.dd"
Output directory: "recovery_bulk"
Disk Size: 3274702848
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carve
d msxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_ca
rved windirs winlnk winpe winprefetch zip accts email gps
Threads: 4
going multi-threaded ... ( 4 )
bulk_extractor      Sat Nov 25 14:01:22 2023
```

Prezentowana zawartość pliku tekstowego, który zawiera informacje o metadanych zdjęć



Podsumowanie procesu odzyskiwania danych.

Uważam, że wszystkie wykorzystane podczas laboratorium narzędzia wyróżniają się na tle innych. Foremost jest zdecydowanie najprostszy, tzn. przedstawia odzyskana dane tylko w sposób konsolowy, nie mamy możliwości podejrzenia zawartości pliku pdf czy zdjęcia, które udało się odzyskać.
Zdecydowanie więcej plików udało się odzyskać przy użyciu narzędzia Scalpel. Ciekawy jest fakt, że przeciwieństwie do Foremost możliwe było otworzenie i przeglądniecie zawartości odzyskanych plików, co stanowi doskonałą nagrodę i gratyfikację trudów dla osoby, które zajmowała się odzyskiwaniem danych. Poprawne i właściwe użycie Scalpel wymagało jednak modyfikacji pliku konfiguracyjnego, czyli odznaczenie odpowiednich opcji, tak aby odzyskać pliki o konkretnych rozszerzeniach.
Na koniec Bulk_Extractor, który generował masę informacji o odzyskanych plikach. Są to bardzo szczegółowe i pracochłonne do przeanalizowania dane, umieszczone w plikach tekstowych. Co może wiązać się z użyciem różnego rodzaju innych narzędzi w celu dokładnego przeanalizowania pozyskanych danych. Bulk_Extractor może okazać się przydatny podczas analizy czy odzyskiwania plików o dużej wadze.

Podczas odzyskiwania nie udało się w żaden sposób odzyskać zarchiwizowanych katalogów (format zip oraz rar). Scalpel natomiast nie odzyskał także pliku exe.

Uważam, że najlepszym do odzyskiwania jest Scalpel, ze względu na jego duże możliwości oraz prosty sposób wykorzystania. Nie mniej jeżeli nie interesuje nas wygląd odzyskanych danych, tylko np. metadane zdjęcia warto użyć Foremost (bo jest szybszy oraz prostszy od Scalpela, nie trzeba modyfikować pliku scalpel.conf).