

Zadanie 1 – Przygotowanie do odzyskiwania danych

użycie komendy `sudo dc3dd wipe=/dev/sdb1`

```
dc3dd 7.2.646 started at 2022-11-28 10:37:32 +0100
compiled options:
command line: dc3dd wipe=/dev/sdb1
device size: 15726592 sectors (probed),      8,052,015,104 bytes
sector size: 512 bytes (probed)
  8052015104 bytes ( 7,5 G ) copied ( 100% ),  666 s, 12 M/s

input results for pattern `00':
  15726592 sectors in

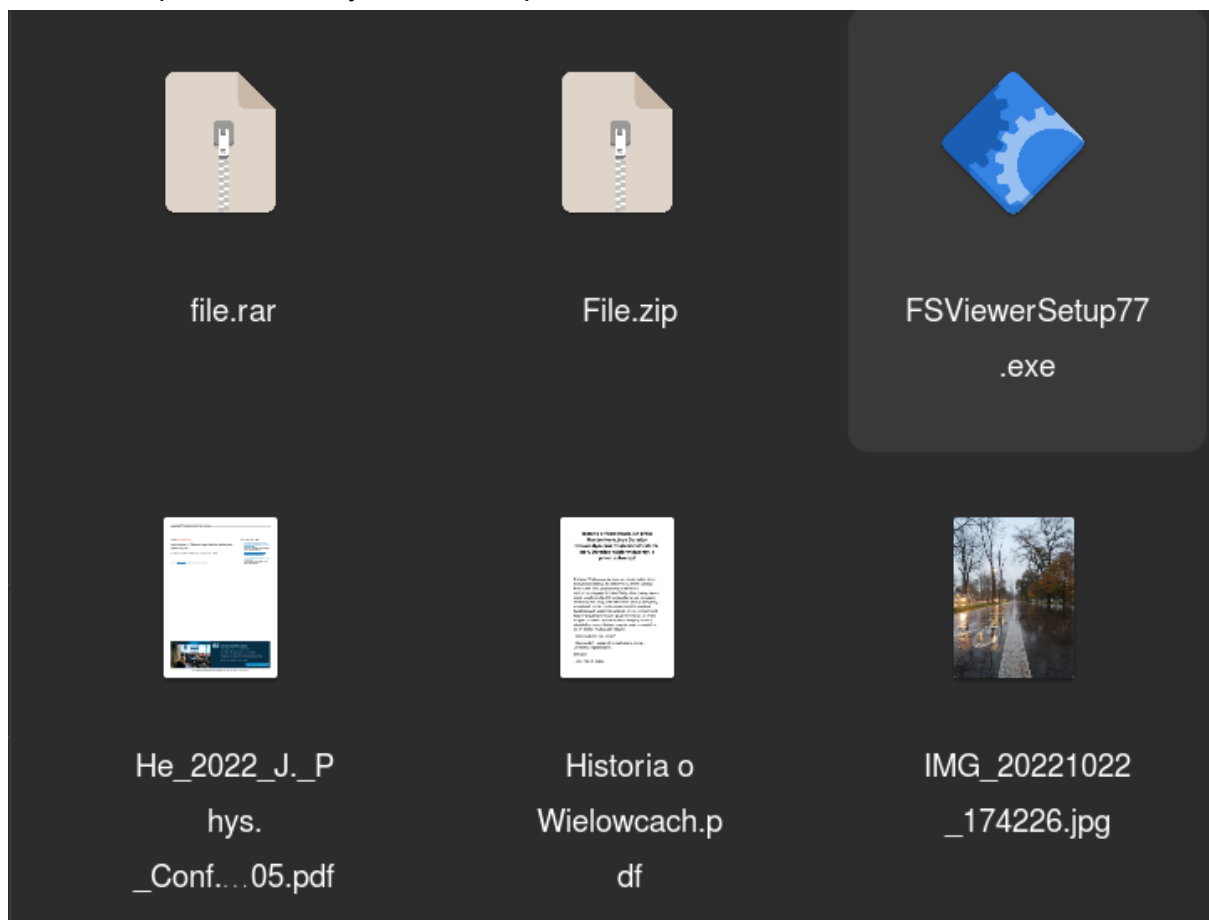
output results for device `/dev/sdb1':
  15726592 sectors out

dc3dd completed at 2022-11-28 10:48:38 +0100
```

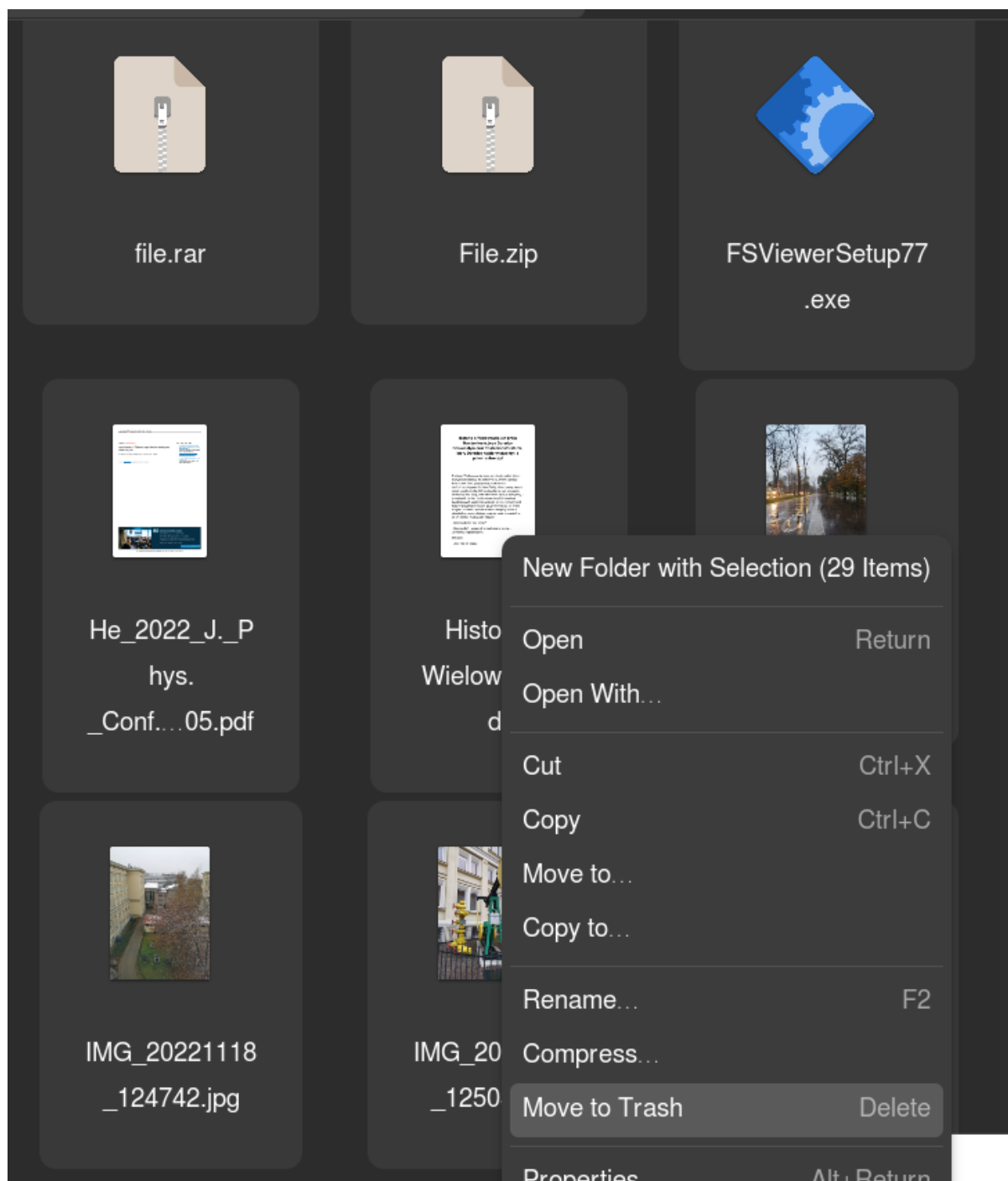
Warto zaznaczyć iż proces trwał naprawdę długo, a wraz z upływem czasu spada prędkość kopiowania danych

Z tego co udało mi się wyczytać, zmiana wielkości I/O oraz sector size na większą by pomogła

Utworzenie plików tekstowych, rar, doc, pdf oraz .exe



Następnie skopiowanie tych plików na nośnik oraz usunięcie



Następnie przeniesienie pliku (95,5 MB) na pendrive

By wykonać kopie binarną najpierw trzeba znaleźć, gdzie znajdują się obraz pendrive (komenda `df`):

```
/dev/sdb1      7861248    138880    7722368    2% /run/media/arek/EBEE-E533
```

```
[arek@fedora lab4] $ sudo dc3dd if=/dev/sdb1 of=/home/arek/astudia/is/lab4/dc3 hash=md5

dc3dd 7.2.646-dirty started at 2022-11-28 11:52:47 +0100
compiled options:
command line: dc3dd if=/dev/sdb1 of=/home/arek/astudia/is/lab4/dc3 hash=md5
device size: 15726592 sectors (probed),      8,052,015,104 bytes
sector size: 512 bytes (probed)
      8052015104 bytes ( 7.5 G ) copied ( 100% ),  448 s, 17 M/s

input results for device `/dev/sdb1':
 15726592 sectors in
   0 bad sectors replaced by zeros
 2fad156417a2a0417bdd1f1a8c78306 (md5)

output results for file `/home/arek/astudia/is/lab4/dc3':
 15726592 sectors out

dc3dd completed at 2022-11-28 12:00:15 +0100
```

checksum się zgadza

```
[arek@fedora lab4] $ md5sum dc3
2fad156417a2a0417bdd1f1a8c78306  dc3
```

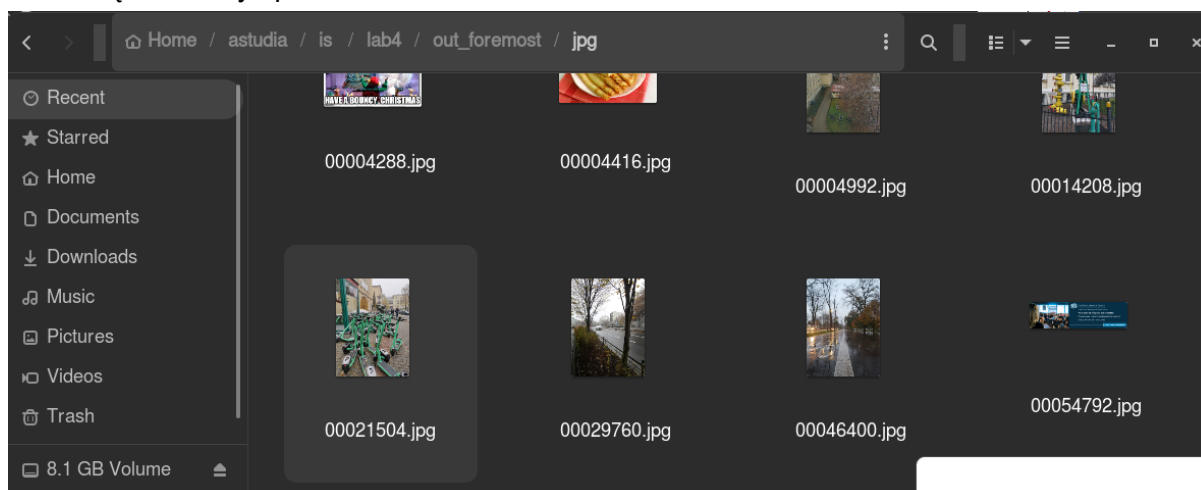
dane zostały poprawnie skopiowane

Zadanie 2 – Foremost

Przykładowe odtworzenie plików z rozszerzeniem .jpg

```
[arek@fedora lab4] $ foremost -t pdf,jpg -i dc3 -o ~/astudia/is/lab4/out_foremost
Processing: dc3
|*****|
```

Udało się odtworzyć pliki:



Są to wszystkie pliki, które były dostępne w obrazie nośnika, a nawet jeden dodatkowy (7 plików w obrazie a 8 w folderze z outputu)

```

[arek@fedora lab4] $ find . -type f \( -name "*.jpg" \)
./IMG_20221022_174226.jpg
./IMG_20221118_125642.jpg
./IMG_20221118_125210.jpg
./IMG_20221118_125034.jpg
./IMG_20221118_124742.jpg
./out_foremost/jpg/00004288.jpg
./out_foremost/jpg/00004416.jpg
./out_foremost/jpg/00004992.jpg
./out_foremost/jpg/00014208.jpg
./out_foremost/jpg/00021504.jpg
./out_foremost/jpg/00029760.jpg
./out_foremost/jpg/00046400.jpg
./out_foremost/jpg/00054792.jpg
./w9fg3-452397450.jpg
./Naleśniki+2+copy-950915506.jpg

```

Foremost tworzy plik tekstowy wraz z raportem - listuje pliki, które udało się odzyskać, rozszerzenia, użytą komendę i konfig

34 FILES EXTRACTED

```

jpg:= 8
zip:= 8
exe:= 1
png:= 13
pdf:= 4

```

Warto zaznaczyć iż foremost ma ustawione domyślnie naprawdę mało rozszerzeń (w naszym przypadku tylko jpg,exe,pdf,zip,rar). Trzeba manualnie w configu dodać odt,epub,dcx)

```

# Word documents
# (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
# doc y 12500000 \xd0\xcf\x11\xe0\xa1\xb1
# docx n 12500000 _rels [Content_Types]
# odt n 12500000 mimetypeapplication META-INF
#

```

oraz zastosować lekko zmienioną komendę:

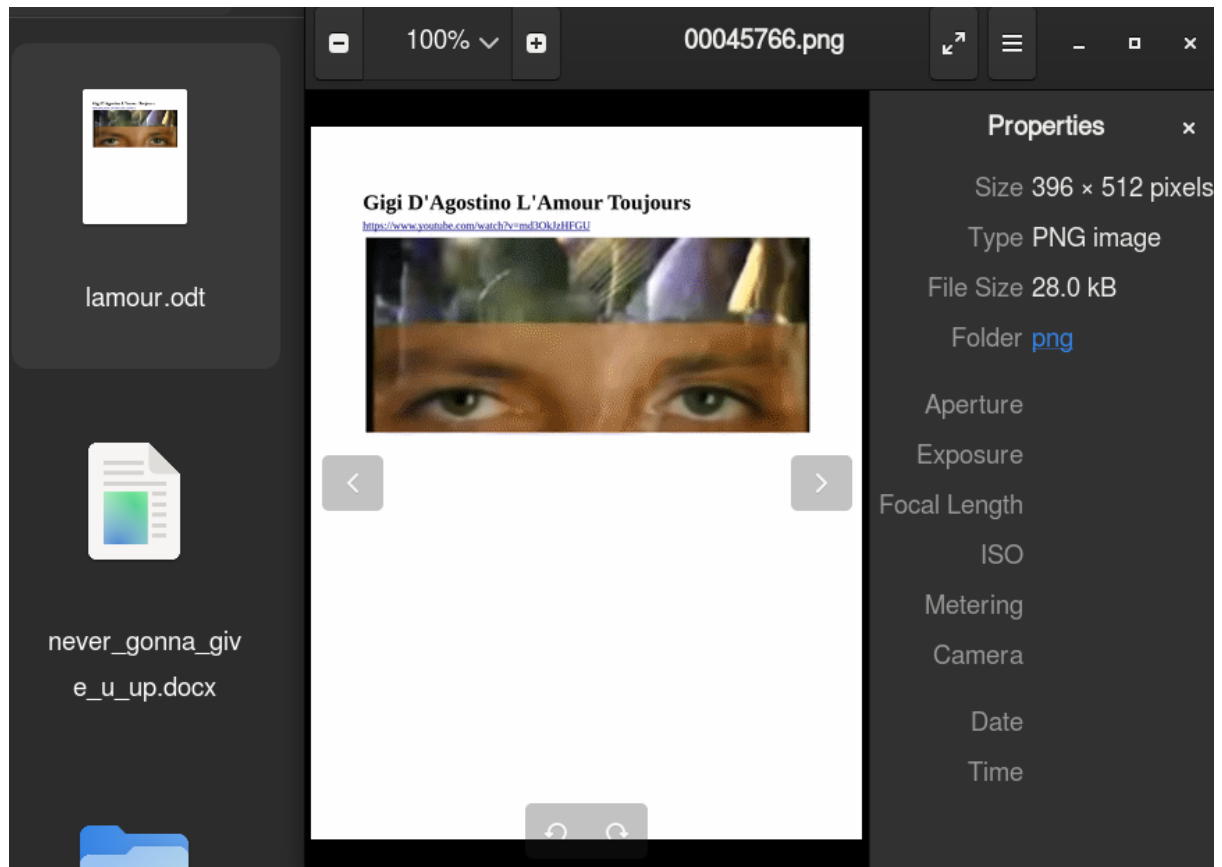
```

[arek@fedora lab4] $ foremost -c /etc/foremost.conf -i dc3 -o ~/astudia/is/lab4/output -T -v

```

Niestety nie udało się wprost odzyskać plików z innym rozszerzeniem. Prawdopodobnie mam błąd w configu 😞

Aczkolwiek nastąpił dziwny zwrot wydarzeń - zawartość, która była w plikach .odt, .epub, .docx znalazła się w folderze png wraz z rzutem zawartości w formie obrazka



Foremost potrafi też wydobyć zdjęcia znajdujące się w środku innych plików (właśnie .odt, .docx, .pdf itp.)

Sprawdźmy więc integralność danych - na przykładzie metadanych zdjęć .jpg

Skierowałem output z komendy `exiftool` obu zdjęć do pliku tekstowego, następnie zastosowałem komendę uniq

```
[arek@fedora lab4] $ cat oryginalne.txt | sort | uniq -D
Aperture : 1.8
Aperture : 1.8
Aperture Value : 1.8
Aperture Value : 1.8
Bits Per Sample : 8
Bits Per Sample : 8
Brightness Value : 0
Brightness Value : 0
Camera Model Name : LYA-L29
Camera Model Name : LYA-L29
Circle Of Confusion : 0.006 mm
Circle Of Confusion : 0.006 mm
Color Components : 3
Color Components : 3
Color Space : sRGB
Color Space : sRGB
Components Configuration : Y, Cb, Cr, -
Components Configuration : Y, Cb, Cr, -
Compressed Bits Per Pixel : 0.95
Compressed Bits Per Pixel : 0.95
Compression : JPEG (old-style)
Compression : JPEG (old-style)
Contrast : Normal
Contrast : Normal
Create Date : 2022:11:18 12:50:35
Create Date : 2022:11:18 12:50:35
Create Date : 2022:11:18 12:50:35.727089
Create Date : 2022:11:18 12:50:35.727089
Custom Rendered : Custom
Custom Rendered : Custom
Date/Time Original : 2022:11:18 12:50:35
Date/Time Original : 2022:11:18 12:50:35
Date/Time Original : 2022:11:18 12:50:35.727089
Date/Time Original : 2022:11:18 12:50:35.727089
```

```

Focal Length      : 5.6 mm
Focal Length      : 5.6 mm
Focal Length      : 5.6 mm (35 mm equivalent: 27.0 mm)
Focal Length      : 5.6 mm (35 mm equivalent: 27.0 mm)
Focal Length In 35mm Format : 27 mm
Focal Length In 35mm Format : 27 mm
Gain Control      : None
Gain Control      : None
GPS Altitude      : 0 m Above Sea Level
GPS Altitude      : 0 m Above Sea Level
GPS Altitude Ref  : Below Sea Level
GPS Altitude Ref  : Below Sea Level
GPS Date Stamp    : 2022:11:18
GPS Date Stamp    : 2022:11:18
GPS Date/Time     : 2022:11:18 11:50:34Z
GPS Date/Time     : 2022:11:18 11:50:34Z
GPS Latitude      : 50 deg 3' 56.07" N
GPS Latitude      : 50 deg 3' 56.07" N
GPS Latitude Ref  : North
GPS Latitude Ref  : North
GPS Longitude     : 19 deg 55' 12.07" E
GPS Longitude     : 19 deg 55' 12.07" E
GPS Longitude Ref : East
GPS Longitude Ref : East
GPS Position      : 50 deg 3' 56.07" N, 19 deg 55' 12.07" E
GPS Position      : 50 deg 3' 56.07" N, 19 deg 55' 12.07" E
GPS Processing Method : GPS
GPS Processing Method : GPS
GPS Time Stamp    : 11:50:34
GPS Time Stamp    : 11:50:34

```

Wniosek - poprawność danych została zachowana (w tym lokalizacja GPS)

Powtórzyłem podobny proces dla innych zdjęć i efekt był ten sam

Następnie próbuje odzyskać pliki bezpośrednio z nośnika

```

[arek@fedora jpg] $ foremost -c /etc/foremost.conf -i /dev/sdb1 -o ~/astudia/is/lab4/ouot_pendrive -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus

```

```

[arek@fedora jpg] $ foremost -c /etc/foremost.conf -i /run/media/arek/EBEE-E533 -o ~/astudia/is/lab4/ouot_pendrive -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Nov 28 15:43:32 2022
Invocation: foremost -c /etc/foremost.conf -i /run/media/arek/EBEE-E533 -o /home/arek/astudia/is/lab4/ouot_pendrive -v
Output directory: /home/arek/astudia/is/lab4/ouot_pendrive
Configuration file: /etc/foremost.conf
Processing: stdin
|-----
File: stdin
Start: Mon Nov 28 15:43:32 2022
Length: Unknown

Num      Name (bs=512)      Size      File Offset      Comment

```

Niestety, komenda nie zadziałała. Ekran się zawiesił i był brak postępów.

Zadanie 3 – Recoverjpeg

Do powyższego narzędzia użyję maszyny virtualnej z kali linuxem (na fedorze jest problem z instalacją)

Najpierw trzeba zamontować pendrive w maszynie

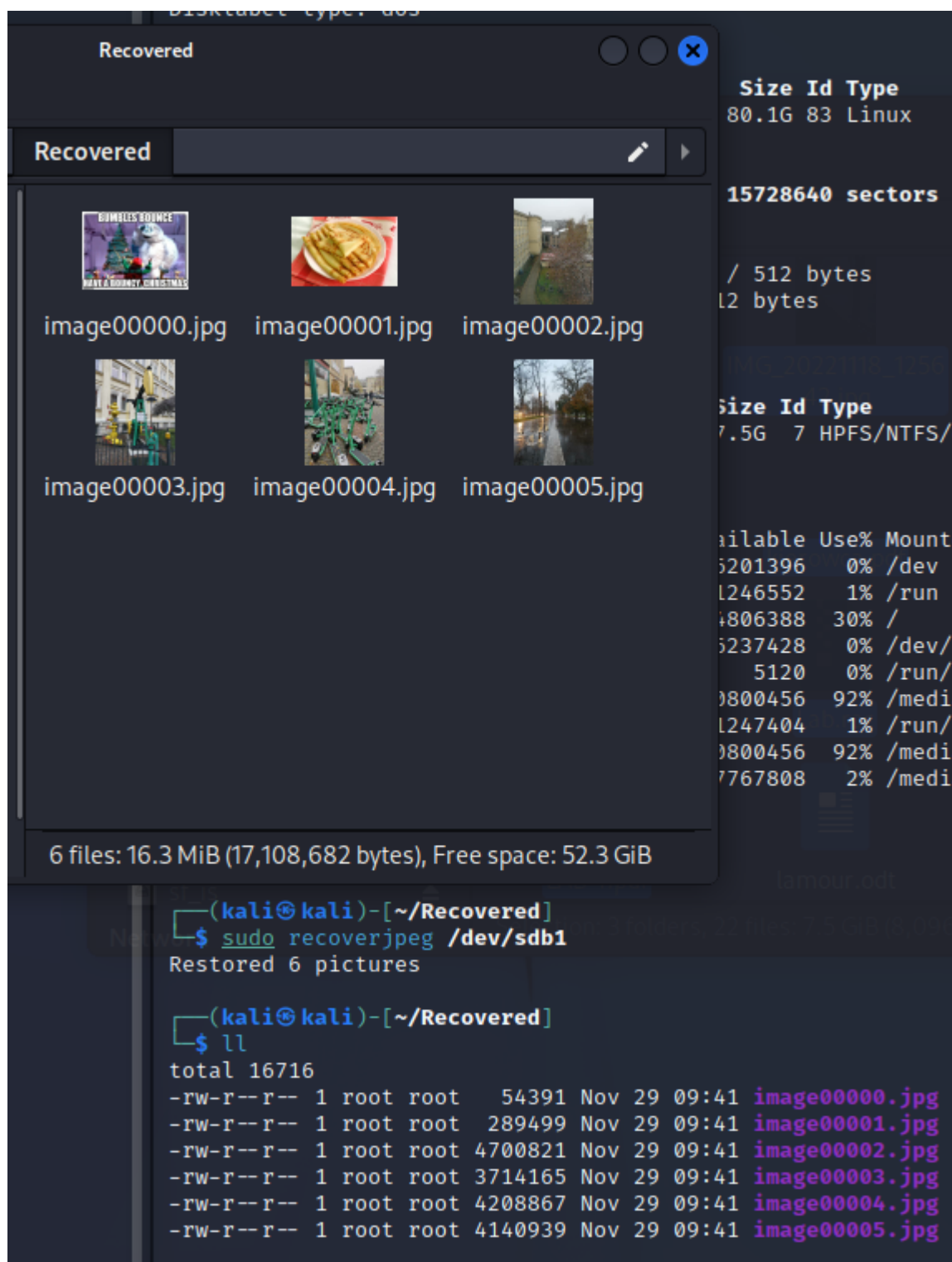
Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sdb1		2048	15728639	15726592	7.5G	7	HPFS/NTFS/exFAT

a następnie wykonuje już komendę z jakże prostą składnią

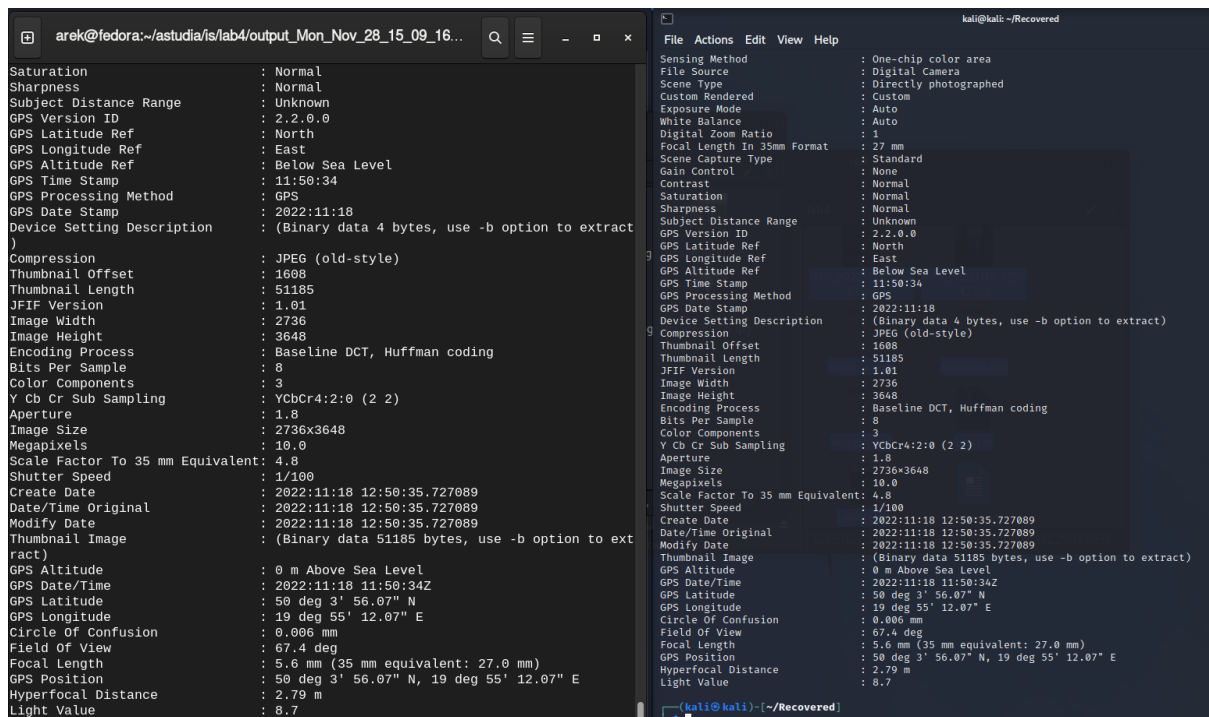
```
(kali㉿kali)-[~/Recovered]  
$ sudo recoverjpeg /dev/sdb1  
Restored 6 pictures
```

Warto zaznaczyć iż program był znacznie wolniejszy od pozostałych (pewnie kwestia ograniczenia maszyny wirtualnej + szybkości pamięci nośnika)

Programowi udało się odnaleźć 6 zdjęć. Jest to liczba mniejsza niż np. foremost. Brakuje jednego zdjęcia oraz prawdopodobnie zdjęcia z zawartości jakiegoś pdf'a/docx'a



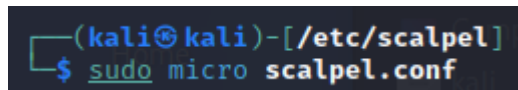
Tak samo jak w innych programach - recoverjpeg nie odzyskuje nazw plików i nadaje swoje



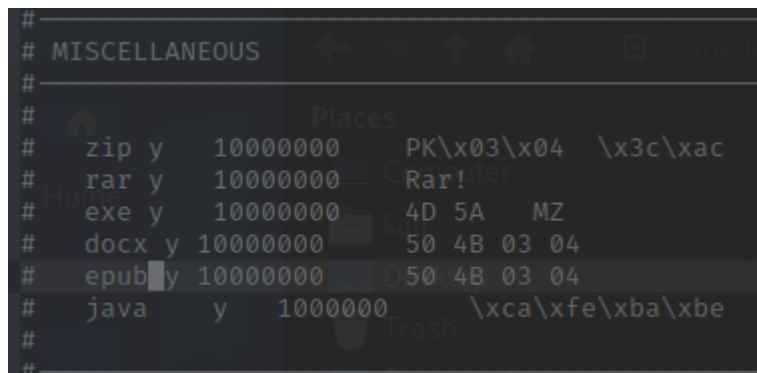
Integralność również została zachowana (również dane lokalizacyjne)
 Sprawdziłem to dla wszystkich odzyskanych plików i również się zgadzało

Zadanie 4 – Scalpel

Edytowanie pliku /etc/scalpel.conf



Dodałem obsługę archiwum .rar, docx, epub, exe według sygnatur z wikipedii



A następnie odznaczyłem interesujące nas opcje

```

Segmentation fault
[arek@fedora lab4] $ sudo scalpel -c /etc/scalpel.conf -o recovered_scalpel -i dc3dd.img
Scalpel version 2.1
Written by Golden G. Richard III and Lodovico Marziale.
Scalpel will write only to empty output directories to avoid
mixing the output from multiple carving operations.
Please specify a different output directory or delete the specified
output directory.
Error opening audit file: Scalpel will write only to empty output directories to avoid
mixing the output from multiple carving operations.
Please specify a different output directory or delete the specified
output directory.
Segmentation fault

```

Wniosek - program nie chciał zadziałać (segmentation fault)

Próbowałem różne obrazy nośników, formaty, dystrybucje linuxa i nic nie pomogło

Po paru godzinach pracy nad odebugowywaniem programemu poddałem się :/

Przesyłam listę rezultatów:

brak

Zadanie 5 – Bulk_Extractor

```

(kali@kali)-[~/lab4]
$ sudo bulk_extractor -e all dc3 -o output_bulk

```

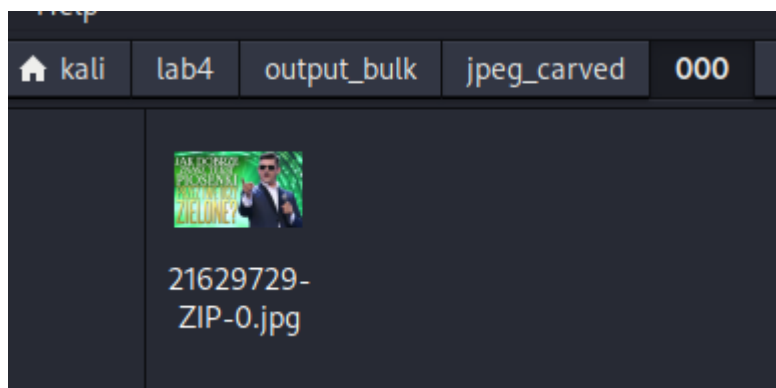
Na maszynie wirtualnej z 2 rdzeniami program działał przez ponad 20 minut!

```

Phase 2. Shutting down scanners
Computing final histograms and shutting down...
Phase 3. Generating stats and printing final usage information
All Threads Finished!
Elapsed time: 1249 sec.
Total MB processed: 8052
Overall performance: 6.445 MBytes/sec 3.223 (MBytes/sec/thread)
sbufs created: 8961053
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data: 0:18:28 (1108.59 seconds)
Time consumer scanners spent waiting for data from producer: 0:00:00 (0.43 seconds)
Average time each consumer spent waiting for data from producer: 0:00:00 (0.00 seconds)
*** More time spent waiting for workers. You need a faster CPU or more cores for improved performance.
Total email features found: 4
(kali@kali)-[~/lab4]

```

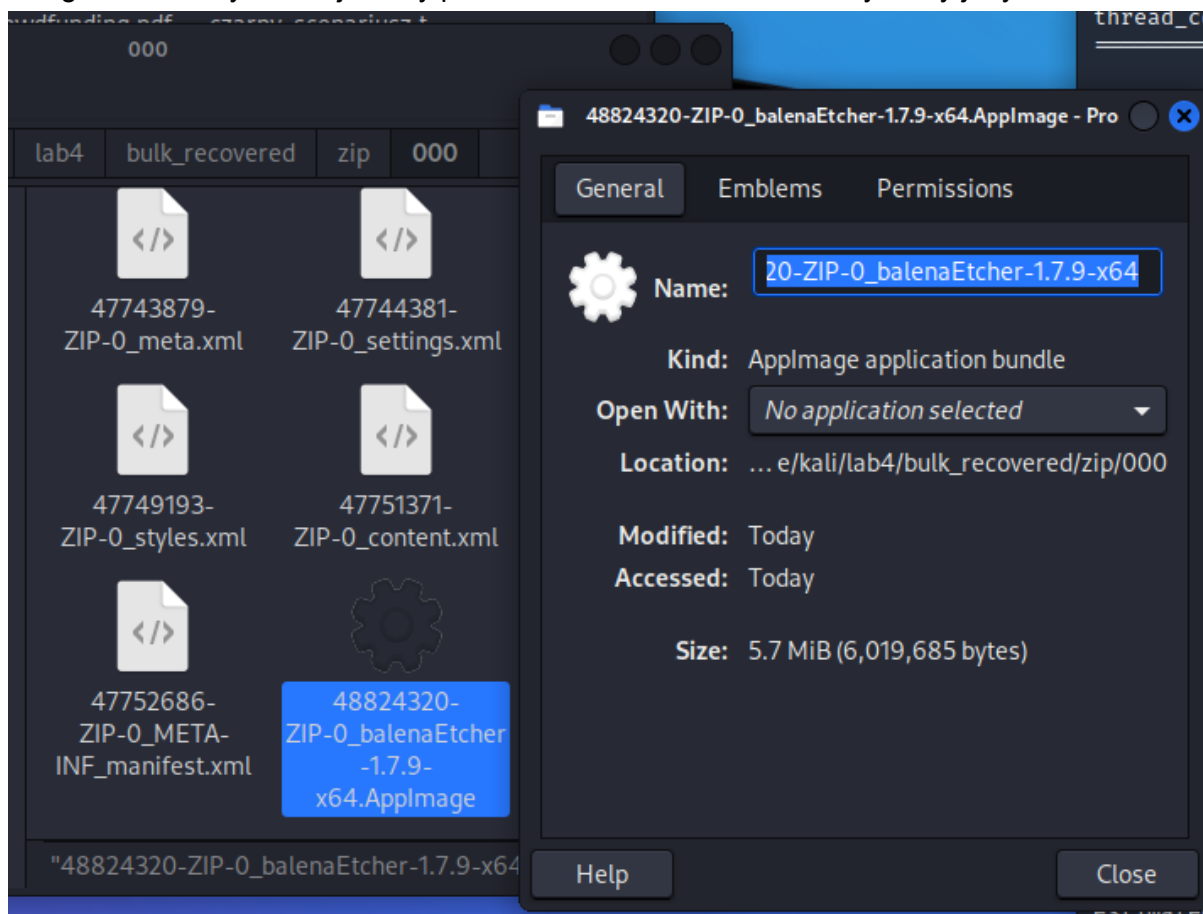
Niestety, w przypadku zdjęć program nie poradził sobie najlepiej



Udało się wydobyć zaledwie jednego .jpg'a w należytym folderze oraz 2 w folderach przeznaczonych na archiwa .zip - z czego jedno zdjęcie się dwukrotnie powieli
Nawet sprawdzanie metadanych zdjęcia nie ma dużo sensu, jeśli i tak jest to obraz graficzny zamiast zdjęcia

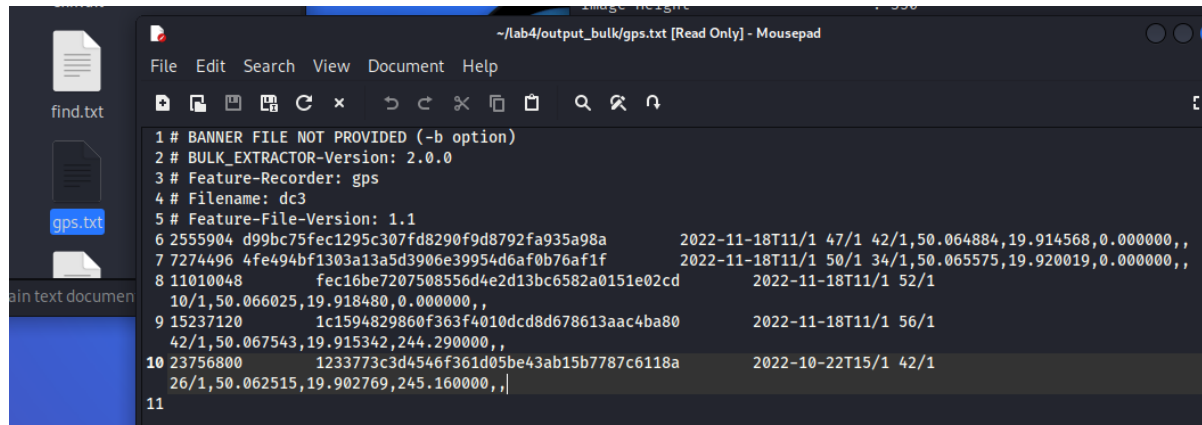
Jeśli chodzi o dane odzyskane z archiwów .zip - w folderze z outputem z bulk_extractora jest wiele plików charakteryzujących metadane plików z pakietu office (.rels, .xml). Udało się znaleźć jedynie 2 obrazki oraz 2 pdfy (które faktycznie były pierwotnie spakowane w jakimś archiwum)

Udało się odnaleźć ślady po wrzuconym pliku .exe. Jednakże nie została zachowana integralność danych - wejściowy plik miał około 100MB, a ten odzyskany jedynie 6MB



Program nawet nie znalazł archiwów .rar

Dziwny okazał się fakt, że mimo iż nie udało się znaleźć zdjęć, istnieje plik gps.txt gdzie znajdują się pewne współrzędne



```
1 # BANNER FILE NOT PROVIDED (-b option)
2 # BULK_EXTRACTOR-Version: 2.0.0
3 # Feature-Recorder: gps
4 # Filename: dc3
5 # Feature-File-Version: 1.1
6 2555904 d99bc75fec1295c307fd8290f9d8792fa935a98a 2022-11-18T11/1 47/1 42/1,50.064884,19.914568,0.000000,,
7 7274496 4fe494bf1303a13a5d3906e39954d6af0b76af1f 2022-11-18T11/1 50/1 34/1,50.065575,19.920019,0.000000,,
8 11010048 fec16be7207508556d4e2d13bc6582a0151e02cd 2022-11-18T11/1 52/1
9 10/1,50.066025,19.918480,0.000000,,
10 15237120 1c1594829860f363f4010dcd8d678613aac4ba80 2022-11-18T11/1 56/1
11 42/1,50.067543,19.915342,244.290000,,
12 23756800 1233773c3d4546f361d05be43ab15b7787c6118a 2022-10-22T15/1 42/1
13 26/1,50.062515,19.902769,245.160000,,|
14
15
```

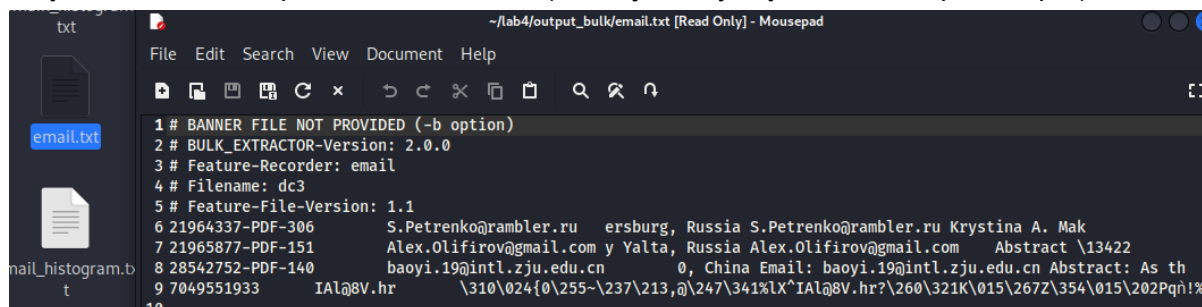
Tak się składa że są to koordynaty, gdzie zostały zrobione zdjęcia telefonem na potrzeby ów raportu

Było 5 zdjęć z geolokalizacją z tego 4 znajdują się w pliku gps.txt i są całkowicie poprawne

Generalnie efektywność bulk_extractora można opisać jako dość biedną - jednakże jego siła kryje się w wszelkich innych typach plików i sygnaturach (na pewno program sprawdzi się lepiej w analizowaniu obrazu systemu, a nie dysku zewnętrznego)

Potrąfi wydobyć przykładowo linki url zawarte w systemie, numery telefonów, adresy email, zapytania DNS

Przykład znalezienia paru adresów email (te znajdowały się w treściach plików .pdf)



```
1 # BANNER FILE NOT PROVIDED (-b option)
2 # BULK_EXTRACTOR-Version: 2.0.0
3 # Feature-Recorder: email
4 # Filename: dc3
5 # Feature-File-Version: 1.1
6 21964337-PDF-306 S.Petrenko@rambler.ru ersburg, Russia S.Petrenko@rambler.ru Krystina A. Mak
7 21965877-PDF-151 Alex.Olifirov@gmail.com y Yalta, Russia Alex.Olifirov@gmail.com Abstract \13422
8 28542752-PDF-140 baoyi.19@intl.zju.edu.cn 0, China Email: baoyi.19@intl.zju.edu.cn Abstract: As th
9 7049551933 IAl@8V.hr \310\024{0\255-\237\213,@\247\341%IX^IAL@8V.hr?\260\321K\015\267Z\354\015\202Pqñ!%
10
```

Co ciekawe, programowi udało się odnaleźć plik z rozszerzeniem .winpe - świadczący o obecności plików instalacyjnych windowsa na nośniku. Faktycznie taka rzecz miała miejsce, wcześniej pendrive służył jako bootowalny nośnik instalacyjny systemu

Dziwi jedynie fakt że przecież dane zostały wyczyszczone i nadpisane (komenda `dc3dd wipe`), a i jakieś ślady pozostały

Zadanie 6 – Podsumowanie

Pierwotnie przypuszczałem iż rezultat każdego z programów będzie podobny - tak się nie stało oraz były wielkie dysproporcje.

Najlepszy w odzyskiwaniu plików używanych na co dzień okazał się **foremost** - prosty w użyciu, efektywny (czas skanowania) oraz udało mu się odzyskać znaczną większość plików w różnych formatach (nie tylko zdjęcia czy pliki tekstowe ale również archiwa). Jeśli miałbym do odzyskania duże ilości plików (np. poprzez przypadkowe usunięcie zawartości całego dysku) z pewnością wybór padłby na foremost

Następnie **recoverjpeg** - chyba zdecydowanie najprostszy w użyciu. Działa relatywnie szybko i skutecznie. Niestety jego słabością jest mało dostępnych formatów (tylko jpg/jpeg oraz mov)

Trudno mi jest określić pracę następnego programu **Bulk_Extractor**. Był on wolny w swym działaniu i odzyskał bardzo mało plików w całości, można wręcz powiedzieć, że nie odzyskał wcale. Jednakże jego zastosowanie jest trochę inne - genialne się sprawdza w wydobywaniu samych metadanych, - przykładowo numerów telefonów, adresów email

A przecież na podstawie samych metadanych idzie ustalić wiele aspektów działania osób w sieci/systemach informatycznych (polecam książkę Niewidzialny w sieci Kevina Mitnicka, autor opisuje fakt jak łatwo jest odtworzyć życie osoby na podstawie samych metadanych)

Z uwagi na niepoprawne działanie oraz irytację program **Scalpel** zostawiam bez interpretacji

Do jak najskuteczniej pracy z narzędziami odzyskiwania plików trzeba użyć nie jednego programu, a najlepiej wielu. Tam, gdzie jednemu nie uda się czegoś odzyskać, być może pomoże inny. Najlepiej sprawdzi się kombinacja - program do odzyskiwania samych plików (np. foremost) oraz program do gromadzenia metadanych (np. bulk_extractor)