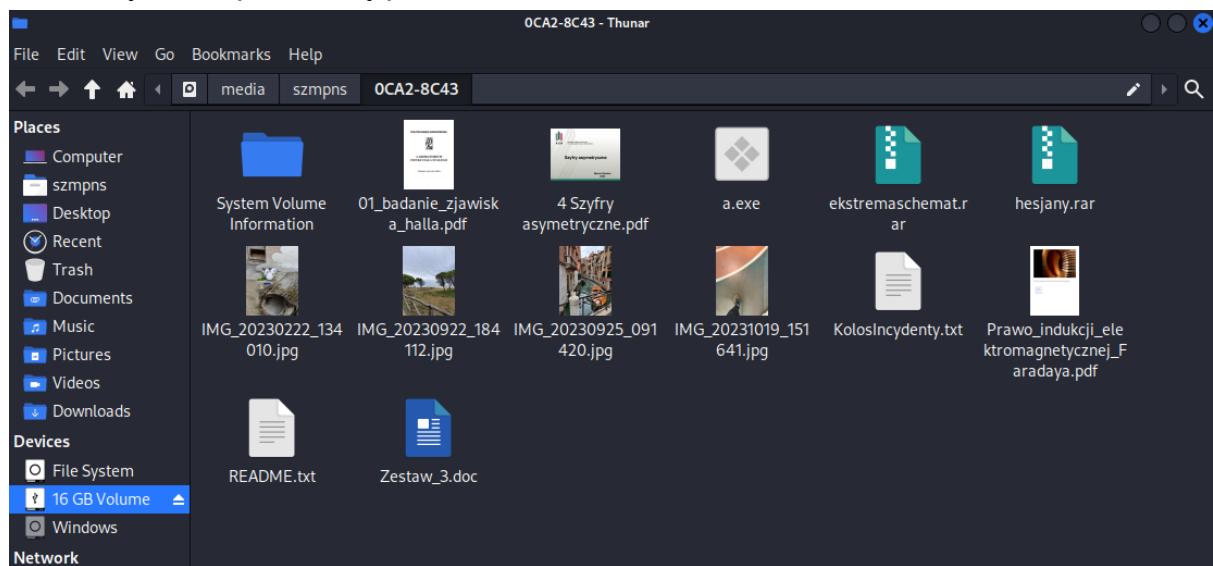


Szymon Kozioł

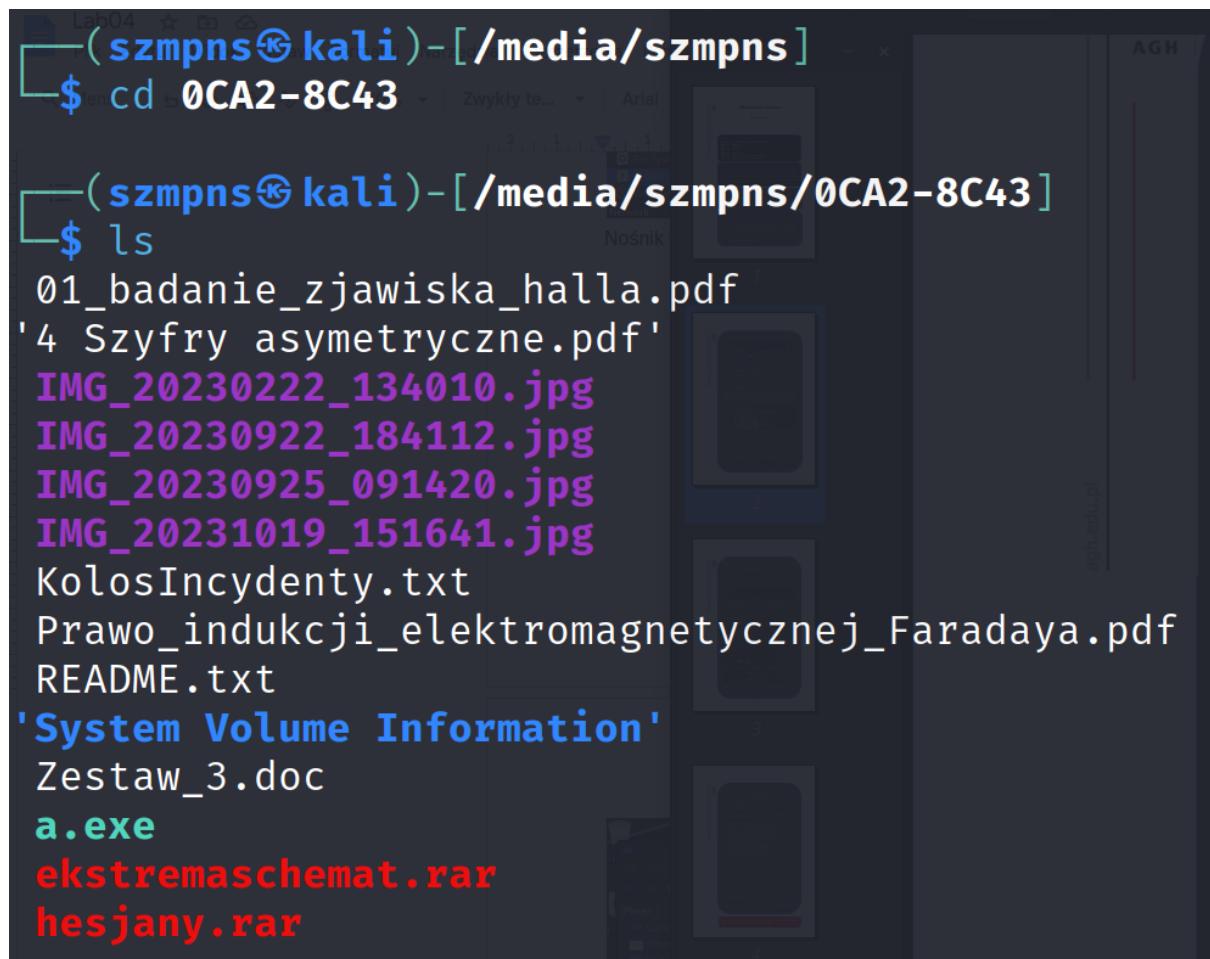
ZADANIE 1:

```
15552479232 bytes ( 14 G ) copied ( 100% ), 3375 s, 4.4 M/s  
input results for pattern `00':  
    30375936 sectors in  
  
output results for device `/dev/sda':  
    30375936 sectors out  
  
dc3dd completed at 2023-12-02 14:04:35 +0100
```

Udało się, teraz przerzucę pliki:



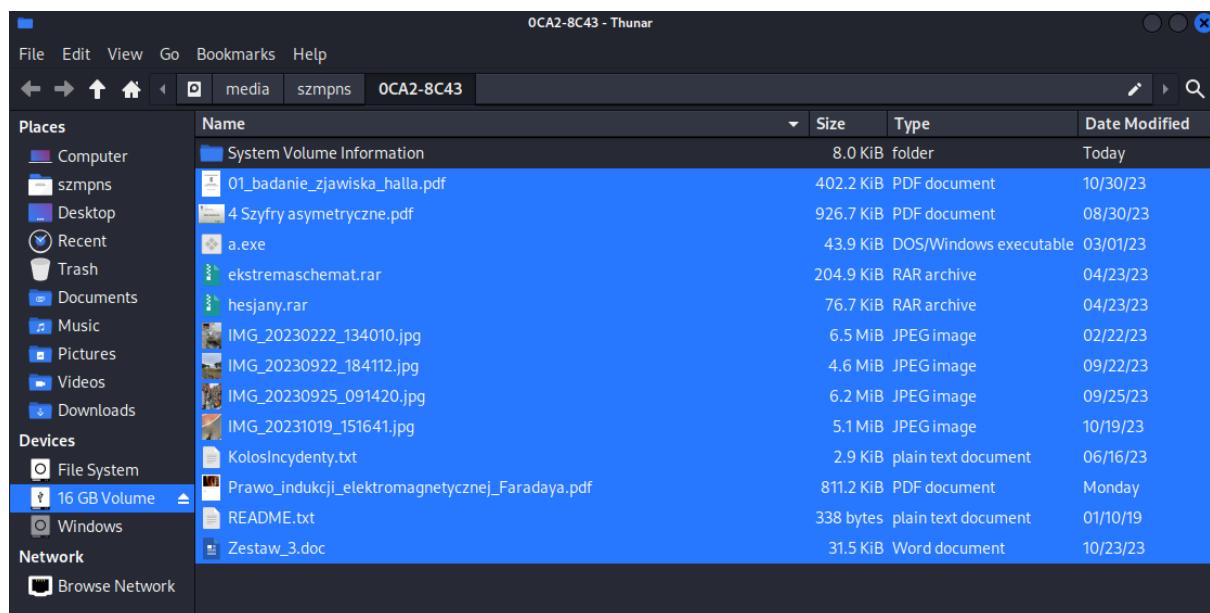
Nośnik w systemie Linux:



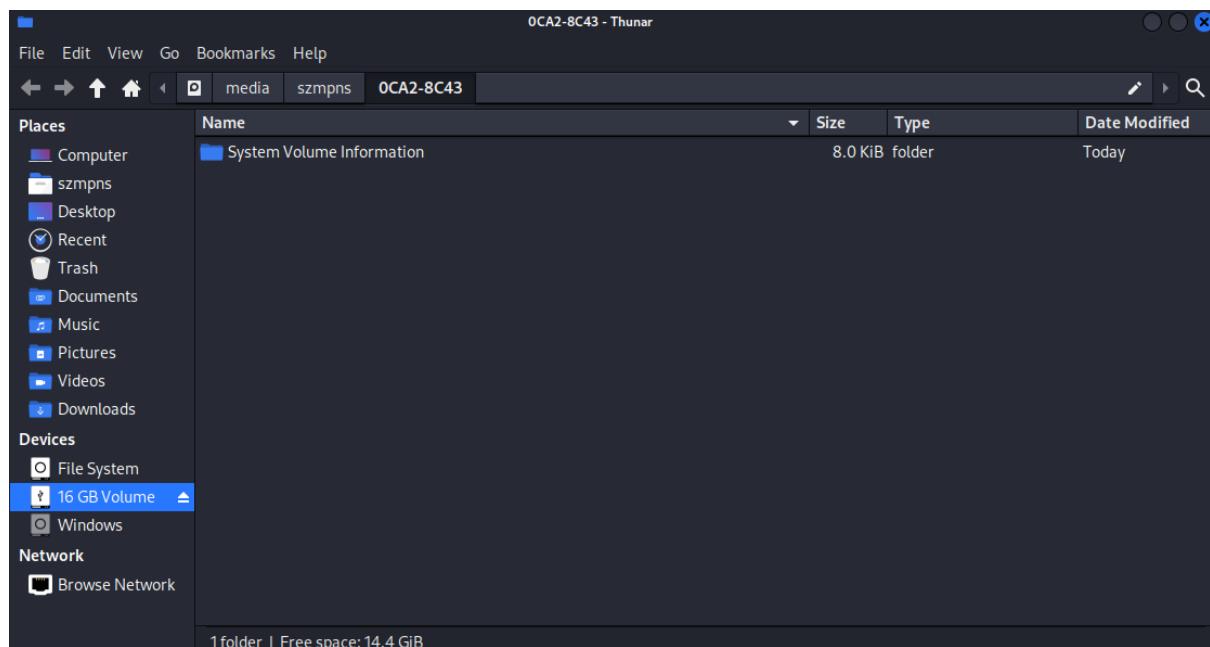
```
(szmpns㉿kali)-[~/media/szmpns]
$ cd 0CA2-8C43

(szmpns㉿kali)-[/media/szmpns/0CA2-8C43]
$ ls
01_badanie_zjawiska_halla.pdf
'4 Szyfry asymetryczne.pdf'
IMG_20230222_134010.jpg
IMG_20230922_184112.jpg
IMG_20230925_091420.jpg
IMG_20231019_151641.jpg
KolosIncydenty.txt
Prawo_indukcji_elektromagnetycznej_Faradaya.pdf
README.txt
'System Volume Information'
Zestaw_3.doc
a.exe
ekstremaschemat.rar
hesjany.rar
```

Usuwanie:



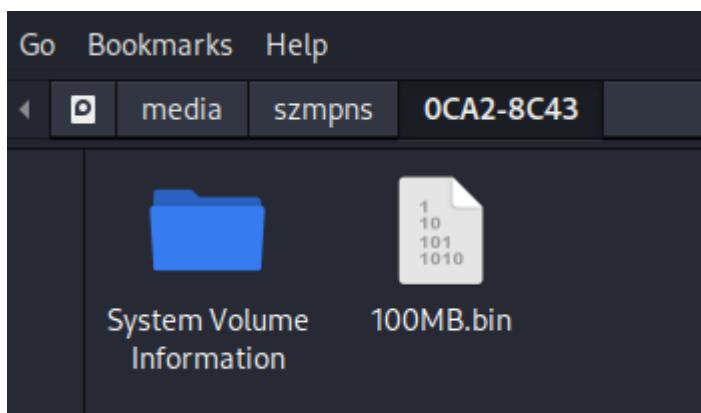
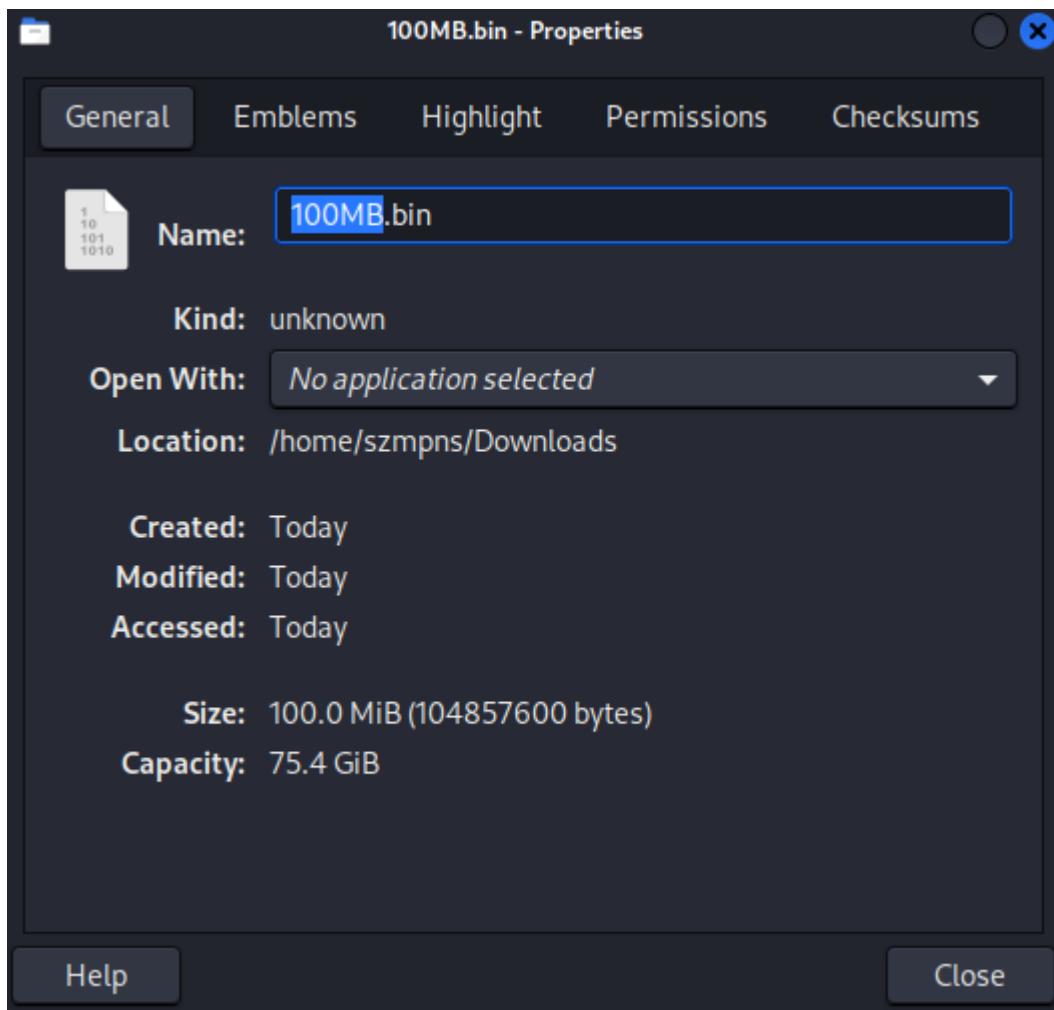
OCA2-8C43 - Thunar				
	Name	Size	Type	Date Modified
Places	System Volume Information	8.0 KiB	folder	Today
Computer	01_badanie_zjawiska_halla.pdf	402.2 KiB	PDF document	10/30/23
szmpns	4 Szyfry asymetryczne.pdf	926.7 KiB	PDF document	08/30/23
Desktop	a.exe	43.9 KiB	DOS/Windows executable	03/01/23
Recent	ekstremaschemat.rar	204.9 KiB	RAR archive	04/23/23
Trash	hesjany.rar	76.7 KiB	RAR archive	04/23/23
Documents	IMG_20230222_134010.jpg	6.5 MiB	JPEG image	02/22/23
Music	IMG_20230922_184112.jpg	4.6 MiB	JPEG image	09/22/23
Pictures	IMG_20230925_091420.jpg	6.2 MiB	JPEG image	09/25/23
Videos	IMG_20231019_151641.jpg	5.1 MiB	JPEG image	10/19/23
Downloads	KolosIncydenty.txt	2.9 KiB	plain text document	06/16/23
Devices	Prawo_indukcji_elektromagnetycznej_Faradaya.pdf	811.2 KiB	PDF document	Monday
File System	README.txt	338 bytes	plain text document	01/10/19
16 GB Volume	Zestaw_3.doc	31.5 KiB	Word document	10/23/23
Windows				
Network				
Browse Network				



```
(szmpns㉿kali)-[/media/szmpns/0CA2-8C43]$ ls
'System Volume Information'
```

Pusto

Następnie pobrałem plik .bin, który ma 100MB i przeniosłem go na pendrive:



```
(szmpns㉿kali)-[/media/szmpns/0CA2-8C43]
$ ls
100MB.bin  'System Volume Information'
```

```
(szmpns㉿kali)-[~/media/szmpns/0CA2-8C43]
$ sudo dc3dd if=/dev/sda of=~/InformatykaSledcza/InfSl_LAB04/backup.img
[sudo] password for szmpns:

dc3dd 7.2.646 started at 2023-12-02 14:51:08 +0100

15552479232 bytes ( 14 G ) copied ( 100% ), 898 s, 17 M/s

input results for device `/dev/sda':
 30375936 sectors in
 0 bad sectors replaced by zeros

output results for file `~/home/szmpns/InformatykaSledcza/InfSl_LAB04/bac
kup.img':
 30375936 sectors out

dc3dd completed at 2023-12-02 15:06:06 +0100
```

```
(szmpns㉿kali)-[~]
$ sudo md5sum /dev/sda
6fad8d37ee4649f45e32927a19a7f9fe  /dev/sda

(szmpns㉿kali)-[~]
$ md5sum ~/InformatykaSledcza/InfSl_LAB04/backup.img
6fad8d37ee4649f45e32927a19a7f9fe  /home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img
```

Zatem kopia jest poprawna. Sukces.

ZADANIE 2:

Obraz:

```
(szmpns㉿kali)-[~]
$ foremost -i ~/InformatykaSledcza/InfSl_LAB04/backup.img -o ~/InformatykaSledcza/InfSl_LAB04/description
Processing: /home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img
|*****| ZADANIE 2: *****|
```

```

└─(szmpns㉿kali)-[~]
$ cd InformatykaSledcza/InfSl_LAB04/description
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ls
audit.txt jpg ole pdf rar
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ls -R
.: .
audit.txt jpg ole pdf rar
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ./jpg:
00033730.jpg 00034670.jpg 00035616.jpg 00058432.jpg 00081908.jpg
00033849.jpg 00034757.jpg 00049040.jpg 00071184.jpg 00082530.jpg
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ./ole:
00083392.ole
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ./pdf:
00032880.pdf 00033728.pdf 00081680.pdf
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ ./rar:
00083616.rar 00084064.rar

```

Prawie wszystkie usunięte pliki znajdują się w utworzonym wcześniej folderze, dodatkowo program wydobył również zdjęcia z plików .pdf i umieścił je w folderze jpg. Plik .doc znajduje się w folderze ole i ma zmieniony format .ole, jednak przy narzędziach wykorzystujących rozszerzenia .doc jest w pełni sprawny i działa tak jak przed usunięciem.

Program nie wydobył jednak pliku a.exe oraz kilku plików .txt. Wydaje się, że narzędzie mogło napotkać trudności, ponieważ pliki te są dużo bardziej podatne na nadpisanie od innych. W celu kontynuowania laboratorium na razie pominę ten fakt i zobaczę jak z tym problemem będą postępowały inne narzędzia odzyskiwania danych z nośnika(np. Scalpel), a gdy one nie zadziałają skutecznie, wrócę do źródła problemu.

Nadmienię, że próbując odzyskać pliki w tych dwóch formatach próbowałem za pomocą komendy dawać foremostowi do zrozumienia czego oczekuje:

```

└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ foremost -t txt,exe -i ~/InformatykaSledcza/InfSl_LAB04/backup.img -
o ~/InformatykaSledcza/InfSl_LAB04/description_new

```

Żadna kombinacja z txt nie działa, natomiast formaty .pdf, .jpg, .rar, czy .exe!!!!) wykonywały się błyskawicznie i wszystko wraz z audytem pojawiało się w nowo utworzonym folderze description_new.

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ foremost -t exe -i ~/InformatykaSledcza/InfSl_LAB04/backup.img -o ~/InformatykaSledcza/InfSl_LAB04/description_new
Processing: /home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img
| ****
*****
***** |
```

Program nie odzyskał natomiast pliku .exe. Audyt wykazał brak jego istnienia. Prawdopodobnie wynika to z tego, że mój plik .exe mógł być uszkodzony, czego nie zauważałem za co bardzo przepraszam.

Z pewnego forum internetowego doczytałem, że:

Currently foremost can recover the following file types:

- jpg - Support for the JFIF and Exif formats including implementations used in modern digital cameras.
- gif
- png
- bmp - Support for windows bmp format.
- avi
- exe - Support for Windows PE binaries, will extract DLL and EXE files along with their compile times.
- mpg - Support for most MPEG files (must begin with 0x000001BA)
- wav
- riff - This will extract AVI and RIFF since they use the same file format (RIFF). note faster than running each separately.
- wmv - Note may also extract -wma files as they have similar format.
- mov
- pdf
- ole - This will grab any file using the OLE file structure. This includes PowerPoint, Word, Excel, Access, and StarWriter
- doc - Note it is more efficient to run OLE as you get more bang for your buck. If you wish to ignore all other ole files then use this.
- zip - Note is will extract .jar files as well because they use a similar format. Open Office docs are just zipâd XML files so they are extracted
as well. These include SXW, SXC, SXI, and SX? for undetermined OpenOffice files.
- rar
- htm
- cpp - C source code detection, note this is primitive and may generate documents other than C code.

zatem narzędzie to prawdopodobnie nie obsługuje plików .txt, stąd cały problem.

Plik audit.txt szczegółowo opisuje cały proces i odzyskane pliki:

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/description]
$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sat Dec 2 15:55:56 2023
Invocation: foremost -i /home/szmpns/InformatykaSledcza/InfSl_LAB04/back
up.img -o /home/szmpns/InformatykaSledcza/InfSl_LAB04/description
Output directory: /home/szmpns/InformatykaSledcza/InfSl_LAB04/descriptio
n
Configuration file: /etc/foremost.conf

File: /home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img
Start: Sat Dec 2 15:55:56 2023
Length: 14 GB (15552479232 bytes)

Num      Name (bs=512)          Size    File Offset   Comment
0:      00033730.jpg           57 KB    17269947
1:      00033849.jpg           37 KB    17330745
2:      00034670.jpg           42 KB    17751220
3:      00034757.jpg           43 KB    17795830
4:      00035616.jpg           6 MB     18235392
5:      00049040.jpg           4 MB     25108480
6:      00058432.jpg           6 MB     29917184
7:      00071184.jpg           5 MB     36446208
8:      00081908.jpg           203 KB   41936924
9:      00082530.jpg           193 KB   42255385
10:     00083392.ole            5 MB     42696704
11:     00083616.rar            204 KB   42811392
12:     00084064.rar            76 KB    43040768
13:     00032880.pdf            402 KB   16834560
14:     00033728.pdf            926 KB   17268736
15:     00081680.pdf            811 KB   41820160
Finish: Sat Dec 2 15:59:54 2023

16 FILES EXTRACTED

jpg:= 10
ole:= 1
rar:= 2
pdf:= 3

Foremost finished at Sat Dec 2 15:59:54 2023
```

Create Date : 2023:09:25 09:14:21.253151
Date/Time Original : 2023:09:25 09:14:21.253151
Modify Date Note : 2023:09:25 09:14:21.253151
Thumbnail Image : (Binary data 48731 bytes, use -b option to extract
) Currently foremost can recover the following file types:
GPS Altitude for the JFIF and Exif formats including implementation specific fields : 70.5 m Above Sea Level
GPS Date/Time : 2023:09:25 07:14:20Z
GPS Latitude : 45 deg 26' 5.10" N
GPS Longitude : 12 deg 20' 6.87" E
Circle Of Confusion : 0.005 mm
Field Of View : 67.4 deg
Focal Length : 4.8 mm (35 mm equivalent: 27.0 mm)
GPS Position : 45 deg 26' 5.10" N, 12 deg 20' 6.87" E
Hyperfocal Distance : 2.59 m
Light Value : 7.8
Notes: foremost can extract AVI and RIFF since they use the same file format. It is faster than running each separately.
It also extract .wma files as they have similar format.

Przywrócone zdjęcia zachowały swoje oryginalne dane.

Pendrive:

```
[szmpns@kali:~] [~] Taki komunikat jest poprawny. Sukces.  
$ sudo foremost -i /dev/sda -o ~/InformatykaSledcza/InfSl_LAB04/description_pendrive  
[sudo] password for szmpns:  
Processing: /dev/sda Obraz:  
|*****|  
*****|  
*****|
```

```
[root@kali]~/InformatykaSledcza/InfSI_LAB04/description_pendrive]
# ls
audit.txt jpg ole pdf rar

[root@kali]~/InformatykaSledcza/InfSI_LAB04/description_pendrive]
# ls -R
.:
audit.txt jpg ole pdf rar

./jpg:
00033730.jpg 00034670.jpg 00035616.jpg 00058432.jpg 00081908.jpg
00033849.jpg 00034757.jpg 00049040.jpg 00071184.jpg 00082530.jpg

./ole:
00083392.ole

./pdf:
00032880.pdf 00033728.pdf 00081680.pdf

./rar:
00083616.rar 00084064.rar
```

Identyczna sytuacja jak w przypadku kopii, jedyna różnica jest taka, że pliki odziedziczyły uprawnienia po dysku zewnętrznym, przez co musiałem zalogować się do roota, aby otworzyć folder.

```
[root@kali]~[/home/.../InformatykaSledcza/InfSl_LAB04/description_pendrive/jpg]
# exiftool 00058432.jpg
ExifTool Version Number : 12.67
File Name               : 00058432.jpg
Directory               : .
File Size                : 6.5 MB
File Modification Date/Time : 2023:12:02 17:01:33+01:00
File Access Date/Time   : 2023:12:02 17:01:33+01:00
File Inode Change Date/Time : 2023:12:02 17:01:33+01:00
```

Metadane zdjęć zachowały się oryginalnie, zmieniona jest tylko data modyfikacji.

Audyt był identyczny jak w przypadku kopii.

ZADANIE 3:

Instalacja:

```
[szmpns@kali] - [~/InformatykaSledcza/InfSl_LAB04]
$ recoverjpeg
Command 'recoverjpeg' not found, but can be installed with:
sudo apt install recoverjpeg
Do you want to install it? (N/y)y
sudo apt install recoverjpeg
Reading package lists... Done
```

Uruchamianie programu:

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ mkdir recover_description
```



```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ sudo recoverjpeg /dev/sda -o ~/InformatykaSledcza/InfSl_LAB04/recover_description
to miejsce, do którego "recoverjpeg" ma zapisać odzyskane pliki JPEG.
2. Przekierowanie wyników do folderu:
```

Narzędzie odzyskało tylko pliki .jpg i to nie wszystkie(tylko 2!!)

```
[szmpns㉿kali)-[~/InformatykaSledcza/InfSI_LAB04/recover_description]
$ ls
image0000.jpg  image0001.jpg
```

Oryginalne metadane zdjęć zostały zachowane, tak jak w przypadku foremost:

```
[~(szmpns㉿kali)-[~/InformatykaSledcza/InfSI_LAB04/recover_description]
$ exiftool image00000.jpg
ExifTool Version Number : 12.67
File Name               : image00000.jpg
Directory               : .
File Size                : 4.8 MB
File Modification Date/Time : 2023:12:02 17:25:49+01:00
File Access Date/Time   : 2023:12:02 17:26:31+01:00
File Inode Change Date/Time : 2023:12:02 17:25:49+01:00
File Permissions         : -rw-r--r--
File Type                : JPEG
File Type Extension     : jpg
```

Jeżeli chodzi o różnice, narzędzie recoverjpeg odzyskało znacznie mniej plików, nie zapewniło żadnej dodatkowej informacji na ten temat, narzędzie zmieniło całkowicie nazwy plików, co jest bardzo niekorzystne z punktu widzenia tego laboratorium jak i całej istoty informatyki śledczej. Jedynym pozytywnym aspektem, był czas działania narzędzia recoverjpeg, który był znacznie szybszy od działania narzędzia foremost.

ZADANIE 4:

```
[~(szmpns㉿kali)-[~/InformatykaSledcza/InfSI_LAB04/description/jpg]
$ cd /etc/scalpel
[~(szmpns㉿kali)-[/etc/scalpel]
$ ls
scalpel.conf
```

- Użyj programu scalpel z podpiętym plikiem informacji z kopii nosnika (.dd).
- Porównaj rezultaty z poprzednio używanymi.

Usuwanie #:

(musiałem wejść przez superusera[sudo nano ...])

```
# GIF and JPG files (very common)
#      gif      y      5000000      \x47\x49\x46\x38\x37\x61      \x00\x3b
#      gif      y      5000000      \x47\x49\x46\x38\x39\x61      \x00\x3b
#      jpg      y      5242880      \xff\xd8\xff???Exif      \xff\xd9
#      jpg      y      5242880      \xff\xd8\xff???JFIF      \xff\xd9
#
```

```
#_
# MICROSOFT OFFICE
#_
# Word documents
#
#      doc      y      10000000      \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00      \xd0\xcf>
#      doc      y      10000000      \xd0\xcf\x11\xe0\xa1\xb1
```

Odkomentowałem jeszcze .pdf, innych rozszerzeń nie znalazłem.

Zaczynam proces:

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ scalpel -o ~/InformatykaSledcza/InfSl_LAB04/scalpel_description ~/InformatykaSledcza/InfSl_LAB04/backup.img
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img"

Image file pass 1/2.
/home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img: 0.1% 10.0 MB 00:00 E

/home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img: 100.0% 14.5 GB 00:00 E
TAPProcessing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 15, elapsed = 93 seconds.
```

Zawartość folderu:

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/scalpel_description]
$ ls
audit.txt  doc-2-0  doc-3-0  jpg-0-0  jpg-1-0  pdf-4-0  pdf-5-0
```

Jak można zauważyć każde rozszerzenie zostało podzielone na dwa foldery.

Jeden z plików pdf został zapisany 2 razy w folderze pdf-4-0 pod dwoma innymi nazwami. Pozostałe pliki .pdf znajdują się w drugim folderze pdf. Zdjęcia w folderze jpg-1-0 są zdjęciami wydobytymi z plików pdf, natomiast zdjęcia z aparatu w folderze jpg-0-0. Niestety tylko jeden z nich nie jest uszkodzony.

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/scalpel_description/jpg-0-0]
$ exiftool 00000002.jpg
ExifTool Version Number : 12.67
File Name : 00000002.jpg
Directory : .
File Size : 50 kB
File Modification Date/Time : 2023:12:02 17:50:51+01:00
File Access Date/Time : 2023:12:02 17:52:56+01:00
File Inode Change Date/Time : 2023:12:02 17:50:51+01:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Warning : JPEG format error

Jak można zauważyć rozszerzenia zostało podzielone na dwa foldery.
Jeden z plików pdf: JPEG 2 razy w folderze pdf-4-0 pod dwoma innymi nazwami. Pozostałe pliki znajdują się w drugim folderze pdf. Zdjęcia w folderze jpg-1-0 są zdjęciami wydobytymi z plików pdf, natomiast zdjęcia z aparatu w folderze jpg-0-0. Niestety tylko jeden z nich nie jest uszkodzony.
```

Nie zachował oryginalnych metadanych.

Zobaczmy jakie informacje da się wyciągnąć ze zdjęcia, które nie jest uszkodzone:

GPS Altitude	: 0 m Above Sea Level
GPS Date/Time	Zawartość folderu : 2023:09:22 16:41:12Z
GPS Latitude	: 45 deg 38' 20.52" N
GPS Longitude	: 13 deg 4' 13.83" E
Circle Of Confusion	: 0.005 mm
Field Of View	: 67.4 deg
Focal Length	Jeden z plików posiada 4.8 mm (35 mm equivalent: 27.0 mm) nazwami. Pozostałe pliki jpg-1-0 są uszkodzone, a jpg-0-0, Niestety typ jpg-0-0 nie posiada oryginalnych nazw, co jest bardzo dużym minusem. Jak do tej pory najlepiej sprawdza się foremost.
GPS Position	: 45 deg 38' 20.52" N, 13 deg 4' 13.83" E
Hyperfocal Distance	: 2.59 m
Light Value	: 7.1

Zachowały się oryginalne metadane.

Porównując do reszty - to narzędzie działa zdecydowanie szybciej od foremost'a, z podobną szybkością co scalpel. Jest skuteczniejsze od scalpel'a, natomiast uszkodzone pliki .jpg nie napawają optymizmem. Do tego narzędzie obsługuje bardzo mało typów plików i tak jak scalpel - nie zachowuje oryginalnych nazw, co jest bardzo dużym minusem. Jak do tej pory najlepiej sprawdza się foremost.



V

Z plusów, narzędzie tworzy plik z audytem, którego treść prezentuje się następująco:

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/scalpel_description]
$ ls
audit.txt doc-2-0 jpg-0-0 jpg-1-0 pdf-4-0 pdf-5-0

(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/scalpel_description]
$ cat audit.txt

Scalpel version 1.60 audit file
Started at Sat Dec 2 17:49:18 2023
Command line:
scalpel -o /home/szmpns/InformatykaSledcza/InfSl_LAB04/scalpel_description /home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img

Output directory: /home/szmpns/InformatykaSledcza/InfSl_LAB04/scalpel_description
Configuration file: /etc/scalpel/scalpel.conf

Opening target "/home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img"

The following files were carved:
File          Start          Chop          Length      Extracted Fr
om
00000013.pdf    17268736     NO        948780      backup.img
00000012.pdf    16834560     NO       1382956      backup.img
00000007.jpg    17795830     NO        482110      backup.img
00000006.jpg    17751220     NO        526720      backup.img
00000005.jpg    17330745     NO        947195      backup.img
00000004.jpg    17269947     NO       1007993      backup.img
00000000.jpg    18235392     NO        42548       backup.img
00000002.jpg    29917184     NO        49872       backup.img
00000001.jpg    25108480     NO        4858576      backup.img
00000003.jpg    36446208     NO        20245       backup.img
00000008.jpg    41936924     NO       1148550      backup.img
00000014.pdf    41820160     NO        830621      backup.img
00000009.jpg    42255385     NO        830089      backup.img
00000011.doc    42696704     YES      10000000      backup.img
00000010.doc    42696704     NO       10000000      backup.img

Completed at Sat Dec 2 17:50:51 2023
```

ZADANIE 5:

Odpowiednio wcześniej stworzyłem sobie folder docelowy bulk_description

Start:

```
└─(szmpns㉿kali)-[~]
└─$ bulk_extractor -o ~/InformatykaSledcza/InfSl_LAB04/bulk_description ~/InformatykaSledcza/InfSl_LAB04/backup.img
bulk_extractor version: 2.0.0
Input file: "/home/szmpns/InformatykaSledcza/InfSl_LAB04/backup.img"
Output directory: "/home/szmpns/InformatykaSledcza/InfSl_LAB04/bulk_description"
Disk Size: 15552479232
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved m
           sxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carved w
           indirs winlnk winpe winprefetch zip accts email gps
Threads: 8
```

```
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: 20.02 sec.
Total MB processed: 15552
Overall performance: 777 MBytes/sec 97.12 (MBytes/sec/thread)
sbufs created: 493767
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data: 0:00:01 (1.20
seconds)
Time consumer scanners spent waiting for data from producer: 0:00:40 (40.91
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: 0
```

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04/bulk_description]
$ ls
aes_keys.txt          httplogs.txt          telephone_histogram.txt
alerts.txt            ip.txt                unrar_carved
ccn.txt               ip_histogram.txt      unrar_carved.txt
ccn_histogram.txt     jpeg_carved          url.txt
ccn_track2.txt        jpeg_carved.txt      url_facebook-address.txt
ccn_track2_histogram.txt json.txt            url_facebook-id.txt
domain.txt            kml_carved.txt       url_histogram.txt
domain_histogram.txt ntfsindx_carved.txt   url_microsoft-live.txt
elf.txt               ntfslogfile_carved.txt url_searches.txt
email.txt             ntfsmft_carved.txt  url_services.txt
email_domain_histogram.txt pii.txt           utmp_carved.txt
email_histogram.txt   pii_teamviewer.txt  vcard.txt
ether.txt             rar.txt              windirs.txt
ether_histogram.txt  report.xml         winlnk.txt
ether_histogram_1.txt rfc822.txt         winpe.txt
evtx_carved.txt      sin.txt            winpe_carved
exif.txt              sqlite_carved.txt  winprefetch.txt
facebook.txt         tcp.txt            zip.txt
find.txt              tcp_histogram.txt
find_histogram.txt
gps.txt
```

Program ten wypakował wszystkie pliki .rar i jestem w stanie je podejrzeć oraz otworzyć. Na tym kończyłyby się wszystkie jego pozytywy. Narzędzie utworzyło masę niepotrzebnych plików, z których nic nie wynika. Poza plikami .rar nie udało się odzyskać nic z elementów usuniętych z pendrive'a, które znajdują się w obrazie.

Szybkość jego działania była średnia.

Trudno coś więcej powiedzieć, na potrzeby tego laboratorium program po prostu się nie sprawdził.

ZADANIE 6:

Najlepszym narzędziem był foremost. Działał sprawnie i był skuteczny. Do tego odzyskał najwięcej plików, zarazem będąc bardzo przejrzystym w obsłudze.

Jeżeli chodzi o niepowodzenia: nie udało mi się odzyskać żadnego pliku .exe. Po konsultacji z kolegami wiem, że im też to się nie udało. Nie mam niestety wiedzy, czy plik był uszkodzony, ale wygląda na to, że nie.

Trudności: na początku użyłem zbyt dużego pendrive'a, co poskutkowało brakiem miejsca na dysku przy zgrywaniu kopii nośnika. Całość była bardzo czasochłonna, ale myślę, że było warto. Nauczyłem się kilku ciekawych i przydatnych rzeczy.

ZADANIE 7:

Pobieram narzędzie regripper

1) NTUSER.DAT

Czy są jakiekolwiek ślady używania Adobe Acrobat?

Nie.

```
[szmpns@kali]-(~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p pdf_recent_files
/usr/lib/regripper/plugins/pdf_recent_files.pl not found.
```

```
[szmpns@kali]-(~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p pdf_docs
/usr/lib/regripper/plugins/pdf_docs.pl not found.
```

Jakie aplikacje są skojarzone z kluczem ApplicationAssociationToasts?

W przypadku tego konkretnego wyniku `IE.HTTP_http`, może to być skojarzenie z Internet Explorerem dotyczące obsługi protokołu HTTP.

```
[smpns@kali]~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p appassoc
Launching appassoc v.20200515
appassoc v.20200515
- Gets contents of user's ApplicationAssociationToasts key
/usr/lib/regripper/plugins/pdf_recent_files.pl not found.
LastWrite: 2016-10-05 09:51:45Z
[~]~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p pdf_docs
/usr/lib/regripper/plugins/pdf_docs.pl not found.
IE.HTTP_http
```

Czy znaleziono dane o kompatybilności aplikacji w AppCompatFlags?

Tak, znaleziono dane o kompatybilności aplikacji w kluczu rejestru `AppCompatFlags`. W wyniku analizy pliku NTUSER.DAT za pomocą RegRippera, w kluczu `Compatibility Assistant\Store` znaleziono wpis odnoszący się do zgodności aplikacji.

Wskazuje on na pewne ustawienia zgodności dotyczące pliku `SpotifySetup.exe`, który został zarejestrowany w tym kluczu. Data i czas tego wpisu to `2013-08-21 23:53:01Z`.

Informacja ta może sugerować, że istnieje zapis dotyczący sposobu, w jaki system Windows traktuje plik instalacyjny aplikacji Spotify (o nazwie `SpotifySetup.exe`) pod kątem kompatybilności. Oznacza to, że system Windows może mieć jakieś informacje o sposobie działania aplikacji Spotify w kontekście zgodności z systemem operacyjnym.

```
[smpns@kali]~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p appcompatflags
Launching appcompatflags v.20200525
appcompatflags v.20200525
(NTUSER.DAT, Software) Extracts AppCompatFlags for Windows.

Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store
2013-08-21 23:53:01Z - SIGN.IE=056ED8 SpotifySetup.exe
```

Jakie są ostatnie czasy zapisu dla Applets?

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04] ostatnie czasy zapisu dla Applets?
$ regripper -r NTUSER.DAT -p applets
Launching applets v.20200525
applets v.20200525
(NTUSER.DAT) Gets contents of user's Applets key
Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time 2016-10-05 09:02:54Z
Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List not found.
```

ostatnia data zapisu dla tego klucza to 2016-10-05 09:02:54Z.

Jednakże, skrypt nie znalazł żadnych informacji na temat listy ostatnio używanych plików w Paint. W przypadku klucza Applets, który często zawiera informacje o ostatnio używanych plikach w różnych aplikacjach systemowych, brak danych o ostatnich plikach wykorzystywanych w Paint. Oznacza to, że w tym konkretnym przypadku nie ma informacji o ostatnio używanych plikach w Paint w tym pliku rejestrze.

Czy istnieje klucz AppSpecific dla Microsoft IntelliPoint?

Nie istnieje.

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04] ostatnio używanych plikach w różnych aplikacjach systemowych, brak danych
$ regripper -r NTUSER.DAT -p intellipoint
/usr/lib/regripper/plugins/intellipoint.pl not found.
```

Jakie pliki zostały ostatnio otwarte za pomocą iexplore.exe?

```
(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p iexplore
/usr/lib/regripper/plugins/iexplore.pl not found.
```

Żadne

Jakie są ustawienia środowiska użytkownika?

```

└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]
$ regripper -r NTUSER.DAT -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2016-10-05 09:14:15Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2016-10-09 19:58:01Z
    Microsoft.InternetExplorer.Default (2)
2016-10-05 09:50:57Z
    winstore_cw5n1h2txyewy!Windows.Store (1)
2016-10-05 09:40:38Z
    C:\Users\bberry\AppData\Local\Microsoft\Windows\INetCache\IE\WN4CJC14\SpotifySetup.exe (1)
2016-10-05 09:14:15Z
    microsoft.windowscommunicationsapps_8wekyb3d8bbwe!Microsoft.WindowsLive.Mail (1)

Value names with no time stamps:
    UEME_CTLCUACount:ctor
    C:\Users\bberry\AppData\Roaming\Spotify\SpWebInst0.exe
    C:\Users\bberry\AppData\Roaming\Spotify\Spotify.exe
    Microsoft.Windows.ControlPanel
    Microsoft.Windows.Explorer

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
2016-10-09 19:58:01Z

```

Czy istnieje klucz AppSpecific dla N...
Nie istnieje.

(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]\$ regripper -r NTUSER.DAT -p userassist
/usr/lib/regripper/plugins

Jakie pliki zostały ostatnio otwarte
/usr/lib/regripper/plugins

Zadno.

W kluczu

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist znajdują się podklucze identyfikowane przez swoje unikalne identyfikatory { ... }.

Każdy z tych identyfikatorów odnosi się do innego zestawienia danych dotyczącego uruchamianych programów.

Daty i czasy wyświetcone obok identyfikatorów oznaczają ostatnią zmianę w tych danych.

Każdy wpis zawiera ścieżkę do

programu (ścieżka\do\programu\program.exe) oraz liczbę uruchomień tego programu ((liczba uruchomień)).

Wartości bez znaczników czasowych (Value names with no time stamps) mogą reprezentować również programy uruchamiane, ale brakuje informacji o dokładnym czasie ich uruchomienia.

Czy znaleziono informacje o Office Internet Server Cache?

W celu znalezienia informacji o "Office Internet Server Cache" w rejestrze załadowanym z pliku NTUSER.DAT, należy poszukiwać odpowiednich kluczy i wartości, które mogą zawierać informacje o tym cache'u. Niestety, bez konkretnych wskazówek odnośnie lokalizacji tych danych, może być trudno znaleźć je w rejestrze.

```
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04] Cac
└─$ regripper -r NTUSER.DAT -p office
/usr/lib/regripper/plugins/office.pl not found.

└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04] Cac
└─$ regripper -r NTUSER.DAT -p office internet nych, może być
/usr/lib/regripper/plugins/office.pl not found.
```

Mi nic nie udało się znaleźć.

Czy istnieją jakiekolwiek ślady użycia WinRAR?

```
└─(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04] er
└─$ regripper -r NTUSER.DAT -p winrar
Launching winrar v.20200526
winrar v.20200526
(NTUSER.DAT) Get WinRAR\ArcHistory entries
Software\WinRAR\ArcHistory not found.
```

Wygląda na to, że nie.

Jakie strony internetowe zostały ostatnio wpisane przez użytkownika?

```
[~(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]$ regripper -r NTUSER.DAT -p ie_history  
/usr/lib/regripper/plugins/ie_history.pl not found.  
Jakie strony internetowe zostały ostatnio wpisane przez użytkownika?  
[~(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]$ regripper -r NTUSER.DAT -p history  
/usr/lib/regripper/plugins/history.pl not found.
```

Jakie są ostatnie czasy dostępu do wpisanych adresów URL?

Jak wyżej.

Czy są jakiekolwiek informacje o zainstalowanym oprogramowaniu Spotify?

```
[~(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB04]$ regripper -r NTUSER.DAT -p app_usage  
/usr/lib/regripper/plugins/app_usage.pl not found.
```