

Laboratorium 4 – Szymon Szkarłat

Zadanie 1. – Przygotowanie do odzyskiwania danych

1. Instalowanie narzędzia *dc3dd*.

```
(kali㉿kali)-[~/Desktop]
$ sudo apt-get install dc3dd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  dc3dd
0 upgraded, 1 newly installed, 0 to remove and 382 not upgraded.
Need to get 118 kB of archives.
After this operation, 502 kB of additional disk space will be used.
Get:1 http://kali.koyanet.lv/kali kali-rolling/main amd64 dc3dd amd64 7.3.1-2
  [118 kB]
Fetched 118 kB in 1s (106 kB/s)
Selecting previously unselected package dc3dd.
(Reading database ... 404894 files and directories currently installed.)
Preparing to unpack .../dc3dd_7.3.1-2_amd64.deb ...
Unpacking dc3dd (7.3.1-2) ...
Setting up dc3dd (7.3.1-2) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

(kali㉿kali)-[~/Desktop]
$
```

2. Podłączenie pendrive'a.

```
(kali㉿kali)-[/media/kali]
$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0       7:0      0   3.6G  1 loop
loop1       7:1      0   3.6G  1 loop
sda         8:0      0  80.1G  0 disk
└─sda1      8:1      0  80.1G  0 part /
sdb         8:16     1   7.5G  0 disk
└─sdb1      8:17     1    3G   0 part /media/kali/6CB4-6588
sr0         11:0     1 1024M  0 rom

(kali㉿kali)-[/media/kali]
$
```

3. Wyświetlenie rezultatu przy pomocy komendy *sudo fdisk -l*.

```
(kali㉿kali)-[~/Desktop]
$ sudo fdisk -l

Disk /dev/sdb: 7.5 GiB, 8053063680 bytes, 15728640 sectors
Disk model: UDisk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0005cc9e

Device      Boot Start      End Sectors Size Id Type
/dev/sdb1   *      2048 6397951 6395904  3G  c W95 FAT32 (LBA)
```

4. Wyczyszczenie pendrive'a przy pomocy wcześniej zainstalowanego narzędzia *dc3dd*.

```
(kali@kali)-[~/Desktop]
$ sudo dc3dd wipe=/dev/sdb1

dc3dd 7.2.646 started at 2023-11-25 12:45:11 -0500
compiled options:
command line dc3dd wipe=/dev/sdb1
device size: 6395904 sectors (probed),    3,274,702,848 bytes
sector size: 512 bytes (probed)

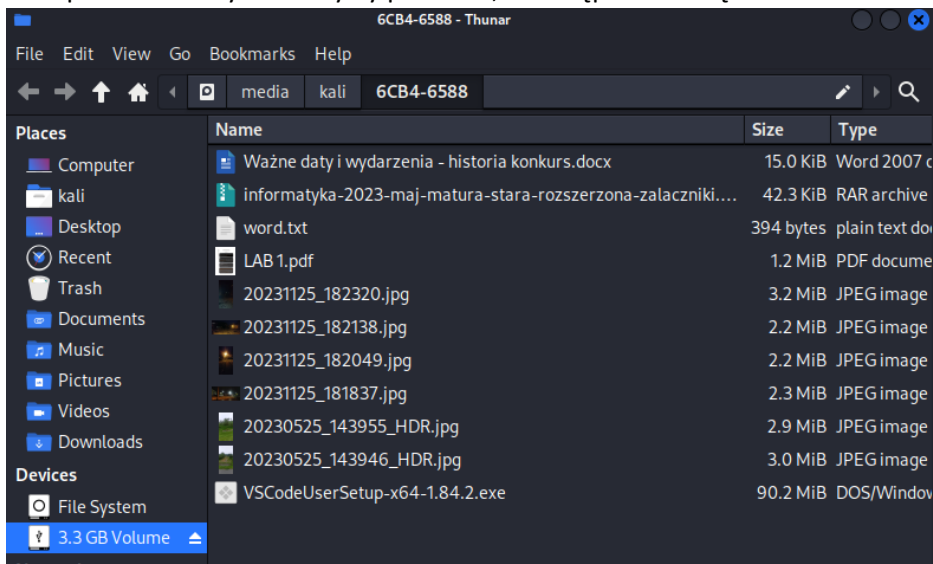
3274702848 bytes ( 3 G ) copied ( 100% ), 317 s, 9.8 M/s

input results for pattern `00':
6395904 sectors in

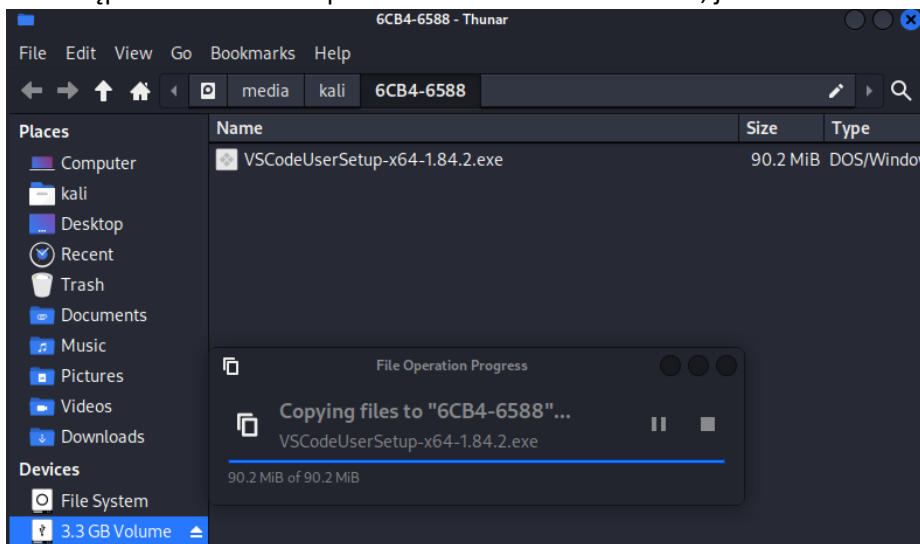
output results for device `/dev/sdb1':
6395904 sectors out

dc3dd completed at 2023-11-25 13:03:19 -0500
```

5. Kopiowanie danych na czysty pendrive, a następnie usunięcie ich



6. Następnie umieszczenie pliku o rozmiarze około 100 MB, jest to instalka do VSCode.



7. Wykonanie kopii binarnej nośnika `/dev/sdb1`, przy pomocy narzędzia `dc3dd`.

```
(kali㉿kali)-[/media/kali] 512 bytes / 512 bytes
$ 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: 2048 6395904 3G c W95 FAT32 (LBA)
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 tworzenia kopii binarnej.

```
3274702848 bytes ( 3 G ) copied ( 100% ), 285 s, 11 M/s
Disk identifier: 0x0005cc9e
3274702848 bytes ( 3 G ) hashed ( 100% ), 5 s, 597 M/s
Device Boot Start End Sectors Size Id Type
input results for device `'/dev/sdb1': 04 3G c W95 FAT32 (LBA)
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)

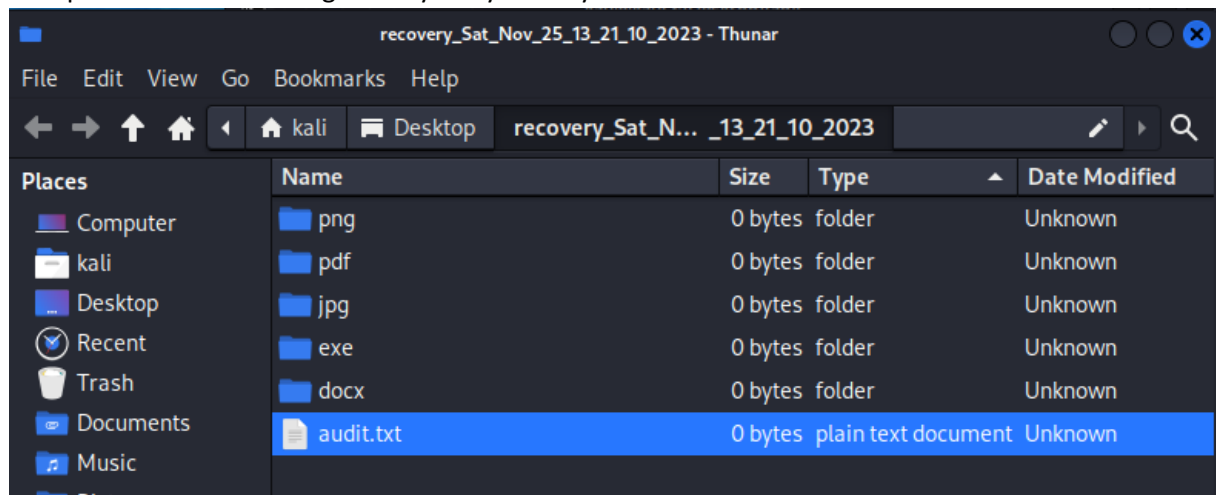
dc3dd completed at 2023-11-25 13:14:30 -0500
```

Zadanie 2. – Foremost

1. Po zainstalowaniu, odzyskiwanie danych za pomocą narzędzia foremost

```
(kali@kali)-[~/Desktop/lab4]
$ sudo foremost -v -t all -i usb-image.dd -o /home/kali/Desktop/recovery -T
Sector size (logical/physical): 512 bytes / 512 bytes
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File type: dos
Disk identifier: 0x0005cc9e
Foremost started at Sat Nov 25 13:21:10 2023
Invocation: foremost -v -t all -i usb-image.dd -o /home/kali/Desktop/recovery
-T
Output directory: /home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023
Configuration file: /etc/foremost.conf
Processing: usb-image.dd
File: usb-image.dd
Start: Sat Nov 25 13:21:10 2023
Length: 3 GB (3274702848 bytes)
```

2. Zaprezentowanie katalogu z odzyskanymi danymi



3. Aby zajrzeć do zawartości katalogu recovery muszą wykonać polecenie `cd`, ale jako root.

Wyświetlenie zawartości katalogu z odzyskanymi danymi, w szczególności zdjęcia w formacie jpg

```
(root@kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023/jpg]
# ls
00019080.jpg 00030160.jpg 00039400.jpg
00025648.jpg 00034720.jpg 00045360.jpg

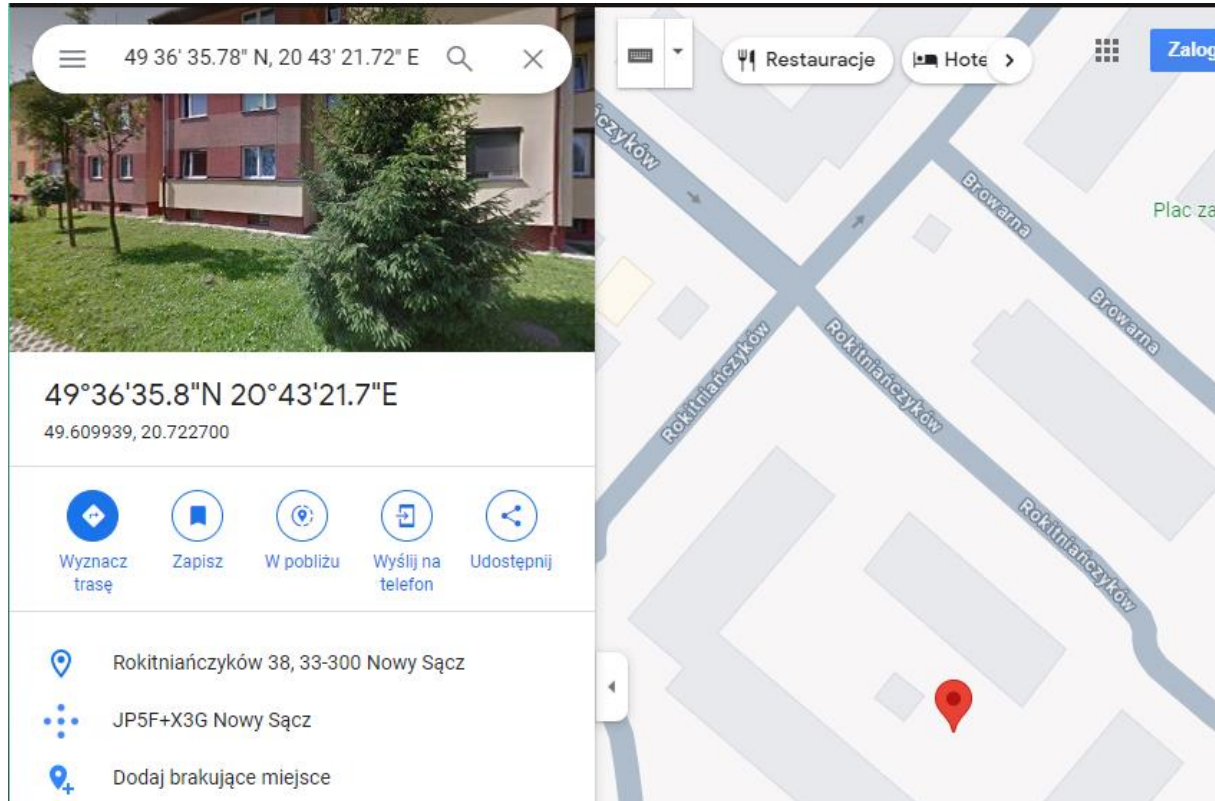
(root@kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023/jpg]
#
```

4. Użycie narzędzia `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

```
xtract)
GPS Altitude      : 344.2 m Below Sea Level
GPS Date/Time     : 2023:11:25 17:23:10Z
GPS Latitude      : 49 deg 36' 35.78" N
GPS Longitude     : 20 deg 43' 21.72" E
Focal Length      : 3.7 mm
GPS Position      : 49 deg 36' 35.78" N, 20 deg 43' 21.72" E
Light Value       : 2.0
```



49°36'35.8"N 20°43'21.7"E
49.609939, 20.722700

Wyznacz trasę Zapisz W pobliżu Wyślij na telefon Udostępnij

Rokitniańczyków 38, 33-300 Nowy Sącz
JP5F+X3G Nowy Sącz
Dodaj brakujące miejsce

5. Niestety nie udało mi się odzyskać pliku w formacie rar, udało się natomiast odzyskać pliki docx, exe, jpg, pdf oraz png.

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

Zadanie 3. – Recoverjpeg

1. Zainstalowanie narzędzia.






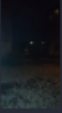
```
(kali㉿kali)-[~/Desktop/lab4]
$ sudo apt install recoverjpeg
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  exif graphicsmagick graphicsmagick-imagemagick-compat
  libgraphicsmagick-q16-3
Suggested packages:
  graphicsmagick-dbg
The following NEW packages will be installed:
  exif graphicsmagick graphicsmagick-imagemagick-compat
  libgraphicsmagick-q16-3 recoverjpeg
0 upgraded, 5 newly installed, 0 to remove and 382 not upgraded.
Need to get 2,253 kB/2,337 kB of archives.
After this operation, 9,543 kB of additional disk space will be used
Do you want to continue? [Y/n] y
Err:1 http://http.kali.org/kali kali-rolling/main amd64 libgraphicsm
```

2. Po wcześniejszej instalacji, użyłem *recoverjpeg*.

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

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

3. Udało się odzyskać 6 zdjęć.

kali Desktop recovery2			
Name	Size	Type	Date Modified
 image00005.jpg	3.0 MiB	JPEG image	Today
 image00004.jpg	2.9 MiB	JPEG image	Today
 image00003.jpg	2.3 MiB	JPEG image	Today
 image00002.jpg	2.2 MiB	JPEG image	Today
 image00001.jpg	2.2 MiB	JPEG image	Today
 image00000.jpg	3.2 MiB	JPEG image	Today

4. Odzyskane zdjęcia da się normalnie podejrzeć i zobaczyć jak wyglądają oraz co się na nich znajduje, w przeciwieństwie do narzędzia Foremost, które ujawniało jedynie metadane zdjęcia. Jest to niewątpliwie przewaga oraz zaleta stosowania *recoverjpeg*.

```
(root@kali)-[/home/kali/Desktop]
# cd recovery2

(root@kali)-[/home/kali/Desktop/recovery2]
# ls
image00000.jpg image00002.jpg image00004.jpg
image00001.jpg image00003.jpg image00005.jpg

(root@kali)-[/home/kali/Desktop/recovery2]
# exiftool 00019080.jpg
Error: File not found - 00019080.jpg

(root@kali)-[/home/kali/Desktop/recovery2]
# exiftool image00000.jpg
ExifTool Version Number      : 12.65
File Name                    : image00000.jpg
Directory                    : .
File Size                    : 3.4 MB
File Modification Date/Time  : 2023:11:25 13:37:14-05:00
File Access Date/Time       : 2023:11:25 13:41:19-05:00
```

Ponadto nazwy są inne niż te, które były oryginalnie, co stanowi kolejną różnicę pomiędzy obydwooma narzędziami (zmiana nazw).

Tak to wyglądało w Foremost.

```
(root@kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023/jpg]
# ls
00019080.jpg 00030160.jpg 00039400.jpg
00025648.jpg 00034720.jpg 00045360.jpg
```

Zadanie 4. – Scalpel

1. *Scalpel* do domyślnie dostępne rozwiązanie, a zatem uprzednia instalacja nie była wymagana.

```
(root@kali)-[/home/kali/Desktop/recovery_Sat_Nov_25_13_21_10_2023/jpg]
# cd /etc/scalpel

(root@kali)-[/etc/scalpel]
# ll
total 12
-rw-r--r-- 1 root root 8669 Dec 26 2022 scalpel.conf

(root@kali)-[/etc/scalpel]
#
```

2. Modyfikacja pliku konfiguracyjnego *scalpel.conf*.

```
root@kali: /etc/scalpel
File Actions Edit View Help
# wpc y 1000000 ?WPC
#
# HTML
#
#
# htm n 50000 <html >html>
#
#
# ADOBE PDF
#
#
# pdf y 5000000 %PDF %EOF\x0d REVERSE
# pdf y 5000000 %PDF %EOF\x0a REVERSE
#
#
# AOL (AMERICA ONLINE)
#
# AOL Mailbox
# mail y 5000000 \x41\x4f\x4c\x56\x4d
#
#
```

3. Uruchomieni narzędzia *scalpel*.

```
(root@kali)-[/home/kali/Desktop]
# scalpel lab4/usb-image.dd -v -o recovery_scalpel
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Output directory: "/home/kali/Desktop/recovery_scalpel"
Configuration file: "/etc/scalpel/scalpel.conf"
Coverage maps directory: "/home/kali/Desktop/recovery_scalpel"
Opening target "/home/kali/Desktop/lab4/usb-image.dd"

Total file size is 3274702848 bytes
Image file pass 1/2
```


Zakończenie

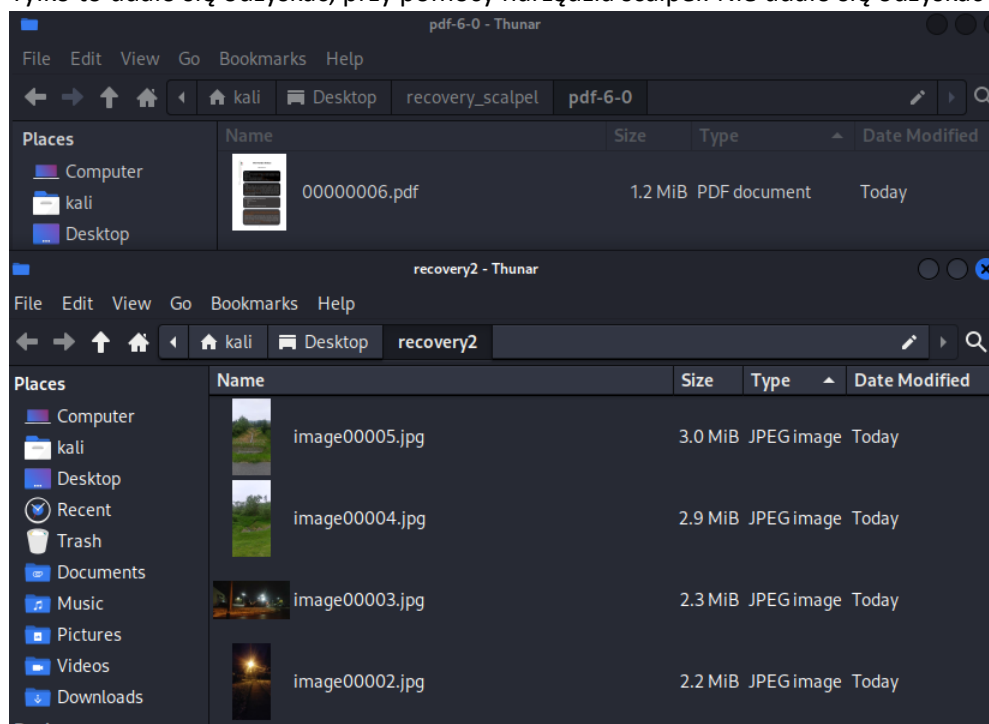
```
OPENING /home/kali/Desktop/recovery_scalpel/jpg-0-0/00000003.jpg
CLOSING /home/kali/Desktop/recovery_scalpel/jpg-0-0/00000003.jpg
lab4/usb-image.dd: 1.0% | 30.0 MB 00:03 ETA
CLOSING /home/kali/Desktop/recovery_scalpel/jpg-0-0/00000004.jpg
OPENING /home/kali/Desktop/recovery_scalpel/jpg-0-0/00000005.jpg
CLOSING /home/kali/Desktop/recovery_scalpel/jpg-0-0/00000005.jpg
lab4/usb-image.dd: 100.0% |*****| 3.0 GB 00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 7, elapsed = 28 seconds.

(root@kali)-[/home/kali/Desktop]
```

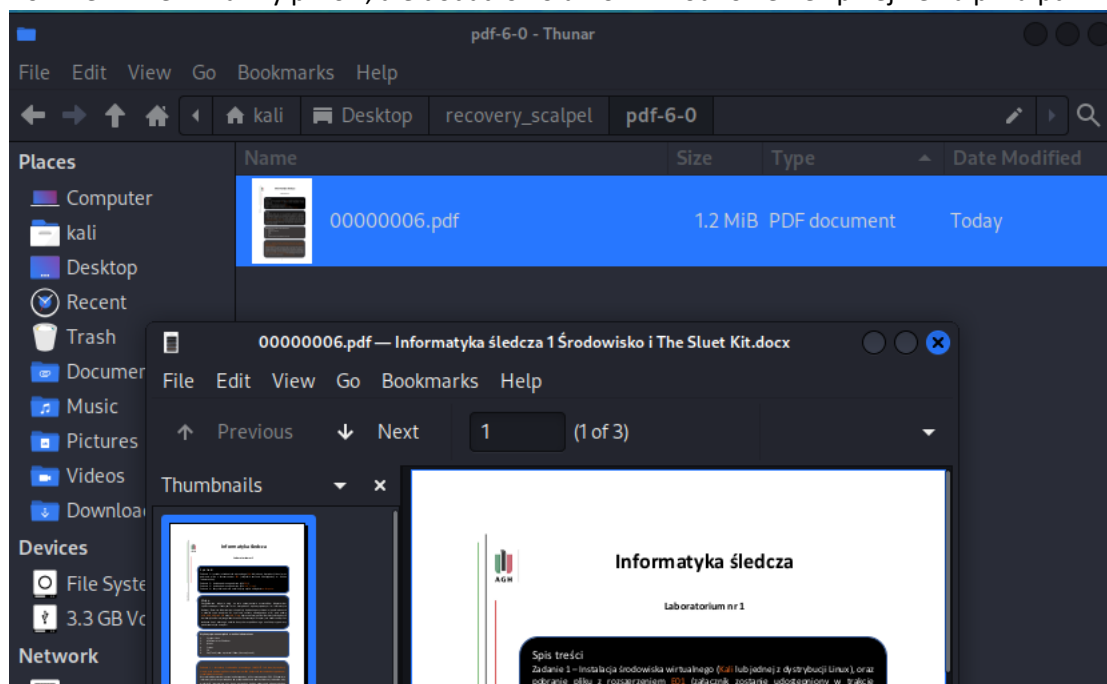
4. *Scalpel* odzyskał jedynie pliki w formacie pdf oraz zdjęcia wraz z metadanymi. W przeciwieństwie do innych narzędzi nie odzyskał np. pliku word oraz exe. Pomimo tego, że opcje te zostały odznaczone w pliku konfiguracyjnym.

```
# 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 /yome/kal 500000000 \x21\x42\x4e\xa5\x6f\xb5\xa6
# recovery_scalpel 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.



Również zmienił nazwy plików, ale dodatkowo umożliwił otwarcie i przejrzanie pliku pdf.



Zdanie 5. - Bulk_Extractor

1. Uruchomienie Bulk_Extractor. 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 mxxml 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
```

2. Prezentowana zawartość pliku tekstowego, który zawiera informacje o metadanych zdjęć

The screenshot shows a Kali Linux desktop environment. In the foreground, there are two windows:

- Thunar File Manager:** The title bar reads "recovery_bulk - Thunar". The address bar shows the path "kali > Desktop > recovery_bulk". The file list contains two files:

Name	Size	Type	Date Modified
gps.txt	704 bytes	plain text document	Today
exif.txt	211.5 KiB	plain text document	Today
- Visual Studio Code:** The title bar reads "gps.txt - Visual Studio Code". The window shows the contents of "gps.txt" with the following text:


```
home > kali > Desktop > recovery_bulk > gps.txt
1 # BANNER FILE NOT PROVIDED (-b option)
2 # BULK_EXTRACTOR-Version: 2.0.0
3 # Feature-Recorder: gps
4 # Filename: lab4/usb-image.dd
5 # Feature-File-Version: 1.1
6 9768972 00000000000000000000000000000000 2023-11-25T17/1 23/1 10/1,49.609940,20.722700,344.299000,,
7 13131788 00000000000000000000000000000000 2023-11-25T17/1 21/1 26/1,49.612084,20.722274,0.000000,,
8 15441932 00000000000000000000000000000000 2023-11-25T17/1 20/1 47/1,49.611038,20.723439,342.799000,,
9 17776652 00000000000000000000000000000000 2023-11-25T17/1 18/1 34/1,49.609954,20.724358,345.299000,,
10 20172812 00000000000000000000000000000000 2023-05-25T14:39:55,,0.000000,,
11 23224332 00000000000000000000000000000000 2023-05-25T14:39:46,,0.000000,,
```

Zadanie 6. – Porównanie poszczególnych narzędzi oraz podsumowanie odzyskiwania danych.

Uważam, że wszystkie wykorzystane podczas laboratorium narzędzia wyróżniają się na tle innych. Foremost jest zdecydowanie najprostszy, tzn. przedstawia odzyskane 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 przeglądanie 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 pracołłonne 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).

Zdanie 7. – Analiza rejestru systemu Windows

Do analizy elementów rejestru systemu Windows można posłużyć się narzędziem *reglookup*. Jest ono przeznaczone do odczytywania elementów rejestru Windowsa i wypisywania ich na standardowe wyjście. Posiada opcję filtrowania. Narzędzie to jest przeznaczone do pracy z rejestrami na systemie Windows NT.

Podaję to w ramach dodatkowych, gdyż uznałem, że dane są zaprezentowane w lepszy sposób przy użyciu *regripper*.

źródło: <https://linux.die.net/man/1/reglookup>

Narzędzie to nie jest dostępne domyślnie, a zatem musiałem je zainstalować.

```
(kali㉿kali)-[~/Desktop]
└─$ sudo apt-get install reglookup
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libregf1
The following NEW packages will be installed:
  libregf1 reglookup
0 upgraded, 2 newly installed, 0 to remove and 1121 not upgraded.
Need to get 59.3 kB of archives.
After this operation, 187 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libregf1 amd64 1.
+svn287-9 [31.8 kB]
```

1. Analiza NTUSER.DAT

- Czy są jakiegokolwiek ślady używania Adobe Acrobat? Adobe Acrobat – tworzy pliki w formacie pdf

```
Launching adobe v.20200522
adobe v.20200522
(NTUSER.DAT) Gets user's Adobe app cRecentFiles values

Could not access Software\Adobe\Adobe Acrobat\AVGeneral\cRecentFiles

Could not access Software\Adobe\Acrobat Reader\AVGeneral\cRecentFiles

_____  
Launching allowedenum v.20200511
```

- Jakie aplikacje są skojarzone z kluczem ApplicationAssociationToasts?

```
Launching appassoc v.20200515
appassoc v.20200515
- Gets contents of user's ApplicationAssociationToasts key

LastWrite: 2016-10-05 09:51:45Z

IE.HTTP_http
```

Przykład przy użyciu reglookup

```
(kali㉿kali)-[~/Desktop]
└─$ reglookup Reg-Windows/NTUSER.DAT | grep -i "ApplicationAssociationToasts"
/Software/Microsoft/Windows/CurrentVersion/ApplicationAssociationToasts,KEY,,2016-10-05 09:51:45
/Software/Microsoft/Windows/CurrentVersion/ApplicationAssociationToasts/IE.HTTP_http,DWORD,0x00000000,
```

- Czy znaleziono dane o kompatybilności aplikacji w 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? Czasy zaprezentowana poniżej

```
Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time 2016-10-05 09:02:54Z
```

- Czy istnieje klucz AppSpecific dla Microsoft IntelliPoint?

```
Launching apppaths v.20200511
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys

Launching appspecific v.20200515
Software\Microsoft\IntelliPoint\AppSpecific not found.
```

- Jakie pliki zostały ostatnio otwarte za pomocą iexplore.exe?

```
iexplore.exe

FirstFolder
LastWrite time: 2016-10-09 19:59:14Z
Note: All value names are listed in MRUListEx order.

C:\Program Files\Internet Explorer\iexplore.exe

LastVisitedPidlMRU
LastWrite time: 2016-10-09 19:59:17Z
Note: All value names are listed in MRUListEx order.

iexplore.exe - My Computer\CLSID_Pictures
```

- Jakie są ustawienia środowiska użytkownika?

```
Launching environment v.20200512
environment v.20200512
(System, NTUSER.DAT) Get environment vars from NTUSER.DAT & System hives

Environment
LastWrite Time: 2016-10-05 09:01:00Z

TMP %USERPROFILE%\AppData\Local\Temp
TEMP %USERPROFILE%\AppData\Local\Temp
```

- Czy znaleziono informacje o Office Internet Server Cache?

Nie udało się znaleźć informacji.

```
Launching tsclient v.20200518
Launching tsclient v.20200518
(NTUSER.DAT) Displays contents of user's Terminal Server Client\Default key

Software\Microsoft\Terminal Server Client\Default not found.

Software\Microsoft\Terminal Server Client\Servers not found.
```

```
(kali㉿kali)-[~/Desktop]
$ reglookup Reg-Windows/NTUSER.DAT | grep -i "Office" | grep -i "Internet"

(kali㉿kali)-[~/Desktop]
$
```

```
(kali㉿kali)-[~/Desktop]
$ reglookup Reg-Windows/NTUSER.DAT | grep -i "Server" | grep -i "Internet"
/Software/Microsoft/Internet Explorer/SQM/ServerFreezeOnUpload,DWORD,0x00000001,
```

- Czy istnieją jakiegokolwiek ślady użycia WinRAR? Nie istnieją, tylko 7-zip.

```
Launching 7-zip v.20210329
sevenzip v.20210329
- Gets records of histories from 7-Zip keys

Software\7-Zip not found.
Software\Wow6432Node\7-Zip not found.
```

```
Launching winrar v.20200526
winrar v.20200526
(NTUSER.DAT) Get WinRAR\ArchHistory entries

Software\WinRAR\ArchHistory not found.
```

```
(kali㉿kali)-[~/Desktop]
$ reglookup Reg-Windows/NTUSER.DAT | grep -i "WinRar"

(kali㉿kali)-[~/Desktop]
$
```

Jakie strony internetowe zostały ostatnio wpisane przez użytkownika?

```
TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time 2016-10-05 09:47:50Z
url1 → http://www.catnews.com/
url2 → http://spotify.com/
url3 → http://pinterest.com/
url4 → http://webmail.student.greendale.xyz/
url5 → http://go.microsoft.com/fwlink/p/?LinkId=255141
```

- Jakie są ostatnie czasy dostępu do wpisanych adresów URL?

```
Launching typedurlstime v.20200526
typedurlstime v.20200526
(NTUSER.DAT) Returns contents of user's TypedURLsTime key.

TypedURLsTime
Software\Microsoft\Internet Explorer\TypedURLsTime
LastWrite Time 2016-10-05 09:47:50Z
url1 → 2016-10-05 09:47:50Z (http://www.catnews.com/)
url2 → 2016-10-05 09:38:22Z (http://spotify.com/)
url3 → 2016-10-05 09:38:16Z (http://pinterest.com/)
url4 → 2016-10-05 09:35:04Z (http://webmail.student.greendale.xyz/)
url5 → 0
```

- Czy są jakiekolwiek informacje o zainstalowanym oprogramowaniu Spotify? Tak, zaprezentowana poniżej.

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

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
```

2. Przeanalizuj plik SAM oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

Możemy tu znaleźć:

- informacje o użytkownikach, dla przykładu administrator. Nazwa użytkownika, SID, pełna nazwa, typ konta, data ostatniego logowania, data resetu hasła, liczbę logowań na konto admina, informacje o tym, że konto nigdy nie wygasa oraz o tym, że konto jest nieaktywne.

```
User Information
-----
Username       : Administrator [500]
SID            : S-1-5-21-4070822719-3404542230-2541167049-500
Full Name      : Administrator
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Mon Nov 23 02:26:36 2015 Z
Name           : 
Last Login Date : Tue Mar 18 10:20:47 2014 Z
Pwd Reset Date  : Tue Mar 18 10:20:51 2014 Z
Pwd Fail Date   : Never
Login Count     : 3
  → Normal user account
  → Password does not expire
  → Account Disabled
```

- dodatkowo możemy uzyskać informacje o grupach, dla przykładu grupa adminów. Jest podana nazwa, kto należy do grupy ostatnie nadpisanie grupy oraz opis tej grupy. Grup tych jest dosyć sporo.

```
Group Membership Information
-----
Group Name      : Administrators [3]
LastWrite       : Wed Oct 5 08:18:55 2016 Z
Group Comment    : Administrators have complete and unrestricted access to the computer/domain
Users           :
  S-1-5-21-226059406-2984137831-1201299043-512
  S-1-5-21-4070822719-3404542230-2541167049-1001
  S-1-5-21-4070822719-3404542230-2541167049-500

Group Name      : Access Control Assistance Operators [0]
LastWrite       : Tue Mar 18 09:52:29 2014 Z
Group Comment    : Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Users           : None
```


3. Przeanalizuj plik.

Informacje znajdujące się w pliku.

```
(kali㉿kali)-[~/Desktop]
$ sudo regripper -r Reg-Windows/SECURITY -a
Launching auditpol v.20200515
auditpol v.20200515
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time 2013-08-22 14:45:09Z

Data Length: 0x90
0x00000000: 00 01 00 00 09 00 00 00 7e 00 00 00 01 00 00 00 .....~.....
0x00000010: 03 00 00 00 03 00 01 00 01 00 01 00 00 00 00 01 .....
0x00000020: 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000050: 00 00 00 00 01 00 01 00 00 00 00 00 00 00 00 00 .....
0x00000060: 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 fe 7f 05 00 .....
0x00000080: 0a 00 0e 00 03 00 04 00 06 00 06 00 04 00 04 00 .....

Launching secrets v.20200517
secrets v.20200517
(Security) Get the last write time for the Policy\Secrets key

Policy\Secrets
LastWrite Time 2016-10-05 08:18:55Z
```

4. Przeanalizuj plik SOFTWARE oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

```
Launching audiodev v.20200525
audiodev v.20200525
(Software) Gets audio capture/render devices

Capture/Input Devices: GUID, Device
{057b6405-73fc-4409-b517-6830ef46f873}, Device: CD Audio
{a7fa8879-432a-449e-bb23-300b92591ea1}, Device: Microphone
{b3bc5a73-1aab-4bfe-a0e5-82a33a5161a5}, Device: Internal AUX Jack

Render/Output Devices: GUID, Device
{1fc10c6e-94e4-43c6-85d8-677699611a8b}, Device: Headphones
{c518a50f-2b6f-4b17-b286-d886c3526024}, Device: Speakers

Launching btconfig v.20200526
Launching btconfig v.20200526
(Software) Determines Bluetooth devices 'seen' by BroadComm drivers

WidComm\BTConfig\Devices not found.
```

Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

2013-08-22 15:37:10Z

AddressBook
Connection Manager
DirectDrawEx
DXM_Runtime
Fontcore
IE40
IE4Data
IE5BAKEX
IEData
MobileOptionPack
MPlayer2
SchedulingAgent
WIC

Launching volinfocache v.20200518

(Software) Gets VolumeInfoCache from Windows Search key

Microsoft\Windows Search\VolumeInfoCache

C: - LastWrite time: 2013-08-22 14:47:14Z

DriveType:

VolumeLabel:

E: - LastWrite time: 2016-11-22 23:01:40Z

DriveType:

VolumeLabel:

Launching winver v.20200525

winver v.20200525

(Software) Get Windows version & build info

ProductName	Windows 8.1 Enterprise Evaluation
BuildLab	9600.winblue_ltsb.160930-0600
BuildLabEx	9600.18505.amd64fre.winblue_ltsb.160930-0600
RegisteredOrganization	
RegisteredOwner	gold_administrator
InstallDate	2015-11-23 02:59:51Z

Launching wow64 v.20200515

wow64 v.20200515

(Software) Gets contents of WOW64\x86 key

WOW64

Microsoft\WOW64\x86 not found.

Microsoft\WOW64\arm not found.

Launching wsh_settings v.20200517

wsh_settings v.20200517

(Software) Gets WSH Settings

Microsoft\Windows Script Host\Settings

Key LastWrite: 2013-08-22 15:37:09Z

DisplayLogo	1
ActiveDebugging	1
SilentTerminate	0
UseWINSAFER	1

Analysis Tip: If Remote value is set to 1, system may be WSH Remoting target


```
Launching tracing v.20200511
Microsoft\Tracing
2015-11-23 02:19:11Z Explorer_RASAPI32
2013-08-22 15:37:09Z IpHlpSvc
2013-08-22 14:45:53Z MPRAPI
2013-08-22 14:47:08Z RASPLAP
```

```
Wow6432Node\Microsoft\Tracing
```

```
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
0 = Elevate without prompting
1 = Prompt for credentials on the secure desktop
2 = Prompt for consent on the secure desktop
3 = Prompt for credentials
4 = Prompt for consent
5 = Prompt for consent for non-Windows binaries (Default)
```

5. Przeanalizuj plik SYSTEM oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

```
ROOT_HUB [2015-11-23 02:19:05Z]
S/N: 4665dfc8360 [2016-11-23 10:57:27Z]
Properties Key LastWrite: 2015-11-23 02:59:51Z
ParentIdPrefix: 562d7ae1ff60
First InstallDate : 2015-11-23 02:19:05Z
InstallDate : 2015-11-23 02:19:05Z
Last Arrival : 2016-11-23 10:57:26Z

ROOT_HUB20 [2015-11-23 02:18:55Z]
S/N: 46280d2b2560 [2016-11-23 10:57:27Z]
Properties Key LastWrite: 2015-11-23 02:59:51Z
First InstallDate : 2015-11-23 02:18:55Z
InstallDate : 2015-11-23 02:18:55Z
Last Arrival : 2016-11-23 10:57:26Z

VID_058F6PID_6387 [2016-11-22 23:01:35Z]
S/N: 99E2116A [2016-11-22 23:01:37Z]
Properties Key LastWrite: 2016-11-22 23:01:37Z
First InstallDate : 2016-11-22 23:01:36Z
InstallDate : 2016-11-22 23:01:36Z
Last Arrival : 2016-11-22 23:01:35Z
Last Removal : 2016-11-22 23:14:03Z

VID_80EE6PID_0021 [2015-11-23 02:19:07Z]
S/N: 562d7ae1ff6061 [2016-11-23 10:57:33Z]
Properties Key LastWrite: 2015-11-23 02:59:51Z
ParentIdPrefix: 66156f3ba60
First InstallDate : 2015-11-23 02:19:08Z
InstallDate : 2015-11-23 02:19:08Z
Last Arrival : 2016-11-23 10:57:30Z
```

```
Launching usbdevices v.20200525
usbdevices v.20200525
(System) Parses Enum\USB key for USB & WPD devices
```

Powyżej pokazałem kilka ciekawostek jakie udało mi się znaleźć przy pomocy narzędzia *regripper*. Jest to narzędzie o dużych możliwościach.

6. Przeanalizuj plik UsrClass.dat oraz podaj 10 najciekawszych informacji znajdujących się w tym pliku.

```
(kali@kali)-[~/Desktop]
└─$ sudo regripper -r Reg-Windows/UsrClass.dat -a
Launching appx v.20200427
appx v.20200427
(NTUSER.DAT, USRCLASS.DAT) Checks for persistence via Universal Windows Platform Apps

Launching clsid v.20200526
clsid v.20200526
(Software, USRCLASS.DAT) Get list of CLSID/registered classes
CLSID not found.

Launching exefile v.20211214
exefile v.20211214
(USRCLASS.DAT,Software) Get file associations using exefile file handler and modified open handler for exefile

Hive Reg-Windows/UsrClass.dat

Launching muicache v.20200525
muicache v.20200525
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache not found.

Local Settings\Software\Microsoft\Windows\Shell\MUICache
LastWrite Time 2016-10-05 09:44:09Z

C:\users\bperry\appdata\roaming\spotify\spotify.exe.FriendlyAppName (Spotify)
C:\users\bperry\appdata\roaming\spotify\spotify.exe.ApplicationCompany (Spotify Ltd)

Launching photos v.20200525
photos v.20200525
(USRCLASS.DAT) Shell/BagMRU traversal in Win7 USRCLASS.DAT hives

Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\microsoft.windowsphotos_8wekyb3d8
bbwe\PersistedStorageItemTable\ManagedByApp key not found.

Launching scriptleturl v.20200525
scriptleturl v.20200525
(Software, USRCLASS.DAT) Check CLSIDs for ScriptletURL subkeys

Launching shellbags v.20200428
shellbags v.20200428
(USRCLASS.DAT) Shell/BagMRU traversal in Win7+ USRCLASS.DAT hives

MRU Time | Modified | Accessed | Created | Zip_Subfolder |
MFT File Ref | Resource | | | |
2016-10-09 20:04:37 | | | | |
```

Podsumowanie

Uważam, że narzędziem o najlepszym zastosowaniu jest *regripper*. W porównaniu do *reglookup* jest to narzędzie czytelniejsze i prostsze w użyciu oraz oferujące bardzo duże możliwości podczas analizy i tworzenia raportów z analizy rejestrów systemu Windows.