

Informatyka śledcza Laboratorium nr 4

Raport – Nikodem Jakubowski

Zadanie 1 – Przygotowanie do odzyskiwania danych.

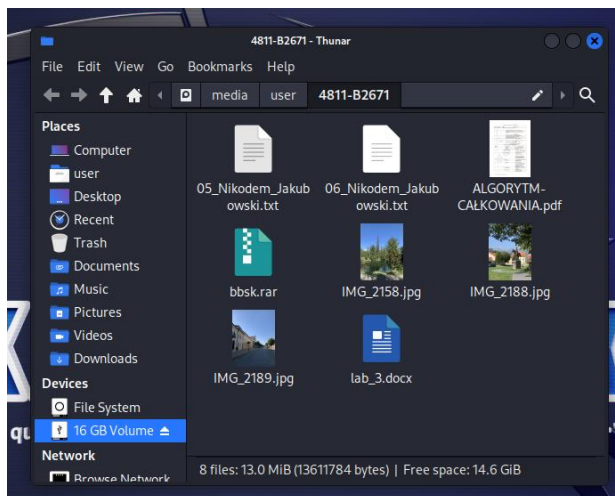
Podpiąłem pendriva i rozpocząłem procedurę czyszczenia („wipe”).

```
(user@user)-[~]
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda   8:0    0 25G  0 disk
├─sda1 8:1    0 24G  0 part /
├─sda2 8:2    0 1K   0 part
├─sda5 8:5    0 975M 0 part [SWAP]
└─sdb   8:16   1 14.6G 0 disk
   ├─sdb1 8:17   1 14.6G 0 part /media/user/340F-38EB
   └─sr0 11:0    1 1024M 0 rom

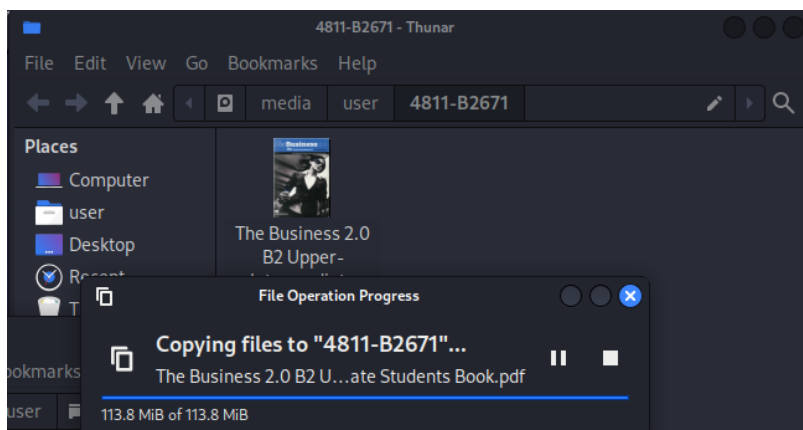
(user@user)-[~]
$ sudo dc3dd wipe=/dev/sdb1
[sudo] password for user:

dc3dd 7.2.646 started at 2023-11-23 15:38:21 +0100
compiled options:
command line dc3dd wipe=/dev/sdb1
device size: 30719936 sectors (probed), 15,728,607,232 bytes
sector size: 512 bytes (probed)
█ 2905538560 bytes ( 2.7 G ) copied ( 18% ), 330 s, 8.4 M/s
```

Przygotowałem pliki, następnie usunąłem je do kosza.



Przeniosłem plik około 100 MB na nośnik.



Rozpocząłem tworzenie kopii.

```
user@kali: ~  
File Actions Edit View Help  
[user@kali]~  
$ sudo dc3dd if=/dev/sdb1 hof=/home/user/Desktop/forensic-images/usb-image.dd hash=md5 log=/home/user/Desktop/file-log verb=on ssz=512  
[sudo] password for user:  
dc3dd 7.2.646 started at 2023-11-24 11:28:42 +0100  
compiled options:  
command line dc3dd if=/dev/sdb1 hof=/home/user/Desktop/forensic-images/usb-image.dd hash=md5 log=/home/user/Desktop/file-log verb=on ssz=512  
device size: 30719936 sectors (probed), 15,728,607,232 bytes  
sector size: 512 bytes (set)  
7667712 bytes ( 7.3 M ) copied ( 0% ), 3 s, 2.3 M/s
```

Ukończenie tworzenia kopii zakończone sukcesem, suma md5 się zgadza.

```
[user@kali]~  
$ sudo dc3dd if=/dev/sdb1 hof=/home/user/Desktop/forensic-images/usb-image.dd hash=md5 log=/home/user/Desktop/file-log verb=on ssz=512  
[sudo] password for user:  
dc3dd 7.2.646 started at 2023-11-24 11:28:42 +0100  
compiled options:  
command line dc3dd if=/dev/sdb1 hof=/home/user/Desktop/forensic-images/usb-image.dd hash=md5 log=/home/user/Desktop/file-log verb=on ssz=512  
device size: 30719936 sectors (probed), 15,728,607,232 bytes  
sector size: 512 bytes (set)  
15728607232 bytes ( 15 G ) copied ( 100% ), 6466 s, 2.3 M/s  
15728607232 bytes ( 15 G ) hashed ( 100% ), 97 s, 155 M/s  
input results for device '/dev/sdb1':  
30719936 sectors in  
0 bad sectors replaced by zeros  
b15a420ce1dff26247634e07c7695c7b (md5)  
output results for file '/home/user/Desktop/forensic-images/usb-image.dd':  
30719936 sectors out  
[ok] b15a420ce1dff26247634e07c7695c7b (md5)  
dc3dd completed at 2023-11-24 13:16:28 +0100
```

Zadanie 2 – Foremost.

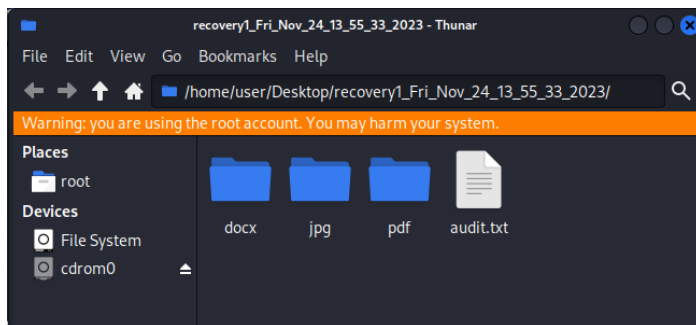
Skorzystanie z foremosta z opcją q (quick).

```
[user@kali]~/Desktop/forensic-images  
$ sudo foremost -v -t all -q -i usb-image.dd -o /home/user/Desktop/recovery1 -T  
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus  
Audit File  
Foremost started at Fri Nov 24 13:55:33 2023  
Invocation: foremost -v -t all -q -i usb-image.dd -o /home/user/Desktop/recovery1 -T  
Output directory: /home/user/Desktop/recovery1_Fri_Nov_24_13_55_33_2023  
Configuration file: /etc/foremost.conf  
Processing: usb-image.dd  
File: usb-image.dd  
Start: Fri Nov 24 13:55:33 2023  
Length: 14 GB (15728607232 bytes)  
Num Name (bs=512) Size File Offset Comment  
0: 00036624.jpg 3 MB 18751488  
1: 00044624.jpg 2 MB 22847488  
2: 00049584.jpg 2 MB 25387008  
foundat_rels/.rels (♦)  
3: 00054112.docx 2 MB 27705344  
4: 00032944.pdf 160 KB 16867328  
*****
```

Bez opcji q można również parsować pliki jpg osadzone w innych plikach.

```
[user@kali]~/Desktop/forensic-images  
$ sudo foremost -v -t all -i usb-image.dd -o /home/user/Desktop/recovery2 -T  
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus  
Audit File  
Foremost started at Fri Nov 24 13:56:36 2023  
Invocation: foremost -v -t all -i usb-image.dd -o /home/user/Desktop/recovery2 -T  
Output directory: /home/user/Desktop/recovery2_Fri_Nov_24_13_56_36_2023  
Configuration file: /etc/foremost.conf  
Processing: usb-image.dd  
File: usb-image.dd  
Start: Fri Nov 24 13:56:36 2023  
Length: 14 GB (15728607232 bytes)  
Num Name (bs=512) Size File Offset Comment  
0: 00036624.jpg 3 MB 18751488  
1: 00044624.jpg 2 MB 22847488  
2: 00049584.jpg 2 MB 25387008  
3: 00059680.jpg 593 KB 30556315  
4: 00060868.jpg 307 KB 31164455  
5: 00061424.jpg 672 KB 31480132  
6: 00062830.jpg 571 KB 32169427  
7: 00063975.jpg 1 MB 32755260  
8: 00066233.jpg 1 MB 33911657  
9: 00068544.jpg 806 KB 35094960  
Finish: Fri Nov 24 14:01:14 2023  
197 FILES EXTRACTED  
jpg== 165  
zip== 1  
png== 30  
pdf== 1
```

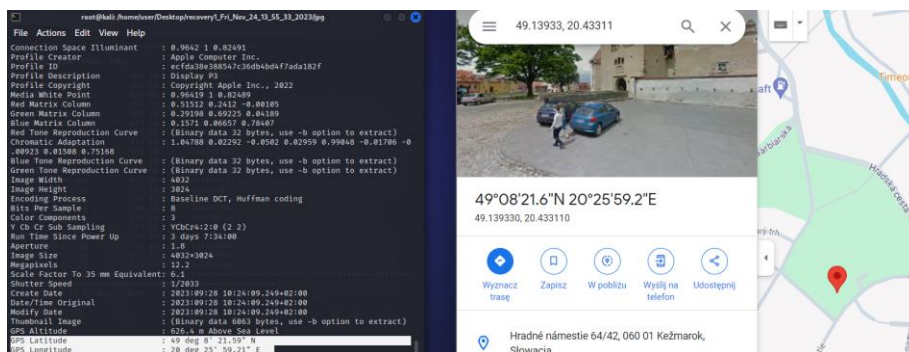
Folder z odzyskanymi danymi.



Odzyskane zdjęcia i metadane. Lokalizacja GPS odczytana przy pomocy exiftool zgadza się z tą, w której zostały zrobione.

```
(root@kali)~/Desktop/recovery1_Fri_Nov_24_13_55_33_2023/jpg
# ls
00036624.jpg 00044624.jpg 00049584.jpg

(root@kali)~/Desktop/recovery1_Fri_Nov_24_13_55_33_2023/jpg
# exiftool 00049584.jpg
ExifTool Version Number      : 12.65
File Name                    : 00049584.jpg
Directory                   : .
File Size                    : 2.3 MB
File Modification Date/Time  : 2023:11:24 13:55:33+01:00
```



Nie udało się jednak odzyskać pliku rar.

```
(user@kali)~/Desktop/forensic-images
$ sudo foremost -v -t rar -q -i usb-image.dd -o /home/user/Desktop/recovery1 -T

Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Nov 24 14:04:19 2023
Invocation: foremost -v -t rar -q -i usb-image.dd -o /home/user/Desktop/recovery1 -T
Output directory: /home/user/Desktop/recovery1_Fri_Nov_24_14_04_19_2023
Configuration file: /etc/foremost.conf
Processing: usb-image.dd
|
File: usb-image.dd
Start: Fri Nov 24 14:04:19 2023
Length: 14 GB (15728607232 bytes)

Num   Name (bs=512)      Size   File Offset   Comment
-----
*****^x@sS*****
*****|*****
Finish: Fri Nov 24 14:04:49 2023

0 FILES EXTRACTED

Foremost finished at Fri Nov 24 14:04:49 2023
```

Zadanie 3 – Recoverjpeg.

Użycie recoverjpeg. Jest on o tyle lepszy, że można dodatkowo wyświetlić odzyskany obraz, a nie tylko metadane.

```
(root@kali)-[/home/user/Desktop]
# recoverjpeg -o jpg-rec /dev/sdb1
Recovered files: 3      Analyzed: 732.0 MiB

jpg-rec - Thunar
Bookmarks  Help
user  Desktop  jpg-rec
image00000.jpg image00001.jpg image00002.jpg

(root@kali)-[/home/user/Desktop]
# cd jpg-rec
(root@kali)-[/home/user/Desktop/jpg-rec]
# ls
image00000.jpg image00001.jpg image00002.jpg
(root@kali)-[/home/user/Desktop/jpg-rec]
# exiftool image00000.jpg
ExifTool Version Number      : 12.65
File Name                    : image00000.jpg
Directory                    : .
File Size                    : 4.1 MB
File Modification Date/Time  : 2023:11:24 14:39:06+01:00
File Access Date/Time       : 2023:11:24 14:41:28+01:00
File Inode Change Date/Time  : 2023:11:24 14:39:06+01:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Make                        : Apple
```

Zadanie 4 – Scalpel.

Scalpel był domyślnie zainstalowany.

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

Użycie scalpel. Z manuala wnioskuję, że plik konfiguracyjny, z wprowadzonymi zmianami, jest domyślnie podpisany.

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

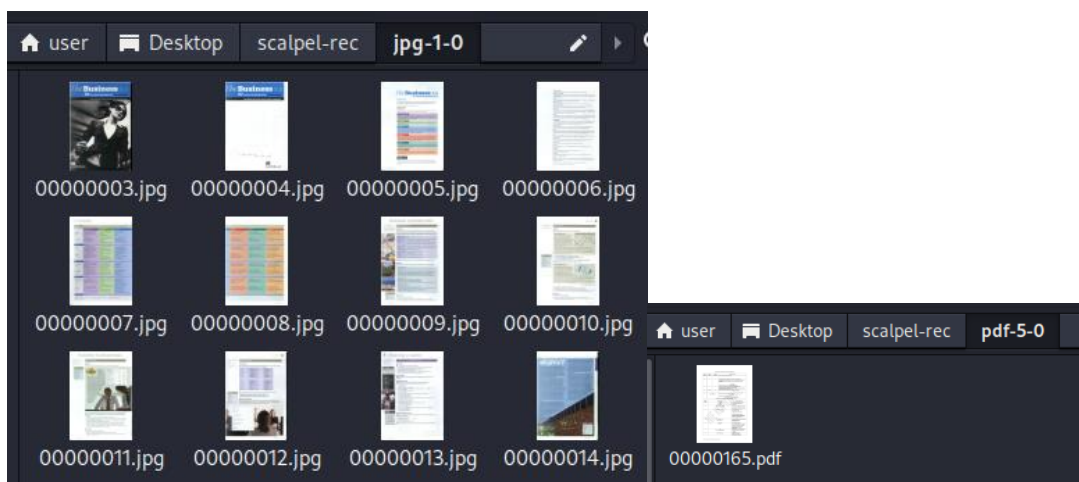
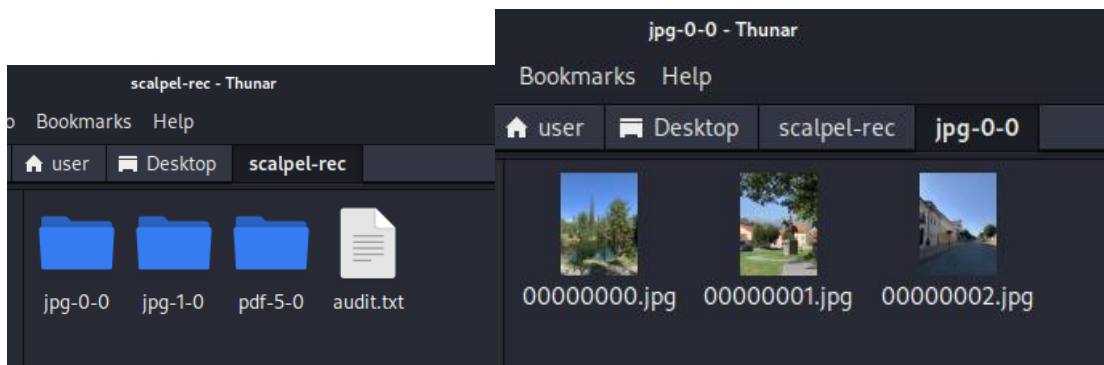
Opening target "/home/user/Desktop/forensic-images/usb-image.dd"

Total file size is 15728607232 bytes
Image file pass 1/2.
Read 10485760 bytes from image file.
forensic-images/usb-image.dd: 0.1% | 10.0 MB 00:00 ETA
Read 10485760 bytes from image file.
forensic-images/usb-image.dd: 0.1% | 20.0 MB 01:26 ETA
A jpg header was found at : 18751488
Memory reallocation performed, total header storage = 101
A jpg footer was found at : 16889564
Memory reallocation performed, total footer storage = 101
A jpg footer was found at : 16989394
A jpg footer was found at : 17004931
A jpg footer was found at : 17040556
```

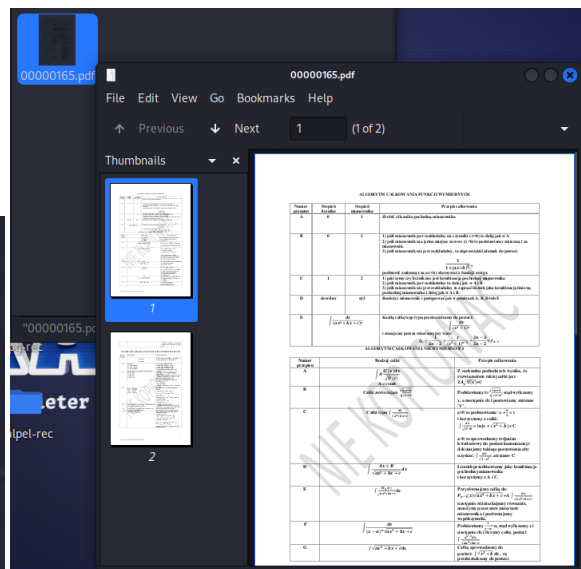
Ukończenie procesu.

```
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000160.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000159.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000158.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000157.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000156.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000155.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000154.jpg
OPENING /home/user/Desktop/scalpel-rec/jpg-1-0/00000161.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000161.jpg
OPENING /home/user/Desktop/scalpel-rec/jpg-1-0/00000162.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000162.jpg
OPENING /home/user/Desktop/scalpel-rec/jpg-1-0/00000163.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000163.jpg
OPENING /home/user/Desktop/scalpel-rec/jpg-1-0/00000164.jpg
CLOSING /home/user/Desktop/scalpel-rec/jpg-1-0/00000164.jpg
forensic-images/usb-image.dd: 100.0% [*****] 14.6 GB 00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 166, elapsed = 195 seconds.
```


Scalpel bardzo mi się spodobał. Wyciągnął z pdf wszystkie jpg i jeszcze można je otwierać. Nie dość, że można oglądać metadane to jeszcze można otwierać pliki.

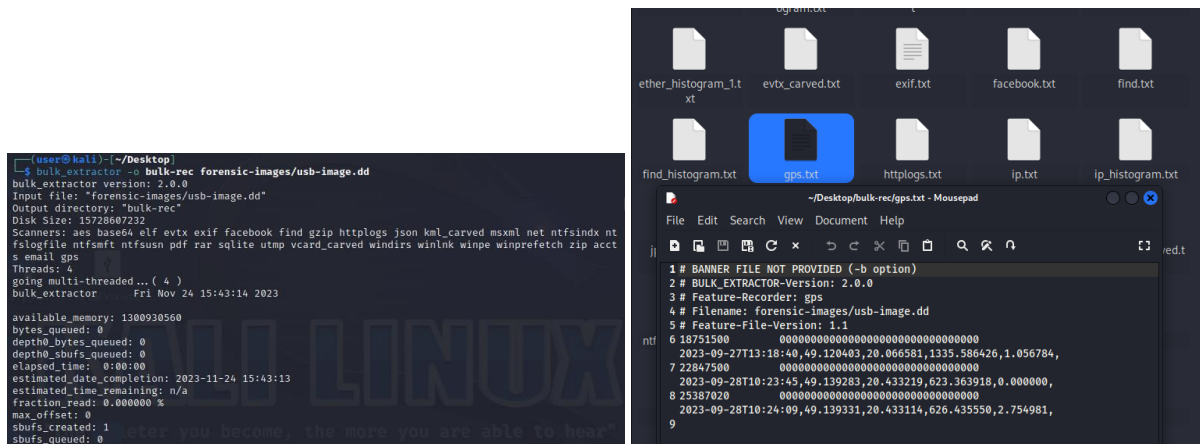


```
(root@kali) ~ # cd /home/user/Desktop
# cd scalpel-rec
# ls
audit.txt  jpg-0-0  jpg-1-0  pdf-5-0
# cd /home/user/Desktop/scalpel-rec
# cd jpg-0-0
# ls
00000000.jpg 00000001.jpg 00000002.jpg
# cd /home/user/Desktop/scalpel-rec/jpg-0-0
# exiftool 00000000.jpg
ExifTool Version Number      : 12.65
File Name                    : 00000000.jpg
Directory                    : .
```



Zadanie 5 – Bulk_Extractor.

Na początek włączyłem wszystkie opcje, by zobaczyć jak szybko pójdzie.



Bulk_extractor wypuścił bardzo dużą ilość danych w formacie .txt, parsował je bardzo szczegółowo i szybko - nawet z tak dużego pliku.

Zadanie 6 – Podsumowanie odzyskiwania danych.

Scalpel wyróżniał się efektywnością, wydobywając wszystkie jpg z pliku pdf i umożliwiając ich otwieranie, robiąc to szybko. Nieco więcej czasu zajmuje ustawienie jego opcji, przez co trzeba o nim trochę doczytać w dokumentacji.

Foremost był intuicyjny, skuteczny i szybki. Niestety nie ma możliwości obejrzenia (w sensie przeglądarki zdjęć/pdf) odzyskanych plików.

Bulk_extractor generował dużo danych w formacie tekstowym, ale może być przydatny w analizie szczegółowej bardzo dużych plików. Te dane mogą być dobrze wykorzystane przez program agregujący.

Preferowane narzędzie: zdecydowanie **Scalpel**, ze względu na: skuteczność, możliwość przeglądania wyglądu plików oraz wyświetlanie metadanych.

Trudności: nie udało się nigdzie odzyskać pliku rar. Kilka razy musiałem kopiować dane z nośnika przy pomocy dc3dd, co jest bardzo czasochłonne. Na początku myślałem, że przydzielając większe zasoby maszynie wirtualnej przyspieszę proces, co nie przyniosło rezultatu. Później zapchałem zagospodarowaną pamięć dla maszyny wirtualnej, co spowodowało jej zablokowanie. Gdy zrobiłem kopię, odłączyłem pendrive. Po czym w drugim zadaniu znowu trzeba było go podpiąć, a system Windows wymagał formatu pendrive i wszystko zaczynało się od nowa... Miałem szczęście, że w domu miałem stary pendrive 16GB, przy większym musiałbym maszynę zostawić na noc albo dzielić na nim partycje, co przyszło mi do głowy po laboratorium.

- Czy istnieje klucz AppSpecific dla Microsoft IntelliPoint? Nie wprost.

```
(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "AppSpe"

(user@kali) ~/Desktop
$

(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "Point"
/Software/Microsoft/Windows/CurrentVersion/Authentication/LogonUI/Notifications/BackgroundCapability/S-1-15-2-367627
9713-3632409675-756843784-3388909659-2454753834-4233625902-1413163418/App.AppX520v4bfs706hs9z4fr2f4nqdakqetyt6.mca/A
ppUserModelId,SZ,CheckPoint.VPN_cw5n1h2txyewy!App,
/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/KEY,,2016-10-09 19:57:35
/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/CPC/KEY,,2016-10-05 09:01:08
/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/CPC/Volume,KEY,,2016-10-09 20:04:04
/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/{8bffc84-9188-11e5-824f-806e6f6e6963},KEY,,2016-10
-09 19:57:35
/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/{8bffc88-9188-11e5-824f-806e6f6e6963},KEY,,2016-10
-09 19:57:35
/Software/Microsoft/Windows/CurrentVersion/SettingSync/SyncData/Namespaces/windowspackagesettings/checkpoint.vpn_cw5n
1h2txyewy,KEY,,2016-10-05 09:04:17
/Software/Microsoft/Windows/CurrentVersion/SettingSync/SyncData/Namespaces/windowspackagesettings/notifications-check
point.vpn_cw5n1h2txyewy,KEY,,2016-10-05 09:04:18
/Software/Microsoft/Windows/CurrentVersion/Themes/ThemeChangesMousePointers,DWORD,0x00000001,

(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "Intelli"
/Software/Microsoft/Internet Explorer/IntelliForms,KEY,,2016-10-05 09:36:54
/Software/Microsoft/Internet Explorer/IntelliForms/AskUser,DWORD,0x00000001,
/Software/Microsoft/Windows/CurrentVersion/ime/IMTC70/IntelliAgent.EscapeFunc,SZ,0x00000000,
/Software/Microsoft/Windows/CurrentVersion/ime/IMTC70/IntelliAgent.EnableFinal,SZ,0x00000001,
/Software/Microsoft/Windows/CurrentVersion/ime/IMTC70/IntelliAgent.AssociatedWord,SZ,0x00000000,
/Software/Microsoft/Windows/CurrentVersion/ime/IMTC70/IntelliAgent.AutoFinalize,SZ,0x00000000,
/Software/Microsoft/Windows/CurrentVersion/ime/IMTC70/IntelliAgent.AutoInputSwitch,SZ,0x00000000,
```

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

```
(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "iexplor"
/Software/Microsoft/Internet Explorer/LowRegistry/Audio/PolicyConfig/PropertyStore/fcc3671b_0_/SZ,{2}.\hdaudiofuc
nc_018ven_83848dev_76808subsys_838476808rev_1034#6994ad04-93ef-11d0-a3cc-00a0c9222196\aspeakertopo\00010001\Devic
e\HardiskVolume2\Program Files (x86)\Internet Explorer\iexplore.exe$25b{00000000-0000-0000-0000-000000000000},
/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.mc_id=WINSTORE_EN-US_OfficeApp_Buy_Text/OpenWithList/a
SZ,iexplore.exe,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{8856F961-340A-11D0-A96B-00C04FD705A2}/iexplore,KEY,,2016-10-09
19:59:04
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{8856F961-340A-11D0-A96B-00C04FD705A2}/iexplore/Type,DWORD,0x00
000001,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{8856F961-340A-11D0-A96B-00C04FD705A2}/iexplore/Flags,DWORD,0x0
0000000,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{8856F961-340A-11D0-A96B-00C04FD705A2}/iexplore/Count,DWORD,0x0
0000006,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{8856F961-340A-11D0-A96B-00C04FD705A2}/iexplore/Time,BINARY,%0
%07%0A%00%00%00%09%00%13%00;%00%04%00%03,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{D27CDB6E-AE6D-11CF-96B8-444553540000}/iexplore,KEY,,2016-10-09
19:58:54
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{D27CDB6E-AE6D-11CF-96B8-444553540000}/iexplore/Type,DWORD,0x00
000001,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{D27CDB6E-AE6D-11CF-96B8-444553540000}/iexplore/Flags,DWORD,0x0
0000000,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{D27CDB6E-AE6D-11CF-96B8-444553540000}/iexplore/Count,DWORD,0x0
0000005,
/Software/Microsoft/Windows/CurrentVersion/Ext/Stats/{D27CDB6E-AE6D-11CF-96B8-444553540000}/iexplore/Time,BINARY,%0
%07%0A%00%00%00%09%00%13%00;%00%06%00%BE%02,
```

- Jakie są ustawienia środowiska użytkownika?

```
(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "env"
/Environment,KEY,,2016-10-05 09:01:00
/Environment/TMP,EXPAND_SZ,%25USERPROFILE%25\AppData\Local\Temp,
/Environment/TEMP,EXPAND_SZ,%25USERPROFILE%25\AppData\Local\Temp,
/Software/Microsoft/Speech/Preferences/AppCompatDisableMSAA/devenv.exe,SZ,,
```

- Czy znaleziono informacje o Office Internet Server Cache? Nie.

```
(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "server"
/Software/Microsoft/Internet Explorer/SQM/ServerFreezeOnUpload,DWORD,0x00000001,
/Software/Microsoft/MediaPlayer/Preferences/AutoMetadataCurrent500ServerErrorCount,DWORD,0x00000000,
/Software/Microsoft/MediaPlayer/Preferences/AutoMetadataCurrent503ServerErrorCount,DWORD,0x00000000,
/Software/Microsoft/MediaPlayer/Preferences/AutoMetadataCurrentOtherServerErrorCount,DWORD,0x00000000,
/Software/Microsoft/Windows/CurrentVersion/Explorer/Advanced/ServerAdminUI,DWORD,0x00000000,

(user@kali) ~/Desktop
$

(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -iE "office@server"

(user@kali) ~/Desktop
$

(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "office" | grep -i "cache"

(user@kali) ~/Desktop
$

(user@kali) ~/Desktop
$ reglookup infs-upel-win/NTUSER.DAT | grep -i "office" | grep -i "cache"
```


- Czy istnieją jakiegokolwiek ślady użycia WinRAR? Nie.

```
(user@kali) ~/Desktop
msf5 > reglookup info-uptel-win/NTUSER.DAT | grep -i "winrar"

(user@kali) ~/Desktop
msf5 > reglookup info-uptel-win/NTUSER.DAT | grep -i "rar"

/Control Panel/Infrared/KEY,2016-10-05 09:01:00
/Control Panel/Infrared/File Transfer,KEY,2016-10-05 09:01:00
/Control Panel/Infrared/File Transfer/AllowSend,DWORD,0x00000001
/Control Panel/Infrared/File Transfer/ShowRecvStatus,DWORD,0x00000001
/Control Panel/Infrared/Global/KEY,2016-10-05 09:01:00
/Control Panel/Infrared/Global/ShowTrayIcon,DWORD,0x00000001
/Control Panel/Infrared/Global/PlaySound,DWORD,0x00000001
/Control Panel/Infrared/Infrared,KEY,2016-10-05 09:01:00
/Control Panel/Infrared/Infrared/DisableCOM,DWORD,0x00000001
/Software/Microsoft/Internet Explorer/LowRegistry/IEShims/NormalizedPaths/C:/Users/berry/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/NONE,(null)
/Software/Microsoft/Internet Explorer/LowRegistry/IEShims/NormalizedPaths/C:/Users/berry/AppData/Local/Microsoft/Windows/Temporary Internet Files/Virtualized/NONE,(null)
/Software/Microsoft/MediaPlayer/Preferences/MediaLibrary/CreateNewDatabase,DWORD,0x00000000
/Software/Microsoft/MediaPlayer/Preferences/LibraryHasBeenRun,DWORD,0x00000000
/Software/Microsoft/MediaPlayer/Preferences/HLE/LocalLib/uuid,0x108946c-1656-4896-9C0B-6CD742C49A9B)
/Software/Microsoft/Windows/CurrentVersion/Explorer/Is/IsFtDistributedLib,DWORD,0x00000001
/Software/Microsoft/Windows/CurrentVersion/Explorer/Disableable/PostSetup/ShellNew/Classes,MULTI_SZ,.bmp|.contact|.jnt|.library-ms|.lnk|.rtf|.txt|.zip|Folder
/Software/Microsoft/Windows/CurrentVersion/Explorer/Shell Folders/{1B3EASDC-B587-4786-BA4F-BD1DC323AAE}.SZ,C:/Users/berry/AppData/Local/Microsoft/Windows/Libraries
/Software/Microsoft/Windows/CurrentVersion/Live/Roaming/RegisteredData,KEY,2016-10-05 09:09:19
/Software/Microsoft/Windows/CurrentVersion/Live/Roaming/RegisteredData/RenewCollectionsInterestDirtty,DWORD,0x00000000
/Software/Microsoft/Windows/CurrentVersion/Live/Roaming/RegisteredData/LastRenewCollectionsInterest,QWORD,0x01D2EE6272D5F6E
```

- Jakie strony internetowe zostały ostatnio wpisane przez użytkownika? Jakie są ostatnie czasy dostępu do wpisanych adresów URL?

```

Software/Microsoft/Windows/Shell/Associations/AAssociations/KV, 2016-10-05 09:03:21
Software/Microsoft/Windows/Shell/Associations/Associations/audiodl-messenger.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/audiodl-svpe.com.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/AlingFinance.KV, 2016-10-05 09:03:13
Software/Microsoft/Windows/Shell/Associations/Associations/bingdownloadink.KV, 2016-10-05 09:03:28
Software/Microsoft/Windows/Shell/Associations/Associations/binghtml-themes.KV, 2016-10-05 09:03:19
Software/Microsoft/Windows/Shell/Associations/Associations/BingMaps.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/bingnews.KV, 2016-10-05 09:03:18
Software/Microsoft/Windows/Shell/Associations/Associations/BingSports.KV, 2016-10-05 09:03:17
Software/Microsoft/Windows/Shell/Associations/Associations/BingTravel.KV, 2016-10-05 09:03:17
Software/Microsoft/Windows/Shell/Associations/Associations/bingweather.KV, 2016-10-05 09:03:21
Software/Microsoft/Windows/Shell/Associations/Associations/Http.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/Http/UserChoice.KV, 2016-10-05 09:01:01
Software/Microsoft/Windows/Shell/Associations/Associations/Http/Hash-S2.BlogPostView.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/Http/UserChoice/ProgId.S1.HTTP.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/Http.KV, 2016-10-05 09:03:01
Software/Microsoft/Windows/Shell/Associations/Associations/Http/UserChoice.KV, 2016-10-05 09:03:01
Software/Microsoft/Windows/Shell/Associations/Associations/Https/Wash_S2.Key3Eg.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/Https/UserChoice/ProgId.S1.HTTP.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/message-messenger.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/microsoftrm.KV, 2016-10-05 09:03:17
Software/Microsoft/Windows/Shell/Associations/Associations/microsofttmsvc.KV, 2016-10-05 09:03:16
Software/Microsoft/Windows/Shell/Associations/Associations/microsoftevents.KV, 2016-10-05 09:03:15
Software/Microsoft/Windows/Shell/Associations/Associations/memote.KV, 2016-10-05 09:03:14
Software/Microsoft/Windows/Shell/Associations/Associations/profile-linker.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-linked-in.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-link-cym.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-linker.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-outlook-com.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-skyve-key.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-walter-com.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/profile-webto-com.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/skyve-key.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/skyve.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/sms.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/Assoc.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/adicaldl-messenger.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/shodansearch.KV, 2016-10-05 09:03:07
Software/Microsoft/Windows/Shell/Associations/Associations/indownloadlink.MT, 2016-10-05 09:03:21
Software/Microsoft/Windows/Shell/Associations/Associations/alcalendar.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/Assoc.KV, 2016-10-05 09:03:11
Software/Microsoft/Windows/Shell/Associations/Associations/xboxgames.KV, 2016-10-05 09:03:16

```

```
[user@kali: ~]$ cd /Desktop
$ reglookup info-super-win/TUSER.DAT | grep -i "url"
C:\Software\Microsoft\AuthCookies/LiveDefault/DIDC/MO_SZ_https://login.live.com,
C:\Software\Microsoft/Internet Explorer/BrowserEmulation/CVIList/PreviousDownload/MO_SZ_https://iecvlist.microsoft.com/I
E11/138749476087/iecompvievlist.xml,
C:\Software\Microsoft/Internet Explorer/Help_Menu_MU_KEY_2016-10-05 09:01:27
C:\Main/InfoShow/FallBack_SZ_yes,
C:\Software/Microsoft/Internet Explorer/Main/Show_InfoInStatusBar_SZ_yes,
C:\Software/Microsoft/Internet Explorer/Main/Show_ToolBar_SZ_yes,
C:\Software/Microsoft/Internet Explorer/SearchScopes/{B633E93D-0776-42FF-A0FF-161688B2E3A1}/TopResultURLFallback_SZ_ht
tp://www.bing.com/search?qs=SearchTermsIsSrc-IE-TopResultURLFallback-ITEMR202,
C:\Software/Microsoft/Internet Explorer/SearchScopes/{B633E93D-0776-42FF-A0FF-161688B2E3A1}/SuggestionsURLFallback_SZ_h
ttp://api.bing.com/cqm.aspx?Query={SearchTerms}&maxwidth={ie:maxwidth}&rowheight={ie:rowheight}&jsectionHeight={ie:
sectionHeight}&lang=US&S202Marker={Language},
C:\Software/Microsoft/Internet Explorer/SearchScopes/{B633E93D-0776-42FF-A0FF-161688B2E3A1}/FaviconURLFallback_SZ_http
t://www.bing.com/favicon.ico,
C:\Software/Microsoft/Internet Explorer/SearchScopes/{B633E93D-0776-42FF-A0FF-161688B2E3A1}/URL_SZhttp://www.bing.com
/search?q={SearchTerms}IsSrc-IE-SearchBoxForm-IESR202,
C:\Software/Microsoft/Internet Explorer/Setup/History/MigrationTime_BINARY_X2CMIXF80MDE7F3ED20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_YES-2016-10-05 09:17:58
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.catnews.com/,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://spotify.com/,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://fast.com/,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://webmail.student.greendale.zy,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://go.microsoft.com/fwlink/?LinkID=259141,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://time.aksv,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x1.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x2.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x3.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x4.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x5.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x6.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x7.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Internet Explorer/TypedURLSZ_HTTPSZhttp://www.x8.BINARY_XBBYQX89KCEUEIEN20x1,
C:\Software/Microsoft/Windows/CurrentVersion/Explorer/SearchPlatform/Preferences/DisableAutoNavigateURL_IOWORD_0+000000
00
```

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

[illegible]

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

Tutaj widać reset hasła o godzinie 3 w nocy.

```
/SAM/Domains/Account/Users/000003E9/ForcePasswordReset,BINARY,%00%00%00%00,
/SAM/Domains/Account/Users/000003E9/UserPasswordHint,BINARY,.%00,
/SAM/Domains/Account/Users/Names/KEY,,2015-11-23 02:59:18
/SAM/Domains/Account/Users/Names/,NONE,(null),
/SAM/Domains/Account/Users/Names/Administrator,KEY,,2015-11-23 02:26:36
/SAM/Domains/Account/Users/Names/Administrator/,0x000001F4,(null),
/SAM/Domains/Account/Users/Names/gold_administrator,KEY,,2015-11-23 02:59:18
/SAM/Domains/Account/Users/Names/gold_administrator/,0x000003E9,(null),
/SAM/Domains/Account/Users/Names/Guest,KEY,,2015-11-23 02:26:36
/SAM/Domains/Account/Users/Names/Guest/,0x000001F5,(null),
/SAM/Domains/Builtin,KEY,,2016-10-05 08:18:55
```

Poniżej mamy kilka informacji: grupy wbudowane oraz ich id, użytkownicy wbudowani, jakie są grupy w strukturze, aktualizacja SKU, grupy i nazwy, informacja o dostępie zdalnym.

```
/SAM/Domains/Builtin/Aliases/Members/S-1-5-21-070822719-340542230-254167049/000003E9/,SZ ,0x02X000  
/SAM/Domains/Builtin/Aliases/Names/Key,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/,NONE,(null),  
/SAM/Domains/Builtin/Aliases/Names/Access Control Assistance Operators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Access Control Assistance Operators,/0=00000243,(null),  
/SAM/Domains/Builtin/Aliases/Names/Administrators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Administrators,/0=00000220,(null),  
/SAM/Domains/Builtin/Aliases/Names/Backup Operators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Backup Operators,/0=00000227,(null),  
/SAM/Domains/Builtin/Aliases/Names/Cryptographic Operators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Cryptographic Operators,/0=00000239,(null),  
/SAM/Domains/Builtin/Aliases/Names/Distributed COM Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Distributed COM Users,/0=00000232,(null),  
/SAM/Domains/Builtin/Aliases/Names/Event Log Readers,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Event Log Readers,/0=00000230,(null),  
/SAM/Domains/Builtin/Aliases/Names/Guests,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Guests,/0=00000222,(null),  
/SAM/Domains/Builtin/Aliases/Names/Hyper-V Administrators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Hyper-V Administrators,/0=00000242,(null),  
/SAM/Domains/Builtin/Aliases/Names/IIS_IUSRSG,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/IIS_IUSRSG,/0=00000238,(null),  
/SAM/Domains/Builtin/Aliases/Names/Network Configuration Operators,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Network Configuration Operators,/0=0000022C,(null),  
/SAM/Domains/Builtin/Aliases/Names/Performance Log Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Performance Log Users,/0=0000022F,(null),  
/SAM/Domains/Builtin/Aliases/Names/Performance Monitor Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Performance Monitor Users,/0=0000022E,(null),  
/SAM/Domains/Builtin/Aliases/Names/Power Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Power Users,/0=00000223,(null),  
/SAM/Domains/Builtin/Aliases/Names/Remote Desktop Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Remote Desktop Users,/0=0000022B,(null),  
/SAM/Domains/Builtin/Aliases/Names/Remote Management Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Remote Management Users,/0=00000244,(null),  
/SAM/Domains/Builtin/Aliases/Names/Replicator,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Replicator,/0=00000228,(null),  
/SAM/Domains/Builtin/Aliases/Names/Users,KEY,,2015-11-23 02:26:35  
/SAM/Domains/Builtin/Aliases/Names/Users,/0=00000221,(null),  
/SAM/Domains/Builtin/Groups,KEY,,2013-08-22 14:45:10  
/SAM/Domains/Builtin/Groups/,NONE,(null),  
/SAM/Domains/Builtin/Groups/Names/Key,,2013-08-22 14:45:10  
/SAM/Domains/Builtin/Groups/Names/,NONE,(null),  
/SAM/Domains/Builtin/Users,KEY,,2013-08-22 14:45:10  
/SAM/Domains/Builtin/Users/Names/Key,,2013-08-22 14:45:10  
/SAM/Domains/Builtin/Users/Names/,NONE,(null),  
/SAM/LastSkuUpgrade,KEY,,2014-03-18 09:52:29  
/SAM/LastSkuUpgrade/,DWORD,0=00000048,  
/SAM/RXACT,KEY,,2013-08-22 14:45:10  
/SAM/RXACT/,NONE,0x1000x00x00x9100x00x00x00x00x00x00
```


Poniżej mamy kilka informacji: wpis dot. domyślnego hasła, aktualizacja jego czasu i wartości, opis jego zabezpieczeń.

[illegible]

Tutaj jest bardzo dużo informacji. Najciekawsze to obecność np. AdobeAcrobat, Excel.

[illegible]

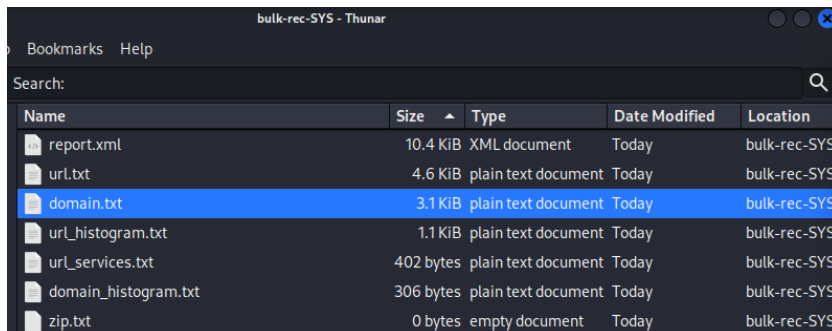
```

Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/SQLLevel,SZ,0
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/DriverOBC8Ver,SZ,02_50
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/APILevel,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/ConnectFunctions,SZ,YYN
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/Setup,EXPAND_SZ,%25WINIDR25\system32\odexl32.dll
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/UsageCount,DWORD,0*00000001
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/Driver,EXPAND_SZ,%25WINIDR25\system32\odbcjt32.dll
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/FileUsage,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Driver do Microsoft Excel (*.xls)/FileExtns,SZ*.xls
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls),KEY,2013-08-22 15:37:01
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/SQLLevel,SZ,0
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/DriverOBC8Ver,SZ,02_50
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/APILevel,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/ConnectFunctions,SZ,YYN
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/Setup,EXPAND_SZ,%25WINIDR25\system32\odexl32.dll
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/UsageCount,DWORD,0*00000001
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/Driver,EXPAND_SZ,%25WINIDR25\system32\odbcjt32.dll
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/FileUsage,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel Driver (*.xls)/FileExtns,SZ*.xls
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls),KEY,2013-08-22 15:37:01
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/SQLLevel,SZ,0
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/DriverOBC8Ver,SZ,02_50
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/APILevel,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/ConnectFunctions,SZ,YYN
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/Setup,EXPAND_SZ,%25WINIDR25\system32\odexl32.dll
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/UsageCount,DWORD,0*00000001
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/Driver,EXPAND_SZ,%25WINIDR25\system32\odbcjt32.dll
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/FileUsage,SZ,1
Wow6432Node\OBC8\OBC8INST.INI\Microsoft Excel-Treiber (*.xls)/FileExtns,SZ*.xls
Wow6432Node\OBC8\OBC8INST.INI\OBC8 Drivers\Driver do Microsoft Excel (*.xls),SZ,Installed
Wow6432Node\OBC8\OBC8INST.INI\OBC8 Drivers\Microsoft Excel Driver (*.xls),SZ,Installed
Wow6432Node\OBC8\OBC8INST.INI\OBC8 Drivers\Microsoft Excel-Treiber (*.xls),SZ,Installed

```

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

Tutaj również mamy bardzo dużo informacji. Potraktuję go bulk_extractor z ciekawości... Trochę danych udało mu się wyciągnąć.



Name	Size	Type	Date Modified	Location
report.xml	10.4 KiB	XML document	Today	bulk-rec-SYS
url.txt	4.6 KiB	plain text document	Today	bulk-rec-SYS
domain.txt	3.1 KiB	plain text document	Today	bulk-rec-SYS
url_histogram.txt	1.1 KiB	plain text document	Today	bulk-rec-SYS
url_services.txt	402 bytes	plain text document	Today	bulk-rec-SYS
domain_histogram.txt	306 bytes	plain text document	Today	bulk-rec-SYS
zip.txt	0 bytes	empty document	Today	bulk-rec-SYS

```
(user@kali)~[~/Desktop]
$ regripper -r infs-upel-win/SYSTEM -a
```

W internecie natrafiłem również na narzędzie regripper, który ma fantastyczne możliwości. Poniżej opis kilku pluginów służących do interpretacji rejestrów Windowsa.

```
(user@kali)~[~/Desktop]
$ regripper -l | head -n 35
1. mpmru v.20200517 [NTUSER.DAT]
   - Gets user's Media Player RecentFileList values
2. shutdown v.20200518 [System]
   - Gets ShutdownTime value from System hive
3. devclass v.20200525 [System]
   - Get USB device info from the DeviceClasses keys in the System hive
4. userassist_tln v.20180710 [NTUSER.DAT]
   - Displays contents of UserAssist subkeys in TLN format
5. appassoc v.20200515 [NTUSER.DAT]
   - Gets contents of user's ApplicationAssociationToasts key
```

Korzystając z manuala regripperera:

-f <hivetype> Specify the hive type/profile to use, could be sam, security, software, system, ntuser.

```
(user@kali)~[~/Desktop]
$ sudo regripper -r infs-upel-win/SYSTEM -f system
```

Opcja -a włącza wszystkie pluginy, które dotyczą danego typu „hive’a” czyli w tłumaczeniu ula (źródła informacji).

```
(user@kali)~[~/Desktop]
$ sudo regripper -r infs-upel-win/SYSTEM -f system -a
```

Wstawiam zdjęcie po wykorzystaniu części z nich oraz ciekawe informacje.


```

Launching usbstor v.20200515
usbstor v.20200515
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

DiskVen_Generic6Prod_Flash_Disk6Rev_8.07 [2016-11-22 23:01:37]
S/N: 99E2116A60 [2016-11-22 23:01:37Z]
Device Parameters LastWrite: [2016-11-22 23:01:37Z]
Properties LastWrite : [2016-11-22 23:01:37Z]
    FriendlyName      : Generic Flash Disk USB Device
    First InstallDate  : 2016-11-22 23:01:37Z
    InstallDate        : 2016-11-22 23:01:37Z
    Last Arrival       : 2016-11-22 23:01:37Z
    Last Removal       : 2016-11-22 23:04:49Z

Launching wpdusenum v.20200515
wpdusenum v.20200515
(System) Get WpdBusEnum subkey info

_??_USBSTOR#DiskVen_Generic6Prod_Flash_Disk6Rev_8.07#99E2116A60#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
DeviceDesc: Flash Disk
Friendly: E:\
Mfg: Generic
Properties Key LastWrite: 2016-11-22 23:01:47Z
    First InstallDate  : 2016-11-22 23:01:48Z
    InstallDate        : 2016-11-22 23:01:48Z
    Last Arrival       : 2016-11-22 23:01:44Z
    Last Removal       : 2016-11-22 23:04:49Z

ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}
##7#SND\SensorsAndLocationEnum\PSensorSNDDevice#10497b1b-ba51-44e5-8318-a65c837b6661
LastWrite: Tue Oct 11 20:05:24 2016 UTC
    DeviceInstance: SND\SensorsAndLocationEnum\LPSensorSNDDevice

##7#SND\WPDBUSENUM\_??_USBSTOR#DiskVen_Generic6Prod_Flash_Disk6Rev_8.07#99E2116A60#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}#10497b1b
LastWrite: Tue Nov 22 23:01:47 2016 UTC
    DeviceInstance: SND\WPDBUSENUM\_??_USBSTOR#DiskVen_Generic6Prod_Flash_Disk6Rev_8.07#99E2116A60#{53f56307-b6bf-11d0-94f2-00a0c91ef

```

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

```

[user@kali:~/Desktop/Info-upel-win]
$ regripper -r UsrClass.dat -a
Launching appx v.20200527
appx v.20200527
(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 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 2016-10-09 09:44:09Z

C:\Users\hperry\AppData\Roaming\spotify\spotify.exe.FriendlyAppName (Spotify)
C:\Users\hperry\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.windows.photos_BeeKb3d8Bwe\PersistedStorageItemTable\ManagedByAp

Launching scripteturl v.20200525
scripteturl v.20200525
(Software, USRCLASS.DAT) Check CLSIDs for ScriptetURL 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 | | | | | | [Control Panel [Desktop\0]]
2016-10-09 19:56:55 | | | | | | [Control Panel\Appearance\Pe
2016-10-09 19:56:55 | | | | | | [Control Panel\Appearance\Pe
2016-10-09 19:57:50 | | | | | | [Control Panel\Appearance\Pe
2016-10-09 19:59:07 | | | | | | [My Computer [Desktop\1\]]
My Computer\CLSID_Pictures

Launching uacbypass v.20200511
uacbypass v.20200511
(USRCLASS.DAT, Software) Get possible UAC bypass settings

```

Ogólny wniosek do zadania 7.

Istnieje kilka wspólnych narzędzi do przeszukiwania rejestrów w linuxie. Są to m.in. regripper i reglookup i nimi głównie się pożytkowałem. Z obu skorzystałem i odkryłem ich opcje.