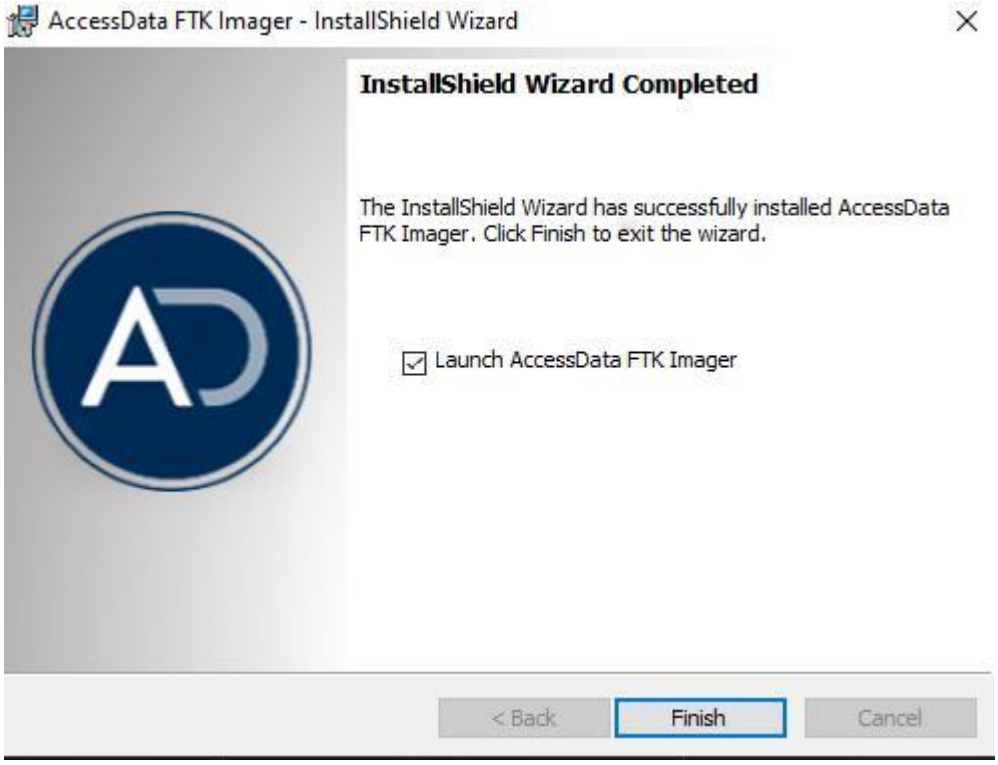
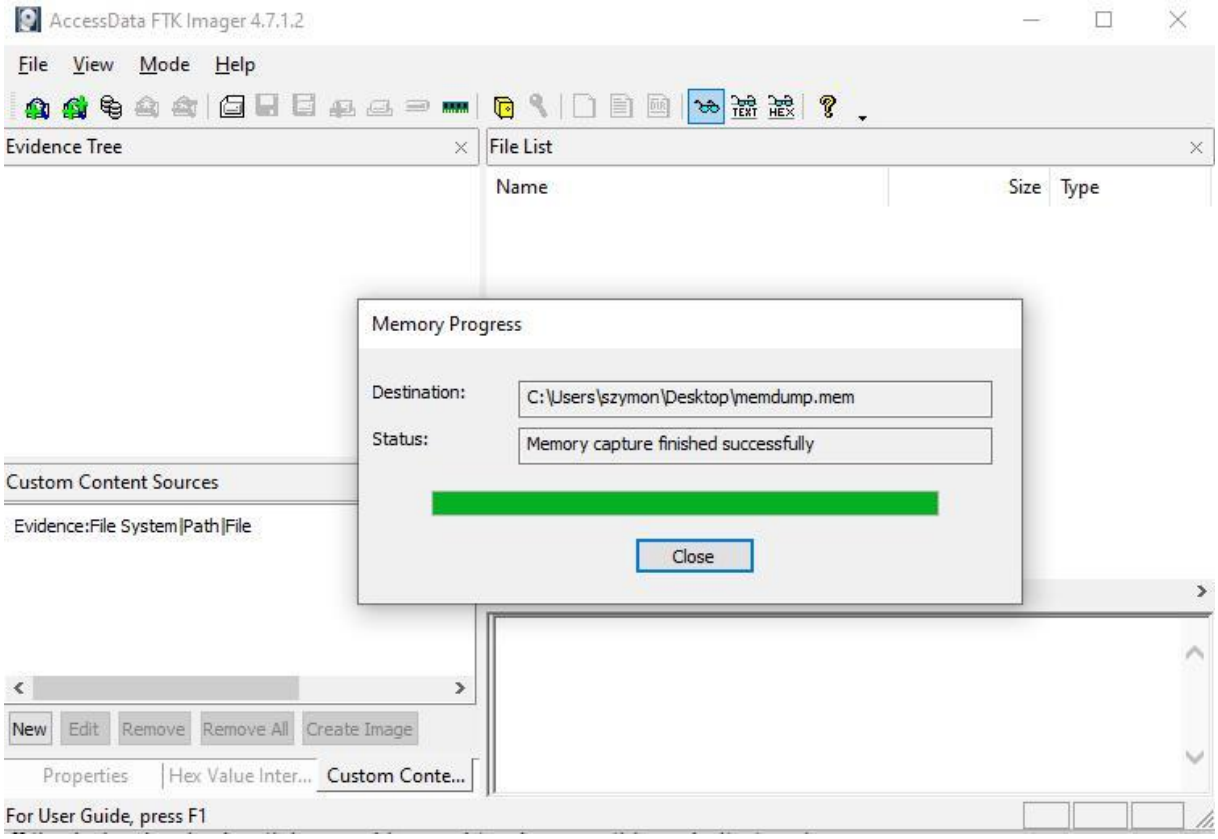
Laboratorium 6. – Szymon Szkarłat

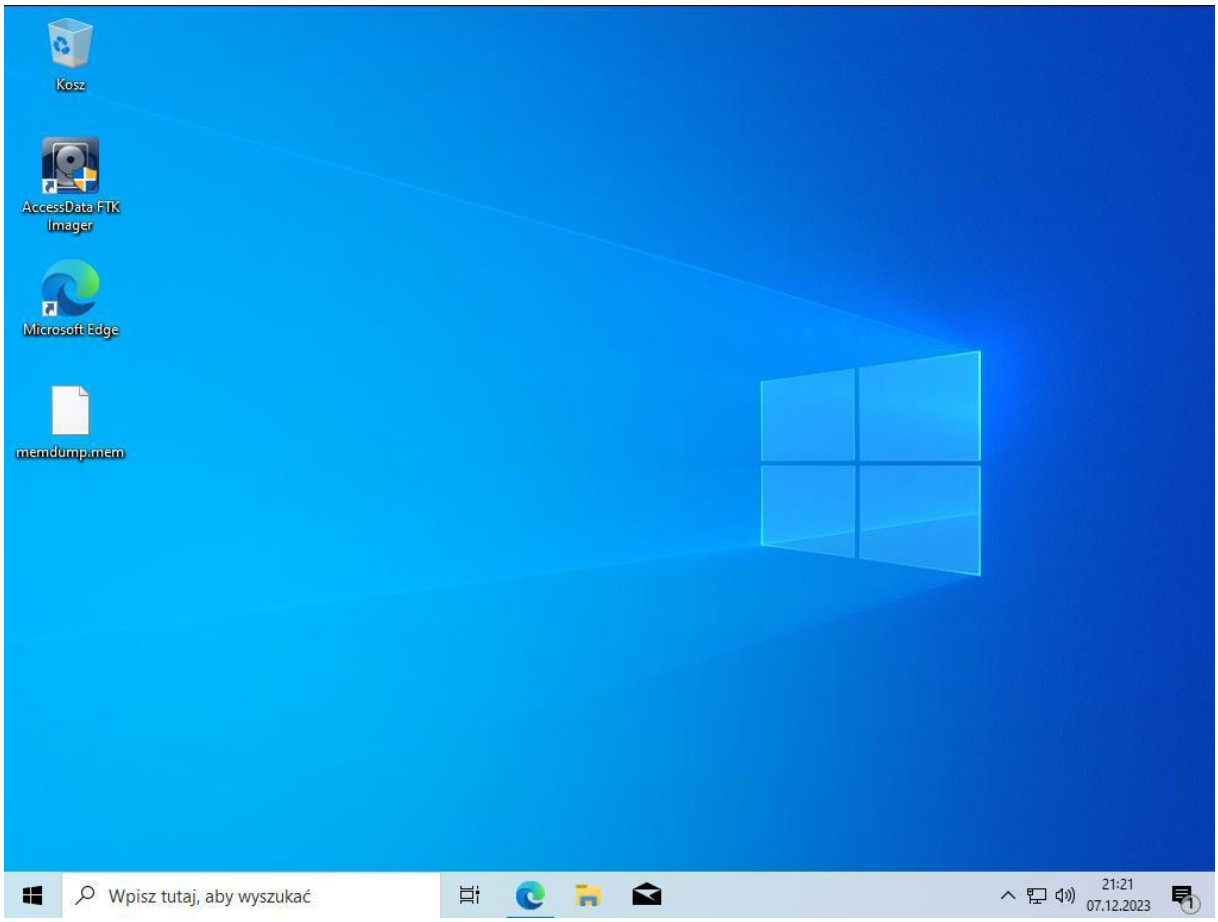
Zadanie 1. – Tworzenie zrzutu pamięci z systemu Windows



Tworzenie dumpa

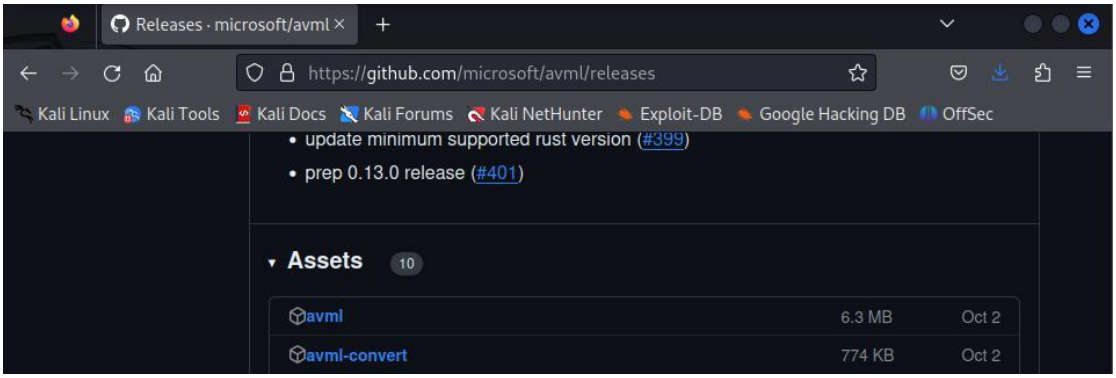


Potwierdzenie użycia FTK Imager



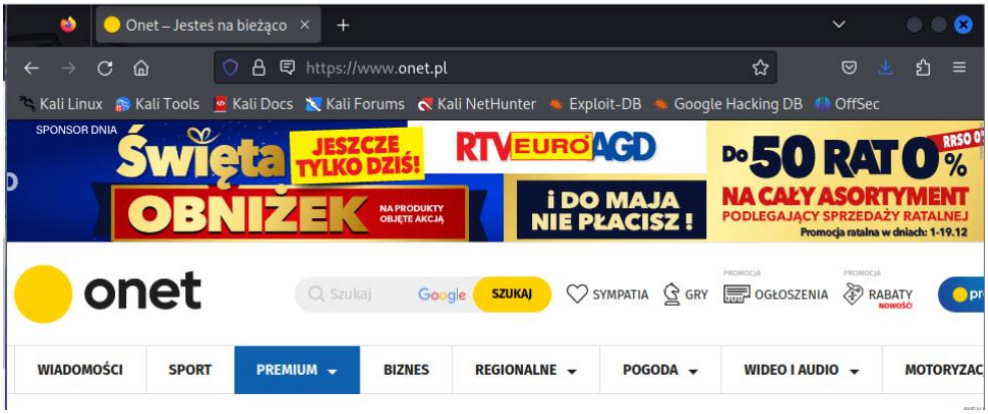
Zadanie 2. – Tworzenie zrzutu z systemu Linux

1. Pobranie programu avml

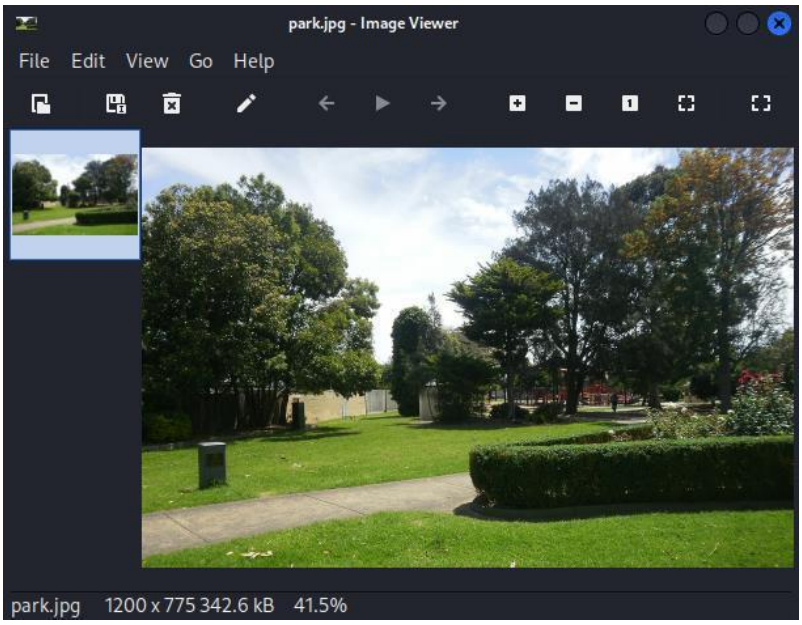


2. Zmiana uprawnień, polecenie: chmod 755

3. Wywołanie dowolnej strony: onet.pl, przy pomocy przeglądarki Firefox



4. Otwarcie zdjęcia w formacie jpg



5. Wykonanie zrzutu pamięci polecenie: sudo ./avml memoryLinux.dmp

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo ./avml memoryLinux.dmp
[sudo] password for kali:
```

Potwierdzenie wykonania zrzutu pamięci.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
avml  code_1.81.1-1691620686_amd64.deb  memoryLinux.dmp  park.jpg
```

Próba odczytania zawartości przy pomocy polecenia strongs.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo strings memoryLinux.dmp
EMiL
PAMS
PAMS
4{,%$l
```

Niestety bez użycia dodatkowych filtrów, czyli bez użycia komendy grep nie jestem w stanie odnaleźć w pamięci informacji o wywołaniu strony internetowej (www.onet.pl) oraz pliku graficznego o nazwie park.jpg. Narzędzie strings generuje mnóstwo informacji, w postaci dużej liczby wierszy wyświetlanych bezpośrednio w terminalu.

Próba wyszukania wywołania strony www.onet.pl, przy pomocy komendy grep.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo strings memoryLinux.dmp | grep onet.pl
```

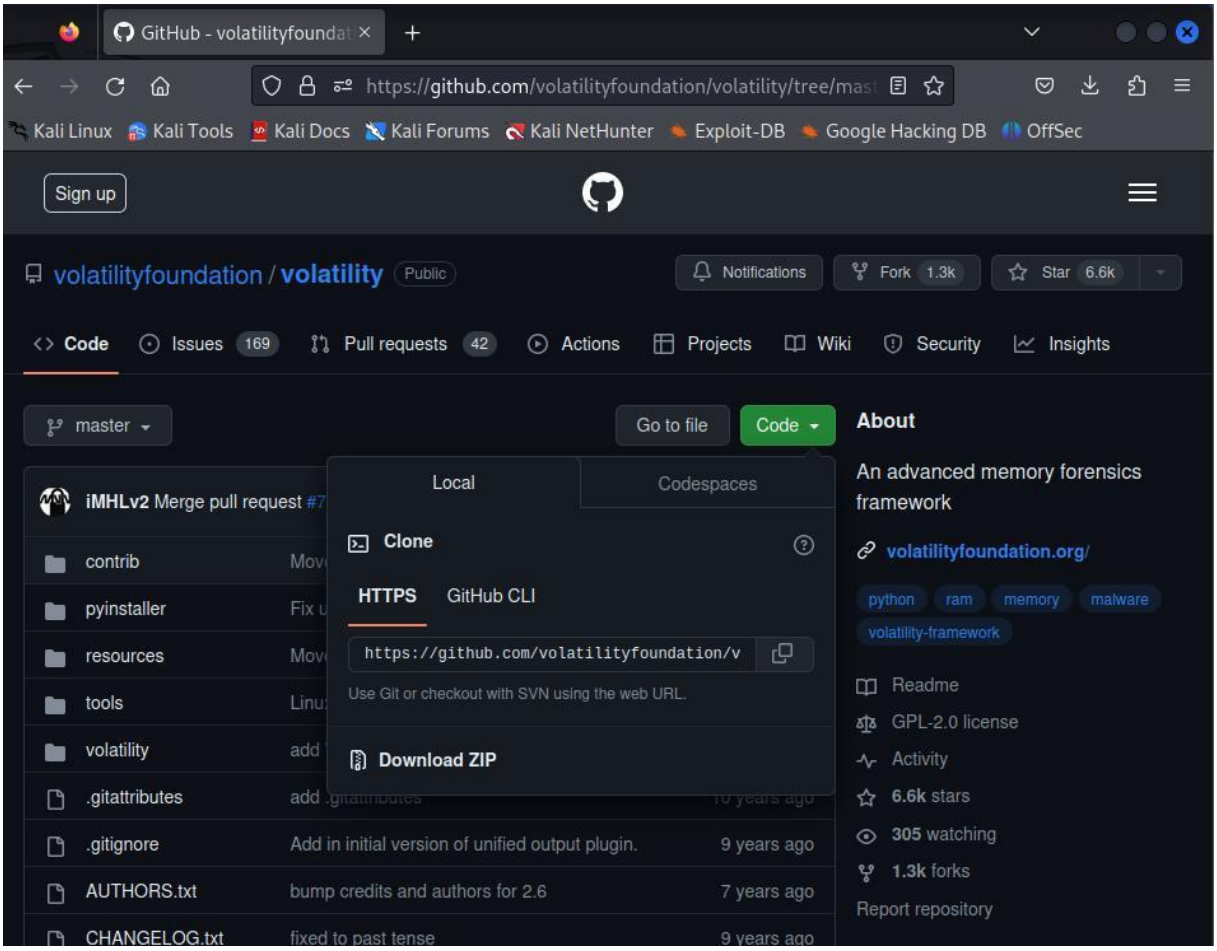
```
https://www.onet.pl
https://www.onet.pl/
https://www.onet.pl/
https:www.onet.pl:443:.:^partitionKey=%28https%2Conet.pl%29:3   0       19698   https:
www.onet.pl:443:www.onet.pl:443::n:1702047166:h3:y:1701960075:n:^partitionKey=%28https
%2Conet.pl%29:|n:y:
access-control-allow-origin: https://www.onet.pl
access-control-allow-origin: https://www.onet.pl
https://www.onet.pl
:https://onet.hit.gemius.pl/__/_1701960761735/rexdot.js?l=100&sendf=24&id=bPo6D0bzSxcu
e3osfkZZIJaE.l0RyeOgSEhsufRYys3.W7&et=view&hsrc=1&initsonar=1&extra=&eventid=0&tz=300&
fv=-&href=https%3A%2F%2Fwww.onet.pl%2F&screen=958×993r1000&col=24&window=958×747&vis=1
&lsdata=-SETERR&fpdata=ZSB8kVPuklA5ywEowyTU21JiyoCTsuJJH76OvYoo5qD.z7&ltime=285&fr=1&r
ef=&inner=_ver%3D346&exid=6571dc391337969f&brts=1701960761&fpcap=
access-control-allow-origin: https://www.onet.pl
file:///home/kali/.mozilla/firefox/6zx38kbc.default-esr/storage/default/https+++www.on
et.pl/cache/caches.sqlite-wal
```

Próba wyszukania wywołania zdjęcia park.jpg, przy pomocy komendy grep.

```
ii/Downloads/park.jpg
ioads/park.jpg
ii/Downloads/park.jpg
file:///home/kali/Downloads/park.jpg
file:///home/kali/Downloads/park.jpg
park.jpg - Image Viewer
park.jpg - Image Viewer
park.jpg - Image Viewer
park.jpg - Image Viewer
file:///home/kali/Downloads/park.jpg
```

Zadanie 3. – Analiza pamięci przy wykorzystaniu programu Volatility.

1. Pobranie programu Volatility przy wykorzytsaniu wirtualnej maszyny z systemem Linux



2. Pobranie przygotowanego obrazu memory3.vmem

3. Przejście do pliku z pobranym frameworkiem Volatility.

4. Sprawdzenie czy program nie potrzebuje żadnych dodatkowych bibliotek

Okazało się, że dodatkowo należało zainstalować biblioteki pycrypto oraz distorm3.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
--2023-12-07 10:30:53--  https://bootstrap.pypa.io/pip/2.7/get-pip.py
Resolving bootstrap.pypa.io (bootstrap.pypa.io)... 151.101.36.175, 2a04:4e42:9::175
Connecting to bootstrap.pypa.io (bootstrap.pypa.io)|151.101.36.175|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1908226 (1.8M) [text/x-python]
Saving to: 'get-pip.py'

get-pip.py           100%[===================>]   1.82M  7.46MB/s    in 0.2s

2023-12-07 10:30:53 (7.46 MB/s) - 'get-pip.py' saved [1908226/1908226]
```

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ sudo python2 get-pip.py
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgra
de your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for P
ython 2.7 in January 2021. More details about Python 2 support in pip can be found at
https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 w
ill remove support for this functionality.
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 1.5 MB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, wheel
Successfully installed pip-20.3.4 wheel-0.37.1

┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ pip2 install --upgrade setuptools
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgra
de your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for P
ython 2.7 in January 2021. More details about Python 2 support in pip can be found at
https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 w
ill remove support for this functionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting setuptools
  Downloading setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
     |████████████████████████████████| 583 kB 1.4 MB/s
Installing collected packages: setuptools
  WARNING: The scripts easy_install and easy_install-2.7 are installed in '/home/kali/
.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, u
se --no-warn-script-location.
Successfully installed setuptools-44.1.1
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install python2-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2-dev libpython2.7 libpython2.7-dev python2.7-dev
The following NEW packages will be installed:
  libpython2-dev libpython2.7 libpython2.7-dev python2-dev python2.7-dev
0 upgraded, 5 newly installed, 0 to remove and 1212 not upgraded.
```

```
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for libc-bin (2.37-7) ...

┌──(kali㉿kali)-[~]
└─$ pip2 install pycrypto
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgra
de your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for P
ython 2.7 in January 2021. More details about Python 2 support in pip can be found at
https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 w
ill remove support for this functionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting pycrypto
```

```
┌──(kali㉿kali)-[~]
└─$ pip2 install distorm3
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgra
de your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for P
ython 2.7 in January 2021. More details about Python 2 support in pip can be found at
https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 w
ill remove support for this functionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting distorm3
  Downloading distorm3-3.5.2.tar.gz (138 kB)
     |████████████████████████████████| 138 kB 1.5 MB/s
```

Po zainstalowaniu dodatkowych bibliotek, nie wyświetlają się błędy, a jedynie „pomoc”.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -h
Volatility Foundation Volatility Framework 2.6.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/kali/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/home/kali/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
                        the Module Output Options below)
  --output-file=OUTPUT_FILE
```

Przechodzę zatem do sprawdzenia podstawowych informacji, które znajdują się na badanym obrazie.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x
86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/memory3.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 18:24:00 UTC+0000
     Image local date and time : 2010-08-15 14:24:00 -0400
```

5. Odpowiedzi na pytania:

a) Jakie sugerowane profile są aktualnie podpowiadane przez program?
WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)

b) Do czego wykorzystywany jest adres KDBG?

KDBG to struktura obsługiwana przez jądro systemu Windows do celów debugowania. Zawiera listę uruchomionych procesów i załadowanych modułów jądra. Zawiera także informacje o wersji, które pozwalają określić, czy zrzut pamięci pochodzi z systemu Windows XP czy Windows 7 oraz jaki dodatek Service Pack został zainstalowany.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem kdbgscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80544ce0
Offset (P)                    : 0x544ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80544cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 2
Build string (NtBuildLab)     : 2600.xpsp_sp2_rtm.040803-2158
PsActiveProcessHead           : 0x80559258 (26 processes)
PsLoadedModuleList            : 0x805531a0 (119 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80544ce0
Offset (P)                    : 0x544ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x80544cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 2
Build string (NtBuildLab)     : 2600.xpsp_sp2_rtm.040803-2158
PsActiveProcessHead           : 0x80559258 (26 processes)
PsLoadedModuleList            : 0x805531a0 (119 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

c) DTB (Directory Table Base) – jest używany do translacji wirtualnego adresu na jaki adres? 0x319000L

d) O czym świadczą dane zawarte w KPCR (Kernel Processor Control Region) w odniesieniu do badanego obrazu?

KPCR reprezentuje region kontrolny procesora jądra. KPCR zawiera informacje o każdym procesorze, które są współdzielone przez jądro i warstwę HAL. W systemie jest tyle KPCR, ile jest procesorów. 6. Wywołanie funkcji, w celu wyświetlenia listy procesów systemu.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x810b1660 System                    4      0     58      183 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      369      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     20      518      0      0 2010-08-11 06:06:23 UTC+0000
```

a) Jakie informacje zawierają poszczególne kolumny:

Offset(V) – adres wirtualny, na którym zaczyna się rekord informacji o procesie PID – numer identyfikacyjny procesu (Process ID) PPID – numer ID rodzica procesu (Parent Process ID)

Thds – liczba wątków, które są skojarzone z danycm procesem (Threads)

Hnds – liczba uchwytów, czyli otwartych obiektów przez proces (Handles)

Sess = numer sesji , w ramach której działa proces

Wow64 – informacja, czy proces działa w trybie WOW64 (Windows-on-Windows 64-bit) Start – data i godzina uruchomienia procesu

Exit – data i godzina zakończenia procesu (jeśli proces został zakończony)

b) O czym świadczy znacznik (V) w rubryce Offset?

Znacznik (V) w rubryce Offset oznacza, że dane są w formacie wirtualnym (Virtual). Oznacza to, że wartości w tej kolumnie są adresami wirtualnymi, a nie fizycznymi. c) Który z niżej opisanych procesów został zakończony i kiedy?

Proces o PID 1136, o nazwie cmd.exe został zakończony 2010-08-15 18:24

d) Dlaczego procesy „System” i „smss.exe” nie posiadają informacji w rubryce Sess?

Procesy "System" i "smss.exe" nie posiadają informacji w rubryce "Sess" (sesja). To wynika z faktu, że te procesy są uruchamiane w kontekście systemowym, niezależnym od sesji użytkownika.

e) Który numer procesu należy do VMwareUser.exe?
Numer procesu (PID) VMwareUser.exe to 452.

7. Jaką zmianę wywołał wskaźnik -P? Porównaj zmianę w procesie VMwareUser.exe.

a) dla opcji pslist

```
0xff374980 VMwareUser.exe          452   1724      6      189      0      0 2010-08-11 06:09:32 UTC+0000
```

b) dla opcji pslist -P

```
0x04b5a980 VMwareUser.exe          452   1724      6      189      0      0 2010-08-11 06:09:32 UTC+0000
```

Jak widać różnica jest w Offsecie, a więc różni się adres wirtualny, w którym zaczyna się rekord.

8. Odpowiedzi na pytania:

a) Co oznaczają wyświetlone wcięcia i kropki?

Wyświetlone wcięcia i kropki reprezentują hierarchię procesów. Każde wcięcie oznacza, że dany proces jest podrzędnym (dzieckiem) procesu znajdującego się bezpośrednio nad nim. Kropki przed nazwami procesów wskazują na poziom hierarchii.

b) Jakiego identyfikatora nie znajdziemy w prezentowanych tabelach?

W prezentowanych tabelach nie znajdziemy identyfikatora sesji (Session ID).

c) Procesem nadrzędnym procesu smss.exe jest…?

Procesem nadrzędnym (rodzicem) procesu smss.exe jest proces o PID (Process ID) równym 4, czyli proces System.

d) Za co odpowiedzialny jest proces smss.exe?

Proces smss.exe (Session Manager Subsystem) jest odpowiedzialny za zarządzanie sesjami logowania w systemie Windows. Jest jednym z pierwszych procesów uruchamianych podczas startu systemu i odpowiada za tworzenie sesji dla użytkowników oraz uruchamianie procesów systemowych.

9. Wyświetlenie załadowanych bibliotek dll w badanym obrazie, z wykorzytsaniem wskaźnika -p dla PID 888.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem dllist -p 888
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
wscntfy.exe pid:    888
Command line : C:\WINDOWS\system32\wscntfy.exe
Service Pack 2

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x01000000     0x6000     0xffff                                C:\WINDOWS\system32\wscntfy.exe
0x7c900000    0xb0000     0xffff
0x7c800000    0xf4000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x77d40000    0x90000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77f10000    0x46000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x7c9c0000   0x814000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x77dd0000    0x9b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x91000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77f60000    0x76000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000   0x102000        0x2                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.
2600.2180_x-ww_a84f1ff9\comctl32.dll
0x20000000    0x2c5000        0x1                               C:\WINDOWS\system32\xpsp2res.dll
0x5ad70000    0x38000        0x2                                C:\WINDOWS\system32\uxtheme.dll
```

10. Użycie polecenia dlldump

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 dlldump -D ~/Desktop/dll_dump/

Volatility Foundation Volatility Framework 2.6.1
Process(V) Name                 Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0xff2ab020 smss.exe             0x048580000 smss.exe             Error: DllBase is paged
0xff2ab020 smss.exe             0x07c900000                      Error: DllBase is paged
```

Tak udało się odzyskać

```
dll
0x80fdc368 logon.scr            0x077f60000 SHLWAPI.dll          OK: module.124.113f368.77f60000
dll
```

11. Wyświetlenie otwartych powiązań „uchwytów” w procesie o PID 1668.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 handles -p 1668 -t Process
Volatility Foundation Volatility Framework 2.6.1
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xff125020   1668      0x378   0x1f0fff Process          cmd.exe(1136)
```

a) Do jakiego procesu należy wskazany PID (1668)?
Proces o PID 1168 należy do procesu cmd.exe.

b) Z jakim procesem wskazany PID (1668) posiada aktywny „uchwyt”?

Proces o PID 1668 (cmd.exe) posiada aktywny "uchwyt" (handle) z procesem o PID 1136, czyli z procesem cmd.exe.

c) Podaj PID odnalezionego aktywnego powiązanego procesu.
PID odnalezionego aktywnego powiązanego procesu to 1136.

12. Wskaźnik (S-1-5-32-544) należy do uprawnień administratora.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 getsids -p 1668
Volatility Foundation Volatility Framework 2.6.1
vmtoolsd.exe (1668): S-1-5-18 (Local System)
vmtoolsd.exe (1668): S-1-5-32-544 (Administrators)
vmtoolsd.exe (1668): S-1-1-0 (Everyone)
vmtoolsd.exe (1668): S-1-5-11 (Authenticated Users)
```

13. Odpowiedzi na pytania

```
C:\WINDOWS\system32\SAMLIB.dll
  File version     : 5.1.2600.2180
  Product version  : 5.1.2600.2180
  Flags            :
  OS               : Windows NT
  File Type        : Dynamic Link Library
  File Date        :
  CompanyName : Microsoft Corporation
  FileDescription : SAM Library DLL
  FileVersion : 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
  InternalName : SAMLib.DLL
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : SAMLib.DLL
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 5.1.2600.2180
```

a) Jaką wersje posiada plik:
C:\WINDOWS\system32\SAMLIB.dll? Wersja to: 5.1.2600.2180

b) OS to Windows NT

```
C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
  File version     : 7.17.512.1
  Product version  : 7.17.512.1
  Flags            :
  OS               : Windows NT
  File Type        : Application
  File Date        :
  CompanyName : ThinPrint AG
  FileDescription : TPAutoConnect User Agent
  FileVersion : 7,17,512,1
  InternalName : TPAutoConnect
  LegalCopyright : Copyright (c) 1999-2009 ThinPrint AG
  OriginalFilename : TPAutoConnect.exe
  ProductName : TPAutoConnect
  ProductVersion : 7,17,512,1
```

c) Wersja to: 7.17.512.1

d) LegalCopyright to: Copyright (c) 1999-2009 ThinPrint AG

14. Wykorzystanie wtyczki odpowiedzialnej za przeglądarkę internetową IE i odpowiedzenie na pytania:

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 iehistory
Volatility Foundation Volatility Framework 2.6.1
```

a) PID to 2044

b) O której została uruchomiona przeglądarka?

```
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Process: 1724 explorer.exe
Cache type "DEST" at 0x1387cd
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:26 UTC+0000
URL: Administrator@http://www.msn.com
Title: MSN.com
```

c) Czy została wyświetlona strona www.yahoo.com? Nie, przedstawia to poniższy screen.

d) Czy została wyświetlona strona www.bing.com? Tak, przedstawia to poniższy screen.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 iehistory | grep -i bing
Volatility Foundation Volatility Framework 2.6.1
Location: http://www.bing.com/partner/primedns.gif

┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 iehistory | grep -i yahoo
Volatility Foundation Volatility Framework 2.6.1
```

15. Wyeksportowanie procesu pod nazwę wuauclt.exe

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ python2 vol.py -f ~/Desktop/memory3.vmem --profile=WinXPSP3x86 procdump -p 468 -D ~/Desktop/Virus/
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x80f94588 0x00400000 wuauclt.exe          OK: executable.468.exe
```

Policzenie hash.

```
┌──(kali㉿kali)-[~/Downloads/volatility-master]
└─$ cd ~/Desktop/Virus

┌──(kali㉿kali)-[~/Desktop/Virus]
└─$ ll
total 112
-rw-r--r-- 1 kali kali 111104 Dec  7 15:02 executable.468.exe

┌──(kali㉿kali)-[~/Desktop/Virus]
└─$ md5sum executable.468.exe
21c183cdabccc7675b50258313812bc7  executable.468.exe

┌──(kali㉿kali)-[~/Desktop/Virus]
└─$
```

Analiza przy pomocy narzędzia VirusTotal wykazała, że plik exe to trojan