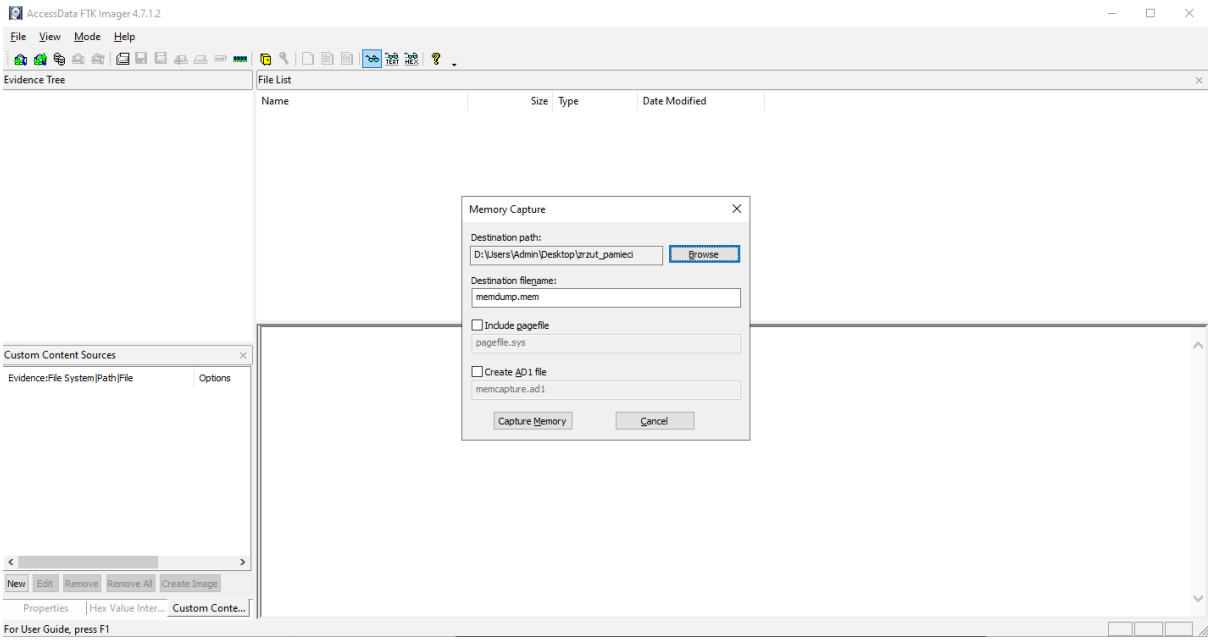
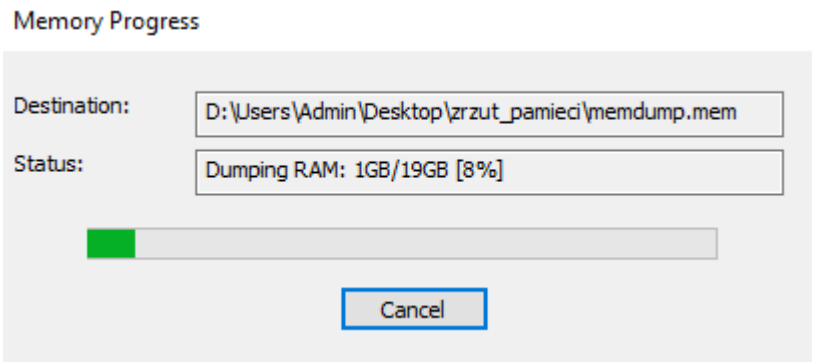
Szymon Kozioł

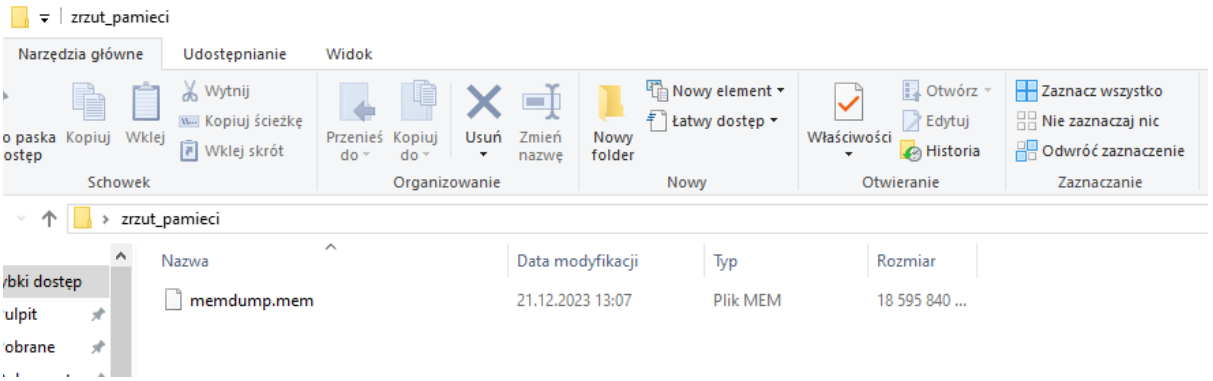
ZADANIE 1:

Wykonanie zrzutu:

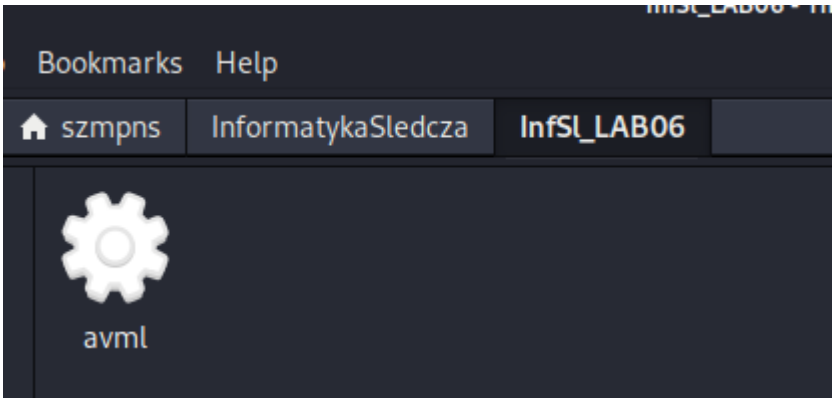




Zrzut znajduje się w docelowym folderze:



ZADANIE 2:




```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06]
└─$ chmod 755 avml
```

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06]
└─$ sudo ./avml kali_mem.dmp
[sudo] password for szmpns:
```

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06]
└─$ sudo strings kali_mem.dmp
EMiL
1uji
DL ;
zacR
-`C`
TrH`
<P0'
-b7vT
+ovZf,f{
jh~uT
-TzG
```

Bardzo trudno jest cokolwiek wyczytać, wyświetlając zawartość w taki sposób.

Wykorzystując komendy systemowe grep + strings jest zdecydowanie łatwiej i szybciej:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06]
└─$ sudo strings kali_mem.dmp| grep wikipedia
english_wikipedia.txt
# see http://en.wikipedia.org/wiki/GUID_Partition_Table#Partition_type_GUIDs
Homepage: https://en.wikipedia.org/wiki/Tnftp
Homepage: https://en.wikipedia.org/wiki/Tnftp
    * From https://en.wikipedia.org/wiki/IEEE_754-1985#Comparing_floating-point_
numbers:
    * From https://en.wikipedia.org/wiki/IEEE_754-1985#Comparing_floating-point_
numbers:
The following license, based on the MIT license (http://en.wikipedia.org/wiki/MI
T_License), applies to the OpenType Layout logic for Biblical Hebrew
```

Znalazłem trochę informacji o stronie, którą wywołałem. Oto jedna z wielu:

```
https://pl.wikipedia.org/wiki/Kokos_w%C5%82a%C5%9Bciwy
wikipedia.org
```

I gdy podałem nazwę pliku .jpg:

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06]
└─$ sudo strings kali_mem.dmp | grep sherry-christian-8Myh76_3M2U-unsplash
file:///home/szmpns/Downloads/sherry-christian-8Myh76_3M2U-unsplash.jpg
er" SCREEN="0" BIN="ristretto" ICON="org.xfce.ristretto" DESCRIPTION="Opening\ s
herry-christian-8Myh76_3M2U-unsplash.jpg" APPLICATION_ID="/usr/share/application
s/org.xfce.ristretto.desktop"
sherry-christian-8Myh76_3M2U-unsplash.jpg - Image Viewer [2/2]
nloads/sherry-christian-8Myh76_3M2U-unsplash.jpg
sherry-christian-8Myh76_3M2U-unsplash.jpg - Image Viewer [2/2]
sherry-christian-8Myh76_3M2U-unsplash.jpg - Image Viewer [2/2]
file:///home/szmpns/Downloads/sherry-christian-8Myh76_3M2U-unsplash.jpg
/home/szmpns/Downloads/sherry-christian-8Myh76_3M2U-unsplash.jpg
sherry-christian-8Myh76_3M2U-unsplash.jpg
```

ZADANIE 3:

5)

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/szmpns/InformatykaSledcza/InfSl_LAB06/m
emory3.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
```

a)
Sugerowane profile:
WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)

b)

Adres KDBG (Kernel Debugger Block) jest wykorzystywany w analizie dumpów pamięci do znalezienia struktur jądra systemu operacyjnego. KDBG zawiera ważne informacje diagnostyczne, takie jak adresy bazowe tablic systemowych, procesów, deskryptorów i inne elementy jądra. Jest to struktura kluczowa w analizie pamięci, ponieważ umożliwia identyfikację ważnych elementów jądra systemu.

c)

DTB (Directory Table Base) służy do translacji wirtualnych adresów pamięci na fizyczne adresy w systemie z użyciem mechanizmu mapowania stron. W przypadku, gdy procesor próbuje uzyskać dostęp do określonego wirtualnego adresu pamięci, DTB pomaga w translacji tego adresu na odpowiadający mu fizyczny adres w pamięci RAM.

d)

Dane zawarte w KPCR (Kernel Processor Control Region) zawierają informacje specyficzne dla procesora i są związane z zarządzaniem i kontrolą pracy rdzenia procesora w kontekście jądra systemu operacyjnego. KPCR przechowuje informacje o stanach rejestrów procesora, priorytetach, obsłudze przerwań, identyfikatorach procesorów i innych istotnych informacjach, które są istotne dla zarządzania procesorem w systemie. Jest to struktura kluczowa dla kontroli funkcji jądra systemu na poziomie procesora.

6)

```
python2 vol.py -f ~/InformatykaSledcza/InfSl_LAB06/memory3.vmem --profile=WinXPSP3x86 pslist
```

```
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
0xff247020 services.exe            676    632     16      269      0      0 2010-08-11 06:06:24
UTC+0000
0xff255020 lsass.exe               688    632     19      344      0      0 2010-08-11 06:06:24
UTC+0000
0xff218230 vmacthlp.exe            844    676      1       24      0      0 2010-08-11 06:06:24
UTC+0000
0x80ff88d8 svchost.exe             856    676     17      199      0      0 2010-08-11 06:06:24
UTC+0000
0xff217560 svchost.exe             936    676     10      272      0      0 2010-08-11 06:06:24
UTC+0000
0x80fbf910 svchost.exe            1028    676     71     1341      0      0 2010-08-11 06:06:24
UTC+0000
0xff22d558 svchost.exe            1088    676      5       80      0      0 2010-08-11 06:06:25
UTC+0000
0xff203b80 svchost.exe            1148    676     14      208      0      0 2010-08-11 06:06:26
UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     13      135      0      0 2010-08-11 06:06:26
UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      221      0      0 2010-08-11 06:06:35
UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      4      100      0      0 2010-08-11 06:06:38
UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      100      0      0 2010-08-11 06:06:39
UTC+0000
0xff25a7e0 alg.exe                 216    676      6      105      0      0 2010-08-11 06:06:39
UTC+0000
0xff364310 wscntfy.exe             888   1028      1       27      0      0 2010-08-11 06:06:49
UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       61      0      0 2010-08-11 06:06:52
UTC+0000
0xff3865d0 explorer.exe           1724   1708     12      341      0      0 2010-08-11 06:09:29
UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       49      0      0 2010-08-11 06:09:31
UTC+0000
0xff374980 VMwareUser.exe          452   1724      6      189      0      0 2010-08-11 06:09:32
UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      134      0      0 2010-08-11 06:09:37
UTC+0000
0xff3ad1a8 IEXPLORE.EXE           2044   1724     10      366      0      0 2010-08-15 18:11:17
UTC+0000
0x80fdc368 logon.scr               124    632      1       15      0      0 2010-08-15 18:21:28
UTC+0000
0xff125020 cmd.exe                1136   1668      0 --------      0      0 2010-08-15 18:24:00
UTC+0000   2010-08-15 18:24:00 UTC+0000
```

a. Informacje zawarte w poszczególnych kolumnach:

- Offset(V): Jest to wirtualny offset, który określa miejsce w pamięci, w którym dany proces znajduje się. Znak (V) oznacza, że wartość ta jest wirtualna.
- Name: Nazwa procesu.
- PID: ID procesu.
- PPID: ID procesu nadrzędnego (rodzica).
- Thds: Liczba wątków (threads) działających w procesie.
- Hnds: Liczba uchwytników (handles) używanych przez proces.
- Sess: ID sesji, do której proces należy.
- Wow64: Informacja o obsłudze 32-bitowych aplikacji na 64-bitowym systemie.
- Start: Data i czas uruchomienia procesu.
- Exit: Data i czas zakończenia procesu (jeśli jest zakończony).

b. Znacznik (V) w rubryce Offset:

Znak (V) w kolumnie Offset oznacza, że wartość jest wirtualnym adresem, a nie fizycznym. Informuje nas o tym, że wartość jest adresem pamięci wirtualnej, co jest typowe dla procesów działających w systemie operacyjnym.

c. Który z niżej opisanych procesów został zakończony i kiedy?

Proces o nazwie `cmd.exe` został zakończony. Data i czas zakończenia to `2010-08-15 18:24:00 UTC+0000`.

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

Procesy "System" i "smss.exe" nie posiadają informacji w kolumnie Sess, ponieważ nie są one przypisane do konkretnej sesji. Są one procesami systemowymi, które działają na bardzo wczesnym etapie uruchomienia systemu operacyjnego i nie są przypisane do konkretnych sesji użytkownika.

e. Który numer procesu należy do VMwareUser.exe?

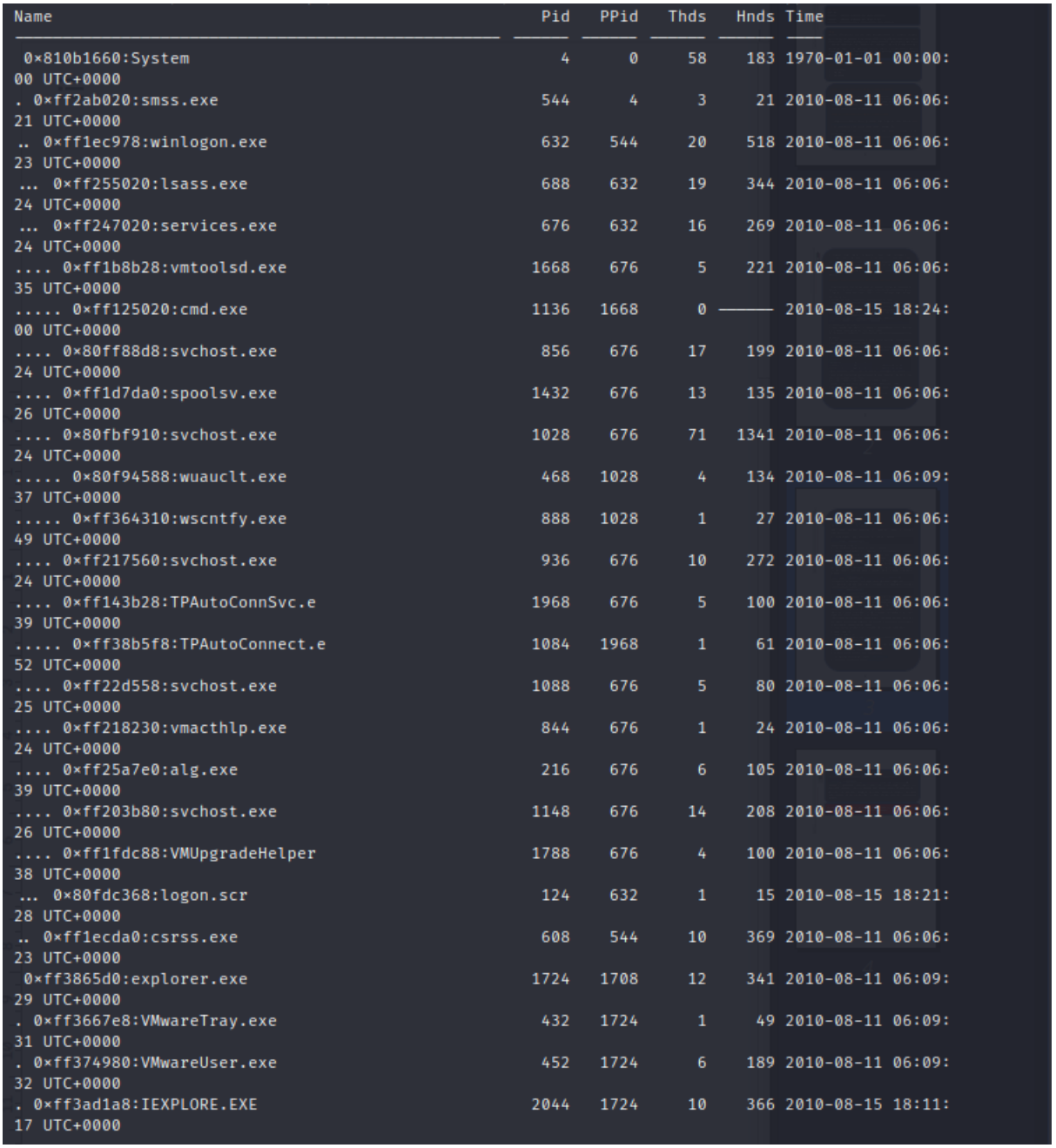
Numer procesu `VMwareUser.exe` to `452`.

7)

Wskaźnik `-P` w poleceniu `pslist` dla Volatility służy do wyświetlania procesów w formacie "precise mode" (tryb precyzyjny), co oznacza bardziej szczegółowe informacje o procesach. Porównując wynik z użyciem i bez użycia `-P`, możemy zauważyć, że tryb precyzyjny dostarcza dodatkowych danych w kolumnie Offset(P).

Zmianie uległa wartość offset. Znacznik -P ustawia adres fizyczny procesu. Jego brak ustawia adres logiczny.

8)



```
Name                                          Pid   PPid   Thds   Hnds Time
---------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                              4      0     58    183 1970-01-01 00:00:
00 UTC+0000
. 0xff2ab020:smss.exe                         544      4      3     21 2010-08-11 06:06:
21 UTC+0000
.. 0xff1ec978:winlogon.exe                    632    544     20    518 2010-08-11 06:06:
23 UTC+0000
... 0xff255020:lsass.exe                      688    632     19    344 2010-08-11 06:06:
24 UTC+0000
... 0xff247020:services.exe                   676    632     16    269 2010-08-11 06:06:
24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                 1668    676      5    221 2010-08-11 06:06:
35 UTC+0000
..... 0xff125020:cmd.exe                     1136   1668      0 ------ 2010-08-15 18:24:
00 UTC+0000
.... 0x80ff88d8:svchost.exe                   856    676     17    199 2010-08-11 06:06:
24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                  1432    676     13    135 2010-08-11 06:06:
26 UTC+0000
.... 0x80fbf910:svchost.exe                  1028    676     71   1341 2010-08-11 06:06:
24 UTC+0000
..... 0x80f94588:wuauclt.exe                  468   1028      4    134 2010-08-11 06:09:
37 UTC+0000
..... 0xff364310:wscntfy.exe                  888   1028      1     27 2010-08-11 06:06:
49 UTC+0000
.... 0xff217560:svchost.exe                   936    676     10    272 2010-08-11 06:06:
24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e              1968    676      5    100 2010-08-11 06:06:
39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e             1084   1968      1     61 2010-08-11 06:06:
52 UTC+0000
.... 0xff22d558:svchost.exe                  1088    676      5     80 2010-08-11 06:06:
25 UTC+0000
.... 0xff218230:vmacthlp.exe                  844    676      1     24 2010-08-11 06:06:
24 UTC+0000
.... 0xff25a7e0:alg.exe                       216    676      6    105 2010-08-11 06:06:
39 UTC+0000
.... 0xff203b80:svchost.exe                  1148    676     14    208 2010-08-11 06:06:
26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper              1788    676      4    100 2010-08-11 06:06:
38 UTC+0000
... 0x80fdc368:logon.scr                      124    632      1     15 2010-08-15 18:21:
28 UTC+0000
.. 0xff1ecda0:csrss.exe                       608    544     10    369 2010-08-11 06:06:
23 UTC+0000
 0xff3865d0:explorer.exe                     1724   1708     12    341 2010-08-11 06:09:
29 UTC+0000
. 0xff3667e8:VMwareTray.exe                   432   1724      1     49 2010-08-11 06:09:
31 UTC+0000
. 0xff374980:VMwareUser.exe                   452   1724      6    189 2010-08-11 06:09:
32 UTC+0000
. 0xff3ad1a8:IEXPLORE.EXE                    2044   1724     10    366 2010-08-15 18:11:
17 UTC+0000
```

a)

Wcięcia i kropki są używane do reprezentacji hierarchii procesów. Każdy kolejny poziom wcięcia reprezentuje zależność hierarchiczną, gdzie wcięcia są używane do wizualnego przedstawienia struktury drzewa procesów. Im większe zagłębienie, tym bardziej zagnieżdżony proces.

b)

W prezentowanych tabelach nie ma wyświetlonej nazwy procesu. Wartości są reprezentowane jako identyfikatory hexadecymalne.

c)

Procesem nadrzędnym dla `smss.exe` jest `System`.

d)

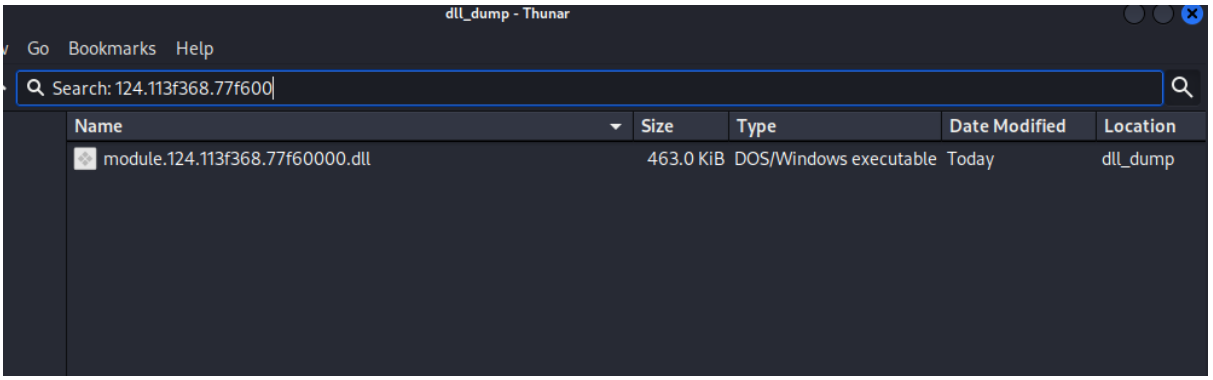
Proces `smss.exe` (Session Manager Subsystem) jest jednym z pierwszych procesów uruchamianych w systemie Windows. Jest odpowiedzialny za zarządzanie sesjami systemowymi, kontrolę procesu logowania (login/logout), tworzenie środowiska dla nowych sesji użytkownika oraz inicjalizację systemu.

9)

```
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
```

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06/volatility]
└─$ python2 vol.py -f ~/InformatykaSledcza/InfSl_LAB06/memory3.vmem --profile=WinXPSP3x86 -p 888
dlllist
```

10)



Udało się.

11)

Offset(V)	Pid	Handle	Access	Type	Details
0×ff125020	1668	0×378	0×1f0fff	Process	cmd.exe(1136)

a)

Proces o PID 1668 należy do `cmd.exe`.

b)

Posiada aktywny „uchwyt” z procesem o PID 1136, który również jest `cmd.exe`.

c)

PID procesu powiązanego z procesem o PID 1668 to 1136.

12)

Wskaźnik należy do uprawnień administratora.

13)

```
┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06/volatility]
└─$ python2 vol.py -f ~/InformatykaSledcza/InfSl_LAB06/memory3.vmem --profile=WinXPSP3x86 verinfo
```

Wycinek z bardzo długiego outputu:

```
  FileDescription : Internet Explorer Peer Objects
  FileVersion : 6.00.2900.2833 (xpsp_sp2_gdr.060124-1515)
  InternalName : iepeers.dll
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : iepeers.dll
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 6.00.2900.2833
C:\WINDOWS\system32\WINSPOOL.DRV
  File version    : 5.1.2600.2180
  Product version : 5.1.2600.2180
  Flags           :
  OS              : Windows NT
  File Type       : Driver
  File Date       :
  CompanyName : Microsoft Corporation
  FileDescription : Windows Spooler Driver
  FileVersion : 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
  InternalName : winspool.drv
  LegalCopyright : \xa9 Microsoft Corporation. All rights reserved.
  OriginalFilename : winspool.drv
  ProductName : Microsoft\xae Windows\xae Operating System
  ProductVersion : 5.1.2600.2180
C:\WINDOWS\system32\mshtmled.dll
  File version    : 6.0.2900.2180
  Product version : 6.0.2900.2180
```

a) 5.1.2600.2180
b) Windows NT
c) 7.17.512.1
d) Copyright © 1999-2009 ThinPrint AG

14)

```
**************************************************
Process: 2044 IEXPLORE.EXE
Cache type "DEST" at 0x24bdf45
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
**************************************************
Process: 2044 IEXPLORE.EXE
Cache type "URL " at 0x3715000
Record length: 0x100
Location: :2010081520100816: Administrator@http://www.msn.com
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:24 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0
**************************************************
Process: 2044 IEXPLORE.EXE
Cache type "URL " at 0x3715100
Record length: 0x100
Location: :2010081520100816: Administrator@:Host: www.msn.com
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:24 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0

┌──(szmpns㉿kali)-[~/InformatykaSledcza/InfSl_LAB06/volatility]
└─$ python2 vol.py -f ~/InformatykaSledcza/InfSl_LAB06/memory3.vmem --profile=WinXPSP3x86 iehistory
```

wycinek długiego outputu i komenda

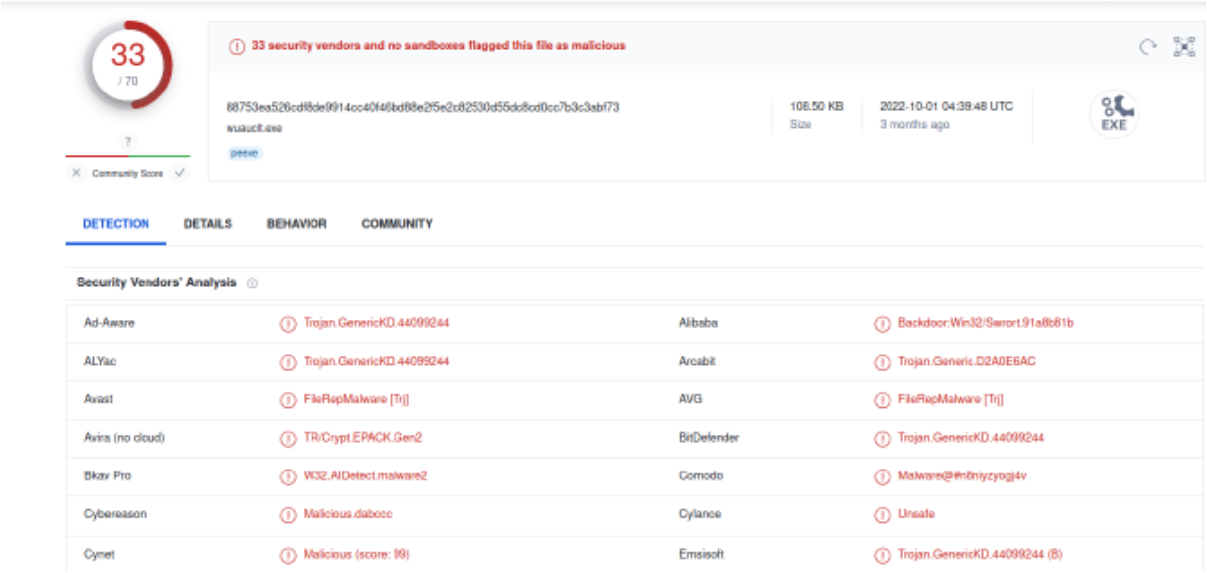
a) 2044
b) 2010-08-15 14:11:24
c) nie
d) nie

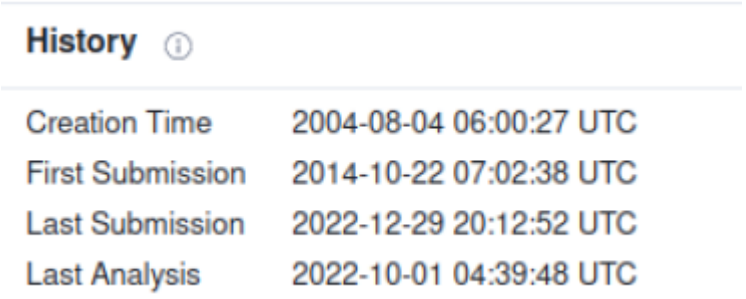
15)

Suma kontrolna:

21c183cdabccc7675b50258313812bc7

Plik zawierał szkodliwe oprogramowanie. Zawierał backdoory i trojany. PLik jest spreparowany pod system operacyjny Windows.





Plik powstał 04.06.2004
W swojej historii posiadał wiele różnych nazw