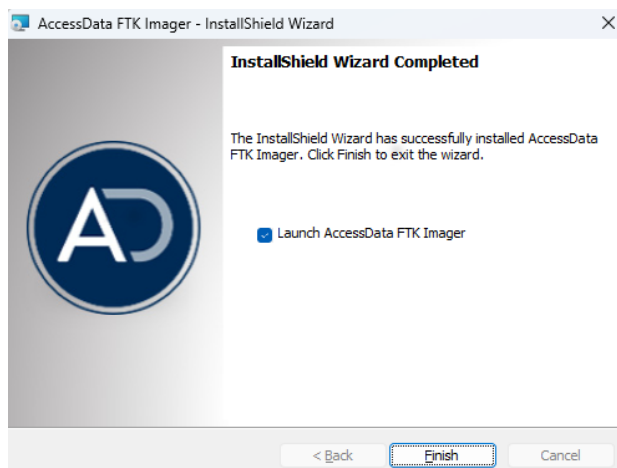


Informatyka śledcza Laboratorium nr 5

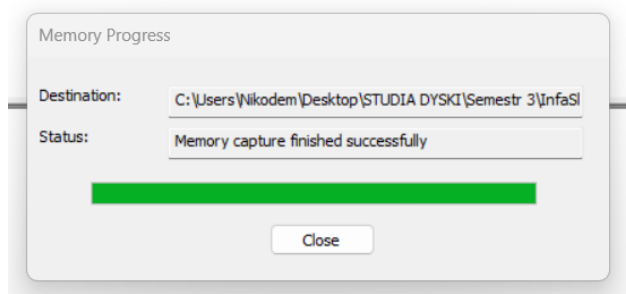
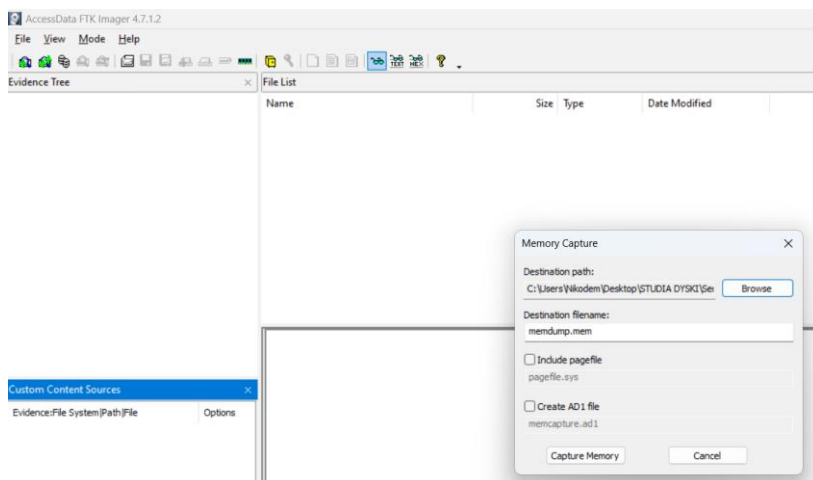
Raport – Nikodem Jakubowski


Zadanie 1 – Tworzenie zrzutu pamięci z systemu Windows.

Pobieram i otwieram FTK Imager.



Tworzę dumpa.



Nazwa	Data modyfikacji	Typ	Rozmiar
 memdump.mem	07.12.2023 15:18	Plik MEM	17 026 304 ...

Zadanie 2 – Tworzenie zrzutu pamięci z systemu Linux

Avml już mam, bo kiedyś korzystałem.

```
(user@kali)-[~]
$ cd Desktop

(user@kali)-[~/Desktop]
$ ll
total 2103164
-rwxr-xr-x 1 user user 6609568 Dec 5 18:11 avml
```

Tworzę dumpa.

```
(user@kali)-[~/Desktop]
$ sudo ./avml nazwa.dmp
```

Bez użycia grepa jest bardzo dużo dziwnych danych i ciężko jest znaleźć coś konkretnego.

```
t",R
q+$?
<2'9
<3%2
5I4~!
SY8?n]
_Ql!
+[q]
Y\nea
I("e
EDP!n4c
$/Bs
9eAQZl
pW4
smAe5
NxT5
.9*c
px2
e$C%
tfsN
knL
Slv*
"2%rB.8
iL`X
+htO
Mk(J
--More--
```

Znalezienie „pudełka” i innych artefaktów przy pomocy grep.

```
(user@kali)-[~/Desktop]
$ sudo strings nazwa.dmp | grep -i pudelek | more
http://pudelek.com/
https://www.google.com/search?client=firefox-b-e&q=pudelek
https://www.google.com/search?client=firefox-b-e&q=pudelek
https://www.google.com/search?client=firefox-b-e&q=pudelek
pudelek
```

```
(user@kali)-[~/Desktop]
$ sudo strings nazwa.dmp | grep -i Logo | more
)0}DNLogo0);QuitGetMode() = "boot"mov --fuPdur!); < 0.1/9ve ==8
cc-logo-diners.svg
cc-logo-discover.png
cc-logo-mastercard.svg
cc-logo-unionpay.svg
https://iet.agh.edu.pl/wp-content/uploads/2021/05/Logo-WIET-2021.png
https://iet.agh.edu.pl/wp-content/uploads/2021/05/Logo-WIET-2021.png
distributor-logo-opensuse.svg
Logo-WIET-2021.png
```

Zadanie 3 – Analiza pamięci przy wykorzystaniu programu Volatility.

Sklonowałem z github pakiet volatility.

```
(user@kali)~[~/Desktop]
$ git clone https://github.com/volatilityfoundation/volatility.git
Cloning into 'volatility' ...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.10 MiB | 2.76 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
```

Udało mi się zainstalować volatility wraz ze wszystkimi dodatkami, tak że jest dostępne w terminalu bash przy pomocy komendy vol.py.

```
(user@kali)~[~/Desktop]
$ vol.py -h | more
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/user/.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/user/.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)
```

Badam profil obrazu.

```
(user@kali)~[~/Desktop]
$ vol.py -f 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 WinXPSP2x86)
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/user/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 : 0xffdff000L
      Image date and time : 2010-08-15 18:24:00 UTC+0000
      Image local date and time : 2010-08-15 14:24:00 -0400
```

Jakie sugerowane profile są aktualnie podpowiadane przez program?

Program sugeruje dwa profile: WinXPSP2x86 i WinXPSP3x86.

Do czego wykorzystywany jest adres KDBG?

Adres KDBG (od Kernel Debugger) jest wykorzystywany w debugowaniu jądra systemu operacyjnego.

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

DTB (Directory Table Base) jest używany do translacji wirtualnego adresu na fizyczny adres w kontekście obszaru pamięci jądra systemu operacyjnego. W tym przypadku wartość DTB wynosi 0x319000L.

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

Dane zawarte w KPCR dla CPU 0 są określone jako 0xffdff000L. KPCR może dostarczać informacji o stanie procesora.

Wyświetlanie listy procesów.

```
(user@kali)~[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 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	
0xff1ecd00	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	wsentfy.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	wuauc.lt.exe	468	1028	4	134	0	0	2010-08-11 06:09:37 UTC+0000	
0xff3ad1a8	IEXPLOR.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

Jakie informacje zawierają poszczególne kolumny: Offset(V), PID, PPID, Thds, Hnds, Sess, Wow64, Start i Exit?

Offset(V): Adres wirtualny, na którym znajduje się informacja o danym procesie.

PID: Numer identyfikacyjny procesu (Process ID).

PPID: Numer identyfikacyjny procesu nadrzędnego (Parent Process ID).

Thds: Liczba wątków procesu (od threads).

Hnds: Liczba uchwytów (handles), czyli odwołań do zasobów systemowych, które proces może używać.

Sess: Numer sesji, do której proces należy.

Wow64: Wartość 1 wskazuje, że proces jest uruchomiony w trybie WoW64 (Windows 32-bit on Windows 64-bit), a 0 oznacza brak trybu WoW64.

Start: Data i czas rozpoczęcia procesu.

Exit: Data i czas zakończenia procesu (jeśli został zakończony).

O czym świadczy znacznik (V) w rubryce Offset?

Znacznik (V) w rubryce Offset oznacza, że adres jest w formie wirtualnej (virtual).

Który z niżej opisanych procesów został zakończony i kiedy?

Proces o numerze 1136 (cmd.exe) został zakończony. Zakończenie nastąpiło dnia 2010-08-15 o godzinie 18:24:00 UTC+0000.

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

Procesy "System" i "smss.exe" nie posiadają informacji w rubryce "Sess", ponieważ są to procesy systemowe, a nie procesy użytkownika.

Który numer procesu należy do VMwareUser.exe?

Proces o nazwie "VMwareUser.exe" ma numer identyfikacyjny PID równy 452.

Wskaźnik -P pokazuje offset w formie fizycznej.

```
(user@kali) ~/Desktop
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 pslist -P
Volatility Foundation Volatility Framework 2.6.1
```

Offset(P)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x01214660	System	4	0	58	183		0		
0x05471020	smss.exe	544	4	3	21		0	2010-08-11 06:06:21 UTC+0000	
0x066f0da0	csrss.exe	608	544	10	369	0	0	2010-08-11 06:06:23 UTC+0000	
0x066f0978	winlogon.exe	632	544	20	518	0	0	2010-08-11 06:06:23 UTC+0000	
0x06015020	services.exe	676	632	16	269	0	0	2010-08-11 06:06:24 UTC+0000	
0x05f47020	lsass.exe	688	632	19	344	0	0	2010-08-11 06:06:24 UTC+0000	
0x06384230	vmacthlp.exe	844	676	1	24	0	0	2010-08-11 06:06:24 UTC+0000	
0x0115b8d8	svchost.exe	856	676	17	199	0	0	2010-08-11 06:06:24 UTC+0000	
0x063c5560	svchost.exe	936	676	10	272	0	0	2010-08-11 06:06:24 UTC+0000	
0x01122910	svchost.exe	1028	676	71	1341	0	0	2010-08-11 06:06:24 UTC+0000	
0x061ef558	svchost.exe	1088	676	5	80	0	0	2010-08-11 06:06:25 UTC+0000	
0x06499b80	svchost.exe	1148	676	14	208	0	0	2010-08-11 06:06:26 UTC+0000	
0x06945da0	spoolsv.exe	1432	676	13	135	0	0	2010-08-11 06:06:26 UTC+0000	
0x069d5b28	vmtoolsd.exe	1668	676	5	221	0	0	2010-08-11 06:06:35 UTC+0000	
0x0655fc88	VMUpgradeHelper	1788	676	4	100	0	0	2010-08-11 06:06:38 UTC+0000	
0x0211ab28	TPAutoConnSvc.e	1968	676	5	100	0	0	2010-08-11 06:06:39 UTC+0000	
0x05f027e0	alg.exe	216	676	6	105	0	0	2010-08-11 06:06:39 UTC+0000	
0x04c2b310	wscntfy.exe	888	1028	1	27	0	0	2010-08-11 06:06:49 UTC+0000	
0x049c15f8	TPAutoConnect.e	1084	1968	1	61	0	0	2010-08-11 06:06:52 UTC+0000	
0x04a065d0	explorer.exe	1724	1708	12	341	0	0	2010-08-11 06:09:29 UTC+0000	
0x04be97e8	VMwareTray.exe	432	1724	1	49	0	0	2010-08-11 06:09:31 UTC+0000	
0x04b5a980	VMwareUser.exe	452	1724	6	189	0	0	2010-08-11 06:09:32 UTC+0000	
0x010f7588	wuauclt.exe	468	1028	4	134	0	0	2010-08-11 06:09:37 UTC+0000	
0x0485d1a8	IEXPLORE.EXE	2044	1724	10	366	0	0	2010-08-15 18:11:17 UTC+0000	
0x0113f368	logon.scr	124	632	1	15	0	0	2010-08-15 18:21:28 UTC+0000	
0x02e47020	cmd.exe	1136	1668	0		0	0	2010-08-15 18:24:00 UTC+0000	2010-08-15 18:24:00 UTC+0000

Przed offset(v) == 0xff374980,po offset(p) 0x04b5a980.

Wyświetlam drzewo procesów.

```
(user@kali) ~/Desktop
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
```

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

Co oznaczają wyświetlone wcięcia i kropki?

Wcięcia i kropki w wyświetlonym drzewie procesów (pstree) są używane do reprezentacji hierarchii procesów.

Jakiego identyfikatora nie znajdziemy w prezentowanych tabelach?

W prezentowanych tabelach brakuje informacji o identyfikatorze sesji (Session ID).

Procesem nadrzędnym procesu smss.exe jest...?

Procesem nadrzędnym procesu smss.exe jest proces o identyfikatorze PID równym 4, czyli proces System.

Za co odpowiedzialny jest proces smss.exe?

Proces smss.exe (Session Manager Subsystem) jest odpowiedzialny za zarządzanie sesjami logowania użytkowników w systemie Windows. Odpowiada za inicjalizację systemu, logowanie użytkowników oraz tworzenie środowiska sesji.

Wyświetlam pluginy dotyczące dll.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 -h | grep -i dll
Volatility Foundation Volatility Framework 2.6.1
dll dump          Dump DLLs from a process address space
dll list          Print list of loaded DLLs for each process
ldrmodules        Detect unlinked DLLs
```

Załadowane biblioteki dll na podstawie procesu wscntfy.exe.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 dlllist -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      0x00000000 C:\WINDOWS\system32\wscntfy.exe
0x7c900000 0x8000      0xffff      0x00000000 C:\WINDOWS\system32\kernel32.dll
0x7c800000 0xf4000     0xffff      0x00000000 C:\WINDOWS\system32\msvcrt.dll
0x77c10000 0x58000     0xffff      0x00000000 C:\WINDOWS\system32\USER32.dll
0x77d40000 0x90000     0xffff      0x00000000 C:\WINDOWS\system32\GDI32.dll
0x77f10000 0x46000     0xffff      0x00000000 C:\WINDOWS\system32\SHELL32.dll
0x7c9c0000 0x814000    0xffff      0x00000000 C:\WINDOWS\system32\ADVAPI32.dll
0x77d00000 0x9b000     0xffff      0x00000000 C:\WINDOWS\system32\RPCRT4.dll
0x77e70000 0x91000     0xffff      0x00000000 C:\WINDOWS\system32\SHLWAPI.dll
0x77f60000 0x76000     0xffff      0x00000000 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9\comctl32.dll
0x773d0000 0x102000    0x2         0x00000000 C:\WINDOWS\system32\xpsp2res.dll
0x20000000 0x2c5000    0x1         0x00000000 C:\WINDOWS\system32\uxtheme.dll
0x5ad70000 0x38000     0x2         0x00000000 C:\WINDOWS\system32\uxtheme.dll
```

Wykorzystanie polecenie dlldump zgodnie z poleceniem.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 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      csrss.exe          Error: DllBase is paged
0xff1ecda0 csrss.exe      0x04a680000      csrss.exe          Error: e_magic 6268 is not a valid DOS signature.
0xff1ecda0 csrss.exe      0x07c900000      csrss.exe          Error: DllBase is paged
0xff1ecda0 csrss.exe      0x075b40000      CSRSRV.dll         Error: DllBase is paged
0xff1ecda0 csrss.exe      0x077d40000      USER32.dll         OK: module.608.66f0da0.77d40000.dll
0xff1ecda0 csrss.exe      0x077e70000      RPCRT4.dll         Error: DllBase is paged
0xff1ecda0 csrss.exe      0x075e90000      sxs.dll            Error: DllBase is paged
0xff1ecda0 csrss.exe      0x077dd0000      ADVAPI32.dll       Error: DllBase is paged
0xff1ecda0 csrss.exe      0x075b50000      basesrv.dll        Error: DllBase is paged
0xff1ecda0 csrss.exe      0x07c800000      KERNEL32.dll       Error: DllBase is paged
0xff1ecda0 csrss.exe      0x077f10000      GDI32.dll          Error: DllBase is paged
0xff1ecda0 csrss.exe      0x075b60000      winsrv.dll         OK: module.608.66f0da0.75b60000.dll
0xff1ec978 winlogon.exe  0x001000000      winlogon.exe       OK: module.632.66f0978.1000000.dll
0xff1ec978 winlogon.exe  0x07c900000      winlogon.exe       OK: module.632.66f0978.7c900000.dll
```

Udało się znaleźć moduł: module.124.113f368.77f60000.dll.

```
(user@kali)-[~/Desktop]
$ find dll_dump/ -type f -name "module.124.113f368.77f60000.dll"
dll_dump/module.124.113f368.77f60000.dll
```

Wyświetlam powiązane uchwyt w procesie o PID 1668.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 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)
```

Do jakiego procesu należy wskazany PID (1168)?

Wskazany PID 1668 należy do procesu cmd.exe.

Z jakim procesem wskazany PID (1168) posiada aktywny „uchwyt”?

Proces o PID 1668 (cmd.exe) posiada aktywny uchwyt do procesu o identyfikatorze PID 1136.

Podaj PID odnalezionego aktywnego powiązanego procesu.

PID 1136.

Użycie getsids.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 getsids
Volatility Foundation Volatility Framework 2.6.1
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (544): S-1-5-18 (Local System)
smss.exe (544): S-1-5-32-544 (Administrators)
smss.exe (544): S-1-1-0 (Everyone)
smss.exe (544): S-1-5-11 (Authenticated Users)
csrss.exe (608): S-1-5-18 (Local System)
csrss.exe (608): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-1-0 (Everyone)
csrss.exe (608): S-1-5-11 (Authenticated Users)
```

Do jakich uprawnień należy wskaźnik (S-1-5-32-544)?

Należy do uprawnień administratorów.

Wykorzystanie funkcji verinfo. Po przeczytaniu dokumentacji zauważyłem, że trzeba użyć regexa.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 verinfo --regex "(?i)C:\\\\WINDOWS\\\\\\\\system32\\\\\\\\SAMLIB\\\\.dll"
Volatility Foundation Volatility Framework 2.6.1
WARNING : volatility.debug : NoneObject as string: Invalid offset 2090327784 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 132504 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 132544 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2090327784 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2090327784 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2090327784 for dereferencing Buffer as String
WARNING : volatility.debug : NoneObject as string: Invalid offset 2089952932 for dereferencing Buffer as String
C:\\WINDOWS\\System32\\SAMLIB.dll
```

Jaką wersję posiada plik: C:\\WINDOWS\\system32\\SAMLIB.dll?

C:\\WINDOWS\\system32\\SAMLIB.dll.

File version : 5.1.2600.2180.

Podaj jego OS.

OS : Windows NT.

Podaj wersje pliku: C:\ProgramFiles\VMware\VMware\Tools\TPAutoConnect.exe.

```
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
```

File version : 7.17.512.1.

Podaj LegalCopyright ww. pliku.

LegalCopyright : Copyright (c) 1999-2009 ThinPrint AG.

Wtyczka odpowiedzialna za przeglądarkę IE.

```
(user@kali)-[~/Desktop]
$ vol.py --info | grep -i IE
Volatility Foundation Volatility Framework 2.6.1
auditpol          - Prints out the Audit Policies from HKLM\SECURITY\Policy\PolAdtEv
iehistory         - Reconstruct Internet Explorer cache / history
```

Podaj PID procesu IEXPLORE.EXE.

PID 2044.

```
*****
Process: 2044 IEXPLORE.EXE
Cache type "URL " at 0xa95000
Record length: 0x100
Location: Visited: Administrator@http://home.microsoft.com
Last modified: 2010-08-15 18:11:19 UTC+0000
Last accessed: 2010-08-15 18:11:19 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c
```

O której została uruchomiona przeglądarka? Poniżej na zdjęciu.

```
*****
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
```

Czy została wyświetlona strona yahoo albo bing? Bing tak, yahoo nie. Było dużo msn.

```
(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 iehistory | grep -i bing
Volatility Foundation Volatility Framework 2.6.1
Location: http://www.bing.com/partner/primedns.gif

(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 iehistory | grep -i yahoo
Volatility Foundation Volatility Framework 2.6.1
```



```

*****
Process: 2044 IEXPLORE.EXE
Cache type "URL " at 0xa77400
Record length: 0x180
Location: http://www.bing.com/partner/primedns.gif
Last modified: 2007-05-30 19:42:28 UTC+0000
Last accessed: 2010-08-15 18:11:22 UTC+0000
File Offset: 0x180, Data Offset: 0x94, Data Length: 0xa4
File: primedns[1].gif
Data: HTTP/1.1 200 OK
Content-Length: 43
Content-Type: image/gif
ETag: 325472601571F31E1BF00674C368D3350000002B

~U:administrator

```

Wyeksportowanie procesu wuaucit.exe.

```

(user@kali)-[~/Desktop]
$ vol.py -f memory3.vmem --profile=WinXPSP2x86 procdump -p 468 -D ~/Desktop/Virus/
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
-----
0x80f94588 0x00400000 wuaucit.exe OK: executable.468.exe

```

Policzenie hasha.

```

(user@kali)-[~/Desktop]
$ cd Virus/

(user@kali)-[~/Desktop/Virus]
$ ll
total 112
-rw-r--r-- 1 user user 111104 Dec 7 19:51 executable.468.exe

(user@kali)-[~/Desktop/Virus]
$ md5sum executable.468.exe
21c183cdabccc7675b50258313812bc7 executable.468.exe

```

Skorzystanie z virustotal.com. Okazuje się, że to trojan.

