

Volatility

NCERT-PUBDOC-2018-3-357

Sadržaj

1	UVOD	3
2	INSTALACIJA ALATA VOLATILITY	4
3	KORIŠTENJE ALATA VOLATILITY ZA ANALIZU SLIKE MEMORIJE.....	8
3.1	IDENTIFIKACIJA SLIKE MEMORIJE	8
3.2	LISTA PROCESA	9
3.3	MEĐUSPREMNIK OPERACIJSKOG SUSTAVA.....	10
3.4	POVIJEST PREGLEDNIKA INTERNET EXPLORER.....	10
3.5	MREŽNE VEZE.....	11
3.6	REGISTAR OPERACIJSKOG SUSTAVA WINDOWS	11
3.7	DATOTEČNI SUSTAV	12
4	ZAKLJUČAK	14

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument je vlasništvo Nacionalnog CERT-a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obvezno navođenje izvora podataka. Zabranjena je bilo kakva distribucija dokumenta u elektroničkom (Web stranice i dr.) ili papirnatom obliku. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNeta, a sve sukladno zakonskim odredbama Republike Hrvatske.

1 Uvod

Sve većom uporabom tehnologije u svakodnevnom životu porasla je i primjena tehnologije u kriminalne svrhe. Tako je stvorena i potreba za računalnom forenzikom – granom informacijske sigurnosti koja se bavi prikupljanjem i analizom tragova nastalih korištenjem računala. Forenzika je potrebna i za pronalaženje tehničkih i ljudskih grešaka u informacijskom sustavu. Unutar računalne forenzike, jedno područje je i forenzika radne memorije koja se bavi prikupljanjem i analizom tragova iz radne memorije računala.

Radna memorija računala važna je iz forenzičke perspektive jer se u njoj nalaze neki tragovi koje nije moguće pronaći drugim metodama računalne forenzike, kao što je forenzika diska odnosno trajne memorije. Također, forenzika radne memorije je posebno zanimljiva kod analize događaja u kojima su tragovi namjerno prikrivani, primjerice kod napada na računalne sustave zloćudnim programima (eng. *malware*).

U posljednjem desetljeću forenzika radne memorije doživjela je veliki razvoj i privukla pažnju većeg broja istraživača i programera. Kao posljedica toga, razvijen je niz alata za forenziku radne memorije od kojih je jedan od najpoznatijih Volatility. Volatility je slobodan softver (eng. *free and open source software*) koji služi za analizu slika radne memorije računala.

Forenziku radne memorije moguće je podijeliti u dva koraka:

- **Pribavljanje (eng. *acquisition*)** – postupak snimanja sadržaja („slike“ = eng. *image*) memorije trenutno pokrenutog sustava u datoteku.
- **Analiza** – analiza snimljene slike memorije u svrhu otkrivanja forenzičkih tragova.

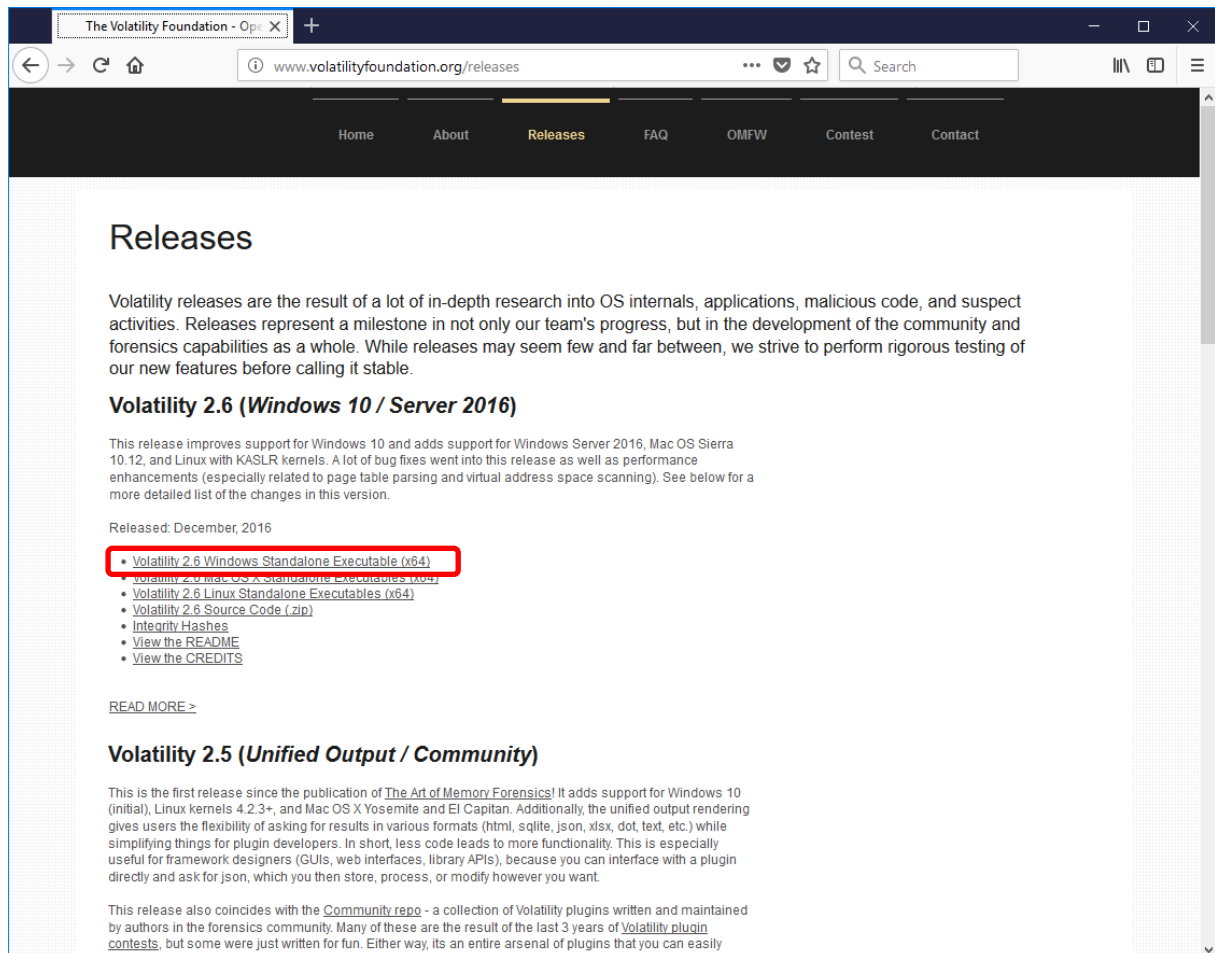
Alat Volatility namijenjen je za analizu slike radne memorije, ali ne i za njeno pribavljanje. Zato, prvo je potrebno nekako pribaviti sliku memorije, primjerice korištenjem programskih alata namijenjenih za to ili preko sklopovlja.

U nastavku dokumenta bit će opisano kako instalirati Volatility te kako ga koristiti za osnovnu analizu slike radne memorije. Pretpostavlja se da je slika radne memorije već nekako pribavljena i pohranjena u datoteku.

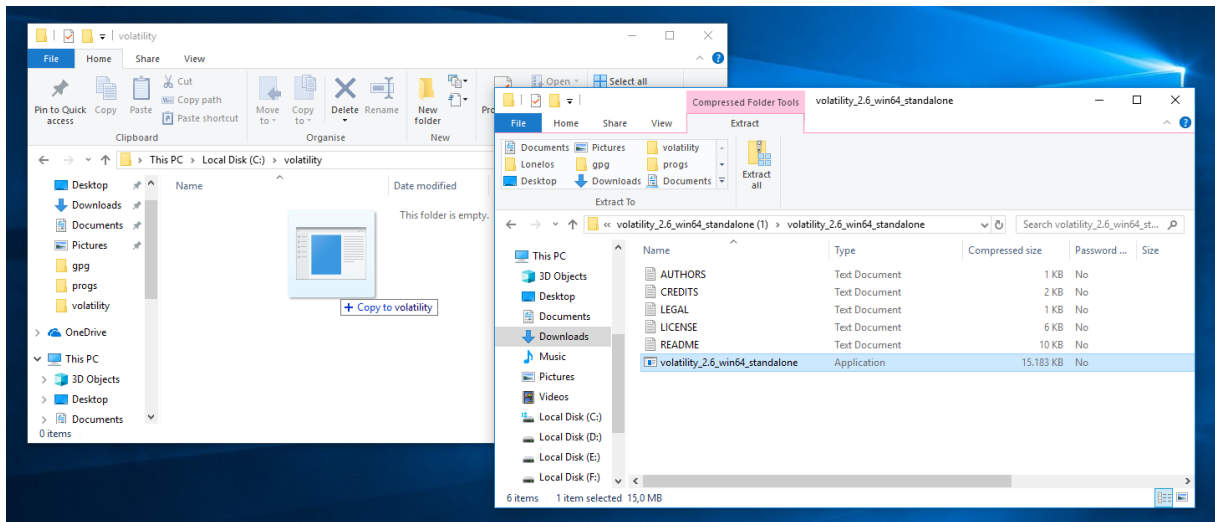
2 Instalacija alata Volatility

Volatility je dostupan za operacijske sustave Windows, Linux i macOS te načelno i za druge platforme na kojima je dostupna okolina za pokretanje Python programa. U ovom će se dokumentu instalacija i primjeri raditi za operacijski sustav Windows 10, no postupak je gotovo identičan i za druge operacijske sustave. Za operacijski sustav Windows, Volatility dolazi kao jedna izvršna datoteka te koristi se izravnim pozivanjem iz naredbenog retka (eng. *command prompt*).

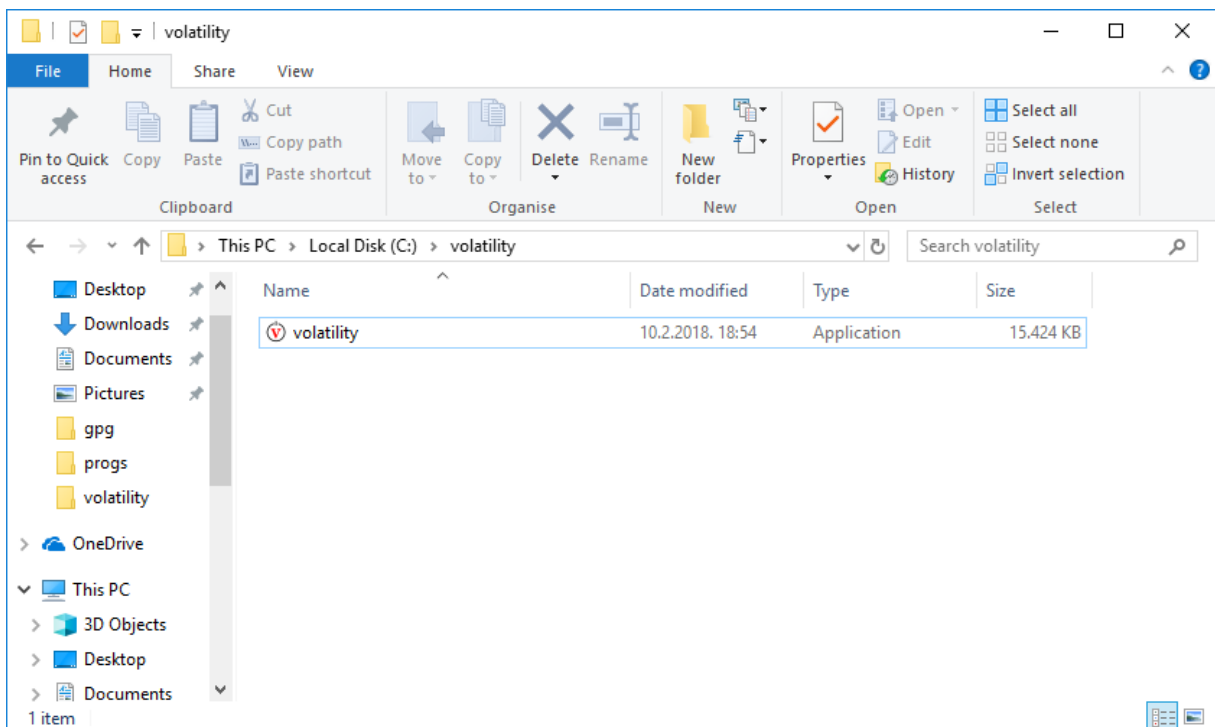
Nakon otvaranja [Web stranice](#) koja sadrži inačice alata Volatility, potrebno preuzeti Volatility pritiskom na odgovarajuću poveznicu kao što je prikazano na slici niže.



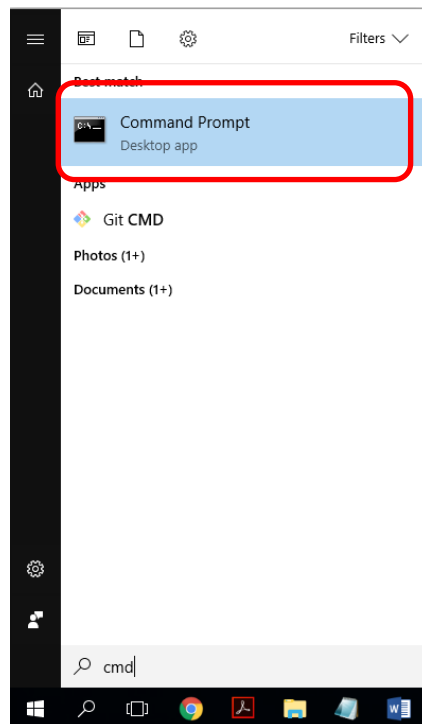
Iz arhive je potrebno izvaditi (eng. *extract*) izvršnu datoteku na disk računala. To je moguće ostvariti povlačenjem i ispuštanjem datoteke iz arhive u direktorij *C:\volatility* u upravitelju datoteka sustava Windows, kao što je prikazano na donjoj slici.



Datoteka naziva *volatility_2.6_win64_standalone.exe* preimenovana je u *volatility.exe* kako bi se olakšalo njeno pozivanje iz naredbenog retka. Na donjoj slici prikazana je izvađena i preimenovana izvršna datoteka alata Volatility u upravitelju datoteka.



Sada je potrebno otvoriti naredbeni redak pritiskom tipke s logom sustava Windows, upisivanjem riječi *cmd* te pritiskom na *Command Prompt* (označeno na donjoj slici).



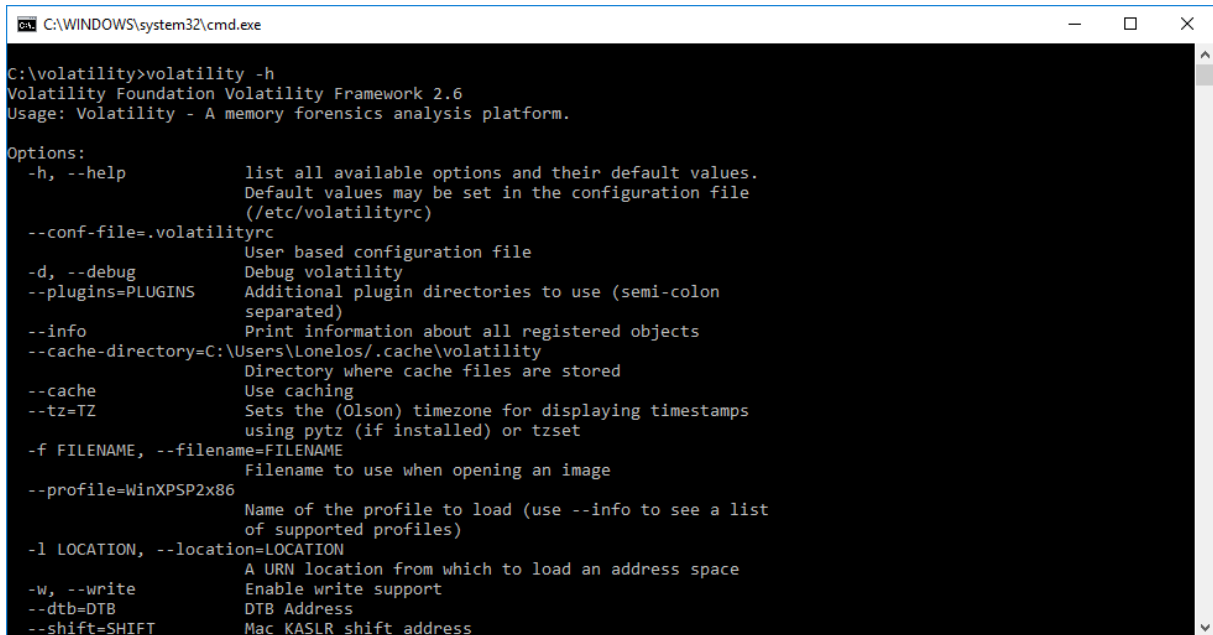
Zatim, potrebno je promijeniti radni direktorij (mapu) naredbenog retka u direktorij u kojem se nalazi Volatility, u ovom slučaju direktorij *C:\volatility*. Pozicioniranje je moguće obaviti naredbom **cd** (eng. *change directory*):

```
cd \volatility
```

A screenshot of a Windows Command Prompt window. The title bar shows the path 'C:\WINDOWS\system32\cmd.exe'. The window content displays the following text: 'Microsoft Windows [Version 10.0.16299.192]', '(c) 2017 Microsoft Corporation. All rights reserved.', 'C:\Users\Lonelos>cd \volatility', and 'C:\volatility>'. The cursor is positioned at the end of the last line.

Ispravnost rada alata Volatility može se ispitati njegovim pozivanjem s parametrom **-h** (*help*) kojim se ispisuje popis dostupnih naredbi te njihovog kratkog opisa:

```
volatility -h
```



```
C:\WINDOWS\system32\cmd.exe
C:\volatility>volatility -h
Volatility Foundation Volatility Framework 2.6
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=.volatilityrc
                    User based configuration file
-d, --debug         Debug volatility
--plugins=PLUGINS  Additional plugin directories to use (semi-colon
                    separated)
--info             Print information about all registered objects
--cache-directory=C:\Users\Lonelos\.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
```

3 Korištenje alata Volatility za analizu slike memorije

Kao što je opisano u uvodu, za analizu je najprije potrebno na neki način pribaviti sliku memorije računala. Sam postupak pribavljanja slike memorije izvan je opsega ovog dokumenta. Jednom kada je slika memorije dostupna, moguće ju je analizirati alatom Volatility.

U ovom poglavlju, korištenje alata Volatility opisano je kroz primjer analize slike memorije jednog virtualnog stroja na kojem je bio pokrenut operacijski sustav Windows 7 Service Pack 1. U narednim primjerima koristi se slika radne memorije s nazivom datoteke *win7dump.elf*. Datoteka je kopirana u direktorij *C:\volatility*, u kojem se nalazi i izvršna datoteka alata Volatility.

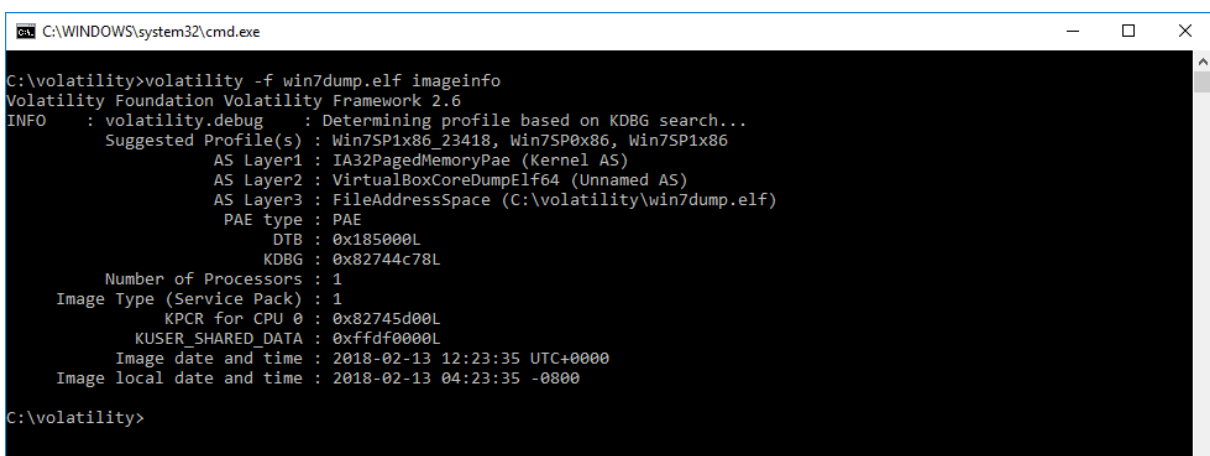
Kako bi alat Volatility znao koju sliku memorije treba analizirati, u pozivu alata iz naredbenog retka koristi se parametar **-f** iza kojeg slijedi putanja do slike memorije. U svim primjerima koristi se slika imena *win7dump.elf* koja se nalazi u istom direktoriju kao i alat Volatility, pa će zato parametar **-f win7dump.elf** biti korišten prilikom svakog poziva alata.

3.1 Identifikacija slike memorije

Za izvođenje sljedećih naredbi, potrebno je otvoriti naredbeni redak te se pozicionirati u direktorij u kojem se nalazi alat Volatility, kao što je opisano u prethodnom poglavlju.

U nekim slučajevima, nije poznato koji operacijski sustav se nalazio na računalu s kojega je snimljena slika memorije, a ta informacija potrebna je alatu Volatility kako bi ispravno radio analizu. Alat Volatility ima naredbu **imageinfo** koji služi za prepoznavanje profila tj. inačice operacijskog sustava s kojeg je snimljena slika memorije. U pozivima alata Volatility koristiti se parametar **--profile=<ime profila>** kako bi Volatility znao pronaći i interpretirati strukture u memoriji specifične za tu inačicu operacijskog sustava. Naredba za otkrivanje informacija o slici memorije je:

```
volatility -f win7dump.elf imageinfo
```



```
C:\WINDOWS\system32\cmd.exe
C:\volatility>volatility -f win7dump.elf imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
      AS Layer3 : FileAddressSpace (C:\volatility\win7dump.elf)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82744c78L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x82745d00L
      KUSER_SHARED_DATA : 0xfffff000L
      Image date and time : 2018-02-13 12:23:35 UTC+0000
      Image local date and time : 2018-02-13 04:23:35 -0800
C:\volatility>
```


U ovom primjeru, Volatility je prepoznao tri potencijalna profila operacijskih sustava, od kojih su sva tri inačice operacijskog sustava Windows 7. Kako je unaprijed poznato da je ovo slika memorije operacijskog sustava Windows 7 SP1, u nastavku će se koristiti profil **Win7SP1x86_23418**, te će sve naredbe počinjati s:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418
```

3.2 Popis procesa

Jedna od korisnih informacija u radnoj memoriji računala je popis procesa koji su bili pokrenuti u trenutku snimanja slike memorije. Za ispis popisa procesa iz slike radne memorije operacijskog sustava Windows koristi se naredba **pslist**. Ispis naredbe istovjetan je popisu procesa u upravitelju zadataka (eng. *task manager*) sustava Windows. Cijela naredba korištena u ovom primjeru je:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 pslist
```

```
C:\WINDOWS\system32\cmd.exe
0x84890b60 svchost.exe      836   452   15    314   0    0 2018-02-13 12:18:21 UTC+0000
0x84c9b5c0 svchost.exe      860   452   32   1113   0    0 2018-02-13 12:18:21 UTC+0000
0x84e5a450 svchost.exe      944   452    6    120   0    0 2018-02-13 12:18:22 UTC+0000
0x84e88a90 svchost.exe     1068  452   19    394   0    0 2018-02-13 12:18:23 UTC+0000
0x84eebc60 spoolsv.exe     1236  452   13    276   0    0 2018-02-13 12:18:25 UTC+0000
0x84f08850 svchost.exe     1296  452   18    322   0    0 2018-02-13 12:18:26 UTC+0000
0x84f13c90 taskhost.exe     1364  452   11    214   1    0 2018-02-13 12:18:26 UTC+0000
0x84f3aa38 dwm.exe         1436  812    3     72   1    0 2018-02-13 12:18:27 UTC+0000
0x84f43858 explorer.exe    1456 1424   24    869   1    0 2018-02-13 12:18:27 UTC+0000
0x84f6f4b8 svchost.exe     1548  452   11    151   0    0 2018-02-13 12:18:28 UTC+0000
0x84f7c030 svchost.exe     1576  452   12    217   0    0 2018-02-13 12:18:28 UTC+0000
0x84ff03e8 cygrunsvr.exe   1736  452    6    101   0    0 2018-02-13 12:18:31 UTC+0000
0x8406e930 cygrunsvr.exe   1876 1736    0  -----  0    0 2018-02-13 12:18:33 UTC+0000 20
18-02-13 12:18:35 UTC+0000
0x84077030 conhost.exe     1896   320    2     33   0    0 2018-02-13 12:18:33 UTC+0000
0x85041d28 sshd.exe        1916 1876    4    100   0    0 2018-02-13 12:18:33 UTC+0000
0x8504b9a0 wlms.exe        1940   452    4     46   0    0 2018-02-13 12:18:34 UTC+0000
0x850663d0 VBoxTray.exe  2016 1456   13    140   1    0 2018-02-13 12:18:35 UTC+0000
0x84ca02d8 sppsvc.exe     1640   452    4    147   0    0 2018-02-13 12:18:37 UTC+0000
0x850c9698 svchost.exe     1264  452    5     92   0    0 2018-02-13 12:18:38 UTC+0000
0x85122368 SearchIndexer.  2260  452   13    641   0    0 2018-02-13 12:18:41 UTC+0000
0x84144d28 iexplore.exe    2988 1456   16    517   1    0 2018-02-13 12:20:13 UTC+0000
0x841646b8 iexplore.exe    3060 2988   33    691   1    0 2018-02-13 12:20:16 UTC+0000
0x851862a8 notepad.exe     3200 1456    1     52   1    0 2018-02-13 12:20:19 UTC+0000
0x851721e8 svchost.exe     3440  452   13    377   0    0 2018-02-13 12:20:38 UTC+0000
0x84249030 SearchProtocol  3828 2260    6    233   0    0 2018-02-13 12:21:45 UTC+0000
0x842458e8 SearchFilterHo  3852 2260    3     80   0    0 2018-02-13 12:21:45 UTC+0000
0x851604e0 taskhost.exe     3952  452    7    169   0    0 2018-02-13 12:22:25 UTC+0000
0x841c08d8 WmiPrvSE.exe   4052  560    8    118   0    0 2018-02-13 12:22:35 UTC+0000
0x8424d030 iexplore.exe     464  2988   28    602   1    0 2018-02-13 12:22:56 UTC+0000
C:\volatility>
```

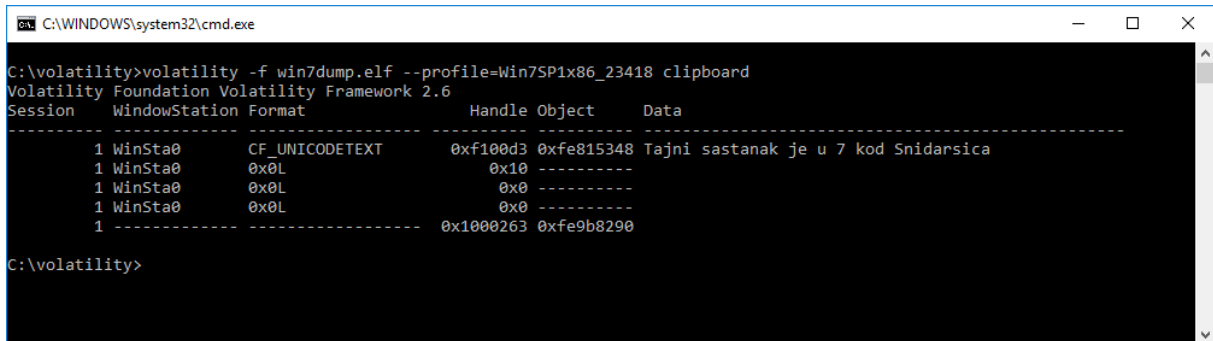
U ispisu naredbe u gornjoj slici moguće je vidjeti, uz ostala obilježja procesa, imena procesa koji su bili pokrenuti. Tako se iz navedenog može pretpostaviti da su na računalu bili pokrenuti programi Internet Explorer (ime procesa *iexplorer.exe*) i Notepad (ime procesa *notepad.exe*).

Važno je napomenuti kako ovo ne mora biti potpuna lista procesa pokrenutih u operacijskom sustavu. Moguće je da je zloćudni program sakrio svoj proces iz liste procesa te ga je zato potrebno potražiti drugim metodama, primjerice naredbom *psscan*.

3.3 Međuspremnik (eng. *clipboard*)

U memoriji se također nalazi sadržaj međuspremnika (eng. *clipboard*) koji se koristi primjerice za spremanje teksta u procesu kopiranja i lijepljena (eng. *copy and paste*). Do sadržaja međuspremnika moguće je doći korištenjem naredbe **clipboard**:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 clipboard
```



```
C:\WINDOWS\system32\cmd.exe
C:\volatility>volatility -f win7dump.elf --profile=win7SP1x86_23418 clipboard
Volatility Foundation Volatility Framework 2.6
Session  WindowStation  Format                Handle  Object  Data
-----
1 WinSta0      CF_UNICODETEXT      0xf10d3 0xfe815348 Tajni sastanak je u 7 kod Snidarsica
1 WinSta0      0x0L                0x10  -----
1 WinSta0      0x0L                0x0  -----
1 WinSta0      0x0L                0x0  -----
1 -----
1 -----                0x1000263 0xfe9b8290

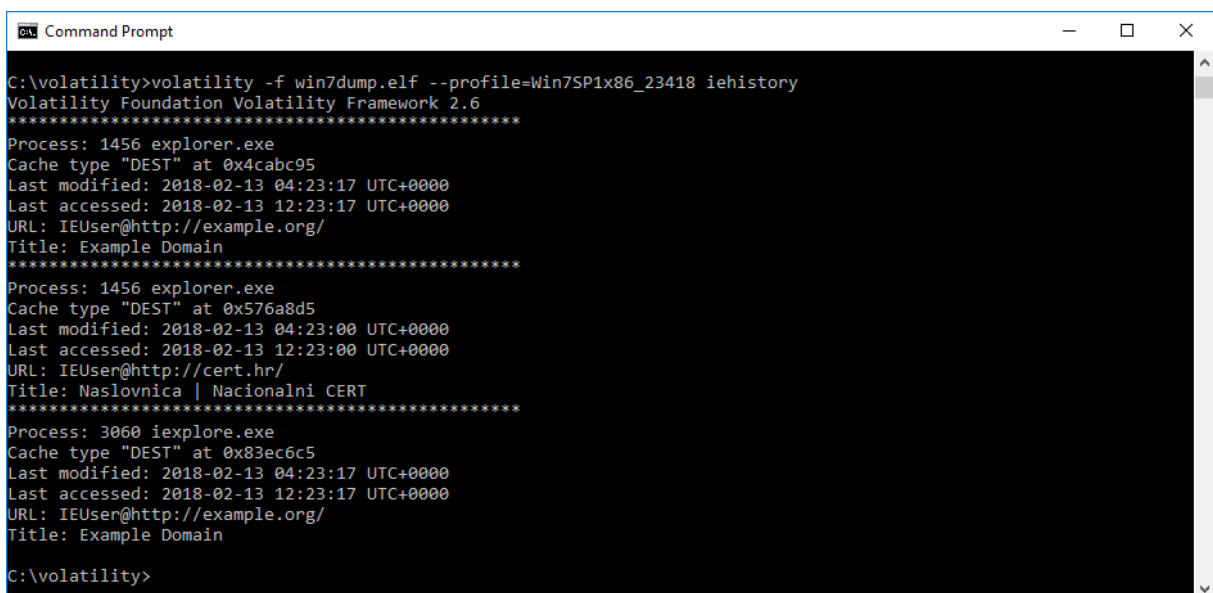
C:\volatility>
```

U ispisu naredbe vidi se kako se u međuspremniku nalazio tekst: „*Tajni sastanak je u 7 kod Snidarsica*“.

3.4 Povijest preglednika Internet Explorer

Kako smo pokretanjem alata Volatility naredbom *pslist* primijetili da je pokrenut proces imena *iexplorer.exe*, moguće je pretpostaviti da je na računalu bio pokrenut Web preglednik *Internet Explorer*. S alatom Volatility dolazi naredba **iehistory** pomoću koje je moguće otkriti neke od Web stranica koje su posjećene u pregledniku Internet Explorer. Naredba **iehistory** poziva se na sljedeći način:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 iehistory
```



```
Command Prompt
C:\volatility>volatility -f win7dump.elf --profile=Win7SP1x86_23418 iehistory
Volatility Foundation Volatility Framework 2.6
*****
Process: 1456 explorer.exe
Cache type "DEST" at 0x4cabc95
Last modified: 2018-02-13 04:23:17 UTC+0000
Last accessed: 2018-02-13 12:23:17 UTC+0000
URL: IEUser@http://example.org/
Title: Example Domain
*****
Process: 1456 explorer.exe
Cache type "DEST" at 0x576a8d5
Last modified: 2018-02-13 04:23:00 UTC+0000
Last accessed: 2018-02-13 12:23:00 UTC+0000
URL: IEUser@http://cert.hr/
Title: Naslovnica | Nacionalni CERT
*****
Process: 3060 iexplore.exe
Cache type "DEST" at 0x83ec6c5
Last modified: 2018-02-13 04:23:17 UTC+0000
Last accessed: 2018-02-13 12:23:17 UTC+0000
URL: IEUser@http://example.org/
Title: Example Domain

C:\volatility>
```

U ispisu se vidi popis posjećenih Web stranica korisnika pod nazivom *IEUser*. Moguće je vidjeti kako je korisnik posjetio Web stranice na adresama *http://example.org/* i *http://cert.hr/*.

3.5 Mrežne veze

Za ispit podataka o mrežnim vezama u operacijskom sustavu Windows koristi se naredba **netscan**. Cijela naredba korištena u ovom primjeru je:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 netscan
```

```

C:\WINDOWS\system32\cmd.exe
0x575fa670  UDPv4  127.0.0.1:1900  *:*  1576  svchost.exe  2018-02-13 12:20:38 UTC+0000
0x575faac0  UDPv4  10.0.2.15:1900  *:*  1576  svchost.exe  2018-02-13 12:20:38 UTC+0000
0x575faf10  UDPv6  :::1900  *:*  1576  svchost.exe  2018-02-13 12:20:38 UTC+0000
0x5746f3c0  TCPv4  0.0.0.0:49156  0.0.0.0:0 LISTENING  452  services.exe
0x574ed440  TCPv4  0.0.0.0:5357  0.0.0.0:0 LISTENING  4  System
0x574ed440  TCPv6  :::5357  :::0  LISTENING  4  System
0x574fd558  TCPv4  10.0.2.15:139  0.0.0.0:0 LISTENING  4  System
0x57204008  TCPv4  10.0.2.15:49251  40.113.87.220:443 ESTABLISHED -1
0x5720f590  TCPv4  10.0.2.15:49254  204.79.197.229:443 ESTABLISHED -1
0x572197f8  TCPv4  10.0.2.15:49259  83.139.67.208:443 ESTABLISHED -1
0x5722a990  TCPv4  10.0.2.15:49304  131.253.61.68:443 CLOSED -1
0x5722ecf8  TCPv4  10.0.2.15:49271  104.103.107.105:443 CLOSE_WAIT -1
0x5722fa60  TCPv4  10.0.2.15:49267  104.103.89.123:443 ESTABLISHED -1
0x57230008  TCPv4  10.0.2.15:49272  104.40.210.32:443 ESTABLISHED -1
0x57232de8  TCPv4  10.0.2.15:49288  204.79.197.203:443 ESTABLISHED -1
0x57236668  TCPv4  10.0.2.15:49293  83.139.67.216:443 CLOSE_WAIT -1
0x57243b30  TCPv4  10.0.2.15:49262  46.137.107.242:443 ESTABLISHED -1
0x57267008  TCPv4  10.0.2.15:49273  64.202.112.28:443 CLOSE_WAIT -1
0x5726aa90  TCPv4  10.0.2.15:49282  161.53.179.68:80  CLOSE_WAIT -1
0x5726b008  TCPv4  10.0.2.15:49278  161.53.179.68:80  CLOSE_WAIT -1
0x5726e500  TCPv4  10.0.2.15:49302  13.107.5.80:443  ESTABLISHED -1
0x5726e8e8  TCPv4  10.0.2.15:49305  93.184.216.34:80  ESTABLISHED -1
0x572749f8  TCPv4  10.0.2.15:49283  172.217.18.14:443 ESTABLISHED -1
0x57276580  TCPv4  10.0.2.15:49281  161.53.179.68:80  CLOSE_WAIT -1
0x572782a8  TCPv4  10.0.2.15:49280  161.53.179.68:80  CLOSE_WAIT -1
0x57281008  TCPv4  10.0.2.15:49279  161.53.179.68:80  CLOSE_WAIT -1
0x57282bc8  TCPv4  10.0.2.15:49284  74.125.133.156:443 ESTABLISHED -1
0x57284a00  TCPv4  10.0.2.15:49285  104.40.210.32:443 ESTABLISHED -1
0x57286008  TCPv4  10.0.2.15:49286  204.79.197.200:443 ESTABLISHED -1
0x57286788  TCPv4  10.0.2.15:49287  204.79.197.200:443 ESTABLISHED -1
0x5728e540  TCPv4  10.0.2.15:49294  185.63.144.1:443  ESTABLISHED -1
0x572936e0  TCPv4  10.0.2.15:49290  54.217.213.201:443 ESTABLISHED -1
0x57294008  TCPv4  10.0.2.15:49295  185.63.144.5:443  ESTABLISHED -1
0x57295de8  TCPv4  10.0.2.15:49298  204.79.197.203:443 ESTABLISHED -1
0x57297c20  TCPv4  10.0.2.15:49299  104.40.210.32:443 ESTABLISHED -1
0x5729c400  TCPv4  10.0.2.15:49301  104.40.210.32:443 ESTABLISHED -1

```

U ispisu naredbe moguće je primijetiti veći broj aktivnih mrežnih veza i priključaka na kojima operacijski sustav prihvaća nove veze. Tako se primjerice može vidjeti da sustav ima otvoren TCP priključak 139 – standardni priključak za NetBIOS protokol. Također, moguće je vidjeti da je uspostavljena veza na računalo 161.53.179.68 na priključku 80 – standardnom priključku za protokol HTTP. Na temelju toga, moguće je pretpostaviti da je korisnik otvarao Web stranicu na nekoj od domena koja odgovara toj IP adresi. U ovom slučaju, na virtualnom stroju bila je otvorena Web stranica na domeni *cert.hr*.

3.6 Registar operacijskog sustava Windows (eng. *Windows registry*)

Registar sustava Windows središnja je baza podataka u kojoj se nalaze konfiguracijski podaci nužni za funkcioniranje sustava. Kako se ti podaci često koriste, dio registra sustava Windows nalazi se u memoriji.

Volatility sadrži više naredbi za čitanje ključeva, vrijednosti i podataka zapisanih u registru. Za čitanje podključeva i vrijednosti u njima u alatu Volatility postoji naredba **printkey**. Naredbi printkey prosljeđuje se parametar **-K** iza kojeg dolazi putanja traženog ključa u registru:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 printkey
-K "Microsoft\Windows\CurrentVersion\Run"
```

```

C:\volatility>volatility -f win7dump.elf --profile=Win7SP1x86_23418 printkey -K "Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: Run (S)
Last updated: 2018-02-13 13:34:50 UTC+0000

Subkeys:

Values:
REG_SZ      bginfo      : (S) C:\BGInfo\Bginfo.exe /accepteula /ic:\bginfo\bgconfig.bgi /timer:0
REG_SZ      VBoxTray    : (S) C:\Windows\system32\VBoxTray.exe
REG_SZ      AllIsOK     : (S) C:\nothing_here\suspicious_program.exe

C:\volatility>

```

U sustavu Windows postoji više mjesta u registru u kojima su zapisani programi koji se pokreću prilikom pokretanja sustava. Jedno od njih je:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

u kojem se nalaze zapisi programa koji se pokreću prijavom bilo kojeg korisnika. U ispisu sa slike moguće je primijetiti kako se tamo nalazi zapis za program imena *suspicious_program.exe* iz direktorija *C:\nothing_here*. Zapisivanje vrijednosti u ovaj podključ u registru česta je tehnika zlonamjernih programa.

3.7 Datotečni sustav (eng. *filesystem*)

Operacijski sustavi koriste datotečne sustave kako bi organizirali datoteke i definirali način njihove pohrane na disk. Datotečni sustavi obično uključuju datotečne tablice u kojima su zapisani podaci koji opisuju hijerarhiju datoteka i direktorija. Operacijski sustav Windows obično koristi datotečni sustav NTFS koji sadržava datotečnu tablicu naziva MFT (*Master File Table*). U datotečnom sustavu NTFS, datoteke vrlo male veličine spremaju se izravno u datotečnu tablicu radi povećanja performansi sustava. Kako se datotečne tablice često koriste u radu operacijskog sustava očekivano je da se one nalaze i u radnoj memoriji.

Naredba **mftparse** alata Volatility pretražuje sliku memorije tražeći moguće datotečne tablice. Nakon pronalaska tablice, naredba ispisuje informacije o datotekama te njihov sadržaj, ako je on bio zapisan u datotečnoj tablici. Naredba se poziva na sljedeći način:

```
volatility -f win7dump.elf --profile=Win7SP1x86_23418 mftparse
```

```

CA\WINDOWS\system32\cmd.exe
Attribute: In Use & File
Record Number: 141419
Link count: 2

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-----
2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 Archive

$FILE_NAME
Creation              Modified              MFT Altered              Access Date              Name/Path
-----
2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 VIRTUA~1\ORACLE~1
.URL

$FILE_NAME
Creation              Modified              MFT Altered              Access Date              Name/Path
-----
2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 2018-01-03 05:02:59 UTC+0000 VIRTUA~1\Oracle V
M VirtualBox Guest Additions.url

$OBJECT_ID
Object ID: ad968a36-43f0-e711-9f9b-08002710b8d0
Birth Volume ID: 80000000-5000-0000-0000-180000000100
Birth Object ID: 33000000-1800-0000-5b40-6e7465726e65
Birth Domain ID: 7453686f-7274-6375-745d-0d0a55524c3d

$DATA
000000000: 5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 [InternetShortcu
000000010: 74 5d 0d 0a 55 52 4c 3d 68 74 74 70 3a 2f 2f 77 t].URL=http://w
000000020: 77 77 2e 76 69 72 74 75 61 6c 62 6f 78 2e 6f 72 ww.virtualbox.or
000000030: 67 0d 0a g..

*****
MFT entry found at offset 0xf3f000
Attribute: In Use & File
Record Number: 135024
Link count: 1

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-- More --

```

U ispisu naredbe na gornjoj slici vidi se primjer datoteke čiji je sadržaj pronađen u datotečnoj tablici. Ime datoteke je *Oracle VM VirtualBox Guest Additions.url*, te je u njoj sadržan prečac na mrežnu stranicu <https://www.virtualbox.org/>.

4 Zaključak

U dokumentu je opisano korištenje jednostavnijih naredba alata Volatility, no već s njima je moguće otkriti brojne korisne forenzičke tragove. Alat Volatility dolazi s velikim brojem naredbi, no moguće ga je i proširiti raznim dodacima kako bi strukture podataka u radnoj memoriji bilo moguće detaljnije analizirati.

Forenzička analiza radne memorije područje je koje se i dalje razvija. Aktivo se provode istraživanja i razvijaju alati koji omogućuju pronalazak i analizu tragova na nove načine. Za provedbu naprednijih postupaka forenzike radne memorije potrebno je detaljnije znanje rada operacijskih sustava te struktura podataka koji se nalaze u memoriji.

Bitno je imati na umu da je u cijelom kontekstu računalne forenzike forenzika radne memorije samo jedna komponenta. Za potpunu sliku o stanju sustava potrebno je provesti i radnje drugih grana računalne forenzike, prvenstveno forenzike diska odnosno trajne memorije te mrežne forenzike.