



Факултет техничких наука
Лабораторија за дигиталну форензику

ФОРЕНЗИКА РАДНЕ MEMOPIJE

Увод у дигиталну форензику
Јелена Драгишић, Светлана Антешевић

Преглед области

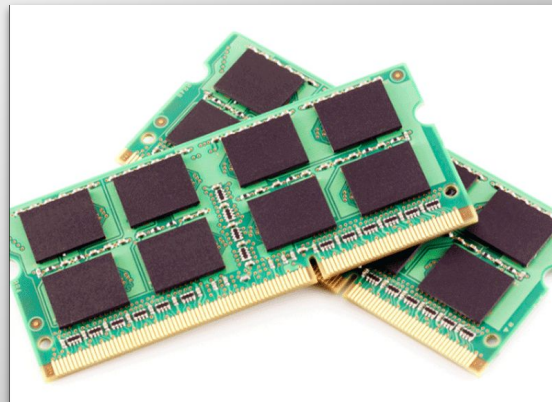
Чиме се бави форензика радне/оперативне меморије?

- Спада под област форензике рачунара.
- Бави се дигиталним доказима који се налазе у радној/оперативној меморији (RAM - Random Access Memory).
- RAM је елемент рачунарског система који складишти рачунарске програме (који се извршавају) и податке које обрађују рачунарски програми (који се извршавају).
- Полупроводничка меморија која има велику брзину читања и писања.

Преглед области

Где се налазе докази?

- Радна/оперативна меморија (RAM - Random Access Memory)
- Виртуелна меморија
 - ◆ Код Windows ОС виртуелна меморија је смештена у фајл pagefile.sys
 - ◆ Код Linux ОС swap партиција представља виртуелну меморију.



Преглед области

Које податке можемо прикупити?

- Податке о процесима
- Системске информације
- Подаци о конекцијама на мрежи
- Криптографски кључеви и лозинке
- Листа извршних команди које су уношене у конзолу

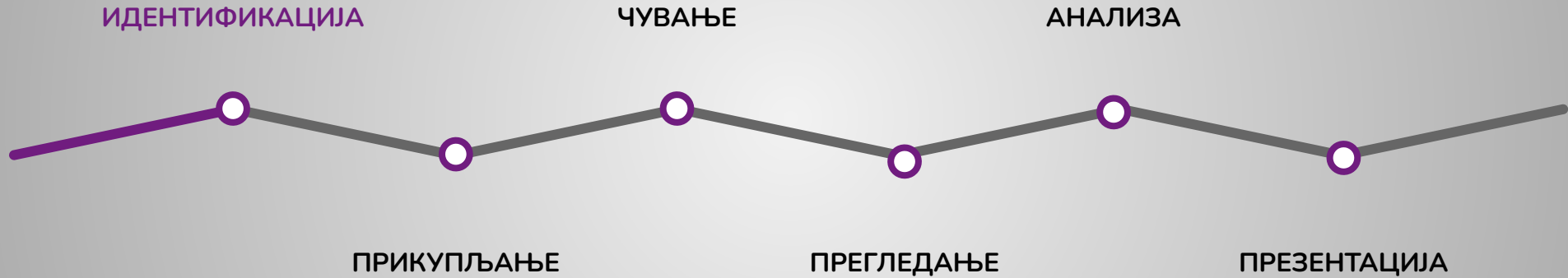
Преглед области

Шта представља изазов?

Радна меморија је нестална (енг. volatile) што значи да се њен садржај губи када се рачунар искључи. Дакле, радну меморију можемо прикупити само на укљученим уређајима.

Можемо утицати на промену доказног материјала приликом прикупљања радне меморије.

Процес форензичке истраге



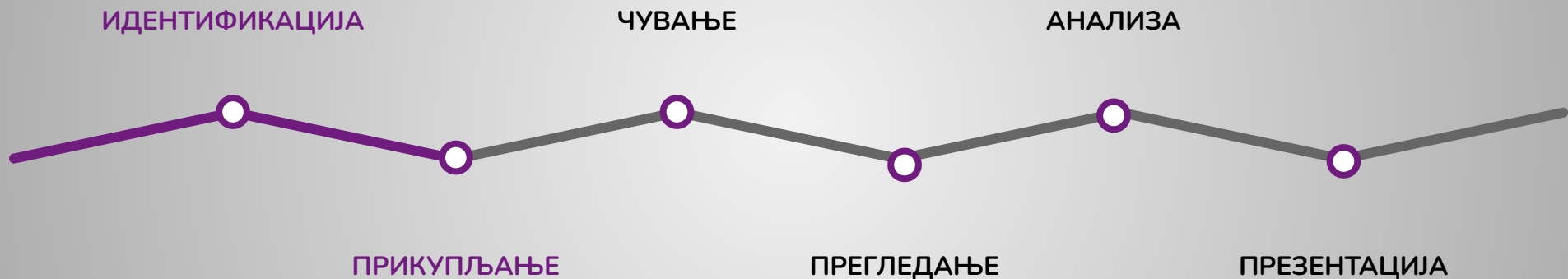
Идентификација

Односи се на детектовање, препознавање и одређивање дигиталних уређаја које треба истражити.

Под идентификацијом се подразумева и читавање идентификатора дигиталних уређаја који се истражују (произвођач, модел, серијски број, верзије радне меморије).

Пример: Идентификовали смо да је рачунар укључен, самим тим знамо да постоје докази у RAM меморији, па их можемо прикупити.

Процес форензичке истраге



Прикупљање

Идентификоване доказе је потребно прикупити коришћењем научно и правно ваљаних метода.

Потребно је припремити медије на којима ћемо складиштити форензичке копије.

Потребно је одабрати одговарајуће алате за прикупљање оперативне меморије у зависности од оперативног система.

Неки од алата за прикупљање су:

- FTK Imager (Windows OC)
- AVML, LiME (Linux OC)

Прикупљање оперативне меморије са Windows ОС

FTK Imager (Forensic Toolkit Imager)

Софтверски алат који је развила компанија AccessData.

Користи се за прикупљање масовне и радне меморије.

Може да се врши и прегледање прикупљене меморије помоћу Forensic Toolkit (FTK) алата.

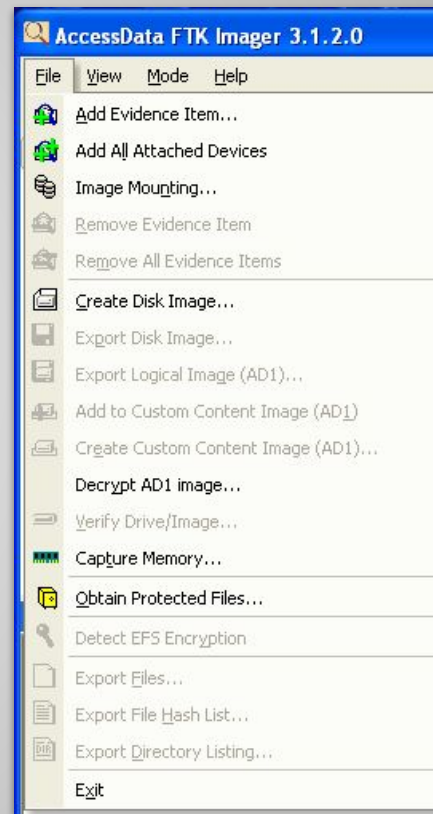
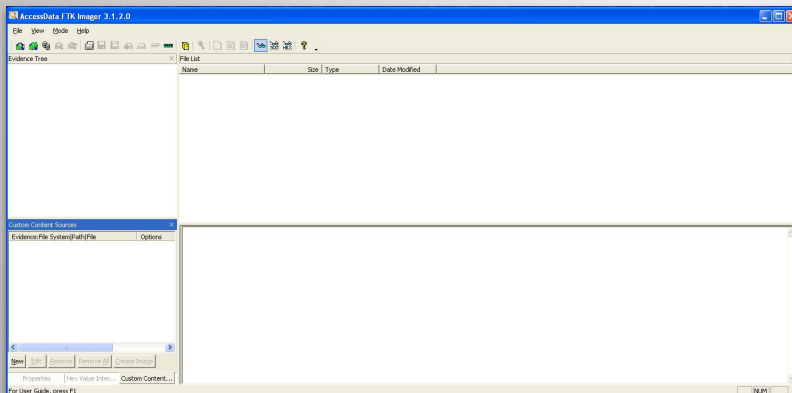
Првенствено је намењен за прикупљање меморије са Windows оперативних система.



Прикупљање оперативне меморије са Windows ОС

FTK Imager (Forensic Toolkit Imager)

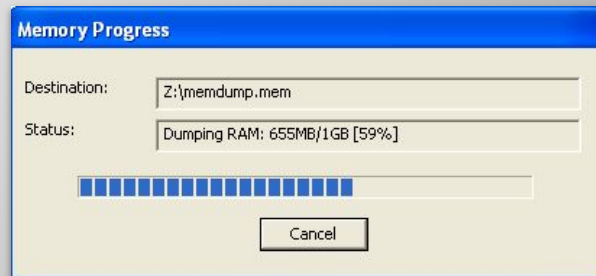
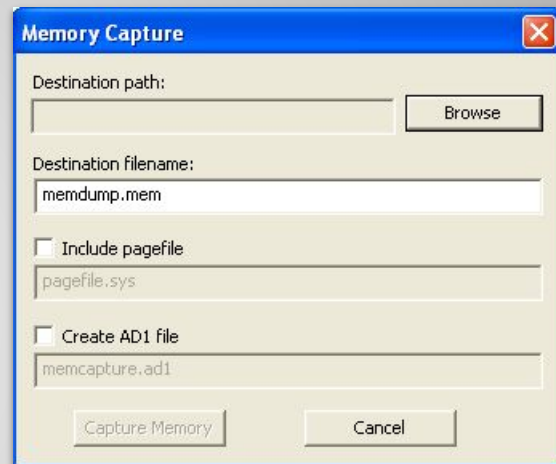
1. Покренемо алат двокликом на иконицу.
2. Отворимо падајући мени File
3. Одаберемо опцију Capture Memory



Прикупљање оперативне меморије са Windows OC

FTK Imager (Forensic Toolkit Imager)

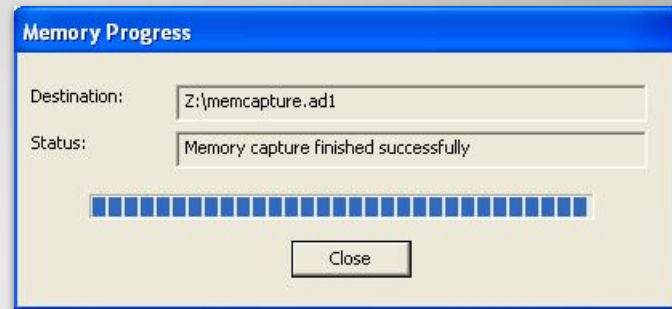
4. У оквиру отвореног прозора можемо изабрати путању где ће нам бити смештена прикупљена радна меморија, назив и екстензију фајла, можемо и означити да желимо да се прикупи pagefile.sys и AD1.
5. Покренемо прикупљање на дугме Capture Memory







Прикупљање оперативне меморије са Windows OC

FTK Imager (Forensic Toolkit Imager)

- Када се прикупљање заврши притиснути Close.
- У оквиру одабраног фолдера можемо видети прикупљене фајлове.



	memcapture.ad1.txt	543 bytes	16:25	☆
	memcapture.ad1	188,1 MB	16:25	☆
	pagefile.sys	1,6 GB	16:22	☆
	memdump.mem	1,1 GB	16:21	☆

Прикупљање оперативне меморије са Linux ОС

AVML (Acquire Volatile Memory for Linux)

microsoft/**avml**

AVML - Acquire Volatile Memory for Linux



Програм командне линије за прикупљање оперативне меморије на Linux оперативним системима који је развила компанија Microsoft.

Може да користи [LiME](#) излазни формат (када се не користи компресија).

Може да користи компресију фајла помоћу [Snappy](#).

Може да врши чување снимљене слике на спољним локацијама преко Azure Blob Store-a или HTTP-a.

Прикупљање оперативне меморије са Linux ОС

AVML (Acquire Volatile Memory for Linux)

Након инсталације алата која је једноставна, потребно је позвати команду за прикупљање којој треба проследити путању и назив фајла са одговарајућом екстензијом.

```
$ sudo ./avml /putanja/RAM.raw
```



Прикупљање виртуелне меморије са Linux ОС

Data Dump (dd)

Уколико желимо да прикупимо **swap** партицију на Linux оперативном систему, можемо помоћу следеће команде добити путању где се она налази и помоћу **dd** алата је прикупити.

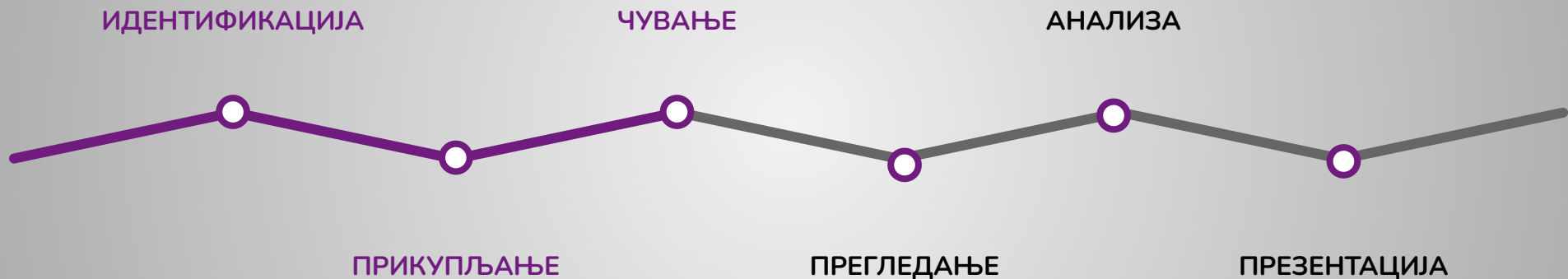
\$ sudo swapon -s

```
pavle@pavle-pc:~/Downloads$ sudo swapon -s
```

Filename	Type	Size	Used	Priority
/dev/sda5	partition	2095100	0	-1

\$ sudo dd if=/dev/sda5 of=/putanja/swap.img conv=noerror,sync

Процес форензичке истраге



Чување

Прикупљени докази морају се сачувати коришћењем физичких, техничких и организационих контрола.

Верификација свих форензичких копија се врши помоћу рачунања хеш вредности (са неким од алгоритама: sha1, sha256, md5) да би се обезбедио интегритет доказа.

- MD5 алгоритам: `$ [sudo] md5sum [path]`
- SHA1 алгоритам: `$ [sudo] sha1sum [path]`

Чување

Ланац доказа - евиденција о томе када и ко је имао приступ доказима.

Факултет техничких наука, Лабораторија за дигиталну форензику, Трг Доситеја Обрадовића 6, 21102 Нови Сад,
+381 214854565, +381 66 8211617, digfor@uns.ac.rs, <https://digfor.ftn.uns.ac.rs/>

ОБРАЗАЦ ЕВИДЕНЦИЈЕ РУКОВАЊА ДОКАЗНИМ МАТЕРИЈАЛОМ

Идентификатор предмета:
Идентификатор доказног материјала:
Произвођач:
Модел:
Серијски број:

Бр.	Датум	Име и презиме	Опис радње	Потпис
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Чување

Докази се чувају у одговарајућем формату датотека који омогућавају компресију података, поделу датотека на више датотека и шифровање датотека.

- Raw format (.raw, .bin, .mem)
- AccessData AD1 format (.ad1)
- LiME format (.lime)
- Hibernation File format (.hiberfil)
- Crash Dump format (.dmp)
- AFF format (.aff)

Процес форензичке истраге



Прегледање и анализа

Volatility Foundation

- Софтверски алат отвореног изворног кода за прегледање и анализу радне меморије који је развила независна и непрофитна организација The Volatility Foundation.
- Модуларна и проширива платформа.
- Могуће је покренути алат на свим платформама које подржавају Python.
- Анализира форензичке копије радне меморије различитих оперативних система из различитих извора података.



Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6

Листу свих доступних plugin-ова и профила можемо видети помоћу команде

→ `$ cd /opt/volatility-2.6`

→ `$ sudo python2 vol.py --info`

Први и најбитнији корак код анализе радне меморије помоћу Volatility алата јесте одредити профил који указује на тип оперативног система који ће алат анализирати. Покретањем модула **imageinfo** можемо утврдити који је одговарајући профил. Уколико профил не постоји у листи профила неопходно је додати га у volatility са следећег [линка](#) или направити профил па га додати.

Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6

Команда за покретање **imageinfo** plugin-a

\$ sudo python2 vol.py -f /putanja/memdump.mem imageinfo

```
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
          : Suggested Profile(s) : WinXPSP1x64, Win2003SP1x64, WinXPSP2x64, Win2003SP2x64
          : AS Layer1          : WindowsAMD64PagedMemory (Kernel AS)
          : AS Layer2          : FileAddressSpace (/media/sf_SharedFolderVM/memdump.mem)
          : PAE type           : No PAE
          : DTB                : 0x3b2000L
          : KDBG               : 0xf80001187cc0L
          : Number of Processors : 2
          : Image Type (Service Pack) : 1
          : KPCR for CPU 0      : 0xffffffff80001189000L
          : KPCR for CPU 1      : 0xffffffffadfe3a6b000L
          : KUSER_SHARED_DATA    : 0xffffffff780000000000L
          : Image date and time  : 2022-03-26 15:21:23 UTC+0000
          : Image local date and time : 2022-03-26 07:21:23 -0800
```


Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6

У наредне команде потребно је укључити предложени профил WinXPSP1x64.

Шаблон за покретање свих осталих plugin-ова је следећи

```
$ sudo python2 vol.py -f /putanja/memdump.mem --profile=WinXPSP1x64 <plugin>
```

Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6 - plugins

Идентификација и анализа процеса:

- **pslist** - Листа свих покренутих процеса.
- **pstree** - Стабло свих покренутих процеса у зависности од parent и child процеса.
- **psscan** - Листа процеса добијена претрагом EPROCESS структуре која представља процес.
- **psxview** - Листа сакривених процеса детаљније.

Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6 - plugins

Анализа мрежних сервиса и конекција:

- **connections** - Листа конекција на мрежи са приказаним локалним и remote адресама (Windows XP and 2003 Only).
- **connscan** - Приказ TCP конекција.
- **sockets** - Приказ листе отворених socket-а.

Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6 - plugins

Анализа DLL (Dynamic Link libraries) скрипти који су специфични за Windows ОС:

- **verinfo** - Информације о PE (portable executable) датотекама.
- **dlllist** - Листа свих покренутих DLLs за сваки процес.
- **getsids** - Враћа покренуте процесе сортиране по редоследу покретања у формату: [process] (PID) [SID] (user)

Прегледање и анализа форензичке слике прикупљене са Windows ОС

Volatility Foundation 2.6 - plugins

- **dumpcerts** - Враћа приватне RSA и јавне SSL кључеве. Неопходно је навести директоријум у који ће се сместити кључеви са додатком [-D <директоријум>]
- **cmdscan** - Враћа историју команди скенирањем _COMMAND_HISTORY
- **cmdline** - Приказује аргументе процеса покренутих помоћу командне линије
- **timeliner** - Креира временску линију од разних артефаката у меморији

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6

Да бисмо прегледали слику прикупљене радне меморије са Linux оперативног система неопходно је да добавимо одговарајући профил који помаже Volatility-ју да прегледа форензичке копије тог оперативног система.

Тај профил у .zip формату је потребно додати у путању

`/opt/volatility-2.6/volatility/plugins/overlays/linux`

Покретањем следеће команде може се видети да ли је Volatility препознао профил који нам треба.

`$ sudo python2 vol.py --plugins=./volatility/plugins --info`

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6

На слици се може видети део излаза од претходно покренуте команде

```
└─$ sudo python2 vol.py --plugins=./volatility/plugins/ --info
Volatility Foundation Volatility Framework 2.6

Profiles
├── linuxLinux_4_4_0-148-genericx64 - A Profile for Linux Linux_4.4.0-148-generic x64
├── VistaSP0x64 - A Profile for Windows Vista SP0 x64
├── VistaSP0x86 - A Profile for Windows Vista SP0 x86
├── VistaSP1x64 - A Profile for Windows Vista SP1 x64
├── VistaSP1x86 - A Profile for Windows Vista SP1 x86
├── VistaSP2x64 - A Profile for Windows Vista SP2 x64
├── VistaSP2x86 - A Profile for Windows Vista SP2 x86
├── Win10x64 - A Profile for Windows 10 x64
├── Win10x64_10586 - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
├── Win10x64_14393 - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
├── Win10x86 - A Profile for Windows 10 x86
├── Win10x86_10586 - A Profile for Windows 10 x86 (10.0.10586.420 / 2016-05-28)
├── Win10x86_14393 - A Profile for Windows 10 x86 (10.0.14393.0 / 2016-07-16)
├── Win2003SP0x86 - A Profile for Windows 2003 SP0 x86
├── Win2003SP1x64 - A Profile for Windows 2003 SP1 x64
├── Win2003SP1x86 - A Profile for Windows 2003 SP1 x86
├── Win2003SP2x64 - A Profile for Windows 2003 SP2 x64
├── Win2003SP2x86 - A Profile for Windows 2003 SP2 x86
└── Win2003SP3x64 - A Profile for Windows 2003 SP3 x64
```

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6

Потребно је укључити профил приликом анализе радне меморије помоћу наредне команде за све plugin-ове:

```
$ sudo python2 vol.py --plugins=./volatility/plugins -f /putanja/RAM.raw  
--profile=LinuxLinux_4_4_0-142-genericx64 <plugin>
```


Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6 - plugins

- **linux_pslist** - Приказује листу стартованих процеса.
- **linux_psaux** - Приказује листу процеса са приказаном командном линијом и временом почетка процеса.
- **linux_pstree** - Враћа приказ parent/child веза између процеса.
- **linux_pidhashtable** - Набраја процесе кроз PID hash табелу.

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6 - plugins

- **linux_mmap** - Штампа листу додељених страница и страница које се налазе у меморији. Приказане су виртуелне и физичке адресе. Одаберите одређене процесе са -p опцијом.
- **linux_bash** - Опоравља bash историју из меморије тј. историју команди које је корисник уносио путем терминала.
- **linux_lsmod** - Можемо прикупити уčitане модуле кернела.

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6 - plugins

- **linux_arp** - исписује ARP табелу (веза између IP и MAC адресе).
- **linux_ifconfig** - враћа информације о активном интерфејсу, укључујући IP адресе, име интерфејса, MAC адресу и да ли је NIC у промискуитетном режиму или не (sniffing)
- **linux_netstat** - враћа активне мрежне конекције

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Volatility Foundation 2.6 - plugins

- **linux_cpufreq** - приказује информације о процесору.
- **linux_iomem** - приказује физичке адресе тренутно резервисане за IO уређаје као што су PCI и меморија видео картице.
- **linux_mount** - враћа листу монтираних извора.
- **linux_volshell** - додатак који омогућава да директно приступите меморији и излистате податке о процесима помоћу **ps()** команде.

Прегледање и анализа форензичке слике прикупљене са Linux ОС



Findaes 1.2

Алат командне линије који претражује AES кључеве тражећи њихове распореде кључева.

Може да пронађе кључеве од 128, 192 и 256 бита, као што су они које користе TrueCrypt и BitLocker.

Првобитно намењен за меморијске слике, може користити произвољне податке.

Прегледање и анализа форензичке слике прикупљене са Linux ОС

Findaes 1.2

Након инсталације програма можемо га покренути над неком форензичком копијом радне меморије помоћу следеће команде

- `$ cd /opt/findaes-1.2`
- `$ sudo ./findaes /putanja/RAM.raw`

```
(kali㉿kali)-[/opt/findaes-1.2]  
$ sudo ./findaes /media/sf_kali/RAM.raw  
Searching /media/sf_kali/RAM.raw  
Found AES-128 key schedule at offset 0x3cd37040:  
c6 89 ff 43 8e 90 af 3c e0 f7 9c e4 9a 52 f4 f2  
Found AES-128 key schedule at offset 0x3cd371a0:  
8e 6e fa e2 cc 8f 02 0b e5 a6 13 d2 72 7f df 89
```

Процес форензичке истраге

ИДЕНТИФИКАЦИЈА

ЧУВАЊЕ

АНАЛИЗА

ПРИКУПЉАЊЕ

ПРЕГЛЕДАЊЕ

ПРЕЗЕНТАЦИЈА



Презентација

Резултати анализе доказа се презентују у писменом облику суду или компанији.

Односи се на процес којим форензичар дели резултате фазе анализе у облику извештаја заинтересованим странама.

Форензичар обично сачињава налаз и мишљење и усмено га брани одговарајући на питања суда, тужиоца и браниоца.

Корисни линкови и књиге

- <https://www.kali.org/docs/>
- <https://www.exterro.com/ftk-imager>
- <https://github.com/microsoft/avml>
- <https://www.volatilityfoundation.org/26>
- <https://community.chocolatey.org/packages/findaes>
- Књига: Digital Forensics with Kali Linux
- Књига: Digital forensics : an academic introduction
- Књига: The Art of Memory Forensics

