



JIFI2018

JORNADAS DE INVESTIGACIÓN ENCUENTRO ACADÉMICO INDUSTRIAL

FACULTAD DE INGENIERÍA UCV

23 - 26 DE OCTUBRE

INVESTIGACIÓN + DESARROLLO + INNOVACIÓN



Facultad de
Ingeniería

Análisis Forense de la Memoria RAM

Ing. Vincenzo Mendillo

Profesor Titular

UCV, USB, UCAB, UNIMET

Director de [STIT Consultores](#)

Coordinador del [Diplomado STIT](#) en Seguridad Informática

<http://mendillo.info> - vmendillo@ieee.org - Twitter: [@vmendillo](#)

Caracas (Venezuela) – Octubre 2018



¿Qué es la Forénsica Digital?

La Forénsica Digital (o Informática Forense) se dedica a investigar incidentes de seguridad y delitos informáticos, (tales como ciberterrorismo, ataques de hackers, penetración de intrusos, fraudes bancarios, etc.), que ocurren en el moderno mundo digital.



Ejemplos de campo de acción de la Forénsica Digital

- Uso o acceso a recursos en forma no autorizada.
- Lectura, sustracción o copiado de información confidencial.
- Interceptación de datos (sniffer, keylogger).
- Introducción de malware (virus, troyano, ransomware, etc.).
- Fraude y alteración de los estados contables.
- Evasión de impuestos con doble contabilidad.
- Falsificación de tarjetas de débito y crédito.
- Tráfico de drogas, contrabando, lavado de dinero.
- Acoso sexual, extorsión, pornografía infantil.
- Secuestro, espionaje, sabotaje, terrorismo.

Análisis forense

Se utilizan herramientas y técnicas sofisticadas para encontrar, preservar y analizar datos digitales "frágiles", que son susceptibles de ser borrados o sufrir alteración.



Kit de Herramientas de Seguridad Informática

- | | |
|---------------------|----------|
| ► 0 FORENSICS Menu | [Ctrl+F] |
| 1 SECURITY Menu | [Ctrl+R] |
| 2 ANTIVIRUS Menu | [Ctrl+A] |
| 3 BACKUP Menu | [Ctrl+B] |
| 4 DOS Menu | [Ctrl+O] |
| 5 UTILITIES Menu | [Ctrl+U] |
| 6 Help | [F1] |
| 7 Boot to first HDD | [F7] |
| 8 Rebuild Main Menu | [F8] |
| 9 Reboot | [F9] |
| 10 Power off | [F10] |



Producido por Vincenzo Mendillo
<http://mendillo.info>
Versión 2.6



- Kali Linux (auditing, hacking, pentesting, forensics)
- CAINE, PALADIN, HELIX (forensics)
- Autopsy, SIFT, FTK Imager (forensics)
- Macrium (backup & restore with WinPE)
- Clonezilla (backup & restore partitions)
- Rescatux (recovery & repair tool)
- ESET System Rescue (antivirus & recovery)
- MSDaRT (Microsoft Diagnostics & Recovery Toolset)
- Kon-Boot (start Windows with blank password)
- NTpw (Change Windows NT Password)
- ResetWindowsPassword (change or reset password)

Se busca información que puede estar cifrada, borrada, camuflada u oculta.

Se reúne la evidencia física y la evidencia digital para litigios internos en una organización (*corporate investigations*) y para juicios civiles o penales.



Video: El trabajo de un Perito Informático Forense



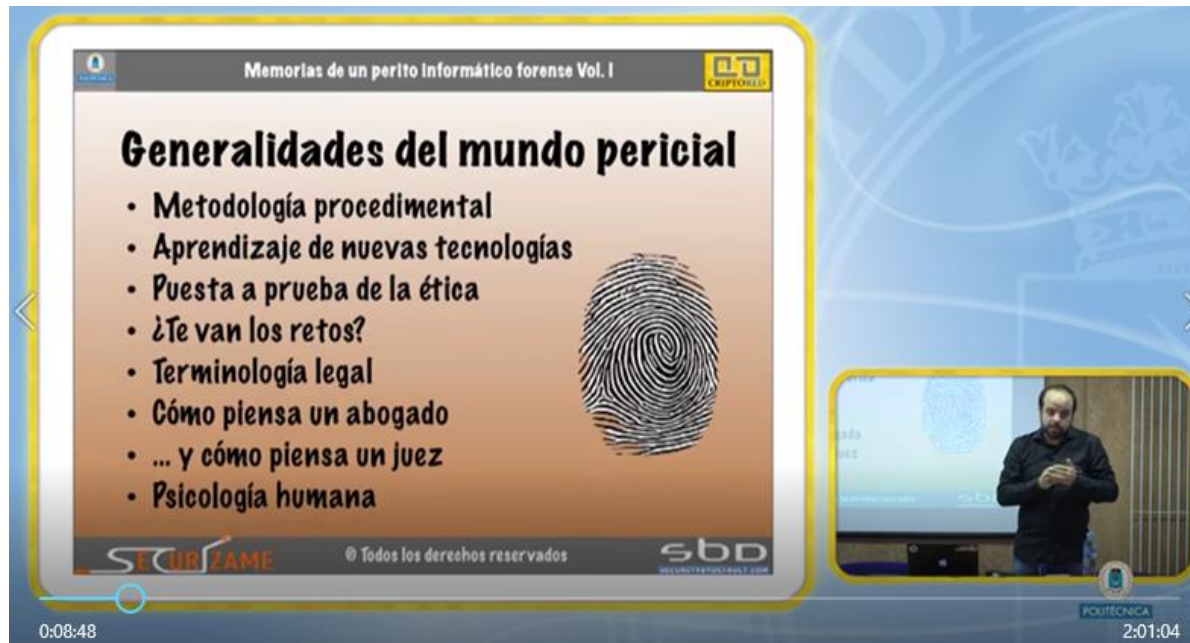
 YouTube



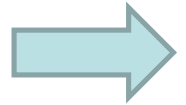
Perito
Informático:
qué hacen y
cómo trabajan.



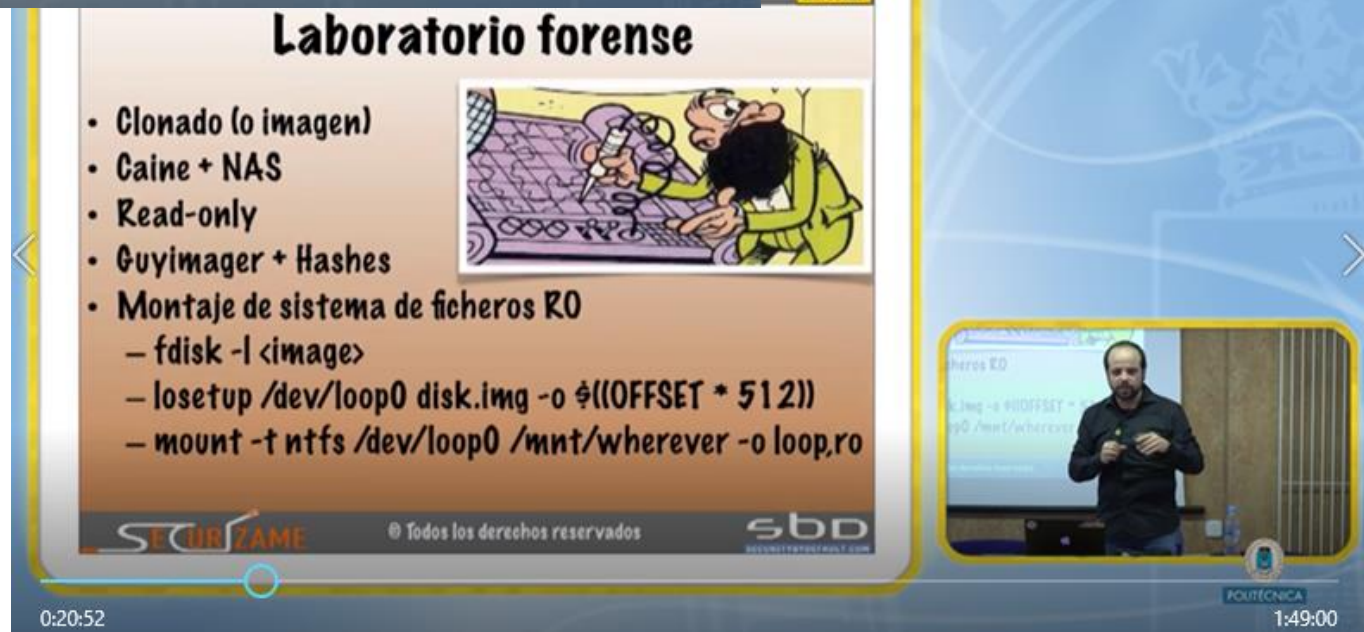
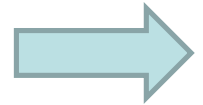
Video: Memorias de un perito informático forense



YouTube



PDF

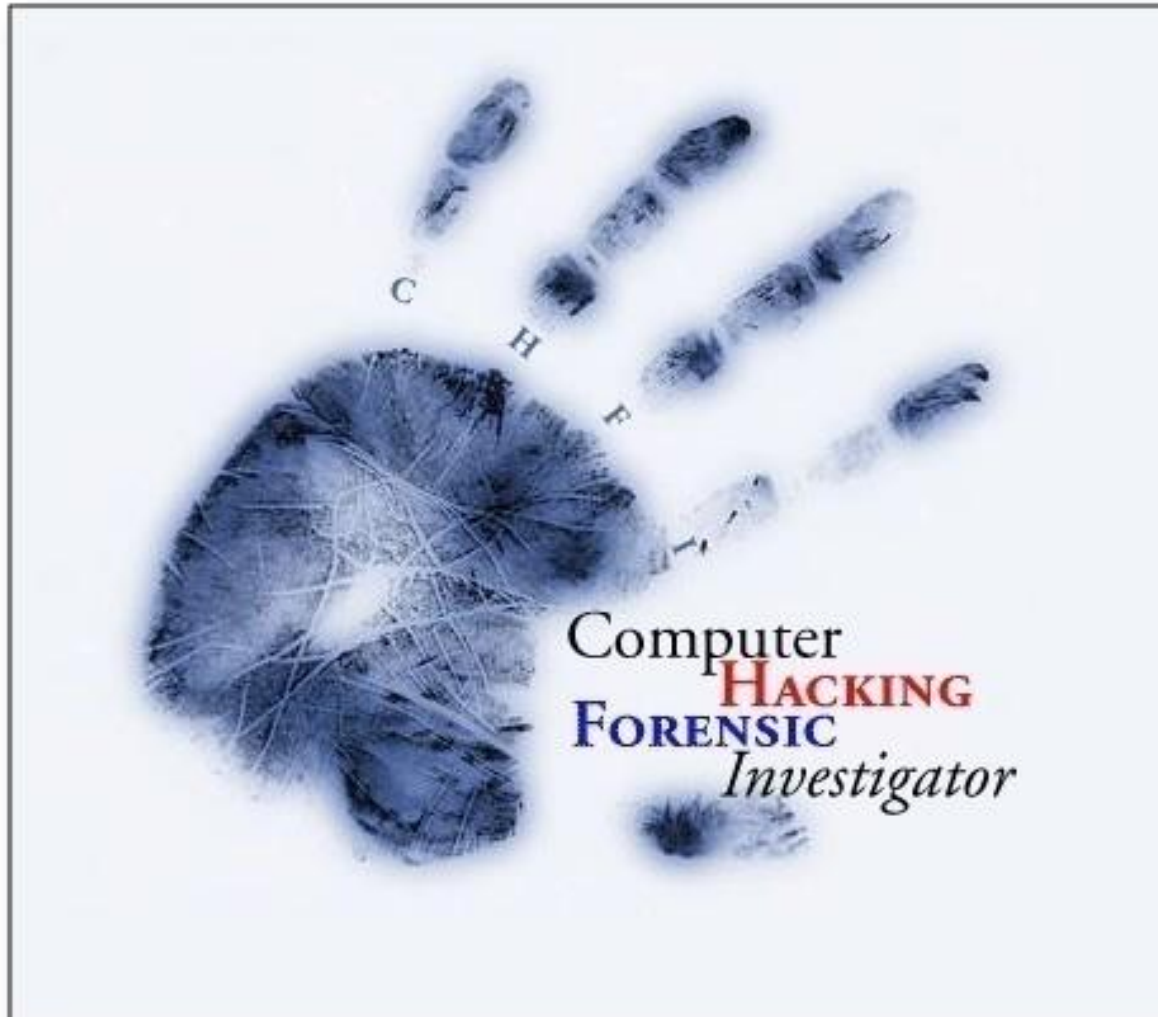


Conferencia presentada en febrero de 2015 en la Universidad Politécnica de Madrid, España, por Lorenzo Martínez, director de Securizame y editor del blog Security By Default.

Certificaciones Profesionales en Forénsica Digital

EC-Council

Hackers are here. Where are you?

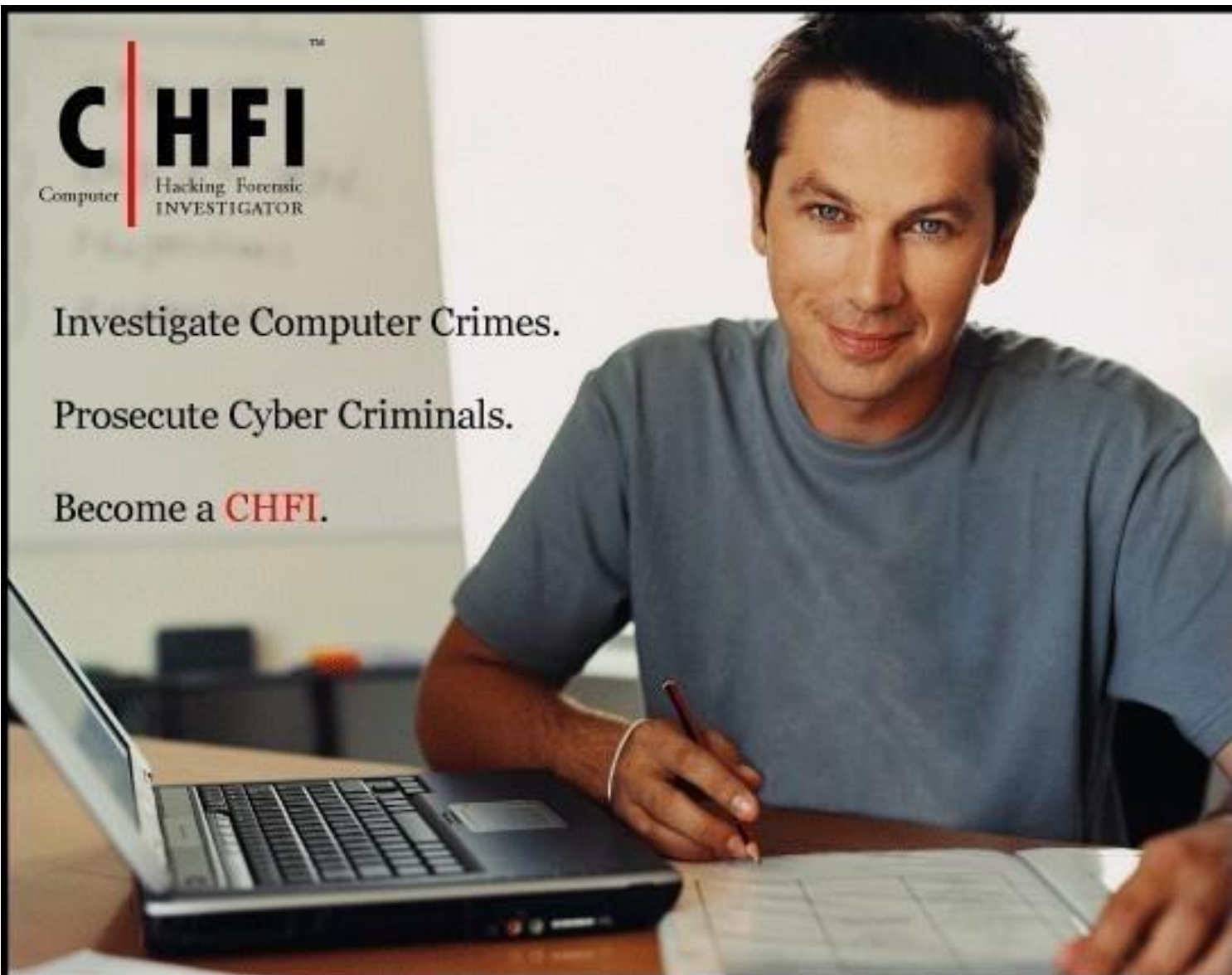




Investigate Computer Crimes.

Prosecute Cyber Criminals.

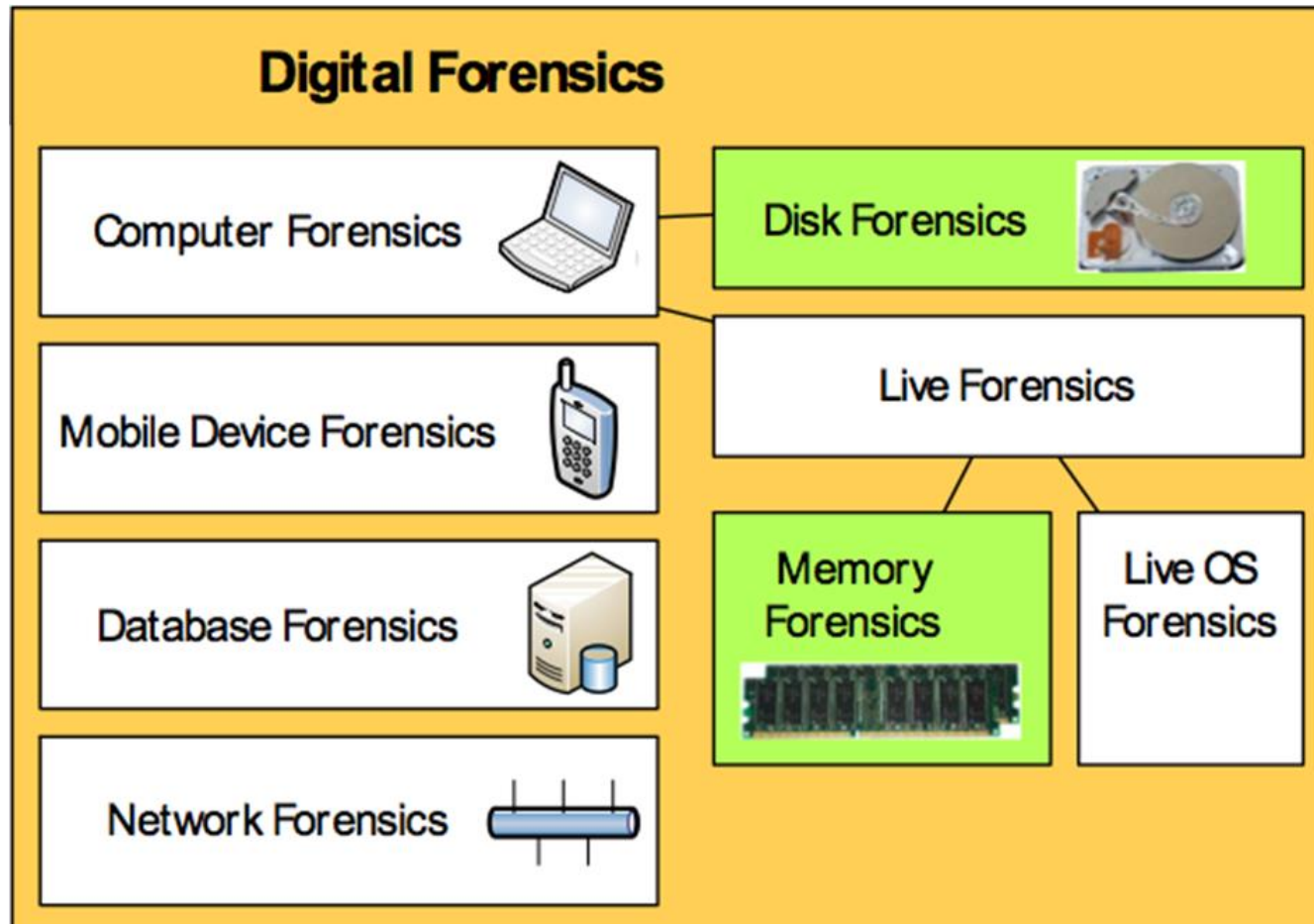
Become a **CHFI**.



<http://www.eccouncil.org>

EC-Council

Las distintas áreas de la Forénsica Digital



Cloud Forensics – NEW!



Análisis forense de la memoria RAM

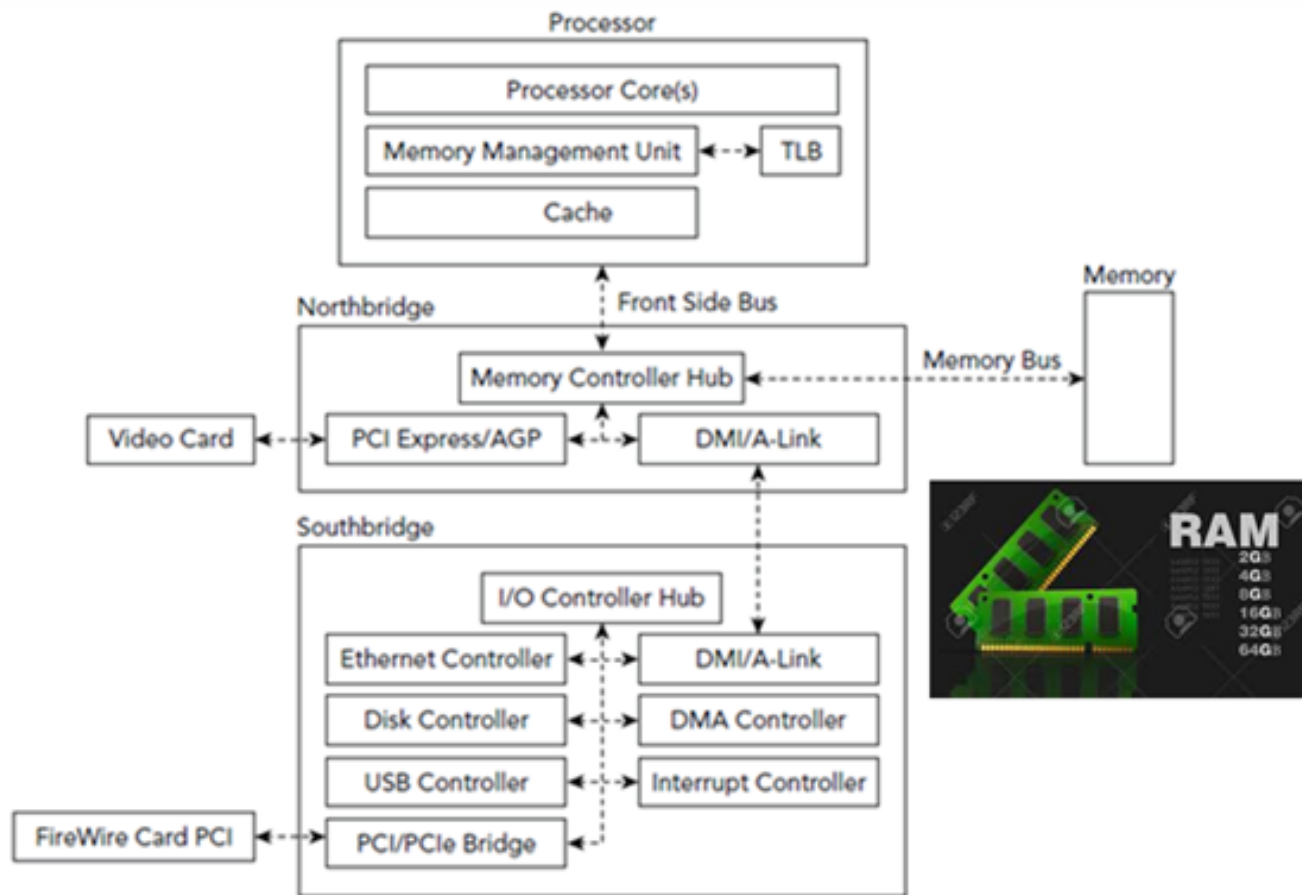
Ciertos ataques, intrusiones y actividades ilícitas no dejan rastros en el disco duro, por lo que sólo será posible encontrar indicios del hecho mediante el análisis de la memoria, por ejemplo identificando qué procesos se estuvieron ejecutando y desde cuándo, que puedan derivar en información relevante para la investigación.

Los datos interesantes que se pueden encontrar en memoria son muy variados, como por ejemplo:

- Procesos: activos, terminados y ocultos
- Hilos (threads)
- Módulos y DLLs
- Archivos abiertos por los procesos
- Conexiones y sockets
- Contenido cifrado
- Claves asociadas a cuentas de usuario
- Entradas del Registry de Windows
- Controladores (drivers)
- Información relacionada con las cuentas de usuario y privilegios

¿Qué es la memoria RAM?

La memoria principal de un computador es conocida como la memoria RAM (*Random Access Memory*) y en los equipos modernos suele ser de varios GB utilizando uno o más chips. Allí se cargan las instrucciones que ejecuta el procesador (CPU), así como los datos de las aplicaciones.

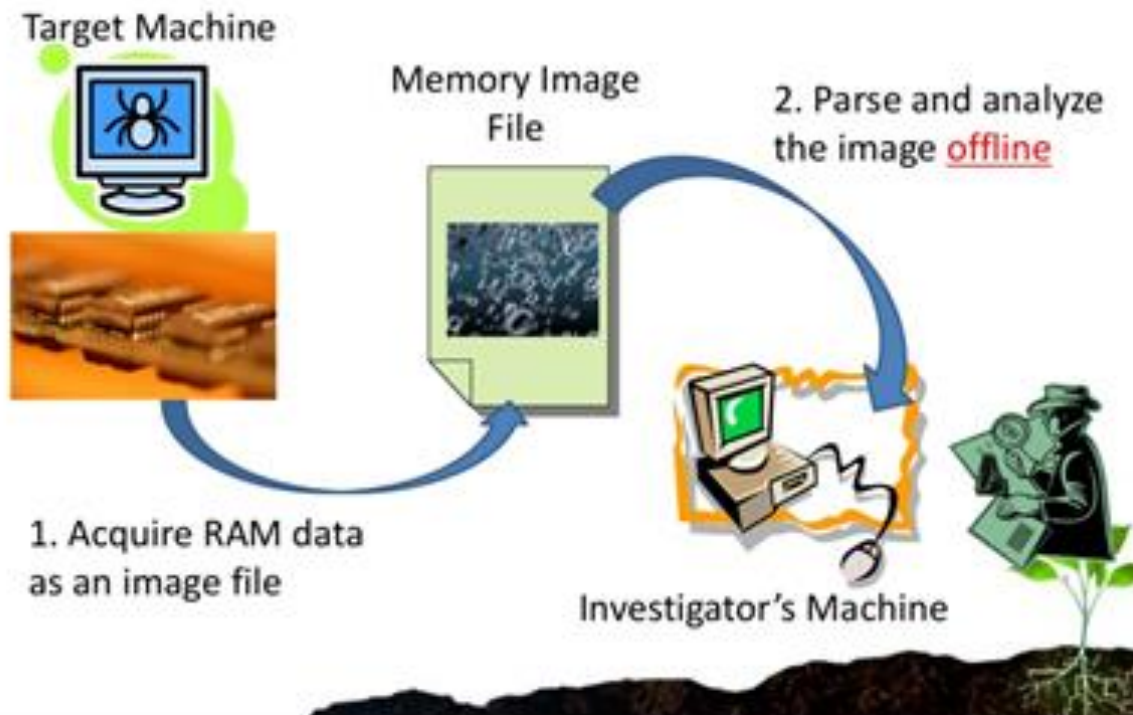


Uno de los principales motivos por los que puede ser necesario la adquisición del contenido de la memoria RAM de un equipo encendido, es descartar la presencia de malware, el cual puede ocasionar que cierta acción parezca realizada por un usuario del equipo a analizar, cuando en realidad es realizada por otro mediante el uso indebido de dicho equipo a distancia.

Este tipo de análisis también permite obtener las claves y contraseñas que estuvieran cargadas en la memoria RAM y que dan indicios de la actividad del usuario.

Otra gran utilidad es el acceso a las claves de cifrado que podrían ser requeridas en el análisis del disco duro del equipo, en caso de que estuviera encriptado.

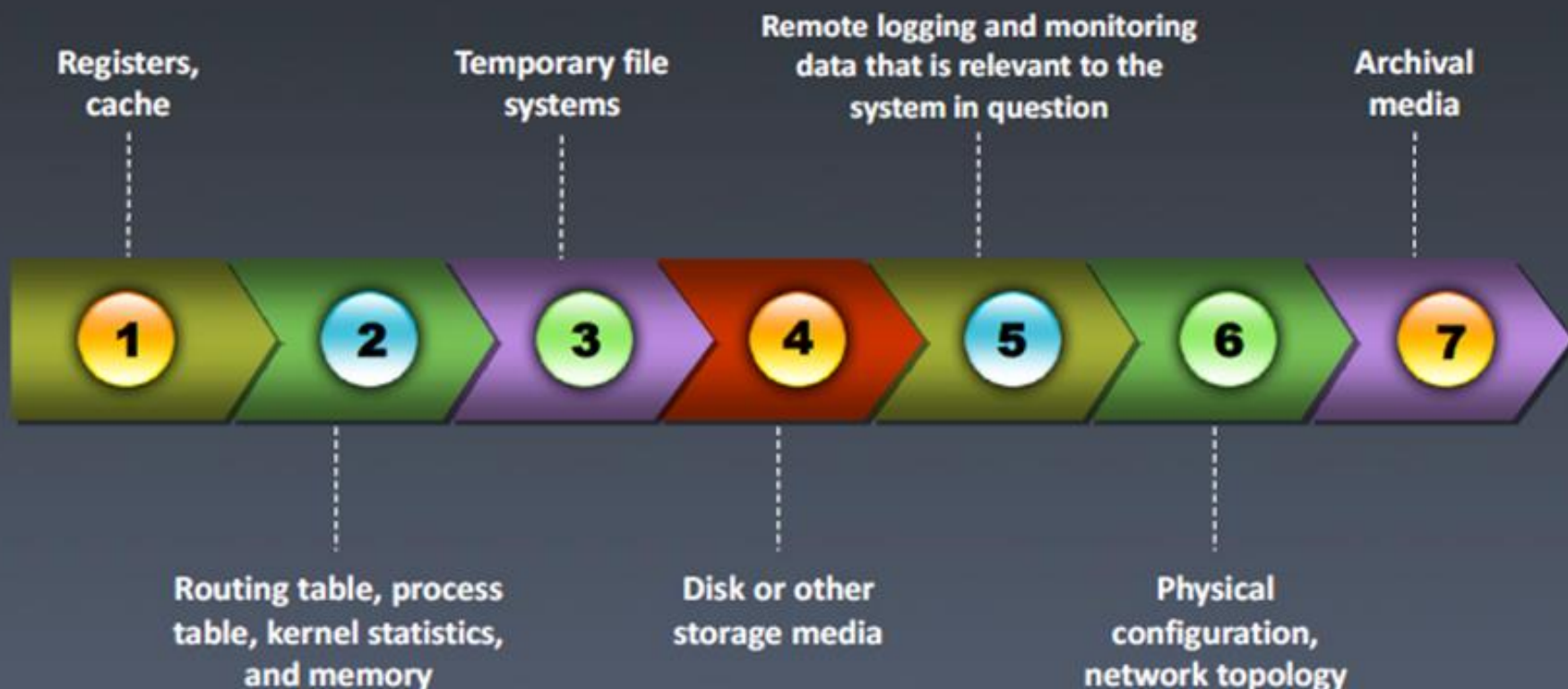
Como la memoria RAM es volátil y si se apaga el equipo, la información que contiene se pierde. Debido a esto, en una investigación, si el equipo está encendido, es posible llevar a cabo el análisis en vivo, pero también existe otra manera: a través de la obtención del volcado de memoria (*memory dump*) donde se copia en un archivo el contenido de toda la memoria en un momento determinado. De esta manera es posible realizar el análisis *post mortem*, con una réplica exacta o "imagen forense" de la memoria del equipo en cuestión.



Order of Volatility

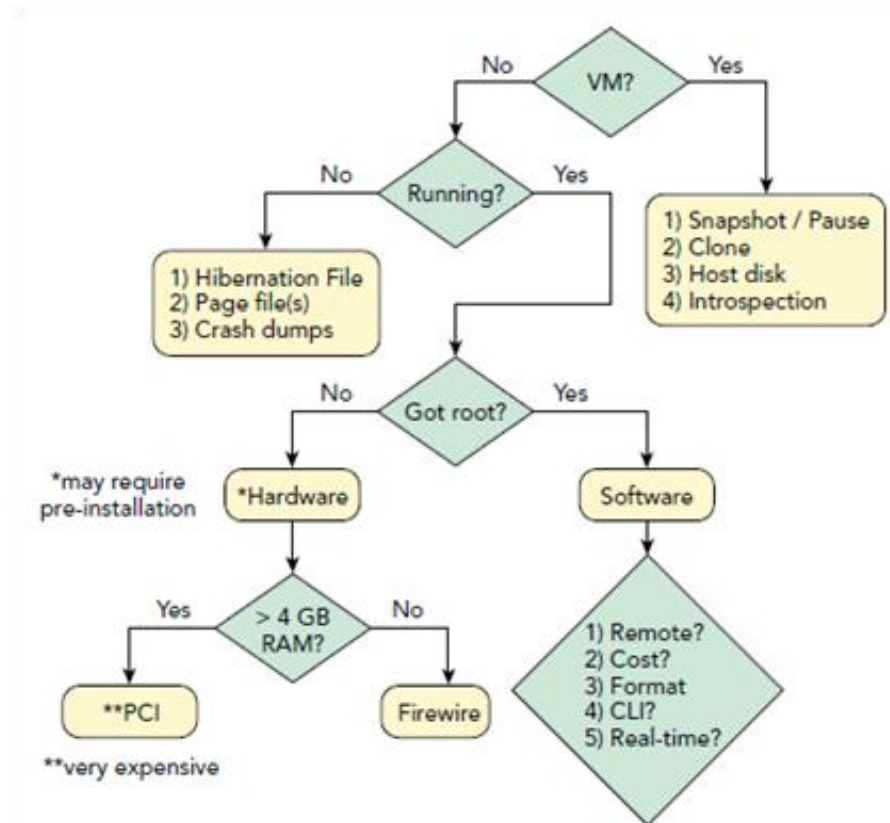


- When collecting evidence, the collection should proceed from the **most volatile to the least volatile**
- The list below is the order of volatility for a typical system:



Herramientas para captura de la memoria

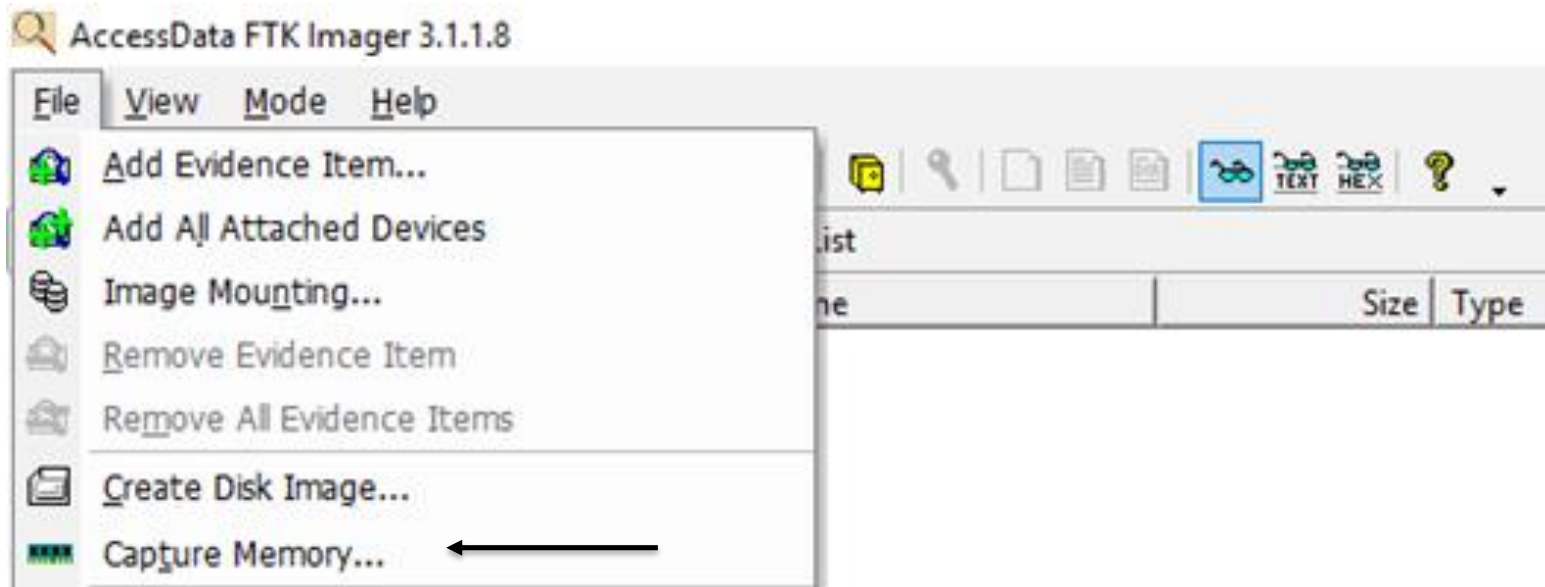
Existen numerosas herramientas comerciales y gratuitas para tal fin, por ejemplo [FTK Imager](#), [DumpIt](#), [Magnet RAM Capture](#), [Live RAM Capturer](#), [F-Response](#), [Memoryze](#), [Redline](#). Una buena lista se encuentra [aquí](#). La mayoría son para Windows. Para Linux se suele utilizar [LiME](#) (Linux Memory Extractor).



FTK Imager

Se trata de una herramienta gratuita muy popular, que forma parte del Forensic Toolkit (FTK) de la empresa AccessData.

Para capturar la memoria RAM es conveniente utilizar FTK Imager Lite, que no requiere instalación, por lo que se puede copiar a un dispositivo externo USB y correr el programa desde allí.



DumpIt

Entre las herramientas más populares que permiten realizar un volcado de memoria, se destaca DumpIt por su sencillez y compatibilidad con las distintas versiones de Windows.

Dumpit no requiere instalación, por lo que se puede copiar a un dispositivo externo USB y correr el programa desde allí. Realiza el volcado de la memoria en el mismo directorio desde donde se ejecuta el programa.

```
DumpIt 3.0.20171123.2
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

Destination path:      \??\C:\Temp\PC-WINDOWS10-20171220-215827.dmp
Computer name:         PC-WINDOWS10

--> Proceed with the acquisition ? [y/n] y

[+] Information:
Dump Type:             Microsoft Crash Dump

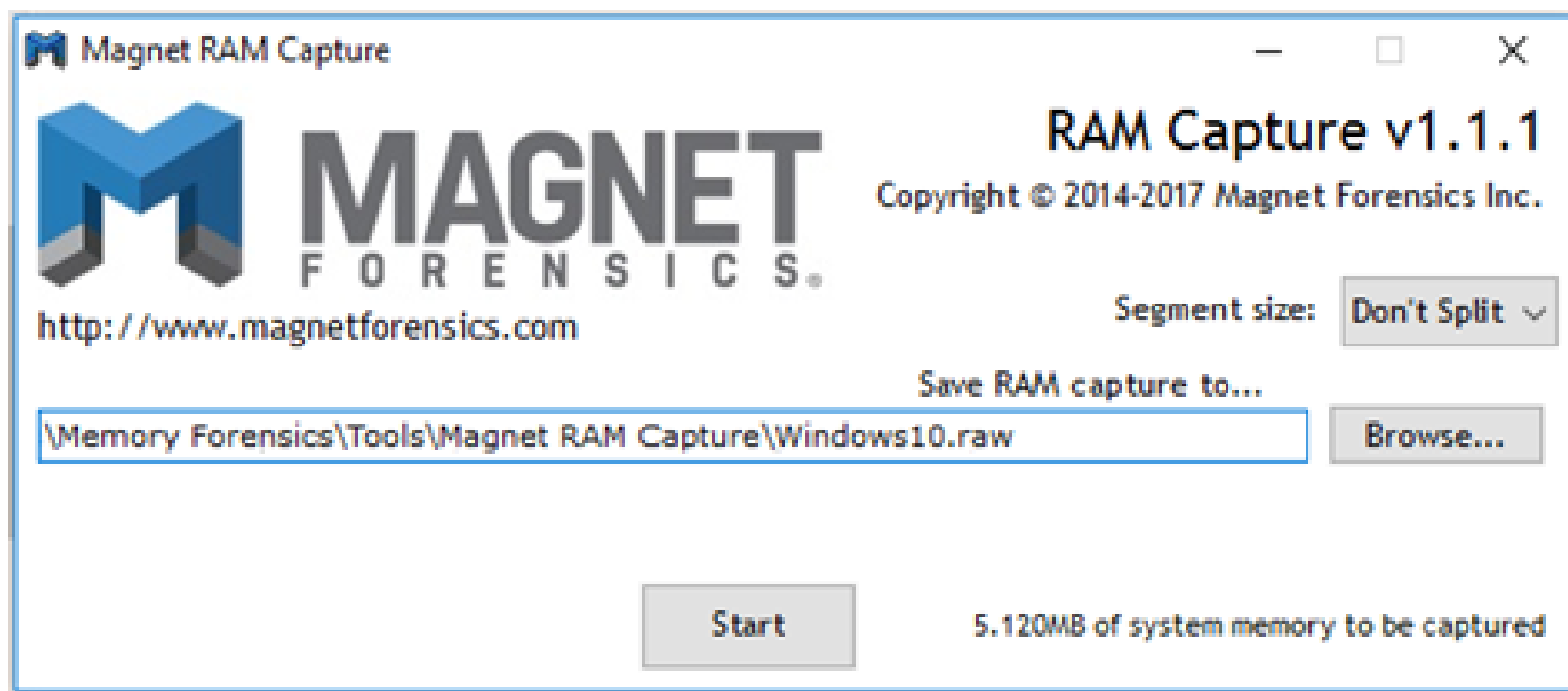
[+] Machine Information:
Windows version:       10.0.14393
MachineId:              00000000-0000-0000-0807-060504030201
TimeStamp:             131582809571121113
Cr3:                   0x1aa000
KdCopyDataBlock:       0xffffffff800d3fdc308
KdDebuggerData:         0xffffffff800d40fa500
KdpDataBlockEncoded:   0xffffffff800d414a108

Current date/time:      [2017-12-20 (YYYY-MM-DD) 22:02:37 (UTC)]
+ Processing... █
```

Magnet RAM Capture

Es una herramienta gratuita de la empresa Magnet Forensics que no requiere instalación, muy liviana (286 KB) y fácil de usar.

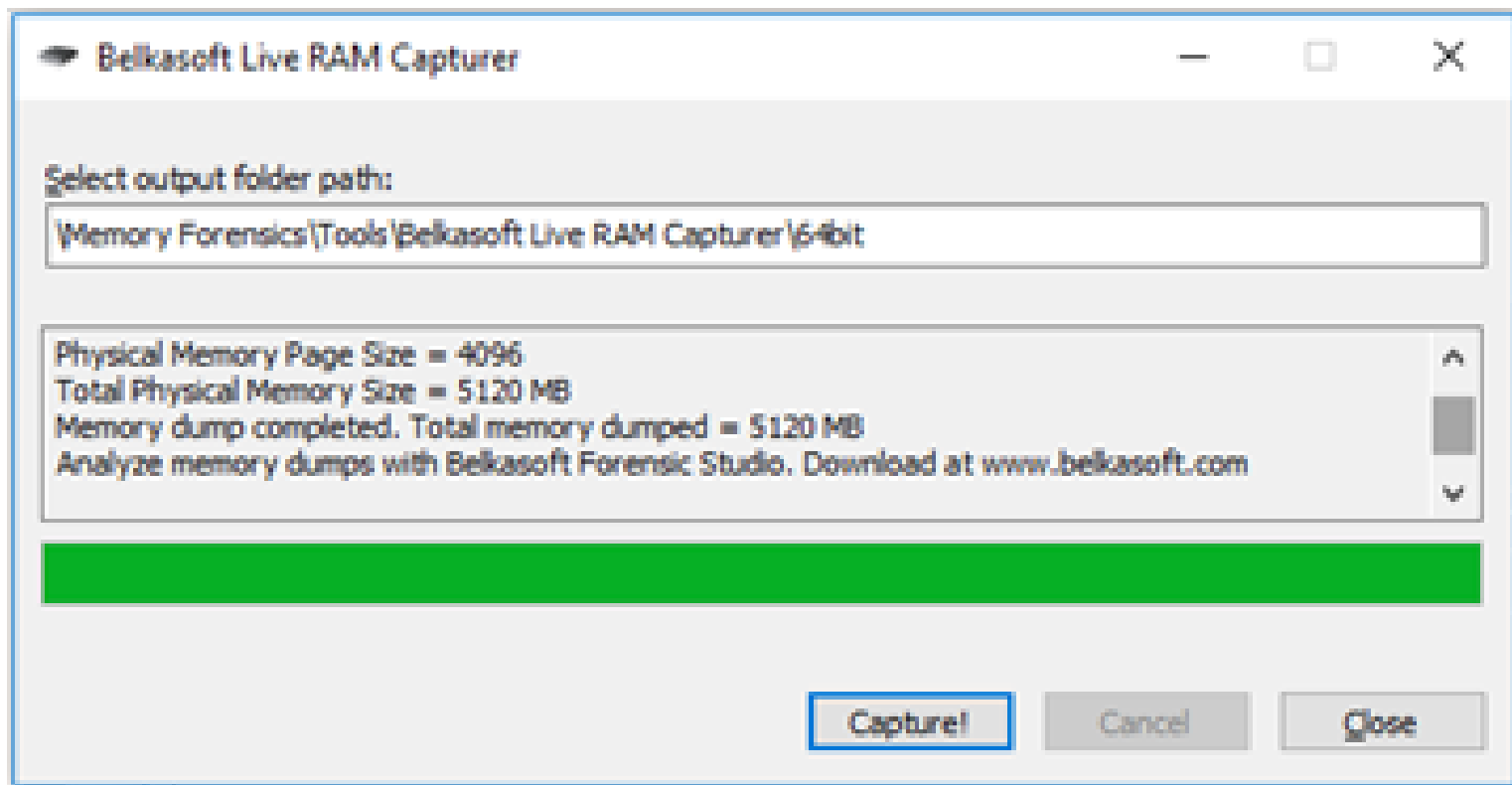
Permite capturar la memoria RAM de sistemas Windows antiguos y modernos, ya sea de 32 bit que de 64 bit.



Belkasoft RAM Capturer

Es una herramienta gratuita de la empresa Belkasoft que no requiere instalación, muy liviana y fácil de usar.

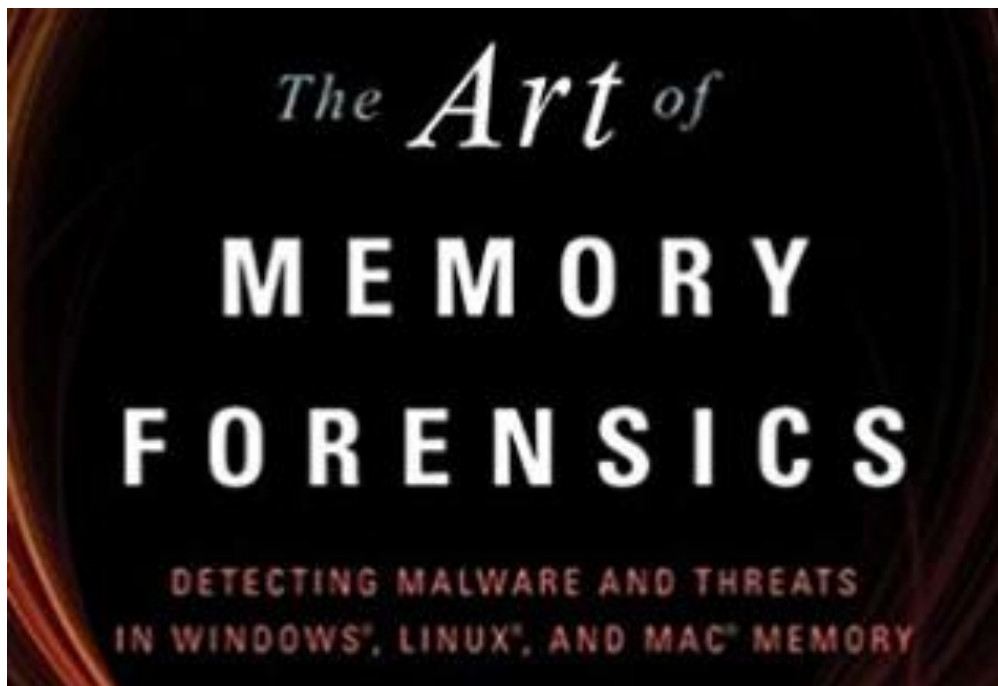
Permite capturar la memoria RAM de sistemas Windows antiguos y modernos, ya sea de 32 bit que de 64 bit.



Análisis de la memoria RAM mediante Volatility Framework

Bajo el patrocinio del [Volatility Foundation](#) un gran número de investigadores y programadores ha ido desarrollando una colección de herramientas open source en lenguaje Python bajo el nombre *Volatility Framework* con el objetivo de facilitar el análisis de la memoria RAM en sistemas Windows, Linux y Mac.

Su uso se explica en detalle en el libro [The Art of Memory Forensics](#).



La potencia de Volatility está dada por más de 200 plugins.

Entre los plugins más populares para Windows se encuentran:
imageinfo, kdbgscan, pslist, pstree, psxview, malfind, svcscan, connections, connscan.

cachedump - Dumps cached domain hashes from memory

cmdline - Display process command-line arguments

cmdscan - Extract command history by scanning for `_COMMAND_HISTORY`

connections - Print list of open connections [Windows XP and 2003 Only]

connscan - Pool scanner for tcp connections

dlllist - Print list of loaded dlls for each process

dumpfiles - Extract memory mapped and cached files

dumpregistry - Dumps registry files out to disk

evtlogs - Extract Windows Event Logs (XP/2003 only)

filescan - Pool scanner for file objects

getsids - Print the SIDs owning each process

hashdump - Dumps passwords hashes (LM/NTLM) from memory

hivedump - Prints out a hive

hivelist - Print list of registry hives.

hivescan - Pool scanner for registry hives

iehistory - Reconstruct Internet Explorer cache / history
imageinfo - Identify information for the image
kdbgscan - Search for and dump potential KDBG values
lsadump - Dump (decrypted) LSA secrets from the registry
malfind - Find hidden and injected code
memdump - Dump the addressable memory for a process
memmap - Print the memory map
moddump - Dump a kernel driver to an executable file sample
modscan - Pool scanner for kernel modules
modules - Print list of loaded modules
printkey - Print a registry key, and its subkeys and values
privs - Display process privileges
procdump - Dump a process to an executable file sample
pslist - Print all running processes by following the EPROCESS lists
psscan - Pool scanner for process objects
pstree - Print process list as a tree
shellbags - Prints ShellBags info
shutdowntime - Print ShutdownTime of machine from registry
sockets - Print list of open sockets
svcsan - Scan for Windows services
userassist - Print userassist registry keys and information
verinfo - Prints out the version information from PE images
volshell - Shell in the memory image
yarascan - Scan process or kernel memory with Yara signatures

The plugin *imageinfo* is used to identify the operating system, service pack, hardware architecture (32 or 64 bit), number of CPUs, time the sample was collected.

There may be more than one profile suggestion if profiles are closely related.

```
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393
          AS Layer1           : Win10AMD64PagedMemory (Kernel AS)
          PAE type            : No PAE
          DTB                  : 0x1aa000L
          KDBG                  : 0xf80055d65500L
          Number of Processors : 2
          Image Type (Service Pack) : 0
          KPCR for CPU 0       : 0xffffffff80055db7000L
          KPCR for CPU 1       : 0xfffffe2017dd26000L
          KUSER_SHARED_DATA    : 0xffffffff78000000000L
          Image date and time   : 2017-12-10 01:03:05 UTC+0000
          Image local date and time : 2017-12-09 21:03:05 -0400
```

Volatility provides several commands for extracting information about processes:

- pslist finds and walks the doubly linked list of processes and prints a summary of the data. This method typically cannot show you terminated or hidden processes.
- pstree takes the output from pslist and formats it in a tree view, so you can easily see parent and child relationships.
- psscan scans for _EPROCESS objects instead of relying on the linked list. This plugin can also find terminated and unlinked (hidden) processes.

Offset(V) it	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xfffffcf034eab26c0	System	4	0	125	0	-----	0	2017-12-09 11:39:18
0xfffffcf0350090800	smss.exe	436	4	2	0	-----	0	2017-12-09 11:39:18
0xfffffcf035158a5c0	smss.exe	616	436	0	-----	0	0	2017-12-09 11:39:39
0xfffffcf0350255300	csrss.exe	624	616	10	0	0	0	2017-12-09 11:39:39
0xfffffcf03515f77c0	smss.exe	700	436	0	-----	1	0	2017-12-09 11:39:39
0xfffffcf03515f4380	wininit.exe	708	616	1	0	0	0	2017-12-09 11:39:39
0xfffffcf0351715080	csrss.exe	720	700	11	0	1	0	2017-12-09 11:39:39
0xfffffcf0351770800	services.exe	796	708	5	0	0	0	2017-12-09 11:39:39
0xfffffcf0351773800	lsass.exe	804	708	7	0	0	0	2017-12-09 11:39:39
0xfffffcf035176d5c0	winlogon.exe	812	700	2	0	1	0	2017-12-09 11:39:39
0xfffffcf035176a800	svchost.exe	920	796	21	0	0	0	2017-12-09 11:39:40
0xfffffcf03517d3580	svchost.exe	984	796	9	0	0	0	2017-12-09 11:39:40
0xfffffcf03517643c0	dwm.exe	648	812	12	0	1	0	2017-12-09 11:39:40
0xfffffcf0351d35400	svchost.exe	1000	796	53	0	0	0	2017-12-09 11:39:40
0xfffffcf035175e800	svchost.exe	1020	796	51	0	0	0	2017-12-09 11:39:40
0xfffffcf0350d563c0	svchost.exe	1060	796	22	0	0	0	2017-12-09 11:39:40

To scan for network artifacts in Windows Vista/7/10 and Windows 2008 Server memory dumps, use the *netscan* plugin. This finds TCP endpoints, TCP listeners, UDP endpoints, and UDP listeners.

It distinguishes between IPv4 and IPv6, prints the local and remote IP (if applicable), the local and remote port (if applicable), the time when the socket was bound or when the connection was established, and the current state (for TCP connections only).

Proto	Local Address	Foreign Address	State	Pid	Owner	Created
UDpv4	0.0.0.0:0	*:*		1020	svchost.exe	2017-12-09
UDpv6	:::0	*:*		1020	svchost.exe	2017-12-09
UDpv4	0.0.0.0:0	*:*		1060	svchost.exe	2017-12-10
UDpv6	fe80::f155:c48b:23ed:d95a:16436	*:*		3260	svchost.exe	2017-12-09
UDpv6	fe80::f155:c48b:23ed:d95a:16436	*:*		3260	svchost.exe	2017-12-09
UDpv4	192.168.250.250:36897	*:*		3260	svchost.exe	2017-12-09
UDpv4	0.0.0.0:0	*:*		5276	Skype.exe	2017-12-09
UDpv6	:::0	*:*		5276	Skype.exe	2017-12-09
UDpv4	0.0.0.0:0	*:*		8168	chrome.exe	2017-12-09
UDpv6	:::0	*:*		8168	chrome.exe	2017-12-09
UDpv4	127.0.0.1:16480	*:*		5276	Skype.exe	2017-12-09
UDpv4	0.0.0.0:0	*:*		5276	Skype.exe	2017-12-09
UDpv6	fe80::c4c4:9f87:3d8b:138b:209	*:*		3260	svchost.exe	2017-12-09
UDpv4	169.254.64.54:53347	*:*		8168	chrome.exe	2017-12-10
UDpv4	0.0.0.0:0	*:*		8168	chrome.exe	2017-12-09
TCPv4	192.168.250.250:5130	40.122.162.208:443	ESTABLISHED	-1		
TCPv4	192.168.250.250:5525	23.34.55.22:443	CLOSE_WAIT	-1		
TCPv4	192.168.250.250:1595	13.107.3.128:443	CLOSED	-1		
TCPv4	192.168.250.250:5155	65.52.108.198:443	ESTABLISHED	-1		
TCPv4	192.168.250.250:9972	204.79.197.222:443	CLOSED	-1		

Obtención de contraseñas mediante Volatility Framework

El archivo que contiene las contraseñas de los usuarios es muy apetecido por los atacantes, pero también es sumamente útil al analista forense, ya con la contraseña se puede ingresar al sistema y analizarlo en vivo.

Windows utiliza el archivo SAM (*Security Account Manager*) para guardar la información relativa a las cuentas de usuario (nombre de usuario, contraseña, descripción del usuario, grupos a los que pertenece, etc.). SAM es el equivalente al archivo `/etc/passwd` de los sistemas Linux/Unix y se encuentra en la carpeta `C:\Windows\System32\Config`.

Ese archivo, así como otros utilizados por el Registro, están ocultos a fin de protegerlos. Además de ser invisible, el archivo SAM está bloqueado, por lo cual no lo puede ni abrir con un editor, ni copiar. La razón es que está siendo utilizado por LSASS (*Local Security Authority Subsystem*). LSASS es el proceso que autoriza y maneja todo el tinglado de las contraseñas utilizadas en Windows.

Las contraseñas se guardan en el archivo SAM mediante hash usando 2 algoritmos distintos.

El primer algoritmo, el hash de LAN Manager (LM), es mucho menos seguro que el segundo, el hash de NTLM. El motivo por el que se utilizan 2 tipo de hash, es para asegurar la compatibilidad con aplicaciones y sistemas operativos anteriores. LM ya no está soportado en Windows Vista/7/8/10, así que hay más seguridad.

Los datos del Registro se guardan físicamente en el disco duro en varios archivos auxiliares llamados hives (por su similitud con una colmena). Los hives contienen una o varias secciones del Registro. En una investigación forense esos archivos son muy valiosos y la mayoría de ellos se encuentran en la carpeta *C:\Windows\System32\Config*.

Sección del Registro	Archivos auxiliares en C:\Windows\System32\Config
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Volatility se aprovecha de que Windows carga el contenido de los hives archivos en la memoria RAM en la medida que los vaya necesitando.

El plugin *hivelist* permite averiguar las direcciones de memoria donde se encuentran esos hives. Seguidamente, con el plugin *hashdump* se procede a extraer los hashes de las contraseñas.

```
INFO      : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86
```

Virtual	Physical	Name
0x87b4ba20	0x3c0c0a20	\Device\HarddiskVolume1\Windows\System32\config\COMPONENTS
0x87b55a20	0x3c192a20	\Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
0x87b7d008	0x3a6a2008	\Device\HarddiskVolume1\Windows\System32\config\SAM ←
0x87b7d6a8	0x3a6a26a8	\Device\HarddiskVolume1\Windows\System32\config\DEFAULT
0x8ab1aa20	0x3c285a20	\Device\HarddiskVolume1\Boot\BCD
0x8f4dba20	0x25828a20	\Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8f565a20	0x251eba20	\Device\HarddiskVolume1\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x90edca20	0x1c1d5a20	\Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0x90f09a20	0x1ab8ea20	\Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x86210008	0x00ac8008	[no name]
0x86226008	0x00a94008	\REGISTRY\MACHINE\SYSTEM ←
0x86246008	0x00a76008	\REGISTRY\MACHINE\HARDWARE
0x87b17a20	0x3c1f5a20	\Device\HarddiskVolume1\Windows\System32\config\SECURITY

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:63d6a39b8467b94ae92ab1931d4079dd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1005:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
hacker:1006:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
```

Búsqueda de malware mediante Volatility Framework

Frecuentemente se recurre a Volatility cuando se sospecha que un equipo ha sido infectado por un malware y hay que evitar que haga mayores daños, por ejemplo infectando otros equipos.

Para tal fin se utiliza el plugin *pslist* para averiguar si hay algún proceso o programa sospechoso corriendo en el equipo al momento de efectuar la captura.

Como ejemplo, revisando la siguiente lista, se descubre que hay 3 instancias de *lsass.exe*, cuando normalmente debería haber una sola instancia.

0x81da5650	winlogon.exe	624	376	19	570	0	0	2010-10-29	17:08
0x82073020	services.exe	668	624	21	431	0	0	2010-10-29	17:08
0x81e70020	lsass.exe	680	624	19	342	0	0	2010-10-29	17:08
0x823315d8	vmacthlp.exe	844	668	1	25	0	0	2010-10-29	17:08
0x81db8da0	svchost.exe	856	668	17	193	0	0	2010-10-29	17:08
0x8210d478	jusched.exe	1712	1196	1	26	0	0	2010-10-29	17:11
0x82279998	imapi.exe	756	668	4	116	0	0	2010-10-29	17:11
0x822b9a10	wuauclt.exe	976	1032	3	133	0	0	2010-10-29	17:12
0x81c543a0	Procmon.exe	660	1196	13	189	0	0	2011-06-03	04:25
0x81fa5390	wmiprvse.exe	1872	856	5	134	0	0	2011-06-03	04:25
0x81c498c8	lsass.exe	868	668	2	23	0	0	2011-06-03	04:26
0x81c47c00	lsass.exe	1928	668	4	65	0	0	2011-06-03	04:26
0x81c0cda0	cmd.exe	968	1664	0	-----	0	0	2011-06-03	04:31

LSASS = Local Security Authority Subsystem Service

Para aprender más

ANÁLISIS DE DATOS VOLÁTILES EN WINDOWS
Análisis de Memoria RAM

ANÁLISIS MEMORIA RAM

Contiene información volátil y frágil ya que se libera y reasigna de forma dinámica



YouTube


Análisis de datos volátiles en Windows

Memoria RAM

- La memoria RAM es una fuente muy importante de información en un proceso forense.
- La información, además de volátil, es frágil, poco de libre y se reasigna de forma dinámica.

Herramientas utilizadas:

- MD5 - Hashes de la memoria RAM
- Volatility - Framework para el análisis de los volátiles RAM



La memoria RAM es una memoria que por su naturaleza se considera volátil.



ANÁLISIS DE DATOS VOLÁTILES EN WINDOWS
Práctica: Análisis de conexiones - Puertos y Conexiones abiertos

YouTube

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601.1
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\INCIBE>
```

El primer comando a ejecutar sería "netstat" con el parámetro "-a", para ver los puertos y las conexiones abiertas en el sistema.

27:07 / 52:08



Video: Introduction to Windows Memory Analysis



Why Memory Forensics?

Everything in the OS traverses RAM

- Network sockets, URLs
- Windows Registry keys
- Hardware configuration
- Passwords, caches, clipboards
- User generated content
- **Malware**



Volatility “Malfind” (Stuxnet)

“If you have a problem, if no one else can help...”

```
root@SIFT-Workstation: /memory
File Edit View Terminal Help
root@SIFT-Workstation:/memory# vol.py -f stuxnet.img malfind --dump-dir ./output_dir/
Volatile Systems Volatility Framework 2.1_alpha
Name      Pid      Start      End      Tag      Hits      Protect
lsass.exe 868      0x00080000 0xf9fff000 Vad      0      PAGE_EXECUTE_READWRITE
Dumped to: ./output_dir/lsass.exe.le498c8.00080000-000f9fff.dmp
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00080020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00080030 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 .....
0x00080040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 .....!.L.!Th
0x00080050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
0x00080060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
0x00080070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.
lsass.exe 1928      0x00080000 0xf9fff000 Vad      0      PAGE_EXECUTE_READWRITE
Dumped to: ./output_dir/lsass.exe.le47c00.00080000-000f9fff.dmp
0x00080000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00080010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00080020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00080030 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 .....
0x00080040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 .....!.L.!Th
0x00080050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
0x00080060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
0x00080070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.
vol.py -f stuxnet.img malfind --dump-dir output_dir
```





Hacks Weekly #6:

Memory Dump Analysis – Extracting Juicy Data

CQURE
ACADEMY

In this post, I will show you how to perform memory dump and how to, by using different types of tools, extract information from the memory dump. Paula Januszkiewicz.





Básica

Criptografía y Esteganografía

Exploiting

Forense

Hacking Web

Análisis de Tráfico

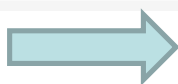
Reversing

Extra

Memory Analysis (150pts)**Dificultad:** ★★★☆☆

Una de las redes internas de cierta organización ha sido víctima de una intrusión. Un IDS ha identificado tráfico inusual que podría reflejar movimientos laterales a otros equipos de la misma red. Se sospecha que los equipos que conforman dicha VLAN hayan podido ser comprometidos. Para investigar el incidente en detalle se ha hecho un volcado de memoria (memory.1221191d.img) de uno de los equipos de la red con el objetivo de obtener información sobre la vía de infección y poder así crear los indicadores de compromiso pertinentes. El analista deberá de investigar el fichero de memoria y tratar de contestar las siguientes cuestiones.

¿Qué vulnerabilidad (CVE-XXXX-XXXX) se ha utilizado para explotar la máquina?

 memory.1221191d.img.zipMemory Analysis Part 2 (150pts)Malware sobre Windows 7 (100pts)

"The most useful technical security book I've read this year. A must-have for all who protect systems from malicious software."

Lenny Zeltser, Security Practice Director at Savvis and Senior Faculty Member at SANS Institute

"The ultimate guide for anyone interested in malware analysis."

Ryan Olson, Director, VeriSign/Defense Rapid Response Team

"Every page is filled with practical malware knowledge, innovative ideas, and useful tools. Worth its weight in gold!"

Aaron Walters, Lead Developer of VirusShare and VP of Security R&D at Tenenock

Malware Analyst's Cookbook and DVD

TOOLS AND TECHNIQUES FOR FIGHTING MALICIOUS CODE

Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard



Professional Expertise Distilled

Windows Malware Analysis Essentials

Master the fundamentals of malware analysis for the Windows platform and enhance your anti-malware skill set

Victor Marak

[PACKT] enterprise 
PUBLISHING professional expertise distilled

SYNGRESS

MALWARE FORENSICS FIELD GUIDE FOR WINDOWS SYSTEMS

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina



SYNGRESS.

MALWARE FORENSICS FIELD GUIDE FOR LINUX SYSTEMS

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina



FREE E-BOOK DOWNLOAD

Malware Forensics

Investigating and Analyzing Malicious Code

The Only Practical, Hands-On Guide to Malicious Code Investigation!

- Collect and Examine Volatile Data from Live Windows and Linux Systems
- Analyze Physical and Process Memory Dumps for Malware Artifacts on Windows and Linux Systems
- Discover and Extract Artifacts from UNIX and Windows Systems

James M. Aquilina
Eoghan Casey
Cameron H. Malin

Curtis W. Rose Technical Editor

"A harrowing guide to where the bad guys hide, and how you can find them."

—Dan Kaminsky, Director of Penetration Testing, IOActive

HACKING

Malware & Rootkits

EXPOSED™

Malware & Rootkits Secrets & Solutions

Michael A. Davis Sean M. Bodmer Aaron LeMasters

Práctica de adiestramiento usando Volatility Framework

Análisis forense de la Memoria RAM

Ing. Vincenzo Mendillo

Objetivo: Familiarizarse con las técnicas para capturar y almacenar los datos volátiles que se encuentran en la memoria RAM de un computador y luego analizarlos con herramientas especializadas como Volatility Framework, para así detectar la posible infección por malware o para rastrear la actividades de un intruso en el sistema o para extraer las evidencias de actividades ilícitas por parte del propio usuario.



Incidentes de Seguridad y Forénsica Digital



Información sobre el curso
Inscripción y formas de pago
Examen demostrativo
Examen real
Exámenes realizados
El perito forense
Memorias de un perito forense
Análisis forense en Windows
Análisis forense en dispositivos móviles
Certificaciones Profesionales
Computer Hacking Forensic Investigator (CHFI)
Certified Cyber Forensics Professional (CCFP)
Certified Computer Forensics Examiner (CCFE)
CyberSecurity Forensic Analyst (CSFA)
GIAC Forensics Certifications
Cursos de formación profesional



CSIRT
EQUIPO DE RESPUESTA A
INCIDENTES DE SEGURIDAD
DE LA INFORMACIÓN





Seguridad de la Información



Información sobre el curso

Breve video de presentación

Inscripción y formas de pago

Examen demostrativo

Examen parcial (real)

Examen general (real)

Exámenes realizados

Certificaciones Profesionales

Certificación PCSI

CISSP/CISM/SSCP/CCFP

CISA/CISM/CSX

Certified Ethical Hacker

Computer Hacking Forensic Investigator (CHFI)

Certified Cyber Forensics Professional (CCFP)

CompTIA Security+

ASOVESINFO

Diplomado STIT

Cursos de formación profesional



XSS
Cross Site Scripting

SQL
Inyección



Tor



Informática Forense

VOIP

WPA / WPA2



Fin de la charla:

Análisis Forense de la Memoria RAM

¡¡Muchas gracias por su atención!!



JIFI2018

Facultad de
Ingeniería



Prof. Vincenzo Mendillo

<http://mendillo.info>

vmendillo@ieee.org

Twitter: @vmendillo

