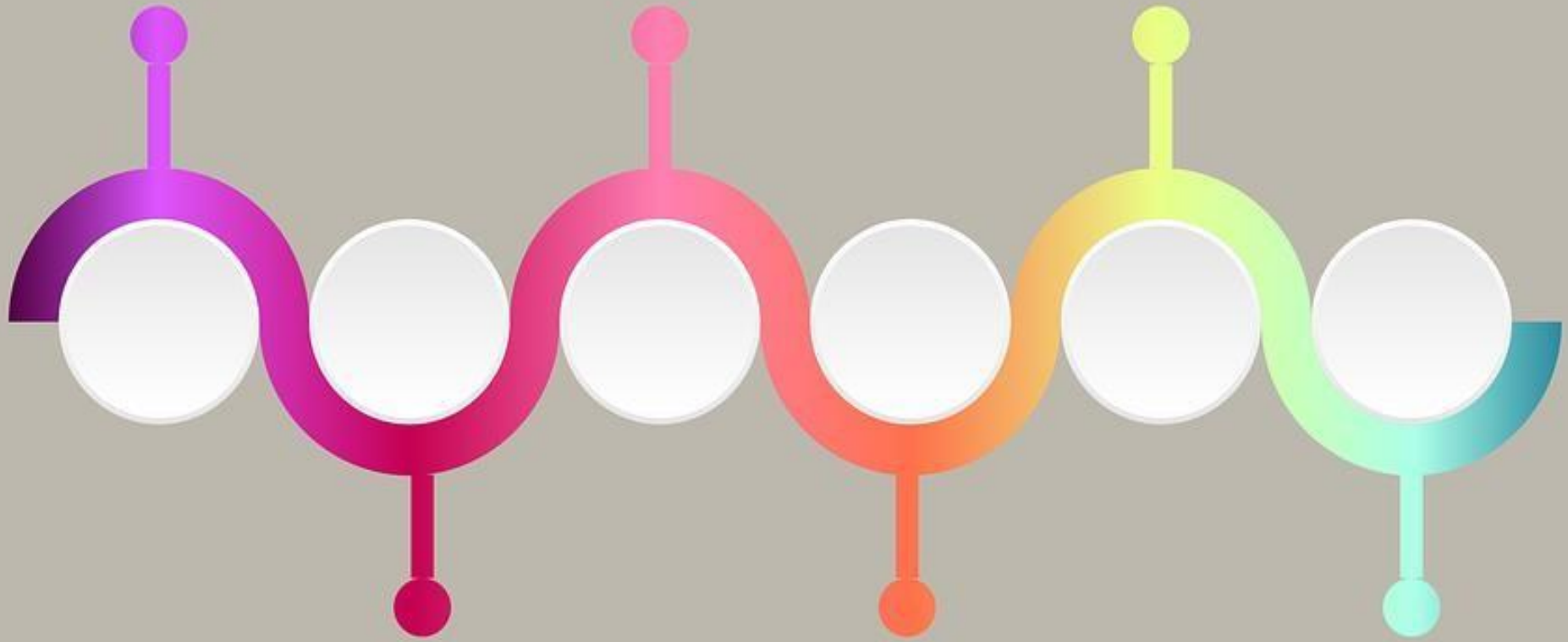

DIGITAL FORENSICS

Índice

Introducción

- **Objetivos**
  - ¿**Qué** hechos han ocurrido?
  - ¿**Quién** ha realizado los hechos?
  - ¿**Cómo** se han realizado?
  - ¿**Cuándo** se han realizado?

Acotar la investigación a un rango temporal



Definir el **alcance** de la investigación

Reconstruir la **línea temporal**

Buenas prácticas

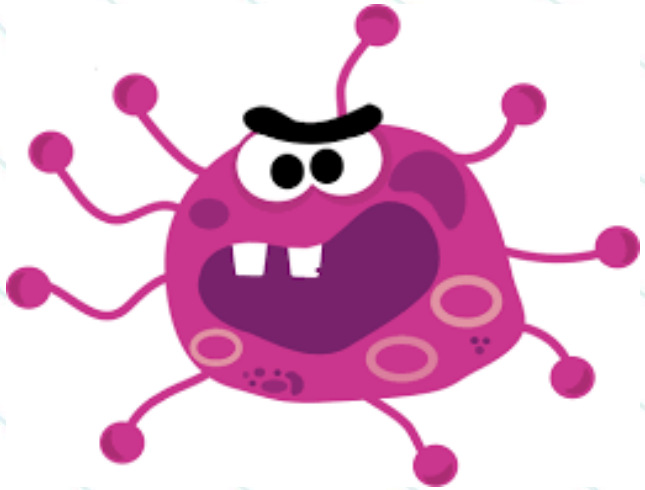
Copias de seguridad: clonado + copia (+copia)

If paranoic==ON then

Utilizad herramientas ligeras

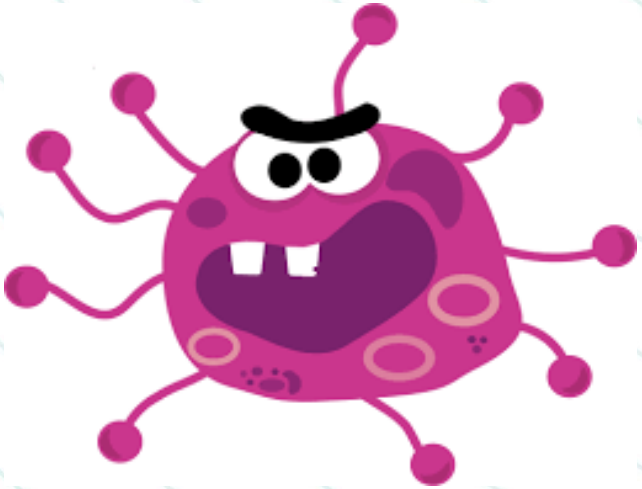
Buenas prácticas

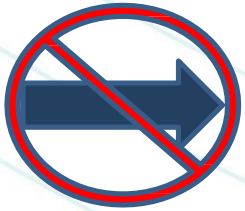
Si infectado con malware → no analizar el equipo con antimalware!



Buenas prácticas

No subir muestras a VT, Hybrid analysis, anyrun…





VirusTotal

Buenas prácticas

Adquiere tantas evidencias como sea posible

Buenas prácticas

Documentación de TODO lo que se haga

Distribuciones Linux forense

SIFT

deft

PALADIN Forensic Suite

The World's Most Popular Linux Forensic Suite

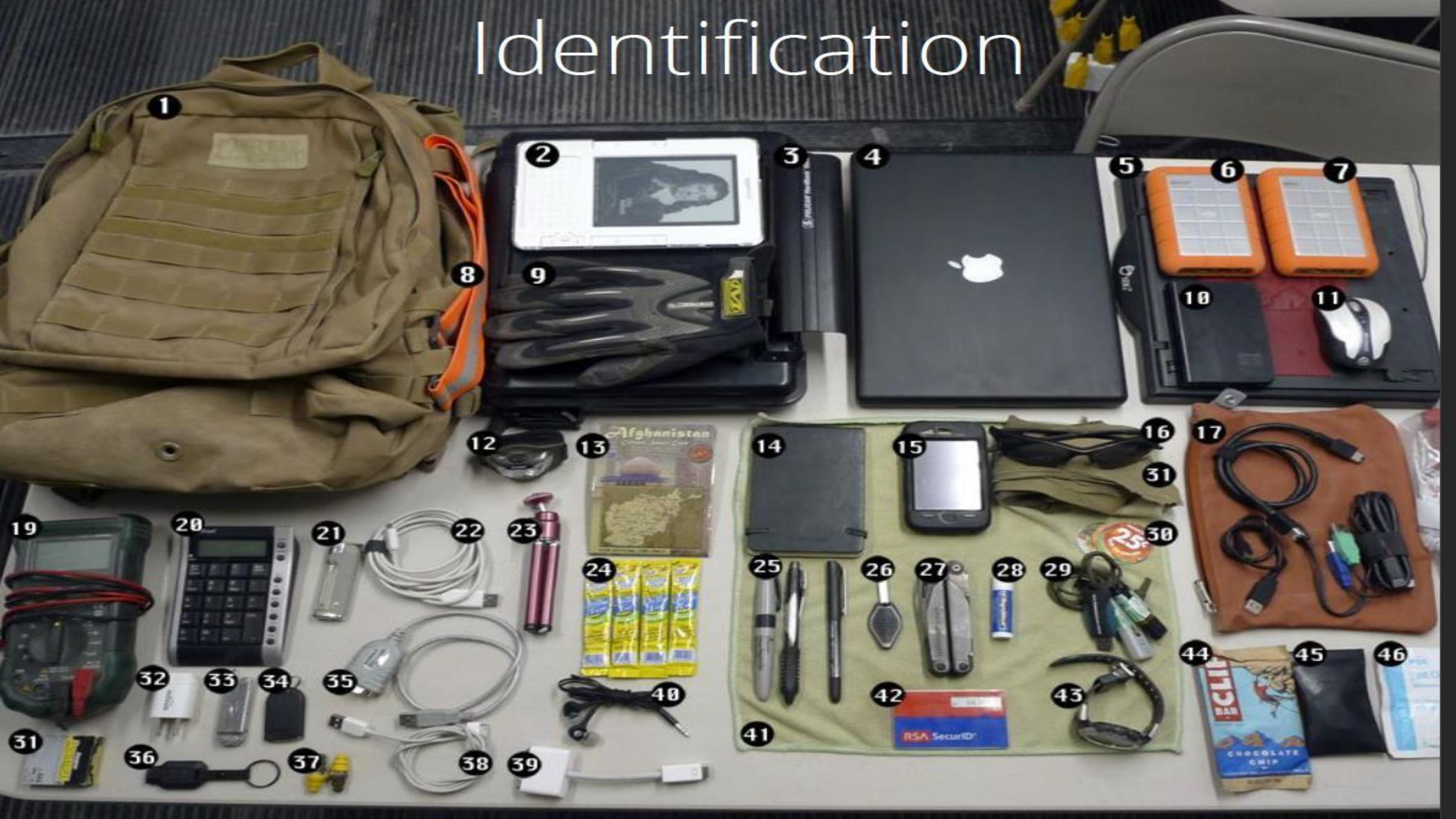
Fases del análisis

Identificación Y adquisición → Preservar → Análisis → Informe

Fases del análisis

Identificación y adquisición → **Preservar** → **Análisis** → **Informe**

Identification



Adquisición

- **Fotografiar la escena**
- **Elementos volátiles**
  - Conexiones de red, procesos…
  - Adquisición memoria RAM
- **Adquisición Disco duro**
  - DESCONECTAR EL CABLE y clonar
- **Pen drives, CDs, DVDs, logs..**

Más Volátil

Menos Volátil

Adquisición evidencias volátiles

- **Fecha**
  - date /t > FechaYHoraDeInicio.txt &time /t >> "FechaYHoraDeInicio.txt"
- **Conexiones de red / información de red**
  - netstat -an | findstr /i "estado listening established" > "PuertosAbiertos.txt"
  - netstat -anob > "AplicacionesConPuertosAbiertos.txt"
  - ipconfig /all > "EstadoDeLaRed.txt"
  - nbtstat -S > "ConexionesNetBIOSEstablecidas.txt"
  - net sessions > "SesionesRemotasEstablecidas.txt"
  - ipconfig /displaydns > "DNSCache.txt"
  - arp -a > "ArpCache.txt"

Adquisición evidencias volátiles

- **Procesos**
  - tasklist > “ProcesosEnEjecución.txt”
  - pslist -t > “Procesos.txt”
  - listdlls > “dlls.txt”
  - handle -a > “Handles.txt”
- **Servicios**
  - sc query > “ServiciosEnEjecución.txt”
- **Tareas programadas**
  - schtasks > “TareasProgramadas.txt”

Adquisición evidencias volátiles

- **Usuarios**
  - netUsers.exe > "UsuariosActualmenteLogueados.txt"
  - netUsers.exe /History > "HistoricoUsuariosLogueados.txt"
- **Portapapeles**
  - InsideClipboard /saveclp > "Portapapeles.clp"
- **Histórico de comandos (cmd)**
  - doskey /history > "HistoricoCMD.txt"
- **Unidades mapeadas**
  - net use > "UnidadesMapeadas.txt"
- **Carpetas compartidas**
  - net share > "CarpetasCompartidas.txt"

Adquisición de evidencias

Adquisición memoria RAM

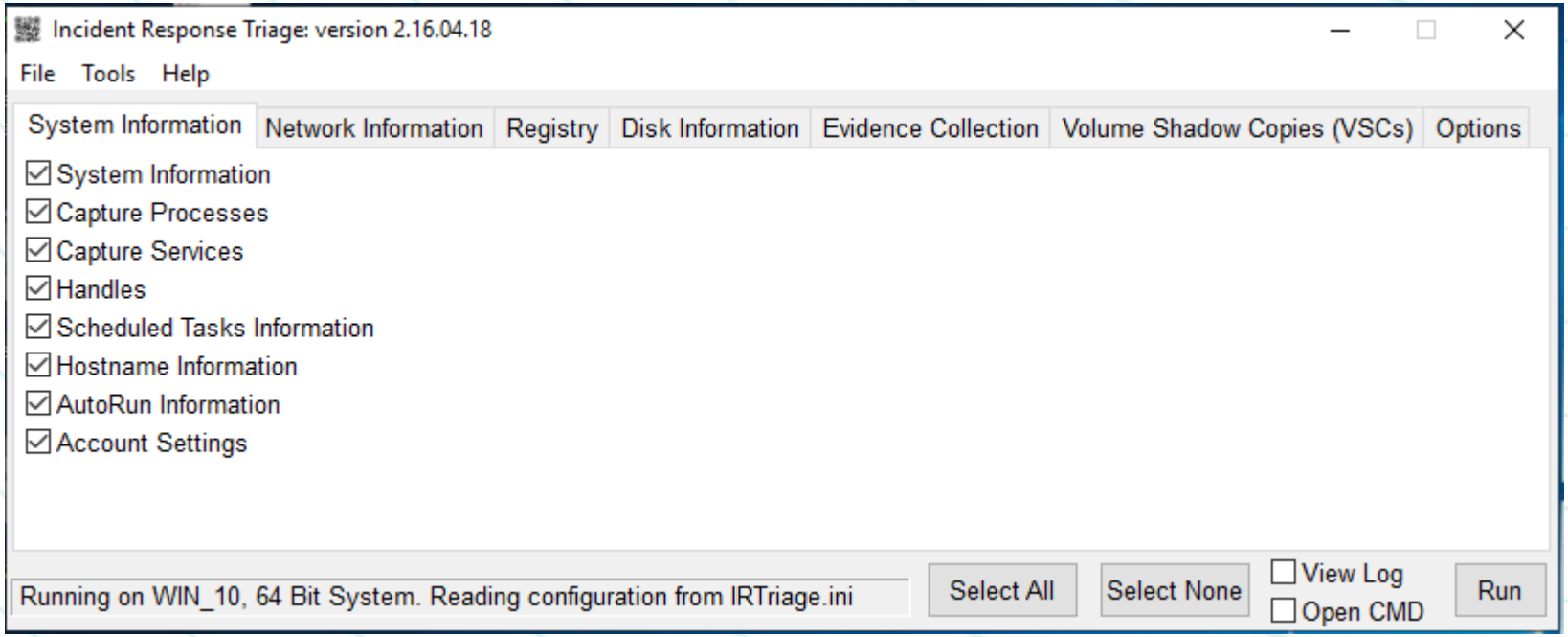
```
DumpIt 3.0.20171010.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\C:\Users\u                    ?\Documents\Tools_forensic\Adquisicion\Comae-Toolkit-3.0
.20171010.1\Comae-Toolkit\x64\PORTATIL0162-20191128-133754.dmp

  Computer name:              PORTATIL0162


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

Adquisición de evidencias

- **Análisis en vivo**
- **Malware oculto a aplicaciones del sistema**
- **Utilizar herramientas de terceros**
- **Tools**
  - Nirsoft nirlauncher
  - Sysinternals suite

Adquisición de evidencias – Triage

- **Adquisición evidencias volátiles y No volátiles**
- **Enfocado para Incident response**



Adquisición de evidencias – No volátiles

- **Adquisición en frío (post mortem)**
- **Copia bit a bit de todo el disco**
- **Herramientas de clonado**
  - Hardware : Clonadora
  - Software: distribuciones Linux (Live CD / USB)

Adquisición de evidencias – No volátiles

- **Clonado de disco mediante Hardware**

Adquisición de evidencias – No volátiles

Clonado de disco mediante Software con bloqueador de escritura

Adquisición de evidencias – No volátiles

- **Clonado de discos mediante software con Live CD**
  - Iniciar Live CD
  - Montar origen como sólo lectura sólo si es necesario
  - Clonar con dd / dcfldd
  - Destino disco externo (USB 3.0)

  - dcfldd if=/dev/xx of=/media/disco_dst/imagen.dd hash=sha1 hashlog=/media/disco_dst/imagen.log

Fases del análisis

Identificación y adquisición → **Preservar** → Análisis → Informe

Preservación de evidencias

Cálculo de hashes

Fases del análisis

Identificación y adquisición → Preservar → **Análisis** → Informe

Análisis memoria RAM

- Caso práctico

- El director de una compañía nos informa que ha abierto un documento y el ordenador ha hecho “cosas raras”

- Definir Cómo ha ocurrido, cuando, y alcance del incidente

Análisis memoria RAM

- Conexiones activas (TCP, UDP, Puertos…)
- Ficheros (dlls, ejecutables, documentos abiertos…)
- Direcciones web, emails, contraseñas
- Comandos escritos por consola
- Contraseñas del sistema
- Elementos ocultos: rootkits
- [...]

Análisis memoria RAM

- **Hiberfil.sys**
  - Contiene imagen raw comprimida
  - Analizar con volatility

- **Pagefile.sys (swapping)**
  - Buscar palabras clave
  - Strings pagefile.sys >> strings_pagefile.txt
  - Grep “cadena” strings_pagefile.txt
  - En Win10: Swapfile.sys

Análisis memoria RAM

Vol.py –f memoria.raw --profile=Win7SP1x64 pslist

```
0xfffffa80192ab060 userinit.exe          2504    436      0 --------      1      0 2018-04-07 08:37:14 UTC+0000   2018-04-07 08:37:45 UTC+0000
0xfffffa8019c52b10 dwm.exe               2512    832      5      126      1      0 2018-04-07 08:37:14 UTC+0000
0xfffffa801a790060 explorer.exe          2536   2504     41     1158      1      0 2018-04-07 08:37:14 UTC+0000
0xfffffa801922e620 vmtoolsd.exe          2616   2536      6      186      1      0 2018-04-07 08:37:17 UTC+0000
0xfffffa801916f720 cmd.exe               2820   2536      1       20      1      0 2018-04-07 08:37:22 UTC+0000
0xfffffa8019182060 conhost.exe           2828    400      2       63      1      0 2018-04-07 08:37:22 UTC+0000
0xfffffa801913cb10 SearchIndexer.        2864    496     13      841      0      0 2018-04-07 08:37:23 UTC+0000
0xfffffa80194d5650 SearchProtocol        2968   2864      0 --------      0      0 2018-04-07 08:37:26 UTC+0000   2018-04-07 08:41:37 UTC+0000
0xfffffa8019748b10 SearchFilterHo        2992   2864      0 --------      0      0 2018-04-07 08:37:26 UTC+0000   2018-04-07 08:40:26 UTC+0000
0xfffffa801a5b9360 svchost.exe           1944    496     14      225      0      0 2018-04-07 08:38:21 UTC+0000
0xfffffa801a17bb10 wmpnetwk.exe          1744    496      9      209      0      0 2018-04-07 08:38:22 UTC+0000
0xfffffa8019c45b10 mscorsvw.exe          2476    496      6       87      0      1 2018-04-07 08:39:03 UTC+0000
0xfffffa801a819b10 mscorsvw.exe          2788    496      6       78      0      0 2018-04-07 08:39:03 UTC+0000
0xfffffa801a81a600 svchost.exe           2908    496     13      361      0      0 2018-04-07 08:39:03 UTC+0000
0xfffffa801a745320 TrustedInstall        1980    496      4      120      0      0 2018-04-07 08:39:51 UTC+0000
0xfffffa801a831b10 PING.EXE              1940   2820      0 --------      1      0 2018-04-07 08:40:01 UTC+0000   2018-04-07 08:40:03 UTC+0000
0xfffffa801a8d7b10 OSPPSVC.EXE           1136    496      6      128      0      0 2018-04-07 08:42:08 UTC+0000
0xfffffa801ab2cb10 python.exe            3020   2536      0 --------      1      0 2018-04-07 08:42:14 UTC+0000   2018-04-07 08:47:34 UTC+0000
0xfffffa801ab35350 conhost.exe           1760    400      0 --------      1      0 2018-04-07 08:42:15 UTC+0000   2018-04-07 08:47:34 UTC+0000
0xfffffa801aa38b10 explorer.exe          1132    620      0 --------      1      0 2018-04-07 08:44:09 UTC+0000   2018-04-07 08:45:10 UTC+0000
0xfffffa801a9c8600 vfgggggg.exe          3208   1132      0 --------      1      0 2018-04-07 08:44:09 UTC+0000   2018-04-07 08:44:38 UTC+0000
0xfffffa801a9c6b10 vfgggggg.exe          2072   3208     23      396      1      1 2018-04-07 08:44:25 UTC+0000
0xfffffa801aec0b10 WmiPrvSE.exe          3632    620     13      333      0      1 2018-04-07 08:44:42 UTC+0000
0xfffffa801b55e060 WmiApSrv.exe          3476    496      5      112      0      0 2018-04-07 08:44:50 UTC+0000
0xfffffa801ae88060 WmiPrvSE.exe          3080    620      7      211      0      1 2018-04-07 08:44:55 UTC+0000
0xfffffa801afbc060 SearchProtocol        2952   2864      7      284      0      0 2018-04-07 08:45:39 UTC+0000
0xfffffa801a91f550 SearchFilterHo        2676   2864      5      104      0      0 2018-04-07 08:45:39 UTC+0000
```

Análisis memoria RAM

Vol.py –f memoria.raw --profile=Win7SP1x64 netscan

```
0x7e7d69b0         UDPv6    :::54792                        *:*                                    864      svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7d8010         UDPv6    ::1:54794                       *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7ec330         UDPv6    fe80::fc4b:861d:db18:9601:54793 *:*                                     1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7eca00         UDPv4    192.168.25.128:54795            *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7edd00         UDPv4    127.0.0.1:54796                 *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7ee010         UDPv6    fe80::fc4b:861d:db18:9601:1900  *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7ee870         UDPv6    ::1:1900                        *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7f0010         UDPv4    192.168.25.128:1900             *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7f0950         UDPv4    127.0.0.1:1900                  *:*                                    1944     svchost.exe    2018-04-07 08:38:22 UTC+0000
0x7e7f5520         UDPv4    0.0.0.0:3702                    *:*                                    864      svchost.exe    2018-04-07 08:39:03 UTC+0000
0x7e7f5520         UDPv6    :::3702                         *:*                                    864      svchost.exe    2018-04-07 08:39:03 UTC+0000
0x7e44c700         TCPv4    192.168.25.128:139              0.0.0.0:0              LISTENING       4        System
0x7e7e5010         TCPv4    0.0.0.0:49155                   0.0.0.0:0              LISTENING       496      services.exe
0x7e7e5010         TCPv6    :::49155                        :::0                   LISTENING       496      services.exe
0x7e8a4010         TCPv4    0.0.0.0:49155                   0.0.0.0:0              LISTENING       496      services.exe
0x7ead2360         TCPv4    0.0.0.0:445                     0.0.0.0:0              LISTENING       4        System
0x7ead2360         TCPv6    :::445                          :::0                   LISTENING       4        System
0x7ee61630         TCPv4    0.0.0.0:49154                   0.0.0.0:0              LISTENING       912      svchost.exe
0x7ee63a80         TCPv4    0.0.0.0:49154                   0.0.0.0:0              LISTENING       912      svchost.exe
0x7ee63a80         TCPv6    :::49154                        :::0                   LISTENING       912      svchost.exe
0x7f372c40         TCPv4    0.0.0.0:5357                    0.0.0.0:0              LISTENING       4        System
0x7f372c40         TCPv6    :::5357                         :::0                   LISTENING       4        System
0x7ee767a0         TCPv6    -:0                             4870:da18:80fa:ffff:4870:da18:80fa:ffff:0 CLOSED          101      3
0x7f566840         TCPv4    192.168.25.128:49219            91.192.100.59:30030    SYN_SENT        -1
0x7fb3bec0         UDPv4    0.0.0.0:0                       *:*                                    984      svchost.exe    2018-04-07 08:38:17 UTC+0000
0x7fb3bec0         UDPv6    :::0                            *:*                                    984      svchost.exe    2018-04-07 08:38:17 UTC+0000
0x7fc0a1e0         UDPv4    0.0.0.0:3702                    *:*                                    1944     svchost.exe    2018-04-07 08:39:03 UTC+0000
0x7fc98a50         TCPv4    0.0.0.0:49156                   0.0.0.0:0              LISTENING       504      lsass.exe
0x7fc98a50         TCPv6    :::49156                        :::0                   LISTENING       504      lsass.exe
0x7fc9f940         TCPv4    0.0.0.0:49156                   0.0.0.0:0              LISTENING       504      lsass.exe
```

Análisis memoria RAM

$ vol.py -f memory.raw --profile=Win7SP1x64 memdump -p 2072 --dump-dir=.

```
$ vol.py -f memory.raw --profile=Win7SP1x64 memdump -p 2072 --dump-dir=.
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing vfggggg.exe [  2072] to 2072.dmp
```

Análisis memoria RAM

Búsqueda del hash en VT

327df0474222b0e5de75b4d807ab867fd3da6059e9913f0f13f8a61a0f323b78

9 / 70

Community Score

9 engines detected this file

327df0474222b0e5de75b4d807ab867fd3da6059e9913f0f13f8a61a0f323b78
executable.2072.exe
assembly peexe

930.50 KB
Size

2019-07-30 00:34:50 UTC
3 months ago

DETECTION DETAILS COMMUNITY

Acronis	Suspicious	CrowdStrike Falcon	Win/malicious_confidence_90% (W)
Microsoft	Trojan:Win32/Zpevdo.A	Qihoo-360	HEUR/QVM19.1.B23D.Malware.Gen
Rising	Trojan.Generic@ML.82 (RDML:mkbZxV...	SentinelOne (Static ML)	DFI - Malicious PE
Sophos ML	Heuristic	Symantec	ML.Attribute.HighConfidence
Trapmine	Malicious.high.ml.score	Ad-Aware	Undetected

Análisis memoria RAM

$ strings 2072.dmp > strings_2072.txt

```
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\antonio
LOCALAPPDATA=C:\Users\antonio\AppData\Local
LOGONSERVER=\\WIN-BK55U1RJNG9
MOZ_PLUGIN_PATH=C:\Program Files\Tracker Software\PDF Viewer\Win32\
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_ARCHITEW6432=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3c03
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files (x86)
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\antonio\AppData\Local\Temp
TMP=C:\Users\antonio\AppData\Local\Temp
USERDOMAIN=WIN-BK55U1RJNG9
USERNAME=antonio
USERPROFILE=C:\Users\antonio
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log
```

Análisis memoria RAM

Extracción de los hives del registro

```
$ vol.py -f memory.raw --profile=Win7SP1x64 dumpregistry --dump-dir=.
Volatility Foundation Volatility Framework 2.6
**************************************************
Writing out registry: registry.0xfffff8a00000f010.no_name.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a0015c1010.ntuserdat.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a0008d7010.SECURITY.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a001dd2410.Syscachehve.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a00486d010.BCD.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a001263010.NTUSERDAT.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a0008e4410.SAM.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a000024010.SYSTEM.reg
```

Análisis en Windows - NTFS

- Sistema ficheros desde Windows NT
- Unidades de almacenamiento hasta 2^{46}GB
- Compresión
- Permite aplicar permisos
- Quotas de disco
- Journaling para recuperación de ficheros
- ADS

Análisis en Windows – NTFS

System file	Filename	MFT Record	Purpose of the File
Master file table	**$Mft**	**0**	**Contains one base file record for each file and folder on an NTFS volume**
Master file table mirror	$MftMirr	1	Guarantees access to the MFT in case of a single-sector failure. It is a duplicate image of the first four records of the MFT.
Log file	**$LogFile**	**2**	**The log file is used by to restore metadata consistency to NTFS after a system failure**
Volume	$Volume	3	Contains information about the volume, such as the volume label and the volume version.
Attribute definitions	$AttrDef	4	Lists attribute names, numbers, and descriptions.
Root File name index	.	5	The root folder.

Análisis en Windows – NTFS

System file	Filename	MFT Record	Purpose of the File
Cluster bitmap	**$Bitmap**	6	Represents the volume by showing free and unused clusters.
Boot Sector	$Boot	7	Includes the BPB used to mount the volume and additional bootstrap loader code used if the volume is bootable.
Bad cluster file	$BadClus	8	Contains bad clusters for a volume.
Security file	$Secure	9	Contains unique security descriptors for all files within a volume.
Upcase table	$Upcase	10	Converts lowercase characters to matching Unicode uppercase characters.
NTFS extension file	$Extend	11	Used for various optional extensions such as quotas, reparse point data, and object identifiers.
		12-15	Reserved for future use

Análisis en Windows – NTFS

MFT

AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- Desktop-Disk0.e01
  - Partition 1 [50184MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Partition 2 [464MB]
  - Unpartitioned Space [basic disk]

File List

Name	Size	Type	Date Modified
$Extend	1	Directory	23/04/2018 16:...
$Recycle.Bin	1	Directory	12/07/2018 20:...
Boot	1	Directory	12/07/2018 0:4...
Documents and Settings	1	Reparse Point	23/04/2018 15:...
logs	1	Directory	16/07/2018 16:...
PerfLogs	1	Directory	11/04/2018 23:...
Program Files	1	Directory	23/07/2018 13:...
Program Files (x86)	1	Directory	30/07/2018 23:...
ProgramData	1	Directory	12/07/2018 20:...
Python36	1	Directory	23/07/2018 15:...
Python37	1	Directory	23/07/2018 15:...
Recovery	1	Directory	06/07/2018 18:...
System Volume Information	1	Directory	08/08/2018 16:...
Tools	1	Directory	13/07/2018 20:...
Users	1	Directory	12/07/2018 20:...

Custom Content Sources

Evidence:File System|Path|File	Options

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00  0···············
10 10 00 00 00 90 00 00 00-90 00 00 00 01 00 00 00  ····ê···ê·····
20 F5 BF 05 00 00 00 0A 00-68 00 4A 00 01 00 00 00  õ¿·····h·J·····
30 05 00 00 00 00 00 05 00-87 76 73 B2 1D 1D D4 01  ·········vs²··Ô·
40 71 CA 53 DB 20 1D D4 01-71 CA 53 DB 20 1D D4 01  qÊSÛ ·Ô·qÊSÛ ·Ô·
50 C4 82 7F 69 23 25 D4 01-00 00 00 00 00 00 00 00  Ä··i#%Ô·········
60 00 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00  ····ê···ê·····
70 04 03 6C 00 6F 00 67 00-73 00 66 00 69 00 6C 00  ··l·o·g·s·f·i·l·
80 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····ê···ê·····
90 18 00 00 00 03 00 00 00-01 00 00 00 00 00 00 00  ····ê···ê·····
```

Análisis en Windows – NTFS

MFT

AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- Desktop-Disk0.e01
  - Partition 1 [50184MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Partition 2 [464MB]
  - Unpartitioned Space [basic disk]

Custom Content Sources

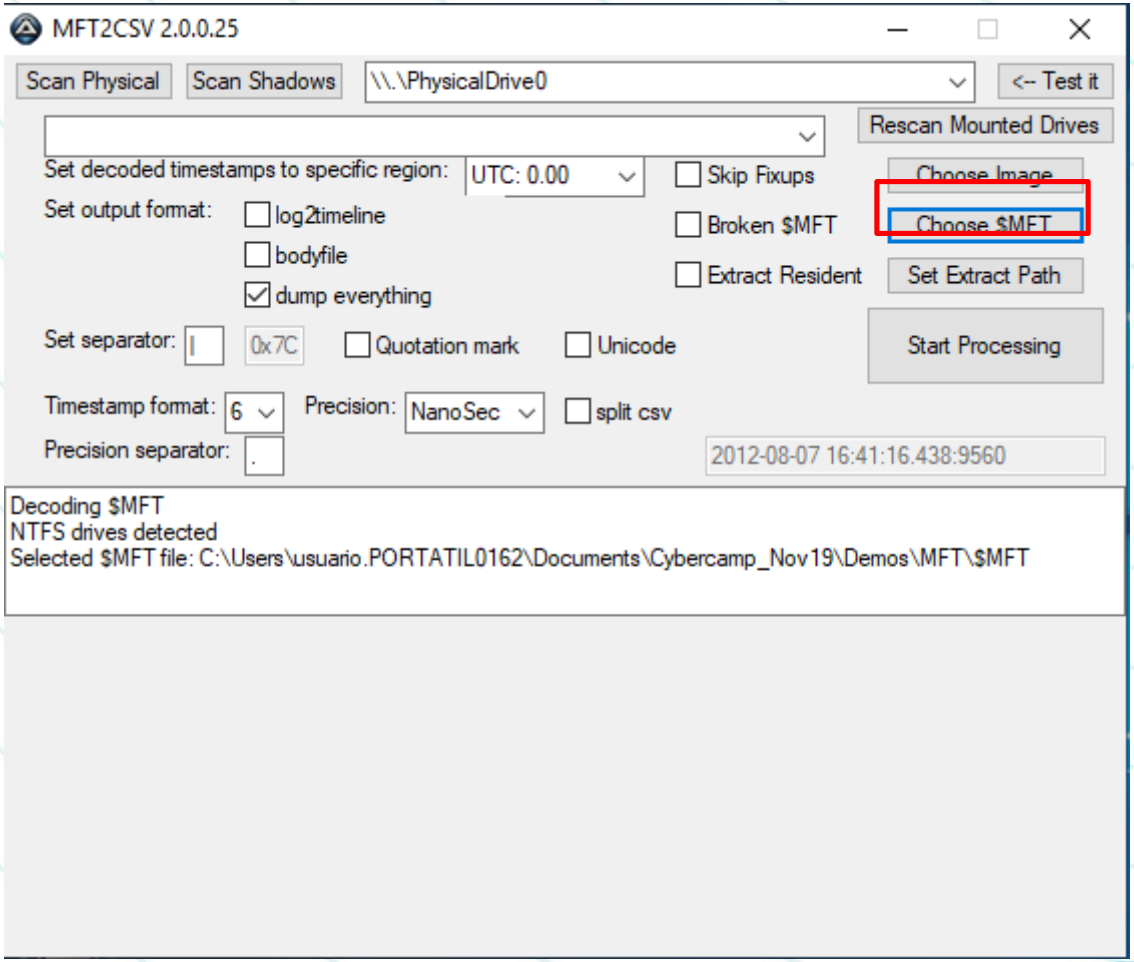
Evidence:File System|Path|File	Options

File List

Name	Size	Type	Date Modified
Windows	1	Directory	08/08/2018 0:0...
Windows.old	1	Directory	21/07/2018 16:...
$AttrDef	3	Regular File	23/04/2018 16:...
$BadClus	0	Regular File	23/04/2018 16:...
$Bitmap	1.569	Regular File	23/04/2018 16:...
$Boot	8	Regular File	23/04/2018 16:...
$I30	8	NTFS Index All...	08/08/2018 0:0...
$LogFile	22.544	Regular File	23/04/2018 16:...
$MFT	380.416	Regular File	23/04/2018 16:...
$MFTMirr	4	Regular File	23/04/2018 16:...
$Secure	1	Regular File	23/04/2018 16:...
$TXF_DATA	1	NTFS Logged ...	08/08/2018 0:0...
$UpCase	128	Regular File	23/04/2018 16:...
$Volume	0	Regular File	23/04/2018 16:...
bootmgr	399	Regular File	06/07/2018 7:1...
BOOTNXT	1	Regular File	11/04/2018 23:...
BOOTSECT.BAK	8	Regular File	06/07/2018 18:...
pagefile.sys	524.288	Regular File	12/07/2018 0:4...
swapfile.sys	393.216	Regular File	13/07/2018 17:...
Windows		$I30 INDX Entry	

Análisis en Windows – NTFS

MFT2CSV



Análisis en Windows – NTFS

MFT

```
$ grep "vfgg" MftDump_2019-11-21_13-20-19.csv
0x057CA400|GOOD|OK||89897|12|1|475|2|vfgggg.exe|:\Users\antonio\AppData\Roaming\vfgggg.exe|FILE
LLOCATED|952832|archive+not_indexed|archive+not_indexed|DOS+WIN32|0|2018-04-07 08:44:02.925:8986|
18-04-07 08:43:54.439:4837|2018-04-07 08:43:54.439:4837|2018-04-07 08:44:02.925:8986|0|2018-04-07
8:44:02.925:8986|2018-04-07 08:44:02.925:8986|2018-04-07 08:44:02.925:8986|2018-04-07 08:44:02.92
8986|0|954368|0|7450624|||||232|01|0|1951682570|344|1024|0|0|0x0003|954368|952832|952832||0|0|0|0
63|||||||||||||||||||||||||||||||||||||||||||||||||||||||||1|0|1|0|0|0|0|1|0|0|0|0|0|0|0
```

Fecha de creación del fichero vfgggg.exe en la MFT
2018-04-07 08:44:02

Análisis en Windows – NTFS

Buscamos en la MFT en dicha fecha

```
sansforensics@siftworkstation -> /m/s/C/D/MFT
$ grep "RecordOffset\|2018-04-07 08" MftDump_2019-11-21_13-20-19.csv > mft_20180407.csv
```

:\Users\antonio\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook	2018-04-07 08:42:29.155:6380
:\Users\antonio\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\AQUE9XME	2018-04-07 08:42:29.155:6380
:\Users\antonio\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\AQUE9XME\Purchase Order 03EDG.doc	2018-04-07 08:42:29.155:6380

:\Users\antonio\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Z5QR0F05\svqxtm[1].hta	2018-04-07 08:43:46.703:3742
:\Users\antonio\AppData\Local\Microsoft\Windows\AppCache	2018-04-07 08:43:47.452:1755
:\Users\antonio\AppData\Local\Microsoft\Windows\AppCache\container.dat	2018-04-07 08:43:47.374:1754
:\Users\antonio\AppData\Local\Microsoft\Windows\AppCache\DX80KDCL	2018-04-07 08:43:47.452:1755
:\Users\antonio\AppData\Local\Microsoft\Windows\AppCache\DX80KDCL\container.dat	2018-04-07 08:43:47.452:1755
:\Users\antonio\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms	2018-04-07 08:43:50.165:0632
:\Users\antonio\AppData\Roaming\vfggggg.exe	2018-04-07 08:44:02.925:8986
:\Users\antonio\AppData\Local\Temp\test 02.exe	2018-04-07 08:43:53.066:6813

Análisis en Windows - Prefetch

- **Característica para mejorar el arranque de las aplicaciones**
- **Sólo existen en Windows cliente**
  - En Windows Server hay que habilitarlo
  - En disco SSD hay que habilitarlo
- **Se crean en %WINDIR%\Prefetch**
- **Archivo .pf se crea la primera vez que se ejecuta la aplicación ➔ Se creará una entrada en la MFT!!**
- **Puede ser eliminado automáticamente ☹**

Análisis en Windows - Prefetch

- **Windows 7**
- **Hasta 128 archivos**
- **Sólo guarda la última ejecución ☹**

- **Windows 8 y posteriores**
- **Hasta 256 archivos**
- **Histórico de 8 ejecuciones ☺**

- **Tools**
  - WinPrefetchView (Nirsoft)
  - PECmd

Análisis en Windows – Prefetch

- **Prefetch**

¡¡No tenemos!! → Disco SSD

Análisis en Windows – NTFS

WinPrefetchView

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
MMC.EXE-887C1698.pf	27/05/2019 12:08:05	18/06/2019 5:18:46	42.619	MMC.EXE	C:\Windows\System32\m...	5	18/06/2019 5:18:36, 18/06/2019 5:16:25, 18/06/2019 5:16:...
LOGONUI.EXE-E35F76FB.pf	27/05/2019 12:08:45	25/11/2019 18:03:24	41.867	LOGONUI.EXE	C:\Windows\System32\Lo...	72	25/11/2019 18:03:13, 25/11/2019 14:18:52, 25/11/2019 11...
WWAHOST.EXE-E7F5DF90.pf	27/05/2019 12:10:03	14/07/2019 7:18:56	73.121	WWAHOST.EXE	C:\Windows\System32\W...	4	14/07/2019 7:18:42, 14/07/2019 7:15:21, 18/06/2019 5:20:...
MICROSOFTEDGECP.EXE-B41F8EC7.pf	27/05/2019 12:10:18	19/07/2019 7:13:10	47.042	MICROSOFTEDGE...	C:\Windows\System32\MI...	26	19/07/2019 7:13:00, 18/07/2019 7:08:47, 17/07/2019 18:0...
EXPLORER.EXE-03C49D11.pf	27/05/2019 13:30:08	15/11/2019 1:25:58	41.865	EXPLORER.EXE	C:\Windows\explorer.exe	12	15/11/2019 1:25:41, 13/11/2019 21:20:57, 31/10/2019 8:3...
VIRTUALBOX.EXE-09EBEA7A.pf	20/06/2019 8:36:56	22/11/2019 16:09:48	32.317	VIRTUALBOX.EXE	C:\PROGRAM FILES\Oracl...	27	22/11/2019 16:09:36, 22/11/2019 9:58:21, 21/11/2019 12:...
7ZG.EXE-D9AA3A0B.pf	20/06/2019 8:39:14	21/11/2019 18:57:21	31.491	7ZG.EXE	C:\PROGRAM FILES\7-Zip...	37	21/11/2019 18:57:20, 21/11/2019 15:11:10, 20/11/2019 17...
Op-EXPLORER.EXE-03C49D11-000000...	20/06/2019 9:26:16	20/11/2019 17:20:45	9.064			7	20/11/2019 17:20:43, 22/07/2019 11:35:00, 14/07/2019 8:...
FRMINST.EXE-06DFB7B5.pf	20/06/2019 9:29:57	20/06/2019 9:30:13	8.257	FRMINST.EXE	C:\PROGRAM FILES\MCA...	2	20/06/2019 9:30:03, 20/06/2019 9:29:53
DXLSETUP-MA.EXE-808D0AE0.pf	20/06/2019 9:30:15	20/06/2019 9:30:15	13.034	DXLSETUP-MA.EXE	C:\PROGRAMDATA\PACK...	2	20/06/2019 9:30:05, 20/06/2019 9:30:05
PICKERHOST.EXE-03F09186.pf	20/06/2019 9:43:10	21/11/2019 13:29:33	43.529	PICKERHOST.EXE	C:\Windows\System32\PI...	3	21/11/2019 13:29:25, 21/11/2019 13:01:19, 20/06/2019 9:...
FTK IMAGER.EXE-C4B29A14.pf	20/06/2019 11:00:18	24/11/2019 12:40:12	27.817	FTK IMAGER.EXE	C:\PROGRAM FILES\ACCE...	25	24/11/2019 12:40:02, 23/11/2019 11:58:14, 23/11/2019 9:...
PREFETCH_PARSER_GUI.EXE-57CBB9E...	20/06/2019 11:05:11	22/11/2019 9:56:10	10.616	PREFETCH_PARSE...	C:\Users\USUARIO.PORTA...	5	22/11/2019 9:56:08, 20/11/2019 17:51:06, 20/11/2019 9:0...
UPDATER.EXE-65FD6398.pf	28/06/2019 11:16:40	19/11/2019 13:18:41	7.040	UPDATER.EXE	C:\PROGRAM FILES\MOZI...	14	19/11/2019 13:18:31, 18/11/2019 12:45:47, 30/10/2019 17...
SUBLIME TEXT BUILD 3207 X64 S-F008...	03/07/2019 9:51:27	03/07/2019 9:51:27	10.163	SUBLIME TEXT BUI...	C:\USERS\USUARIO.PORT...	1	03/07/2019 9:51:17
SUBLIME TEXT BUILD 3207 X64 S-3A7...	03/07/2019 9:51:35	03/07/2019 9:51:35	9.830	SUBLIME TEXT BUI...	C:\USERS\USUARIO.PORT...	1	03/07/2019 9:51:25

Filename	Full Path	Device Path	Index
$MFT	C:\Windows\System32\glu32.dll	\VOLUME{01d34ca787e53170-a08857ef}\$MFT	51
MSVCP100.DLL	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\MSVCP100.DLL	7
MSVCR100.DLL	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\MSVCR100.DLL	6
QT_ES.QM	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\NLS\QT_ES.QM	71
VIRTUALBOX_ES.QM	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\NLS\VIRTUALBOX_ES.QM	70
QMINIMAL.DLL	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\PLATFORMS\QMINIMAL.DLL	64
QOFFSCREEN.DLL	C:\PROGRAM FILES\Oracle\VIRT...	\VOLUME{01d34ca787e53170-a08857ef}\PROGRAM FILES\ORACLE\VIRTUALBOX\PLATFORMS\QOFFSCREEN.DLL	65

Análisis en Windows - Registro

- **BD jerárquica**
- **Configuración de Sistema Operativo, aplicaciones y usuarios**
  - Perfiles cada usuario
  - Aplicaciones instaladas
  - Información conexiones de red
  - Configuración de carpetas
  - Iconos
  - Elementos hardware
  - Histórico de USB
  - Contraseñas de los usuarios
  - …

Análisis en Windows - Registro

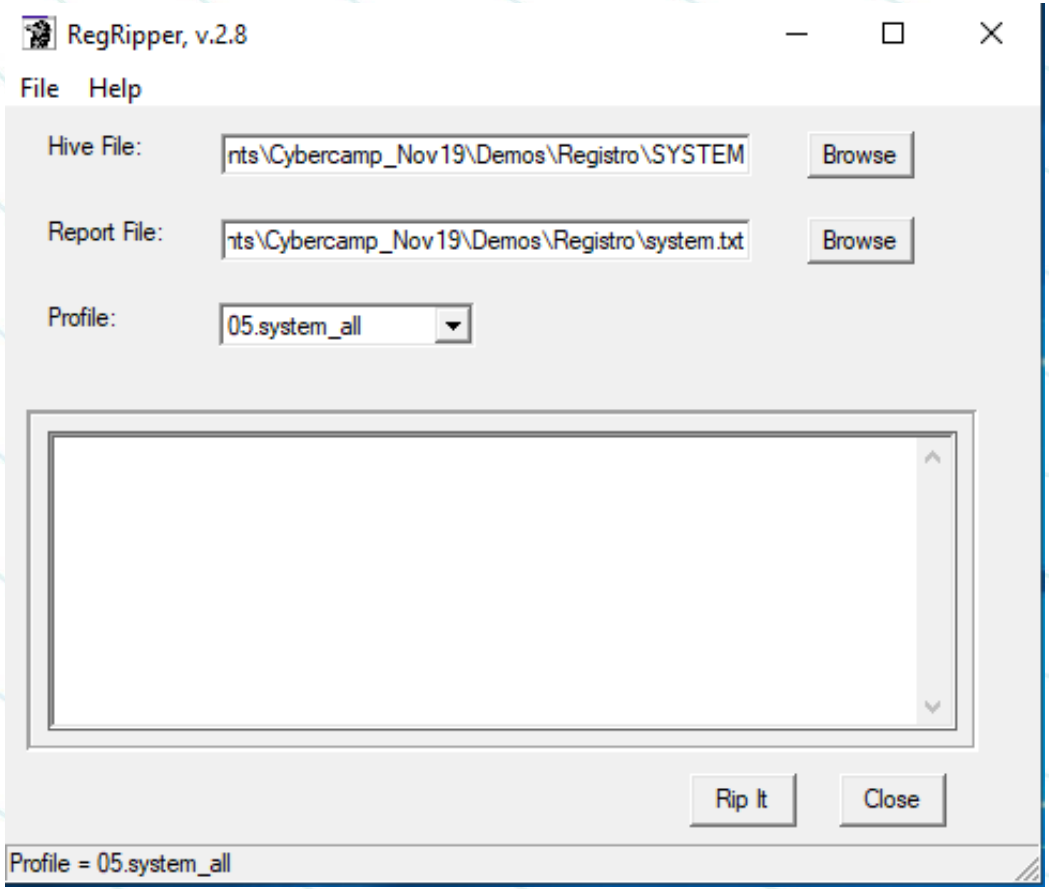
- **HKEY_CURRENT_USER**
  - Información relativa al usuario actual del sistema
- **HKEY_USERS**
  - Información de todos los perfiles del sistema
- **HKEY_LOCAL_MACHINE**
  - Información de la configuración del sistema (para cualquier usuario)
- **HKEY_CLASSES_ROOT**
  - Información de la asociación de archivos y aplicaciones
- **HKEY_CURRENT_CONFIG**
  - Información relativa al hardware del sistema

Análisis en Windows - Registro

- **Hives**
  - %WINDIR%\System32\Config\SAM
  - %WINDIR%\System32\Config\Security
  - %WINDIR%\System32\Config\Software
  - %WINDIR%\System32\Config\System
  - %WINDIR%\System32\Config\Default
- **(<= Win XP)**
  - \Documents and Setting\user\NTUSER.DAT
- **(>=Win 7)**
  - %SystemRoot%\Users*username*\NTUSER.DAT
  - %SystemRoot%\Users\AppData\Local\Microsoft\Windows\UsrClass.dat

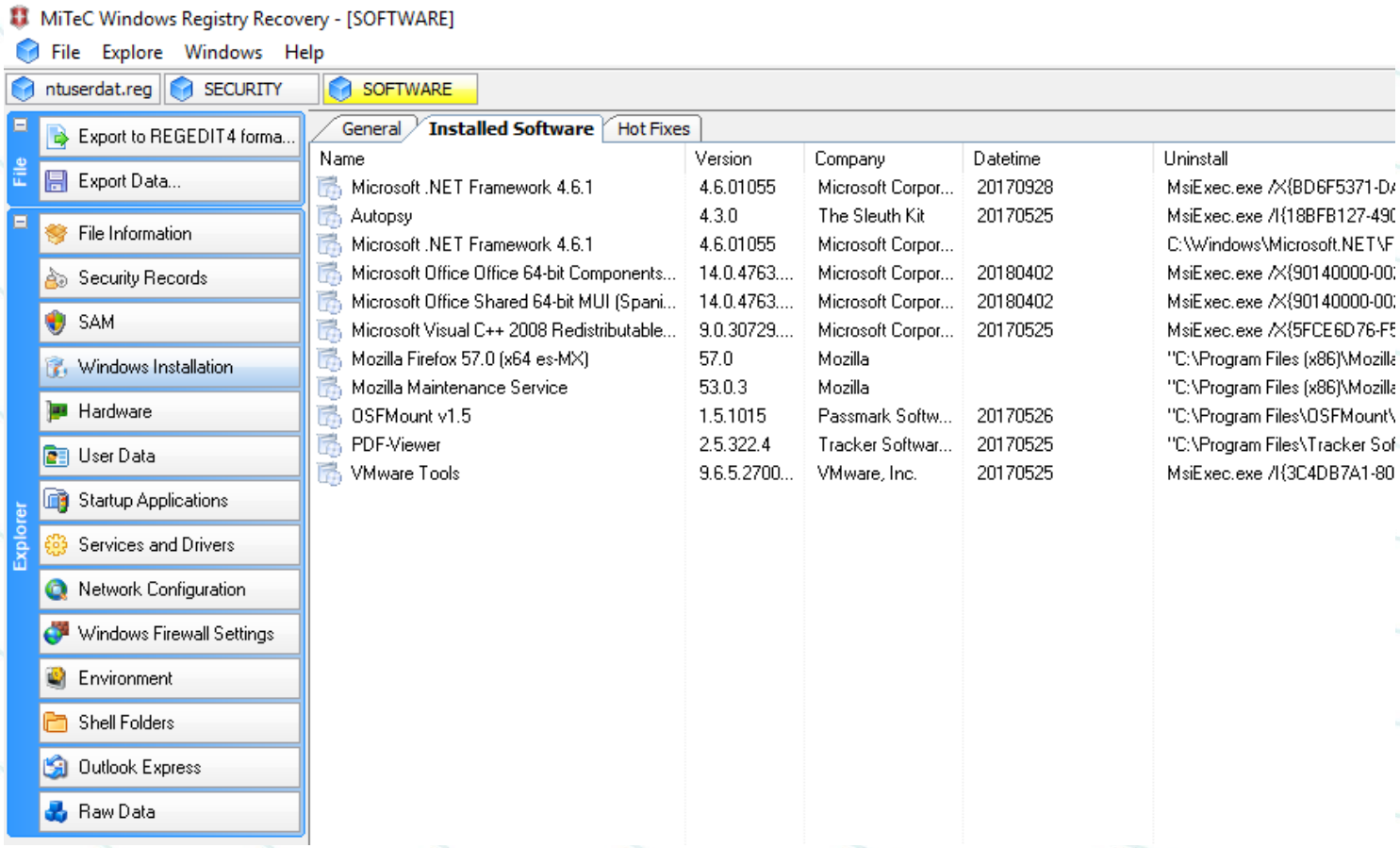
Windows Analysis – Registry

- **RegRipper**



Windows Analysis – Registry

- **WRR**



Windows Analysis – Registry

- **Mecanismo de persistencia**
- **Aplicaciones ejecutadas al inicio del sistema**

  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Once

```
user_run v.20140115
(NTUSER.DAT) [Autostart] Get autostart key contents from NTUSER.DAT hive

Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Sat Apr  7 08:44:42 2018 (UTC)
  ghh: C:\Users\antonio\AppData\Roaming\temp\tempgh.exe
  dttrgsdcd: C:\Users\antonio\AppData\Roaming\vfggggg.exe -boot

Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
```

Análisis en Windows - Registro

- **UsserAssist**
  - Apps con GUI ejecutados por un usuario desde Windows Explorer
  - NTUSER.DAT
  - \Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
  - ROT13

- **Tools**
  - Registry Explorer

Análisis en Windows - Registro

- **Registry Explorer**

Values | UserAssist

Arrastre una columna aquí para agrupar por dicha columna

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
ABC	=	=	ABC	= 2018-04-07 00:00:00
{System32}\cmd.exe	7	44	0d, 0h, 19m, 28s	2018-04-07 08:37:22
{Program Files x86}\Microsoft Office\Office14\OUTLOOK.EXE	2	11	0d, 0h, 06m, 06s	2018-04-07 08:42:04
C:\Python27\python.exe	1	4	0d, 0h, 01m, 49s	2018-04-07 08:42:14

Análisis en Windows - Registro

- **USB conectados en el sistema**
- **SYSTEM\CurrentControlSet\Enum\USB**
- **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- **Las carpetas vienen determinadas por Vendor&Product&NumSerie**
- **Tools:**
  - USBDeview
  - Autopsy

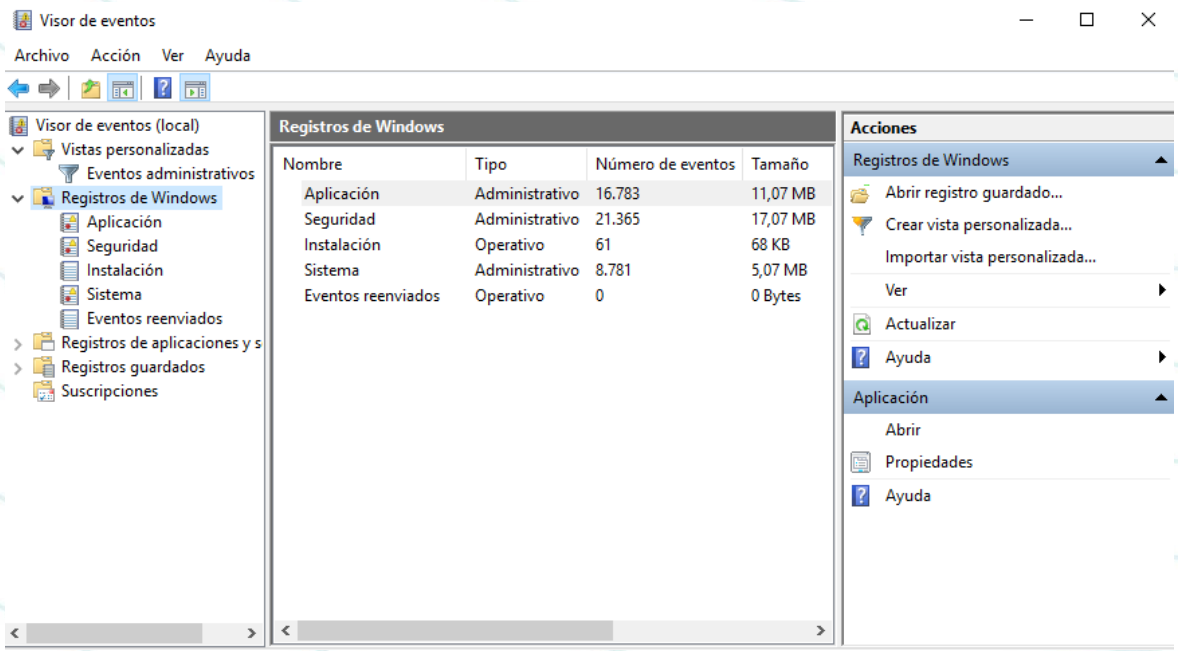
Análisis en Windows - Registro

- **USBDeview**

Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug Date
Concentrador raíz USB	Unknown	No	Yes	No	Yes			25/05/2017 22:49:16	07/04/2018 10:36:50
Concentrador raíz USB	Unknown	No	Yes	No	Yes			25/05/2017 22:49:16	07/04/2018 10:36:50
Dispositivo compuesto USB	Unknown	No	Yes	No	No			25/05/2017 22:49:18	07/04/2018 10:36:51
Dispositivo de entrada USB	HID (Human Interface Device)	No	Yes	No	No			25/05/2017 22:49:18	07/04/2018 10:36:51
Dispositivo de entrada USB	HID (Human Interface Device)	No	Yes	No	No			25/05/2017 22:49:18	07/04/2018 10:36:51
Generic USB Hub		No	Yes	No	Yes			25/05/2017 22:49:18	07/04/2018 10:36:51
SanDisk Ultra Fit USB Device	Mass Storage	No	Yes	No	No		4C531148600927111234	25/05/2017 22:54:53	28/05/2017 16:32:51
GOODRAM 4GB USB Device	Mass Storage	No	Yes	No	No		8F0057AAAA229013	26/05/2017 20:51:18	27/05/2017 10:07:36
Dispositivo compuesto USB	Unknown	No	Yes	No	No	F:	0123456789ABCDEF	28/05/2017 16:56:44	28/05/2017 16:56:45
Dispositivo de almacenamiento ...	Mass Storage	No	Yes	No	No	F:		28/05/2017 16:56:45	28/05/2017 16:56:45
ADB Interface	Vendor Specific	No	No	No	No			28/05/2017 16:56:45	28/05/2017 16:56:45
Kingston DataTraveler 2.0 USB D...	Mass Storage	No	Yes	No	No		1C6F654E3FD0FE3189177841	17/11/2017 17:13:48	02/04/2018 20:00:37
Kingston DataTraveler 3.0 USB D...	Mass Storage	No	Yes	No	No	E:	408D5C1E8E4FB06079646880	15/01/2018 22:44:54	07/04/2018 10:36:52
SanDisk Cruzer Blade USB Device	Mass Storage	No	Yes	No	No		4C532000060412103162	23/01/2018 22:13:59	23/01/2018 22:14:21

Análisis en Windows – Event Log

- **Registra eventos y actividades del sistema**
  - Inicio/cierre sesión del usuario
  - Inicio/apagado del sistema
  - Inicio/fin de un servicio
  - Errores de aplicaciones
  - Cambio de políticas
  - Tracking de procesos
  - […]



Análisis en Windows – Event Log

- **Windows 2003 y XP**
  - %WINDIR%\System32\config*.evt
- **Windows vista o superior**
  - %WINDIR%\system32\winevt\Logs*.evtx

- **Tools**
  - Event Viewer (Windows)
  - EvtxExplorer (Eric Zimmerman’s tools)

  - Evtxcmd.exe -f evtx_file --csv path --csvf output_file.csv

Análisis en Windows – Timeline

Timeline Windows Event Log

```
LogParser.exe -i:evt -o:csv "Select
RecordNumber,TO_UTCTIME(TimeGenerated),EventID,Source
Name,ComputerName,SID,Strings from "C:\path_evtx\*.evtx"" >
C:\path\events_logparser.csv
```

Análisis en Windows – Event log

¿Qué buscar en el event log?

Intentos de login SMB
Log de Powershell
Log de Terminal Server
Creación de servicios
Login de usuarios remotos

Navegadores – Internet Explorer

- **En Windows XP y Windows 7**
- **Index.dat**
  - Archivo oculto y de sistema
  - Índice de referencias de las páginas visitadas
  - Incluye visitas con Explorer.exe
  - Lista no sincronizada, no se borra con las opciones de IE

  - C:\users\user\AppData\Local\Micorsoft\Windows\History

Navegadores – Internet Explorer

- **Windows XP y Windows 7**
- **Archivos temporales, Cache y cookies**
  - --- Win7 ---
  - C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
  - C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Cookies

  - --- XP ---
  - C:\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.ie5
  - C:\Documents and Settings\%username%\Cookies
  - C:\Documents and Settings\%username%\Local Settings\History\history.ie5

Navegadores – Internet Explorer

- **En Windows 8 y Windows 10**
- **No existe index.dat → WebCacheV*.dat**
- **Formato EDB (Extensible Storage Engine)**
- **Temporales**
  - C:\Users\<username>\Local\Microsoft\Windows\Temporary Internet Files
- **Historial navegación, cache y cookies**
  - C:\Users\username\AppData\Local\Microsoft\Windows\WebCache
- **Tools**
  - LibeseDB
  - ESEDatabaseView de nirsoft

Navegadores – Firefox

- **Formato SQLite**
- **Histórico de sitios: places.sqlite**
- **Autocompletar: FormHistory.sqlite**
- **Cookies: cookies.sqlite**
- **Passwords: signons.sqlite**
- **Certificados: cert8.db y cert9.d**

- **Ubicaciones**
  - XP → C:\Documents and Settings\usuario\Dataos de programa \Mozilla\Firefox\Profiles
  - Win7 o superior → C:\Users\usaurio\AppData\Roaming\Mozilla\Firefox

Navegadores – Chrome

- **Formato SQLite**
- **Histórico de sitios: History**
- **Cookies: cookies**
- **Passwords: Login.Dat**

- **Ubicaciones**
  - C:\Documents and Settings\usuario\Configuración local\Datos de programa\Google\Chrome
  - %UserProfile%\AppData\local\Google\Chrome\User Data\
  - %UserProfile%\AppData\local\Google\Chrome\User Data\Default\Cache

Navegadores

Browsing History View

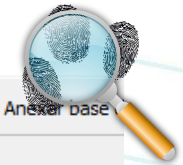
BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time	Visit Count	Visited From	Web Browser	User Prof
https://www.bing.com/		23/10/2018 4:16:34	1		Internet Explorer 10/11 / Edge	admin
https://www.bing.com/search?q=obtener+ayuda+con+el+explorador+de+archivos+en+windows%c2%a010&...		23/10/2018 4:16:34	1		Internet Explorer 10/11 / Edge	admin
https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e34...		23/10/2018 4:16:34	1		Internet Explorer 10/11 / Edge	admin
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1540286179&rver=6.0.5286.0&wp=MBI_SSL&wr...		23/10/2018 4:16:35	1		Internet Explorer 10/11 / Edge	admin
https://www.bing.com/orgid/idtoken/nosignin		23/10/2018 4:16:35	2		Internet Explorer 10/11 / Edge	admin
https://www.google.es/search?q=bankia&oq=bankia&aqs=chrome..69i57j0l5.1148j0j8&sourceid=chrome&ie=...	bankia - Buscar con ...	23/10/2018 10:48:36	1		Chrome	admin
https://support.microsoft.com/hub/4338813/windows-help		23/10/2018 11:08:29	1	https://su...	Chrome	admin
https://go.microsoft.com/fwlink/?LinkId=517009		23/10/2018 11:08:29	1		Chrome	admin
https://support.microsoft.com/windows		23/10/2018 11:08:29	1	https://go....	Chrome	admin
https://support.microsoft.com/es-es/hub/4338813/windows-help	Ayuda de Windows	23/10/2018 11:08:30	1		Chrome	admin
https://support.microsoft.com/es-es/hub/4338813/windows-help?os=windows-10	Ayuda de Windows	23/10/2018 11:08:30	1		Chrome	admin
https://www.google.es/search?q=bankia&oq=bankia&aqs=chrome..69i57j0l5.1135j1j7&sourceid=chrome&ie=...	bankia - Buscar con ...	30/10/2018 15:57:23	1		Chrome	admin

Navegadores

SQLite



DB Browser for SQLite - C:\Users\usuario.PORTATIL0162\Documents\evidencias\W10_dell\places.sqlite

Archivo Editar Ver Herramientas Ayuda

Nueva base de datos | Abrir base de datos | Guardar cambios | Deshacer cambios | Abrir proyecto | Guardar proyecto | Anexar base

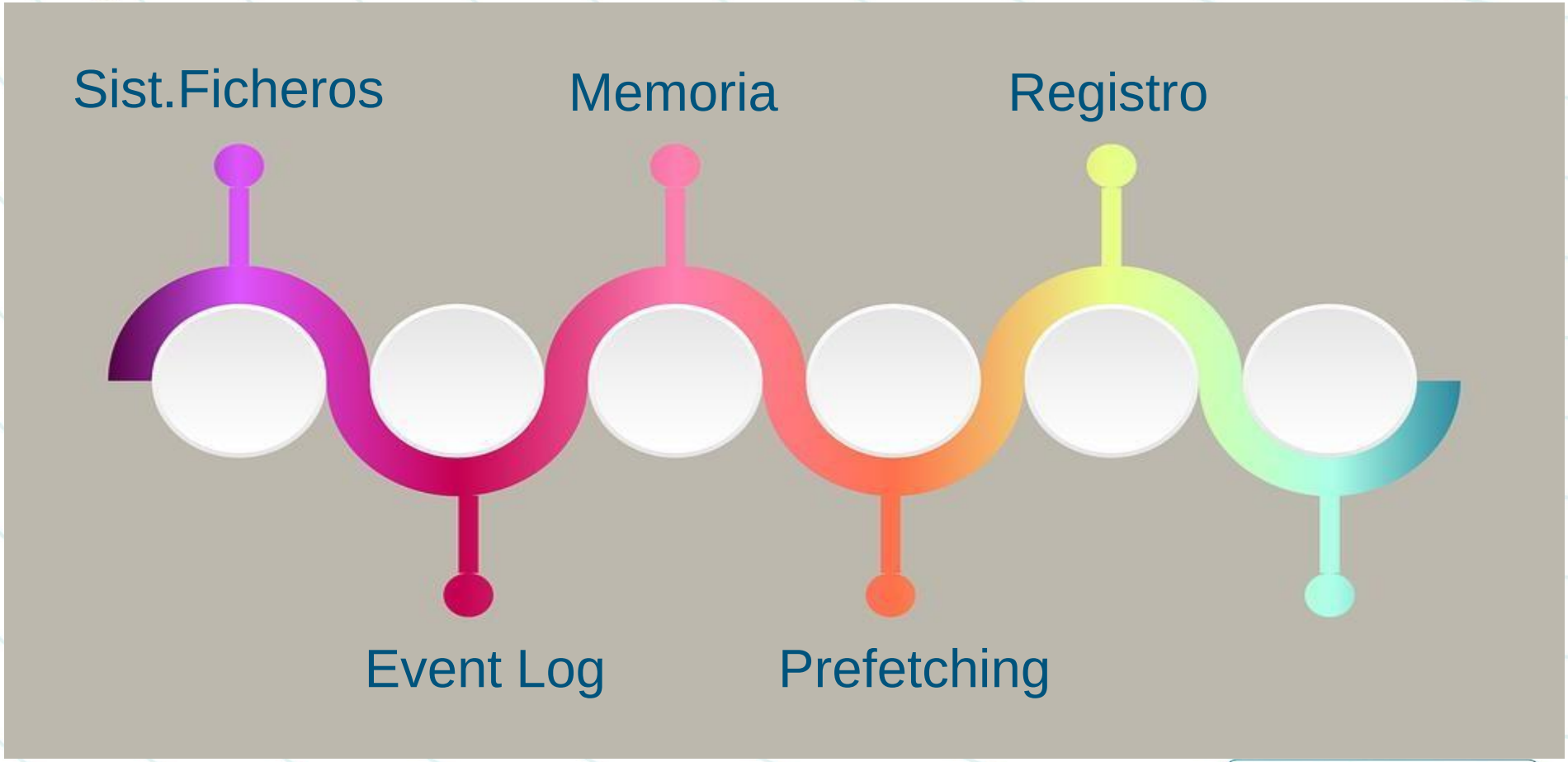
Estructura | Hoja de datos | Editar pragmas | Ejecutar SQL

SQL 1

```
1  select url, datetime((last_visit_date/1000000), 'unixepoch', 'utc') as lastvisit,
2  title, visit_count, typed, hidden from moz_places
3
```

	url	lastvisit	title	visit_count	typed
7	https://www.virtualbox.org/	2019-06-20 06:22:19	Oracle VM VirtualBox	1	0
8	https://www.virtualbox.org/wiki/Downloads	2019-06-20 06:23:03	Downloads – Oracle VM VirtualBox	1	0
9	https://www.google.com/search?client=firef...	2019-06-20 06:39:21	sift - Buscar con Google	1	1
10	https://www.google.com/search?client=firef...	2019-06-20 06:39:32	sift forensic - Buscar con Google	1	0
11	https://digital-forensics.sans.org/community...	2019-07-19 06:37:54	SIFT Workstation Download	2	0
12	https://digital-forensics.sans.org/community...	2019-06-20 06:39:42	*NULL*	1	0
13	https://digital-forensics.sans.org/login	2019-06-20 06:39:44	Digital Forensics Training | Incident Response Tr...	1	0
14	https://www.google.com/search?client=firef...	2019-06-20 09:00:52	autopsy forensic - Buscar con Google	1	1
15	https://www.sleuthkit.org/autopsy/	2019-07-18 05:55:28	Autopsy	2	0
16	https://www.sleuthkit.org/autopsy/downloa...	2019-06-20 09:01:02	Autopsy: Download	1	0

Análisis en Windows - Timeline



Análisis en Windows – Timeline

- TimeLine del sistema de ficheros

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ analyzeMFT.py -f ../MFT/\$MFT -b mft_body.txt
```

- Convertir de bodyfile a formato TLN

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ bodyfile.pl -f mft_body.txt -s WIN-BK55U1RJNG9 > mft_tln.txt
```

Análisis en Windows – Timeline

- **Timeline de la memoria**

```
sansforensics@siftworkstation -> /m/s/C/D/memoria
$ vol.py -f memory.raw --profile=Win7SP1x64 timeliner --output=body --output-file=../TimeLine/memoria_body.txt
Volatility Foundation Volatility Framework 2.6
Outputting to: ../TimeLine/memoria_body.txt
```

- **Convertir body file a TLN**

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ bodyfile.pl -f memory_body.txt -s PC1 > memoria_tln.txt
```

Análisis en Windows – Timeline

- **Timeline del registro**

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ regtime.pl -m HKLM-USER-Antonio -r ../Registro/ntuserdat.reg >> registro_tln.txt
```

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ regtime.pl -m HKLM-SOFTWARE -r ../Registro/SOFTWARE >> registro_tln.txt
```

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ regtime.pl -m HKLM-SYSTEM -r ../Registro/SYSTEM >> registro_tln.txt
```

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ regtime.pl -m HKLM-SAM -r ../Registro/SAM >> registro_tln.txt
```

```
sansforensics@siftworkstation -> /m/s/C/D/TimeLine
$ regtime.pl -m HKLM-SECURITY -r ../Registro/SECURITY >> registro_tln.txt
```

Análisis en Windows – Timeline

- **Unificar todo…**

$ parse.pl -f memoria_tln.txt -o -c > timeline_all.csv

$ parse.pl -f mft_tln.txt -o -c >> timeline_all.csv

$ parse.pl -f registro_tln.txt -o -c >> timeline_all.csv

-o ordena más antiguos a más recientes
-c output en formato csv

Análisis en Windows

Autopsy

Fases del análisis

Identificación y adquisición → Preservar → Análisis → Informe

Informes

- Documentar durante el proceso
- Información del descubrimiento del incidente
- Información inicial (entrevistas sysadmin, usuarios)
- Información del proceso
  - Antecedentes, adquisición y análisis
- Objetivo de la investigación
- Herramientas utilizadas, especificar la versión
- Resultados reproducibles por un tercero
- Debe ser completo

Informes – Estructura del informe

Resumen ejecutivo

- Nº caso
- Información de los analistas
- Objetivo y alcance de la investigación
- Información general del incidente
- Conclusiones generales

Información inicial / Antecedentes

- Detalles del incidente
- Fechas del incidente
- Información de notificación o hallazgo del incidente

Evidencias

- Información relativa a las evidencias adquiridas
- Ubicación
- Listado de evidencias adquiridas
- Herramientas utilizadas (versión)
- Preservación de las evidencias

Informes – Estructura del informe

Análisis y evaluación

- Evaluación o investigación inicial
- Análisis de las evidencias
- Herramientas utilizadas (versión)

Conclusiones

- Hechos relevantes y conclusiones

Anexos

- Documentación adicional
- Logs (proxy, IDS, Firewall..)
- Metodología de los atacantes
- Recomendaciones

Referencias - Tools

FTK Imager
https://accessdata.com/product-download/

Autopsy
https://www.sleuthkit.org/autopsy/

SIFT SANS
https://digital-forensics.sans.org/community/downloads

OSForensics
https://www.osforensics.com/

Sysinternals
https://docs.microsoft.com/en-us/sysinternals/

Nirsoft nirlauncher
https://launcher.nirsoft.net/

Referencias - Tools

Dumpit
https://www.comae.com/

Ram Capturer
https://belkasoft.com/ram-capturer

Windows Registry Recovery
http://www.mitec.cz/wrr.html

Reg Ripper
https://github.com/keydet89/RegRipper2.8

Registry Explorer
https://ericzimmerman.github.io/#!index.md

Win PrefetchView
https://www.nirsoft.net/utils/win_prefetch_view.html

Referencias - Tools

NTFS Log Tracker
https://sites.google.com/site/forensicnote/ntfs-log-tracker

JumpListsView
https://www.nirsoft.net/utils/jump_lists_view.html

Thumbcache viewer
https://thumbcacheviewer.github.io/

Browsing History View
https://www.nirsoft.net/utils/browsing_history_view.html

Foremost Photorec
https://www.cgsecurity.org/wiki/PhotoRec

Referencias - Tools

IRTriage
https://github.com/AJMartel/IRTriage

Bambiraptor
https://www.brimorlabsblog.com/2016/12/live-response-collection-bambiraptor.html

CyLR
https://github.com/orlikoski/CyLR

Volatility
https://github.com/volatilityfoundation/volatility

Lime
https://github.com/504ensicslabs/lime

Referencias - Tools

Incident response tools
https://github.com/meirwah/awesome-incident-response

Forensic tools
https://github.com/cugu/awesome-forensics

Awesome CSIRT
https://github.com/shrekts/awesome-csirt

Referencias - Trainings

CTF UNIZAR
https://ctf.unizar.es/ratas_inminentes/home

ENISA
https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

CIRCL Forensics Training
https://www.circl.lu/services/forensic-training-materials/

Atenea CCN CTFs