Windows Forense

Ing. Julio Iglesias Pérez

Winternals

“Windows Sysinternals es una parte de la página web de Microsoft TechNet que ofrece recursos técnicos y herramientas para gestionar, diagnosticar, solucionar problemas y supervisar un entorno de Microsoft Windows. Originalmente, el sitio web de Sysinternals (antes conocido como ntinternals) fue creado en 1996 y fue operado por la empresa Winternals Software LP, que se encuentra en Austin, Texas. Fue iniciado por los desarrolladores de software Bryce Cogswell y Mark Russinovich. Microsoft adquirió Winternals y sus activos el 18 de julio de 2006.

El sitio web contó con varias herramientas de software para administrar y supervisar equipos que ejecutan Microsoft Windows. El software ahora se puede encontrar en Microsoft. La compañía también vende servicios de recuperación de datos y las ediciones profesionales de sus herramientas de software libre.”

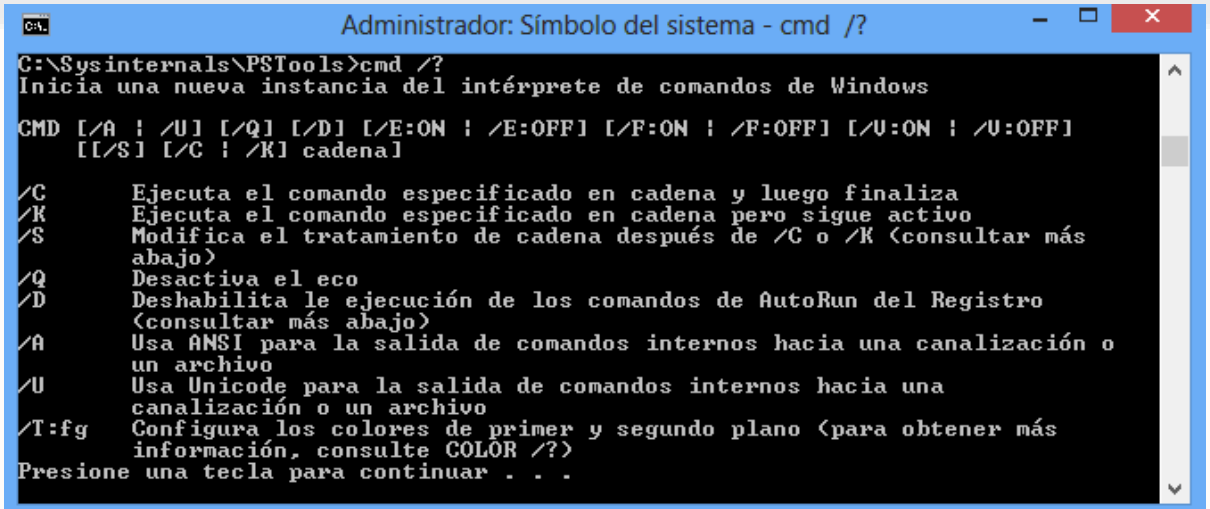
http://en.wikipedia.org/wiki/Winternals

Ayuda comandos

Los comandos que veremos a continuación pueden tener sus variantes o argumentos más específicos para realizar tareas más precisas.

Para ver la lista de argumentos del comando se debe utilizar el parámetro ***/?*** al final del comando, por ejemplo:

cmd /?



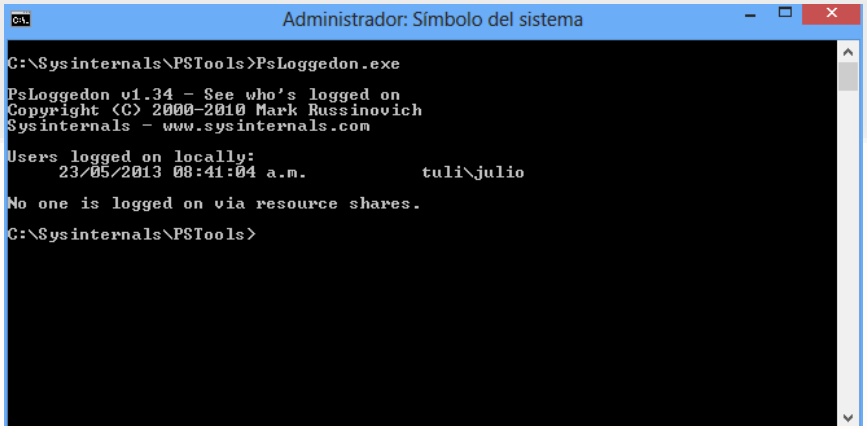
Recolectando información volátil

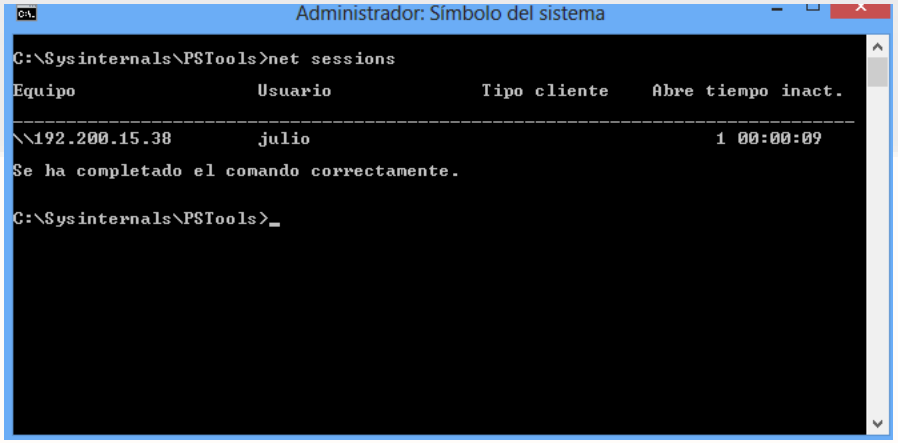
- A continuación veremos cómo recolectar información volátil

Usuarios loguedos

Con los comandos:

- PsLoggedon
- Net sessions





Usuarios logueados

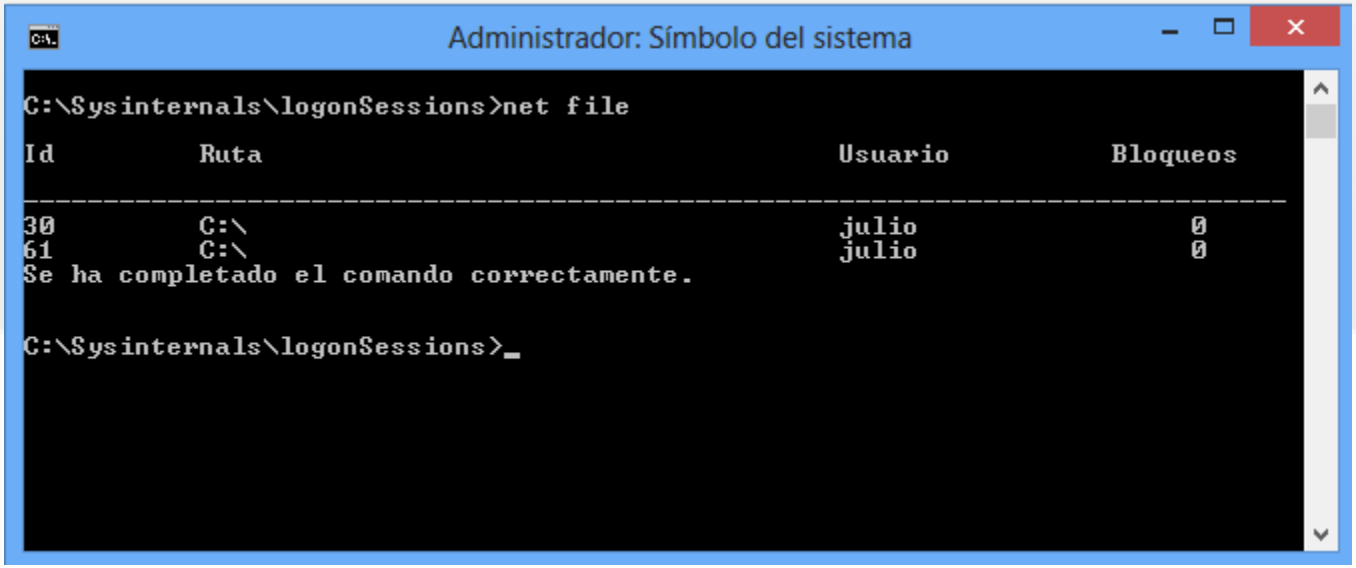
LogonSessions

Administrador: Símbolo del sistema

```
C:\Sysinternals\logonSessions>logonsessions.exe

Logonsesions v1.21
Copyright (C) 2004-2010 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com


[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\TULI$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   23/05/2013 08:40:34 a.m.
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00008bbc:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   23/05/2013 08:40:34 a.m.
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:000003e4:
    User name:    WORKGROUP\TULI$
    Auth package: Negotiate
    Logon type:   Service
    Session:      0
```

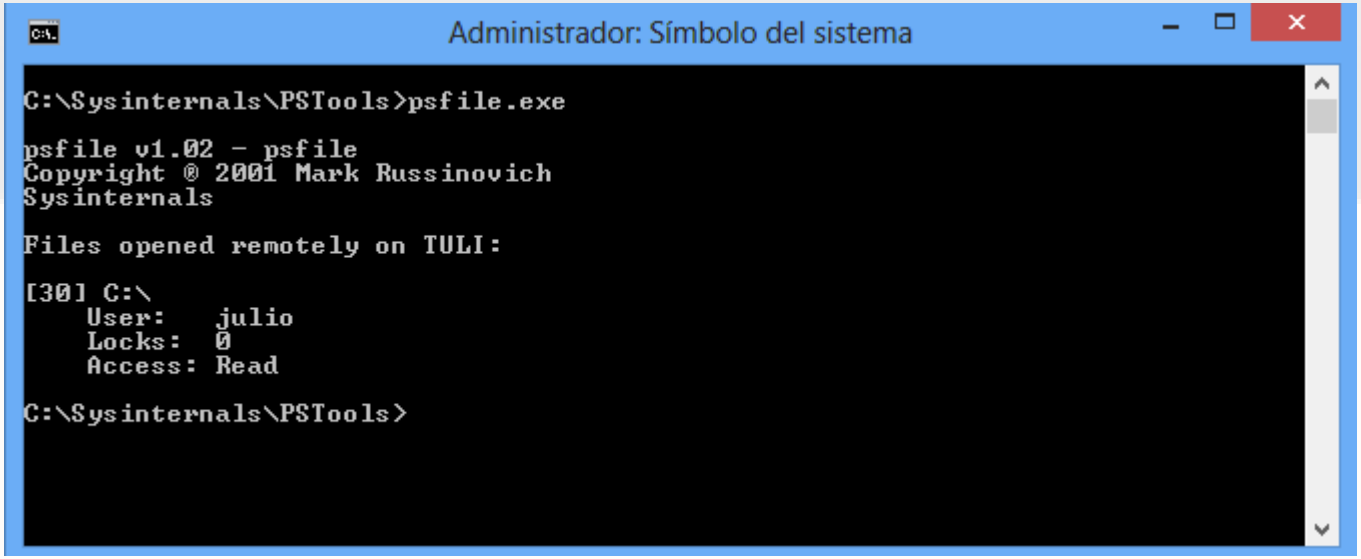
Archivos abiertos

- Net file



Archivos abiertos

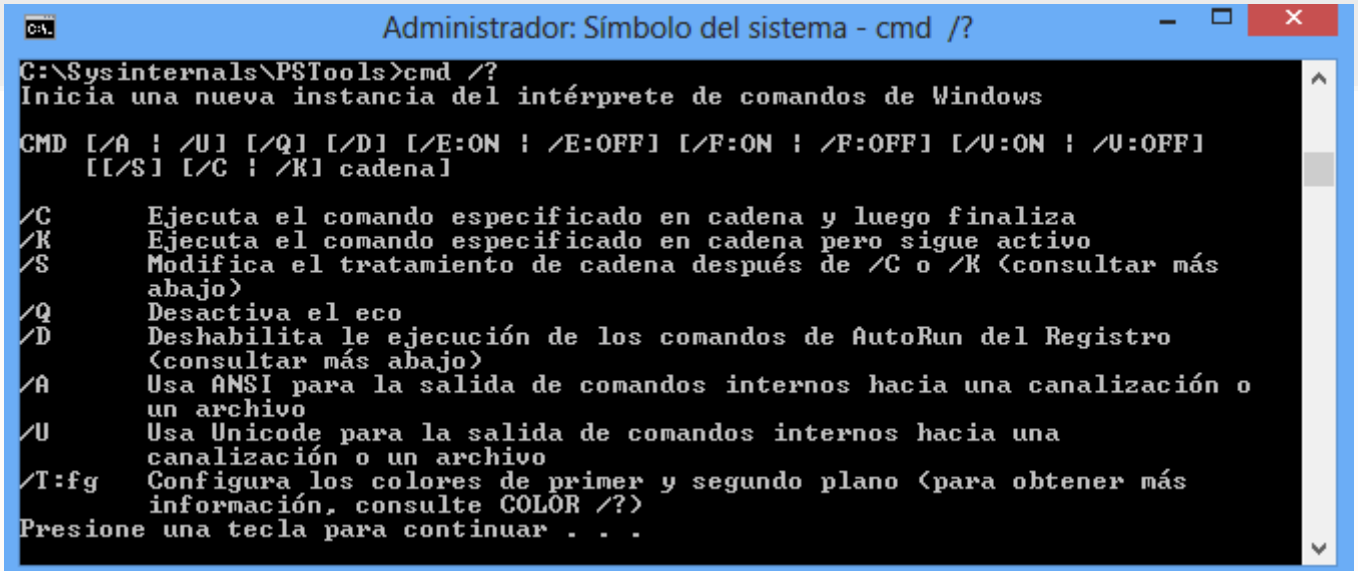
- psfile



Información de la Red

Nbtstat Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP usando NBT (NetBIOS sobre TCP/IP).

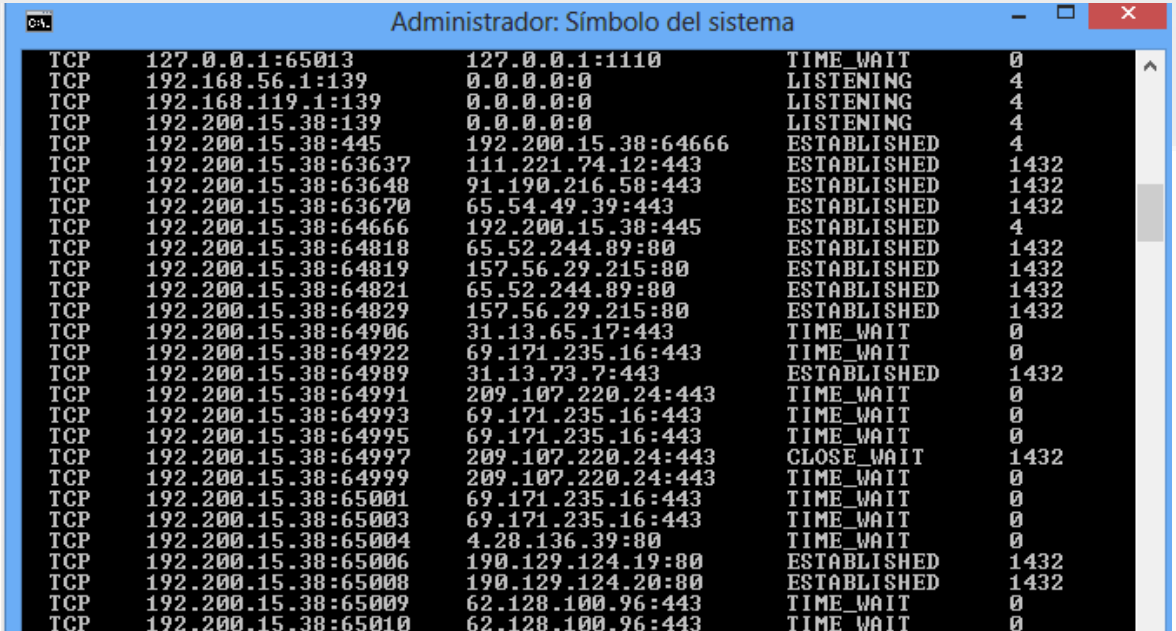
Por ejemplo ***nbtstat –c*** muestra la caché NetBIOS



Información de la Red

Netstat Muestra estadísticas del protocolo y conexiones TCP/IP actuales.

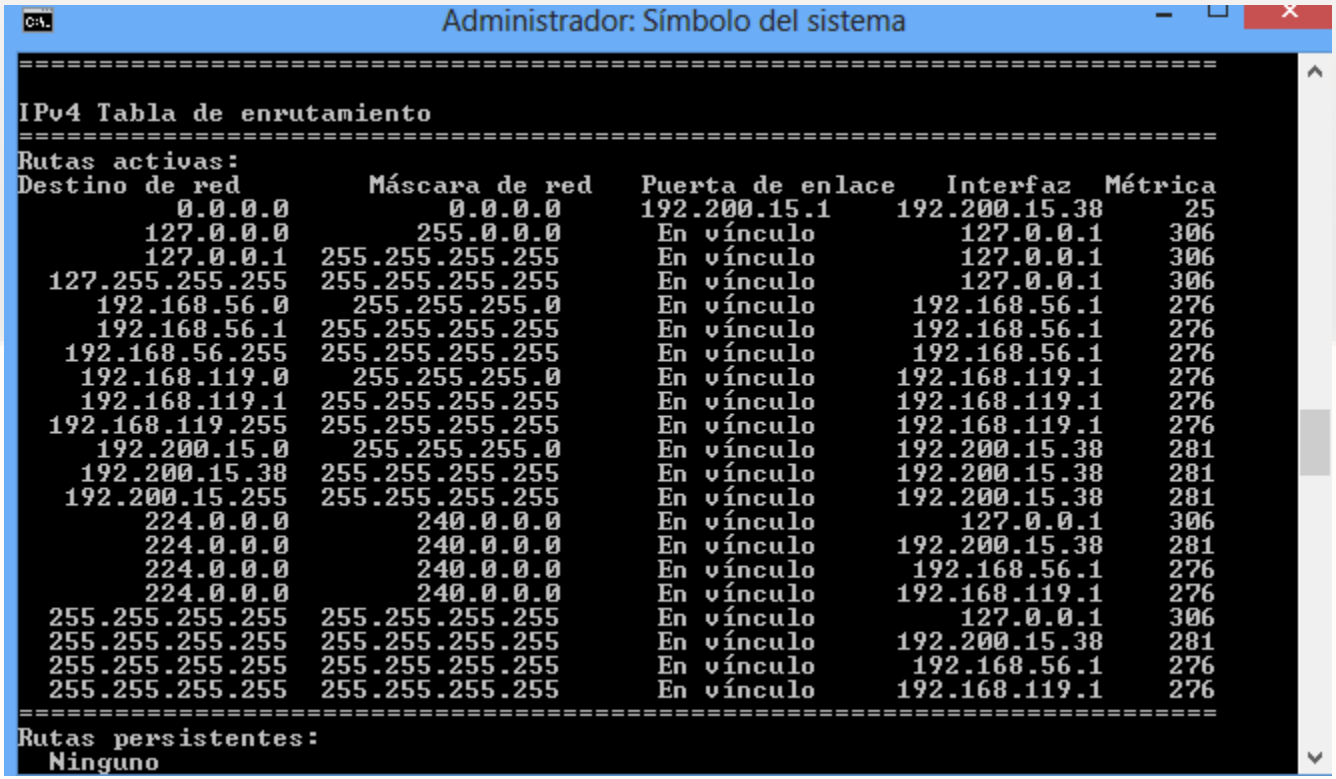
Por ejemplo al ejecutar ***netstat -ona***




```
  TCP    127.0.0.1:65013        127.0.0.1:1110         TIME_WAIT       0
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.119.1:139      0.0.0.0:0              LISTENING       4
  TCP    192.200.15.38:139      0.0.0.0:0              LISTENING       4
  TCP    192.200.15.38:445      192.200.15.38:64666    ESTABLISHED     4
  TCP    192.200.15.38:63637    111.221.74.12:443      ESTABLISHED     1432
  TCP    192.200.15.38:63648    91.190.216.58:443      ESTABLISHED     1432
  TCP    192.200.15.38:63670    65.54.49.39:443        ESTABLISHED     1432
  TCP    192.200.15.38:64666    192.200.15.38:445      ESTABLISHED     4
  TCP    192.200.15.38:64818    65.52.244.89:80        ESTABLISHED     1432
  TCP    192.200.15.38:64819    157.56.29.215:80       ESTABLISHED     1432
  TCP    192.200.15.38:64821    65.52.244.89:80        ESTABLISHED     1432
  TCP    192.200.15.38:64829    157.56.29.215:80       ESTABLISHED     1432
  TCP    192.200.15.38:64906    31.13.65.17:443        TIME_WAIT       0
  TCP    192.200.15.38:64922    69.171.235.16:443      TIME_WAIT       0
  TCP    192.200.15.38:64989    31.13.73.7:443         ESTABLISHED     1432
  TCP    192.200.15.38:64991    209.107.220.24:443     TIME_WAIT       0
  TCP    192.200.15.38:64993    69.171.235.16:443      TIME_WAIT       0
  TCP    192.200.15.38:64995    69.171.235.16:443      TIME_WAIT       0
  TCP    192.200.15.38:64997    209.107.220.24:443     CLOSE_WAIT      1432
  TCP    192.200.15.38:64999    209.107.220.24:443     TIME_WAIT       0
  TCP    192.200.15.38:65001    69.171.235.16:443      TIME_WAIT       0
  TCP    192.200.15.38:65003    69.171.235.16:443      TIME_WAIT       0
  TCP    192.200.15.38:65004    4.28.136.39:80         TIME_WAIT       0
  TCP    192.200.15.38:65006    190.129.124.19:80      ESTABLISHED     1432
  TCP    192.200.15.38:65008    190.129.124.20:80      ESTABLISHED     1432
  TCP    192.200.15.38:65009    62.128.100.96:443      TIME_WAIT       0
  TCP    192.200.15.38:65010    62.128.100.96:443      TIME_WAIT       0
```

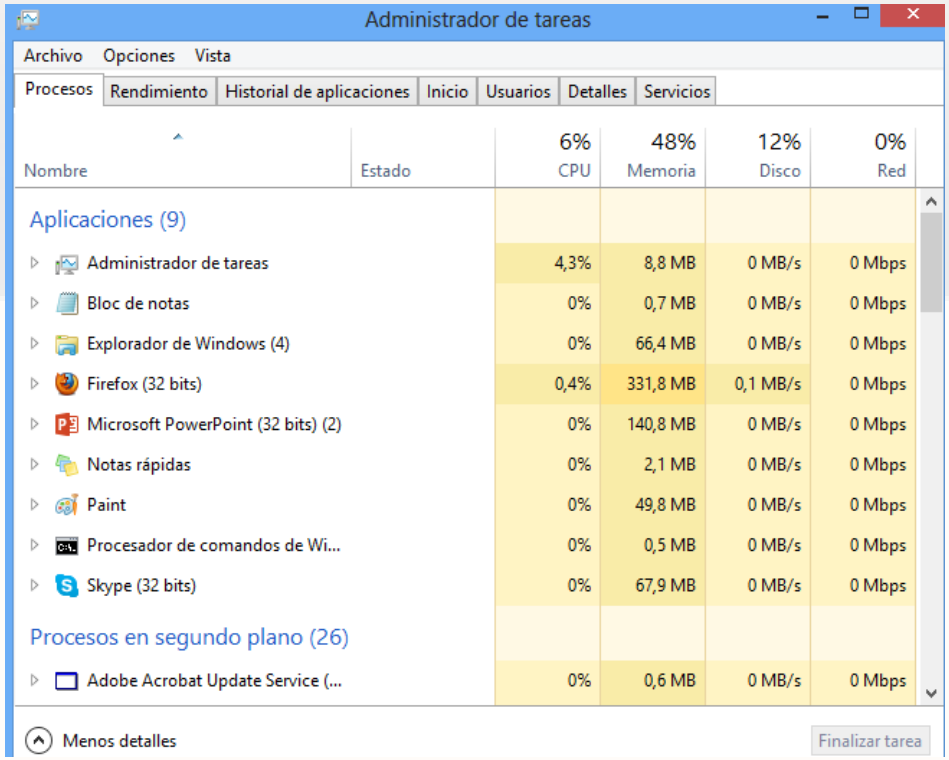
Información de la Red

Con ***netstat –r*** podemos ver la Tabla de Enrutamiento



Información de los Procesos

Desde administrador de tareas podemos ver los procesos del Sistema y los recursos que consume



Información de los Procesos

Otros comandos útiles para obtener información de los Procesos

- Tasklist: Muestra información de los procesos en la consola
- Pslist: Herramienta Systernals que proporciona información compacta de los procesos
- ListDlls: Muestra las librerías relacionadas con cada proceso

Tasklist

Administrador: Símbolo del sistema

```
^C
C:\Sysinternals\ListDlls>tasklist /v

Nombre de imagen                PID Nombre de sesión Núm. de ses Uso de memor Est
ado           Nombre de usuario                                    Tiempo de CP Tít
ulo de ventana
========================= ======== ================ =========== ============ ===
============ ============================================== ============ ===
=============================================================================
System Idle Process              0 Services                   0         20 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:06:28 N/D

System                           4 Services                   0      3.804 KB Unk
nown          N/D                                                    0:03:53 N/D

smss.exe                       404 Services                   0        908 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:00 N/D

csrss.exe                      644 Services                   0      4.264 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:02 N/D

wininit.exe                    704 Services                   0      3.444 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:00 N/D

csrss.exe                      732 Console                    1      7.728 KB Run
ning          NT AUTHORITY\SYSTEM                                    0:01:31 N/D

services.exe                   780 Services                   0      9.988 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:09 N/D

winlogon.exe                   800 Console                    1      8.016 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:00 N/D

lsass.exe                      820 Services                   0     13.056 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:05 N/D

svchost.exe                    932 Services                   0      9.464 KB Unk
nown          NT AUTHORITY\SYSTEM                                    0:00:02 N/D

svchost.exe                    980 Services                   0      9.156 KB Unk
nown          NT AUTHORITY\Servicio de red                           0:00:07 N/D
```

Pslist

Administrador: Símbolo del sistema

```
C:\Sysinternals\PSTools>pslist.exe

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for TULI:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   4    0      0      0:01:59.711     0:00:00.000
System                4   8 160 1060    160      0:03:54.272    32:35:55.846
smss                404  11   2   36    288      0:00:00.156    32:35:55.846
csrss               644  13   9  417   1960      0:00:02.671    32:35:30.564
wininit             704  13   2   72    896      0:00:00.156    32:35:28.564
csrss               732  13  11  421   2428      0:01:31.781    32:35:28.548
services            780   9  14  258   5868      0:00:09.562    32:35:28.001
winlogon            800  13   3  144   1384      0:00:00.390    32:35:28.001
lsass               820   9   7  943   6368      0:00:05.812    32:35:27.954
svchost             932   8   7  386   3612      0:00:02.984    32:35:27.689
svchost             980   8   9  440   5432      0:00:07.265    32:35:27.579
svchost             424   8  22  811  16764      0:00:11.328    32:35:27.517
dwm                 656  13   5  226  70596      0:03:59.331    32:35:27.485
svchost             824   8  44 1719  18972      0:00:18.265    32:35:27.423
svchost             772   8  17  566  12292      0:00:07.375    32:35:27.376
svchost            1124   8  21  631  70636      0:06:45.500    32:35:27.282
svchost            1236   8  33  820  19120      0:00:42.984    32:35:27.095
spoolsv            1424   8  10  336   3328      0:00:00.437    32:35:26.845
svchost            1460   8  21  447  19884      0:00:11.531    32:35:26.829
armsvc             1664   8   3   75   1096      0:00:00.031    32:35:24.095
kms                1716   8   3   48    800      0:00:00.015    32:35:23.845
svchost            1852   8   7  142   2132      0:00:00.234    32:35:23.688
TeamViewer_Service  1892   8   6  940   3744      0:00:00.343    32:35:23.673
vmnat              1948   8   5   97   1492      0:00:00.296    32:35:23.626
wlms               1976   8   3   38    572      0:00:00.046    32:35:23.595
vmware-authd       2044   8   7  225   3656      0:00:20.734    32:35:23.470
vmnetdhcp          2092   8   3   50   1112      0:00:00.062    32:35:22.891
vmware-usbarbitrator64  2112   8   4  151   1980      0:00:00.109    32:35:22.876

taskhostex         2080   8  10  270   6804      0:00:04.203    32:34:58.312
```

ListDlls

Administrador: Símbolo del sistema

```
^C
C:\Sysinternals\ListDlls>Listdlls.exe

ListDLLs v3.1 - List loaded DLLs
Copyright (C) 1997-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

------------------------------------------------------------------------------
smss.exe pid: 404
Command line: \SystemRoot\System32\smss.exe

Base                    Size       Path
0x00000000c2b60000   0x25000    C:\Windows\System32\smss.exe
0x000000000808b0000   0x1be000   C:\Windows\SYSTEM32\ntdll.dll
------------------------------------------------------------------------------
csrss.exe pid: 644
Command line: %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSec
tion=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerD
ll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off Ma
xRequestThreads=16

Base                    Size       Path
0x0000000090aa0000   0x7000     C:\Windows\system32\csrss.exe
0x000000000808b0000   0x1be000   C:\Windows\SYSTEM32\ntdll.dll
0x000000007d870000   0x13000    C:\Windows\system32\CSRSRV.dll
0x000000007d850000   0x12000    C:\Windows\system32\basesrv.DLL
0x000000007d810000   0x32000    C:\Windows\system32\winsrv.DLL
0x000000007e090000   0x14c000   C:\Windows\system32\USER32.dll
0x000000007da90000   0xf3000    C:\Windows\SYSTEM32\kernelbase.dll
0x000000007e6d0000   0x136000   C:\Windows\SYSTEM32\kernel32.dll
0x000000007df40000   0x140000   C:\Windows\system32\GDI32.dll
0x000000007d800000   0xd000     C:\Windows\system32\sxssrv.DLL
0x000000007d710000   0xb2000    C:\Windows\system32\sxs.dll
0x000000007ee80000   0x140000   C:\Windows\system32\RPCRT4.dll
0x000000007d620000   0xa000     C:\Windows\system32\CRYPTBASE.dll
0x000000007d5c0000   0x5c000    C:\Windows\system32\bcryptPrimitives.dll
------------------------------------------------------------------------------
wininit.exe pid: 704
Command line: wininit.exe
```

Mapeo de Procesos a Puerto(s)

TCPView

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Lo...	Local Port	Remote Address	Remote Port	State	S
avp.exe	1432	TCP	tuli.vi...	63637	111.221.74.12	https	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	63648	91.190.216.58	https	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	63670	65.54.49.39	https	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	64818	65.52.244.89	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	64819	157.56.29.215	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	64821	65.52.244.89	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	64829	157.56.29.215	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65246	31.13.78.65	https	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65264	63.251.85.33	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65271	65.52.103.78	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65276	69.31.75.224	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65288	23.33.187.99	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65291	66.235.139.153	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65295	64.4.11.30	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65297	157.56.148.23	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65309	107.14.43.251	http	ESTABLISHED	
avp.exe	1432	TCP	tuli.vi...	65317	157.56.23.43	http	ESTABLISHED	

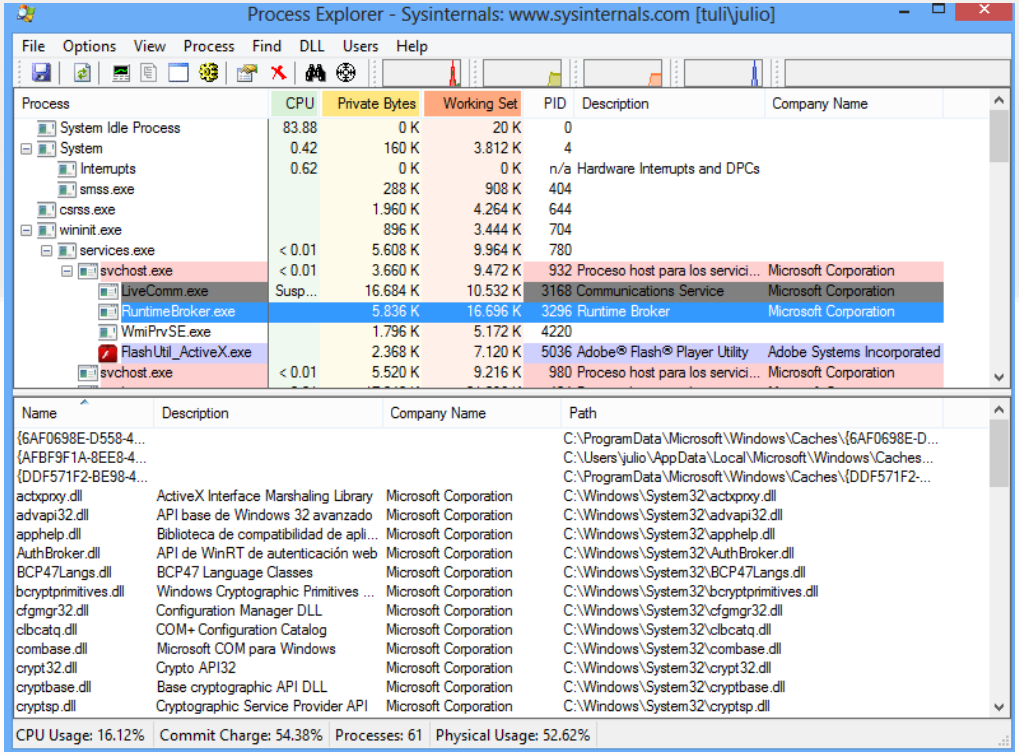
Mapeo de Procesos a Puerto(s)

netstat –o permite ver los puertos utilizados por los PIDs (Process Identifiers)

```
C:\Sysinternals\PSTools>netstat -o

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    127.0.0.1:1110         tuli:63634             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:63647             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:63669             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:64814             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:64816             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:64817             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:64826             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:65245             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:65326             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:65329             ESTABLISHED     1432
  TCP    127.0.0.1:1110         tuli:65336             ESTABLISHED     1432
  TCP    127.0.0.1:63634        tuli:nfsd-status       ESTABLISHED     4804
  TCP    127.0.0.1:63647        tuli:nfsd-status       ESTABLISHED     4804
  TCP    127.0.0.1:63669        tuli:nfsd-status       ESTABLISHED     4804
  TCP    127.0.0.1:64814        tuli:nfsd-status       ESTABLISHED     2656
  TCP    127.0.0.1:64816        tuli:nfsd-status       ESTABLISHED     2656
  TCP    127.0.0.1:64817        tuli:nfsd-status       ESTABLISHED     2656
  TCP    127.0.0.1:64826        tuli:nfsd-status       ESTABLISHED     2656
  TCP    127.0.0.1:65245        tuli:nfsd-status       ESTABLISHED     4248
  TCP    127.0.0.1:65247        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65259        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65263        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65269        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65274        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65286        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65290        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65294        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65296        tuli:nfsd-status       TIME_WAIT       0
  TCP    127.0.0.1:65304        tuli:nfsd-status       TIME_WAIT       0
```

Memoria del Proceso

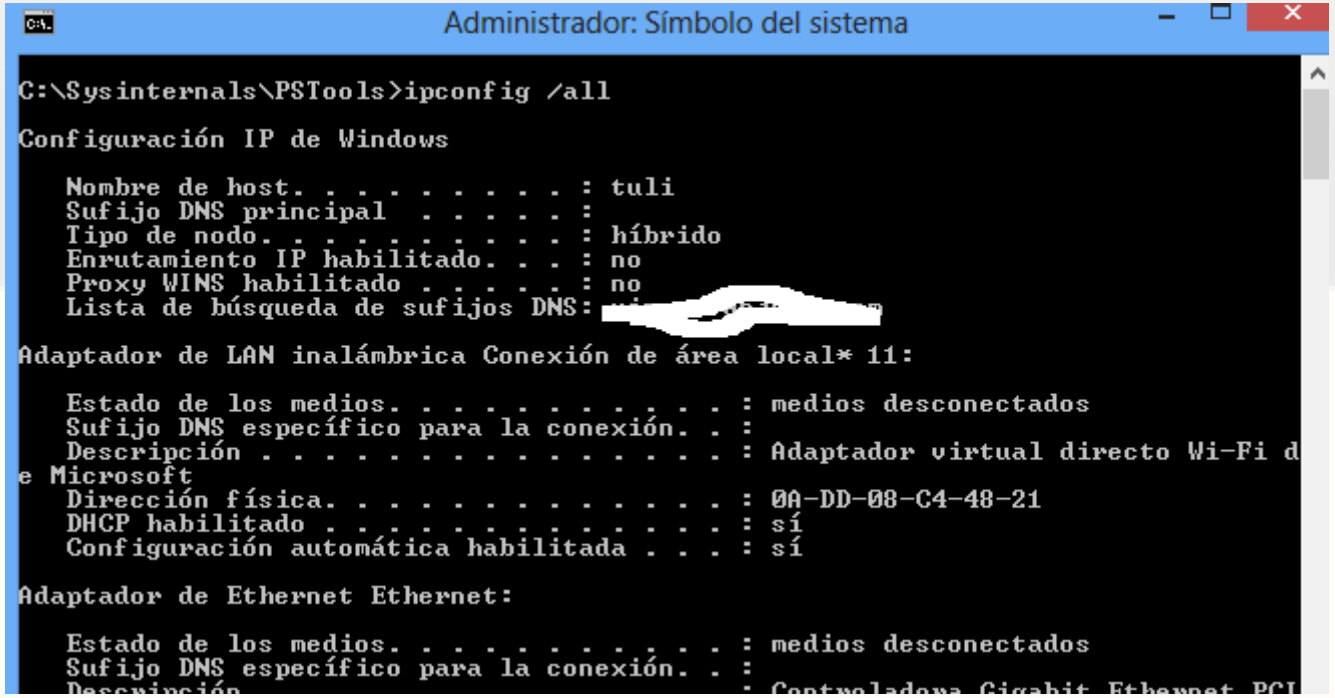
El programa ProcessExplorer puede ayudar a detectar programas maliciosos o sospechosos



Para volcado de memoria utilizar programas como pmdump o userdump

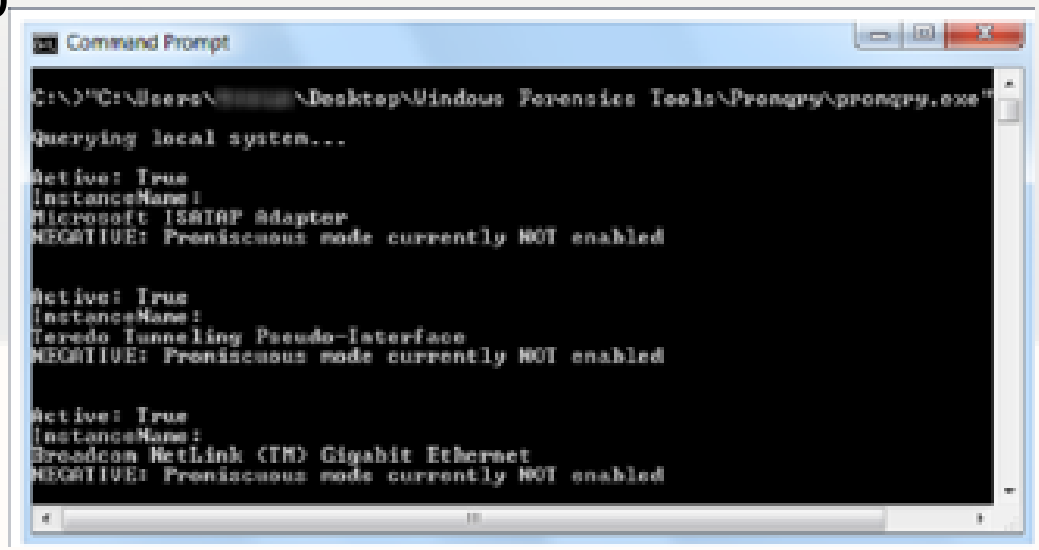
Estado de la red

Ipconfig permite ver información sobre las tarjetas NIC y Wireless



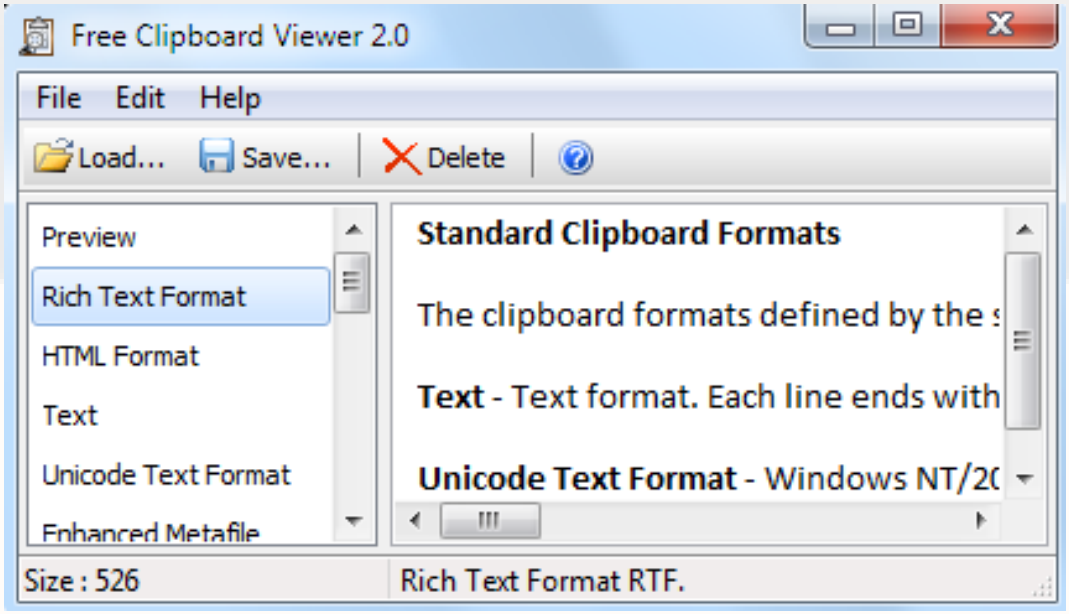
Estado de la red

Promqry permite ver si existen tarjetas de red en modo promiscuo



Portapapeles

El portapapeles guarda temporalmente información copiada (Ctrl C)

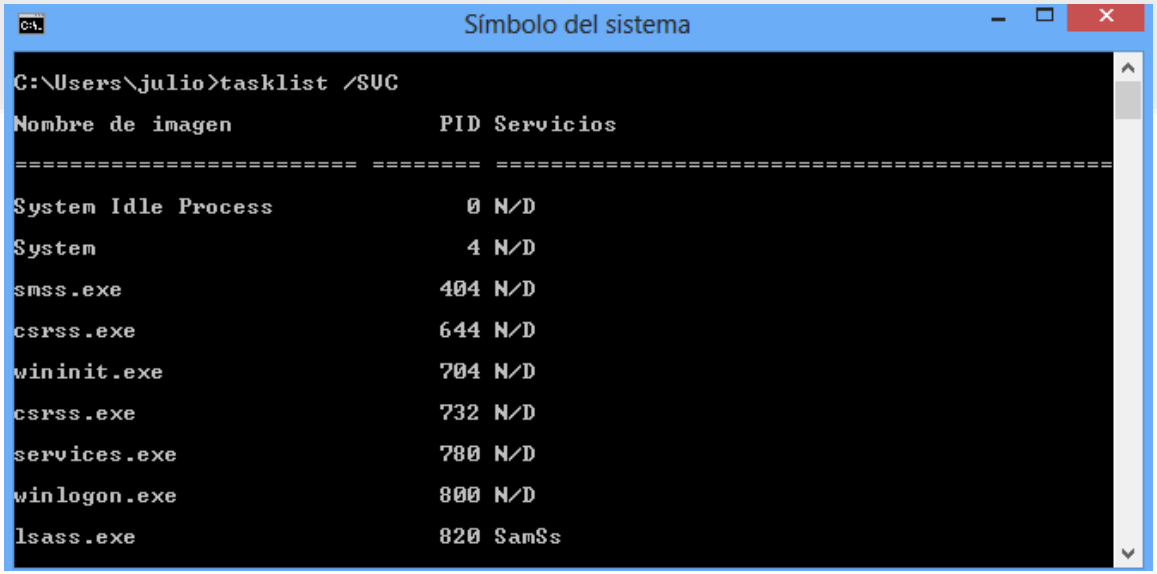


Free Clipboard Viewer 2.0 permite ver lo que está copiado en el Portapapeles

Servicios

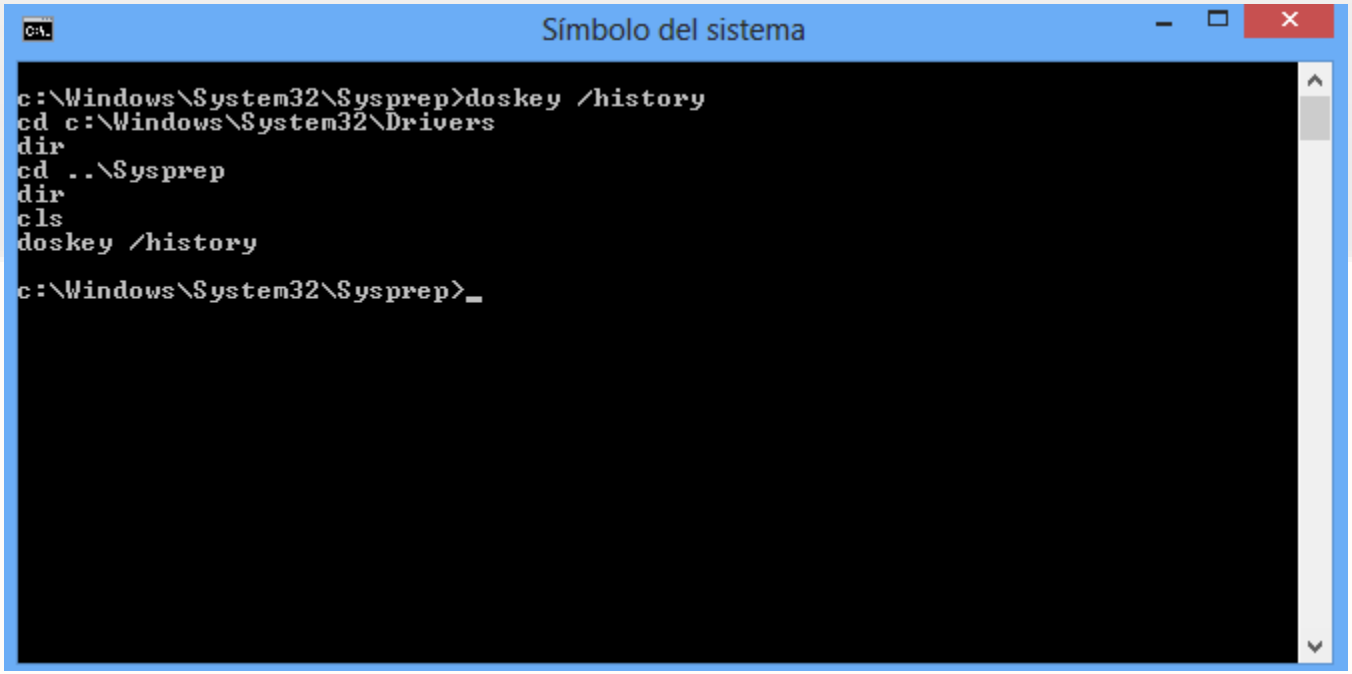
Muchos malware pueden ser instalados como servicios.

Para ver los servicios del S.O. ejecutamos el comando services.msc o bien ***tasklist /SVC***



Historial de comandos

Doskey /history nos muestra el historial de comandos introducidos en la consola actual



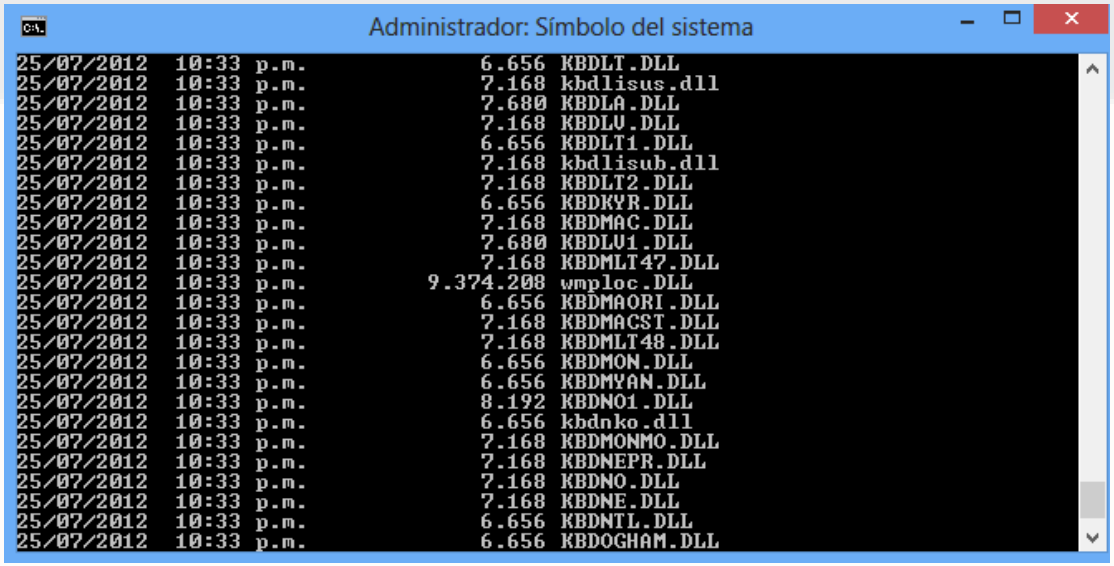
Recolectando información no volátil

- A continuación veremos cómo recolectar información no volátil

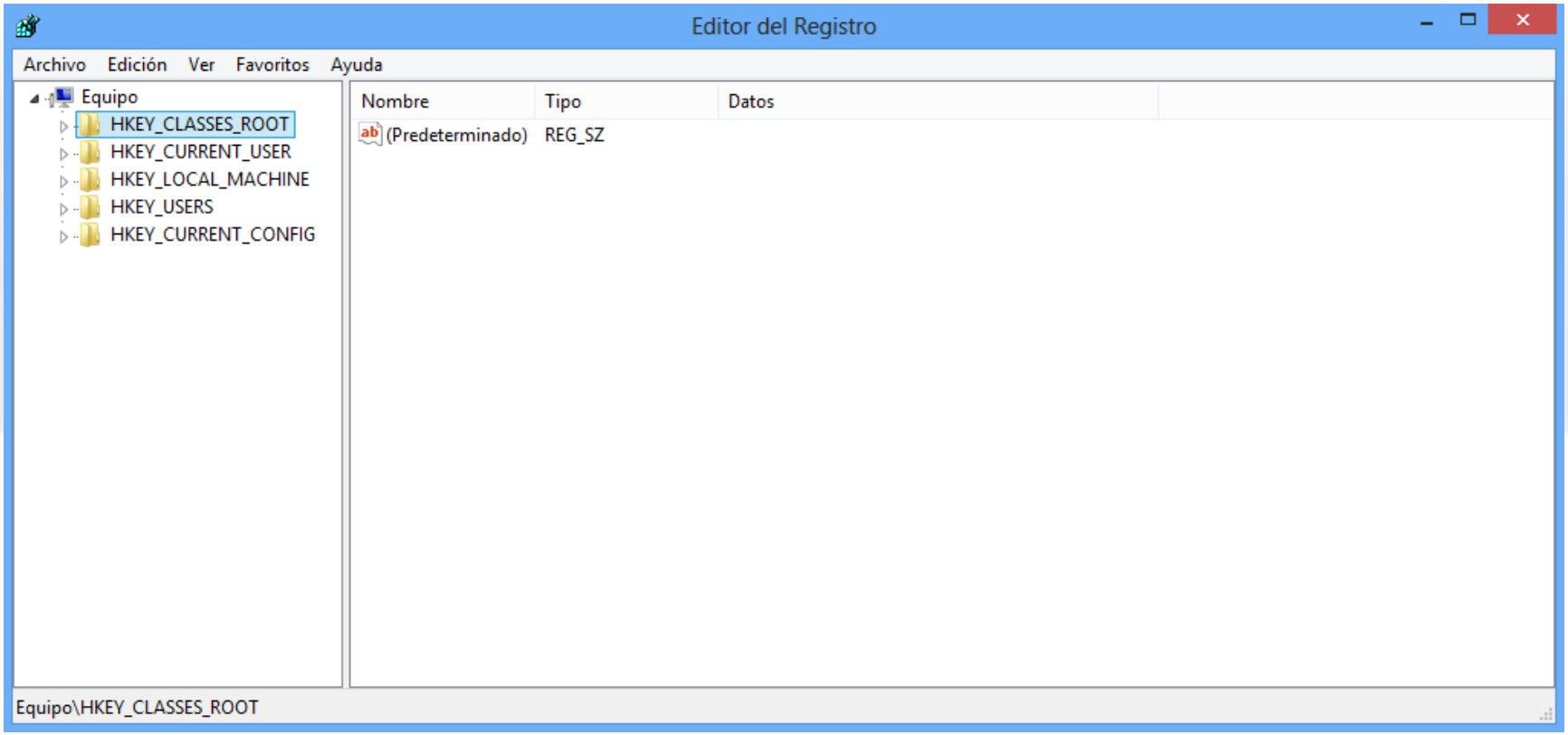
Examinando el Sistema de Archivos

Con el comando ***dir /o:d under systemroot%\system32***

Esto habilita al investigador a obtener información sobre la fecha y hora de la instalación del S.O., como también de los Service Packs, parches y subdirectorios que se actualizaron



El registro de Windows



El registro de Windows

- El registro de Windows es un conjunto de archivos que contienen información acerca de cómo funciona un equipo de computación, en otras palabras es tan sólo una base de datos jerárquica donde Windows almacena su propia configuración, la del hardware, la de las aplicaciones instaladas y la personalización de cada usuario, si se han creado perfiles.

El registro de Windows

La Información en el Registro se ordena en un sistema de árbol como las carpetas y ficheros, muy parecido al explorador. En el Registro, la información se guarda en claves. Estas son similares a las carpetas. Las claves pueden tener subclaves igual que las carpetas tienen subcarpetas. El dato contenido en una clave se llama valor. Algo como un fichero. Los datos en realidad pueden tener muchos formatos y pueden ser una cadena, un número o una serie de números.

El registro de Windows

Secciones del Registro

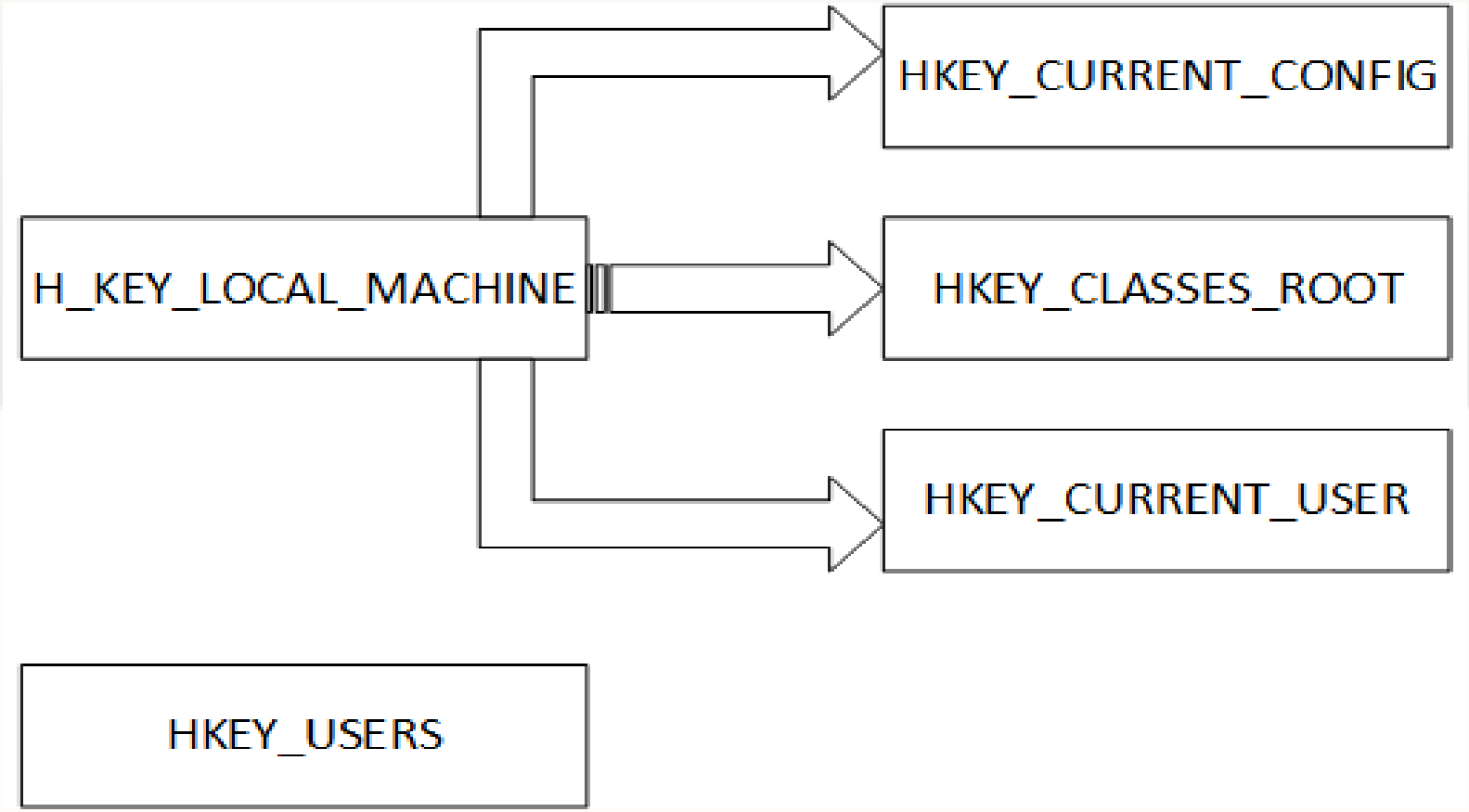
El registro está dividido en 5 secciones que son:

- **HKEY_CURRENT_USER:** Contiene la información de configuración del usuario que ha iniciado sesión. Las carpetas del usuario, los colores de la pantalla y la configuración del Panel de control se almacenan aquí. Esta clave a veces aparece abreviada como HKCU.
- **HKEY_LOCAL_MACHINE:** Contiene información de configuración específica del equipo (para cualquier usuario). Esta clave a veces aparece abreviada como HKLM.

El registro de Windows

- **HKEY_CLASSES_ROOT:** La información que se almacena aquí garantiza que cuando abra un archivo con el Explorador de Windows se abrirá el programa correcto. Contiene la relación entre las extensiones de archivos (lo que está al final del nombre de archivo, después del punto), y los archivos en el sistema. También la puedes encontrar en la subclave de HKEY_LOCAL_MACHINE\Software.
- **HKEY_CURRENT_CONFIG:** Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.
- **HKEY_USERS:** Contiene todos los perfiles de usuario cargados activamente en el equipo. HKEY_CURRENT_USER es una subclave de HKEY_USERS. HKEY_USERS puede aparecer abreviada como HKU.

El registro de Windows



El registro de Windows

Tipos de datos utilizados en el Registro

- **Valor de cadena REG_SZ:** Cadena de texto de longitud fija.
- **Valor binario REG_BINARY:** Datos binarios sin formato. La mayoría de la información sobre componentes de hardware se almacena en forma de datos binarios y se muestra en formato hexadecimal en el Editor del Registro.
- **Valor DWORD REG_DWORD:** Datos representados por un número de 4 bytes de longitud (un valor entero de 32 bits). Muchos parámetros de controladores de dispositivo y servicios son de este tipo y se muestran en el Editor del Registro en formato binario, hexadecimal o decimal.

El registro de Windows

- **Valor de cadena múltiple:** REG_MULTI_SZ Cadena múltiple. Valores que contienen listas o valores múltiples; este es el formato cuya lectura resulta más sencilla. Las entradas aparecen separadas por espacios, comas u otros signos de puntuación.
- **Valor de cadena expandible:** REG_EXPAND_SZ Cadena de datos de longitud variable. Este tipo de datos incluye variables que se resuelven cuando un programa o servicio utiliza los datos.

El registro de Windows

Ubicación de los Archivos del Registro

1. El primer directorio, en el se guardan los archivos más importantes, se encuentra en:
2. C:\Windows\System32\config\
3. Entre otros están los siguientes archivos que contienen datos de las ramas correspondientes:
    1. Security - HKEY_LOCAL_MACHINE\SECURITY
    2. Software - HKEY_LOCAL_MACHINE\SOFTWARE
    3. Sam - HKEY_LOCAL_MACHINE\SAM
    4. System - HKEY_LOCAL_MACHINE\SYSTEM
    5. Default - HKEY_USERS\.DEFAULT

El registro de Windows

1. En cada carpeta de usuario se encuentra un archivo de nombre Ntuser.dat, contiene los datos referentes a la rama de dicho usuario.
   La ruta es: C:\Users\NombreDeUsuario\Ntuser.dat
2. Un tercer archivo se encuentra en: C:\Users\NombreDeUsuario\AppData\Local\Microsoft\Windows\UsrClass.dat
3. Otros archivos se encuentran en: C:\Windows\ServiceProfiles\LocalService
4. La localización de todos está registrada en la siguiente clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist
   Como comprenderás no es factible hacer un respaldo manualmente de los archivos del registro, para eso lo ideal es emplear el comando REGEDIT /E

El registro de Windows

- Regedit.exe
- Reg.exe

El registro de Windows

Algunos registros importantes

- MACHINE/System/CurrentControlSet/Control/Session Manager/Memory Management/ClearPageFileAtShutdown
- Este registro le indica al S.O. que limpie el archivo de paginación cuando éste se apague. Cuando el S.O. se apague, la información del archivo de paginación permanecerá en el Disco, esta información puede ser porciones de conversaciones IM, contraseñas descifradas, y otras cadenas y bits que pueden proporcionar información importante para la investigación.

El registro de Windows

Más registros importantes

- NKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\Disablelastaccess
  - Valor Disablelastaccess a 1
- Windows XP y Windows Server 2003 tienen la habilidad de deshabilitar la actualización de los últimos accesos en los archivos

El registro de Windows

Más registros importantes

- AutoRuns
- Muchas áreas en el registro son referidas como ubicaciones de auto inicio, y tienen la habilidad de proveer inicio automático a las aplicaciones
- Estas aplicaciones inician cuando el Sistema Inicia, inicia sesión el usuario y cuando un usuario realiza una acción en particular
- Se puede recolectar información específica de algunos valores o llaves con el comando reg.exe o la herramienta AutoRuns

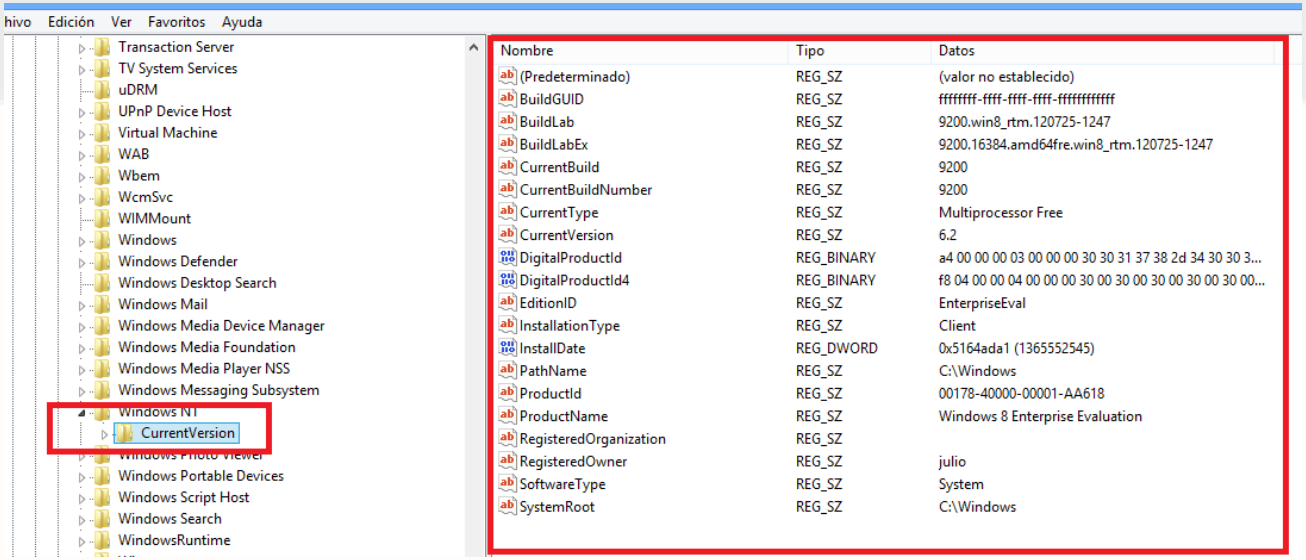
Examinando el Registro

- Nombre actual del equipo: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
- Encontrar el momento en que el equipo fue apagado la última vez en: HEY_LOCAL_MACHINE\System\ControlSet00x\Control\Windows

  Generalmente será ControlSet001, o ControlSet002

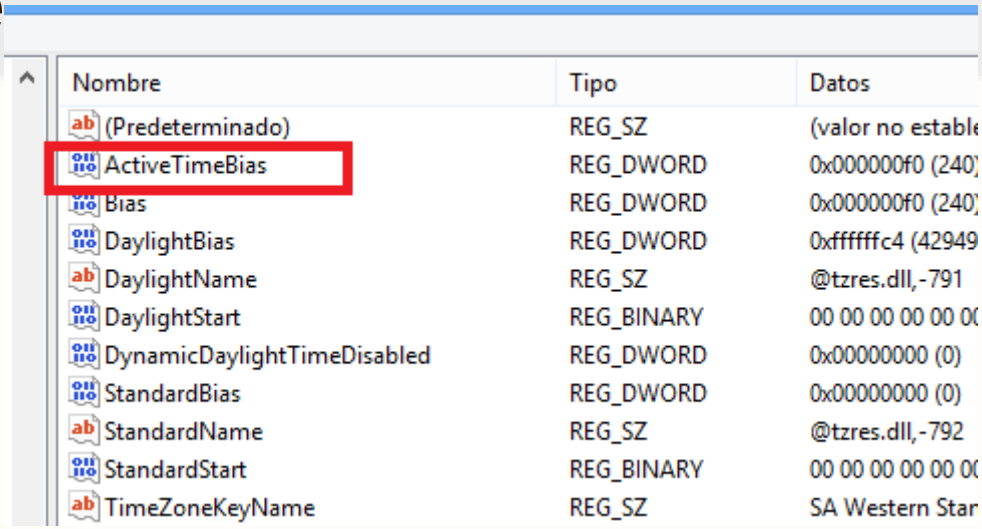
Examinando el Registro

- Información sobre Nombre del producto, versión, etc. Se encuentra en la clave: HEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion



Examinando el Registro

- La Información sobre la Zona Horaria se encuentra en: HEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
- ActiveTimeBias permite normalizar o traducir las horas a otras fuentes



Examinando el Registro

- La información sobre recursos compartidos se encuentra en: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\Shares

Examinando el Registro

- Cuando un usuario inicia sesión, algunas claves del registro son accedidas y analizadas:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

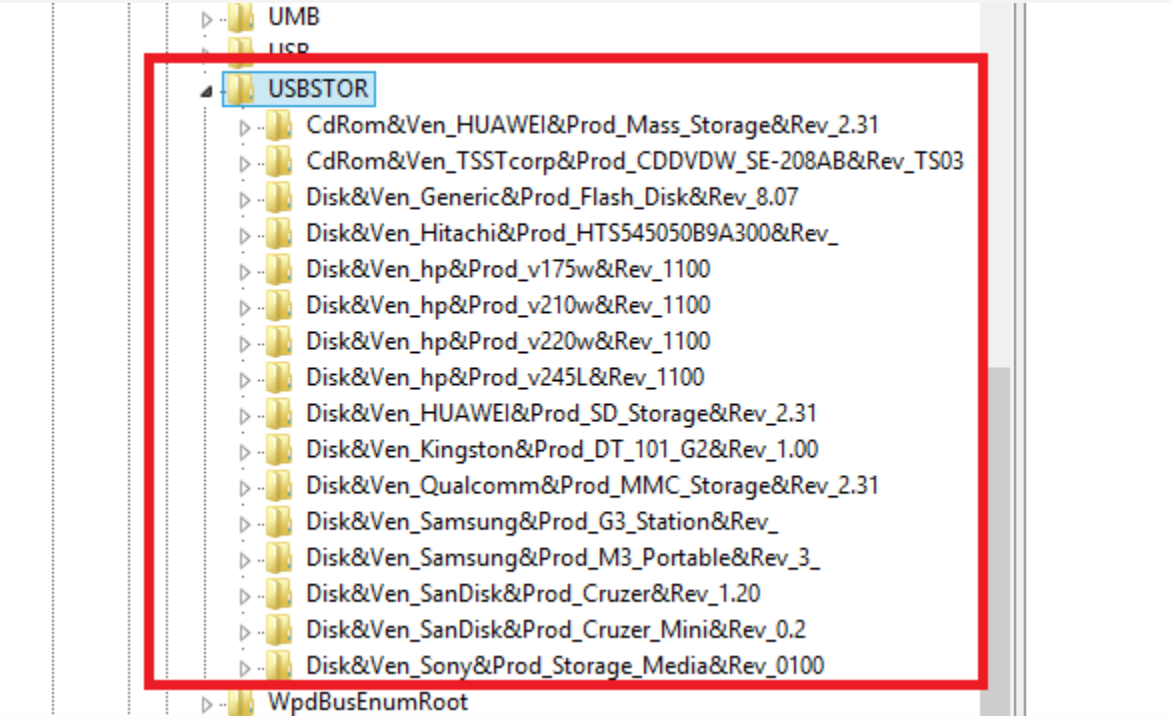
Examinando el registro

- Las ubicaiones del Registro de auto inicio son accedidos cuando el usuario realiza cualquier acción como abrir una aplicación como Internet Explorer, Outlook, etc.
- Buscar malware en estas ubicaciones
  - HKEY_LOCAL_MACHINE\Software\Classes\Exefile\Shell\Open\command
  - HKEYE_CLASSES_ROOT\Exefile\Shell\Open\Comand
- Windows provee la habilidad de alertar funciones externas con ciertos eventos que ocurren en el sistema, como cuando un usuario inicia o cierra sesión o cuando el protecctor de pantalla inicia. Estas notificaciónes están en:
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Examinando el Registro

- Cuando un dispositivo USB es conectado al equipo, el Administrador de Plug and Play (PnP Manager) consulta el descriptor del dispositivo en el firmware buscando información sobre el dispositivo
- El Administrador PnP utiliza esta información para localizar el controlador apropiado para el dispositivo, y carga el controlador si es necesario
- Cuando un dispositivo es identificado, la clave de registro será creada debajo de la clave:
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

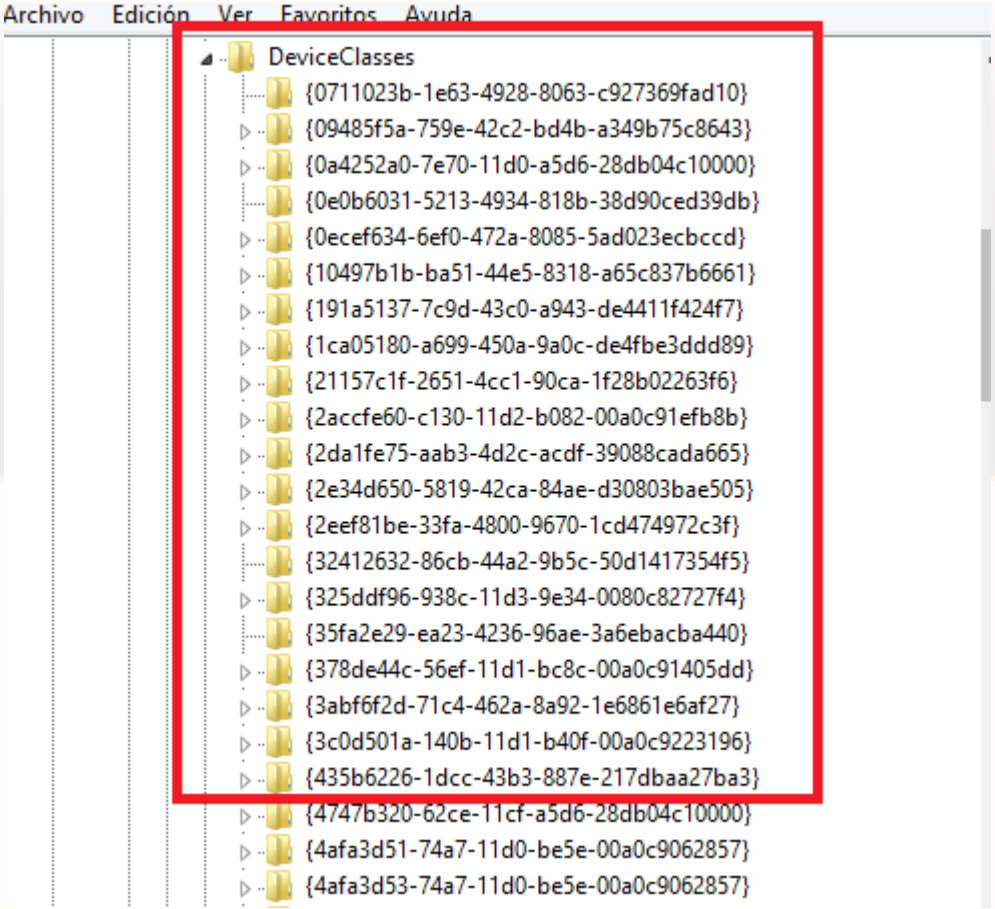
Examinando el Registro



Examinando el Registro

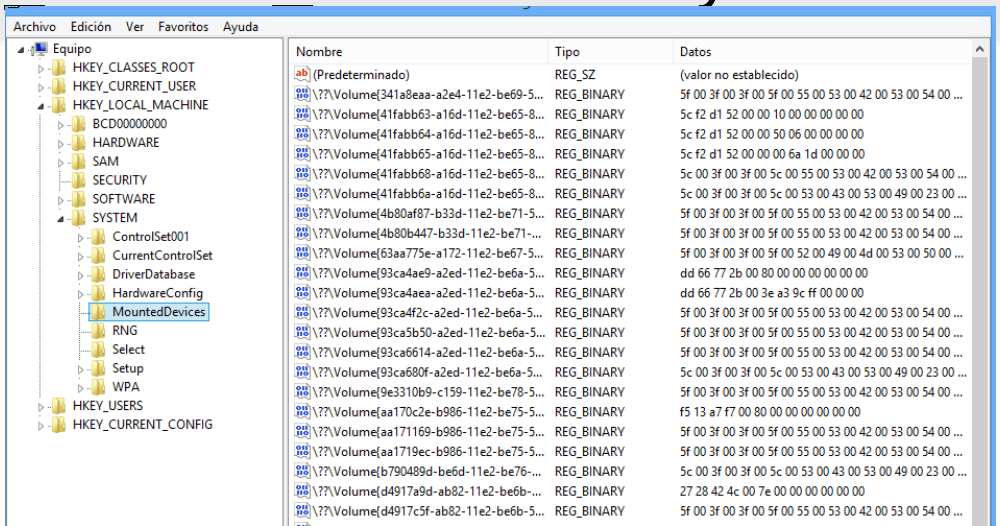
- ParentIdPrefix determina la última vez que un dispositivo USB fue conectado. Este valor puede ser utilizado para correlacionar información adicional en conjunto con el registro.
- Navegar hasta la clave: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\DeviceClasses
- Acá están los GUIDs (Identificadores Globales Únicos) para discos y dispositivos de almacenamiento

Examinando el Registro



Examinando el Registro

- La clave MountedDevices almacena información sobre varios dispositivos y volúmenes montados en el sistema de archivo NTFS
- La ruta es: HKEY_LOCAL_MACHINE\System\MountedDevice



Microsoft Security Identifiers

- La ubicación de los Microsoft Security IDs se encuentra en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- La herramienta **Magical Jelly Bean Keyfinder** revela el CD-Key de Windows 7

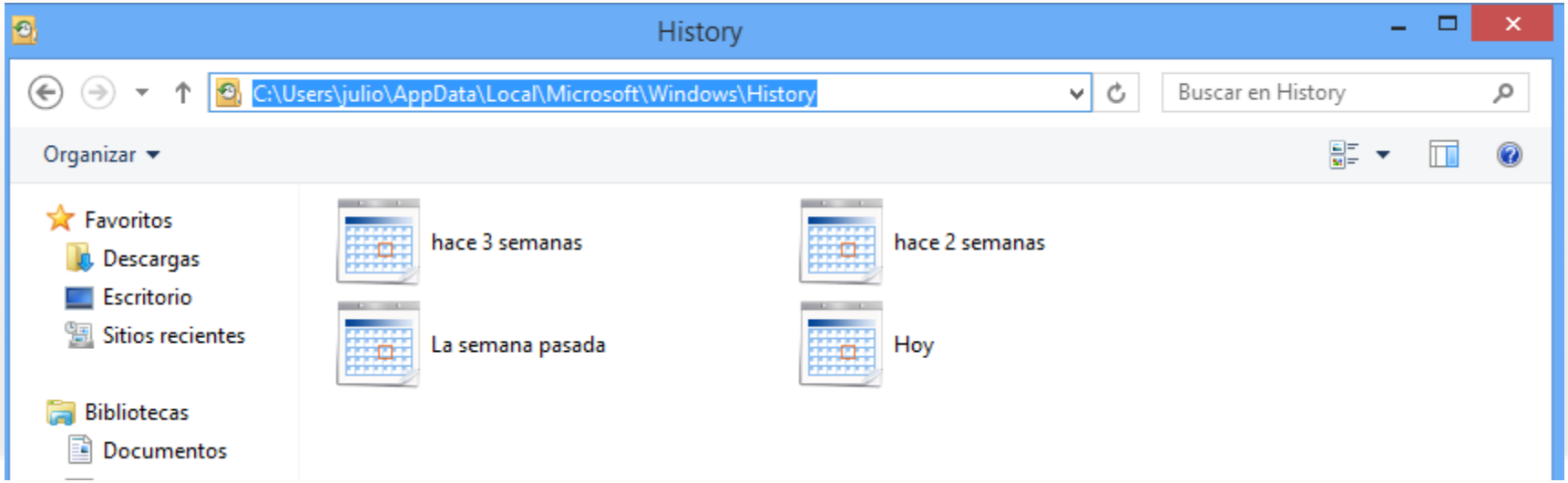
Visor de Eventos

1. El visor de eventos cambia de acuerdo a qué eventos están siendo auditados y cómo son configurados
2. Elegir que datos se quieren recolectar
3. Utilizar herramientas como psloglist.exe para recibir información de los registros de eventos
4. Copiar los archivos .evt desde el Sistema

Archivo Index.dat

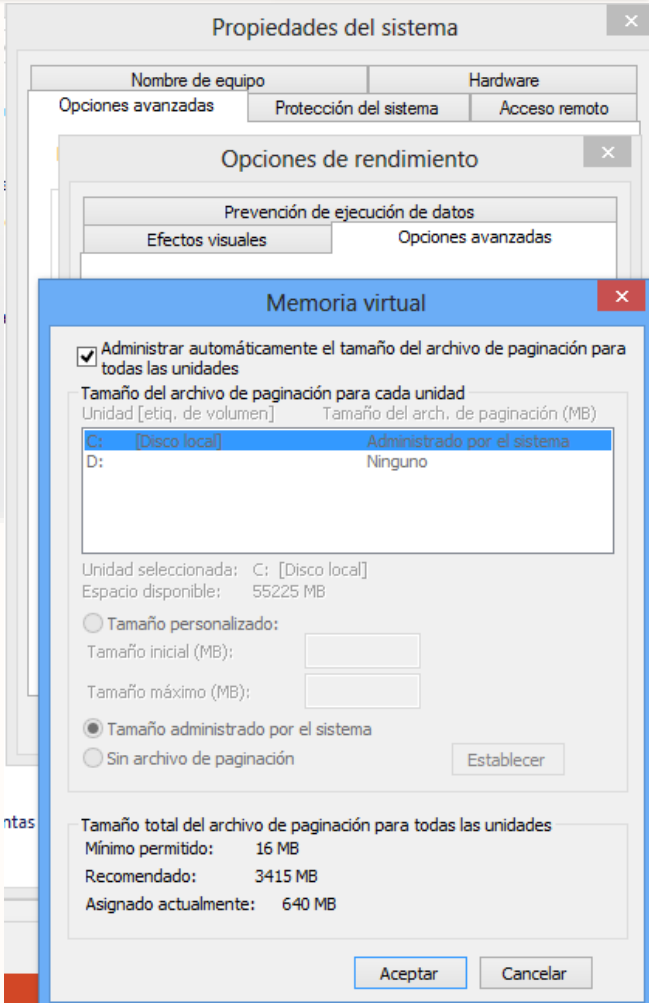
- Este archivo es utilizado por el navegador Internet Explorer como una base de datos activa, la cual corre mientras el usuario está logueado en Windows
- Es un repositorio de información redundante, como URLs visitadas, consultas de búsquedas, archivos abiertos recientemente, información de auto completar
- Existen archivos index.dat separados para el historial de Internet Explorer, caché y cookies

Archivo Index.dat

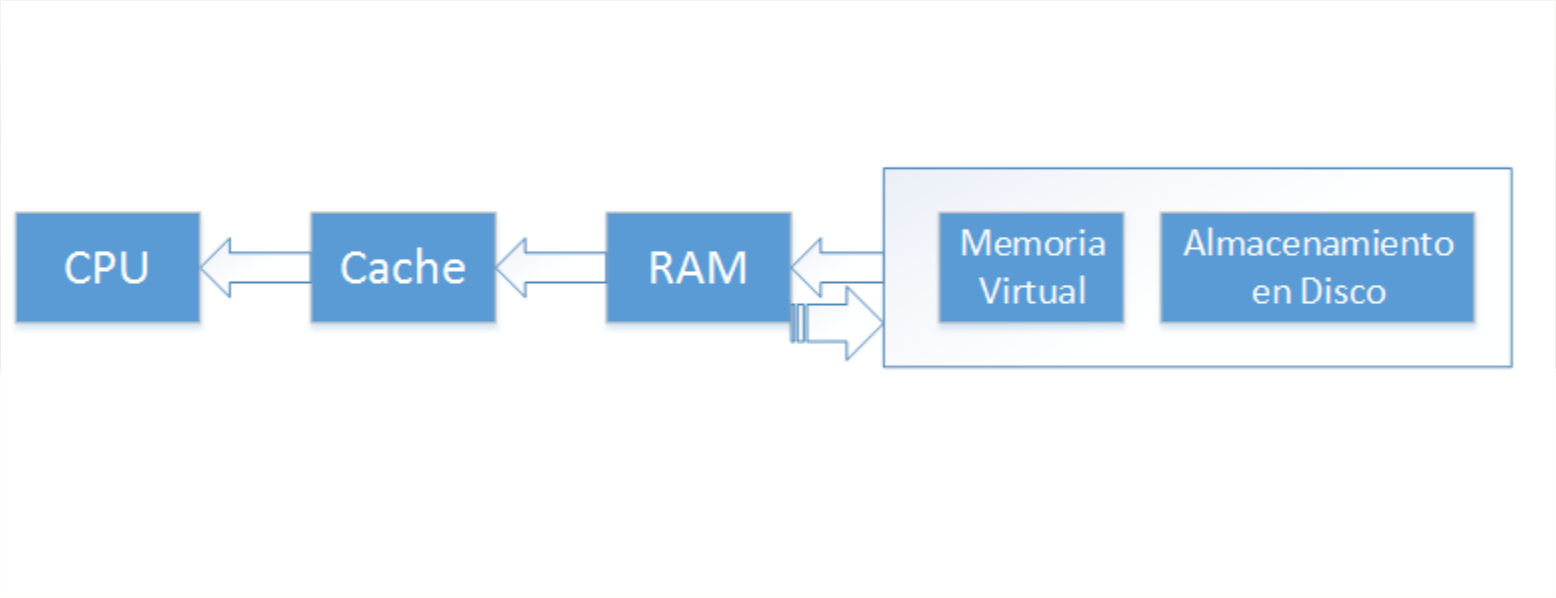


Memoria Virtual

- La memoria Virtual (o lógica) es un concepto que permite a los programadores utilizar un rango grande de memoria o direcciones de almacenamiento para datos guardados.
- Se puede utilizar herramientas como X-Ways Forensics para escanear la memoria virtual



Memoria Virtual



Archivo de Intercambio

- Un archivo de intercambio es espacio del disco duro utilizado como una extensión de la Memoria Virtual de la RAM de un equipo
- Estos archivos contienen información relevante como: archivos abiertos y sus contenidos, sitios Web visitados, chats online, correos enviados y recibidos
- En Windows, el archivo de intercambio está escondido (pagefile.sys)
- El registro del archivo de intercambio se encuentra en: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Particiones Escondidas

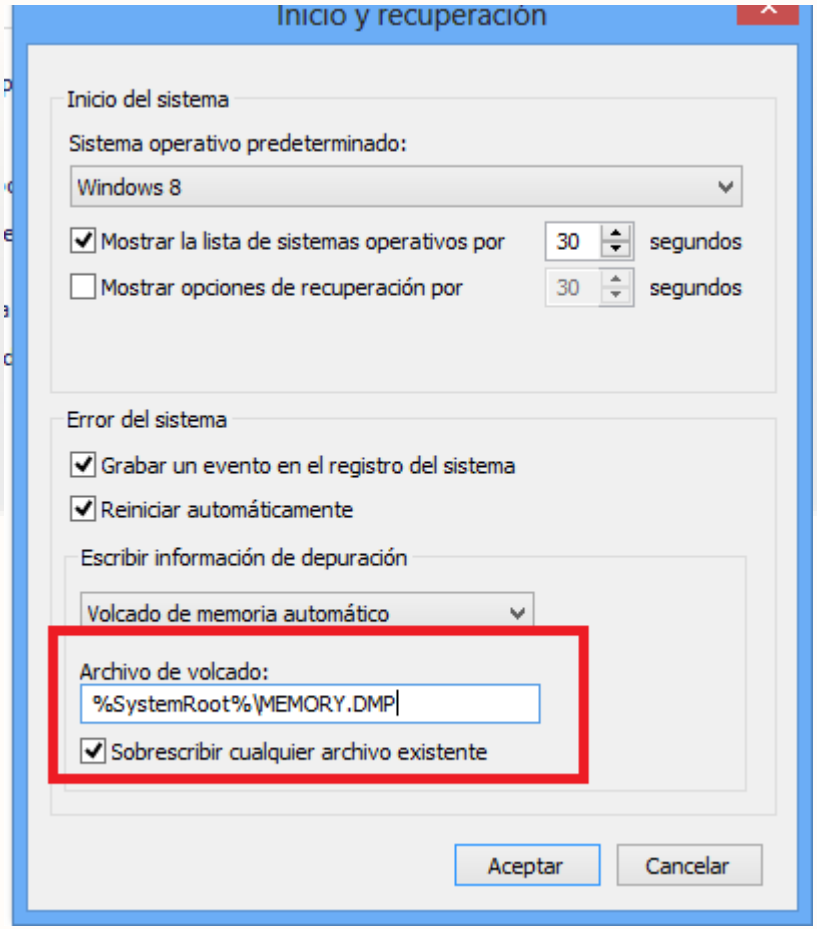
- Una partición escondida es una sección lógica del disco que no está accesible al Sistema Operativo
- Las particiones escondidas pueden contener archivos, carpetas, datos confidenciales o almacenar backup del Sistema
- Herramientas como Partition Login ayudan a recolectar información desde la partición escondida.
- Partition Logic puede crear, eliminar, borrar, formatear, desfragmentar, cambiar el tamaño, copiar y mover particiones

Análisis de la Memoria de Windows

Volcado de Memoria

- El volcado de la memoria registra información que ayuda a identificar el motivo por el cuál el equipo se detiene sin esperarlo
- Incluye información como mensajes de detención, procesador detenido y una lista de controladores cargados
- Los archivos de volcado de memoria pueden ser cargados utilizando una herramienta de revisión de volcado y puede verificar la creación apropiada de los mismos

Análisis de la Memoria de Windows



Recolectando Memoria del Proceso

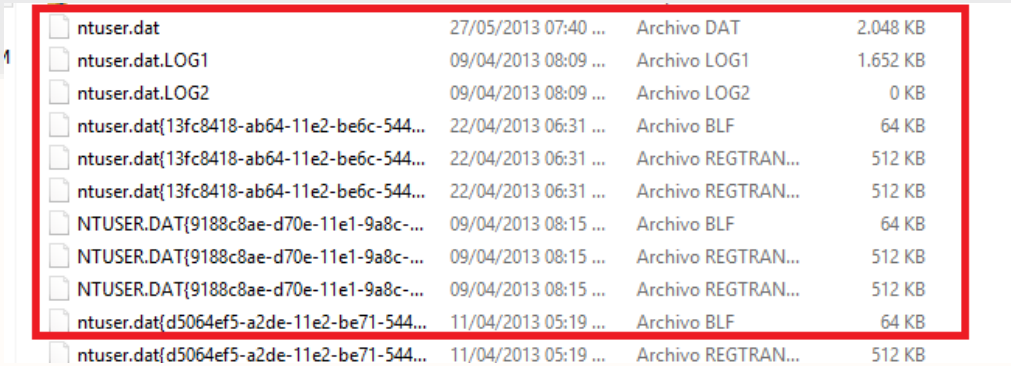
1. Recolectar los contenidos de la memoria del proceso disponible en un archivo de volcado de RAM
2. La herramienta pmdump.exe permite volcar los contenidos de las memorias de los procesos sin detenerse en el proceso
3. Process Dumper (pd.exe) vuelca el espacio entero junto con metadatos adicionales y el ambiente del proceso a la consola; redirecciona la salida a un archivo o socket
4. Userdump.exe vuelca cualquier proceso sin adjuntarlo al depurador y sin determinar el proceso una vez que el volcado haya sido completado

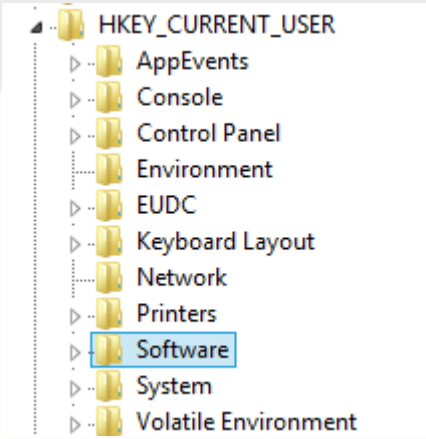
Recolectando Memoria del Proceso

1. Otras herramientas incluyen:
    1. BinText: Extrae código ASCII, Unicode, cadenas de recursos y demás de los archivos de volcado
    2. Handle.exe: Provee una lista de "manijas" que hayan sido abiertas por los procesos
    3. listdlls.exe: Muestra la ruta completa y la versión de varios módulos cargados por los procesos

Actividades del Usuario

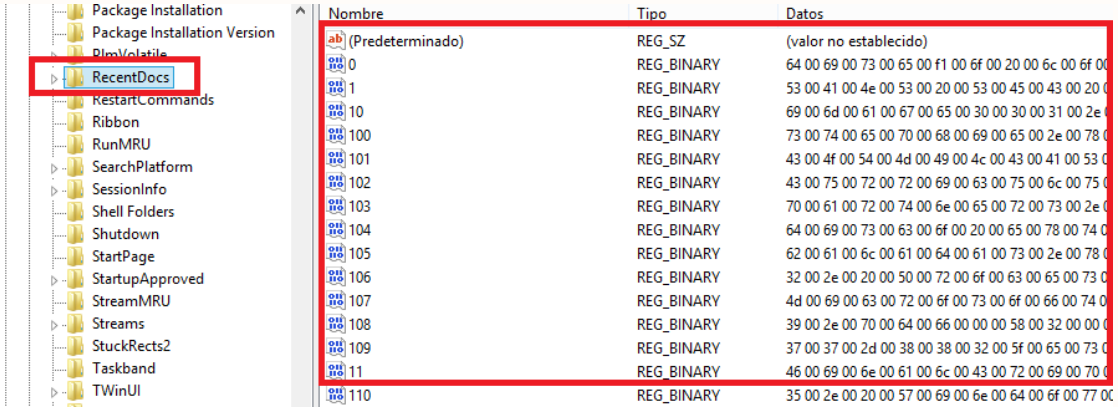
- Los registros de seguimiento de las actividades del usuario se encuentran en el archivo NTUSER.DAT
- La gran cantidad de actividades del usuario se encuentran en HKEY_CURRENT_USER





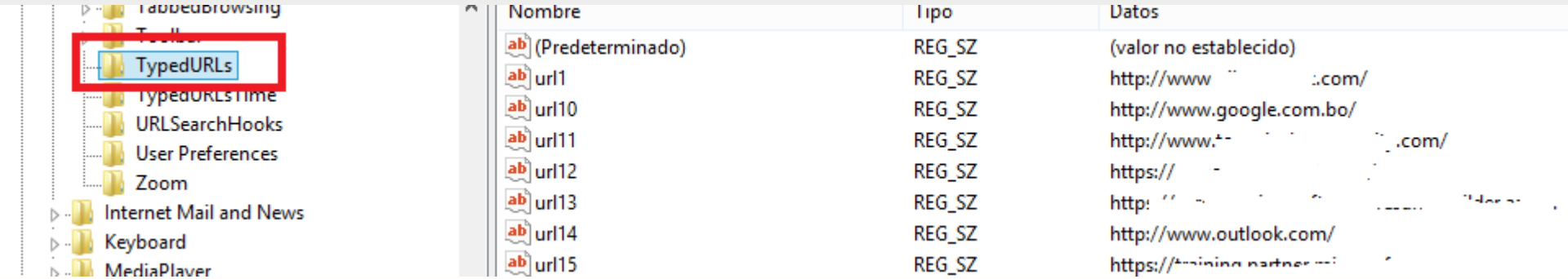
Listas MRU

- Las aplicaciones mantienen una lista MRU, que es una lista de archivos que tienen a lo que más se accedió recientemente
- La clave en cuestión es RecentDocs en HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



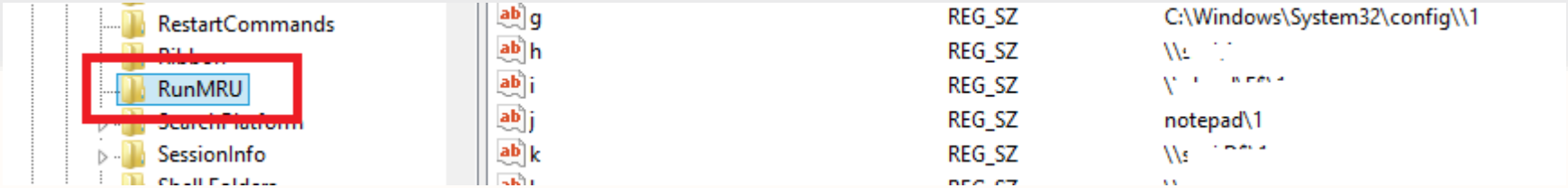
Listas MRU cont.

- Otro registro importante es TypedURLs que mantiene una lista de URLs que el usuario ha escrito en la barra de direcciones HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



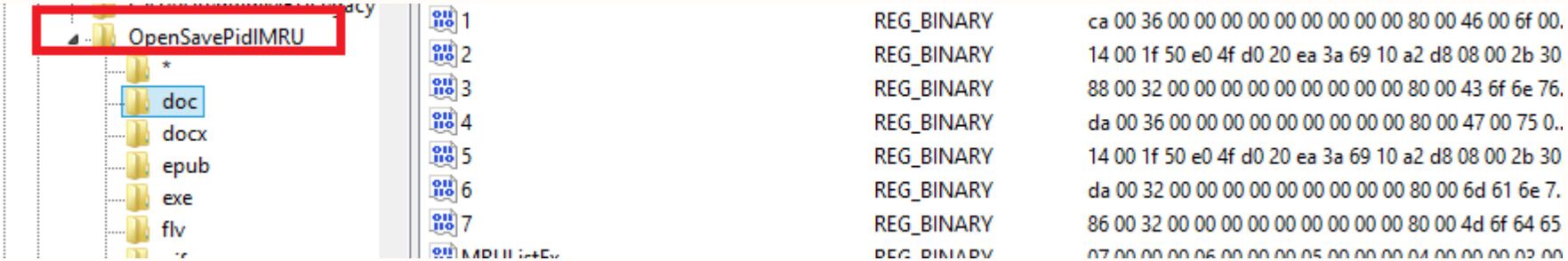
Listas MRU cont.

- Otro similar es el RunMRU que contiene la lista de valores escritos en el cuadro "Ejecutar como" HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU



Listas MRU cont.

- El siguiente mantiene una lista de archivos abiertos o guardados con “Abrir” o “Guardar como” (valga la redundancia) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU



Y más MRU

- La clave HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Map Network Drive MRU muestra las Unidades de Red
- La clave HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 muestra los volumenes que el usuario agregó con "net use"

Analizando los puntos de restauración desde el Registro

- El propósito de los puntos de restauración es tomar una instantánea del sistema, de manera que el usuario pueda restaurar a una versión previa
- Los ajustes de puntos de restauración están en: HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore
- Para ver los puntos de restauración enumerados ir a: \System Volume Information restore {GUID}\RP##

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Notas
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Todos los valores en esta clave son ejecutados al Iniciar el Sistema
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce	Todos los valores en esta clave son ejecutados al Iniciar el Sistema y borrados luego (se ejecuta una sola vez)
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon	El valor Shell será ejecutado cuando cualquier usuario inicie sesión. Este valor está ajustado a explorer.exe, pero puede ser cambiado a otro Explorador en una ubicación distinta

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Notas
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components	Cada subclave representa un componente instalado. Todas las subclaves son monitoreadas, y el valor SubPath en las subclaves.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	Valor Load, si está presente, ejecuta utilizando explorer.exe luego de que inicia
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run	Si Explorer y run están presentes, los valores debajo son ejecutados luego de que Explorer inicie

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Notas
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager	El valor BootExecute contiene archivos que son aplicaciones nativas ejecutadas antes de la ejecución de Windows
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	Contiene una lista de servicios que se ejecutan cuando el Sistema inicia. Si el valor Start es 2, el inicio es automático. Si el valor es 3, el inicio es manual. Si el valor es 4, el servicio está deshabilitado
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries	Estas subclaves son para servicios por capas, todos los valores son ejecutados antes de que el Usuario inicie sesión

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Nota
HKEY_LOCAL_MACHINE\System\ControlSet\Control\WOW	Cuando una aplicación de 16 bits es ejecutada, el programa listado en el valor cmdline es ejecutado
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Todos los valores en la subclave se ejecutan cuando el usuario inicia sesión
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce	Todos los valores en esta subclave se ejecutan cuando el usuario inicia sesión y luego es borrado
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup	Para este usuario específico, la clave es utilizada solo para configuración, luego un cuadro de diálogo hace el seguimiento de los progresos que los valores de esta clave se ejecutan de una en una

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Nota
HKEY_CURRENT_USER\Control Panel\Desktop	Para el usuario específico, el protector de pantalla está habilitado, un valor llamado srnsave.exe está presente.
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows	Para el usuario específico, la cadena especificada en el valor es ejecutada cuando el usuario inicie sesión
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	Para el usuario específico, la cadena especificada en el valor es ejecutada cuando el usuario inicie sesión

Determinando las ubicaciones del inicio del Sistema

Clave de Registro	Nota
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	El valor Startup será C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup donde %username% es el nombre del usuario actual
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	El valor Startup será %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Acá se encuentran las rutas de le los Documentos, escritorio, etc. públicos

Análisis de Navegadores, caché, cookies e historial

Internet Explorer

- Todas las actividades del usuario en Internet Explorer están almacenadas en: C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5
- Los directorios de Actividad de IE que contienen las actividades de historial sin contenido en caché local: C:\Users\%username%\AppData\Local\Microsoft\Windows\History
- Las cookies C:\Users\%username%\AppData\Local\Microsoft\Windows\Cookies
- Investigar estos tres directorios para buscar información almacenada de actividad de Internet

Análisis de Navegadores, caché, cookies e historial

Chrome

- El Historial, cookies, caché y favoritos se encuentran especialmente en el directorio: C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default

Análisis de Navegadores, caché, cookies e historial

Firefox

- En Fireforx, la caché está almacenada en C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\Cache
- Las cookies en Firefox están en: C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\cookies.sqlite
- El historial en Firefox se encuentra en C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\places.sqlite

Análisis de Navegadores, caché, cookies e historial

Herramientas de análisis

- IECookiesView
- IECacheView
- IEHistoryView
- MozillaCookiesView
- MozillaCacheView
- MozillaHisotryView
- ChromeCookiesView
- ChromeCacheView
- ChromeHistoryView

Cálculo MD5

MD5: “*En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.*
La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida”

http://es.wikipedia.org/wiki/MD5

Cálculo MD5: Ejemplos

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida:

- *MD5("Esto sí es una prueba de MD5") = e99008846853ff3b725c27315e469fbc*

Un simple cambio en el mensaje nos da un cambio total en la codificación hash, en este caso cambiamos dos letras, el «sí» por un «no».

- *MD5("Esto no es una prueba de MD5") = dd21d99a468f3bb52a136ef5beef5034*

Otro ejemplo sería la codificación de un campo vacío:

- *MD5("") = d41d8cd98f00b204e9800998ecf8427e*

Cálculo MD5

En otras palabras, el algoritmo MD5 toma un mensaje de longitud arbitraria como entrada y produce como salida una huella digital de 128 bits, conocida en iglés como "message digest" (resumen del mensaje)

Cálculo MD5

¿Por qué calcular MD5?

- La copia o imagen de los datos no siempre generan una imagen idéntica
- Es necesario realizar el cálculo, tanto en el original como en la copia para ver si coinciden sus hashes.
- El hash MD5 es utilizado para varios procesos:
  - Revisar la integridad de los mensajes
  - Identificar datos duplicados
  - Cifrar datos
- Algunas herramientas utilizadas para calcular MD5 son HashCalc, MD5 Calculator, HashMyFiles, etc.

Análisis de Archivo

Papelera de Reciclaje

- La Papelera permite al usuario recuperar y restaurar archivos y directorios. Cuando un archivo es eliminado, un subdirectorio es creado por el usuario dentro del directorio de la Papelera con el UID, por ejemplo: C:\RECYCLER\S-1-5-21-1456685445-548310587-1100
- Cuando un archivo es motivo a la Papelera, es renombrado utilizando la convención: <letra de unidad original><#>.<extensión original>

Análisis de Archivo

Puntos de restauración del sistema (RP.log)

- Rp.log es el archivo de punto de restauración dentro del directorio de puntos de restauración (RPxx)
- Incluye el valor indicando el tipo del punto de restauración; un nombre descriptivo para evento de punto de restauración, y el objeto de tiempo de archivo de 64-bit indicando cuando fue creado el punto de restauración
- La descripción del punto de restauración puede ser útil para la información con respecto a la instalación o eliminación de una aplicación
- Los puntos de restauración son creados cuando las aplicaciones y controladores no firmados son instalados, cuando son realizadas auto actualizaciones y operaciones de restauración

Análisis de Archivo

Puntos de restauración del sistema (RP.log)

1. La clave System y los archivos de aplicaciones son monitoreados continuamente de manera que el sistema puede ser restaurado a un estado en particular
2. Los cambios de los archivos son registrados en los archivos change.log, que están localizados en los directorios de puntos de restauración
3. Los cambios son detectados por el controlador de puntos del sistema de archivos, el nombre original es registrado dentro de change.log con el número de secuencia, que tipo de cambio ocurrió, etc.
4. Los archivos monitoreados son preservados y copiados al directorio de punto de restauración y renombrados al formato Axxxxxxxx.ext, donde x representa una secuencia numérica y .ext es la extensión original del archivo
5. Primero el archivo change.log es adjunto con la secuencia numérica y un nuevo archivo change.log es creado cuando el sistema es reiniciado

Análisis de Archivo

Accesos Directos

- Los accesos directos tienen la extensión .lnk
- Herramientas como AccessData's Forensics Toolkit (FTK), Windows File Analyzer (WFA), y EnCase son utilizadas para analizar los contenidos de los archivos .lnk y revelar información incrustada en los mismos

Análisis de Archivo

Documentos PDF (Portable Document Format)

- Estos archivos pueden contener metadatos como el nombre del autor, fecha de creación y la aplicación utilizada para la creación del archivo
- Herramientas como los scripts pdfmeta.pl y pdfdmp.pl permiten extraer los meta datos
- También se puede ver cierta información haciendo clic en Archivo, Propiedades

Análisis de Archivo

Archivos de imagen

- Los archivos de imagen como JPEG contienen información de la fotografía, como por ejemplo ubicación donde la foto fue tomada
- Los metadatos disponibles en JPEG depende de la aplicación que la creó o modificó
- Recolectar información EXIF (Exhangable Image File Format), esto incluye el modelo y fabricante de la cámara
- Utilizar herramientas como Exifer, IrfanView, y Image::MetaData::JPEG para ver, revisar y modificar los metadatos de las imágenes JPEG
- ProDiscover muestra datos EXIF encontrados en las imágenes JPEG

Recolectando Información utilizando herramientas

- Utilizar herramientas sniffer como Wireshark para reconectar información de conectividad en la red. Esto ayudará a determinar si existe algún malware intentando comunicarse con un Sistema Remoto
- Alternativamente, abrir puertos para monitorear conexiones
- Registrar actividad en puertos TCP y UDP con la ayuda de la herramienta Port Reporter
- Utilizar la herramienta Process Monitor para ver archivos y claves de registro que han sido creados o modificados y la actividad en el tiempo

Proceso de Revisión de Malware

- Asegurarse que todas las herramientas de monitoreo estén actualizadas y correctamente configuradas
- Crear una ubicación de almacenamiento de los logs
- Preparar el malware para analizarlo
- Preparar una línea base de herramientas para instantáneas
- Habilitar herramientas de monitoreo en tiempo real
- Lanzar el malware
- Detener las herramientas de monitoreo en tiempo real y guardar los datos
- Lanzar una segunda instantánea y guardar los datos

Metadatos

Metadatos

- Describen como y cuando y por quien fue recolectado un conjunto de datos y cuál es su formato
- Algunos ejemplos son: Nombre de organización, nombre de autor, nombre de equipo, nombre de la red, texto escondido, versiones de documentos, información de plantillas, vistas personalizadas, etc.

Metadatos

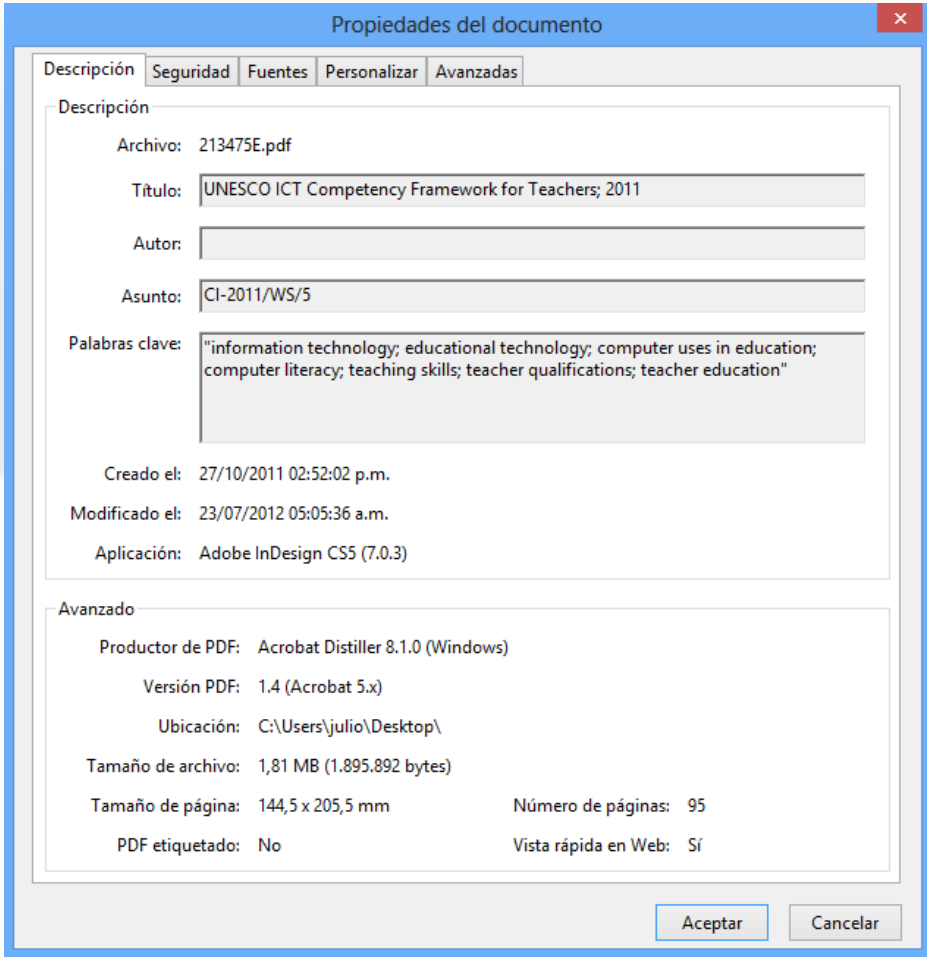
Tipos de Metadatos

- Metadatos descriptivos: Describe un recursos para propósitos como descubrimiento e identificación. Incluye información como título, abstract, autor, palabras clave
- Metadatos estructurales: Información que facilita la navegación, presentación y recursos electrónicos, como por ejemplo como las páginas son ordenadas en capítulos
- Metadatos administrativos: Provee información para ayudar a administrar un recurso (como por ej, cuando y cómo fue creado), incluyendo el tipo de archivo y otra información técnica y quién accedió a él.

Metadatos

Metadatos en los archivos PDF

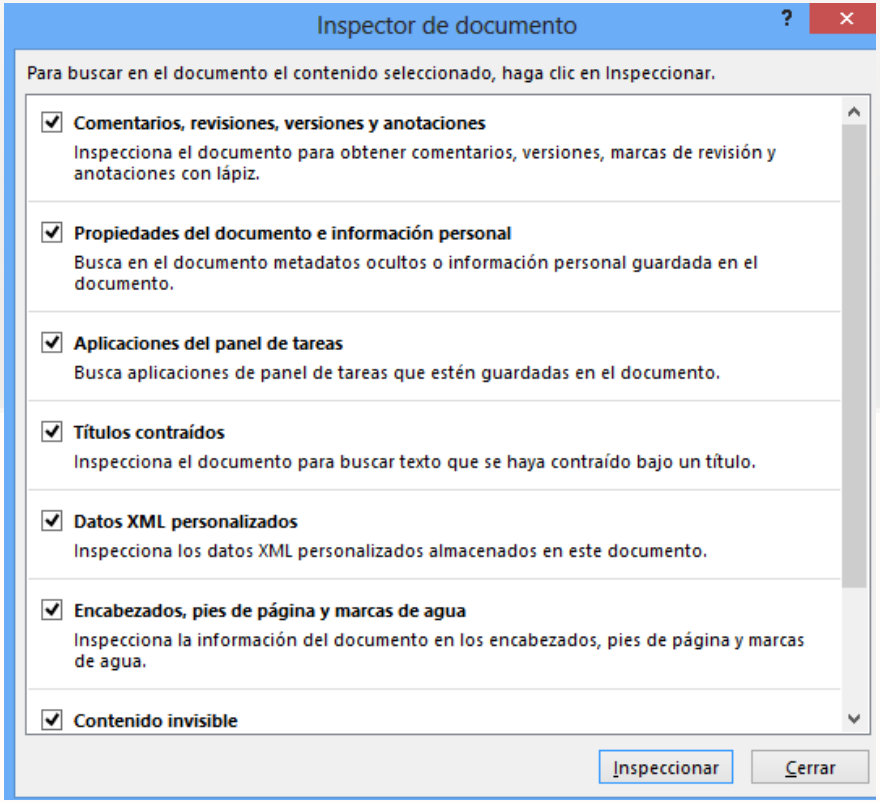
Para ver los metadatos en los PDF abrir el Adobe Reader y hacer clic en Archivo, Propiedades



Metadatos

Metadatos en archivos Word

Para visualizar los metadatos en Word, hacer clic en Información, Inspeccionar Documento



Metadata Analyzer

Es una herramienta analítica que permite revisar documentos Office

Registros (LOGS)

Entendiendo los Eventos

- Los logs de eventos son una variedad de eventos que ocurren día a día en los Sistemas Windows
- Algunos eventos son almacenados por defecto y algunas configuraciones de auditoria son mantenidas por la clave de registro PolAdEvt
- La clave de registro mantiene la configuración de log de eventos: HEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\<Log del Evento>

Registros (LOGS)
Tipos de Eventos

Tipo de Inicio	Título	Descripción
2	Interactive	Este inicio indica que el usuario ha iniciado sesión en la consola
3	Network	Un usuario o equipo ha iniciado en este equipo desde la red ya sea, utilizando net use, recurso compartido, o net view
4	Batch	Reservado para aplicaciones que ejecutan archivos por lotes
5	Servicie	Inicio de servicio
6	Proxy	No soportado
7	Desbloqueo	El usuario ha desbloqueado la estación de trabajo
8	NetworkClearText	Un usuario ha iniciado sesión en la red, y las credenciales han pasado sin cifrar

Registros (LOGS)
Tipos de Eventos

Tipo de Inicio	Título	Descripción
9	NewCredentials	Un proceso o subproceso clonado es concurrente pero nuevas credenciales especificadas para conexiones salientes
10	RemoteInteractive	Inicio de sesión por Terminal Services o Escritorio Remoto
11	CachedInteractive	Un usuario se ha logueado en el equipo con credenciales que están almacenadas localmente en el equipo
12	Cached Remote Interactive	Igual que RemoteInteractive, utilizado internamente para propósitos de auditoría
13	CachedUnlock	El intento de logueo es para desbloquear una estación de trabajo

Registros (LOGS)

Estructura de Registro de Eventos

Offset	Tamaño	Descripción
0	4 bytes	Longitud del registro de eventos o el tamaño del registro en bytes
4	4 bytes	Reservado, número mágico
8	4 bytes	Número de registro
12	2 bytes	Tiempo generado: medido en tiempo Unix, o el número de segundos transcurrido entre 00:00:00 1 Enero 1970 en UTC (Universal Coordinate Time)
16	2 bytes	Tiempo escrito: medido en tiempo Unix, o el número de segundos transcurrido entre 00:00:00 1 Enero 1970 en UTC (Universal Coordinate Time)
20	2 bytes	Identificador del Evento, que es especificado en la fuente del evento y únicamente identifica el evento; el ID de evento es utilizado a lo largo con el nombre de la fuente para ubicar la cadena de descripción apropiada dentro del archivo de mensaje

Registros (LOGS)

Estructura de Registro de Eventos

Offset	Tamaño	Descripción
24	2 bytes	Tipo de evento (0x01 = Error, 0x10 = Falla, 0x08 = Exito, 0x04 = Información, 0x02 = Advertencia)
26	2 bytes	Número de cadenas
28	2 bytes	Categoría de eventos
30	2 bytes	Banderas reservadas
32	4 bytes	Registro de cierre
36	4 bytes	Cadena offset; compensación de las cadenas de descripción dentro de este registro

Registros (LOGS)

Offset	Tamaño	Descripción
40	4 bytes	Longitud del SID del usuario, medido en bytes (si está en 0, no hay un SID provisto)
44	4 bytes	Compensar al SID del usuario Longitud de los datos, longidut de los datos binarios asociados con este evento
48	4 bytes	Compensar a los datos

Registros (LOGS)

El comando wevtutil permite recuperar información sobre los logs de eventos de Windows

Ejecutar **wevtutil /?** para ver las opciones

- **wevtutil el**
  Lista los registros de eventos disponibles en el Sistema
- **wevtutil gl log name**
  Lista la información de configuración sobre un log de evento específico
- La información mostrada por este comando está también disponible en HKEY_LOCAL_MACHINE\System\ControlSet00x\Services\EventLog\nombre de log

Registros (LOGS)

IIS Logs

- Utilizar los logs generados por el servidor Web para ver ataques hacia el mismo
- Los logs del Servidor Web IIS se encuentran en %WinDir%\System32
- Los archivos de log están en texto ASCII lo cual implica que son fácilmente accesibles

Registros (LOGS)

IIS Logs

- A la consola se la accede ya sea por iis.msc o inetmgr.
- Buscar los logs creados diariamente en el formato exaammdd.log donde
- aammdd: se refiere al año, mes y día
- Ex: se refiere al formato extendido
- Cada nombre de cambo en el log está relacionado con las siguientes letras:
  - c: acciones del cliente
  - s: acciones del servidor
  - cs: acciones de cliente a servidor
  - sc: acciones del servidor al cliente

Registros (LOGS)

IIS Logs

- Los logs de IIS están en formato W3C y se muestran a continuación:

Registros (LOGS)

Nombre del Campo	Descripción	Registrado por defecto
date	Fecha en que la actividad ocurrió	Si
time	Hora y actividad ocurrida, expresado en UTC (GMT)	Si
c-ip	Dirección IP del cliente que hizo la solicitud	Si
cs-username	Nombre de usuario autenticado del usuario que accedió al servidor. Los usuarios anónimos son anotados por un guión	Si
s-sitename	Nombre del servicio de internet y número de instancia que estuvo sirviendo en la solicitud	No
s-computername	Nombre del servidor que generó la entrada en el log	No

Registros (LOGS)

Nombre del Campo	Descripción	Registrado por defecto
s-ip	Dirección IP del servidor donde fue generado el log	Si
s-port	Número del puerto que fue utilizado por la conexión	Si
cs-method	Acción solicitada por el cliente, generalmente método GET	Si
cs-uri-stem	Objetivo de la acción del cliente (default.htm, index.htm, etc.)	Si
cs-uri-query	Cualquier consulta realizada por el cliente	Si
sc-status	Código del estado HTTP enviado por el servidor al cliente	Si

Registros (LOGS)

Nombre del Campo	Descripción	Registrado por defecto
sc-win32-status	Código de estado de Windows retornado por el servidor	No
sc-bytes	Número de bytes que el servidor envió al cliente	No
cs-bytes	Número de bytes que el servidor recibió del cliente	No
time-taken	Tiempo que la acción solicitada tardó, expresada en milisegundos	No
cs-version	Versión del protocolo (HTTP o FTP) que cliente usó	No
cs-host	Nombre del encabezado del host si es que hay	No

Registros (LOGS)

Nombre del Campo	Descripción	Registrado por defecto
cs(User-Agent)	Tipo de navegador utilizado por el cliente	Si
cs(Cookie)	Contenido de las cookies (enviadas o recibidas) si es que las hubo	No
cs(Referrer)	Último sitio visitado por el usuario.	No
sc-substatus	Código de error del subestado	Si

Registros (LOGS)

Analizando los Logs FTP

- FTP (File Transfer Protocol) sirve para enviar y recibir archivos
- Los logs FTP se encuentran almacenados en %WinDir%\System32\LogFiles\MSFTPSCV1\exaammdd.log
- Los logs FTP no registran los siguientes campos comparados con los Web IIS:
  - cs-uri-query
  - cs-host
  - cs(User-Agent)
  - cs(Cookie)
  - cds(referrer)
  - sc-substatus

Registros (LOGS)

Códigos de error

Código de error	Descripción
1xx	Respuestas preliminares positivas
120	Servicio listo en nnn minutos
125	Conexión de datos ya iniciada para trasnferencia
150	Estado del archivo listo para abrir conexión de datos
2xx	Respuestas positivas de terminación
202	Comando no implementado en este sitio
211	Estado del sistema o respuesta de ayuda del sistema
212	Estado del directorio
213	Estado del archivo

Registros (LOGS)

Código de error	Descripción
214	Mensaje de ayuda
214	Nombre del tipo del sistema, donde "nombre" es el nombre oficial del sistema
220	Servicio listo para el nuevo usuario
221	Conexión de servicio de control cerrada
225	Conexión de datos abierta sin transferencia en progreso
226	Cerrando conexión de datos. Solicitud de acción de archivo realizada (ejemplo, transferencia de archivo)
227	Ingresando en modo pasivo
230	Logueo de usuario en proceso
250	Acción de archivo solicitada y completa (OK)

Registros (LOGS)

Código de error	Descripción
257	Creada nombre de ruta}
3xx	Replicas intermediarias positivas
331	Nombre de usuario OK, se necesita contraseña
332	Necesita cuenta para logueo
350	Acción de archivo solicitada pendiente de más información
4xx	Respuestas transitorias de finalización negativas
421	Servicio no disponible - cerrando control de conexión
425	No se puede abrir conexión de datos
426	Conexión cerrada - transferencia abortada
450	Solicitud de archivo no tomada - Archivo no disponible
451	Solicitud de acción abortada - Error local en el proceso
452	Solicitud de acción no tomada - Espacio de almacenamiento insuficiente en el Sistema
5xx	Negativas permanentes de respuestas de finalización

Registros (LOGS)

Analizando los Logs de DHCP

- DHCP asigna dinámicamente direcciones IP a los equipos
- La actividad del servicio DHCP se guarda en el log c:\%SystemRoot%\System32\DHCP
- Los logs son almacenados diariamente en DhcpSrvLog-XXX.log donde XXX representa el día de la semana cuando el log fue creado

Registros (LOGS)

El formato del Log DHCP está representado a continuación

Campo	Descripción
ID	Código del evento
Date	Fecha que fue registrado por el servicio DHCP
Time	Hora que fue registrado por el servicio DHCP
Description	Descripción de este evento DHCP
IP Address	Dirección concedida al cliente
Host Name	Nombre host del cliente DHCP que obtuvo la concesión
MAC Address	La dirección MAC (Media Access Control Address) utilizada por el adaptador NIC del cliente a la cual le asignó la dirección IP

Registros (LOGS)

Analizando los Logs de DHCP

- DHCP asigna dinámicamente direcciones IP a los equipos
- La actividad del servicio DHCP se guarda en el log c:\%SystemRoot%\System32\DHCP
- Los logs son almacenados diariamente en DhcpSrvLog-XXX.log donde XXX representa el día de la semana cuando el log fue creado

Registros (LOGS)

- Los logs del Firewall están presentes en %SystemRoot%\pfirewall.log
- El nombre y ruta del log de configuraciones del Firewall están almacenadas en el archivo objects.data, el cual está almacenado en %SystemRoot%\System32\wbem\Repository\FS

Registros (LOGS)

- Utilizar Microsoft Log Parser
- Sirve para extraer archivos log, archivos XML y archivos CSV
- El comando utilizado es: LogParser.exe -o:DATAGRID "select * from system"

Log Parser

Edit View Format

E...	Re...	TimeG...	Time...	E...	E...	Eve...	Ev...	Event...	SourceName	Strings	Com...	S...	Message	Data
Sy...	1	2013-...	2013-...	6...	4	Infor...	0	None	EventLog	WINDOWS-UJ49S6B|...	wind...	N...	El nombre NetBIOS y el nombre de host DNS de este equipo han cambiado de WINDOWS-UJ49S6B a WI...	NULL
Sy...	2	2013-...	2013-...	6...	4	Infor...	0	None	EventLog	6.02.|9200|Multiproces...	wind...	N...	Microsoft (R) Windows (R) 6.02. 9200 Multiprocessor Free.	NULL
Sy...	3	2013-...	2013-...	6...	4	Infor...	0	None	EventLog	NULL	wind...	N...	Se inició el servicio de Registro de eventos.	DD0704000200090017003...
Sy...	4	2013-...	2013-...	12	4	Infor...	0	None	Microsoft-Wi...	6|2|9200|16384|0|0|201...	wind...	S...	The description for Event ID 12 in Source "Microsoft-Windows-Kernel-General" cannot be found. The local ...	NULL
Sy...	5	2013-...	2013-...	20	4	Infor...	0	None	Microsoft-Wi...	false|false	wind...	S...	The description for Event ID 20 in Source "Microsoft-Windows-Kernel-Boot" cannot be found. The local co...	NULL
Sy...	6	2013-...	2013-...	27	4	Infor...	0	None	Microsoft-Wi...	0	wind...	S...	The description for Event ID 27 in Source "Microsoft-Windows-Kernel-Boot" cannot be found. The local co...	NULL
Sy...	7	2013-...	2013-...	18	4	Infor...	0	None	Microsoft-Wi...	2	wind...	S...	The description for Event ID 18 in Source "Microsoft-Windows-Kernel-Boot" cannot be found. The local co...	NULL
Sy...	8	2013-...	2013-...	32	4	Infor...	0	None	Microsoft-Wi...	0	wind...	S...	The description for Event ID 32 in Source "Microsoft-Windows-Kernel-Boot" cannot be found. The local co...	NULL
Sy...	9	2013-...	2013-...	15	4	Infor...	0	None	Microsoft-Wi...	NULL	wind...	N...	Se restringió el sistema a una marca periódica por exclusión en el administrador de errores.	NULL
Sy...	10	2013-...	2013-...	6	4	Infor...	0	None	Microsoft-Wi...	0x0|6|2|8|FileInfo|2012-...	wind...	S...	Filtro de sistema de archivos 'FileInfo' (6.2, 2012-07-25T22:28:02.000000000Z) correctamente cargado y reg...	NULL

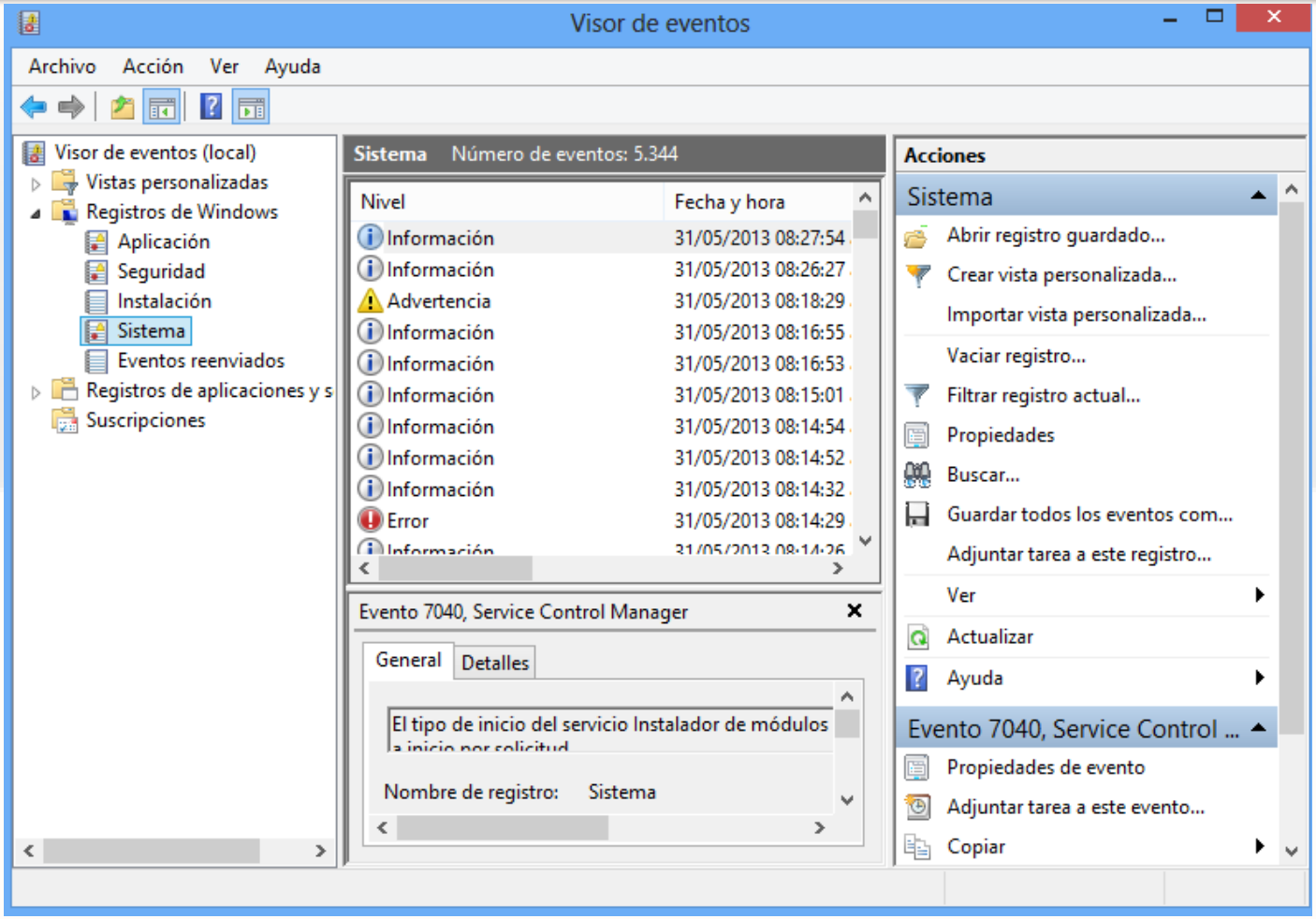
Auditoría

- Cuando un atacante compromete un Sistema, suele deshabilitar la Auditoría
- Las modificaciones a la directiva de auditoría son guardadas como ID de evento 4902 (Windows 7) y 612 (Windows XP)
- Para ver las directivas de auditoría se debe ejecutar secpol.msc, Directivas Locales, Directivas de Auditoría

Visor de eventos

- El visor de eventos registra acontecimientos suscitados en el Sistema como: cambios hechos en el S.O., configuración de hardware, instalación de controladores, inicio y detención de servicios, etc.
- Para abrirlo se debe ejecutar el comando: %windir%\system32\eventvwr.msc /s o bien abrirlo desde Panel de Control, Sistema, Herramientas administrativas, Visor de Eventos
- Los eventos se almacenan en %windir%\System32\config

Visor de Eventos



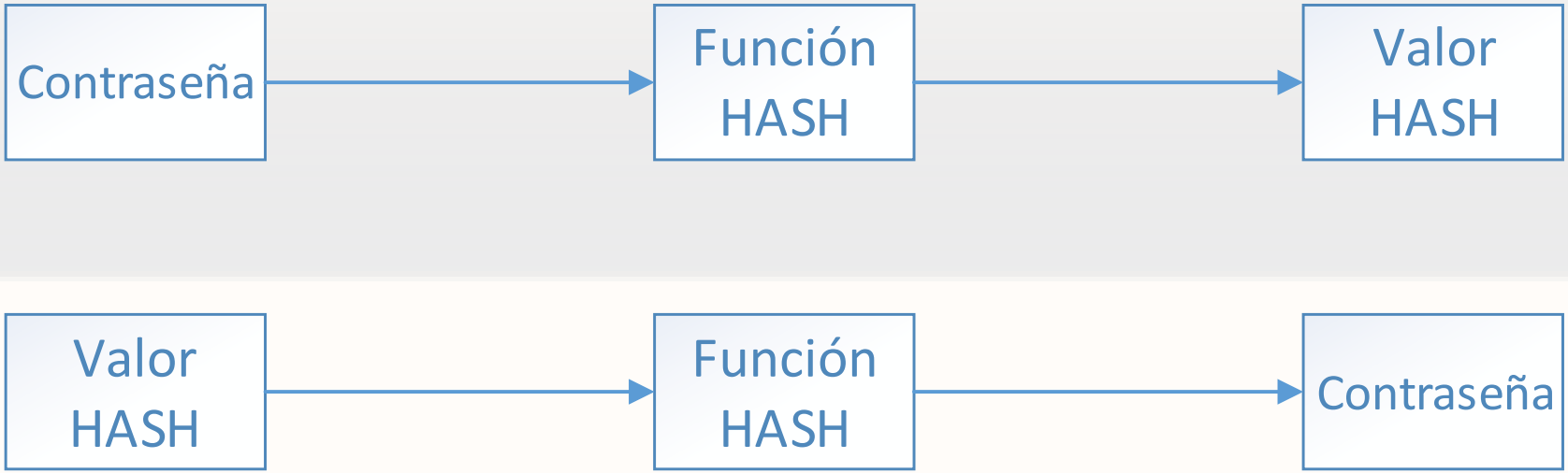
Contraseñas en Windows

- Los Sistemas Windows almacenan las cuentas de usuario y sus contraseñas en el archivo SAM (Security Account Manager) o bien en Active Directory
- La información local es almacenada en el archivo SAM que se encuentra en %windir%\System32\Config
- Una copia adicional del archivo SAM se encuentra en %windir%\Repair

Contraseñas en Windows

- La base de datos de los controladores de dominio se encuentran el el archivo ntds.dit que está ubicado en %windir%\ntds del equipo controlador de dominio
- Las contraseñas pasan a través de un algoritmo y son convertidas en valores numéricos (Hash). Windows utiliza dos funciones hash:
  - Hash NT LanMan (NTLM)
  - Hash LanMan (LM)

Contraseñas en Windows



Contraseñas en Windows

- Una manera de crackear las contraseñas es adivinando contraseñas. Se crean contraseñas y se comparan los hashes, si los hashes coinciden entonces se adivinó la contraseña.
- Existen otros métodos de crackear las contraseñas, como por ejemplo utilizando sniffers y herramientas de crack de contraseñas

Herramientas Forenses

- OS Forensics: Extrae datos forenses en los equipos, identifica archivos y actividad sospechosa
- Helix3 Pro: Es un Live CD que se enfoca en respuesta a incidentes, para Sistemas MAC OS, Windows y Linux
- X-Ways Forensics: Observa y vuelca la memoria RAM (física y virtual), permite clonar discos, realizar imágenes, incluso bajo DOS, soporta FAT, NTFS, EXT, CDFS y UDF
- Windows Forensics Toolchest (WFT): Está diseñada para proveer una respuesta Forense en vivo respetable y automática
- Sigverif: Sirve para verificar si los controladores de dispositivo están digitalmente firmados

Herramientas Forenses

- Computer Online Forensics Evidence Extractor (COFEE): Desarrollada por Microsoft y ayuda a los investigadores forenses a extraer evidencia desde equipos Windows, ayuda a identificar fraude, robos, pornografía infantil entre otras cosas
- System Explorer: Software para exploración y administración de System Internals. Provee una detallada información sobre tareas, procesos, módulos, inicios, addons de IE, desinstaladores, Windows, servicios, controladores de dispositivo, conexiones y archivos abiertos
- System Scanner: Tiene la habilidad de buscar información más específica sobre los procesos, subprocesos, DLLs, etc.

Herramientas Forenses

- SecretExplorer: Herramienta de inspección y mantenimiento que permite explorar el almacenamiento protegido de Windows
- RegScanner: Esta pequeña herramienta permite escanear el Registro, encontrar los valores deseados que coincidan con un criterio de búsqueda
- Alien Registry Viewer: Similar a RegEdit pero a diferencia de éste, trabaja con archivos independientes del registro
- MultiMon: Herramienta de monitoreo multifuncional que muestra salidas detalladas de varias actividades del registro en tiempo real
- CurrProcess: Muestra la lista de todos los procesos que se están ejecutando en el sistema y crea un reporte HTML

Herramientas Forenses

- Process Explorer: muestra información sobre los DLLs que los procesos están utilizando
- Security Task Manager: Muestra información detallada de todos los procesos en ejecución, su ruta, descripción, valor de seguridad, tiempo de inicio, ícono
- PrcView: Muestra información de los procesos en ejecución
- ProcHeapViewer: Enumera rápidamente el cúmulo de procesos
- Memory Viewer: Muestra ver la configuración de la memoria del Sistema
- PMDump: Vuelca el contenido de la memoria del procesador a un archivo sin detener los procesos

Herramientas Forenses

- Word Extractor: Herramienta que interpreta palabras humanas desde el lenguaje máquina, permite encontrar trampas en los juegos, texto escondido o contraseñas en archivos (exe, bin, dll, etc.)
- Belkasoft Evidence Center: Ayuda a los investigadores a buscar, analizar y almacenar evidencia digital encontrada en historial de Messentger, IE, y Outlook
- Metadata Assistant: Analiza archivos Word, Excel y Powerpoint para determinar la cantidad de metadatos existentes
- HstEx: Solución forense de recuperación de datos que permite recuperar datos eliminados de historial de navegadores, archivos caché y demás

Herramientas Forenses

- XpoLog Center Suite: Solución que investiga y accede a datos log de aplicaciones críticas
- LogViewer Pro: Permite visualizar archivos log
- Event Log Explorer: Software que permite ver, monitorear y analizar eventos registrados en los logs de Seguridad, Sistema y Aplicación de Windows
- LogMeister: Herramienta de monitoreo de logs de aplicaciones y sistema que permite capturar datos de fuentes dispersas, incluyendo archivos de texto, logs locales y remotos y RSS

Herramientas Forenses

- ProDiscover Forensics: Herramienta de seguridad que permite encontrar los datos en un equipo en riesgo mientras protege la evidencia y crea reportes de evidencia de calidad para utilizarlos en procedimientos legales
- PyFlag: Es una herramienta FLAG (Forensic and Log Analysis GUI) forense capaz de analizar logs y grandes cantidades de unidades para investigación forense
- LiveWire Ingestigator: Examina Sistemas rápida y discretamente, capturando datos relevantes
- ThumbsDisplay: Es una herramienta que examina los archivos Thumbs.db y presenta un reporte
- DriveLook: Herramienta que permite investigar unidades

Muchas gracias