

AUTOVOL

V.1.0 (15/11/18), Diseñado por Juan Pablo Puentes Páez



Para la automatización de los procesos realizados por Volatility, se hizo uso de lenguaje batch, desarrollando una aplicación desde la Shell de Windows.

La misma permite la ejecución de series de comandos, de manera automática, evitando la necesidad de reescribir textos o tener conocimientos de los comandos y su funcionamiento interno.

La aplicación cuenta con las siguientes funciones:

```
-----
1   Especificar nombre de archivo de volcado
2   Obtener Información del archivo de volcado
3   Especificar un perfil de SO
4   Listar procesos activos en el momento del volcado
5   Listar los identificadores de seguridad (SIDs)
6   Listar comandos CMD ejecutados previos al volcado
7   Listar procesos con privilegios
8   Listar Logs
9   Listar historial de navegación
10  Cambiar ruta de Volatility
11  Salir
-----
```

La primera permite establecer el nombre del archivo de volcado, junto con su extensión y ruta relativa o absoluta.

```
-----
Especifique la ubicación del archivo de volcado
1. Ruta del AutoVol.bat
2. Otra ubicación

> Seleccione una opción [1-2]: 1

> Escriba el nombre del archivo de volcado con su extensión (Ex: volcado_ram.mem):
memdump2.mem
-----
```

La segunda opción permite analizar el archivo de volcado, y así poder identificar el S.O al que fue realizado el volcado (en caso de desconocerse), y poder elegir el perfil adecuado para el análisis.

```
Analizando memdump2.mem ...
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXP
SP2x86)
           AS Layer1 : IA32PagedMemoryPae (Kernel AS)
           AS Layer2 : FileAddressSpace (F:\AutoVol 1.0\memdump2.mem)
           PAE type : PAE
                   DTB : 0xa8f000L
                   KDBG : 0x8054d2e0L
           Number of Processors : 2
           Image Type (Service Pack) : 3
                   KPCR for CPU 0 : 0xffdff000L
                   KPCR for CPU 1 : 0xf9c2c000L
                   KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-11-15 14:52:37 UTC+0000
           Image local date and time : 2018-11-15 15:52:37 +0100
```

El cual puede ser seleccionado en la opción 3 del menú

```
Elija el perfil que desee manejar
-----
1 VistaSP0x64 - A Profile for Windows Vista SP0 x64
2 VistaSP0x86 - A Profile for Windows Vista SP0 x86
3 VistaSP1x64 - A Profile for Windows Vista SP1 x64
4 VistaSP1x86 - A Profile for Windows Vista SP1 x86
5 VistaSP2x64 - A Profile for Windows Vista SP2 x64
6 VistaSP2x86 - A Profile for Windows Vista SP2 x86
7 Win10x64 - A Profile for Windows 10 x64
8 Win10x86 - A Profile for Windows 10 x86
9 Win2003SP0x86 - A Profile for Windows 2003 SP0 x86
10 Win2003SP1x64 - A Profile for Windows 2003 SP1 x64
11 Win2003SP1x86 - A Profile for Windows 2003 SP1 x86
12 Win2003SP2x64 - A Profile for Windows 2003 SP2 x64
13 Win2003SP2x86 - A Profile for Windows 2003 SP2 x86
14 Win2008R2SP0x64 - A Profile for Windows 2008 R2 SP0 x64
15 Win2008R2SP1x64 - A Profile for Windows 2008 R2 SP1 x64
16 Win2008SP1x64 - A Profile for Windows 2008 SP1 x64
17 Win2008SP1x86 - A Profile for Windows 2008 SP1 x86
18 Win2008SP2x64 - A Profile for Windows 2008 SP2 x64
19 Win2008SP2x86 - A Profile for Windows 2008 SP2 x86
20 Win2012R2x64 - A Profile for Windows Server 2012 R2 x64
21 Win2012x64 - A Profile for Windows Server 2012 x64
22 Win7SP0x64 - A Profile for Windows 7 SP0 x64
23 Win7SP0x86 - A Profile for Windows 7 SP0 x86
24 Win7SP1x64 - A Profile for Windows 7 SP1 x64
25 Win7SP1x86 - A Profile for Windows 7 SP1 x86
26 Win81U1x64 - A Profile for Windows 8.1 Update 1 x64
27 Win81U1x86 - A Profile for Windows 8.1 Update 1 x86
28 Win8SP0x64 - A Profile for Windows 8 x64
29 Win8SP0x86 - A Profile for Windows 8 x86
30 Win8SP1x64 - A Profile for Windows 8.1 x64
31 Win8SP1x86 - A Profile for Windows 8.1 x86
32 WinXPSP1x64 - A Profile for Windows XP SP1 x64
33 WinXPSP2x64 - A Profile for Windows XP SP2 x64
33 WinXPSP2x86 - A Profile for Windows XP SP2 x86
34 WinXPSP3x86 - A Profile for Windows XP SP3 x86
-----
> Seleccione una opcion [1-34]: 34
```

De forma que, una vez establecida la ruta del archivo de volcado y el perfil a utilizar, se puede acceder a las funciones restantes

```
Archivo a analizar: memdump2.mem
Perfil de S.O.: "WinXPSP3x86"
-----
```

Como lo es la lista de los procesos activos en el momento del volcado

0x8166caa8 smss.exe	492	4	3	19	-----	0	2018
-11-15 14:44:48 UTC+0000							
0x81461020 csrss.exe	556	492	11	331	0	0	2018
-11-15 14:44:49 UTC+0000							
0x814308c8 winlogon.exe	580	492	19	507	0	0	2018
-11-15 14:44:49 UTC+0000							
0x81301020 services.exe	624	580	15	245	0	0	2018
-11-15 14:44:50 UTC+0000							
0x815e8378 lsass.exe	636	580	22	349	0	0	2018
-11-15 14:44:51 UTC+0000							
0x814c24c0 svchost.exe	808	624	16	194	0	0	2018
-11-15 14:44:51 UTC+0000							
0x816eada0 svchost.exe	876	624	11	263	0	0	2018
-11-15 14:44:52 UTC+0000							
0x81457938 svchost.exe	972	624	71	1355	0	0	2018
-11-15 14:44:52 UTC+0000							
0x814bf7c0 svchost.exe	1060	624	6	85	0	0	2018
-11-15 14:44:52 UTC+0000							
0x813ce020 svchost.exe	1168	624	14	188	0	0	2018
-11-15 14:44:52 UTC+0000							
0x816adb28 spoolsv.exe	1264	624	10	109	0	0	2018
-11-15 14:44:53 UTC+0000							
0x815d7300 explorer.exe	1608	1572	13	360	0	0	2018
-11-15 14:44:55 UTC+0000							
0x81218898 ctfdmon.exe	1712	1608	1	74	0	0	2018
-11-15 14:44:57 UTC+0000							
0x812e87b0 alg.exe	1476	624	6	108	0	0	2018
-11-15 14:45:21 UTC+0000							
0x812bb5f0 wscntfy.exe	1492	972	1	37	0	0	2018
-11-15 14:45:21 UTC+0000							
0x813d9790 wuauclt.exe	1576	972	4	123	0	0	2018
-11-15 14:46:20 UTC+0000							
0x81688020 wpabaln.exe	1604	580	1	67	0	0	2018
-11-15 14:46:55 UTC+0000							
0x815ae8d8 msmsgs.exe	1448	808	3	165	0	0	2018
-11-15 14:49:28 UTC+0000							
0x8163abb0 FTK Imager.exe	684	1608	8	228	0	0	2018
-11-15 14:52:17 UTC+0000							

Presione una tecla para continuar . . .

Los identificadores de seguridad (SIDs)

```

wscntfy.exe (1492): S-1-5-11 (Authenticated Users)
wscntfy.exe (1492): S-1-5-5-0-53573 (Logon Session)
wscntfy.exe (1492): S-1-2-0 (Local (Users with the ability to log in locally))
wuaucflt.exe (1576): S-1-5-21-448539723-1682526488-725345543-1004 (Daniel)
wuaucflt.exe (1576): S-1-5-21-448539723-1682526488-725345543-513 (Domain Users)
wuaucflt.exe (1576): S-1-1-0 (Everyone)
wuaucflt.exe (1576): S-1-5-32-544 (Administrators)
wuaucflt.exe (1576): S-1-5-32-545 (Users)
wuaucflt.exe (1576): S-1-5-4 (Interactive)
wuaucflt.exe (1576): S-1-5-11 (Authenticated Users)
wuaucflt.exe (1576): S-1-5-5-0-53573 (Logon Session)
wuaucflt.exe (1576): S-1-2-0 (Local (Users with the ability to log in locally))
wpabaln.exe (1604): S-1-5-21-448539723-1682526488-725345543-1004 (Daniel)
wpabaln.exe (1604): S-1-5-21-448539723-1682526488-725345543-513 (Domain Users)
wpabaln.exe (1604): S-1-1-0 (Everyone)
wpabaln.exe (1604): S-1-5-32-544 (Administrators)
wpabaln.exe (1604): S-1-5-32-545 (Users)
wpabaln.exe (1604): S-1-5-4 (Interactive)
wpabaln.exe (1604): S-1-5-11 (Authenticated Users)
wpabaln.exe (1604): S-1-5-5-0-53573 (Logon Session)
wpabaln.exe (1604): S-1-2-0 (Local (Users with the ability to log in locally))
msmsgs.exe (1448): S-1-5-21-448539723-1682526488-725345543-1004 (Daniel)
msmsgs.exe (1448): S-1-5-21-448539723-1682526488-725345543-513 (Domain Users)
msmsgs.exe (1448): S-1-1-0 (Everyone)
msmsgs.exe (1448): S-1-5-32-544 (Administrators)
msmsgs.exe (1448): S-1-5-32-545 (Users)
msmsgs.exe (1448): S-1-5-4 (Interactive)
msmsgs.exe (1448): S-1-5-11 (Authenticated Users)
msmsgs.exe (1448): S-1-5-5-0-53573 (Logon Session)
msmsgs.exe (1448): S-1-2-0 (Local (Users with the ability to log in locally))
FTK Imager.exe (684): S-1-5-21-448539723-1682526488-725345543-1004 (Daniel)
FTK Imager.exe (684): S-1-5-21-448539723-1682526488-725345543-513 (Domain Users)

FTK Imager.exe (684): S-1-1-0 (Everyone)
FTK Imager.exe (684): S-1-5-32-544 (Administrators)
FTK Imager.exe (684): S-1-5-32-545 (Users)
FTK Imager.exe (684): S-1-5-4 (Interactive)
FTK Imager.exe (684): S-1-5-11 (Authenticated Users)
FTK Imager.exe (684): S-1-5-5-0-53573 (Logon Session)
FTK Imager.exe (684): S-1-2-0 (Local (Users with the ability to log in locally))

Presione una tecla para continuar . . .

```

Los comandos utilizados en consola al momento del volcado

```

Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: csrss.exe Pid: 556
Console: 0x5427c8 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: ?Tmbolo del sistema
Title: ??mbolo del sistema

```

Listado de los procesos y sus privilegios

```

684 FTK Imager.exe      23 SeChangeNotifyPrivilege      Present,Enabled
,Default Receive notifications of changes to files or directories
684 FTK Imager.exe      8 SeSecurityPrivilege           Present
    Manage auditing and security log
684 FTK Imager.exe     17 SeBackupPrivilege            Present
    Backup files and directories
684 FTK Imager.exe     18 SeRestorePrivilege           Present
    Restore files and directories
684 FTK Imager.exe     12 SeSystemtimePrivilege        Present
    Change the system time
684 FTK Imager.exe     19 SeShutdownPrivilege          Present
    Shut down the system
684 FTK Imager.exe     24 SeRemoteShutdownPrivilege    Present
    Force shutdown from a remote system
684 FTK Imager.exe      9 SeTakeOwnershipPrivilege      Present
    Take ownership of files/objects
684 FTK Imager.exe     20 SeDebugPrivilege             Present
    Debug programs
684 FTK Imager.exe     22 SeSystemEnvironmentPrivilege  Present
    Edit firmware environment values
684 FTK Imager.exe     11 SeSystemProfilePrivilege      Present
    Profile system performance
684 FTK Imager.exe     13 SeProfileSingleProcessPrivilege Present
    Profile a single process
684 FTK Imager.exe     14 SeIncreaseBasePriorityPrivilege Present
    Increase scheduling priority
684 FTK Imager.exe     10 SeLoadDriverPrivilege        Present,Enabled
    Load and unload device drivers
684 FTK Imager.exe     15 SeCreatePagefilePrivilege     Present
    Create a pagefile
684 FTK Imager.exe      5 SeIncreaseQuotaPrivilege       Present
    Increase quotas
684 FTK Imager.exe     25 SeUndockPrivilege            Present,Enabled
    Remove computer from docking station
684 FTK Imager.exe     28 SeManageVolumePrivilege       Present
    Manage the files on a volume
684 FTK Imager.exe     29 SeImpersonatePrivilege        Present,Enabled
,Default Impersonate a client after authentication
684 FTK Imager.exe     30 SeCreateGlobalPrivilege       Present,Enabled
,Default Create global objects

Presione una tecla para continuar . . .

```





La lista de logs, generados en la ruta especificada

```

Listando Logs en memdump2.mem con perfil "WinXPSP3x86" ...
Volatility Foundation Volatility Framework 2.6
Parsed data sent to secevent.txt
Parsed data sent to appevent.txt
Parsed data sent to sysevent.txt

Los logs generados se almacenaron en la ruta /output
Presione una tecla para continuar . . .

```

(F:) > AutoVol 1.0 > output		
Nombre	Fecha de modifica...	Ti
 appevent.txt	15/11/2018 9:10 p....	Ar
 secevent.txt	15/11/2018 9:10 p....	Ar
 sysevent.txt	15/11/2018 9:10 p....	Ar
 historial.txt	15/11/2018 8:48 p....	Ar

El historial de navegación

```
Listando historial en memdump2.mem con perfil "WinXPSP3x86" ...
Volatility Foundation Volatility Framework 2.6
*****
Process: 1608 explorer.exe
Cache type "DEST" at 0x111635
Last modified: 2018-11-15 15:46:44 UTC+0000
Last accessed: 2018-11-15 14:46:46 UTC+0000
URL: Daniel@http://www.bing.com/search?q=google.com&q=n&form=QBRE&sp=-1&pq=&sc=
0-0&sk=&cvid=EDBFE27C4CD5443697C473F390D0F92F
Title: google.com - Bing
*****
Process: 1608 explorer.exe
Cache type "DEST" at 0x14546d
Last modified: 2018-11-15 15:47:14 UTC+0000
Last accessed: 2018-11-15 14:47:16 UTC+0000
URL: Daniel@http://www.bing.com/search?srch=106&FORM=AS6&q=descargar+buscaminas
Title: descargar buscaminas - Bing
*****
Process: 1608 explorer.exe
Cache type "DEST" at 0x15b695
Last modified: 2018-11-15 15:50:37 UTC+0000
Last accessed: 2018-11-15 14:50:38 UTC+0000
URL: Daniel@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
```

Y demás funciones automatizadas gracias a la herramienta.

Los resultados de opciones como listar procesos, listar SIDs, listar historial, y demás opciones con salida extensa, generan un archivo .txt que es almacenado en la ruta /output, dentro del directorio del programa.

Dichos archivos son sobrescritos cada vez que se ejecutan los comandos, por lo que pueden ser movidos a una ruta distinta en caso de querer conservar copia de los mismos.

Documento y Software disponibles en GitHub <https://github.com/JuanPabloP/AutoVol>