

# Analyse mémoire

Mars 2023

# Agenda

- Motivation
- Collecte mémoire (sources et outils)
- Principes d'analyse sous Windows et Linux
- Volatility pour l'analyse d'empreintes windows
  - Processes
  - Noyau
  - Réseau

# Agenda

- 9h30 – 11h : cours
- 11h : test Volatility 3
- 13h30 – 15h10 : analyse de dumps
- 15h10 : QCM

# Pourquoi?

- Obtenir de l'information sur le système en cours d'exécution, sans passer par l'API système:
  - Processus et fils d'exécution (Thread)
  - Connexions réseau en cours
  - Secrets: mot de passe, clés cryptographiques ...
  - Fichiers ouverts
  - Registre Windows, journaux systèmes
- Détection des rootkits
  - Pour s'exécuter, un malware doit être présent en mémoire, non protégé par un packer ou de l'offuscation
  - Certains malware ne se trouvent qu'en mémoire

# Sources de mémoire volatile

- Mémoire vive
- Fichier d'hibernation  
(%systemdrive%/hiberfil.sys)
- Fichier de pagination  
(%systemdrive%/pagefile.sys)
- Crash Dump
- Fichier mémoire des machines virtuelles
  - VMware (.vmem), Hyper-V (.bin), Parallels (.mem), VirtualBox (.sav)

# Préserver au mieux l'état du système

Mémoire volatile,

donc à collecter en premier. Garder le câble réseau branché si possible (connections réseau).

Eviter de polluer le système,

donc ne pas installer l'outil de collecte

Ne pas modifier la mémoire persistante,

donc ne pas stocker l'image mémoire sur le disque dur

⇒ Outils à exécuter depuis un périphérique amovible, et y stocker l'image,

ou transférer l'image par le réseau,

à condition de chiffrer le contenu au vol

# Acquisition de la mémoire

Gratuits pour un usage non commercial:

- FTK Imager (AccessData)
- winpmem

Gratuit

- Dumplt (Magnet)

# Dumplt (windows)

<https://www.magnetforensics.com/resources/magnet-dumpit-for-windows>

By Matthieu Suiche

Très simple d'utilisation

- Mettre l'outil sur une clé USB d'une taille > à la taille de la mémoire à collecter
- Exécuter l'outil avec les droits administrateur

Pour DumpIt 3: `dumpit /T RAW /N /Q`



# FTK Imager

<https://www.exterro.com/ftk-imager>

## Fonctionnalités:

- Interface graphique
- Permet aussi la collecte d'image disque
- Conversion de formats
- « montage » de partition
- Collecte de fichiers protégés (Registre)

# Linux

AVML (Microsoft) :

<https://github.com/microsoft/avml>

Dumpit

<https://github.com/MagnetForensics/dumpit-linux>

# Arsenal Recon Image Mounter

Pour le montage d'image bitlocker

<https://arsenalrecon.com/downloads>

# Find strings in memory

## 1. Extract strings

- Strings by [sysinternals](#) (ascii and unicode)
- Strings ([GNU binutils](#))

## 2. Use grep for keywords

## 3. BulkExtractor

[https://github.com/simsong/bulk\\_extractor](https://github.com/simsong/bulk_extractor)

# Retrouver les objets du système d'exploitation

1. Trouver la structure Kernel Debugger Data Block (KDBG), pointée by Kernel Processor Control Region ([KPCR](#))
2. Trouvez la liste des processus en cours d'exécution (EPROCESS)
3. Trouvez les Process Environment Block (PEB) qui décrivent les processus: ligne de commande, régions mémoire, ...

# The Volatility framework

- Ecrit en Python, open source, portable
- Pour analyser Windows, Linux, Mac OS
- API et système de Plug-ins  
<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>
- Historique:
  - Ancêtres: [DFRWS 2005](#), [FATKit](#), [Volatools](#)
  - [Volatility 1.1.1](#) (Win XP SP2, 08/2007)
  - Volatility 2.0 (Win7, Win2008, 32bits, 08/2011)
  - Volatility 2.2 (Linux support, 10/2012)
  - Volatility 2.4 (Win8/Win2012/Mavericks Support, 08/2014)
  - Volatility 2.6 (Win10 improvements, Server 2016)
  - Volatility 3.0 (2019)

# using Volatility: pslist

```
K:\afti_forensic>volatility-2.4.standalone.exe -f "i:\winxp_sp3\Windows XP Professional-3940642f.vmem"  
--profile=WinXPSP3x86 pslist
```

Volatility Foundation Volatility Framework 2.4

Offset (V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x823c8830	System	4	0	46	194	-----	0		
0x820679e8	smss.exe	552	4	3	17	-----	0	2014-12-20 20:53:52 UTC+0000	
0x81f39930	csrss.exe	616	552	8	232	0	0	2014-12-20 20:53:54 UTC+0000	
0x82206020	winlogon.exe	640	552	22	281	0	0	2014-12-20 20:53:54 UTC+0000	
0x81f18020	services.exe	684	640	18	246	0	0	2014-12-20 20:53:54 UTC+0000	
0x81e4f020	lsass.exe	696	640	22	296	0	0	2014-12-20 20:53:54 UTC+0000	
0x82135880	vmacthlp.exe	852	684	2	26	0	0	2014-12-20 20:53:54 UTC+0000	
0x821f5da0	svchost.exe	864	684	7	123	0	0	2014-12-20 20:53:54 UTC+0000	
0x81f016e8	svchost.exe	936	684	10	185	0	0	2014-12-20 20:53:54 UTC+0000	
0x822ca390	svchost.exe	1028	684	29	406	0	0	2014-12-20 20:53:55 UTC+0000	
0x81f1a020	svchost.exe	1076	684	4	56	0	0	2014-12-20 20:53:55 UTC+0000	
0x81f5b998	svchost.exe	1136	684	3	76	0	0	2014-12-20 20:53:56 UTC+0000	
0x8214f020	spoolsv.exe	1468	684	6	51	0	0	2014-12-20 20:53:57 UTC+0000	
0x82282020	userinit.exe	1568	640	2	45	0	0	2014-12-20 20:53:57 UTC+0000	
0x81f06a80	explorer.exe	1588	1568	19	333	0	0	2014-12-20 20:53:57 UTC+0000	
0x82011980	vmtoolsd.exe	1692	1588	1	52	0	0	2014-12-20 20:53:58 UTC+0000	
0x82011da0	ctfmon.exe	1716	1588	1	75	0	0	2014-12-20 20:53:58 UTC+0000	

# using Volatility: Linux profiles

## Problème:

Il existe des dizaines de versions du kernel Linux et des centaines de configurations possibles

## Comment créer un profil Linux depuis une clé USB:

- Linux memory grabber (Hal Pomeranz)  
<https://github.com/halpomeranz/lmg>

## Bonus, le script *lmg* effectue aussi la capture avec LiME:

- Linux Memory Extractor (Joe Sylve)  
<https://github.com/504ensicsLabs/LiME>

Mettre System.map et module.dwarf dans une archive .zip (ubuntu-14041.zip) dans volatility/plugins/overlays/linux/



# using Volatility: linux\_pslist

```
forensics@ubuntu:~/volatility$ python vol.py -f ubuntu-2014-12-21_11.54.35-memory.lime  
--profile=Linuxubuntu-14041x64 linux_pslist
```

Volatility Foundation Volatility Framework 2.4

Offset	Name	Pid	Uid	Gid	DTB	StartTime
0xffff88003dbd0000	init	1	0	0	0x3d2d0000	0
0xffff88003dbd17f0	kthreadd	2	0	0	-0x1	0
0xffff88003dbd2fe0	ksoftirqd/0	3	0	0	-0x1	0
0xffff88003dbd47d0	kworker/0:0	4	0	0	-0x1	0
0xffff88003dbd5fc0	kworker/0:0H	5	0	0	-0x1	0
0xffff88003dbf97f0	rcu_sched	7	0	0	-0x1	0
0xffff88003dbfafe0	rcuos/0	8	0	0	-0x1	0
0xffff88003dbfc7d0	rcuos/1	9	0	0	-0x1	0
0xffff88003dbfdfc0	rcuos/2	10	0	0	-0x1	0
...						
0xffff88003669afe0	bash	18388	1000	1000	0x3bee0000	0
0xffff880039a45fc0	gedit	18459	1000	1000	0xad54000	0
0xffff88003668dfc0	kworker/u128:0	18468	0	0	-0x1	0
0xffff88003bed97f0	kworker/u128:2	18584	0	0	-0x1	0
0xffff88003c2397f0	kworker/u128:3	18929	0	0	-0x1	0
0xffff88003b5edfc0	sudo	18968	0	1000	0x3b15d000	0
0xffff88003a290000	lmg	18969	0	0	0x3b6db000	0
0xffff88000010dfc0	insmod	18988	0	0	0x3c3b6000	0
0xffff8800001097f0	systemd-udev	18989	0	0	0x3c2d3000	0

# using Volatility: linux\_netstat

```
forensics@ubuntu:~/volatility$ python vol.py -f ubuntu-2014-12-21_11.54.35-memory.lime  
--profile=Linuxubuntu-14041x64 linux_netstat|grep -i tcp
```

Volatility Foundation Volatility Framework 2.4

TCP	127.0.1.1	:	53	0.0.0.0	:	0	LISTEN	dnsmasq/1134
TCP	::1	:	54643	::1	:	0	CLOSE_WAIT	cups-browsed/1170
TCP	::1	:	54644	::1	:	0	CLOSE_WAIT	indicator-print/2083
TCP	::1	:	631	::	:	0	LISTEN	cupsd/2365
TCP	127.0.0.1	:	631	0.0.0.0	:	32792	LISTEN	cupsd/2365
TCP	192.168.182.132	:	42356	91.189.92.11	:	0	CLOSE_WAIT	unity-scope-hom/3068
TCP	192.168.182.132	:	56406	91.189.92.10	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42219	91.189.92.11	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	56408	91.189.92.10	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42221	91.189.92.11	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	56410	91.189.92.10	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42223	91.189.92.11	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	56412	91.189.92.10	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42645	91.189.92.23	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42225	91.189.92.11	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42642	91.189.92.23	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	35596	91.189.92.24	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	35594	91.189.92.24	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42647	91.189.92.23	:	0	CLOSE_WAIT	gvfsd-http/3146
TCP	192.168.182.132	:	42643	91.189.92.23	:	0	CLOSE_WAIT	gvfsd-http/3146

# Volatility: processes

**Pslist:** énumère les process « comme Windows ».

Ne trouve pas les process « cachés »

Volatility Foundation Volatility Framework 2.4

Offset (V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x823c8830	System	4	0	46	194	-----	0		
0x820679e8	smss.exe	552	4	3	17	-----	0	2014-12-20 20:53:52 UTC+0000	
0x81f39930	csrss.exe	616	552	8	232	0	0	2014-12-20 20:53:54 UTC+0000	
0x82206020	winlogon.exe	640	552	22	281	0	0	2014-12-20 20:53:54 UTC+0000	
0x81f18020	services.exe	684	640	18	246	0	0	2014-12-20 20:53:54 UTC+0000	
0x81e4f020	lsass.exe	696	640	22	296	0	0	2014-12-20 20:53:54 UTC+0000	
0x82135880	vmacthlp.exe	852	684	2	26	0	0	2014-12-20 20:53:54 UTC+0000	

**Pstree:** hiérarchie des process

Name	Pid	PPid	Thds	Hnds	Time
0x823c8830:System	4	0	58	276	1970-01-01 00:00:00 UTC+0000
. 0x820679e8:smss.exe	552	4	3	19	2014-12-20 20:53:52 UTC+0000
.. 0x82206020:winlogon.exe	640	552	18	322	2014-12-20 20:53:54 UTC+0000
... 0x81f08ac8:wpabaln.exe	1220	640	1	67	2015-01-25 18:35:52 UTC+0000
... 0x81f18020:services.exe	684	640	17	355	2014-12-20 20:53:54 UTC+0000
.... 0x8227ec38:vmtoolsd.exe	172	684	8	283	2014-12-20 20:54:14 UTC+0000
.... 0x8223dda0:imapi.exe	1804	684	5	116	2015-01-24 15:03:21 UTC+0000
.... 0x822ca390:svchost.exe	1028	684	77	1476	2014-12-20 20:53:55 UTC+0000
..... 0x8228fd30:wuauc1t.exe	836	1028	8	178	2015-01-25 18:35:51 UTC+0000

# Volatility: processes (2)

**Psxview:** énumère les process via plusieurs méthodes et compare les résultats

Permet de lister les process « cachés » ou ceux terminés

Offset (P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x02335880	vmacthlp.exe	852	True	True	True	True	True	True	True	
0x02211980	vmtoolsd.exe	1692	True	True	True	True	True	True	True	
0x0234f020	spoolsv.exe	1468	True	True	True	True	True	True	True	
0x024ca390	svchost.exe	1028	True	True	True	True	True	True	True	
0x0215b998	svchost.exe	1136	True	True	True	True	True	True	True	
0x023c8498	TPAutoConnSvc.e	2000	True	True	True	True	True	True	True	
0x02206aa0	wmiprvse.exe	1352	True	True	True	True	True	True	False	
0x02406020	winlogon.exe	640	True	True	True	True	True	True	True	
0x023c75a8	cmd.exe	788	True	True	True	True	True	True	True	
0x01f8eb18	DumpIt.exe	204	True	True	True	True	True	True	True	
0x0248fd30	wuaucflt.exe	836	True	True	True	True	True	True	True	
0x02211da0	ctfmon.exe	1716	True	True	True	True	True	True	True	
0x0247ec38	vmtoolsd.exe	172	True	True	True	True	True	True	True	
...										
0x023f5da0	svchost.exe	864	True	True	True	True	True	True	True	
0x0234d558	alg.exe	1064	True	True	True	True	True	True	True	
0x02106a80	explorer.exe	1588	True	True	True	True	True	True	True	
0x02360c10	wscntfy.exe	1356	True	True	True	True	True	True	True	
0x021016e8	svchost.exe	936	True	True	True	True	True	True	False	
0x0243dda0	imapi.exe	1804	True	True	True	True	True	True	True	
0x02139930	csrss.exe	616	True	True	True	True	False	True	True	
0x025c8830	System	4	True	True	True	True	False	False	False	
0x022679e8	smss.exe	552	True	True	True	True	False	False	False	
0x1d726008	x?=?NtFs`q??	32...8	False	False	False	False	False	False	True	
0x024161d0		1672	False	True	False	False	False	False	False	2015-01-25 18:37:37 UTC+0000

# Processes, dll

**dlllist:** énumère les dll (bibliothèques dynamiques) importées

Permet de comprendre les fonctionnalités utilisées par le process

```
*****
csrss.exe pid:      608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
                ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
                ProfileControl=Off MaxRequestThreads=16
Service Pack 2

Base              Size  LoadCount Path
-----
0x4a680000      0x5000      0xffff \\??\C:\WINDOWS\system32\csrss.exe
0x7c900000      0xb0000      0xffff C:\WINDOWS\system32\ntdll.dll
0x75b40000       0xb000      0xffff C:\WINDOWS\system32\CSRSRV.dll
0x75b50000      0x10000       0x3 C:\WINDOWS\system32\basesrv.dll
0x75b60000      0x4a000       0x2 C:\WINDOWS\system32\winsrv.dll
0x77d40000      0x90000       0x6 C:\WINDOWS\system32\USER32.dll
0x7c800000      0xf4000       0xe C:\WINDOWS\system32\KERNEL32.dll
0x77f10000      0x46000       0x5 C:\WINDOWS\system32\GDI32.dll
0x75e90000      0xb0000       0x1 C:\WINDOWS\system32\sxs.dll
0x77dd0000      0x9b000       0x3 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000      0x91000       0x3 C:\WINDOWS\system32\RPCRT4.dll
*****
```

**dlldump:** pour extraire les dll sur disque

```
python vol.py -f ~/Desktop/win7_trial_64bit.raw --profile=Win7SP0x64 dlldump -p 1068 -D dlls/
```

# Processes, handles

**handles:** énumère les objets système liés aux process: mutant, file, token, key, process, timer, etc ([31 types](#))

Très utile pour détecter des signes de compromission (IOC), comme les noms des mutants par exemple

Offset (V)	Pid	Handle	Access	Type	Details
0x810b1660	4	0x4	0x1f0fff	Process	System(4)
0x810b0020	4	0x8	0x0	Thread	TID 12 PID 4
0xe10192c0	4	0xc	0xf003f	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\MEMORY MANAGEMENT\PREFETCHPARAMETERS
0xe1019880	4	0x10	0x0	Key	
0xe13b4578	4	0x14	0x2001f	Key	MACHINE\SYSTEM\SETUP
0xe101d140	4	0x18	0x20019	Key	MACHINE\HARDWARE\DESCRIPTION\SYSTEM\MULTIFUNCTIONADAPTER
...					
0xe13be308	4	0x30	0x20019	Key	MACHINE\SYSTEM\CONTROLSET001\SERVICES\EVENTLOG
0x810aa3a0	4	0x34	0x1f0003	Event	TRKWKs_EVENT
0xff255020	4	0x88	0x28	Process	lsass.exe (688)
0x810d0870	4	0x90	0x1f03ff	Thread	TID 96 PID 4
0xe13c50d0	4	0x94	0x20019	Key	MACHINE\SYSTEM\CONTROLSET001\SERVICES\ACPI\PARAMETERS
0xe14cbb0	4	0x9c	0x2001f	Key	MACHINE\HARDWARE\DEVICEMAP\SCSI\SCSI PORT 2\SCSI BUS 0\TARGET ID 0\LOGICAL UNIT ID 0
0x81045960	4	0xa0	0x1f0003	Event	VxKernel2VoldEvent
...					
0xe14c95c0	4	0xb4	0x2001f	Key	MACHINE\HARDWARE\DEVICEMAP\SCSI\SCSI PORT 2
0xe14c9020	4	0xb8	0x2001f	Key	MACHINE\HARDWARE\DEVICEMAP\SCSI
0xe14cbc48	4	0xbc	0x2001f	Key	MACHINE\HARDWARE\DEVICEMAP\SCSI
0xe14cc5d0	4	0xc4	0xf000f	Directory	WinDfs
0xe14cb708	4	0xcc	0xf000f	Directory	Harddisk0
0x80f03db0	4	0x1dc	0x3	File	\Device\Ip
0x80ffae30	4	0x1e0	0x1f01ff	File	\Device\RawIp\47
0x80f65400	4	0x234	0x120089	File	\Device\Tcp

## Filtrage par type : -t

```
python vol.py -f ~/Desktop/win7_trial_64bit.raw --profile=Win7SP0x64 handles -p 1068 -t Mutant
```

# Processes, getsids

**getsids:** énumère les privilèges (Security Identifiers) liés aux process  
Il faut identifier des processus avec des droits anormalement élevés

```
csrss.exe (608): S-1-5-18 (Local System)
csrss.exe (608): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-1-0 (Everyone)
csrss.exe (608): S-1-5-11 (Authenticated Users)
winlogon.exe (632): S-1-5-18 (Local System)
winlogon.exe (632): S-1-5-32-544 (Administrators)
winlogon.exe (632): S-1-1-0 (Everyone)
winlogon.exe (632): S-1-5-11 (Authenticated Users)
services.exe (676): S-1-5-18 (Local System)
services.exe (676): S-1-5-32-544 (Administrators)
services.exe (676): S-1-1-0 (Everyone)
services.exe (676): S-1-5-11 (Authenticated Users)
lsass.exe (688): S-1-5-18 (Local System)
lsass.exe (688): S-1-5-32-544 (Administrators)
lsass.exe (688): S-1-1-0 (Everyone)
lsass.exe (688): S-1-5-11 (Authenticated Users)
vmacthlp.exe (844): S-1-5-18 (Local System)
vmacthlp.exe (844): S-1-5-32-544 (Administrators)
vmacthlp.exe (844): S-1-1-0 (Everyone)
vmacthlp.exe (844): S-1-5-11 (Authenticated Users)
svchost.exe (856): S-1-5-18 (Local System)
svchost.exe (856): S-1-5-32-544 (Administrators)
svchost.exe (856): S-1-1-0 (Everyone)
svchost.exe (856): S-1-5-11 (Authenticated Users)
```

# Mémoire des process

**Memmap:** affiche les zones mémoire associées à un process

```
python vol.py -f dump.mem --profile=WinXPSP2x86Memmap -p 1788
```

```
VMUpgradeHelper pid: 1788
```

Virtual	Physical	Size	DumpFileOffset	(offset dans le fichier dump)
0x00020000	0x04a58000	0x1000	0x0	
0x0012a000	0x07d90000	0x1000	0x1000	
0x00150000	0x07c0d000	0x1000	0x2000	
0x00151000	0x077ce000	0x1000	0x3000	
0x00153000	0x00fa2000	0x1000	0x4000	
0x00155000	0x00e82000	0x1000	0x5000	
0x0015a000	0x00ea1000	0x1000	0x6000	
0x0015b000	0x007e2000	0x1000	0x7000	
0x0015c000	0x07d68000	0x1000	0x8000	
0x0015d000	0x00e29000	0x1000	0x9000	

**Memdump:** pour extraire ces zones

```
python vol.py -f dump.mem --profile=WinXPSP2x86 -p 1788 memdump -D out
```



# Mémoire des process (2)

**vaddump:** parcourt l'arbre de la mémoire allouée dynamiquement avec virtualalloc et sauvegarde chaque section séparément

```
K:\afti_forensic\volatility-2.4>python vol.py -f dump.vmem --profile=WinXPSP2x86 vaddump -p 216 -D out
Volatility Foundation Volatility Framework 2.4
```

Pid	Process	Start	End	Result
216	alg.exe	0x00190000	0x0019ffff	out\alg.exe.5f027e0.0x00190000-0x0019ffff.dmp
216	alg.exe	0x00020000	0x00020fff	out\alg.exe.5f027e0.0x00020000-0x00020fff.dmp
216	alg.exe	0x00010000	0x00010fff	out\alg.exe.5f027e0.0x00010000-0x00010fff.dmp
216	alg.exe	0x00080000	0x00082fff	out\alg.exe.5f027e0.0x00080000-0x00082fff.dmp

**vadinfo:** information détaillée sur ces zones mémoire

```
VAD node @ 0xff134d60 Start 0x00080000 End 0x00082fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
ControlArea @ff245490 Segment e17ab678
NumberOfSectionReferences: 0 NumberOfPfnReferences: 0
NumberOfMappedViews: 13 NumberOfUserReferences: 13
Control Flags: Commit: 1, HadUserReference: 1
First prototype PTE: e17ab6b8 Last contiguous PTE: e17ab6c8
Flags2: Inherit: 1, SecNoChange: 1
```

# Journaux système (event logs)

**evtlogs:** extrait les journaux systèmes. XP and 2003 only

```
python vol.py -f dump\sality.vmem --profile=WinXPSP2x86 evtlogs --save-evt -D out_
```

```
Volatility Foundation Volatility Framework 2.4
Saved raw .evt file to secevent.evt
Parsed data sent to secevent.txt
Saved raw .evt file to appevent.evt
Parsed data sent to appevent.txt
Saved raw .evt file to sysevent.evt
Parsed data sent to sysevent.txt
```

## Sysevents.txt:

```
2010-06-10 12:01:43 UTC+0000|sysevent.evt|MACHINENAME|N/A|EventLog|6009|Info|5.01.;2600;
    Service Pack 2;Uniprocessor Free
2010-06-10 12:01:43 UTC+0000|sysevent.evt|MACHINENAME|N/A|EventLog|6005|Info|N/A
2010-06-10 12:02:06 UTC+0000|sysevent.evt|MACHINENAME|N/A|Serial|2|Info|\Device\Serial0;
    \Device\Serial0
2010-06-10 12:02:06 UTC+0000|sysevent.evt|MACHINENAME|N/A|Serial|2|Info|\Device\Serial1;
    \Device\Serial1
2010-06-10 16:04:44 UTC+0000|sysevent.evt|BILLY-DB5B96DD3|N/A|EventLog|6011|Info|MACHINENAME;
```

# Modules noyau

**modules:** liste les modules noyau

Offset (V)	Name	Base	Size	File
0x810dbe68	ntoskrnl.exe	0x804d7000	0x1f6280	\WINDOWS\system32\ntkrnlpa.exe
0x810dbe00	hal.dll	0x806ce000	0x20380	\WINDOWS\system32\hal.dll
0x810dbd98	kdcom.dll	0xfc99b000	0x2000	\WINDOWS\system32\KDCOM.DLL
0x810dbd28	BOOTVID.dll	0xfc8ab000	0x3000	\WINDOWS\system32\BOOTVID.dll
0x810dbcc0	ACPI.sys	0xfc36c000	0x2e000	ACPI.sys
0x810d6008	WMILIB.SYS	0xfc99d000	0x2000	\WINDOWS\system32\DRIVERS\WMILIB.SYS
0x810d6fa0	pci.sys	0xfc35b000	0x11000	pci.sys
0x810d6f30	isapnp.sys	0xfc49b000	0x9000	isapnp.sys

**modscan:** scan la mémoire pour trouver des modules (y compris ceux cachés, ou anciens)

Offset (P)	Name	Base	Size	File
0x0000000001058d80	serenum.sys	0xfc93b000	0x4000	\SystemRoot\system32\DRIVERS\serenum.sys
0x000000000105ad70	vmmemctl.sys	0xfc9f7000	0x2000	\\?\C:\Program Files\VMware\VMware Tools\Drivers\memctl\
	vmmemctl.sys			
0x000000000105f0c8	dump_vm SCSI.sys	0xfbf36000	0x3000	\SystemRoot\System32\Drivers\dump_vm SCSI.sys
0x00000000010664a8	srv.sys	0xf355d000	0x53000	\SystemRoot\system32\DRIVERS\srv.sys
0x0000000001067700	mrxdav.sys	0xf35d8000	0x2d000	\SystemRoot\system32\DRIVERS\mrxdav.sys
0x000000000106f050	rasacd.sys	0xfc174000	0x3000	\SystemRoot\system32\DRIVERS\rasacd.sys
0x000000000106f8c8	Msfs.SYS	0xfc7c3000	0x5000	\SystemRoot\System32\Drivers\Msfs.SYS
0x0000000001070e60	i8042prt.sys	0xfc53b000	0xd000	\SystemRoot\system32\DRIVERS\i8042prt.sys
0x000000000108be28	dump_SCSIport.sys	0xfbf3a000	0x4000	\SystemRoot\System32\Drivers\dump_diskdump.sys

# Table des appels système

**ssdt:** affiche la table des appels systèmes et quel binaire l'implémente

```
[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80501030 with 284 entries
  Entry 0x0000: 0x8059849a (NtAcceptConnectPort) owned by ntoskrnl.exe
  Entry 0x0001: 0x805e5666 (NtAccessCheck) owned by ntoskrnl.exe
  Entry 0x0002: 0x805e8ec4 (NtAccessCheckAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0003: 0x805e5698 (NtAccessCheckByType) owned by ntoskrnl.exe
  Entry 0x0004: 0x805e8efe (NtAccessCheckByTypeAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0005: 0x805e56ce (NtAccessCheckByTypeResultList) owned by ntoskrnl.exe
  Entry 0x0006: 0x805e8f42 (NtAccessCheckByTypeResultListAndAuditAlarm) owned by ntoskrnl.exe
  Entry 0x0007: 0x805e8f86 (NtAccessCheckByTypeResultListAndAuditAlarmByHandle) owned by ntoskrnl.exe
...
SSDT[1] at bf997600 with 667 entries
  Entry 0x1000: 0xbf934ffe (NtGdiAbortDoc) owned by win32k.sys
  Entry 0x1001: 0xbf946a92 (NtGdiAbortPath) owned by win32k.sys
  Entry 0x1002: 0xbf8bf295 (NtGdiAddFontResourceW) owned by win32k.sys
  Entry 0x1003: 0xbf93e718 (NtGdiAddRemoteFontToDC) owned by win32k.sys
  Entry 0x1004: 0xbf9480a9 (NtGdiAddFontMemResourceEx) owned by win32k.sys
...
```

## filtrage:

```
$ grep -v win32k.sys ssdt.txt | grep -v ntoskrnl.exe
[x86] Gathering all referenced SSDTs from KTHREADs...
Finding appropriate address space for tables...
SSDT[0] at 80501030 with 284 entries
SSDT[1] at bf997600 with 667 entries
```

# Recherche d'objets système en mémoire

**driverscan:** recherche les structure DRIVER\_OBJECT en mémoire

Offset(P)	#Ptr	#Hnd	Start	Size	Service	Key	Name	Driver Name
0x0000000001058388	4	0	0xfc76b000	0x6b00	Fdc		Fdc	\Driver\Fdc
0x0000000001058e28	4	0	0xfc93b000	0x3c80	serenum		serenum	\Driver\serenum
...								
0x00000000010cd5f8	4	0	0xfc211000	0x8c480	Ntfs		Ntfs	\FileSystem\Ntfs

**filescan:** les fichiers ouverts et le type d'accès

Offset(P)	#Ptr	#Hnd	Access	Name
0x000000000096ca0	1	0	R--r-d	\Device\HarddiskVolume1\Documents and Settings\Administrator\Start Menu\Programs\Windows Media Player.lnk
0x0000000000353ad0	1	0	R--rwd	\Device\HarddiskVolume1\WINDOWS\system32\crypt32.dll
0x0000000000353cb8	1	0	R--rwd	\Device\HarddiskVolume1\WINDOWS\system32\apphelp.dll
0x00000000003f3f08	1	0	R--r-d	\Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0x0000000000471028	4	1	RW----	\Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT

Et aussi

**mutantscan,**

**symlinkscan,**

**thrdscan** (utilisé par psxview): pour les threads

**dumpfiles:** trouve des sections mémoires associés à un fichier

# Réseau (XP et 2003)

## connections: connections TCP actives

Offset (V)	Local Address	Remote Address	Pid
0x81e87620	172.16.112.128:1038	41.168.5.140:8080	1484

## connscan: scanne les connections TCP

Offset (P)	Local Address	Remote Address	Pid
0x01eacc00	192.168.16.129:1039	65.55.185.26:443	1068
0x01fd3170	192.168.16.129:1040	207.46.21.58:80	1068

## sockets: sockets TCP, UDP, RAW

Offset (V)	PID	Port	Proto	Protocol	Address	Create Time
0x81ddb780	664	500	17	UDP	0.0.0.0	2012-07-22 02:42:53 UTC+0000
0x82240d08	1484	1038	6	TCP	0.0.0.0	2012-07-22 02:44:45 UTC+0000
0x81dd7618	1220	1900	17	UDP	172.16.112.128	2012-07-22 02:43:01 UTC+0000
0x82125610	788	1028	6	TCP	127.0.0.1	2012-07-22 02:43:01 UTC+0000
0x8219cc08	4	445	6	TCP	0.0.0.0	2012-07-22 02:42:31 UTC+0000
0x81ec23b0	908	135	6	TCP	0.0.0.0	2012-07-22 02:42:33 UTC+0000
0x82276878	4	139	6	TCP	172.16.112.128	2012-07-22 02:42:38 UTC+0000
0x82277460	4	137	17	UDP	172.16.112.128	2012-07-22 02:42:38 UTC+0000
0x81e76620	1004	123	17	UDP	127.0.0.1	2012-07-22 02:43:01 UTC+0000
0x82172808	664	0	255	Reserved	0.0.0.0	2012-07-22 02:42:53 UTC+0000
0x81e3f460	4	138	17	UDP	172.16.112.128	2012-07-22 02:42:38 UTC+0000
0x821f0630	1004	123	17	UDP	172.16.112.128	2012-07-22 02:43:01 UTC+0000

et aussi **sockscan**

# Réseau (Vista et +)

## netscan: connections TCP et UDP actives

K:\afti\_forensic\volatility-2.4>python vol.py -f 20150106-214021.raw --profile=Win7SP1x64 netscan

Offset (V)	Local Address	Remote Address	Pid	Foreign Address	State	Pid	Owner	Created
Offset (P)	Proto	Local Address	Foreign Address					
0x4df1a10	UDPv4	0.0.0.0:50505	*:*			2652	svchost.exe	2015-01-06 21:34:26 UTC+0000
0x4df1a10	UDPv6	:::50505	*:*			2652	svchost.exe	2015-01-06 21:34:26 UTC+0000
0x3d646c70	UDPv4	0.0.0.0:5355	*:*			416	svchost.exe	2015-01-06 21:35:16 UTC+0000
0x3d647ec0	UDPv4	127.0.0.1:1900	*:*			2652	svchost.exe	2015-01-06 21:35:13 UTC+0000
0x3d64bc90	UDPv4	0.0.0.0:5355	*:*			416	svchost.exe	2015-01-06 21:35:16 UTC+0000
0x3d64bc90	UDPv6	:::5355	*:*			416	svchost.exe	2015-01-06 21:35:16 UTC+0000
0x3dd22d20	UDPv4	0.0.0.0:3702	*:*			2652	svchost.exe	2015-01-06 21:35:18 UTC+0000
0x3dd22d20	UDPv6	:::3702	*:*			2652	svchost.exe	2015-01-06 21:35:18 UTC+0000
0x3dd23350	UDPv4	0.0.0.0:0	*:*			416	svchost.exe	2015-01-06 21:35:13 UTC+0000
0x3dd23350	UDPv6	:::0	*:*			416	svchost.exe	2015-01-06 21:35:13 UTC+0000
0x3d654cf0	TCPv4	192.168.1.42:139	0.0.0.0:0	LISTENING		4	System	
0x3d827480	TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING		4	System	
0x3d827480	TCPv6	:::5357	:::0	LISTENING		4	System	
0x3d8cc010	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING		536	lsass.exe	
0x3d8cc010	TCPv6	:::49156	:::0	LISTENING		536	lsass.exe	
0x3d8dfd70	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING		536	lsass.exe	
0x3dalc7b0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING		888	svchost.exe	
0x3dbe6340	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING		528	services.exe	
0x3dbe7af0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING		528	services.exe	
0x3dbe7af0	TCPv6	:::49155	:::0	LISTENING		528	services.exe	
0x3dbef1b0	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING		4	System	
0x3dbef1b0	TCPv6	:::445	:::0	LISTENING		4	System	
0x3dc94aa0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING		712	svchost.exe	
0x3dc98820	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING		712	svchost.exe	
0x3dc98820	TCPv6	:::135	:::0	LISTENING		712	svchost.exe	
0x3dc9ec60	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING		420	wininit.exe	
0x3dc9ec60	TCPv6	:::49152	:::0	LISTENING		420	wininit.exe	
0x3dcb5930	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING		420	wininit.exe	
0x3dcff830	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING		760	svchost.exe	
0x3dcff830	TCPv6	:::49153	:::0	LISTENING		760	svchost.exe	
0x3dcaecf0	TCPv6	:-0	e8a9:e702:80fa:ffff:e8a9:e702:80fa:ffff:0	CLOSED		1	???????	
0x3dd55200	TCPv4	:-0	56.139.242.2:0	CLOSED		1004	svchost.exe	
0x3e151650	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING		760	svchost.exe	
0x3e19f010	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING		888	svchost.exe	
0x3e19f010	TCPv6	:::49154	:::0	LISTENING		888	svchost.exe	
0x3e198500	TCPv4	:-0	56.139.242.2:0	CLOSED		2		
0x3fa5a010	UDPv4	127.0.0.1:50327	*:*			2284	iexplore.exe	2015-01-06 21:36:55 UTC+0000
0x3faafae0	UDPv4	127.0.0.1:65250	*:*			1396	iexplore.exe	2015-01-06 21:37:00 UTC+0000
0x3fae2670	UDPv4	127.0.0.1:54923	*:*			2328	iexplore.exe	2015-01-06 21:36:46 UTC+0000

# Registre

**hivelist:** liste les ruches présentes en mémoire et le fichier associé

Virtual	Physical	Name
0xelc49008	0x036dc008	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.d
0xelc41b60	0x04010b60	\Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xela39638	0x021eb638	\Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass
0xela33008	0x01f98008	\Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60	0x06b7db60	\Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008	0x06c48008	\Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60	0x06ae4b60	\SystemRoot\System32\Config\SECURITY
0xe1544008	0x06c4b008	\Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xel3ae580	0x01bbd580	[no name]
0xe101b008	0x01867008	\Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978	0x01824978	[no name]
0xe1e158c0	0x009728c0	\Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.d
0xe1da4008	0x00f6e008	\Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT

**printkey:** permet l'affichage d'une valeur de clé de registre. Ex: `printkey -K "Microsoft\Security Center\Svc"`

Volatility Foundation Volatility Framework 2.4  
Legend: (S) = Stable (V) = Volatile

-----  
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software  
Key name: Svc (S)  
Last updated: 2010-08-15 17:43:26 UTC+0000

Subkeys:

Values:  
REG\_DWORD AntiVirusOverride : (S) 1  
REG\_DWORD AntiVirusDisableNotify : (S) 1  
REG\_DWORD FirewallDisableNotify : (S) 1  
REG\_DWORD FirewallOverride : (S) 1  
REG\_DWORD UpdatesDisableNotify : (S) 1  
REG\_DWORD UacDisableNotify : (S) 1



# Registre, actions utilisateurs

## userassist: lancement des applications

```
REG_BINARY      %windir%\system32\cmd.exe :
Count:          2
Focus Count:    3
Time Focused:   0:03:04.659000
Last updated:   2015-01-06 21:35:51 UTC+0000
0x00000000  00 00 00 00 02 00 00 00 03 00 00 00 5f cf 02 00  ....._...
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 60 8a 7b be  .....`.{.
0x00000040  f8 29 d0 01 00 00 00 00  .....).
REG_BINARY      %windir%\explorer.exe :
Count:          1
Focus Count:    3
Time Focused:   0:00:33.464000
Last updated:   2015-01-06 21:36:08 UTC+0000
0x00000000  00 00 00 00 01 00 00 00 03 00 00 00 c4 80 00 00  .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 60 3e 22 c8  .....`>".
0x00000040  f8 29 d0 01 00 00 00 00  .....).

```

## shellbags: parcours de l'arborescence des fichiers avec Windows Explorer (ici -output=body)

```
Scanning for registries....
Gathering shellbag items and building path tree...
0|[SHELLBAGS FILE ENTRY] Name: Users/Attrs: RO, DIR/FullPath: C:\Users\Registry: \??\C:\Users\forensics\AppData\Local\Microsoft\
Windows\UsrClass.dat /Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0/LW: 2015-01-06 21:35:39 UTC+0000|
0|-----|0|0|0|1419103052|1419103052|1247541610|1247541610
0|[SHELLBAGS FILE ENTRY] Name: forensics/Attrs: DIR/FullPath: C:\Users\forensics /Registry: \??\C:\Users\forensics\AppData\Local\Microsoft\
Windows\UsrClass.dat /Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0/LW: 2015-01-06 21:35:44 UTC+0000|
0|-----|0|0|0|1419103124|1419103124|1419103052|1419103052

```

# Système de fichiers, MFT

**mftparser:** extrait la MFT de la mémoire (ici -output=body)

```
python vol.py -f dump.vmem --profile=WinXPSP3x86 mftparser --output=body  
> mftparser.txt
```

Scanning for MFT entries and building directory, this can take a while

```
0|[MFT FILE NAME] SYSTEM~1\ RESTO~1\RP15\snapshot\ R62E7~1 (Offset: 0x1400)|11745|---a-----c-I---|  
0|0|0|1281506955|1281506955|1281506955|1281506955  
0|[MFT STD INFO] SYSTEM~1\ RESTO~1\RP15\snapshot\ R62E7~1 (Offset: 0x1400)|11745|---a-----c-I---|  
0|0|0|1281506955|1281506955|1281506955|1281506955  
0|[MFT FILE NAME] SYSTEM~1\ RESTO~1\RP15\snapshot\ REGISTRY_MACHINE_SYSTEM (Offset: 0x1400)|11745|---a-----c  
0|0|0|1281506955|1281506955|1281506955|1281506955  
0|[MFT FILE NAME] SYSTEM~1\ RESTO~1\RP15\snapshot\ R25B6~1 (Offset: 0x1800)|11746|---a-----c-I---|  
0|0|0|1281506956|1281506956|1281506956|1281506956  
0|[MFT STD INFO] SYSTEM~1\ RESTO~1\RP15\snapshot\ R25B6~1 (Offset: 0x1800)|11746|---a-----c-I---|  
0|0|0|1281506956|1281506956|1281506956|1281506956
```

```
c:\sleuthkit-4.1.2-win32\bin\mactime.pl -b mftparser.txt > mftparser_tl.txt
```

```
Thu Jan 06 2011 15:36:56      70144 ..c. ---a----- 0          0          55741      [MFT STD_INFO]  
Documents and Settings\Administrator\Desktop\A977C3~1.EXE (Offset: 0x1b084400)  
Thu Jan 06 2011 15:37:00      7680 .a.. ---a----- 0          0          2031      [MFT STD_INFO]  
WINDOWS\system32\rasadhlp.dll (Offset: 0x2442c00)  
Thu Jan 06 2011 15:37:01      0 .a.. ---a----- 0          0          100969     [MFT STD_INFO]  
Documents and Settings\Administrator\Cookies\AD6E43~1.TXT (Offset: 0xed6e400)
```

# timeliner

**timeliner:** clacée une supertime regroupant des informations de nombreux plugin

```

0 m... ----- 0      0      0      [THREAD] System PID: 4/TID: 12
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 616
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 620
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 624
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 628
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 640
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 644
0 .acb ----- 0      0      0      [THREAD] csrss.exe PID: 608/TID: 648
0 .acb ----- 0      0      0      [THREAD] winlogon.exe PID: 632/TID: 636
Wed Aug 11 2010 08:06:24 0 mach ----- 0      0      0      [Handle (Key)] MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\
WINLOGON svchost.exe PID: 856/PPID: 676/POffset: 0x0115b8d8
0 mach ----- 0      0      0      [Handle (Key)] MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\
WINLOGON winlogon.exe PID: 632/PPID: 544/POffset: 0x066f0978
0 mach ----- 0      0      0      [Handle (Key)] MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\
WINLOGON\CREDENTIALS winlogon.exe PID: 632/PPID: 544/POffset: 0x066f0978

Wed Aug 11 2010 08:06:35 0 mach ----- 0      0      0      [Handle (Key)] MACHINE\SYSTEM\CONTROLSET001\SERVICES\LANMANSERVER\
PARAMETERS svchost.exe PID: 1028/PPID: 676/POffset: 0x01122910
0 .acb ----- 0      0      0      [PROCESS] vmtoolsd.exe PID: 1668/PPID: 676/POffset: 0x069d5b28
0 mach ----- 0      0      0      [SOCKET] LocalIP: 0.0.0.0/Protocol: 255(Reserved) PID: 688/
POffset: 0x0x06237b70
0 mach ----- 0      0      0      [SOCKET] LocalIP: 0.0.0.0:4500/Protocol: 17(UDP) PID: 688/
POffset: 0x0x069d5250
0 mach ----- 0      0      0      [SOCKET] LocalIP: 0.0.0.0:500/Protocol: 17(UDP) PID: 688/
POffset: 0x0x05f44008

...
Sun Aug 15 2010 19:38:54 0 mach ----- 0      0      0      [SOCKET] LocalIP: 0.0.0.0:1048/Protocol: 6(TCP) PID: 1028/POffset: 0x0x04be3c
0 mach ----- 0      0      0      [SOCKET] LocalIP: 127.0.0.1:1047/Protocol: 17(UDP) PID: 1028/POffset: 0x0x061
Sun Aug 15 2010 19:39:06 0 m... ----- 0      0      0      [THREAD] svchost.exe PID: 1028/TID: 532
Sun Aug 15 2010 19:39:34 0 m... ----- 0      0      0      [THREAD] svchost.exe PID: 1028/TID: 1692
Sun Aug 15 2010 19:39:40 0 m... ----- 0      0      0      [THREAD] lsass.exe PID: 688/TID: 740

...
Sun Aug 15 2010 19:43:26 0 mach ----- 0      0      0      [Handle (Key)] MACHINE\SOFTWARE\MICROSOFT\SECURITY CENTER svchost.exe
PID: 1028/PPID: 676/POffset: 0x01122910
0 mach ----- 0      0      0      [Handle (Key)] USER\S-1-5-21-1614895754-436374069-839522115-500\
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\USERASSIST\{75048700-EF1F-11D0-9888-006097DEACF9}\COUNT explorer.exe
PID: 1724/PPID: 1708/POffset: 0x04a065d0
0 mach ----- 0      0      0      [Handle (Key)] USER\S-1-5-21-1614895754-436374069-839522115-500\
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS VMwareUser.exe PID: 452/PPID: 1724/POffset: 0x04b5a980
```

# Résumé

- Examiner en premier les connections réseaux et les adresses IP destination. Quelle est leur réputation ?
- Examiner les processus (pslist, psxview), leur parent, le nombre d'exemplaire d'un processus du même nom (le nom peut être usurpé). Est-il lancé depuis le bon répertoire ? A-t-il le bon processus père (pstree) ? N'a-t-il pas trop de droits (getssids) pour ce qu'il est censé faire. N'utilise-t-il pas trop de ressources (handles) ? Trop ou trop peu de bibliothèques externes utilisées (dlllist) et des fonctions utilisées surprenantes (aucun lien avec les fonctionnalités « officielles » du processus) ? Quels sont les processus injectés (malfind), les appels systèmes modifiés (ssdt) ?

# Résumé (2)

- Quelles sont les sessions en cours (sessions) ? Plug-in [Hashdump](#) pour les authentifiants et comptes de domaine stockés en mémoire
- Vérifier les processus lancés au démarrage (autoruns, printkey)
- Quelles sont les dernières applications lancées (userassist), les derniers fichiers créés (mftparser)

# Autres plug-ins

- Chrome history, Firefox history, PreFetch, UnInstallInfo (C. David Lassalle, Jr)

<https://github.com/superponible/volatility-plugins>

```
$ python vol.py --plugins=volatility-plugins-master -f memdump.mem --  
profile=Win7SP1x64 chromehistory >chromehistory.txt
```

- Autoruns (Thomas Chopita)

<https://github.com/tomchop/volatility-autoruns>

avec d'autres plug-in:

- <https://github.com/volatilityfoundation/community>

# Pour aller plus loin

Pour des exemples et plus de détails

<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>

Dump mémoires, pour s'entraîner

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

<https://code.google.com/p/volatility/wiki/FAQ>

[#Are there any public memory samples available that I can use for](#)

## The Art Of Memory Forensics

