**Analyse mémoire Windows**

**Récupérer les hash de la capture**

volatility -f dump.raw --profile=Win7SP1x86 hashdump

*Administrator:500:aad3b435b51404e……3c59d7e0c089c0:::*

*Guest:501:aad3b435b51404eeaad3……e0d16ae931b73c59d7e0c089c0:::*

*John Doe:1000:aad3b435b51404e……53e3dbf6e6831ecce60725930:::*

**Afficher les valeurs de registre**

volatility -f dump.raw --profile Win7SP1x86 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"

*----------------------------*

*Registry: \??\C:\Users\John Doe\ntuser.dat*

*Key name: Run (S)*

*Last updated: 2013-01-12 14:13:19*

*Subkeys:*

*Values:*

*REG\_SZ RESTART\_STICKY\_NOTES : (S) C:\Windows\System32\Malware.exe*

*REG\_SZ IEPreload : (S) "C:\Users\John Doe\AppData\Roaming\malware.exe*

**Afficher les commandes en cours**

volatility -f dump.raw --profile Win7SP1x86 cmdline

*AvastUI.exe pid: 2720*

*Command line : "C:\Program Files\AVAST Software\Avast\AvastUI.exe" /nogui*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*StikyNot.exe pid: 2744*

*Command line : "C:\Windows\System32\StikyNot.exe"*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*iexplore.exe pid: 2772*

*Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*SearchIndexer. pid: 2900*

*Command line : C:\Windows\system32\SearchIndexer.exe /Embedding*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*wmpnetwk.exe pid: 3176*

*Command line : "C:\Program Files\Windows Media Player\wmpnetwk.exe"*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

**Afficher les fichiers de la mémoire en cache**

volatility -f memory.dmp --profile=Win7SP1x86 filescan

**Extraire tous les fichiers en cache (Long et gourmand en stockage)**

volatility -f memory.dmp --profile=Win7SP1x86 dumpfiles -D files/ > files.txt

**Extraire un fichier particulier**

volatility -f memory.dmp --profile=Win7SP0x86 dumpfiles -D filedump/ -Q 0x000000001ee20118

#0x000000001ee20118 est l'adresse du fichier indiqué dans filescan

**Extraire un processus en mémoire**

volatility -f memory.dmp --profile=Win7SP0x86 procexedump -D procdump/ -p 2772