Sommaire

[1. Retrouver le Hostname d’une machine 1](#_Toc155035451)

# 1. Retrouver le Hostname d’une machine

Lancer volatility et utiliser les commandes suivantes :

1. Trouver le profile correspondant
2. Trouver l’hexadécimal correspondant au système
3. Utiliser l’hexadécimal pour retrouver le hostname

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "C:\Users\samy2\Bureau\ch2.dmp" --profile=Win7SP1x86\_23418 imageinfo

Volatility Foundation Volatility Framework 2.6

INFO : volatility.debug : Determining profile based on KDBG search...

Suggested Profile(s) : Win7SP1x86\_23418, Win7SP0x86, Win7SP1x86

AS Layer1 : IA32PagedMemoryPae (Kernel AS)

AS Layer2 : FileAddressSpace (C:\Users\samy2\Bureau\ch2.dmp)

PAE type : PAE

DTB : 0x185000L

KDBG : 0x82929be8L

Number of Processors : 1

Image Type (Service Pack) : 0

KPCR for CPU 0 : 0x8292ac00L

KUSER\_SHARED\_DATA : 0xffdf0000L

Image date and time : 2013-01-12 16:59:18 UTC+0000

Image local date and time : 2013-01-12 17:59:18 +0100

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "C:\Users\samy2\Bureau\ch2.dmp" --profile=Win7SP1x86\_23418 hivelist

Volatility Foundation Volatility Framework 2.6

Virtual Physical Name

---------- ---------- ----

0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE

0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT

0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat

0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat

0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM

0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY

0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT

0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT

0x8b20c008 0x039e1008 [no name]

0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM

0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE

0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "C:\Users\samy2\Bureau\ch2.dmp" --profile=Win7SP1x86\_23418 printkey -o 0x8b21c008 -K 'ControlSet001\Control\ComputerName\ComputerName'

Volatility Foundation Volatility Framework 2.6

Legend: (S) = Stable (V) = Volatile

----------------------------

Registry: \REGISTRY\MACHINE\SYSTEM

Key name: ComputerName (S)

Last updated: 2013-01-12 00:58:30 UTC+0000

Subkeys:

Values:

REG\_SZ : (S) mnmsrvc

REG\_SZ ComputerName : (S) WIN-ETSA91RKCFP