

# forens

- [Isma](#)
- [nagib](#)

# Isma

user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive\$ date && md5sum ram.raw && date

```
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$ date && md5sum disk.raw && date
Sat Mar  1 12:51:01 PM CET 2025
52d37fddf9f9079938cb369029082f7a  disk.raw
Sat Mar  1 12:51:02 PM CET 2025
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$
```

user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive\$ date && md5sum ram.raw && date

```
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$ date && md5sum ram.raw && date
Sat Mar  1 12:52:59 PM CET 2025
e7ecd0038dc178141ef2ee61b6633a  ram.raw
Sat Mar  1 12:53:01 PM CET 2025
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$
```

user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive\$ tar -cvf archive.tar disk.raw ram.raw

```
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$ tar -cvf archive.tar disk.raw ram.raw
disk.raw
ram.raw
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$
```

user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive\$ date && md5sum archive.tar && date

```
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$ date && md5sum archive.tar && date
Sat Mar  1 01:16:04 PM CET 2025
63656d137622dd1a6ab393b67ab8de0b  archive.tar
Sat Mar  1 01:16:06 PM CET 2025
user@debian:/mnt/hgfs/esgi/4jan/forensic/exam/archive$
```

# nagib

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py -f ./raw/ram.raw imageinfo
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py -f ./raw/ram.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win10x64_19041
                               AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                               AS Layer2 : FileAddressSpace (/root/volatility/raw/ram.raw)
                               PAE type  : No PAE
                               DTB       : 0x1aa002L
                               KDBG      : 0xf80170010b20L
           Number of Processors : 1
           Image Type (Service Pack) : 0
           KPCR for CPU 0       : 0xffffffff8016e42000L
           KUSER_SHARED_DATA    : 0xffffffff7800000000L
           Image date and time  : 2025-02-27 10:06:12 UTC+0000
           Image local date and time : 2025-02-27 02:06:12 -0800
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw p
```

Afin de trouver des PID intéressant a exploiter

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw sessions
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw sessions
Volatility Foundation Volatility Framework 2.6.1
*****
Session(V): ffff8e0174a57000 ID: 0 Processes: 50
PagedPoolStart: ffff8b0d00000000 PagedPoolEnd ffff8b2cffffffff
Process: 424 csrss.exe 2025-02-27 19:02:21 UTC+0000
Process: 496 wininit.exe 2025-02-27 19:02:22 UTC+0000
Process: 616 services.exe 2025-02-27 19:02:23 UTC+0000
Process: 628 lsass.exe 2025-02-27 19:02:23 UTC+0000
Process: 704 fontdrvhost.exe 2025-02-27 19:02:24 UTC+0000
Process: 772 svchost.exe 2025-02-27 19:02:24 UTC+0000
Process: 820 svchost.exe 2025-02-27 19:02:25 UTC+0000
Process: 984 svchost.exe 2025-02-27 19:02:28 UTC+0000
Process: 1012 svchost.exe 2025-02-27 19:02:28 UTC+0000
Process: 248 svchost.exe 2025-02-27 19:02:28 UTC+0000
Process: 352 svchost.exe 2025-02-27 19:02:28 UTC+0000
Process: 1076 svchost.exe 2025-02-27 19:02:30 UTC+0000
Process: 1224 svchost.exe 2025-02-27 19:02:32 UTC+0000
Process: 1336 VBoxService.exe 2025-02-27 19:02:33 UTC+0000
Process: 1492 svchost.exe 2025-02-27 10:02:37 UTC+0000
Process: 1620 svchost.exe 2025-02-27 10:02:38 UTC+0000
Process: 1636 svchost.exe 2025-02-27 10:02:38 UTC+0000
Process: 1644 svchost.exe 2025-02-27 10:02:38 UTC+0000
Process: 1668 svchost.exe 2025-02-27 10:02:38 UTC+0000
Process: 1800 spoolsv.exe 2025-02-27 10:02:39 UTC+0000
Process: 1836 svchost.exe 2025-02-27 10:02:39 UTC+0000
Process: 1932 svchost.exe 2025-02-27 10:02:40 UTC+0000
Process: 1632 svchost.exe 2025-02-27 10:02:44 UTC+0000
Process: 2320 svchost.exe 2025-02-27 10:02:51 UTC+0000
Process: 2372 MicrosoftEdgeU 2025-02-27 10:02:52 UTC+0000
Process: 2388 CompatTelRunne 2025-02-27 10:02:52 UTC+0000
Process: 2476 MsMpEng.exe 2025-02-27 10:02:53 UTC+0000
Process: 2624 svchost.exe 2025-02-27 10:02:53 UTC+0000
Process: 2732 WmiPrvSE.exe 2025-02-27 10:02:54 UTC+0000
Process: 2764 sppsvc.exe 2025-02-27 10:02:54 UTC+0000
Process: 2948 conhost.exe 2025-02-27 10:02:58 UTC+0000
Process: 2224 svchost.exe 2025-02-27 10:03:00 UTC+0000
Process: 3028 SearchIndexer. 2025-02-27 10:03:02 UTC+0000
Process: 3512 NisSrv.exe 2025-02-27 10:03:21 UTC+0000
Process: 3576 AggregatorHost 2025-02-27 10:03:22 UTC+0000
Process: 3648 svchost.exe 2025-02-27 10:03:27 UTC+0000
Process: 3832 SearchFilterHo 2025-02-27 10:03:35 UTC+0000
Process: 3876 TrustedInstall 2025-02-27 10:03:43 UTC+0000
Process: 3916 TiWorker.exe 2025-02-27 10:03:44 UTC+0000
Process: 3952 CompatTelRunne 2025-02-27 10:03:46 UTC+0000
Process: 4180 MoUsoCoreWorke 2025-02-27 10:04:03 UTC+0000
Process: 4392 svchost.exe 2025-02-27 10:04:05 UTC+0000
Process: 4456 Usoclient.exe 2025-02-27 10:04:05 UTC+0000
Process: 788 SecurityHealth 2025-02-27 10:04:44 UTC+0000
Process: 5260 SearchProtocol 2025-02-27 10:04:53 UTC+0000
Process: 5328 svchost.exe 2025-02-27 10:04:54 UTC+0000
Process: 5680 audiodg.exe 2025-02-27 10:05:10 UTC+0000
Process: 5032 svchost.exe 2025-02-27 10:05:41 UTC+0000
Process: 5812 SppExtComObj.E 2025-02-27 10:05:55 UTC+0000
Process: 5612 svchost.exe 2025-02-27 10:06:00 UTC+0000
*****
```

```
Session(V): fffff8e0175680000 ID: 1 Processes: 28
PagedPoolStart: fffff8b0d00000000 PagedPoolEnd fffff8b2cfffffffff
Process: 504 csrss.exe 2025-02-27 19:02:22 UTC+0000
Process: 552 winlogon.exe 2025-02-27 19:02:22 UTC+0000
Process: 696 fontdrvhost.ex 2025-02-27 19:02:24 UTC+0000
Process: 912 dwm.exe 2025-02-27 19:02:26 UTC+0000
Process: 2156 sihost.exe 2025-02-27 10:02:49 UTC+0000
Process: 2172 svchost.exe 2025-02-27 10:02:49 UTC+0000
Process: 2268 taskhostw.exe 2025-02-27 10:02:51 UTC+0000
Process: 2420 taskhostw.exe 2025-02-27 10:02:52 UTC+0000
Process: 2520 taskhostw.exe 2025-02-27 10:02:53 UTC+0000
Process: 2920 ctfmon.exe 2025-02-27 10:02:57 UTC+0000
Process: 3244 userinit.exe 2025-02-27 10:03:13 UTC+0000
Process: 3264 explorer.exe 2025-02-27 10:03:13 UTC+0000
Process: 3456 SearchProtocol 2025-02-27 10:03:21 UTC+0000
Process: 1264 svchost.exe 2025-02-27 10:03:53 UTC+0000
Process: 3348 smartscreen.ex 2025-02-27 10:03:56 UTC+0000
Process: 1900 notepad.exe 2025-02-27 10:03:58 UTC+0000
Process: 3616 TextInputHost. 2025-02-27 10:04:00 UTC+0000
Process: 1296 StartMenuExper 2025-02-27 10:04:01 UTC+0000
Process: 4356 RuntimeBroker. 2025-02-27 10:04:04 UTC+0000
Process: 4700 SearchApp.exe 2025-02-27 10:04:11 UTC+0000
Process: 4824 RuntimeBroker. 2025-02-27 10:04:16 UTC+0000
Process: 1232 RuntimeBroker. 2025-02-27 10:04:33 UTC+0000
Process: 4172 SecurityHealth 2025-02-27 10:04:42 UTC+0000
Process: 4136 VBoxTray.exe 2025-02-27 10:04:44 UTC+0000
Process: 712 OneDrive.exe 2025-02-27 10:04:45 UTC+0000
Process: 5292 dllhost.exe 2025-02-27 10:04:54 UTC+0000
Process: 5800 cmd.exe 2025-02-27 10:05:13 UTC+0000
Process: 5808 conhost.exe 2025-02-27 10:05:13 UTC+0000
```

---> ICI ON TROUVE EXPLORER 3264

Examinez les variables d'environnement des processus utilisateur comme `explorer.exe` (PID 3264)  
./vol.py --profile=Win10x64\_19041 -f raw/ram.raw envvars -p 3264



```

root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw envvars -p 3264
Volatility Foundation Volatility Framework 2.6.1

```

Pid	Process	Block	Variable	Value
3264	explorer.exe	0x000000007f77970	ALLUSERSPROFILE	C:\ProgramData
3264	explorer.exe	0x000000007f77970	APPDATA	C:\Users\cyberdog\AppData\Roaming
3264	explorer.exe	0x000000007f77970	CommonProgramFiles	C:\Program Files\Common Files
3264	explorer.exe	0x000000007f77970	CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
3264	explorer.exe	0x000000007f77970	CommonProgramW6432	C:\Program Files\Common Files
3264	explorer.exe	0x000000007f77970	COMPUTERNAME	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	ComSpec	C:\Windows\system32\cmd.exe
3264	explorer.exe	0x000000007f77970	DriverData	C:\Windows\System32\Drivers\DriverData
3264	explorer.exe	0x000000007f77970	FPS_BROWSER_APP_PROFILE_STRING	Internet Explorer
3264	explorer.exe	0x000000007f77970	FPS_BROWSER_US...ROFILE_STRING	Default
3264	explorer.exe	0x000000007f77970	HOMEDRIVE	C:
3264	explorer.exe	0x000000007f77970	HOMEPATH	\Users\cyberdog
3264	explorer.exe	0x000000007f77970	LOCALAPPDATA	C:\Users\cyberdog\AppData\Local
3264	explorer.exe	0x000000007f77970	LOGONSERVER	\\DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	NUMBER_OF_PROCESSORS	1
3264	explorer.exe	0x000000007f77970	OneDrive	C:\Users\cyberdog\OneDrive
3264	explorer.exe	0x000000007f77970	OS	Windows_NT
3264	explorer.exe	0x000000007f77970	Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\cyberdog\AppData\Local\Microsoft\WindowsApps;.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
3264	explorer.exe	0x000000007f77970	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
3264	explorer.exe	0x000000007f77970	PROCESSOR_ARCHITECTURE	AMD64
3264	explorer.exe	0x000000007f77970	PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 154 Stepping 4, GenuineIntel
3264	explorer.exe	0x000000007f77970	PROCESSOR_LEVEL	6
3264	explorer.exe	0x000000007f77970	PROCESSOR_REVISION	9a04
3264	explorer.exe	0x000000007f77970	ProgramData	C:\ProgramData
3264	explorer.exe	0x000000007f77970	ProgramFiles	C:\Program Files
3264	explorer.exe	0x000000007f77970	ProgramFiles(x86)	C:\Program Files (x86)
3264	explorer.exe	0x000000007f77970	ProgramW6432	C:\Program Files
3264	explorer.exe	0x000000007f77970	PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
3264	explorer.exe	0x000000007f77970	PUBLIC	C:\Users\Public
3264	explorer.exe	0x000000007f77970	SESSIONNAME	Console
3264	explorer.exe	0x000000007f77970	SystemDrive	C:
3264	explorer.exe	0x000000007f77970	SystemRoot	C:\Windows
3264	explorer.exe	0x000000007f77970	TEMP	C:\Users\cyberdog\AppData\Local\Temp
3264	explorer.exe	0x000000007f77970	TMP	C:\Users\cyberdog\AppData\Local\Temp
3264	explorer.exe	0x000000007f77970	USERDOMAIN	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	USERDOMAIN_ROAMINGPROFILE	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	USERNAME	cyberdog
3264	explorer.exe	0x000000007f77970	USERPROFILE	C:\Users\cyberdog
3264	explorer.exe	0x000000007f77970	windir	C:\Windows

USER = cyberdog

```

root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw envvars -p 3264
Volatility Foundation Volatility Framework 2.6.1

```

Pid	Process	Block	Variable	Value
3264	explorer.exe	0x000000007f77970	ALLUSERSPROFILE	C:\ProgramData
3264	explorer.exe	0x000000007f77970	APPDATA	C:\Users\cyberdog\AppData\Roaming
3264	explorer.exe	0x000000007f77970	CommonProgramFiles	C:\Program Files\Common Files
3264	explorer.exe	0x000000007f77970	CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
3264	explorer.exe	0x000000007f77970	CommonProgramW6432	C:\Program Files\Common Files
3264	explorer.exe	0x000000007f77970	COMPUTERNAME	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	ComSpec	C:\Windows\system32\cmd.exe
3264	explorer.exe	0x000000007f77970	DriverData	C:\Windows\System32\Drivers\DriverData
3264	explorer.exe	0x000000007f77970	FPS_BROWSER_APP_PROFILE_STRING	Internet Explorer
3264	explorer.exe	0x000000007f77970	FPS_BROWSER_US...ROFILE_STRING	Default
3264	explorer.exe	0x000000007f77970	HOMEDRIVE	C:
3264	explorer.exe	0x000000007f77970	HOMEPATH	\Users\cyberdog
3264	explorer.exe	0x000000007f77970	LOCALAPPDATA	C:\Users\cyberdog\AppData\Local
3264	explorer.exe	0x000000007f77970	LOGONSERVER	\\DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	NUMBER_OF_PROCESSORS	1
3264	explorer.exe	0x000000007f77970	OneDrive	C:\Users\cyberdog\OneDrive
3264	explorer.exe	0x000000007f77970	OS	Windows_NT
3264	explorer.exe	0x000000007f77970	Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\cyberdog\AppData\Local\Microsoft\WindowsApps;.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
3264	explorer.exe	0x000000007f77970	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
3264	explorer.exe	0x000000007f77970	PROCESSOR_ARCHITECTURE	AMD64
3264	explorer.exe	0x000000007f77970	PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 154 Stepping 4, GenuineIntel
3264	explorer.exe	0x000000007f77970	PROCESSOR_LEVEL	6
3264	explorer.exe	0x000000007f77970	PROCESSOR_REVISION	9a04
3264	explorer.exe	0x000000007f77970	ProgramData	C:\ProgramData
3264	explorer.exe	0x000000007f77970	ProgramFiles	C:\Program Files
3264	explorer.exe	0x000000007f77970	ProgramFiles(x86)	C:\Program Files (x86)
3264	explorer.exe	0x000000007f77970	ProgramW6432	C:\Program Files
3264	explorer.exe	0x000000007f77970	PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
3264	explorer.exe	0x000000007f77970	PUBLIC	C:\Users\Public
3264	explorer.exe	0x000000007f77970	SESSIONNAME	Console
3264	explorer.exe	0x000000007f77970	SystemDrive	C:
3264	explorer.exe	0x000000007f77970	SystemRoot	C:\Windows
3264	explorer.exe	0x000000007f77970	TEMP	C:\Users\cyberdog\AppData\Local\Temp
3264	explorer.exe	0x000000007f77970	TMP	C:\Users\cyberdog\AppData\Local\Temp
3264	explorer.exe	0x000000007f77970	USERDOMAIN	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	USERDOMAIN_ROAMINGPROFILE	DESKTOP-N40M1FH
3264	explorer.exe	0x000000007f77970	USERNAME	cyberdog
3264	explorer.exe	0x000000007f77970	USERPROFILE	C:\Users\cyberdog
3264	explorer.exe	0x000000007f77970	windir	C:\Windows

Nom ordinateur = DESKTOP-N40M1FH

Trouver la version de l'OS :

```
./vol.py --profile=Win10x64_19041 -f raw/ram.raw kdbgscan
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw kdbgscan
Volatility Foundation Volatility Framework 2.6.1
*****
Instantiating KDBG using: Unnamed AS Win10x64_19041 (6.4.19041 64bit)
Offset (V)           : 0xf80170010b20
Offset (P)           : 0x3800b20
KdCopyDataBlock (V)  : 0xf8016f9219f8
Block encoded        : Yes
Wait never           : 0x7f1920ab006d4f27
Wait always          : 0x36a7890ff92e18
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win10x64_19041
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)   : 19041.1.amd64fre.vb_release.1912
PsActiveProcessHead         : 0xffffffff8017002e070 (81 processes)
PsLoadedModuleList          : 0xffffffff8017003a320 (173 modules)
KernelBase                  : 0xffffffff8016f410000 (Matches MZ: True)
Major (OptionalHeader)      : 10
Minor (OptionalHeader)      : 0
KPCR                        : 0xffffffff8016e420000 (CPU 0)
```

sortie :

- Le système est bien "Win10x64\_19041" (Windows 10 64-bit)
- Service Pack: 0
- Build string: "19041.1.amd64fre.vb\_release.1912"

Cela correspond à Windows 10 version 2004 (également connue sous le nom de "May 2020 Update"). Le nombre "19041" est la build exacte de Windows 10, et l'architecture est 64-bit (amd64).

Pour vérifier si Windows Defender est actif dans l'image mémoire, vous pouvez examiner plusieurs aspects :

1. Vérifiez les processus liés à Windows Defender :

```
./vol.py --profile=Win10x64_19041 -f raw/ram.raw pslist | grep -i "defender\|msmp"
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw pslist | grep -i "defender\|msmp"
Volatility Foundation Volatility Framework 2.6.1
0xffffda019d1a7280 MsMpEng.exe          2476    616    29      0      0      0 2025-02-27 10:02:53 UTC+0000
```

D'après votre sortie du plugin `sessions` partagée précédemment, je vois déjà que le processus `MsMpEng.exe` (PID 2476) est en cours d'exécution. C'est le service principal de Windows Defender, donc cela indique qu'il est probablement actif.

2. Vérifiez les services Windows liés à Windows Defender :

```
./vol.py --profile=Win10x64_19041 -f raw/ram.raw svcscan | grep -i  
"defender\|msmp\|wdfilter\|windefend"
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw svcscan | grep -i "defender\|msmp\|wdfilter\|windefend"  
Volatility Foundation Volatility Framework 2.6.1  
Display Name: Windows Defender Firewall  
Service Name: WinDefend  
Display Name: Microsoft Defender Antivirus Service  
Binary Path: "C:\Program Files\Windows Defender\MsMpEng.exe"  
Display Name: Microsoft Defender Antivirus Network Inspection Service  
Binary Path: "C:\Program Files\Windows Defender\NisSrv.exe"  
Display Name: Microsoft Defender Antivirus Network Inspection System Driver  
Service Name: WdFilter  
Display Name: WdFilter  
Binary Path: \FileSystem\WdFilter
```

3 : Examinez les clés de registre liées à Windows Defender pour voir sa configuration :

```
./vol.py --profile=Win10x64_19041 -f raw/ram.raw printkey -K "Microsoft\Windows Defender"
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw printkey -K "Microsoft\Windows Defender"  
Volatility Foundation Volatility Framework 2.6.1  
Legend: (S) = Stable (V) = Volatile  
  
-----  
Registry: \SystemRoot\System32\Config\SOFTWARE  
Key name: Windows Defender (S)  
Last updated: 2025-02-27 09:54:04 UTC+0000  
  
Subkeys:  
(S) Exclusions  
(S) Features  
(S) Miscellaneous Configuration  
(S) MpEngine  
(S) NIS  
(S) Quarantine  
(S) Real-Time Protection  
(S) Remediation  
(S) Reporting  
(S) Scan  
(S) Signature Updates  
(S) Spynet  
(S) Threats  
(S) UX Configuration  
(S) WCOS  
(S) Windows Defender Exploit Guard  
  
Values:  
REG_SZ ProductAppDataPath : (S) C:\ProgramData\Microsoft\Windows Defender  
REG_EXPAND_SZ ProductIcon : (S) @%ProgramFiles%\Windows Defender\EppManifest.dll,-100  
REG_EXPAND_SZ ProductLocalizedName : (S) @%ProgramFiles%\Windows Defender\EppManifest.dll,-1000  
REG_EXPAND_SZ RemediationExe : (S) windowsdefender://  
REG_DWORD ProductType : (S) 2  
REG_BINARY InstallTime : (S)  
  
REG_SZ InstallLocation : (S) C:\Program Files\Windows Defender\  
REG_DWORD ManagedDefenderProductType : (S) 0  
REG_BINARY OOBInstallTime : (S)  
0x00000000 84 77 0e d9 48 89 db 01 .w..H...  
REG_DWORD ProductStatus : (S) 0
```

4/ Vous pouvez également examiner les processus `SecurityHealthService` qui sont aussi liés à Windows Defender dans les versions récentes de Windows 10 :

```
./vol.py --profile=Win10x64_19041 -f raw/ram.raw pslist | grep -i "securityhealth"
```

```
root@DESKTOP-BPQ10UP:~/volatility# ./vol.py --profile=Win10x64_19041 -f raw/ram.raw pslist | grep -i "securityhealth"  
Volatility Foundation Volatility Framework 2.6.1  
0xffffda019554e340 SecurityHealth 4172 3264 7 0 1 0 2025-02-27 10:04:42 UTC+0000  
0xffffda019550e240 SecurityHealth 788 616 15 0 0 0 2025-02-27 10:04:44 UTC+0000
```

Je remarque également dans vos données de session que `SecurityHealth` est en cours d'exécution (PID 788 et 4172), ce qui est un autre indicateur que Windows Defender est probablement actif.



La présence des processus `MsMpEng.exe` et `SecurityHealth` suggère fortement que Windows Defender était actif au moment de la capture mémoire, mais une analyse plus approfondie avec les commandes ci-dessus vous donnera plus de détails sur sa configuration exacte.

-----

après votre analyse, il est clair que Windows Defender est actif sur le système. Voici plusieurs indicateurs qui le confirment :

1. Services liés à Windows Defender en cours d'exécution :
  - "Microsoft Defender Antivirus Service" (`MsMpEng.exe`)
  - "Microsoft Defender Antivirus Network Inspection Service" (`NisSrv.exe`)
  - "Windows Defender Firewall" (`WinDefend`)
  - Le pilote "WdFilter" est également chargé
2. Les clés de registre pour Windows Defender contiennent de nombreuses sous-clés actives, notamment :
  - "Real-Time Protection" indique que la protection en temps réel est configurée
  - "Scan", "Signature Updates", "Remediation" et autres composants essentiels
3. Deux processus `SecurityHealth` sont en cours d'exécution (PID 788 et 4172), ce qui est typique d'une installation de Windows Defender fonctionnelle
4. Le processus `MsMpEng.exe` (moteur principal de Defender) que vous aviez identifié précédemment

La valeur "ProductStatus : 0" dans le registre pourrait indiquer un statut spécifique, mais la présence de tous les processus actifs et des services en fonctionnement confirme que Windows Defender est bien activé et opérationnel sur le système au moment de la capture mémoire.

Cette information peut être importante dans votre analyse forensique car elle indique que le système disposait d'une protection antivirus active, ce qui pourrait influencer votre évaluation des risques ou l'analyse d'un éventuel incident de sécurité.

## EN PLUS

application :

keylogger[backspace]?action=add&username=\pctotaldefender\sqlite3.dllsoftware\microsoft\windows\currentversion\runprocess monitor - sysinternals: [www.sysinternals.com](http://www.sysinternals.com)