

TP Volatility Guillaume Sanchez

1) Testez et expliquez en détail le format et les résultats des commandes suivantes :

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.info :

```
(venv) nkapop-os:~/Documents/outils/volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.info
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0x82801000
DTB 0x185000
Symbols jar:file:/home/nk/Documents/outils/volatility3/volatility3/symbols/windows.zip!windows/ntkrpamp.pdb/5B308B4ED6464159B87117C711E7340C-2.json.xz
Is64Bit False
IsPAE True
Layer_name 0 WindowsIntelPAE
Memory_layer 1 FileLayer
KdDebuggerDataBlock 0x82929be8
NTBuildLab 7600.16385.x86fre.win7_rtm.09071
CSDVersion 0
KdVersionBlock 0x82929bc0
Major/Minor 15.7600
MachineType 332
KeNumberProcessors 1
SystemTime 2013-01-12 16:59:18:00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 6
NtMinorVersion 1
PE_MajorOperatingSystemVersion 6
PE_MinorOperatingSystemVersion 1
PE_Machine 332
PE_TimeDateStamp Mon Jul 13 23:15:19 2009
```

Cette commande permet de récupérer des informations générales sur le système Windows contenu dans le dump mémoire.

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.pslist :

```
(venv) nkapop-os:~/Documents/outils/volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.pslist
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4 0 System 0x87978b78 103 3257 N/A False 2013-01-12 16:38:09.000000 UTC N/A Disabled
388 4 smss.exe 0x88c3ed40 2 29 N/A False 2013-01-12 16:38:09.000000 UTC N/A Disabled
404 396 csrss.exe 0x8929fd40 9 469 0 False 2013-01-12 16:38:14.000000 UTC N/A Disabled
456 396 wininit.exe 0x892ac2b8 3 77 0 False 2013-01-12 16:38:14.000000 UTC N/A Disabled
468 448 csrss.exe 0x88d03a00 10 471 1 False 2013-01-12 16:38:14.000000 UTC N/A Disabled
500 448 winlogon.exe 0x892ce4d0 3 111 1 False 2013-01-12 16:38:14.000000 UTC N/A Disabled
500 456 services.exe 0x896294c0 6 205 0 False 2013-01-12 16:38:16.000000 UTC N/A Disabled
576 456 lsass.exe 0x896427b8 6 566 0 False 2013-01-12 16:38:16.000000 UTC N/A Disabled
584 456 lsm.exe 0x8962f7e8 10 142 0 False 2013-01-12 16:38:16.000000 UTC N/A Disabled
692 560 svchost.exe 0x8962f030 10 353 0 False 2013-01-12 16:38:21.000000 UTC N/A Disabled
764 560 svchost.exe 0x897b5c20 7 263 0 False 2013-01-12 16:38:23.000000 UTC N/A Disabled
832 560 svchost.exe 0x89805420 19 435 0 False 2013-01-12 16:38:23.000000 UTC N/A Disabled
904 560 svchost.exe 0x89852918 17 409 0 False 2013-01-12 16:38:24.000000 UTC N/A Disabled
928 560 svchost.exe 0x8986b030 26 869 0 False 2013-01-12 16:38:24.000000 UTC N/A Disabled
1084 560 svchost.exe 0x898911a8 10 257 0 False 2013-01-12 16:38:26.000000 UTC N/A Disabled
1172 560 svchost.exe 0x898b2790 15 475 0 False 2013-01-12 16:38:27.000000 UTC N/A Disabled
1220 560 AvastSvc.exe 0x898a7868 66 1180 0 False 2013-01-12 16:38:28.000000 UTC N/A Disabled
1712 560 spoolsv.exe 0x8a0f9c40 14 338 0 False 2013-01-12 16:38:58.000000 UTC N/A Disabled
1748 560 svchost.exe 0x8a102748 18 310 0 False 2013-01-12 16:38:58.000000 UTC N/A Disabled
1872 560 spssvc.exe 0x88ced4d0 4 143 0 False 2013-01-12 16:39:02.000000 UTC N/A Disabled
1968 560 vntoolsd.exe 0x8a16d4e0 6 220 0 False 2013-01-12 16:39:14.000000 UTC N/A Disabled
336 560 vlm.exe 0x95a1c7e0 4 45 0 False 2013-01-12 16:39:21.000000 UTC N/A Disabled
448 560 VMUpgradeHelp 0x8a1f5030 4 89 0 False 2013-01-12 16:39:21.000000 UTC N/A Disabled
1612 560 TPAutoConnSvc. 0x9542a030 9 135 0 False 2013-01-12 16:39:23.000000 UTC N/A Disabled
2352 560 taskhost.exe 0x87ac8620 8 149 1 False 2013-01-12 16:40:24.000000 UTC N/A Disabled
2496 904 dm.exe 0x87ad4d0 5 77 1 False 2013-01-12 16:40:25.000000 UTC N/A Disabled
2548 2484 explorer.exe 0x87ae0030 24 766 1 False 2013-01-12 16:40:27.000000 UTC N/A Disabled
2568 1612 TPAutoConnect. 0x87ae2880 5 146 1 False 2013-01-12 16:40:28.000000 UTC N/A Disabled
2608 468 conhost.exe 0x87a9c288 1 35 1 False 2013-01-12 16:40:28.000000 UTC N/A Disabled
2668 2548 VMWareTray.exe 0x87b02438 5 80 1 False 2013-01-12 16:40:29.000000 UTC N/A Disabled
2676 2548 VMWareUser.exe 0x87a9a220 8 190 1 False 2013-01-12 16:40:30.000000 UTC N/A Disabled
2720 2548 AvastUI.exe 0x87b784b0 14 220 1 False 2013-01-12 16:40:31.000000 UTC N/A Disabled
2744 2548 StickyNot.exe 0x898f8c0 8 135 1 False 2013-01-12 16:40:32.000000 UTC N/A Disabled
2772 2548 iexplore.exe 0x87b6b030 2 74 1 False 2013-01-12 16:40:34.000000 UTC N/A Disabled
2996 560 SearchIndexer. 0x898fb518 13 636 0 False 2013-01-12 16:40:38.000000 UTC N/A Disabled
3176 560 wmpnetwk.exe 0x87bd35b0 9 240 0 False 2013-01-12 16:40:48.000000 UTC N/A Disabled
3352 560 svchost.exe 0x89f3d2c0 9 141 0 False 2013-01-12 16:40:58.000000 UTC N/A Disabled
3452 2548 swriter.exe 0x87c6a2a0 1 19 1 False 2013-01-12 16:41:01.000000 UTC N/A Disabled
3512 3452 soffice.exe 0x87ba4030 1 28 1 False 2013-01-12 16:41:03.000000 UTC N/A Disabled
3556 3544 soffice.bin 0x95a83d18 0 1 1 False 2013-01-12 16:41:05.000000 UTC 2013-01-12 16:41:39.000000 UTC Disabled
3564 3512 soffice.bin 0x87b0ca58 12 408 1 False 2013-01-12 16:41:05.000000 UTC N/A Disabled
3624 560 svchost.exe 0x89f1d3e8 14 348 0 False 2013-01-12 16:41:22.000000 UTC N/A Disabled
1232 2548 taskmgr.exe 0x95a95c18 6 116 1 False 2013-01-12 16:42:29.000000 UTC N/A Disabled
3152 2548 cmd.exe 0x87bf7030 1 23 1 False 2013-01-12 16:44:58.000000 UTC N/A Disabled
2238 468 conhost.exe 0x87c595b0 2 54 1 False 2013-01-12 16:44:58.000000 UTC N/A Disabled
1616 2772 cmd.exe 0x89898030 2 101 1 False 2013-01-12 16:55:49.000000 UTC N/A Disabled
2168 468 conhost.exe 0x95a826b0 2 49 1 False 2013-01-12 16:55:50.000000 UTC N/A Disabled
1136 2548 iexplore.exe 0x95a9f678 18 454 1 False 2013-01-12 16:57:44.000000 UTC N/A Disabled
3044 1136 iexplore.exe 0x87d4d338 37 937 1 False 2013-01-12 16:57:46.000000 UTC N/A Disabled
1728 832 audiodg.exe 0x87c98040 5 117 0 False 2013-01-12 16:58:11.000000 UTC N/A Disabled
3144 3152 winpmem-1.3.1. 0x87c6b4d0 1 23 1 False 2013-01-12 16:59:17.000000 UTC N/A Disabled
```

Cette commande affiche la liste des processus actifs (programmes en cours d'exécution) au moment où le dump mémoire a été capturé.

[illegible]

```
python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | more :
```

Cette commande permet d'afficher tous les handles ouverts (objets système) par un processus spécifique — ici, le processus dont le PID est 1136.

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | select-string File | more adapté en python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | grep File | more sur linux :

```
(venv) [root@kali:~/Documents/CC_Niveau2]# python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | grep File | more
1136ressiexplo.exe 0x892c3db08 scan8x8g FileMutant 0x1f0001 RasPBFile
1136 iexplo.exe 0x87da1470 0x18 File 0x12019f \Device\NaswSP_Open
1136 iexplo.exe 0x87da48640 0x1c File 0x120089 \Device\NaswSxn
1136 iexplo.exe 0x896cead8 0x40 File 0x120089 \Device\HarddiskVolume1\Program Files\Internet Explorer\en-US\iexplore.exe.mui
1136 iexplo.exe 0x89fa1610 0xc8 File 0x100020 \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
1136 iexplo.exe 0x8974f1a0 0xe8 File 0x100020 \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
1136 iexplo.exe 0x87dc2990 0xf0 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{2F55D46D-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x8a134c10 0x130 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
1136 iexplo.exe 0x98ae2800 0x138 Section 0x2 C:\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat_49152
1136 iexplo.exe 0x8a10f730 0x148 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
1136 iexplo.exe 0x87b6ebc8 0x154 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
1136 iexplo.exe 0x9492b040 0x1a8 File 0x100001 \Device\KSecCD
1136 iexplo.exe 0x87da3750 0x234 File 0x100080 \Device\Nsi
1136 iexplo.exe 0x87ae7408 0x24c File 0x120089 \Device\HarddiskVolume1\Windows\System32\en-US\urlmon.dll.mui
1136 iexplo.exe 0x87a6da98 0x304 File 0x100020 \Device\HarddiskVolume1\Users\John Doe\Desktop
1136 iexplo.exe 0x8838ec98 0x454 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{2F55D46D-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x8a1a8890 0x460 File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF0D5AB10AB7495357.TMP
1136 iexplo.exe 0x87b0cc00 0x47c File 0x120089 \Device\HarddiskVolume1\Windows\Fonts\StaticCache.dat
1136 iexplo.exe 0x87b3ae00 0x4a0 File 0x100020 \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
1136 iexplo.exe 0x87d9a288 0x51c File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF077B88B350A1EDC4.TMP
1136 iexplo.exe 0x87dc2b78 0x578 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\Cache\index.dat
1136 iexplo.exe 0x88bdec18 0x588 File 0x120089 \Device\HarddiskVolume1\Windows\System32\en-US\oleaccr.dll.mui
1136 iexplo.exe 0x8a1307f8 0x67c File 0x120089 \Device\KSecCD
1136 iexplo.exe 0x87bd9370 0x5e0 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{2F55D46F-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x89f8e840 0x5fc File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DFF1B534C38558A33.TMP
1136 iexplo.exe 0x8a137f80 0x61c File 0x100081 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Suggested Sites--feed.ms
1136 iexplo.exe 0x87b4c1e8 0x624 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Suggested Sites--feed.ms
1136 iexplo.exe 0x87d8fbb8 0x62c File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF1099E6C55A71776F.TMP
1136 iexplo.exe 0x87bba5c8 0x634 File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF081A8849DF6AFA7.TMP
1136 iexplo.exe 0x8a04c520 0x650 File 0x120089 \Device\HarddiskVolume1\Windows\System32\en-US\KernelBase.dll.mui
1136 iexplo.exe 0x898dbb20 0x664 File 0x120089 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb.ms
1136 iexplo.exe 0x954e0d98 0x66c File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DFA63F59B0C681C479.TMP
1136 iexplo.exe 0x8a137940 0x674 File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF58AB08AA5E8C2C2E.TMP
1136 iexplo.exe 0x8a1307f8 0x67c File 0x120089 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb.ms
1136 iexplo.exe 0x87c74bb8 0x680 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Web Slice Gallery--feed.ms
1136 iexplo.exe 0x89ff7a70 0x688 File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF492DD69AB833AC61.TMP
1136 iexplo.exe 0x87d8d918 0x68c File 0x100081 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Web Slice Gallery--feed.ms
1136 iexplo.exe 0x95489730 0x694 File 0x13019f \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Temp\~DF0A247EB32CE4CAD9.TMP
1136 iexplo.exe 0x87c483c8 0x6b8 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\SuggestedSites.dat
1136 iexplo.exe 0x87c4a1e0 0x6c8 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Roaming\Microsoft\Windows\Internet\Files\Low\SuggestedSites.dat
1136 iexplo.exe 0x87c170e0 0x6dc File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013011220130113\index.dat
dex.dat
```

Cette commande permet d'afficher uniquement les *fichiers* ouverts par le processus dont le PID est 1136 dans l'image mémoire CC_Niveau2.dmp.

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | select-string File | select-string "John Doe" adapté en python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | grep File | grep "John Doe" sur Linux :

```
(venv) [root@kali:~/Documents/CC_Niveau2]# python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.handles --pid 1136 | grep File | grep "John Doe"
1136ressiexplo.exe 0x87dc29908 scan8x8g FileMutant 0x1f0001 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{2F55D46D-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x8a134c10 0x130 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
1136 iexplo.exe 0x98ae2800 0x138 Section 0x2 C:\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat_49152
1136 iexplo.exe 0x8a10f730 0x148 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
1136 iexplo.exe 0x87b6ebc8 0x154 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
1136 iexplo.exe 0x87ad6a98 0x304 File 0x100020 \Device\HarddiskVolume1\Users\John Doe\Desktop
1136 iexplo.exe 0x8838ec98 0x454 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{2F55D46C-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x87d9370 0x500 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{2F55D46F-5CD9-11E2-BEEA-000C290020D}.dat
1136 iexplo.exe 0x8a137f80 0x61c File 0x100081 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Suggested Sites--feed.ms
1136 iexplo.exe 0x87b4c1e8 0x624 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Suggested Sites--feed.ms
1136 iexplo.exe 0x898dbb20 0x664 File 0x120089 \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb.ms
1136 iexplo.exe 0x8a1307f8 0x67c File 0x120089 \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Microsoft\Feeds\FeedsStore.feedsdb.ms
1136 iexplo.exe 0x87c74bb8 0x680 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Web Slice Gallery--feed.ms
1136 iexplo.exe 0x87d8d918 0x68c File 0x100081 \Device\HarddiskVolume1\Users\JOHNDO-1\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A9203D}\WebSlices\Web Slice Gallery--feed.ms
1136 iexplo.exe 0x87c483c8 0x6b8 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\SuggestedSites.dat
1136 iexplo.exe 0x87c4a1e0 0x6c8 File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Roaming\Microsoft\Windows\Internet\Files\Low\SuggestedSites.dat
1136 iexplo.exe 0x87c170e0 0x6dc File 0x12019f \Device\HarddiskVolume1\Users\John Doe\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013011220130113\index.dat
```

Cette commande permet d'afficher uniquement les fichiers ouverts par le processus PID 1136 qui contiennent le nom "John Doe" dans leur chemin d'accès ou leur nom de fichier.

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp -o "fichier_dump"
windows.dumpfile --pid 1136 --virtaddr 0x87c4a1e0 :

```
(venv) hkappop-es:~/Documents/outils/volatility$ mkdir fichier_dump
(venv) hkappop-es:~/Documents/outils/volatility$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp -o "fichier_dump" windows.dumpfile --pid 1136 --virtaddr 0x87c4a1e0
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0x87c4a1e0 index.dat file.0x87c4a1e0.0x954f21d8.DataSectionObject.index.dat.dat
SharedCacheMap 0x87c4a1e0 index.dat file.0x87c4a1e0.0x87ac2de0.SharedCacheMap.index.dat.vach
(venv) hkappop-es:~/Documents/outils/volatility$ cd fichier_dump/
(venv) hkappop-es:~/Documents/outils/volatility/fichier_dump$ ll
total 316
drwxrwxr-x 2 nk nk 4096 juin 11 13:55 /
drwxrwxr-x 1 nk nk 4096 juin 11 13:55 ./
-rw-r----- 1 nk nk 262144 juin 11 13:55 file.0x87c4a1e0.0x87ac2de0.SharedCacheMap.index.dat.vach
-rw-r----- 1 nk nk 126976 juin 11 13:55 file.0x87c4a1e0.0x954f21d8.DataSectionObject.index.dat.dat
```

Cette commande permet d'extraire un objet mémoire (comme un fichier ou un module) à partir d'une adresse virtuelle spécifique (0x87c4a1e0), qui est mappée dans le processus dont le PID est 1136, et elle enregistre le contenu extrait dans un fichier nommé fichier_dump

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.cmdline | more :

```
(venv) hkappop-es:~/Documents/outils/volatility$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.cmdline | more
Volatility 3 Framework 2.26.2 PDB scanning finished
PID Process Args
4 System -
180 smss.exe \SystemRoot\System32\smss.exe
184 csrss.exe \SystemRoot\System32\csrss.exe ObjectDirectory\Windows SharedSection=1024,12288,512 Windows-Dr SubSystemType=Windows ServerDll=basesrv,1 ServerDll=win32srv
0\Initialization,3 ServerDll=win32srv\ConServerDllInitialization,3 ServerDll=win32srv,4 ProfileControl=off MaxRequestThreads=16
188 wininit.exe
448 csrss.exe \SystemRoot\System32\csrss.exe ObjectDirectory\Windows SharedSection=1024,12288,512 Windows-Dr SubSystemType=Windows ServerDll=basesrv,1 ServerDll=win32srv
0\Initialization,3 ServerDll=win32srv\ConServerDllInitialization,3 ServerDll=win32srv,4 ProfileControl=off MaxRequestThreads=16
588 winlogon.exe
596 services.exe C:\Windows\System32\services.exe
598 lsass.exe C:\Windows\System32\lsass.exe
602 lsass.exe C:\Windows\System32\lsass.exe
604 smss.exe C:\Windows\System32\smss.exe -k DesktopLaunch
764 svchost.exe C:\Windows\System32\svchost.exe -k RPCSS
832 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
984 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
988 svchost.exe C:\Windows\System32\svchost.exe -k Netlogon
1084 svchost.exe C:\Windows\System32\svchost.exe -k LocalService
1124 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService
1228 AvastSvc.exe "C:\Program Files\AVAST Software\Avast\AvastSvc.exe"
1712 spoolsv.exe C:\Windows\System32\spoolsv.exe
1748 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetwork
1872 spssvc.exe "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
1968 vmtoolsd.exe
236 wls.exe -
448 VMToolsd.exe
1612 TPAutoConnSvc.exe "C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe"
2382 taskhost.exe
2496 dm.exe "C:\Windows\System32\dm.exe"
2498 explorer.exe C:\Windows\Explorer.exe
2568 TPAutoConnSvc.exe -s -i vmtoolsd -a COM1 -F 10
2608 conhost.exe
2676 VMwareTray.exe "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
2728 VMwareTray.exe "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
2744 vmtoolsd.exe "C:\Program Files\AVAST Software\Avast\vmtoolsd.exe" /angui
2744 stikybot.exe "C:\Windows\System32\stikybot.exe"
2772 explorer.exe "C:\Users\John.Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\explorer.exe"
2808 SearchIndexer.exe C:\Windows\System32\SearchIndexer.exe /Embedding
3176 vmtoolsd.exe "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
3332 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetwork
3452 writer.exe -
3512 soffice.exe -
3556 soffice.bin -
3564 soffice.bin "C:\Program Files\LibreOffice 3.6\program\writer.exe" "-a" "C:\Users\John.Doe\Documents\Procedure Wimpendump.odt" "--writer" "-env:000_CMD=C:\Users\John.Doe\Doc
uments"
3624 svchost.exe C:\Windows\System32\svchost.exe -k secsscs
3732 taskmgr.exe "C:\Windows\System32\taskmgr.exe" /a
3732 cmd.exe "C:\Windows\System32\cmd.exe"
3728 conhost.exe
3748 cmd.exe cmd.exe
3748 conhost.exe \??:C:\Windows\System32\conhost.exe
3844 explorer.exe "C:\Program Files\Internet Explorer\explorer.exe"
3844 explorer.exe "C:\Program Files\Internet Explorer\explorer.exe" SCODEF:1136 CRD0AT:71977
3778 audiodg.exe C:\Windows\System32\AUDIOIO.DLL Hx298
3844 vmtoolsd-1.3.1 vmtoolsd-1.3.1.exe -env dmp
```

Cette commande permet d'afficher la ligne de commande exacte utilisée pour lancer chaque processus dans l'image mémoire CC_Niveau2.dmp

```
python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp  
windows.registry.userassist.UserAssist | more :
```

[illegible]

Cette commande permet d'extraire et décoder les clés UserAssist de la base de registre Windows contenue dans une image mémoire (dump). Elle nous montre le nom des programmes utilisés par l'utilisateur, leur chemin d'accès, un compteur d'exécution, les dernières dates d'exécution et parfois des GUID ou chemins associés à des raccourcis.

```
python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.hashdump |  
more:
```

```

[setenv]
setenv PATH %PATH%;C:\Python\python.exe;C:\ProgramFiles\CC\Microsoft\Windows\Hashdump\1.0.0
/home/robert/Documents/outils/volatility/volatility.py framework/operation.py:281 FutureWarning: This API (volatility.plugins.windows.registry.hashdump.Hashdump.run) will be removed in the first release after 2025-09-25. This plugin has been renamed, please call volatility.plugins.windows.registry.hashdump.Hashdump.run rather than volatility.plugins.WindowsRegistry.Hashdump.run
warning:warn:
volatility 3 framework/operation.py:180 FutureWarning: This plugin (volatility.plugins.windows.hashdump.Hashdump) has been renamed and will be removed in the first release after 2025-09-25. Please ensure all method calls to this pl
warning:warn:
volatility 3 framework/operation.py:180 FutureWarning: This plugin (volatility.plugins.windows.hashdump.Hashdump) has been renamed and will be removed in the first release after 2025-09-25. Please ensure all method calls to this pl
warning:warn:
volatility 3 framework/2.76.2
User rid lshash oshash
Administrator 500 aad3b435b51404eeaad3b435b51404e 31d6cfed1ae31b73159d7e0c689c0
Guest 001 aad3b435b51404eeaad3b435b51404e 31d6cfed1ae31b73159d7e0c689c0
User 002 aad3b435b51404eeaad3b435b51404e 31d6cfed1ae31b73159d7e0c689c0

```

Cette commande permet d'extraire les hashes de mots de passe des comptes utilisateurs Windows contenus dans le dump mémoire CC_Niveau2.dmp.

```
python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.hivelist
```

```
(venv) nk@pop-os:~/Documents/ouils/volatility: $ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.hivelist
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Offset FileFullPath File output
0x8b20c008 Disabled
0x8b21c008 \REGISTRY\MACHINE\SYSTEM Disabled
0x8b23c008 \REGISTRY\MACHINE\HARDWARE Disabled
0x8ee66008 \Device\HarddiskVolume1\Boot\BCD Disabled
0x8ee66740 \SystemRoot\System32\Config\SOFTWARE Disabled
0x90ac9d00 \SystemRoot\System32\Config\DEFAULT Disabled
0x9670e9d0 ???\C:\Users\John Doe\ntuser.dat Disabled
0x9670fd00 ???\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
0x9aad6148 \SystemRoot\System32\Config\SAM Disabled
0x9ab25008 \SystemRoot\System32\Config\SECURITY Disabled
0x9aba79d0 ???\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT Disabled
0x9abb1720 ???\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT Disabled
```

Cette commande extrait la liste des "hives" (ruche) de la base de registre Windows contenue dans le dump mémoire.

**python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.printkey -
-offset 0x8b21c008 key
"ConsoleSet001\Control\ComputerName\ComputerName":**

```
(venv) [root@kali:~/Documents/ouils/volatility]# python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.printkey --offset 0x8b21c008 --key "ConsoleSet001\Control\ComputerName\ComputerName"
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Last Write Time Hive Offset Type Key Name Data Volatile
-
0x8b21c008 Key \REGISTRY\MACHINE\SYSTEM\ConsoleSet001\Control\ComputerName\ComputerName - - -
```

Cette commande permet de lire une clé spécifique du registre Windows, située dans une hive mémoire à une adresse donnée (offset).

Pour ce faire, vous devrez adapter les solutions Volatility 2 présentes dans le fichier PDF fourni afin qu'elles fonctionnent avec Volatility 3. Expliquez chaque étape.

Dans un premier temps, il faut déterminer le type de système d'exploitation :

```
(venv) ntkrmpmp-c:\Documents\outils\volatility3\volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.info
volatility 3 Framework 2.26.2
Progress: 100.00% PDB scanning finished
variable Value
Kernel Base 0x82801000
DTB 0x185000
Symbols jar:file:/home/nk/Documents/outils/volatility3/volatility3/symbols/windows.zip!windows/ntkrmp.pdb/5B308B4ED6464159B87117C711E7340C-2.json.xz
Is64Bit False
IsPAE True
layer_name 0 WindowsIntelPAE
memory_layer 1 Filelayer
kdDebuggerDataBlock 0x82929be8
NTBuildLab 7600.16385.x86fre.win7_rtm.09071
CSVersion 0
kdVersionBlock 0x82929bc0
Major/Minor 15.7600
MachineType 332
keNumberProcessors 1
SystemTime 2013-01-12 16:59:18+00:00
ntSystemRoot C:\Windows
ntProductType NtProductWinNt
ntMajorVersion 6
ntMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine 332
PE TimeDateStamp Mon Jul 13 23:15:19 2009
```

Ensuite, on affiche les processus

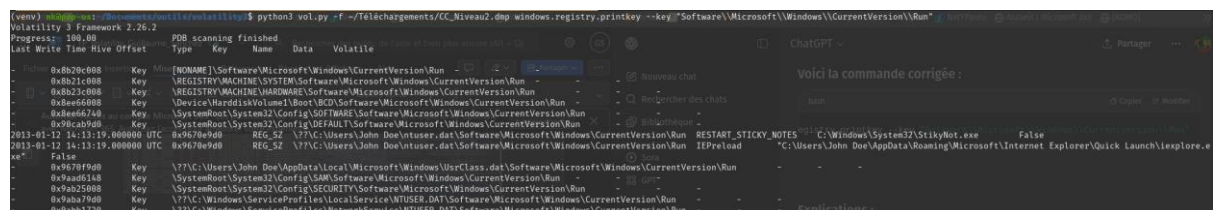
[illegible]

Dans toutes ces informations, on peut voir deux lignes suspectes, un programme “iexplore.exe” utilise un cmd :

```
2772 2548 iexplore.exe 0x070b030 2 74 1 False 2013-01-12 16:40:34.000000 UTC N/A \Device\HarddiskVolume1\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
1616 2772 cmd.exe 0x07099030 2 101 1 False 2013-01-12 16:55:49.000000 UTC N/A \Device\HarddiskVolume1\Windows\System32\cmd.exe cmd.exe C:\Windows\system32\cmd.exe
```

On affiche le chemin absolu du programme à l’aide de la commande :

python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.printkey -key "Software\\Microsoft\\Windows\\CurrentVersion\\Run" :



```
(venv) nh@pnp-ws:~/Documents/ouils/volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.registry.printkey --key "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
Volatility 3 Framework 2.26.2
Progress: 100.00
Last Write Time Hive Offset Type Key Name Data Volatile
-----
0x8b20c008 Key [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] -
0x8b21c008 Key [HKEY_MACHINE\SYSTEM\Software\Microsoft\Windows\CurrentVersion\Run] -
0x8b22c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b23c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b24c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b25c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b26c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b27c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b28c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b29c008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x8b2ac008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
2013-01-12 14:13:19.000000 UTC 0x9670e9d0 REG_SZ \??C:\Users\John Doe\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Run IEPreload "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" False
2013-01-12 14:13:19.000000 UTC 0x9670e9d0 REG_SZ \??C:\Users\John Doe\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Run IEPreload "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" False
0x9578f900 Key [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] -
0x95a0d148 Key [HKEY_MACHINE\SYSTEM\Software\Microsoft\Windows\CurrentVersion\Run] -
0x95a25008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x95a37008 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
0x95a4b128 Key [HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] -
```

On remarque que l’utilisateur utilisant le programme est un certain John Doe:

```
2013-01-12 14:13:19.000000 UTC 0x9670e9d0 REG_SZ \??C:\Users\John Doe\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Run IEPreload "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" False
```

Niveau 4 :

Dans un premier temps, je passe la commande **python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.netscan** et je lui rajoute un “grep 2772” qui correspond au pid de “iexplorer.exe”.

```
(venv) nh@pnp-ws:~/Documents/ouils/volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.netscan | grep 2772
0x1ddeb4f8 100.0TCPv4 127.0.0.1DB scan49178fin127.0.0.1 12080 ESTABLISHED 2772 iexplore.exe -
```

Si on repasse la commande sans le grep, nous avons beaucoup d’ip en 192.168 qui apparaissent.

On réalise la commande **python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp -o fichier_dump/ windows.memmap --dump --pid 2772** et je place le résultat dans fichier_dump/pid.2772.dmp

En utilisant un lecteur d'hexadécimal comme xxd sur linux, on peut retrouver les ligne suivant qui semble intéressantes:

```
076E89C0  1D 00 01 00 05 00 00 08 43 00 3A 00 5C 00 57 00 .....C.:.\W.
076E89D0  69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 73 00 i.n.d.o.w.s.\s.
076E89E0  79 00 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 y.s.t.e.m.3.2.\.
076E89F0  63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 00 00 c.m.d...e.x.e...
076E8A00  2D 00 20 00 72 00 6D 00 64 00 69 00 72 00 20 00 -. .r.m.d.i.r. .
076E8A10  20 00 2F 00 73 00 20 00 54 00 45 00 4D 00 50 00 ./s. .T.E.M.P.
076E8A20  32 00 33 00 00 00 2E 00 31 00 36 00 38 00 2E 00 2.3....1.6.8...
076E8A30  30 00 2E 00 32 00 32 00 20 00 33 00 33 00 38 00 0...2.2. .3.3.8.
076E8A40  39 00 20 00 79 00 6F 00 75 00 72 00 63 00 73 00 9. .y.o.u.r.c.s.
076E8A50  65 00 63 00 72 00 65 00 74 00 2E 00 63 00 6F 00 e.c.r.e.t...c.o.
076E8A60  2E 00 74 00 76 00 20 00 34 00 34 00 33 00 20 00 ..t.v. .4.4.3. .
076E8A70  00 00 6D 00 70 00 5C 00 54 00 45 00 4D 00 50 00 ..m.p.\.T.E.M.P.
076E8A80  32 00 33 00 5C 00 74 00 63 00 70 00 72 00 65 00 2.3.\.t.c.p.r.e.
076E8A90  6C 00 61 00 79 00 2E 00 65 00 78 00 65 00 22 00 l.a.y...e.x.e."
```

Visiblement l'ip serait 192.168.0.22 3389 yourcsecret.co.tv 443