Memory Forensics using Volatility Workbench

November 8, 2020 By Raj Chandel

Volatility Workbench is a GUI version of one of the most popular tool Volatility for analyzing the artifacts from a memory dump. It is available free of cost, open-source, and runs on the Windows Operating system. You can download it from **Here**.

You can refer to the previous article **Memory Forensics: Using Volatility** from here,

Table of Contents

- Printkey
- Hashdump
- Lsadump
- Shellbags
- Getservicesids
- Getservicesids
- Dumpregistry
- Mbrparser
- Mftparser

Features of Volatility Workbench

1. A forensic investigator does not have to worry about remembering the parameters of the command line.
2. It has made it easier to store dump information to a file on disk.
3. There is a drop-down list that contains the commands and its brief description.
4. It records the time stamp of the commands that were previously executed.

Download the tool and run it. Now choose the dump file that you have previously created and select the profile of the image that was created which could be used in place of imageinfo command. Now click on Refresh Process List and you can run all the commands.

Hunting rootkits and malicious code

It tends to run a scan on the memory dump and looks around for the presence of a rootkit or a malicious code that would not be easily seen in the system but could be running in the background.

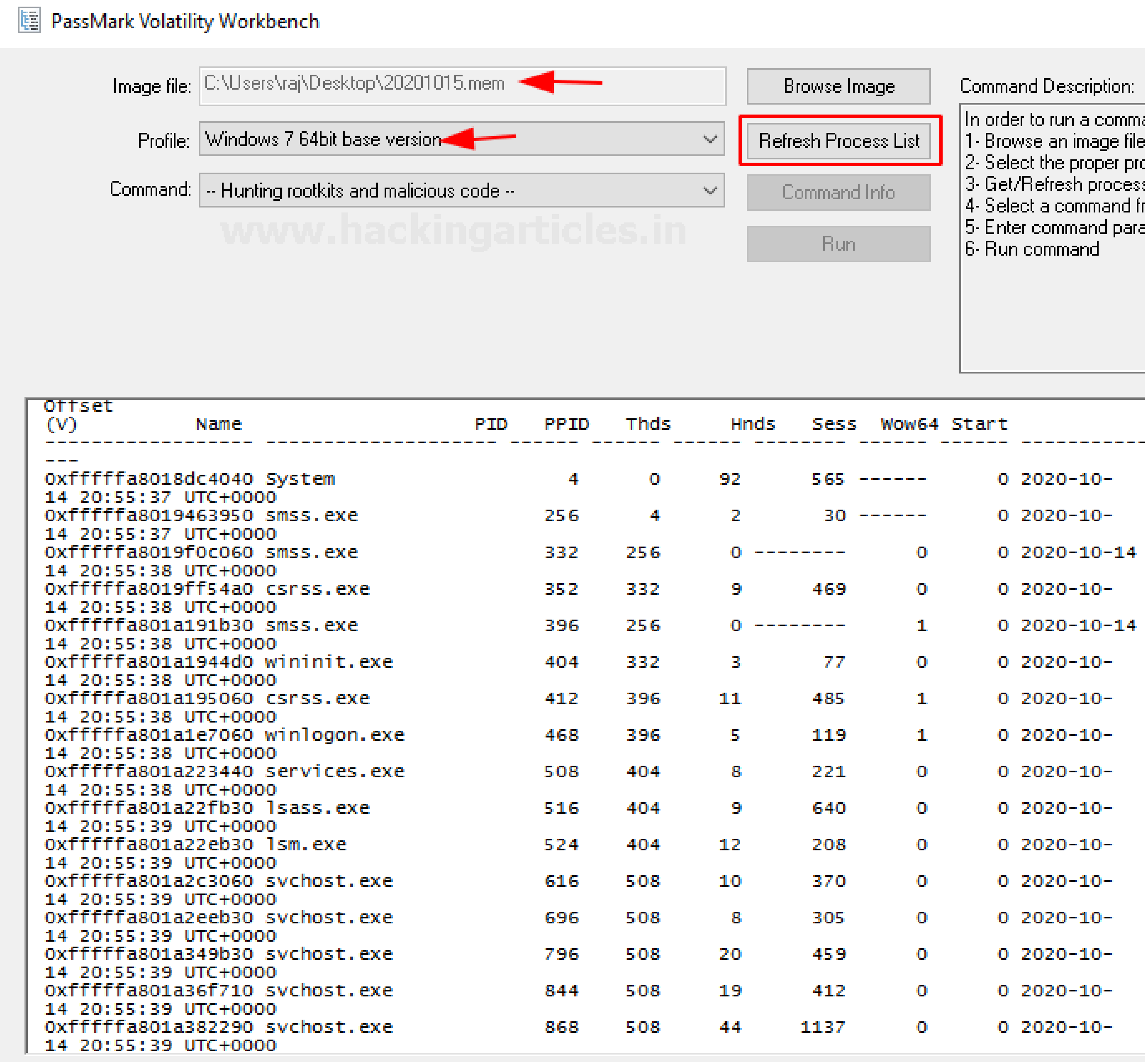


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: -- Hunting rootkits and malicious code --

Command Description:

In order to run a comma
1- Browse an image file
2- Select the proper pro
3- Get/Refresh process
4- Select a command fr
5- Enter command para
6- Run command

```
Offset
(V)          Name                    PID   PPID    Thds      Hnds    Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ -----------
---
0xfffffa8018dc4040 System                    4      0     92      565 ------      0 2020-10-
14 20:55:37 UTC+0000
0xfffffa8019463950 smss.exe                256      4      2       30 ------      0 2020-10-
14 20:55:37 UTC+0000
0xfffffa8019f0c060 smss.exe                332    256      0 --------      0      0 2020-10-14
14 20:55:38 UTC+0000
0xfffffa8019ff54a0 csrss.exe               352    332      9      469      0      0 2020-10-
14 20:55:38 UTC+0000
0xfffffa801a191b30 smss.exe                396    256      0 --------      1      0 2020-10-14
14 20:55:38 UTC+0000
0xfffffa801a1944d0 wininit.exe             404    332      3       77      0      0 2020-10-
14 20:55:38 UTC+0000
0xfffffa801a195060 csrss.exe               412    396     11      485      1      0 2020-10-
14 20:55:38 UTC+0000
0xfffffa801a1e7060 winlogon.exe            468    396      5      119      1      0 2020-10-
14 20:55:38 UTC+0000
0xfffffa801a223440 services.exe            508    404      8      221      0      0 2020-10-
14 20:55:38 UTC+0000
0xfffffa801a22fb30 lsass.exe               516    404      9      640      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a22eb30 lsm.exe                 524    404     12      208      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a2c3060 svchost.exe             616    508     10      370      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a2eeb30 svchost.exe             696    508      8      305      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a349b30 svchost.exe             796    508     20      459      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a36f710 svchost.exe             844    508     19      412      0      0 2020-10-
14 20:55:39 UTC+0000
0xfffffa801a382290 svchost.exe             868    508     44     1137      0      0 2020-10-
14 20:55:39 UTC+0000
```

Malfind

It is a command which helps in finding a hidden code or a code that has been injected into the user’s memory. It doesn’t generally detect the presence of a DLL in a process but instead locates them.

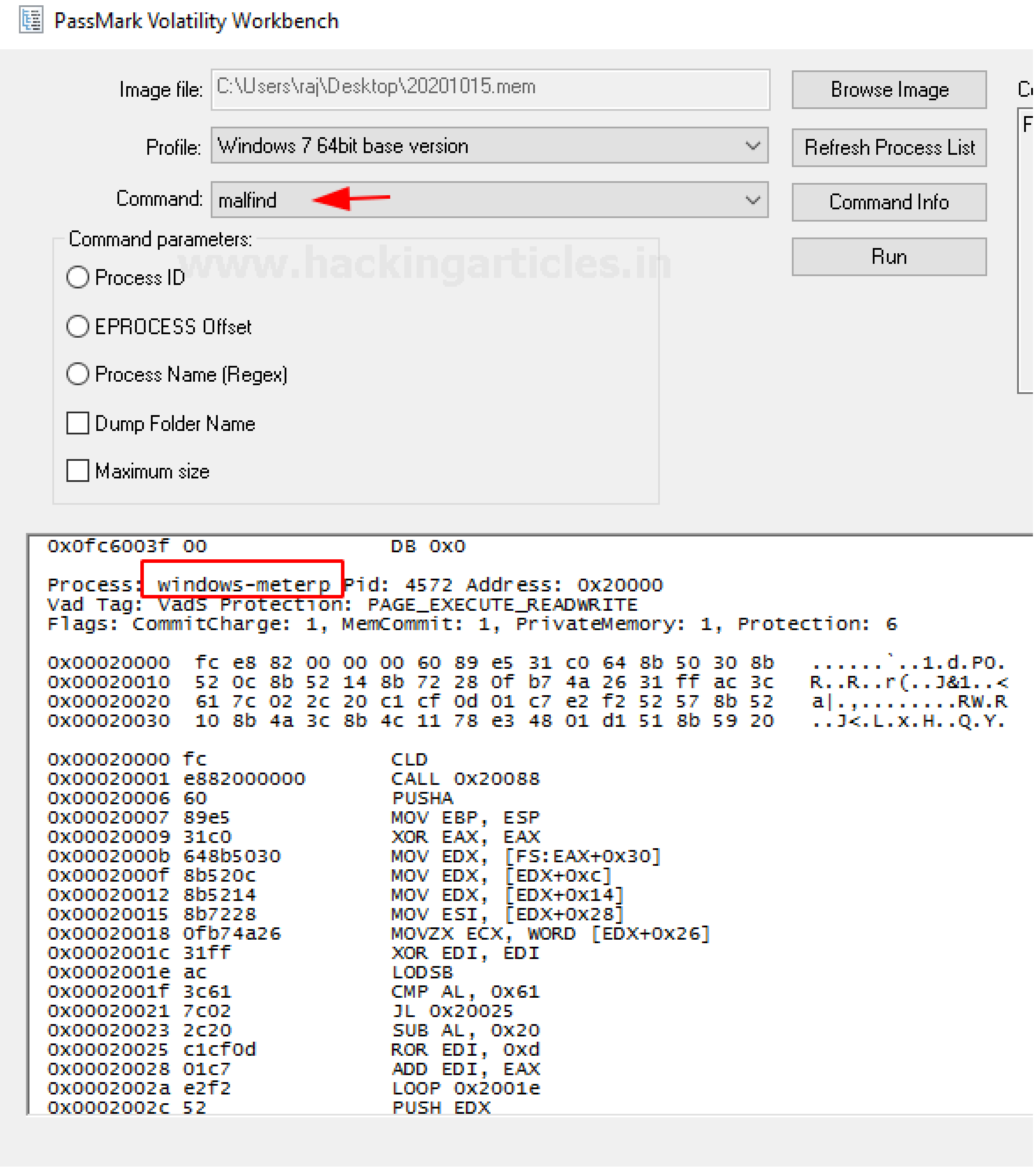


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: malfind

```
0x0fc6003f 00                  DB 0x0

Process: windows-meterp Pid: 4572 Address: 0x20000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00020000  fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30 8b   ......`..1.d.P0.
0x00020010  52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c   R..R..r(..J&1..<
0x00020020  61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52   a|.,........RW.R
0x00020030  10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1 51 8b 59 20   ..J<.L.x.H..Q.Y.

0x00020000 fc                  CLD
0x00020001 e882000000          CALL 0x20088
0x00020006 60                  PUSHA
0x00020007 89e5                MOV EBP, ESP
0x00020009 31c0                XOR EAX, EAX
0x0002000b 648b5030            MOV EDX, [FS:EAX+0x30]
0x0002000f 8b520c              MOV EDX, [EDX+0xc]
0x00020012 8b5214              MOV EDX, [EDX+0x14]
0x00020015 8b7228              MOV ESI, [EDX+0x28]
0x00020018 0fb74a26            MOVZX ECX, WORD [EDX+0x26]
0x0002001c 31ff                XOR EDI, EDI
0x0002001e ac                  LODSB
0x0002001f 3c61                CMP AL, 0x61
0x00020021 7c02                JL 0x20025
0x00020023 2c20                SUB AL, 0x20
0x00020025 c1cf0d              ROR EDI, 0xd
0x00020028 01c7                ADD EDI, EAX
0x0002002a e2f2                LOOP 0x2001e
0x0002002c 52                  PUSH EDX
```

psxview

This command usually helps in discovering any hidden processes in the plugin present in the memory dump.

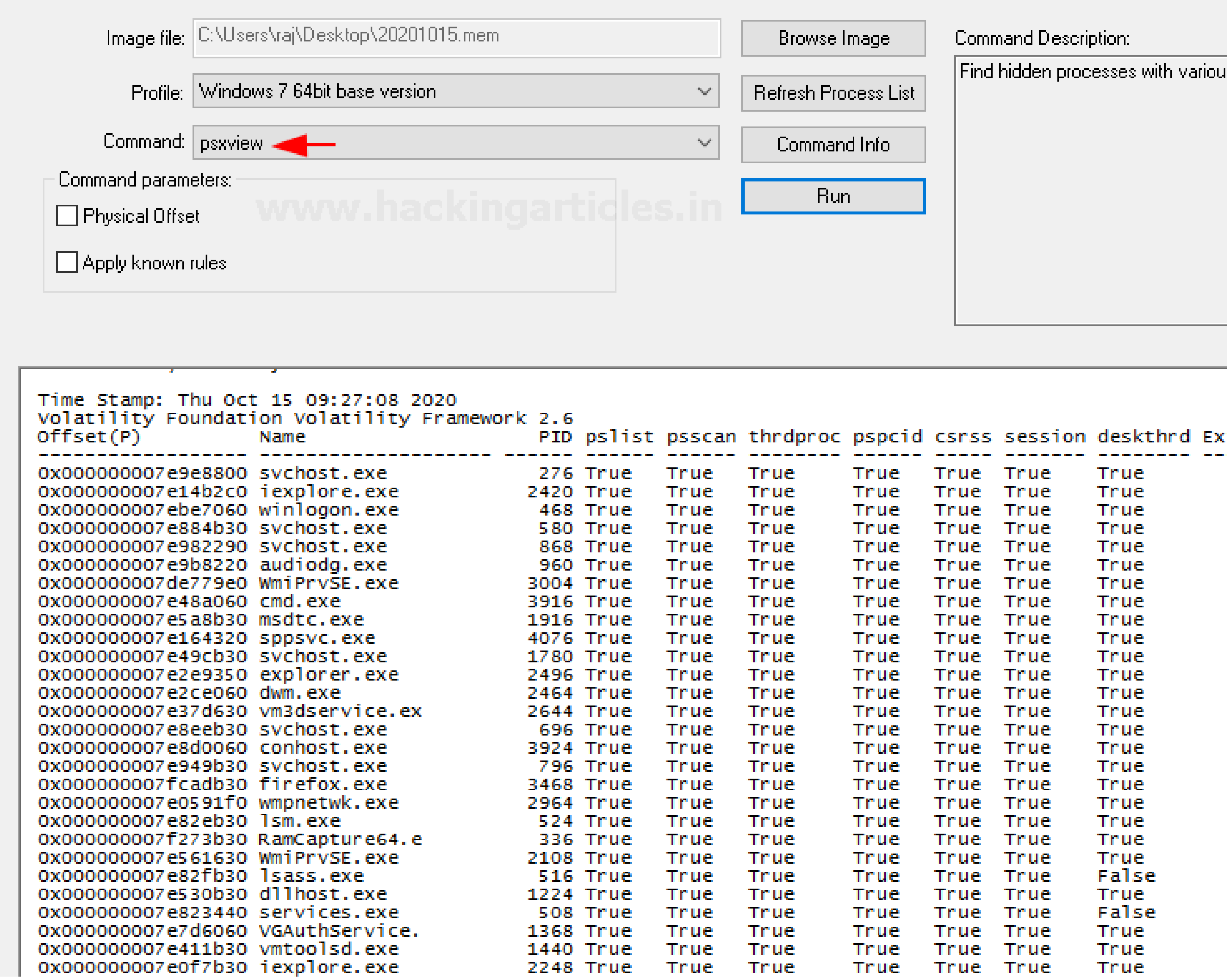


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: psxview

Command parameters:

□ Physical Offset

□ Apply known rules

Command Description:

Find hidden processes with variou

```
Time Stamp: Thu Oct 15 09:27:08 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd Ex
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --
0x000000007e9e8800 svchost.exe             276 True   True   True     True   True  True    True
0x000000007e14b2c0 iexplore.exe           2420 True   True   True     True   True  True    True
0x000000007ebe7060 winlogon.exe            468 True   True   True     True   True  True    True
0x000000007e884b30 svchost.exe             580 True   True   True     True   True  True    True
0x000000007e982290 svchost.exe             868 True   True   True     True   True  True    True
0x000000007e9b8220 audiodg.exe             960 True   True   True     True   True  True    True
0x000000007de779e0 WmiPrvSE.exe           3004 True   True   True     True   True  True    True
0x000000007e48a060 cmd.exe                3916 True   True   True     True   True  True    True
0x000000007e5a8b30 msdtc.exe              1916 True   True   True     True   True  True    True
0x000000007e164320 sppsvc.exe             4076 True   True   True     True   True  True    True
0x000000007e49cb30 svchost.exe            1780 True   True   True     True   True  True    True
0x000000007e2e9350 explorer.exe           2496 True   True   True     True   True  True    True
0x000000007e2ce060 dwm.exe                2464 True   True   True     True   True  True    True
0x000000007e37d630 vm3dservice.ex         2644 True   True   True     True   True  True    True
0x000000007e8eeb30 svchost.exe             696 True   True   True     True   True  True    True
0x000000007e8d0060 conhost.exe            3924 True   True   True     True   True  True    True
0x000000007e949b30 svchost.exe             796 True   True   True     True   True  True    True
0x000000007fcadb30 firefox.exe            3468 True   True   True     True   True  True    True
0x000000007e0591f0 wmpnetwk.exe           2964 True   True   True     True   True  True    True
0x000000007e82eb30 lsm.exe                 524 True   True   True     True   True  True    True
0x000000007f273b30 RamCapture64.e          336 True   True   True     True   True  True    True
0x000000007e561630 WmiPrvSE.exe           2108 True   True   True     True   True  True    True
0x000000007e82fb30 lsass.exe               516 True   True   True     True   True  True    False
0x000000007e530b30 dllhost.exe            1224 True   True   True     True   True  True    True
0x000000007e823440 services.exe            508 True   True   True     True   True  True    False
0x000000007e7d6060 VGAuthService.         1368 True   True   True     True   True  True    True
0x000000007e411b30 vmtoolsd.exe           1440 True   True   True     True   True  True    True
0x000000007e0f7b30 iexplore.exe           2248 True   True   True     True   True  True    True
```

Timers

It displays the timer of the kernel and all the associated timers present in the memory dump of the system.

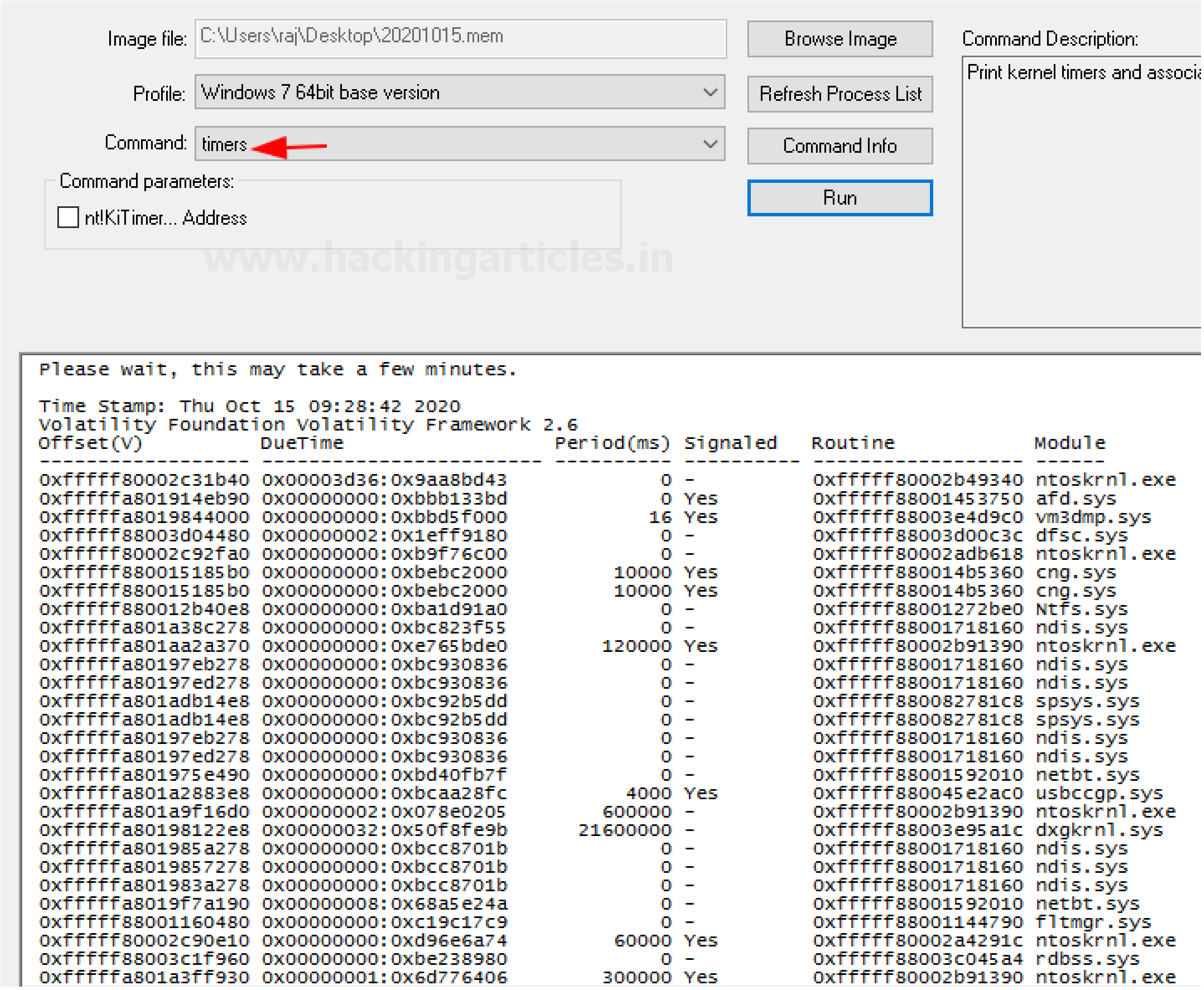


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: timers

Command parameters:

□ nt!KiTimer... Address

Command Description:

Print kernel timers and associa

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:28:42 2020
Volatility Foundation Volatility Framework 2.6
Offset(V)          DueTime                  Period(ms) Signaled   Routine            Module
------------------ ------------------------ ----------- ---------- ------------------ ------
0xfffff80002c31b40 0x00003d36:0x9aa8bd43              0 -          0xfffff80002b49340 ntoskrnl.exe
0xfffffa801914eb90 0x00000000:0xbbb133bd              0 Yes        0xfffff88001453750 afd.sys
0xfffffa8019844000 0x00000000:0xbbd5f000             16 Yes        0xfffff88003e4d9c0 vm3dmp.sys
0xfffff88003d04480 0x00000002:0x1eff9180              0 -          0xfffff88003d00c3c dfsc.sys
0xfffff80002c92fa0 0x00000000:0xb9f76c00              0 -          0xfffff80002adb618 ntoskrnl.exe
0xfffff880015185b0 0x00000000:0xbebc2000          10000 Yes        0xfffff880014b5360 cng.sys
0xfffff880015185b0 0x00000000:0xbebc2000          10000 Yes        0xfffff880014b5360 cng.sys
0xfffff880012b40e8 0x00000000:0xba1d91a0              0 -          0xfffff88001272be0 Ntfs.sys
0xfffffa801a38c278 0x00000000:0xbc823f55              0 -          0xfffff88001718160 ndis.sys
0xfffffa801aa2a370 0x00000000:0xe765bde0         120000 Yes        0xfffff80002b91390 ntoskrnl.exe
0xfffffa80197eb278 0x00000000:0xbc930836              0 -          0xfffff88001718160 ndis.sys
0xfffffa80197ed278 0x00000000:0xbc930836              0 -          0xfffff88001718160 ndis.sys
0xfffffa801adb14e8 0x00000000:0xbc92b5dd              0 -          0xfffff880082781c8 spsys.sys
0xfffffa801adb14e8 0x00000000:0xbc92b5dd              0 -          0xfffff880082781c8 spsys.sys
0xfffffa80197eb278 0x00000000:0xbc930836              0 -          0xfffff88001718160 ndis.sys
0xfffffa80197ed278 0x00000000:0xbc930836              0 -          0xfffff88001718160 ndis.sys
0xfffffa801975e490 0x00000000:0xbd40fb7f              0 -          0xfffff88001592010 netbt.sys
0xfffffa801a2883e8 0x00000000:0xbcaa28fc           4000 Yes        0xfffff880045e2ac0 usbccgp.sys
0xfffffa801a9f16d0 0x00000002:0x078e0205         600000 -          0xfffff80002b91390 ntoskrnl.exe
0xfffffa80198122e8 0x00000032:0x50f8fe9b       21600000 -          0xfffff88003e95a1c dxgkrnl.sys
0xfffffa801985a278 0x00000000:0xbcc8701b              0 -          0xfffff88001718160 ndis.sys
0xfffffa8019857278 0x00000000:0xbcc8701b              0 -          0xfffff88001718160 ndis.sys
0xfffffa801983a278 0x00000000:0xbcc8701b              0 -          0xfffff88001718160 ndis.sys
0xfffffa8019f7a190 0x00000008:0x68a5e24a              0 -          0xfffff88001592010 netbt.sys
0xfffff88001160480 0x00000000:0xc19c17c9              0 -          0xfffff88001144790 fltmgr.sys
0xfffff80002c90e10 0x00000000:0xd96e6a74          60000 Yes        0xfffff80002a4291c ntoskrnl.exe
0xfffff88003c1f960 0x00000000:0xbe238980              0 -          0xfffff88003c045a4 rdbss.sys
0xfffffa801a3ff930 0x00000001:0x6d776406         300000 Yes        0xfffff80002b91390 ntoskrnl.exe
```

Getsids

This command can be used to view the Security Identifiers that are associated with a particular process. With the help of this command, you can identify if any malicious process has taken any privilege escalation.

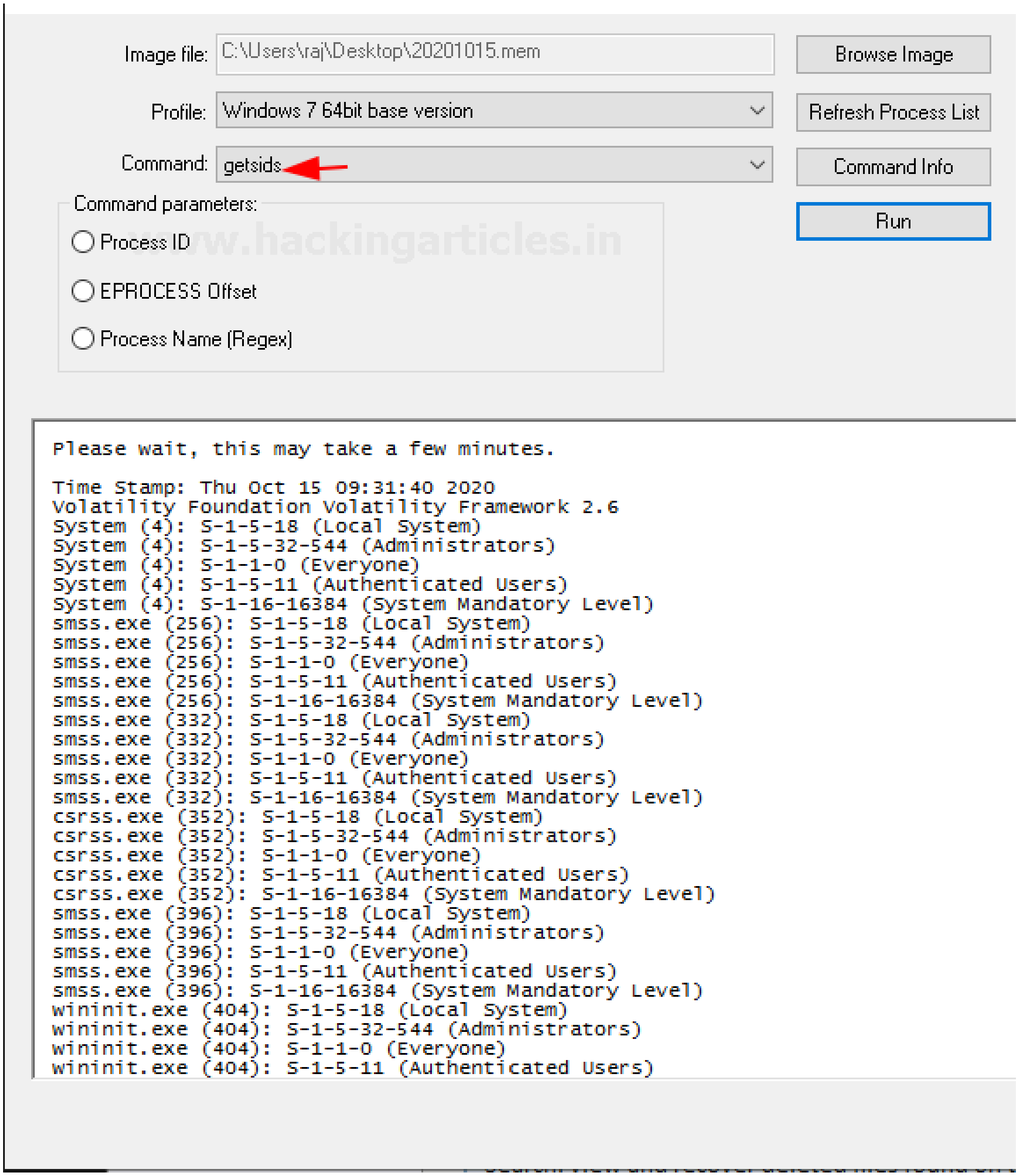


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: getsids

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:31:40 2020
Volatility Foundation Volatility Framework 2.6
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
System (4): S-1-16-16384 (System Mandatory Level)
smss.exe (256): S-1-5-18 (Local System)
smss.exe (256): S-1-5-32-544 (Administrators)
smss.exe (256): S-1-1-0 (Everyone)
smss.exe (256): S-1-5-11 (Authenticated Users)
smss.exe (256): S-1-16-16384 (System Mandatory Level)
smss.exe (332): S-1-5-18 (Local System)
smss.exe (332): S-1-5-32-544 (Administrators)
smss.exe (332): S-1-1-0 (Everyone)
smss.exe (332): S-1-5-11 (Authenticated Users)
smss.exe (332): S-1-16-16384 (System Mandatory Level)
csrss.exe (352): S-1-5-18 (Local System)
csrss.exe (352): S-1-5-32-544 (Administrators)
csrss.exe (352): S-1-1-0 (Everyone)
csrss.exe (352): S-1-5-11 (Authenticated Users)
csrss.exe (352): S-1-16-16384 (System Mandatory Level)
smss.exe (396): S-1-5-18 (Local System)
smss.exe (396): S-1-5-32-544 (Administrators)
smss.exe (396): S-1-1-0 (Everyone)
smss.exe (396): S-1-5-11 (Authenticated Users)
smss.exe (396): S-1-16-16384 (System Mandatory Level)
wininit.exe (404): S-1-5-18 (Local System)
wininit.exe (404): S-1-5-32-544 (Administrators)
wininit.exe (404): S-1-1-0 (Everyone)
wininit.exe (404): S-1-5-11 (Authenticated Users)
```

Cmdscan

This plugin helps in searching the memory dump for the command the user must have used the cmd.exe application. This command is highly used if the attacker's command activity is to be traced.

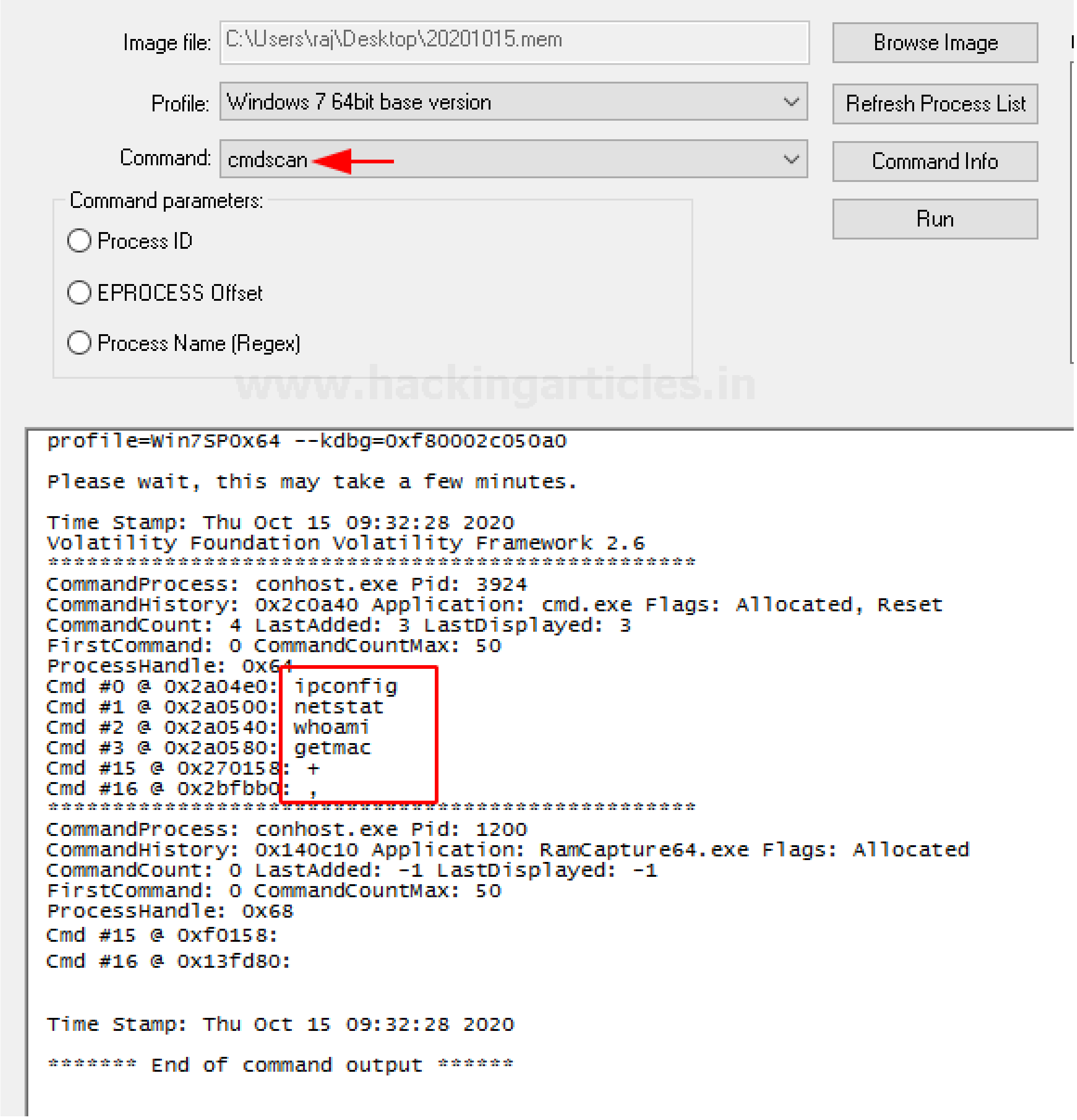


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: cmdscan

Command parameters:

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

```
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:32:28 2020
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3924
CommandHistory: 0x2c0a40 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 4 LastAdded: 3 LastDisplayed: 3
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 @ 0x2a04e0: ipconfig
Cmd #1 @ 0x2a0500: netstat
Cmd #2 @ 0x2a0540: whoami
Cmd #3 @ 0x2a0580: getmac
Cmd #15 @ 0x270158: +
Cmd #16 @ 0x2bfbb0: ,
**************************************************
CommandProcess: conhost.exe Pid: 1200
CommandHistory: 0x140c10 Application: RamCapture64.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x68
Cmd #15 @ 0xf0158:
Cmd #16 @ 0x13fd80:


Time Stamp: Thu Oct 15 09:32:28 2020

******* End of command output ******
```

Consoles

This command is similar to cmdscan and helps to find if the attacker had typed anything in cmd or had executed anything via the backdoor.

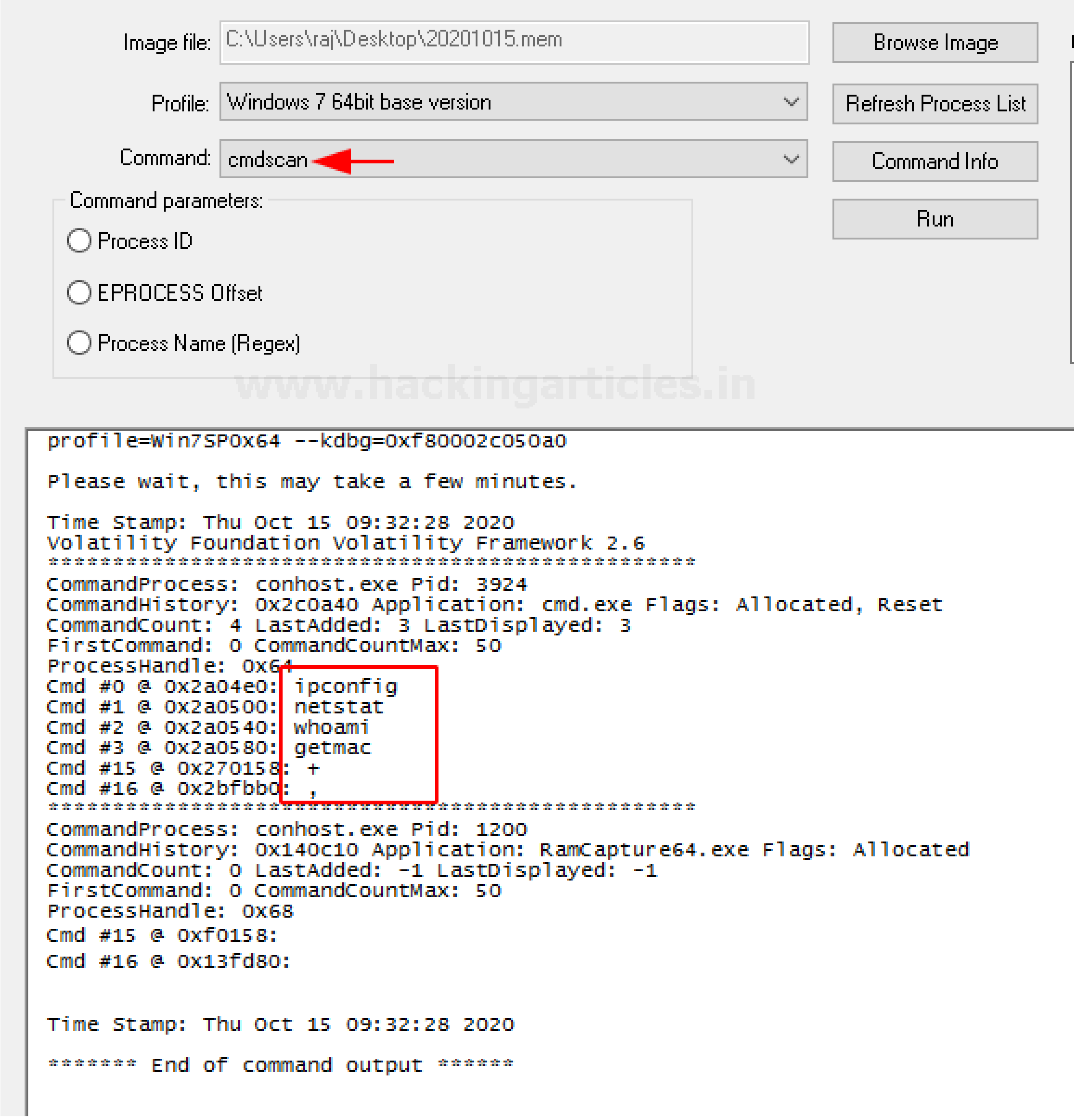


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: cmdscan

```
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:32:28 2020
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3924
CommandHistory: 0x2c0a40 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 4 LastAdded: 3 LastDisplayed: 3
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 @ 0x2a04e0: ipconfig
Cmd #1 @ 0x2a0500: netstat
Cmd #2 @ 0x2a0540: whoami
Cmd #3 @ 0x2a0580: getmac
Cmd #15 @ 0x270158: +
Cmd #16 @ 0x2bfbb0: ,
**************************************************
CommandProcess: conhost.exe Pid: 1200
CommandHistory: 0x140c10 Application: RamCapture64.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x68
Cmd #15 @ 0xf0158:
Cmd #16 @ 0x13fd80:


Time Stamp: Thu Oct 15 09:32:28 2020

******* End of command output ******
```

Privs

This command displays the privileges assigned to the processes that are enabled or not enabled by default.

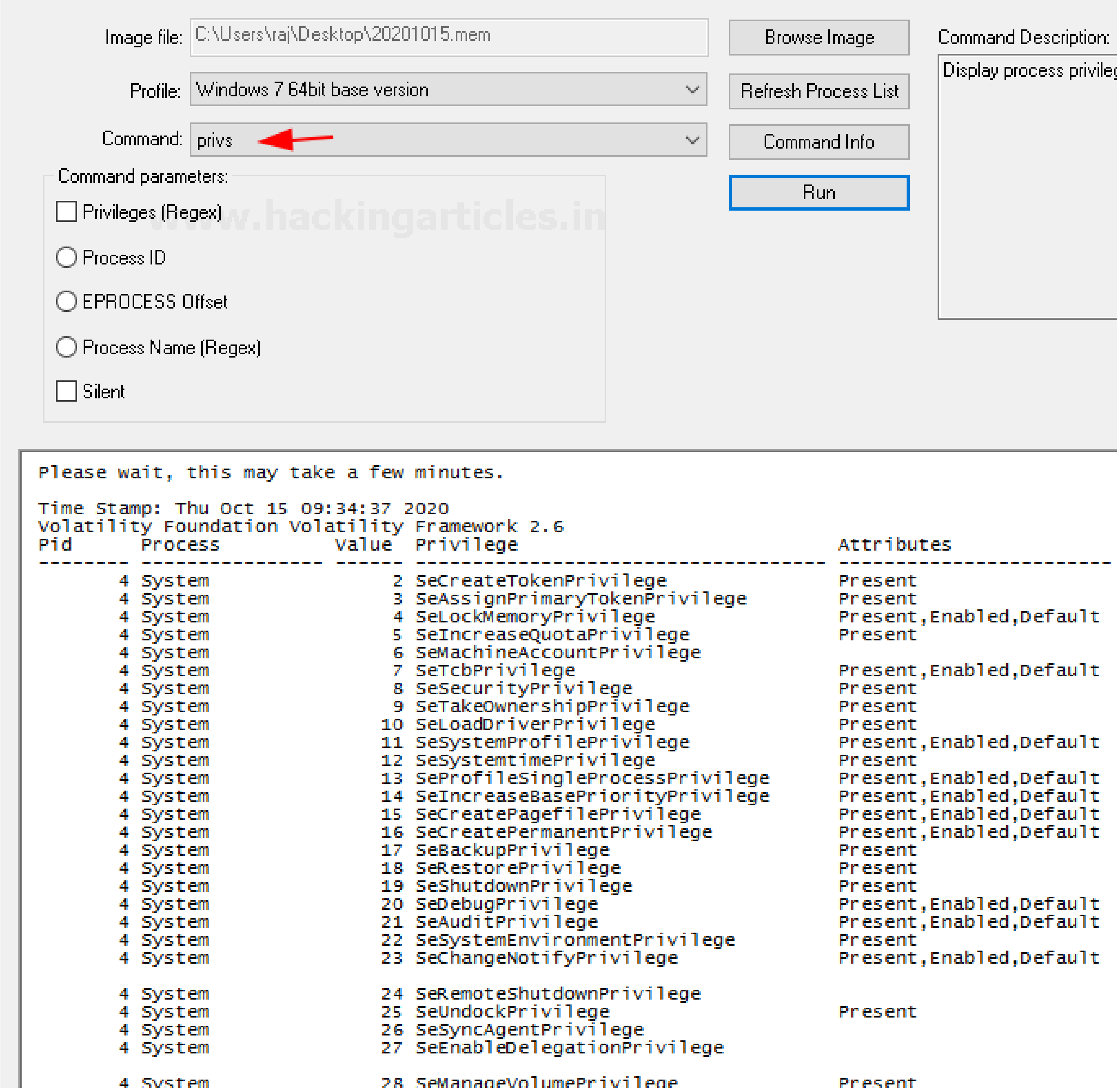


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: privs

Command parameters:

□ Privileges (Regex)

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

□ Silent

Command Description:

Display process privileg

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:34:37 2020
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                            Attributes
-------- ---------------- ------ ------------------------------------ ------------------------
       4 System                2 SeCreateTokenPrivilege               Present
       4 System                3 SeAssignPrimaryTokenPrivilege        Present
       4 System                4 SeLockMemoryPrivilege                Present,Enabled,Default
       4 System                5 SeIncreaseQuotaPrivilege             Present
       4 System                6 SeMachineAccountPrivilege
       4 System                7 SeTcbPrivilege                       Present,Enabled,Default
       4 System                8 SeSecurityPrivilege                  Present
       4 System                9 SeTakeOwnershipPrivilege             Present
       4 System               10 SeLoadDriverPrivilege                Present
       4 System               11 SeSystemProfilePrivilege             Present,Enabled,Default
       4 System               12 SeSystemtimePrivilege                Present
       4 System               13 SeProfileSingleProcessPrivilege      Present,Enabled,Default
       4 System               14 SeIncreaseBasePriorityPrivilege      Present,Enabled,Default
       4 System               15 SeCreatePagefilePrivilege            Present,Enabled,Default
       4 System               16 SeCreatePermanentPrivilege           Present,Enabled,Default
       4 System               17 SeBackupPrivilege                    Present
       4 System               18 SeRestorePrivilege                   Present
       4 System               19 SeShutdownPrivilege                  Present
       4 System               20 SeDebugPrivilege                     Present,Enabled,Default
       4 System               21 SeAuditPrivilege                     Present,Enabled,Default
       4 System               22 SeSystemEnvironmentPrivilege         Present
       4 System               23 SeChangeNotifyPrivilege              Present,Enabled,Default

       4 System               24 SeRemoteShutdownPrivilege
       4 System               25 SeUndockPrivilege                    Present
       4 System               26 SeSyncAgentPrivilege
       4 System               27 SeEnableDelegationPrivilege

       4 System               28 SeManageVolumePrivilege              Present
```

Envars

This command displays all the variables in the process, its environment along with its current directory.

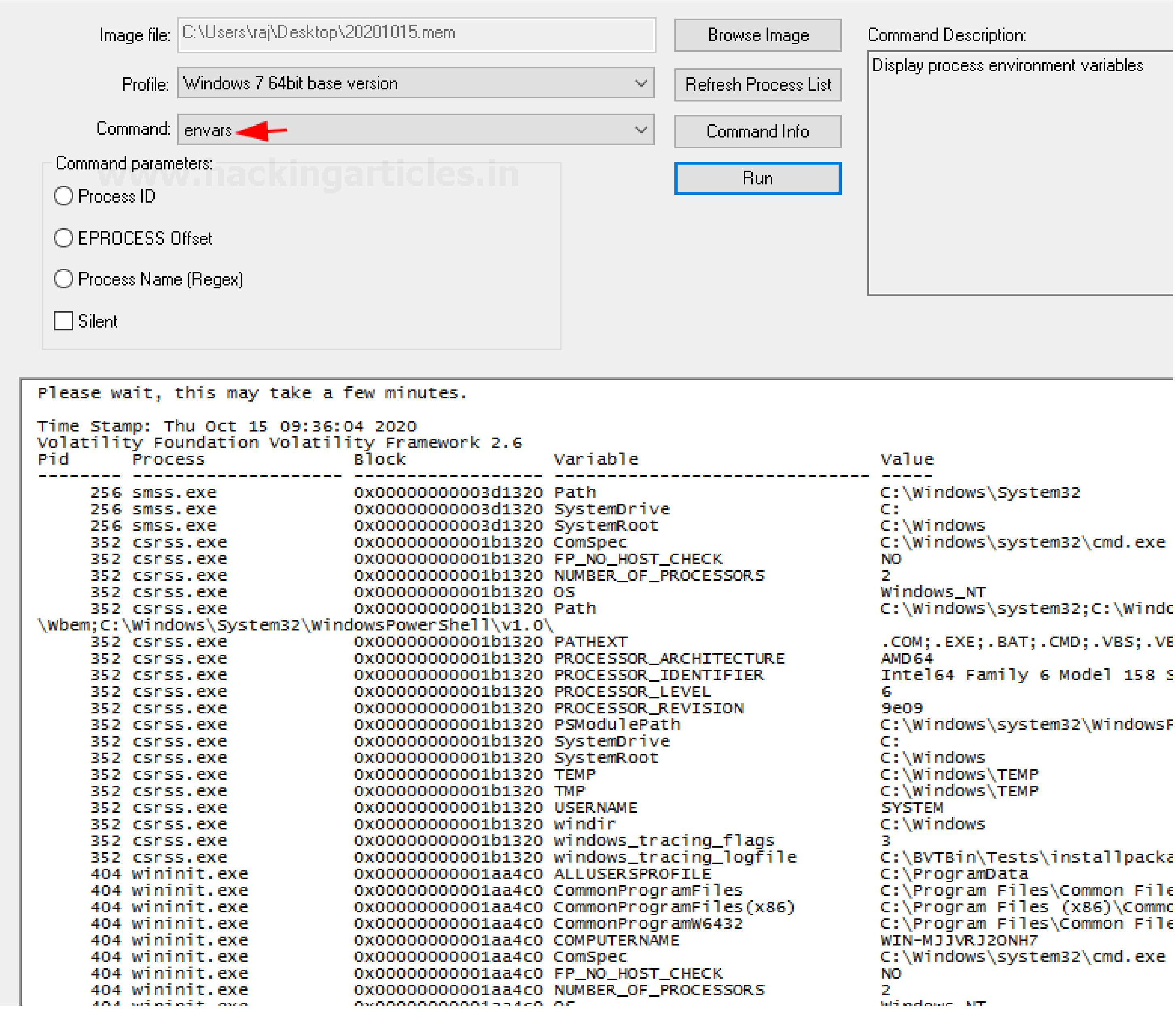


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: envars

Command parameters:

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

□ Silent

Command Description:

Display process environment variables

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:36:04 2020
Volatility Foundation Volatility Framework 2.6
Pid      Process              Block              Variable                       Value
-------- -------------------- ------------------ ------------------------------ -----
     256 smss.exe             0x00000000003d1320 Path                           C:\Windows\System32
     256 smss.exe             0x00000000003d1320 SystemDrive                    C:
     256 smss.exe             0x00000000003d1320 SystemRoot                     C:\Windows
     352 csrss.exe            0x00000000001b1320 ComSpec                        C:\Windows\system32\cmd.exe
     352 csrss.exe            0x00000000001b1320 FP_NO_HOST_CHECK               NO
     352 csrss.exe            0x00000000001b1320 NUMBER_OF_PROCESSORS           2
     352 csrss.exe            0x00000000001b1320 OS                             Windows_NT
     352 csrss.exe            0x00000000001b1320 Path                           C:\Windows\system32;C:\Windc
\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
     352 csrss.exe            0x00000000001b1320 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VE
     352 csrss.exe            0x00000000001b1320 PROCESSOR_ARCHITECTURE         AMD64
     352 csrss.exe            0x00000000001b1320 PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 158 S
     352 csrss.exe            0x00000000001b1320 PROCESSOR_LEVEL                6
     352 csrss.exe            0x00000000001b1320 PROCESSOR_REVISION             9e09
     352 csrss.exe            0x00000000001b1320 PSModulePath                   C:\Windows\system32\WindowsF
     352 csrss.exe            0x00000000001b1320 SystemDrive                    C:
     352 csrss.exe            0x00000000001b1320 SystemRoot                     C:\Windows
     352 csrss.exe            0x00000000001b1320 TEMP                           C:\Windows\TEMP
     352 csrss.exe            0x00000000001b1320 TMP                            C:\Windows\TEMP
     352 csrss.exe            0x00000000001b1320 USERNAME                       SYSTEM
     352 csrss.exe            0x00000000001b1320 windir                         C:\Windows
     352 csrss.exe            0x00000000001b1320 windows_tracing_flags          3
     352 csrss.exe            0x00000000001b1320 windows_tracing_logfile        C:\BVTBin\Tests\installpacka
     404 wininit.exe          0x00000000001aa4c0 ALLUSERSPROFILE                C:\ProgramData
     404 wininit.exe          0x00000000001aa4c0 CommonProgramFiles             C:\Program Files\Common File
     404 wininit.exe          0x00000000001aa4c0 CommonProgramFiles(x86)        C:\Program Files (x86)\Commc
     404 wininit.exe          0x00000000001aa4c0 CommonProgramW6432             C:\Program Files\Common File
     404 wininit.exe          0x00000000001aa4c0 COMPUTERNAME                   WIN-MJJVRJ2ONH7
     404 wininit.exe          0x00000000001aa4c0 ComSpec                        C:\Windows\system32\cmd.exe
     404 wininit.exe          0x00000000001aa4c0 FP_NO_HOST_CHECK               NO
     404 wininit.exe          0x00000000001aa4c0 NUMBER_OF_PROCESSORS           2
     404 wininit.exe          0x00000000001aa4c0 OS                             Windows_NT
```

Verinfo

This command displays the version information that is present in the PE files. It helps identify any binaries and also correlates with other files.

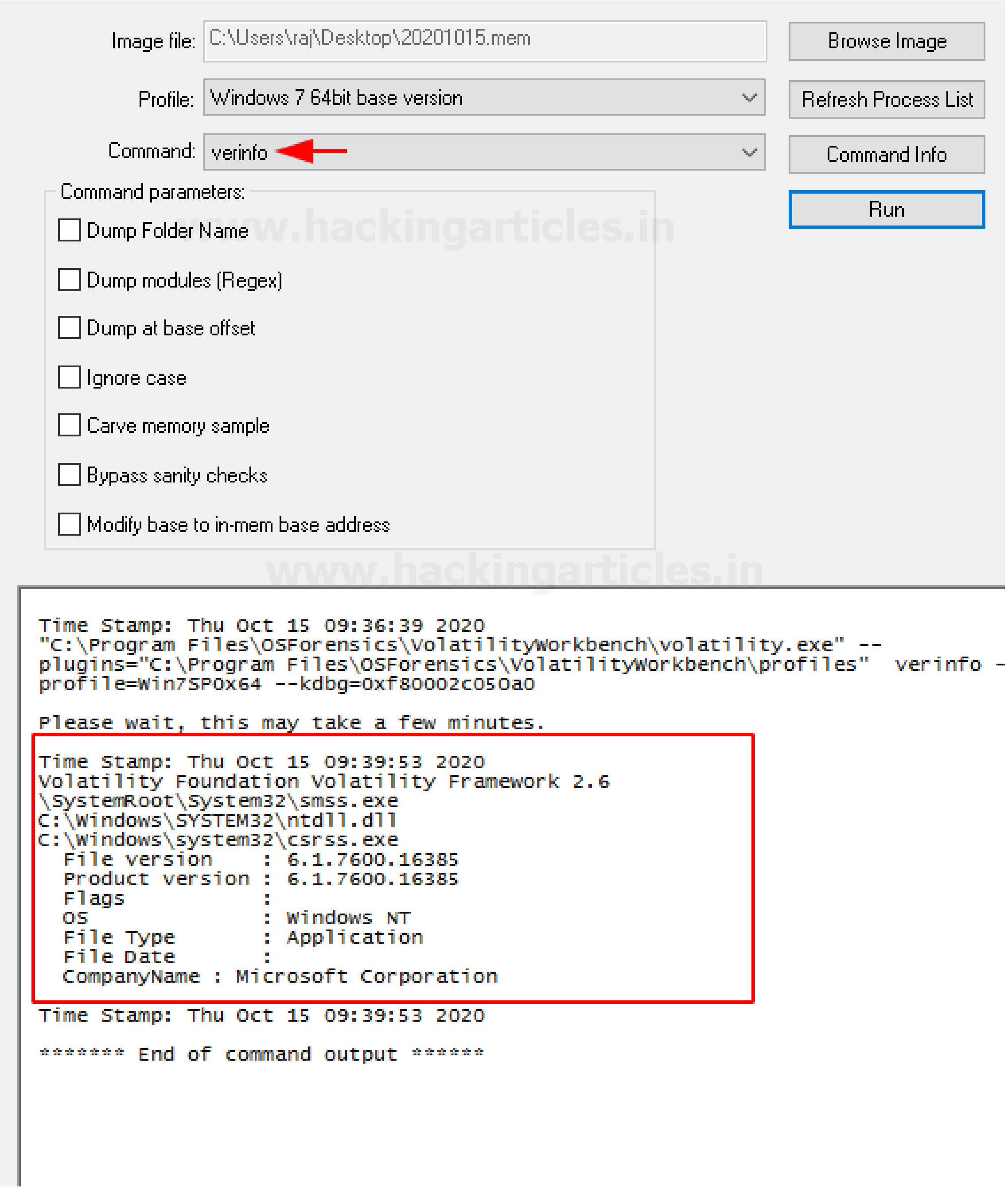


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: verinfo

Command parameters:

- ☐ Dump Folder Name
- ☐ Dump modules (Regex)
- ☐ Dump at base offset
- ☐ Ignore case
- ☐ Carve memory sample
- ☐ Bypass sanity checks
- ☐ Modify base to in-mem base address

```
Time Stamp: Thu Oct 15 09:36:39 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  verinfo -
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:39:53 2020
Volatility Foundation Volatility Framework 2.6
\SystemRoot\System32\smss.exe
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\system32\csrss.exe
  File version    : 6.1.7600.16385
  Product version : 6.1.7600.16385
  Flags           :
  OS              : Windows NT
  File Type       : Application
  File Date       :
  CompanyName : Microsoft Corporation
Time Stamp: Thu Oct 15 09:39:53 2020

******* End of command output ******
```

Memmap

This command shows the exact pages that are present on the page of a specific process. It also shows the virtual address of the page and the size of its page.

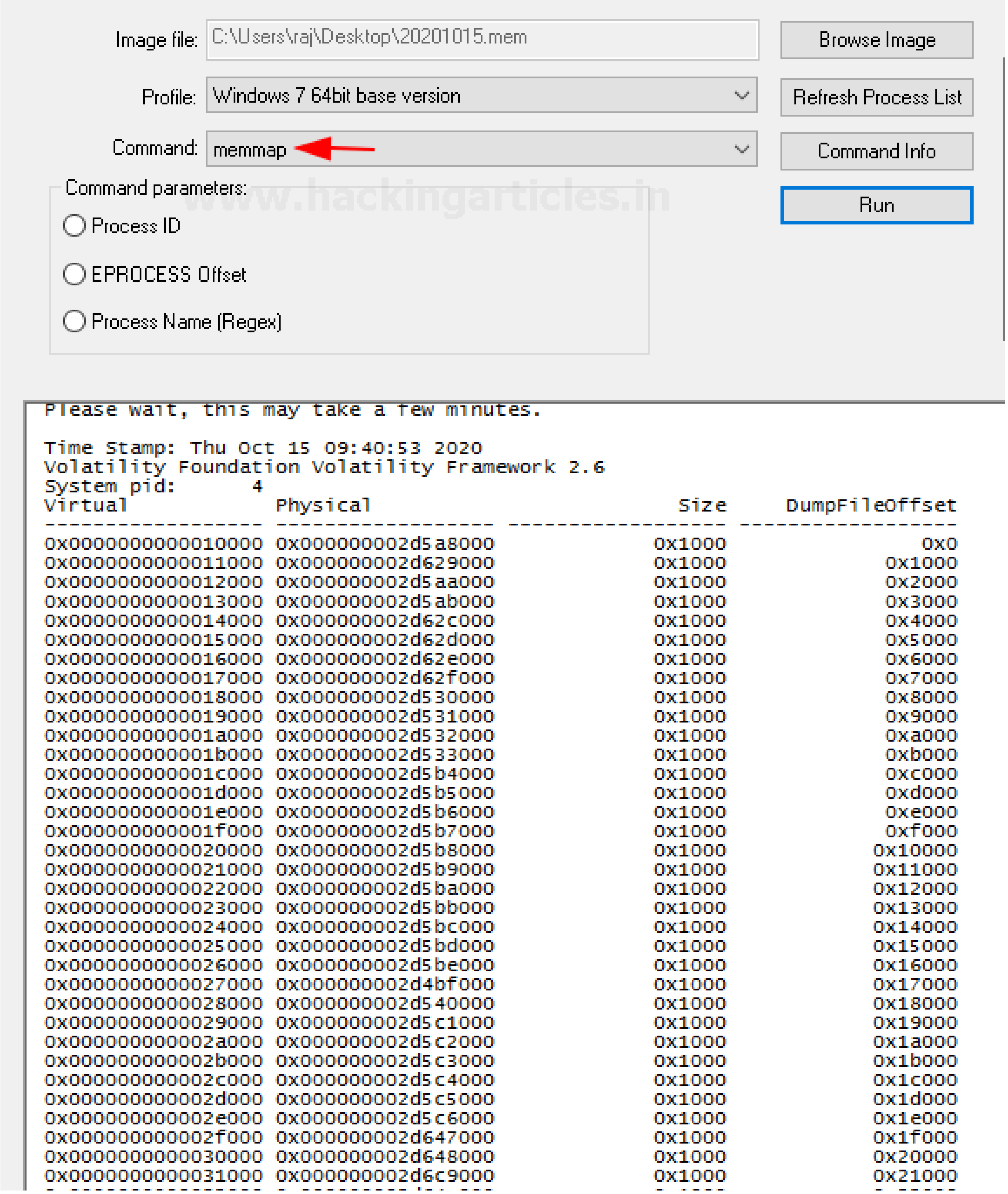


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: memmap

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:40:53 2020
Volatility Foundation Volatility Framework 2.6
System pid:      4
Virtual            Physical                         Size     DumpFileOffset
------------------ ------------------ ------------------ ------------------
0x0000000000010000 0x000000002d5a8000             0x1000                0x0
0x0000000000011000 0x000000002d629000             0x1000             0x1000
0x0000000000012000 0x000000002d5aa000             0x1000             0x2000
0x0000000000013000 0x000000002d5ab000             0x1000             0x3000
0x0000000000014000 0x000000002d62c000             0x1000             0x4000
0x0000000000015000 0x000000002d62d000             0x1000             0x5000
0x0000000000016000 0x000000002d62e000             0x1000             0x6000
0x0000000000017000 0x000000002d62f000             0x1000             0x7000
0x0000000000018000 0x000000002d530000             0x1000             0x8000
0x0000000000019000 0x000000002d531000             0x1000             0x9000
0x000000000001a000 0x000000002d532000             0x1000             0xa000
0x000000000001b000 0x000000002d533000             0x1000             0xb000
0x000000000001c000 0x000000002d5b4000             0x1000             0xc000
0x000000000001d000 0x000000002d5b5000             0x1000             0xd000
0x000000000001e000 0x000000002d5b6000             0x1000             0xe000
0x000000000001f000 0x000000002d5b7000             0x1000             0xf000
0x0000000000020000 0x000000002d5b8000             0x1000            0x10000
0x0000000000021000 0x000000002d5b9000             0x1000            0x11000
0x0000000000022000 0x000000002d5ba000             0x1000            0x12000
0x0000000000023000 0x000000002d5bb000             0x1000            0x13000
0x0000000000024000 0x000000002d5bc000             0x1000            0x14000
0x0000000000025000 0x000000002d5bd000             0x1000            0x15000
0x0000000000026000 0x000000002d5be000             0x1000            0x16000
0x0000000000027000 0x000000002d4bf000             0x1000            0x17000
0x0000000000028000 0x000000002d540000             0x1000            0x18000
0x0000000000029000 0x000000002d5c1000             0x1000            0x19000
0x000000000002a000 0x000000002d5c2000             0x1000            0x1a000
0x000000000002b000 0x000000002d5c3000             0x1000            0x1b000
0x000000000002c000 0x000000002d5c4000             0x1000            0x1c000
0x000000000002d000 0x000000002d5c5000             0x1000            0x1d000
0x000000000002e000 0x000000002d5c6000             0x1000            0x1e000
0x000000000002f000 0x000000002d647000             0x1000            0x1f000
0x0000000000030000 0x000000002d648000             0x1000            0x20000
0x0000000000031000 0x000000002d6c9000             0x1000            0x21000
```

Vadinfo

This command usually displays information about a particular process’s VAD nodes. It displays the VAD Flags control flags, VAD tags.

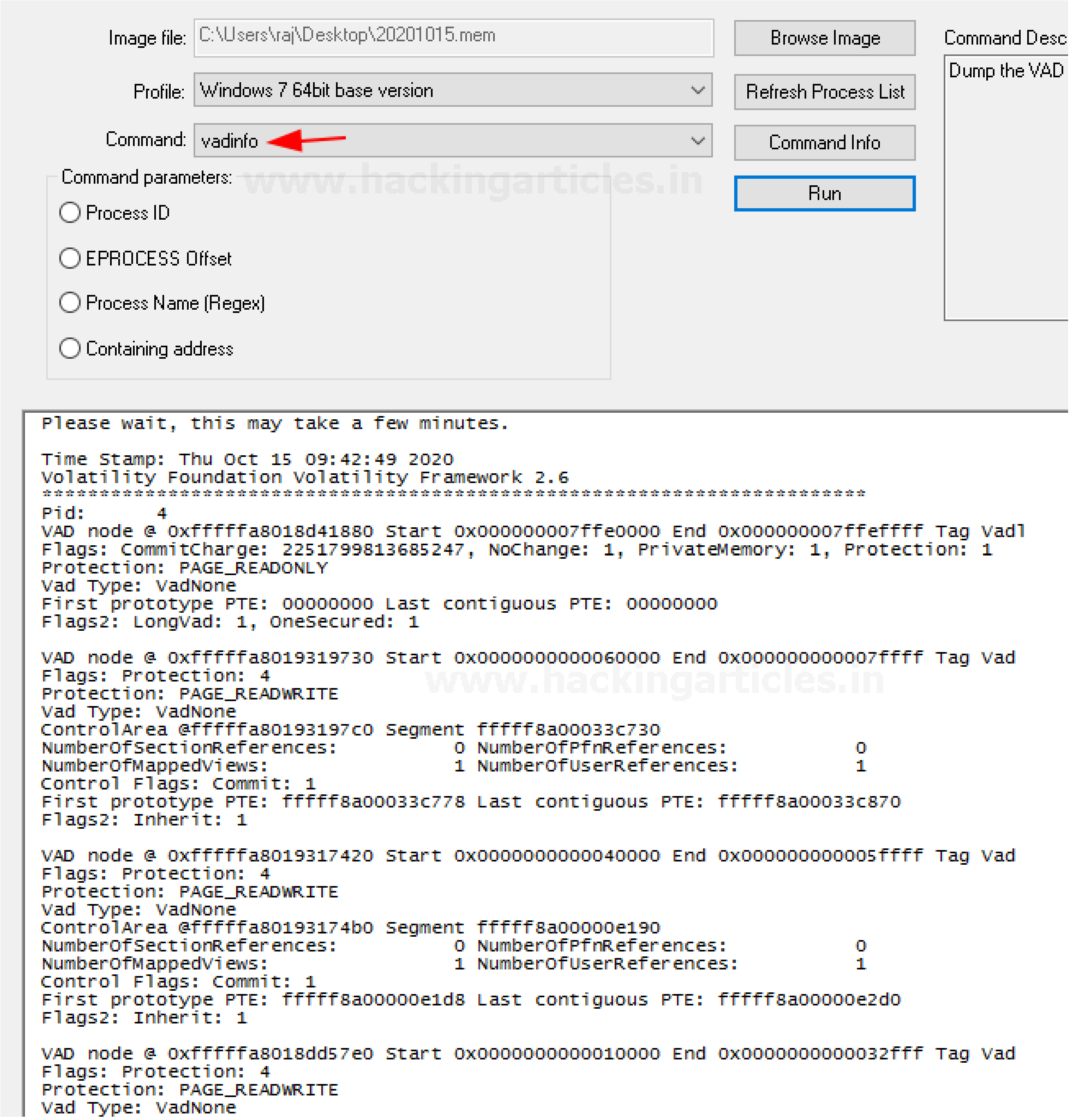


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: vadinfo

Command parameters:

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

○ Containing address

Command Desc

Dump the VAD

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:42:49 2020
Volatility Foundation Volatility Framework 2.6
************************************************************************
Pid:      4
VAD node @ 0xfffffa8018d41880 Start 0x000000007ffe0000 End 0x000000007ffeffff Tag Vadl
Flags: CommitCharge: 2251799813685247, NoChange: 1, PrivateMemory: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone
First prototype PTE: 00000000 Last contiguous PTE: 00000000
Flags2: LongVad: 1, OneSecured: 1

VAD node @ 0xfffffa8019319730 Start 0x0000000000060000 End 0x000000000007ffff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
ControlArea @fffffa80193197c0 Segment fffff8a00033c730
NumberOfSectionReferences:          0 NumberOfPfnReferences:           0
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: Commit: 1
First prototype PTE: fffff8a00033c778 Last contiguous PTE: fffff8a00033c870
Flags2: Inherit: 1

VAD node @ 0xfffffa8019317420 Start 0x0000000000040000 End 0x000000000005ffff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
ControlArea @fffffa80193174b0 Segment fffff8a00000e190
NumberOfSectionReferences:          0 NumberOfPfnReferences:           0
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: Commit: 1
First prototype PTE: fffff8a00000e1d8 Last contiguous PTE: fffff8a00000e2d0
Flags2: Inherit: 1

VAD node @ 0xfffffa8018dd57e0 Start 0x0000000000010000 End 0x0000000000032fff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
```

Vadwalk

It is a command that is used to display all the VAD nodes in a tabular form.

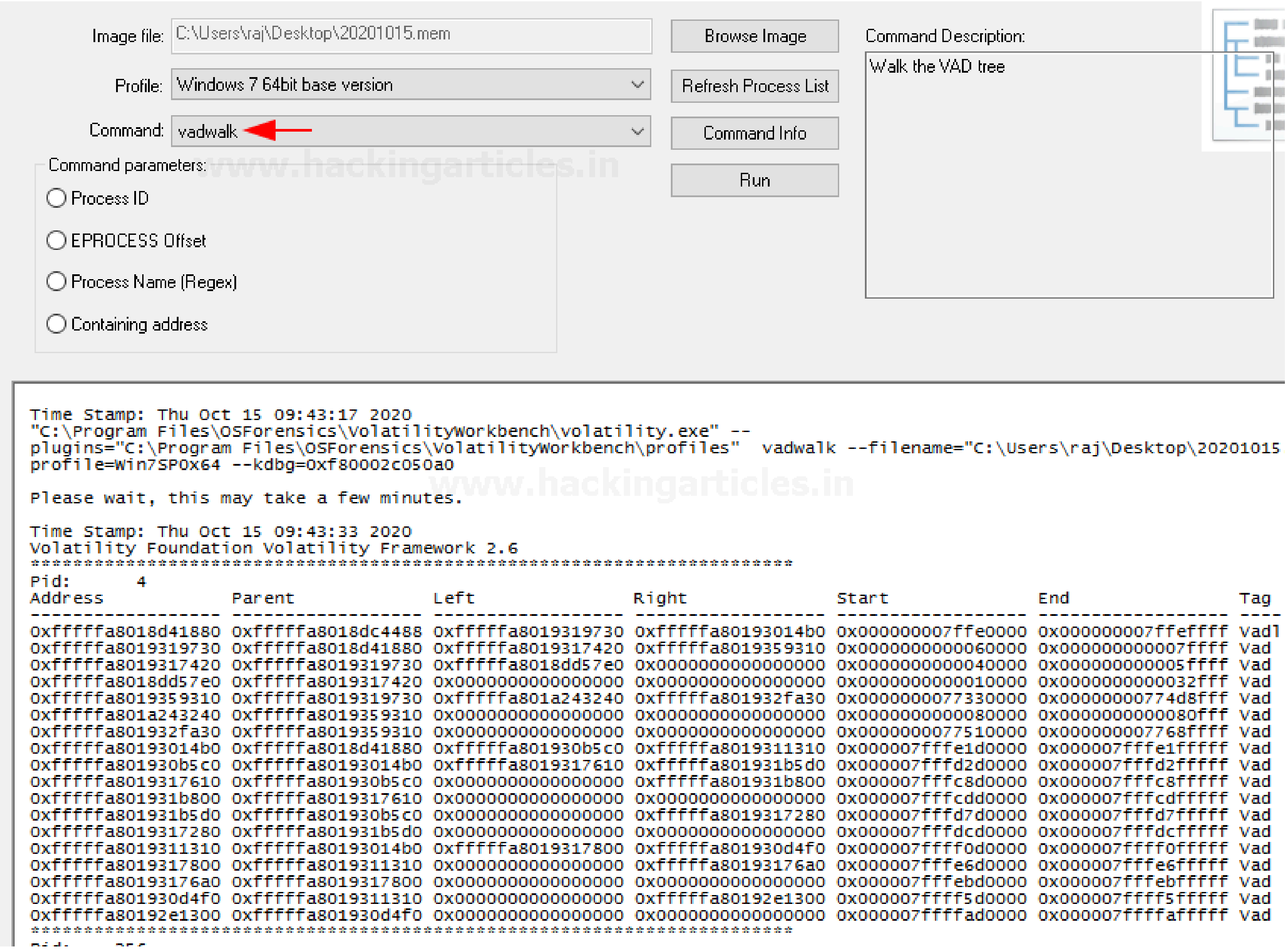


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: vadwalk

Command Description: Walk the VAD tree

```
Time Stamp: Thu Oct 15 09:43:17 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  vadwalk --filename="C:\Users\raj\Desktop\20201015
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:43:33 2020
Volatility Foundation Volatility Framework 2.6
************************************************************************
Pid:      4
Address            Parent             Left               Right              Start              End                Tag
------------------ ------------------ ------------------ ------------------ ------------------ ------------------ ----
0xfffffa8018d41880 0xfffffa8018dc4488 0xfffffa8019319730 0xfffffa80193014b0 0x000000007ffe0000 0x000000007ffeffff Vadl
0xfffffa8019319730 0xfffffa8018d41880 0xfffffa8019317420 0xfffffa8019359310 0x0000000000060000 0x000000000007ffff Vad
0xfffffa8019317420 0xfffffa8019319730 0xfffffa8018dd57e0 0x0000000000000000 0x0000000000040000 0x000000000005ffff Vad
0xfffffa8018dd57e0 0xfffffa8019317420 0x0000000000000000 0x0000000000000000 0x0000000000010000 0x000000000032ffff Vad
0xfffffa8019359310 0xfffffa8019319730 0xfffffa801a243240 0xfffffa801932fa30 0x0000000077330000 0x00000000774d8fff Vad
0xfffffa801a243240 0xfffffa8019359310 0x0000000000000000 0x0000000000000000 0x0000000000080000 0x0000000000080fff Vad
0xfffffa801932fa30 0xfffffa8019359310 0x0000000000000000 0x0000000000000000 0x0000000077510000 0x000000007768ffff Vad
0xfffffa80193014b0 0xfffffa8018d41880 0xfffffa801930b5c0 0xfffffa8019311310 0x000007fffe1d0000 0x000007fffe1fffff Vad
0xfffffa801930b5c0 0xfffffa80193014b0 0xfffffa8019317610 0xfffffa801931b5d0 0x000007fffd2d0000 0x000007fffd2fffff Vad
0xfffffa8019317610 0xfffffa801930b5c0 0x0000000000000000 0xfffffa801931b800 0x000007fffc8d0000 0x000007fffc8fffff Vad
0xfffffa801931b800 0xfffffa8019317610 0x0000000000000000 0x0000000000000000 0x000007fffcdd0000 0x000007fffcdfffff Vad
0xfffffa801931b5d0 0xfffffa801930b5c0 0x0000000000000000 0xfffffa8019317280 0x000007fffd7d0000 0x000007fffd7fffff Vad
0xfffffa8019317280 0xfffffa801931b5d0 0x0000000000000000 0x0000000000000000 0x000007fffdcd0000 0x000007fffdcfffff Vad
0xfffffa8019311310 0xfffffa80193014b0 0xfffffa8019317800 0xfffffa801930d4f0 0x000007ffff0d0000 0x000007ffff0fffff Vad
0xfffffa8019317800 0xfffffa8019311310 0x0000000000000000 0xfffffa80193176a0 0x000007fffe6d0000 0x000007fffe6fffff Vad
0xfffffa80193176a0 0xfffffa8019317800 0x0000000000000000 0x0000000000000000 0x000007fffebd0000 0x000007fffebfffff Vad
0xfffffa801930d4f0 0xfffffa8019311310 0x0000000000000000 0xfffffa80192e1300 0x000007ffff5d0000 0x000007ffff5fffff Vad
0xfffffa80192e1300 0xfffffa801930d4f0 0x0000000000000000 0x0000000000000000 0x000007ffffad0000 0x000007ffffafffff Vad
************************************************************************
Pid:      256
```

Vadtree

This process displays the VAD nodes in a tree form.

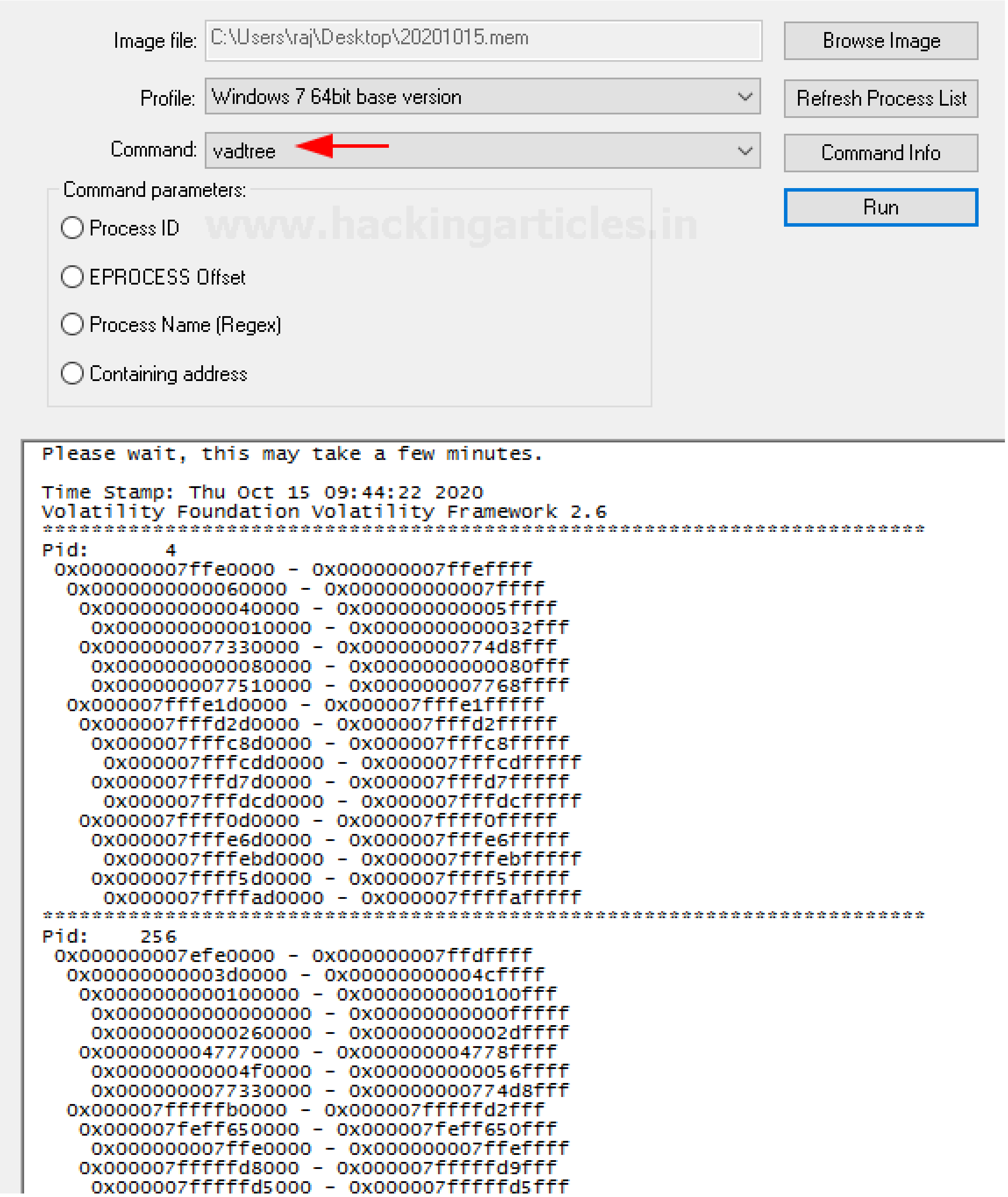


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: vadtree

Command parameters:

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

○ Containing address

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:44:22 2020
Volatility Foundation Volatility Framework 2.6
************************************************************************
Pid:      4
 0x000000007ffe0000 - 0x000000007ffeffff
  0x0000000000060000 - 0x000000000007ffff
   0x0000000000040000 - 0x000000000005ffff
    0x0000000000010000 - 0x0000000000032fff
   0x0000000077330000 - 0x00000000774d8fff
    0x0000000000080000 - 0x0000000000080fff
    0x0000000077510000 - 0x000000007768ffff
  0x000007fffe1d0000 - 0x000007fffe1fffff
   0x000007fffd2d0000 - 0x000007fffd2fffff
    0x000007fffc8d0000 - 0x000007fffc8fffff
     0x000007fffcdd0000 - 0x000007fffcdfffff
    0x000007fffd7d0000 - 0x000007fffd7fffff
     0x000007fffdcd0000 - 0x000007fffdcfffff
   0x000007ffff0d0000 - 0x000007ffff0fffff
    0x000007fffe6d0000 - 0x000007fffe6fffff
     0x000007fffebd0000 - 0x000007fffebfffff
    0x000007ffff5d0000 - 0x000007ffff5fffff
     0x000007ffffad0000 - 0x000007ffffafffff
************************************************************************
Pid:    256
 0x000000007efe0000 - 0x000000007ffdffff
  0x00000000003d0000 - 0x00000000004cffff
   0x0000000000100000 - 0x0000000000100fff
    0x0000000000000000 - 0x00000000000fffff
    0x0000000000260000 - 0x00000000002dffff
   0x0000000047770000 - 0x000000004778ffff
    0x00000000004f0000 - 0x000000000056ffff
    0x0000000077330000 - 0x00000000774d8fff
  0x000007fffffb0000 - 0x000007fffffd2fff
   0x000007feff650000 - 0x000007feff650fff
    0x000000007ffe0000 - 0x000000007ffeffff
   0x000007fffffd8000 - 0x000007fffffd9fff
    0x000007fffffd5000 - 0x000007fffffd5fff
```

iehistory

This Plugin helps in recovering the fragments of the Internet explore history index.dat named cache files. It displays FTP and HTTP links that were accessed, links that were redirected, any deleted entries.

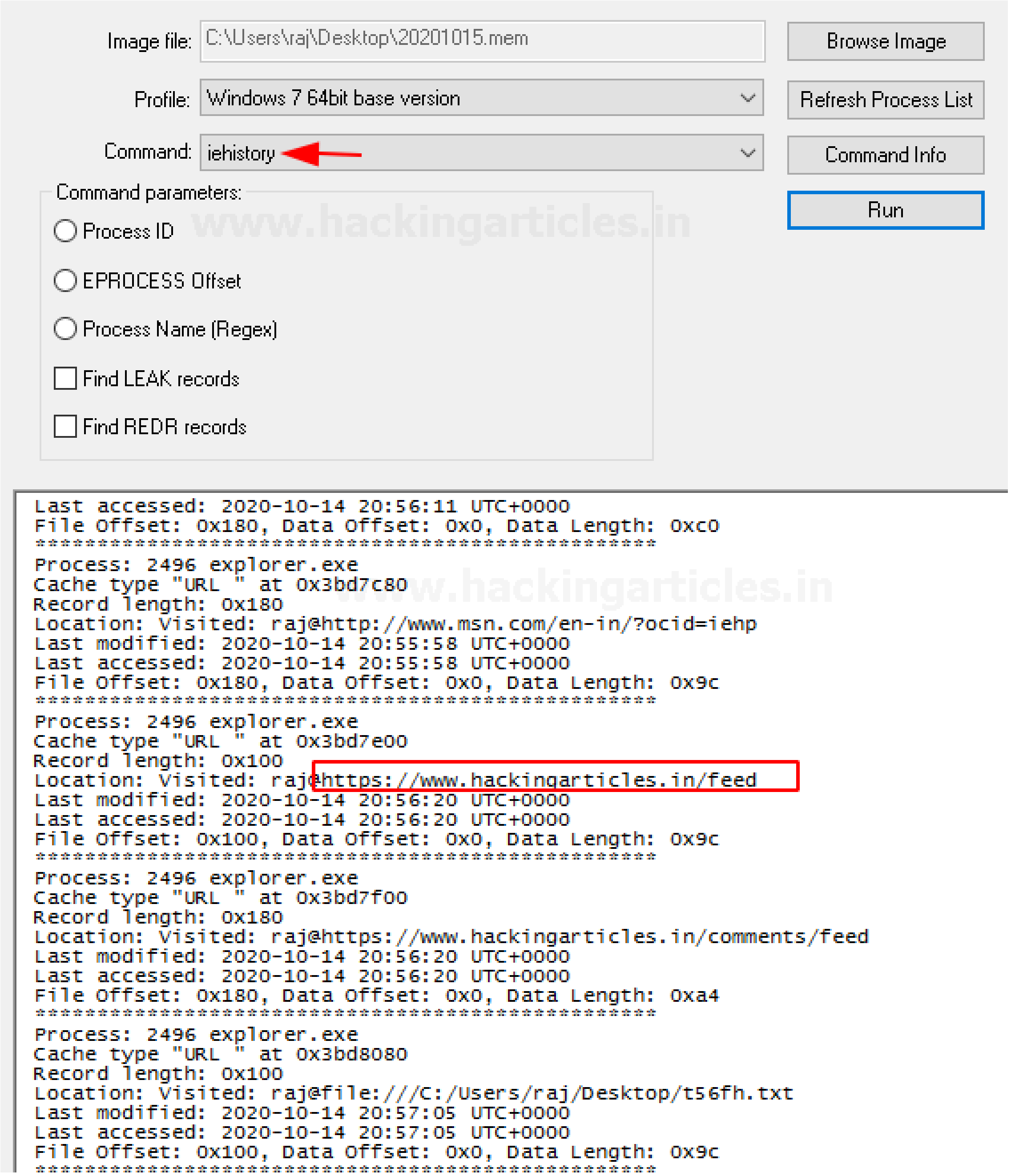


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: iehistory

Command parameters:

○ Process ID

○ EPROCESS Offset

○ Process Name (Regex)

□ Find LEAK records

□ Find REDR records

```
Last accessed: 2020-10-14 20:56:11 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0xc0
**************************************************
Process: 2496 explorer.exe
Cache type "URL " at 0x3bd7c80
Record length: 0x180
Location: Visited: raj@http://www.msn.com/en-in/?ocid=iehp
Last modified: 2020-10-14 20:55:58 UTC+0000
Last accessed: 2020-10-14 20:55:58 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0x9c
**************************************************
Process: 2496 explorer.exe
Cache type "URL " at 0x3bd7e00
Record length: 0x100
Location: Visited: raj@https://www.hackingarticles.in/feed
Last modified: 2020-10-14 20:56:20 UTC+0000
Last accessed: 2020-10-14 20:56:20 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c
**************************************************
Process: 2496 explorer.exe
Cache type "URL " at 0x3bd7f00
Record length: 0x180
Location: Visited: raj@https://www.hackingarticles.in/comments/feed
Last modified: 2020-10-14 20:56:20 UTC+0000
Last accessed: 2020-10-14 20:56:20 UTC+0000
File Offset: 0x180, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 2496 explorer.exe
Cache type "URL " at 0x3bd8080
Record length: 0x100
Location: Visited: raj@file:///C:/Users/raj/Desktop/t56fh.txt
Last modified: 2020-10-14 20:57:05 UTC+0000
Last accessed: 2020-10-14 20:57:05 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c
**************************************************
```

Modules

This command is used to list the kernel drivers that are present in the system.

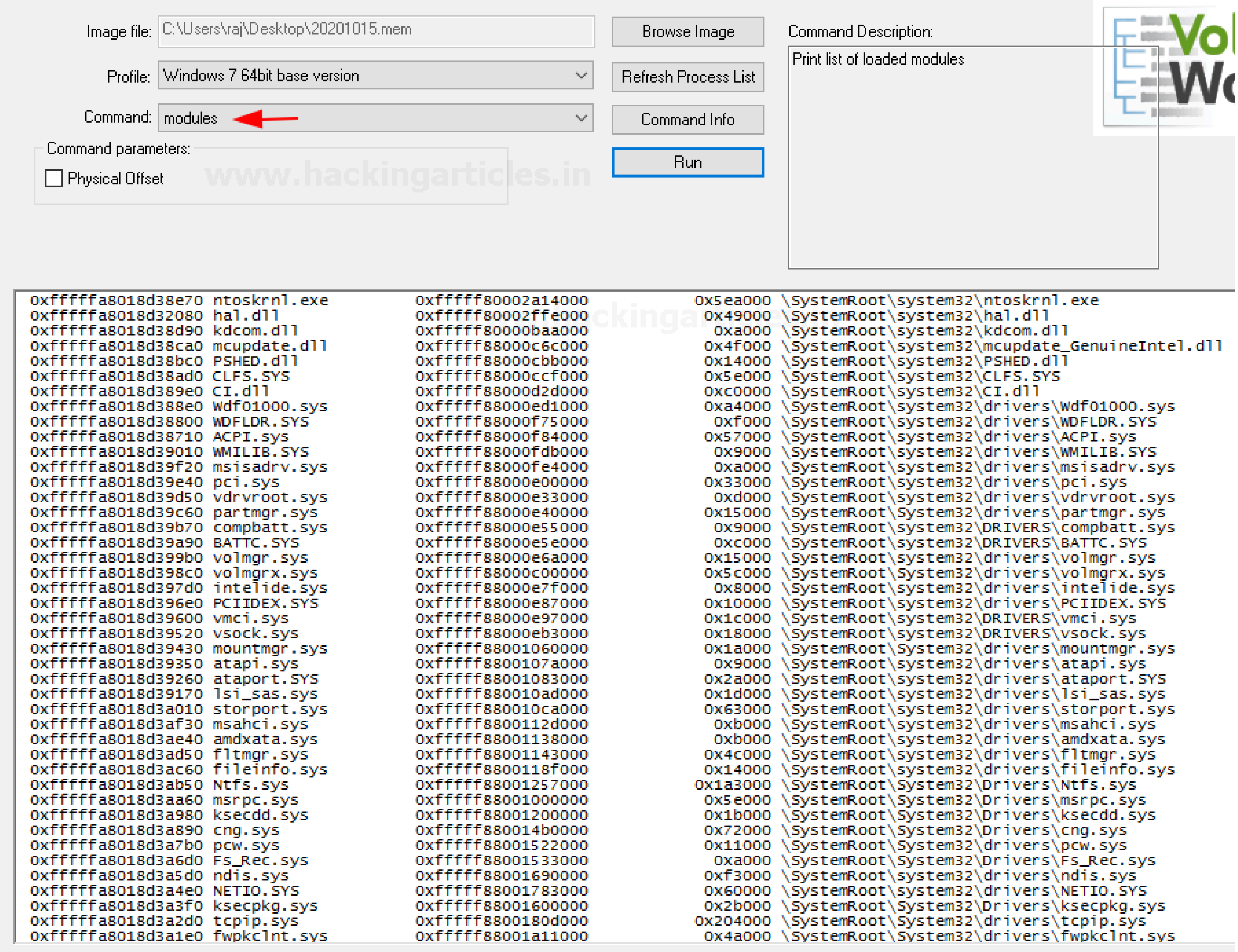


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: modules

Command parameters:

□ Physical Offset

Command Description:

Print list of loaded modules

```
0xfffffa8018d38e70 ntoskrnl.exe        0xfffff80002a14000     0x5ea000 \SystemRoot\system32\ntoskrnl.exe
0xfffffa8018d32080 hal.dll             0xfffff80002ffe000      0x49000 \SystemRoot\system32\hal.dll
0xfffffa8018d38d90 kdcom.dll           0xfffff80000baa000       0xa000 \SystemRoot\system32\kdcom.dll
0xfffffa8018d38ca0 mcupdate.dll        0xfffff88000c6c000      0x4f000 \SystemRoot\system32\mcupdate_GenuineIntel.dll
0xfffffa8018d38bc0 PSHED.dll           0xfffff88000cbb000      0x14000 \SystemRoot\system32\PSHED.dll
0xfffffa8018d38ad0 CLFS.SYS            0xfffff88000ccf000      0x5e000 \SystemRoot\system32\CLFS.SYS
0xfffffa8018d389e0 CI.dll              0xfffff88000d2d000      0xc0000 \SystemRoot\system32\CI.dll
0xfffffa8018d388e0 Wdf01000.sys        0xfffff88000ed1000      0xa4000 \SystemRoot\system32\drivers\Wdf01000.sys
0xfffffa8018d38800 WDFLDR.SYS          0xfffff88000f75000       0xf000 \SystemRoot\system32\drivers\WDFLDR.SYS
0xfffffa8018d38710 ACPI.sys            0xfffff88000f84000      0x57000 \SystemRoot\system32\drivers\ACPI.sys
0xfffffa8018d39010 WMILIB.SYS          0xfffff88000fdb000       0x9000 \SystemRoot\system32\drivers\WMILIB.SYS
0xfffffa8018d39f20 msisadrv.sys        0xfffff88000fe4000       0xa000 \SystemRoot\system32\drivers\msisadrv.sys
0xfffffa8018d39e40 pci.sys             0xfffff88000e00000      0x33000 \SystemRoot\system32\drivers\pci.sys
0xfffffa8018d39d50 vdrvroot.sys        0xfffff88000e33000       0xd000 \SystemRoot\system32\drivers\vdrvroot.sys
0xfffffa8018d39c60 partmgr.sys         0xfffff88000e40000      0x15000 \SystemRoot\System32\drivers\partmgr.sys
0xfffffa8018d39b70 compbatt.sys        0xfffff88000e55000       0x9000 \SystemRoot\system32\DRIVERS\compbatt.sys
0xfffffa8018d39a90 BATTC.SYS           0xfffff88000e5e000       0xc000 \SystemRoot\system32\DRIVERS\BATTC.SYS
0xfffffa8018d399b0 volmgr.sys          0xfffff88000e6a000      0x15000 \SystemRoot\system32\drivers\volmgr.sys
0xfffffa8018d398c0 volmgrx.sys         0xfffff88000c00000      0x5c000 \SystemRoot\System32\drivers\volmgrx.sys
0xfffffa8018d397d0 intelide.sys        0xfffff88000e7f000       0x8000 \SystemRoot\system32\drivers\intelide.sys
0xfffffa8018d396e0 PCIIDEX.SYS         0xfffff88000e87000      0x10000 \SystemRoot\system32\drivers\PCIIDEX.SYS
0xfffffa8018d39600 vmci.sys            0xfffff88000e97000      0x1c000 \SystemRoot\system32\DRIVERS\vmci.sys
0xfffffa8018d39520 vsock.sys           0xfffff88000eb3000      0x18000 \SystemRoot\system32\DRIVERS\vsock.sys
0xfffffa8018d39430 mountmgr.sys        0xfffff88001060000      0x1a000 \SystemRoot\System32\drivers\mountmgr.sys
0xfffffa8018d39350 atapi.sys           0xfffff8800107a000       0x9000 \SystemRoot\system32\drivers\atapi.sys
0xfffffa8018d39260 ataport.SYS         0xfffff88001083000      0x2a000 \SystemRoot\system32\drivers\ataport.SYS
0xfffffa8018d39170 lsi_sas.sys         0xfffff880010ad000      0x1d000 \SystemRoot\system32\drivers\lsi_sas.sys
0xfffffa8018d3a010 storport.sys        0xfffff880010ca000      0x63000 \SystemRoot\system32\drivers\storport.sys
0xfffffa8018d3af30 msahci.sys          0xfffff8800112d000       0xb000 \SystemRoot\system32\drivers\msahci.sys
0xfffffa8018d3ae40 amdxata.sys         0xfffff88001138000       0xb000 \SystemRoot\system32\drivers\amdxata.sys
0xfffffa8018d3ad50 fltmgr.sys          0xfffff88001143000      0x4c000 \SystemRoot\system32\drivers\fltmgr.sys
0xfffffa8018d3ac60 fileinfo.sys        0xfffff8800118f000      0x14000 \SystemRoot\system32\drivers\fileinfo.sys
0xfffffa8018d3ab50 Ntfs.sys            0xfffff88001257000     0x1a3000 \SystemRoot\System32\Drivers\Ntfs.sys
0xfffffa8018d3aa60 msrpc.sys           0xfffff88001000000      0x5e000 \SystemRoot\System32\Drivers\msrpc.sys
0xfffffa8018d3a980 ksecdd.sys          0xfffff88001200000      0x1b000 \SystemRoot\System32\Drivers\ksecdd.sys
0xfffffa8018d3a890 cng.sys             0xfffff880014b0000      0x72000 \SystemRoot\System32\Drivers\cng.sys
0xfffffa8018d3a7b0 pcw.sys             0xfffff88001522000      0x11000 \SystemRoot\System32\drivers\pcw.sys
0xfffffa8018d3a6d0 Fs_Rec.sys          0xfffff88001533000       0xa000 \SystemRoot\System32\Drivers\Fs_Rec.sys
0xfffffa8018d3a5d0 ndis.sys            0xfffff88001690000      0xf3000 \SystemRoot\system32\drivers\ndis.sys
0xfffffa8018d3a4e0 NETIO.SYS           0xfffff88001783000      0x60000 \SystemRoot\system32\drivers\NETIO.SYS
0xfffffa8018d3a3f0 ksecpkg.sys         0xfffff88001600000      0x2b000 \SystemRoot\System32\Drivers\ksecpkg.sys
0xfffffa8018d3a2d0 tcpip.sys           0xfffff8800180d000     0x204000 \SystemRoot\System32\drivers\tcpip.sys
0xfffffa8018d3a1e0 fwpkclnt.sys        0xfffff88001a11000      0x4a000 \SystemRoot\System32\drivers\fwpkclnt.sys
```

SSDT

This command is used to list the functions present in the original and GUI SSDTs. It displays the index, the name of the function, and the owner of the driver of each entry in the SSDT.

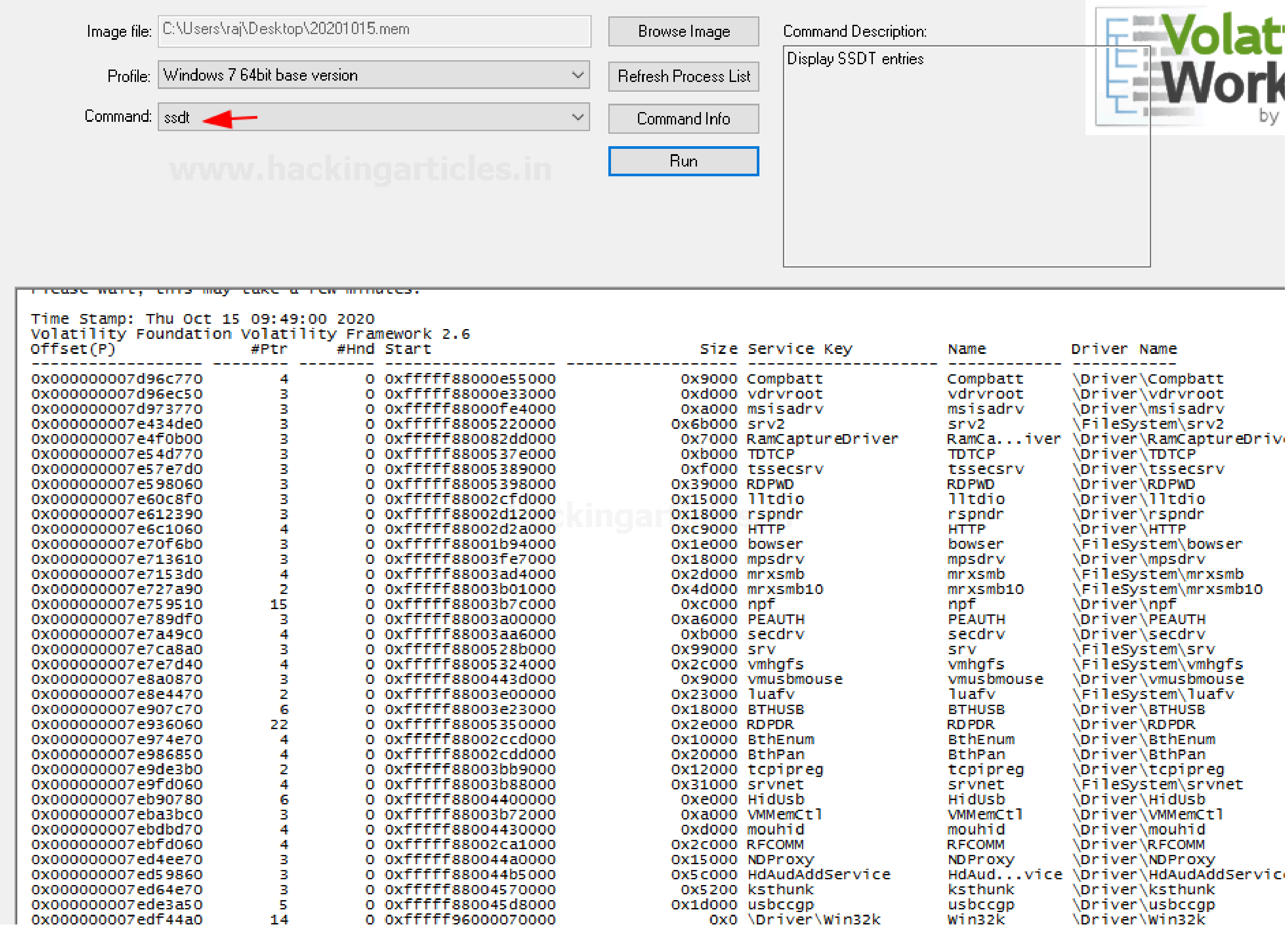


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: ssdt

Command Description:
Display SSDT entries

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:49:00 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr     #Hnd Start                            Size Service Key          Name         Driver Name
------------------ -------- -------- ------------------ ------------------ -------------------- ------------ -----------
0x000000007d96c770        4        0 0xfffff88000e55000             0x9000 Compbatt             Compbatt     \Driver\Compbatt
0x000000007d96ec50        3        0 0xfffff88000e33000             0xd000 vdrvroot             vdrvroot     \Driver\vdrvroot
0x000000007d973770        3        0 0xfffff88000fe4000             0xa000 msisadrv             msisadrv     \Driver\msisadrv
0x000000007e434de0        3        0 0xfffff88005220000            0x6b000 srv2                 srv2         \FileSystem\srv2
0x000000007e4f0b00        3        0 0xfffff880082dd000             0x7000 RamCaptureDriver     RamCa...iver \Driver\RamCaptureDriv
0x000000007e54d770        3        0 0xfffff8800537e000             0xb000 TDTCP                TDTCP        \Driver\TDTCP
0x000000007e57e7d0        3        0 0xfffff88005389000             0xf000 tssecsrv             tssecsrv     \Driver\tssecsrv
0x000000007e598060        3        0 0xfffff88005398000            0x39000 RDPWD                RDPWD        \Driver\RDPWD
0x000000007e60c8f0        3        0 0xfffff88002cfd000            0x15000 lltdio               lltdio       \Driver\lltdio
0x000000007e612390        3        0 0xfffff88002d12000            0x18000 rspndr               rspndr       \Driver\rspndr
0x000000007e6c1060        4        0 0xfffff88002d2a000            0xc9000 HTTP                 HTTP         \Driver\HTTP
0x000000007e70f6b0        3        0 0xfffff88001b94000            0x1e000 bowser               bowser       \FileSystem\bowser
0x000000007e713610        3        0 0xfffff88003fe7000            0x18000 mpsdrv               mpsdrv       \Driver\mpsdrv
0x000000007e7153d0        4        0 0xfffff88003ad4000            0x2d000 mrxsmb               mrxsmb       \FileSystem\mrxsmb
0x000000007e727a90        2        0 0xfffff88003b01000            0x4d000 mrxsmb10             mrxsmb10     \FileSystem\mrxsmb10
0x000000007e759510       15        0 0xfffff88003b7c000             0xc000 npf                  npf          \Driver\npf
0x000000007e789df0        3        0 0xfffff88003a00000            0xa6000 PEAUTH               PEAUTH       \Driver\PEAUTH
0x000000007e7a49c0        4        0 0xfffff88003aa6000             0xb000 secdrv               secdrv       \Driver\secdrv
0x000000007e7ca8a0        3        0 0xfffff8800528b000            0x99000 srv                  srv          \FileSystem\srv
0x000000007e7e7d40        4        0 0xfffff88005324000            0x2c000 vmhgfs               vmhgfs       \FileSystem\vmhgfs
0x000000007e8a0870        3        0 0xfffff8800443d000             0x9000 vmusbmouse           vmusbmouse   \Driver\vmusbmouse
0x000000007e8e4470        2        0 0xfffff88003e00000            0x23000 luafv                luafv        \FileSystem\luafv
0x000000007e907c70        6        0 0xfffff88003e23000            0x18000 BTHUSB               BTHUSB       \Driver\BTHUSB
0x000000007e936060       22        0 0xfffff88005350000            0x2e000 RDPDR                RDPDR        \Driver\RDPDR
0x000000007e974e70        4        0 0xfffff88002ccd000            0x10000 BthEnum              BthEnum      \Driver\BthEnum
0x000000007e986850        4        0 0xfffff88002cdd000            0x20000 BthPan               BthPan       \Driver\BthPan
0x000000007e9de3b0        2        0 0xfffff88003bb9000            0x12000 tcpipreg             tcpipreg     \Driver\tcpipreg
0x000000007e9fd060        4        0 0xfffff88003b88000            0x31000 srvnet               srvnet       \FileSystem\srvnet
0x000000007eb90780        6        0 0xfffff88004400000             0xe000 HidUsb               HidUsb       \Driver\HidUsb
0x000000007eba3bc0        3        0 0xfffff88003b72000             0xa000 VMMemCtl             VMMemCtl     \Driver\VMMemCtl
0x000000007ebdbd70        4        0 0xfffff88004430000             0xd000 mouhid               mouhid       \Driver\mouhid
0x000000007ebfd060        4        0 0xfffff88002ca1000            0x2c000 RFCOMM               RFCOMM       \Driver\RFCOMM
0x000000007ed4ee70        3        0 0xfffff880044a0000            0x15000 NDProxy              NDProxy      \Driver\NDProxy
0x000000007ed59860        3        0 0xfffff880044b5000            0x5c000 HdAudAddService      HdAud...vice \Driver\HdAudAddServic
0x000000007ed64e70        3        0 0xfffff88004570000             0x5200 ksthunk              ksthunk      \Driver\ksthunk
0x000000007ede3a50        5        0 0xfffff880045d8000            0x1d000 usbccgp              usbccgp      \Driver\usbccgp
0x000000007edf44a0       14        0 0xfffff96000070000                0x0 \Driver\Win32k       Win32k       \Driver\Win32k
```

Driverscan

This command can be used to find the DRIVER_OBJECT present in the physical memory by making use of a pool tag scan.

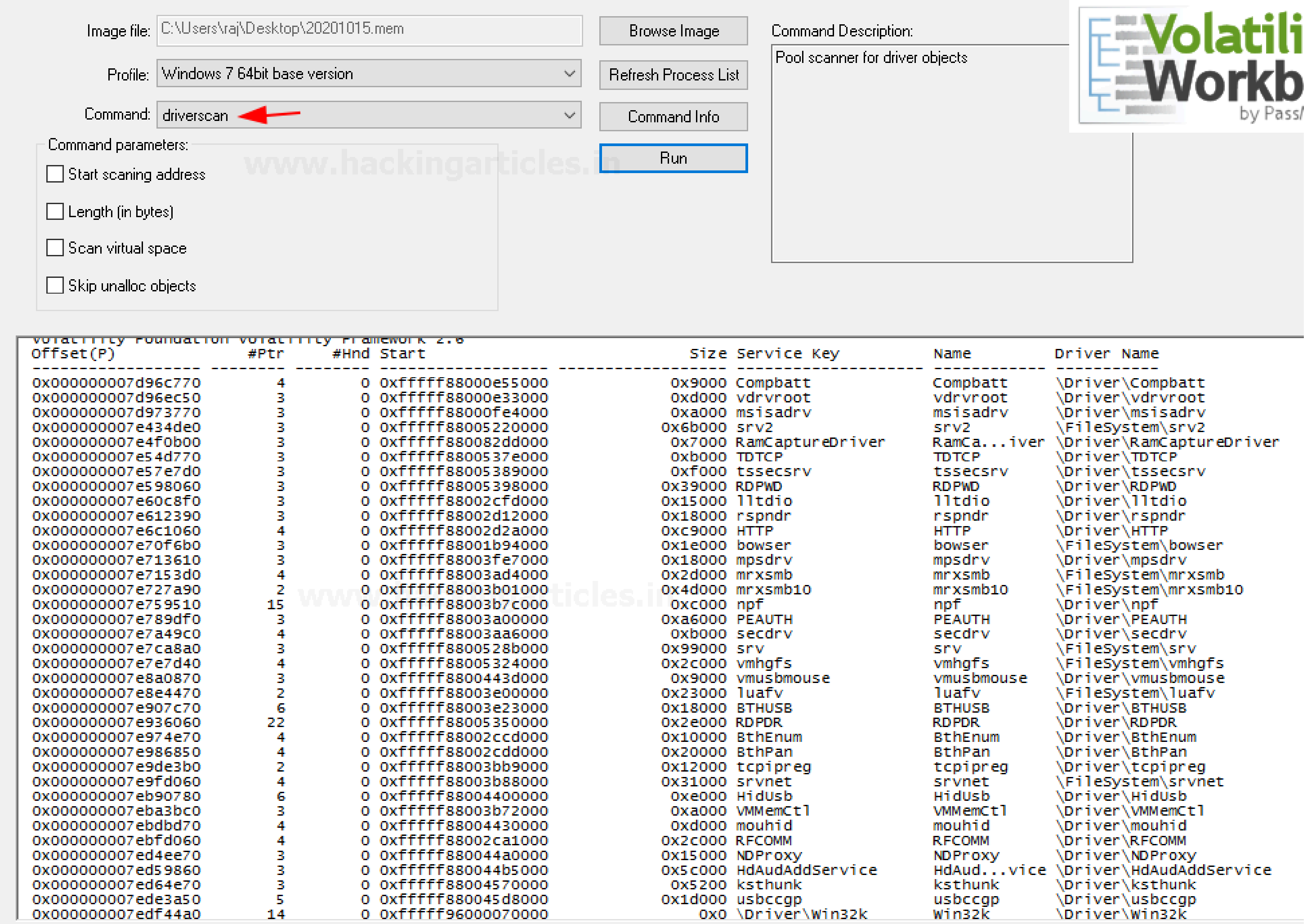


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: driverscan

Command parameters:

□ Start scaning address

□ Length (in bytes)

□ Scan virtual space

□ Skip unalloc objects

Command Description:

Pool scanner for driver objects

```
Volatility Foundation Volatility Framework 2.6
Offset(P)              #Ptr     #Hnd Start                            Size Service Key          Name         Driver Name
------------------ -------- -------- ------------------ ------------------ -------------------- ------------ ------------
0x000000007d96c770        4        0 0xfffff88000e55000             0x9000 Compbatt             Compbatt     \Driver\Compbatt
0x000000007d96ec50        3        0 0xfffff88000e33000             0xd000 vdrvroot             vdrvroot     \Driver\vdrvroot
0x000000007d973770        3        0 0xfffff88000fe4000             0xa000 msisadrv             msisadrv     \Driver\msisadrv
0x000000007e434de0        3        0 0xfffff88005220000            0x6b000 srv2                 srv2         \FileSystem\srv2
0x000000007e4f0b00        3        0 0xfffff880082dd000             0x7000 RamCaptureDriver     RamCa...iver \Driver\RamCaptureDriver
0x000000007e54d770        3        0 0xfffff8800537e000             0xb000 TDTCP                TDTCP        \Driver\TDTCP
0x000000007e57e7d0        3        0 0xfffff88005389000             0xf000 tssecsrv             tssecsrv     \Driver\tssecsrv
0x000000007e598060        3        0 0xfffff88005398000            0x39000 RDPWD                RDPWD        \Driver\RDPWD
0x000000007e60c8f0        3        0 0xfffff88002cfd000            0x15000 lltdio               lltdio       \Driver\lltdio
0x000000007e612390        3        0 0xfffff88002d12000            0x18000 rspndr               rspndr       \Driver\rspndr
0x000000007e6c1060        4        0 0xfffff88002d2a000            0xc9000 HTTP                 HTTP         \Driver\HTTP
0x000000007e70f6b0        3        0 0xfffff88001b94000            0x1e000 bowser               bowser       \FileSystem\bowser
0x000000007e713610        3        0 0xfffff88003fe7000            0x18000 mpsdrv               mpsdrv       \Driver\mpsdrv
0x000000007e7153d0        4        0 0xfffff88003ad4000            0x2d000 mrxsmb               mrxsmb       \FileSystem\mrxsmb
0x000000007e727a90        2        0 0xfffff88003b01000            0x4d000 mrxsmb10             mrxsmb10     \FileSystem\mrxsmb10
0x000000007e759510       15        0 0xfffff88003b7c000             0xc000 npf                  npf          \Driver\npf
0x000000007e789df0        3        0 0xfffff88003a00000            0xa6000 PEAUTH               PEAUTH       \Driver\PEAUTH
0x000000007e7a49c0        4        0 0xfffff88003aa6000             0xb000 secdrv               secdrv       \Driver\secdrv
0x000000007e7ca8a0        3        0 0xfffff8800528b000            0x99000 srv                  srv          \FileSystem\srv
0x000000007e7e7d40        4        0 0xfffff88005324000            0x2c000 vmhgfs               vmhgfs       \FileSystem\vmhgfs
0x000000007e8a0870        3        0 0xfffff8800443d000             0x9000 vmusbmouse           vmusbmouse   \Driver\vmusbmouse
0x000000007e8e4470        2        0 0xfffff88003e00000            0x23000 luafv                luafv        \FileSystem\luafv
0x000000007e907c70        6        0 0xfffff88003e23000            0x18000 BTHUSB               BTHUSB       \Driver\BTHUSB
0x000000007e936060       22        0 0xfffff88005350000            0x2e000 RDPDR                RDPDR        \Driver\RDPDR
0x000000007e974e70        4        0 0xfffff88002ccd000            0x10000 BthEnum              BthEnum      \Driver\BthEnum
0x000000007e986850        4        0 0xfffff88002cdd000            0x20000 BthPan               BthPan       \Driver\BthPan
0x000000007e9de3b0        2        0 0xfffff88003bb9000            0x12000 tcpipreg             tcpipreg     \Driver\tcpipreg
0x000000007e9fd060        4        0 0xfffff88003b88000            0x31000 srvnet               srvnet       \FileSystem\srvnet
0x000000007eb90780        6        0 0xfffff88004400000             0xe000 HidUsb               HidUsb       \Driver\HidUsb
0x000000007eba3bc0        3        0 0xfffff88003b72000             0xa000 VMMemCtl             VMMemCtl     \Driver\VMMemCtl
0x000000007ebdbd70        4        0 0xfffff88004430000             0xd000 mouhid               mouhid       \Driver\mouhid
0x000000007ebfd060        4        0 0xfffff88002ca1000            0x2c000 RFCOMM               RFCOMM       \Driver\RFCOMM
0x000000007ed4ee70        3        0 0xfffff880044a0000            0x15000 NDProxy              NDProxy      \Driver\NDProxy
0x000000007ed59860        3        0 0xfffff880044b5000            0x5c000 HdAudAddService      HdAud...vice \Driver\HdAudAddService
0x000000007ed64e70        3        0 0xfffff88004570000             0x5200 ksthunk              ksthunk      \Driver\ksthunk
0x000000007ede3a50        5        0 0xfffff880045d8000            0x1d000 usbccgp              usbccgp      \Driver\usbccgp
0x000000007edf44a0       14        0 0xfffff96000070000                0x0 \Driver\Win32k       Win32k       \Driver\Win32k
```

File Scan

This command can be used to find File_object that is present in the physical memory by making use of a pool tag scan. This command will help in finding open files in the system dump even if they are hidden with the help of rootkit,

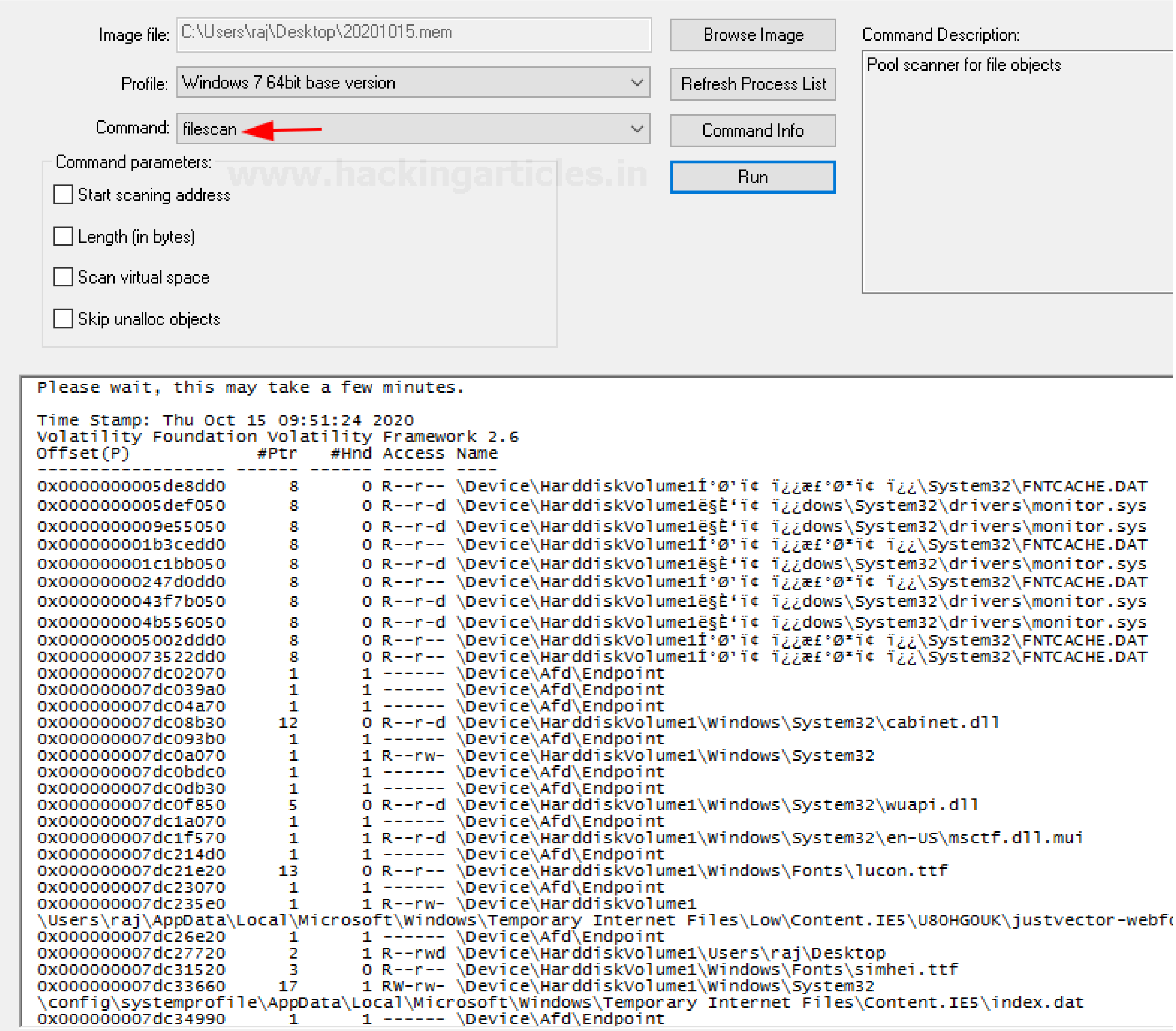


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: filescan

Command parameters:

☐ Start scaning address

☐ Length (in bytes)

☐ Scan virtual space

☐ Skip unalloc objects

Command Description:

Pool scanner for file objects

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:51:24 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x000000005de8dd0       8      0 R--r-- \Device\HarddiskVolume1İ'Ø'ï¢ ï¿¿æ£'Ø*ï¢ ï¿¿\System32\FNTCACHE.DAT
0x000000005def050       8      0 R--r-d \Device\HarddiskVolume1ë§Ė'ï¢ ï¿¿dows\System32\drivers\monitor.sys
0x000000009e55050       8      0 R--r-d \Device\HarddiskVolume1ë§Ė'ï¢ ï¿¿dows\System32\drivers\monitor.sys
0x00000001b3cedd0       8      0 R--r-- \Device\HarddiskVolume1İ'Ø'ï¢ ï¿¿æ£'Ø*ï¢ ï¿¿\System32\FNTCACHE.DAT
0x00000001c1bb050       8      0 R--r-d \Device\HarddiskVolume1ë§Ė'ï¢ ï¿¿dows\System32\drivers\monitor.sys
0x0000000247d0dd0       8      0 R--r-- \Device\HarddiskVolume1İ'Ø'ï¢ ï¿¿æ£'Ø*ï¢ ï¿¿\System32\FNTCACHE.DAT
0x000000043f7b050       8      0 R--r-d \Device\HarddiskVolume1ë§Ė'ï¢ ï¿¿dows\System32\drivers\monitor.sys
0x00000004b556050       8      0 R--r-d \Device\HarddiskVolume1ë§Ė'ï¢ ï¿¿dows\System32\drivers\monitor.sys
0x000000005002ddd0      8      0 R--r-- \Device\HarddiskVolume1İ'Ø'ï¢ ï¿¿æ£'Ø*ï¢ ï¿¿\System32\FNTCACHE.DAT
0x0000000073522dd0      8      0 R--r-- \Device\HarddiskVolume1İ'Ø'ï¢ ï¿¿æ£'Ø*ï¢ ï¿¿\System32\FNTCACHE.DAT
0x000000007dc02070      1      1 ------ \Device\Afd\Endpoint
0x000000007dc039a0      1      1 ------ \Device\Afd\Endpoint
0x000000007dc04a70      1      1 ------ \Device\Afd\Endpoint
0x000000007dc08b30     12      0 R--r-d \Device\HarddiskVolume1\Windows\System32\cabinet.dll
0x000000007dc093b0      1      1 ------ \Device\Afd\Endpoint
0x000000007dc0a070      1      1 R--rw- \Device\HarddiskVolume1\Windows\System32
0x000000007dc0bdc0      1      1 ------ \Device\Afd\Endpoint
0x000000007dc0db30      1      1 ------ \Device\Afd\Endpoint
0x000000007dc0f850      5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\wuapi.dll
0x000000007dc1a070      1      1 ------ \Device\Afd\Endpoint
0x000000007dc1f570      1      1 R--r-d \Device\HarddiskVolume1\Windows\System32\en-US\msctf.dll.mui
0x000000007dc214d0      1      1 ------ \Device\Afd\Endpoint
0x000000007dc21e20     13      0 R--r-- \Device\HarddiskVolume1\Windows\Fonts\lucon.ttf
0x000000007dc23070      1      1 ------ \Device\Afd\Endpoint
0x000000007dc235e0      1      1 R--rw- \Device\HarddiskVolume1
\Users\raj\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\U8OHGOUK\justvector-webf
0x000000007dc26e20      1      1 ------ \Device\Afd\Endpoint
0x000000007dc27720      2      1 R--rwd \Device\HarddiskVolume1\Users\raj\Desktop
0x000000007dc31520      3      0 R--r-- \Device\HarddiskVolume1\Windows\Fonts\simhei.ttf
0x000000007dc33660     17      1 RW-rw- \Device\HarddiskVolume1\Windows\System32
\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
0x000000007dc34990      1      1 ------ \Device\Afd\Endpoint
```

Mutant scan

This command is used to scan the physical memory of kmutant objects by making use of pool tag scanning.

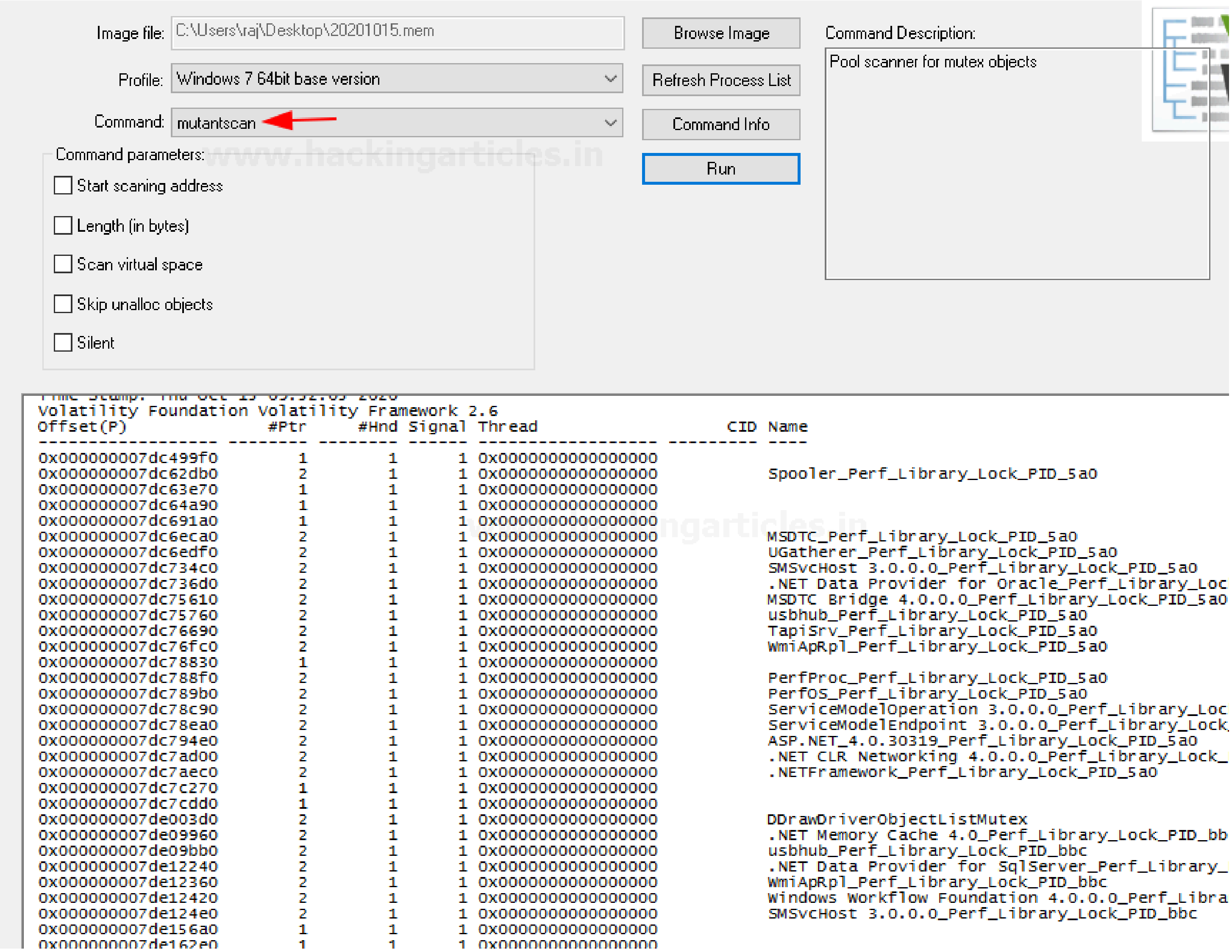


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: mutantscan

Command parameters:

- □ Start scaning address
- □ Length (in bytes)
- □ Scan virtual space
- □ Skip unalloc objects
- □ Silent

Command Description:

Pool scanner for mutex objects

```
Time Stamp: Thu Oct 15 05:32:05 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)                  #Ptr     #Hnd Signal Thread                     CID Name
------------------ -------- -------- ------ ------------------ --------- ----
0x000000007dc499f0        1        1      1 0x0000000000000000
0x000000007dc62db0        2        1      1 0x0000000000000000           Spooler_Perf_Library_Lock_PID_5a0
0x000000007dc63e70        1        1      1 0x0000000000000000
0x000000007dc64a90        1        1      1 0x0000000000000000
0x000000007dc691a0        1        1      1 0x0000000000000000
0x000000007dc6eca0        2        1      1 0x0000000000000000           MSDTC_Perf_Library_Lock_PID_5a0
0x000000007dc6edf0        2        1      1 0x0000000000000000           UGatherer_Perf_Library_Lock_PID_5a0
0x000000007dc734c0        2        1      1 0x0000000000000000           SMSvcHost 3.0.0.0_Perf_Library_Lock_PID_5a0
0x000000007dc736d0        2        1      1 0x0000000000000000           .NET Data Provider for Oracle_Perf_Library_Loc
0x000000007dc75610        2        1      1 0x0000000000000000           MSDTC Bridge 4.0.0.0_Perf_Library_Lock_PID_5a0
0x000000007dc75760        2        1      1 0x0000000000000000           usbhub_Perf_Library_Lock_PID_5a0
0x000000007dc76690        2        1      1 0x0000000000000000           TapiSrv_Perf_Library_Lock_PID_5a0
0x000000007dc76fc0        2        1      1 0x0000000000000000           WmiApRpl_Perf_Library_Lock_PID_5a0
0x000000007dc78830        1        1      1 0x0000000000000000
0x000000007dc788f0        2        1      1 0x0000000000000000           PerfProc_Perf_Library_Lock_PID_5a0
0x000000007dc789b0        2        1      1 0x0000000000000000           PerfOS_Perf_Library_Lock_PID_5a0
0x000000007dc78c90        2        1      1 0x0000000000000000           ServiceModelOperation 3.0.0.0_Perf_Library_Loc
0x000000007dc78ea0        2        1      1 0x0000000000000000           ServiceModelEndpoint 3.0.0.0_Perf_Library_Lock
0x000000007dc794e0        2        1      1 0x0000000000000000           ASP.NET_4.0.30319_Perf_Library_Lock_PID_5a0
0x000000007dc7ad00        2        1      1 0x0000000000000000           .NET CLR Networking 4.0.0.0_Perf_Library_Lock_
0x000000007dc7aec0        2        1      1 0x0000000000000000           .NETFramework_Perf_Library_Lock_PID_5a0
0x000000007dc7c270        1        1      1 0x0000000000000000
0x000000007dc7cdd0        1        1      1 0x0000000000000000
0x000000007de003d0        2        1      1 0x0000000000000000           DDrawDriverObjectListMutex
0x000000007de09960        2        1      1 0x0000000000000000           .NET Memory Cache 4.0_Perf_Library_Lock_PID_bb
0x000000007de09bb0        2        1      1 0x0000000000000000           usbhub_Perf_Library_Lock_PID_bbc
0x000000007de12240        2        1      1 0x0000000000000000           .NET Data Provider for SqlServer_Perf_Library_
0x000000007de12360        2        1      1 0x0000000000000000           WmiApRpl_Perf_Library_Lock_PID_bbc
0x000000007de12420        2        1      1 0x0000000000000000           Windows Workflow Foundation 4.0.0.0_Perf_Libra
0x000000007de124e0        2        1      1 0x0000000000000000           SMSvcHost 3.0.0.0_Perf_Library_Lock_PID_bbc
0x000000007de156a0        1        1      1 0x0000000000000000
0x000000007de162e0        1        1      1 0x0000000000000000
```

Thrdscan

This command is used to find the ethread objects that are present in the physical memory with the help of a pool tag scan. It contains certain fields that can identify its parent processes which can help in finding hidden processes.

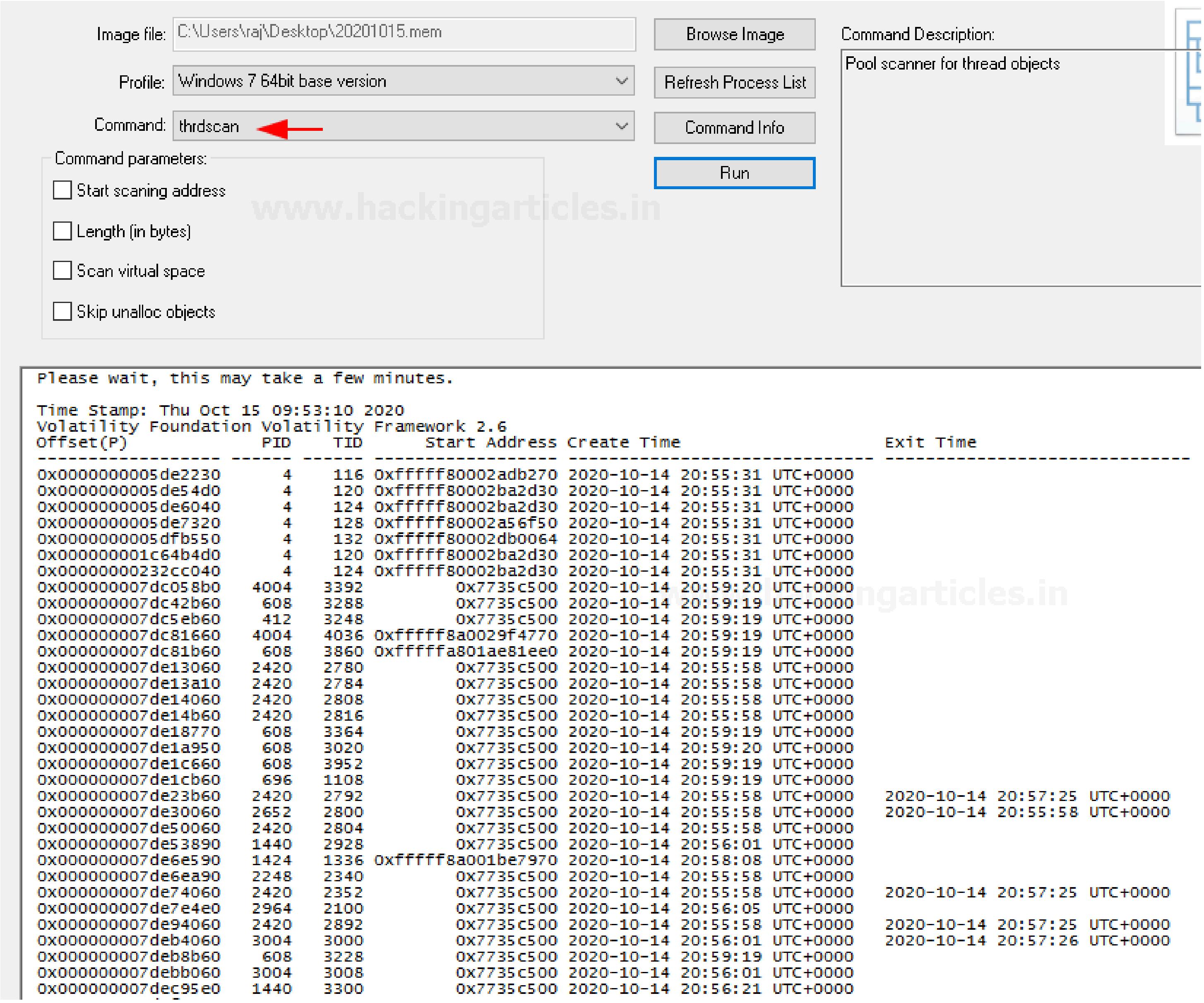


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: thrdscan

Command parameters:

- □ Start scaning address
- □ Length (in bytes)
- □ Scan virtual space
- □ Skip unalloc objects

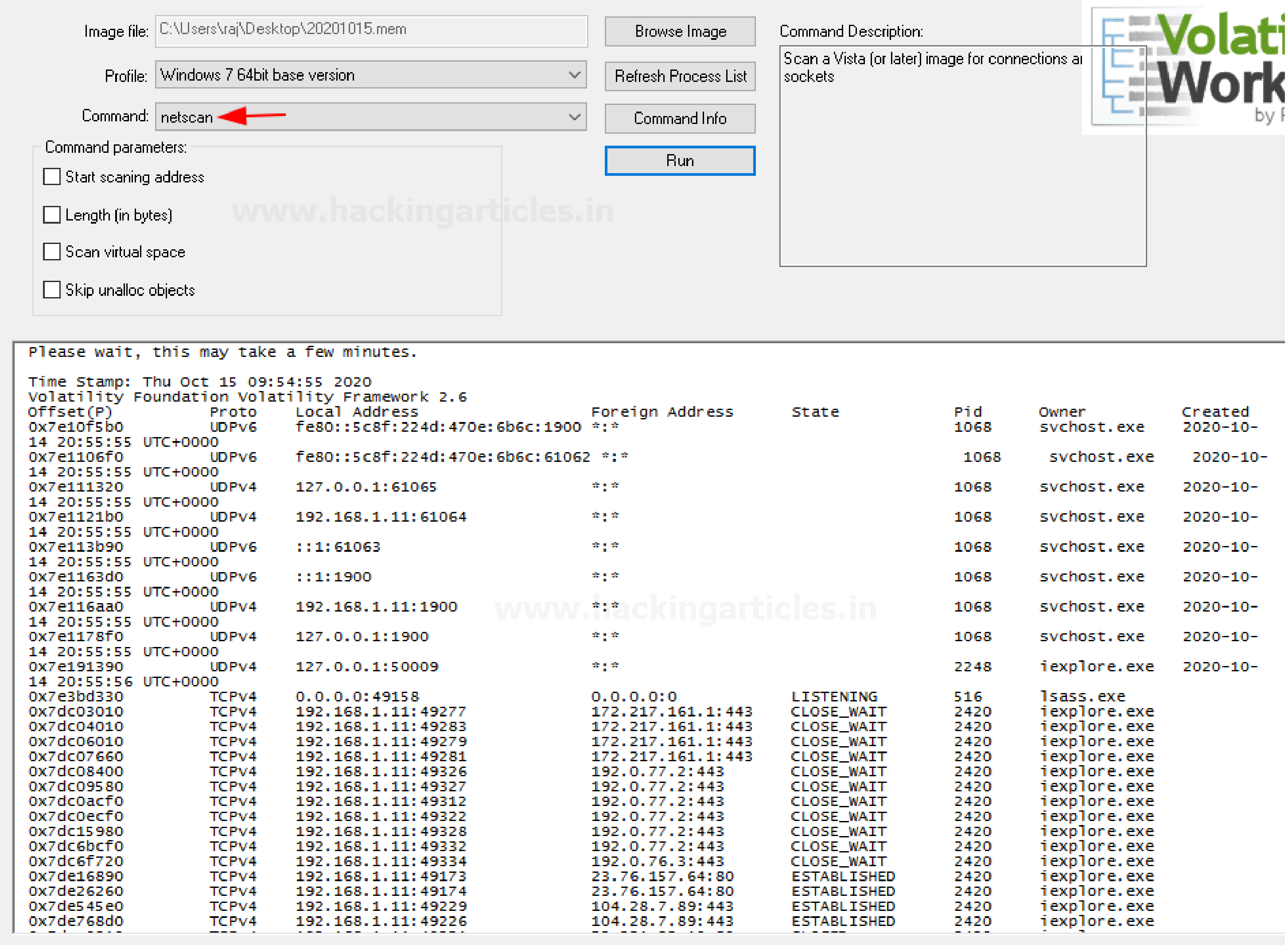
Command Description:
Pool scanner for thread objects

```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:53:10 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)             PID    TID      Start Address Create Time                    Exit Time
------------------ ------ ------ ------------------ ------------------------------ ------------------------------
0x0000000005de2230      4    116 0xfffff80002adb270 2020-10-14 20:55:31 UTC+0000
0x0000000005de54d0      4    120 0xfffff80002ba2d30 2020-10-14 20:55:31 UTC+0000
0x0000000005de6040      4    124 0xfffff80002ba2d30 2020-10-14 20:55:31 UTC+0000
0x0000000005de7320      4    128 0xfffff80002a56f50 2020-10-14 20:55:31 UTC+0000
0x0000000005dfb550      4    132 0xfffff80002db0064 2020-10-14 20:55:31 UTC+0000
0x000000001c64b4d0      4    120 0xfffff80002ba2d30 2020-10-14 20:55:31 UTC+0000
0x00000000232cc040      4    124 0xfffff80002ba2d30 2020-10-14 20:55:31 UTC+0000
0x000000007dc058b0   4004   3392         0x7735c500 2020-10-14 20:59:20 UTC+0000
0x000000007dc42b60    608   3288         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007dc5eb60    412   3248         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007dc81660   4004   4036 0xfffff8a0029f4770 2020-10-14 20:59:19 UTC+0000
0x000000007dc81b60    608   3860 0xfffffa801ae81ee0 2020-10-14 20:59:19 UTC+0000
0x000000007de13060   2420   2780         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de13a10   2420   2784         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de14060   2420   2808         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de14b60   2420   2816         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de18770    608   3364         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007de1a950    608   3020         0x7735c500 2020-10-14 20:59:20 UTC+0000
0x000000007de1c660    608   3952         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007de1cb60    696   1108         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007de23b60   2420   2792         0x7735c500 2020-10-14 20:55:58 UTC+0000   2020-10-14 20:57:25 UTC+0000
0x000000007de30060   2652   2800         0x7735c500 2020-10-14 20:55:58 UTC+0000   2020-10-14 20:55:58 UTC+0000
0x000000007de50060   2420   2804         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de53890   1440   2928         0x7735c500 2020-10-14 20:56:01 UTC+0000
0x000000007de6e590   1424   1336 0xfffff8a001be7970 2020-10-14 20:58:08 UTC+0000
0x000000007de6ea90   2248   2340         0x7735c500 2020-10-14 20:55:58 UTC+0000
0x000000007de74060   2420   2352         0x7735c500 2020-10-14 20:55:58 UTC+0000   2020-10-14 20:57:25 UTC+0000
0x000000007de7e4e0   2964   2100         0x7735c500 2020-10-14 20:56:05 UTC+0000
0x000000007de94060   2420   2892         0x7735c500 2020-10-14 20:55:58 UTC+0000   2020-10-14 20:57:25 UTC+0000
0x000000007deb4060   3004   3000         0x7735c500 2020-10-14 20:56:01 UTC+0000   2020-10-14 20:57:26 UTC+0000
0x000000007deb8b60    608   3228         0x7735c500 2020-10-14 20:59:19 UTC+0000
0x000000007debb060   3004   3008         0x7735c500 2020-10-14 20:56:01 UTC+0000
0x000000007dec95e0   1440   3300         0x7735c500 2020-10-14 20:56:21 UTC+0000
```

Netscan

This plugin helps in finding network-related artifacts present in the memory dump. It makes use of pool tag scanning. This plugin finds all the TCP endpoints, TCP listeners, UDP endpoints, and UDP listeners. It provides details about the local and remote IP and also about the local and remote port



```
Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:54:55 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7e10f5b0         UDPv6    fe80::5c8f:224d:470e:6b6c:1900 *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e1106f0         UDPv6    fe80::5c8f:224d:470e:6b6c:61062 *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e111320         UDPv4    127.0.0.1:61065                *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e1121b0         UDPv4    192.168.1.11:61064             *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e113b90         UDPv6    ::1:61063                      *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e1163d0         UDPv6    ::1:1900                       *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e116aa0         UDPv4    192.168.1.11:1900              *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e1178f0         UDPv4    127.0.0.1:1900                 *:*                                   1068     svchost.exe    2020-10-
14 20:55:55 UTC+0000
0x7e191390         UDPv4    127.0.0.1:50009                *:*                                   2248     iexplore.exe   2020-10-
14 20:55:56 UTC+0000
0x7e3bd330         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING        516      lsass.exe
0x7dc03010         TCPv4    192.168.1.11:49277             172.217.161.1:443    CLOSE_WAIT       2420     iexplore.exe
0x7dc04010         TCPv4    192.168.1.11:49283             172.217.161.1:443    CLOSE_WAIT       2420     iexplore.exe
0x7dc06010         TCPv4    192.168.1.11:49279             172.217.161.1:443    CLOSE_WAIT       2420     iexplore.exe
0x7dc07660         TCPv4    192.168.1.11:49281             172.217.161.1:443    CLOSE_WAIT       2420     iexplore.exe
0x7dc08400         TCPv4    192.168.1.11:49326             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc09580         TCPv4    192.168.1.11:49327             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc0acf0         TCPv4    192.168.1.11:49312             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc0ecf0         TCPv4    192.168.1.11:49322             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc15980         TCPv4    192.168.1.11:49328             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc6bcf0         TCPv4    192.168.1.11:49332             192.0.77.2:443       CLOSE_WAIT       2420     iexplore.exe
0x7dc6f720         TCPv4    192.168.1.11:49334             192.0.76.3:443       CLOSE_WAIT       2420     iexplore.exe
0x7de16890         TCPv4    192.168.1.11:49173             23.76.157.64:80      ESTABLISHED      2420     iexplore.exe
0x7de26260         TCPv4    192.168.1.11:49174             23.76.157.64:80      ESTABLISHED      2420     iexplore.exe
0x7de545e0         TCPv4    192.168.1.11:49229             104.28.7.89:443      ESTABLISHED      2420     iexplore.exe
0x7de768d0         TCPv4    192.168.1.11:49226             104.28.7.89:443      ESTABLISHED      2420     iexplore.exe
```

Hivescan

This command is used to find the physical address of the registry hives that are present in the memory. It is there to support the hivelist.

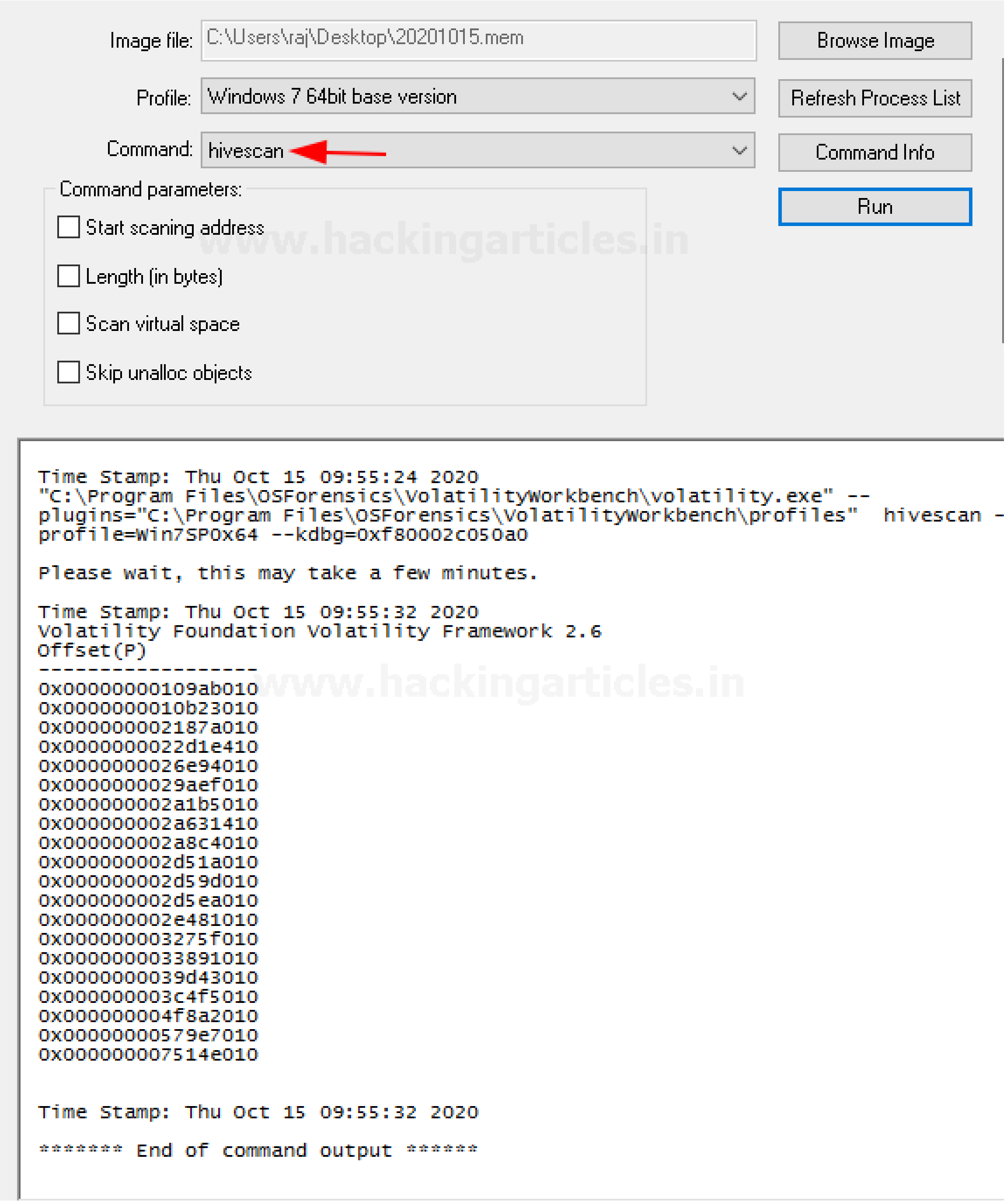


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: hivescan

Command parameters:

☐ Start scaning address

☐ Length (in bytes)

☐ Scan virtual space

☐ Skip unalloc objects

```
Time Stamp: Thu Oct 15 09:55:24 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  hivescan -
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:55:32 2020
Volatility Foundation Volatility Framework 2.6
Offset(P)
------------------
0x00000000109ab010
0x0000000010b23010
0x000000002187a010
0x0000000022d1e410
0x0000000026e94010
0x0000000029aef010
0x000000002a1b5010
0x000000002a631410
0x000000002a8c4010
0x000000002d51a010
0x000000002d59d010
0x000000002d5ea010
0x000000002e481010
0x000000003275f010
0x0000000033891010
0x0000000039d43010
0x000000003c4f5010
0x000000004f8a2010
0x00000000579e7010
0x000000007514e010


Time Stamp: Thu Oct 15 09:55:32 2020

******* End of command output ******
```

Hivelist

This command can be used to locate the virtual addresses present in the registry hives in memory, and their entire paths to hive on the disk.

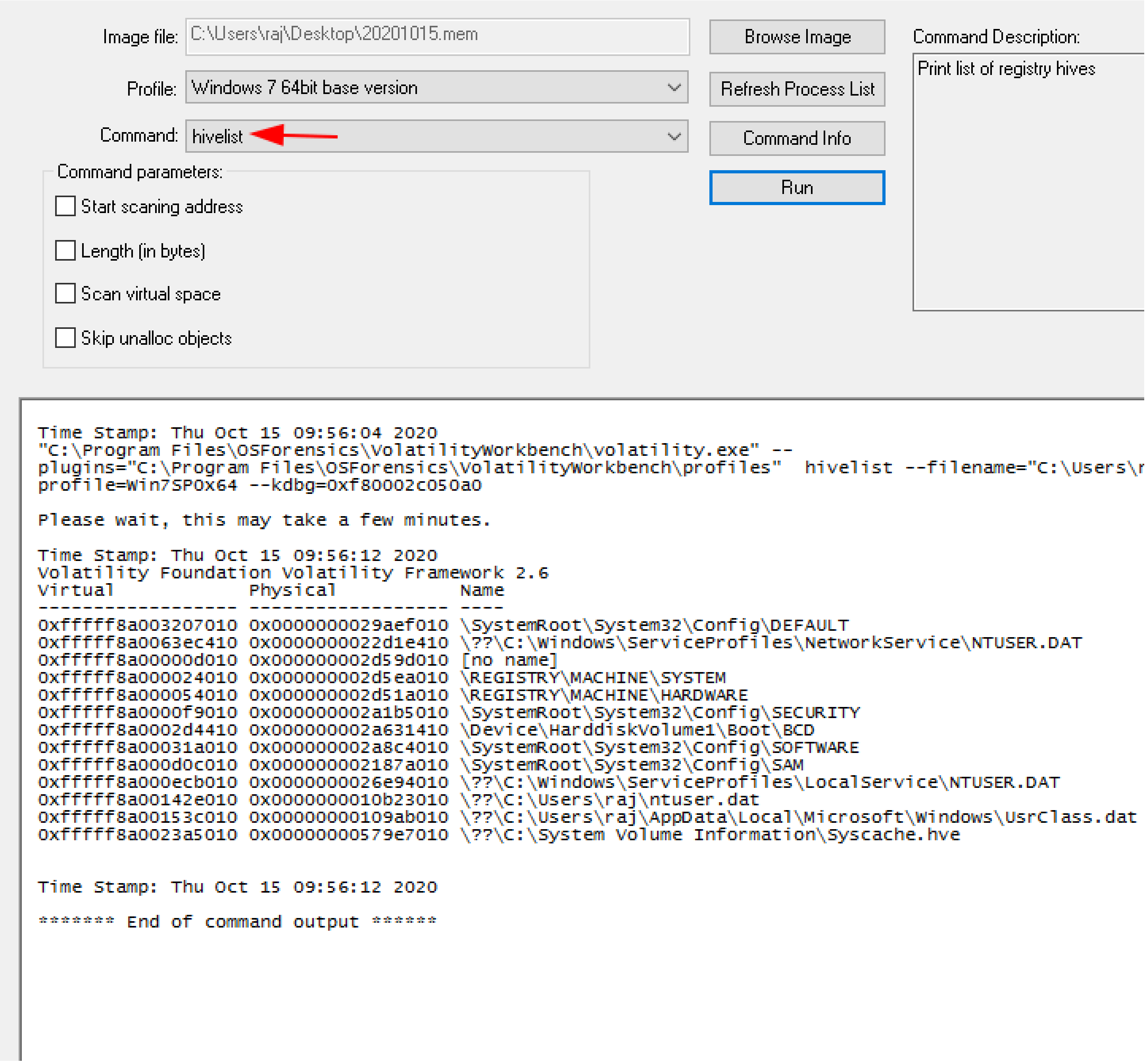


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: hivelist

Command parameters:

- □ Start scaning address
- □ Length (in bytes)
- □ Scan virtual space
- □ Skip unalloc objects

Command Description: Print list of registry hives

```
Time Stamp: Thu Oct 15 09:56:04 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  hivelist --filename="C:\Users\r
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:56:12 2020
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a003207010 0x0000000029aef010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0063ec410 0x0000000022d1e410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00000d010 0x000000002d59d010 [no name]
0xfffff8a000024010 0x000000002d5ea010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000054010 0x000000002d51a010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000f9010 0x000000002a1b5010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0002d4410 0x000000002a631410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00031a010 0x000000002a8c4010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000d0c010 0x000000002187a010 \SystemRoot\System32\Config\SAM
0xfffff8a000ecb010 0x0000000026e94010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00142e010 0x0000000010b23010 \??\C:\Users\raj\ntuser.dat
0xfffff8a00153c010 0x00000000109ab010 \??\C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0023a5010 0x00000000579e7010 \??\C:\System Volume Information\Syscache.hve


Time Stamp: Thu Oct 15 09:56:12 2020

******* End of command output ******
```

Printkey

This command is used to display the values, data, subkeys, and data types that are present in a specified registry.

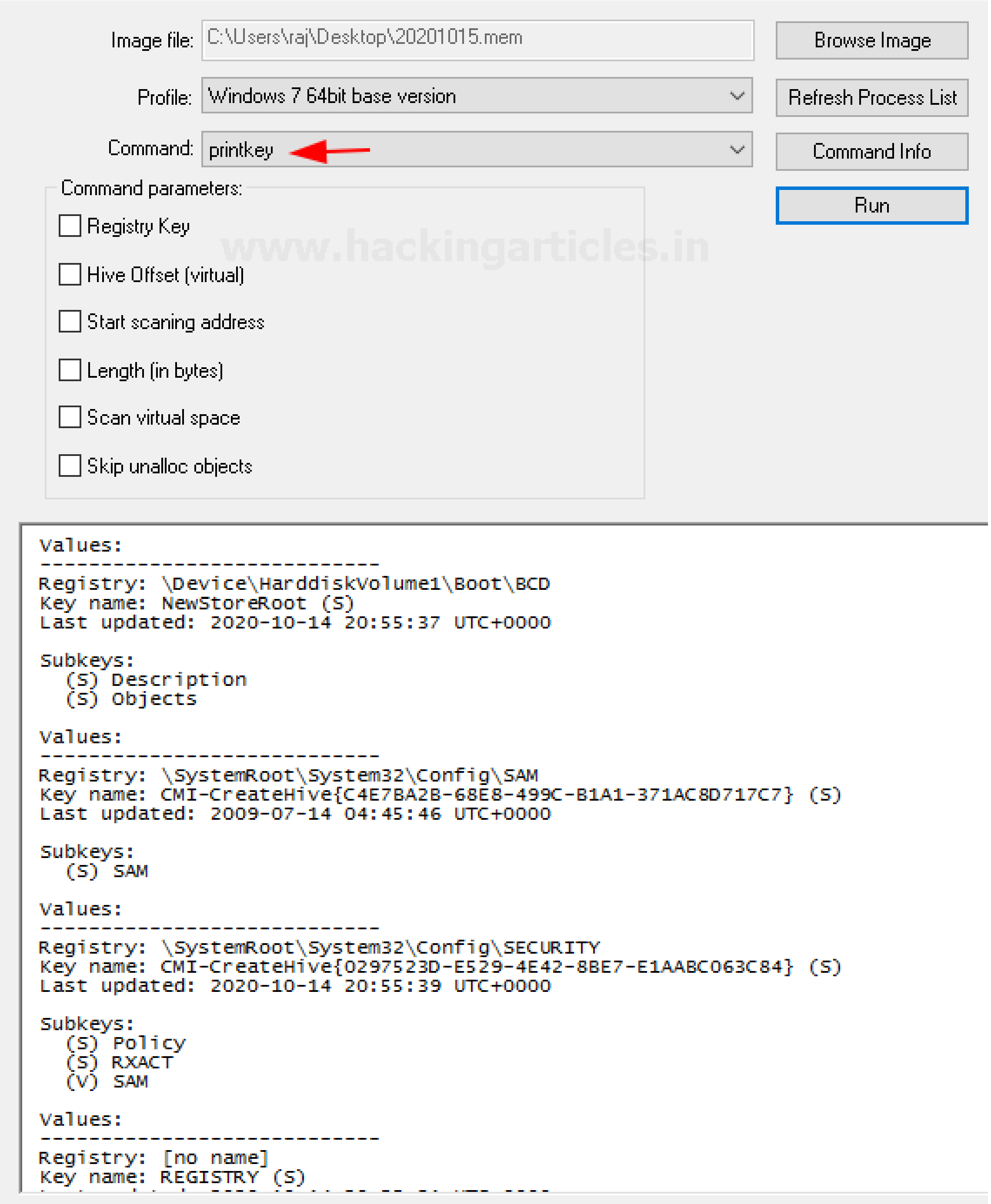


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: printkey

Command parameters:

- ☐ Registry Key
- ☐ Hive Offset (virtual)
- ☐ Start scaning address
- ☐ Length (in bytes)
- ☐ Scan virtual space
- ☐ Skip unalloc objects

```
Values:
----------------------------
Registry: \Device\HarddiskVolume1\Boot\BCD
Key name: NewStoreRoot (S)
Last updated: 2020-10-14 20:55:37 UTC+0000

Subkeys:
  (S) Description
  (S) Objects

Values:
----------------------------
Registry: \SystemRoot\System32\Config\SAM
Key name: CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7} (S)
Last updated: 2009-07-14 04:45:46 UTC+0000

Subkeys:
  (S) SAM

Values:
----------------------------
Registry: \SystemRoot\System32\Config\SECURITY
Key name: CMI-CreateHive{0297523D-E529-4E42-8BE7-E1AABC063C84} (S)
Last updated: 2020-10-14 20:55:39 UTC+0000

Subkeys:
  (S) Policy
  (S) RXACT
  (V) SAM

Values:
----------------------------
Registry: [no name]
Key name: REGISTRY (S)
```

Hashdump

This command can be used to extract and decrypt cached domain credentials stored in the registry which can be availed from the memory dump. The hashes that are availed from the memory dump can be cracked using John the Ripper, Hashcat, etc

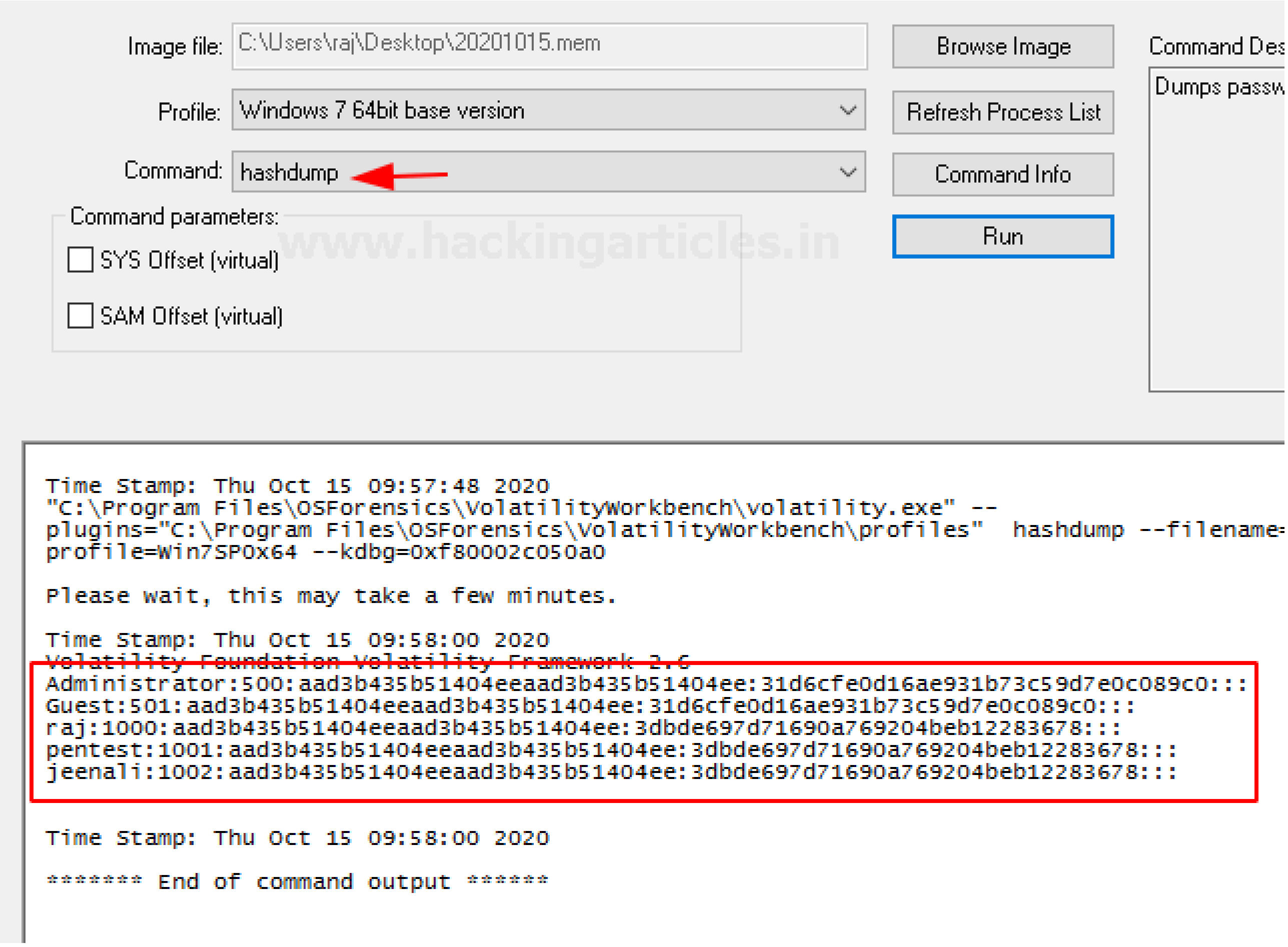


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: hashdump

Command parameters:

☐ SYS Offset (virtual)

☐ SAM Offset (virtual)

```
Time Stamp: Thu Oct 15 09:57:48 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  hashdump --filename=
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:58:00 2020
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
raj:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
pentest:1001:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
jeenali:1002:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::

Time Stamp: Thu Oct 15 09:58:00 2020

******* End of command output ******
```

Lsadump

This command is used to dump LSA secrets from the registry in the memory dump. This plugin gives out information like the default password, the RDP public key, etc.

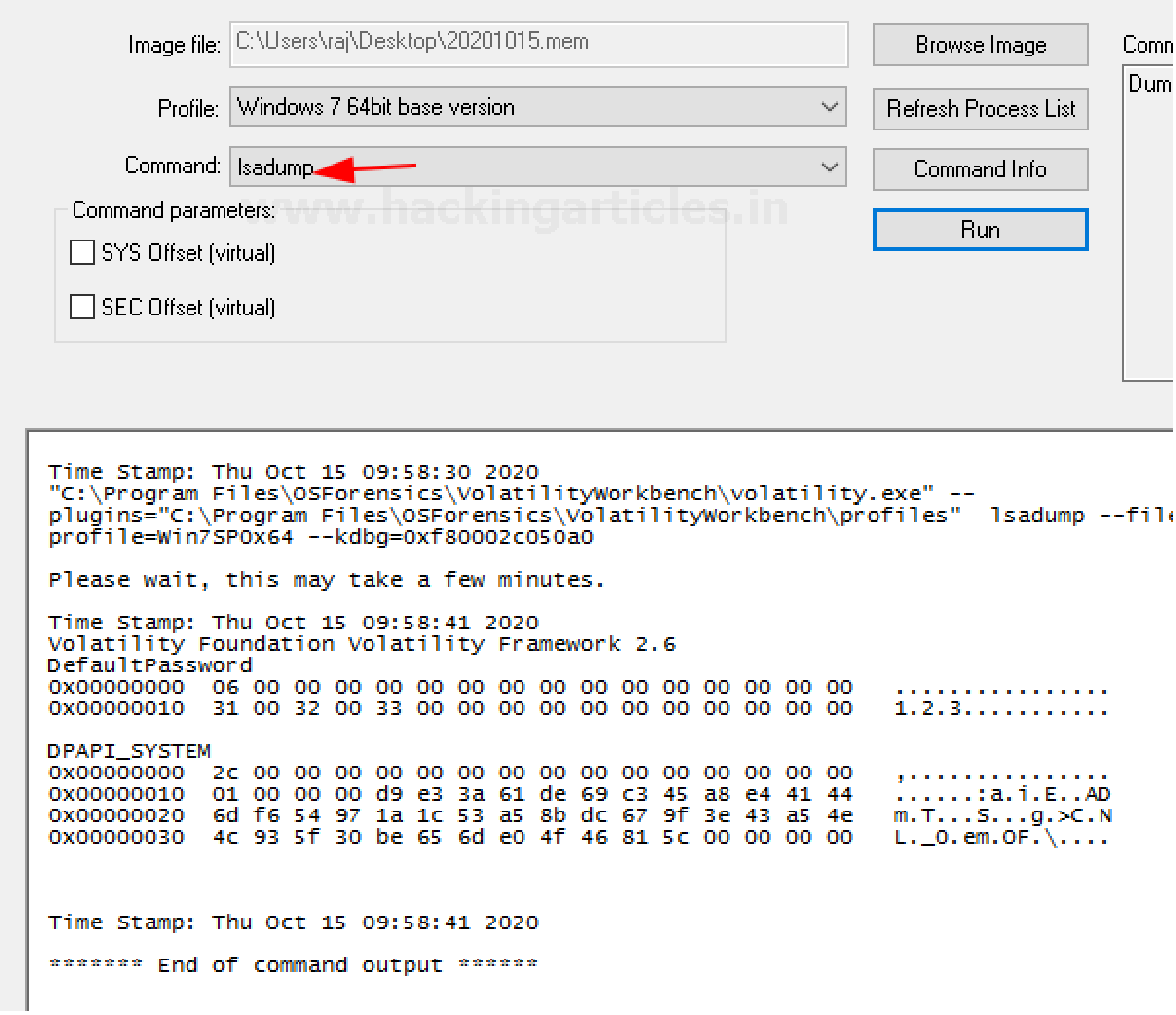


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: lsadump

Command parameters:

□ SYS Offset (virtual)

□ SEC Offset (virtual)

```
Time Stamp: Thu Oct 15 09:58:30 2020
"C:\Program Files\OSForensics\VolatilityWorkbench\volatility.exe" --
plugins="C:\Program Files\OSForensics\VolatilityWorkbench\profiles"  lsadump --fil
profile=Win7SP0x64 --kdbg=0xf80002c050a0

Please wait, this may take a few minutes.

Time Stamp: Thu Oct 15 09:58:41 2020
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000  06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  31 00 32 00 33 00 00 00 00 00 00 00 00 00 00 00   1.2.3...........

DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 d9 e3 3a 61 de 69 c3 45 a8 e4 41 44   ......:a.i.E..AD
0x00000020  6d f6 54 97 1a 1c 53 a5 8b dc 67 9f 3e 43 a5 4e   m.T...S...g.>C.N
0x00000030  4c 93 5f 30 be 65 6d e0 4f 46 81 5c 00 00 00 00   L._0.em.OF.\....



Time Stamp: Thu Oct 15 09:58:41 2020

******* End of command output ******
```

Shellbags

This command usually parses and prints the shellbag information that is obtained from the registry.

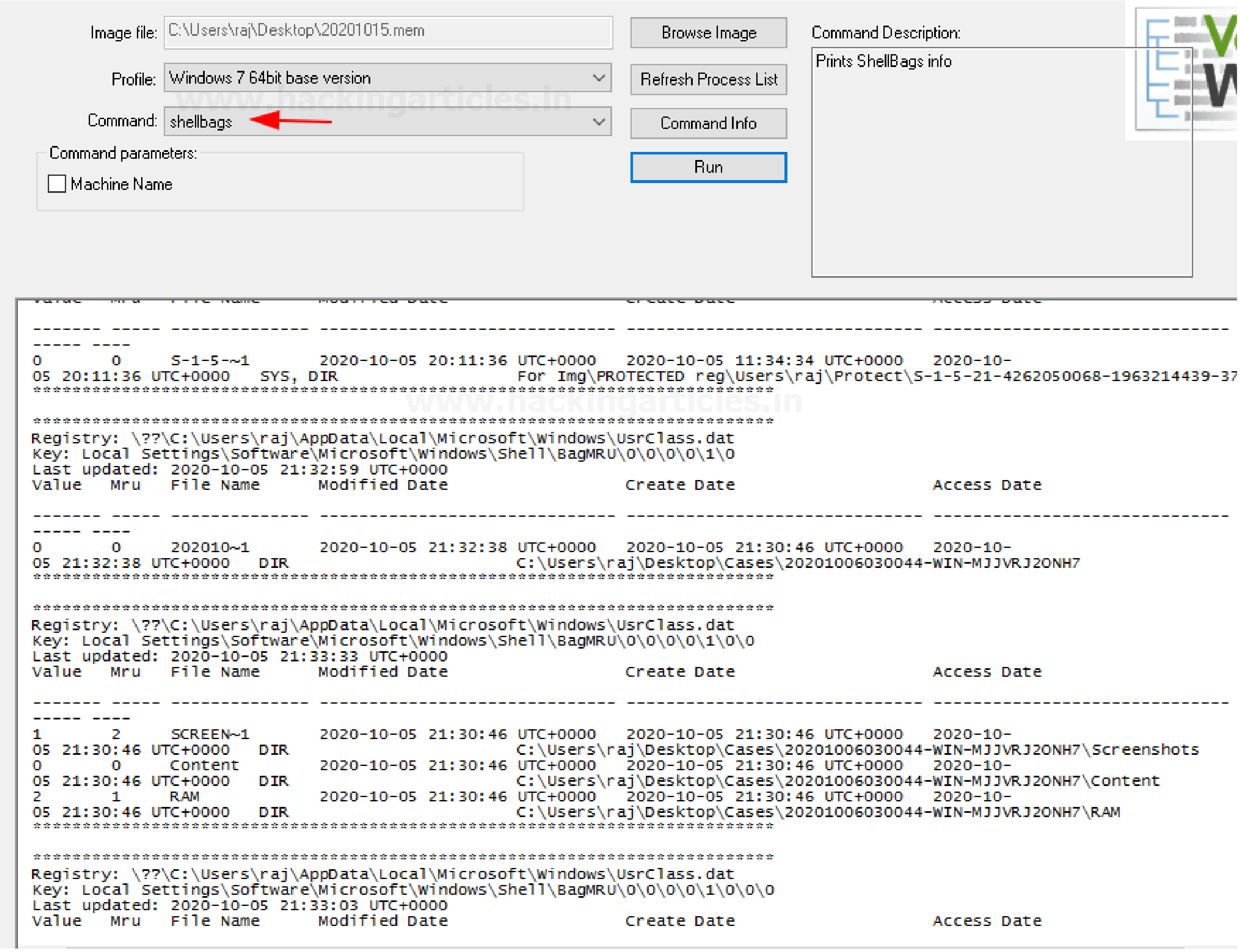


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: shellbags

Command parameters:

□ Machine Name

Command Description:

Prints ShellBags info

```
------- ----- -------------- ------------------------------ ------------------------------ ------------------------------
----- ----
0       0     S-1-5-~1       2020-10-05 20:11:36 UTC+0000   2020-10-05 11:34:34 UTC+0000   2020-10-
05 20:11:36 UTC+0000   SYS, DIR                            For Img\PROTECTED reg\Users\raj\Protect\S-1-5-21-4262050068-1963214439-37
***************************************************************************

***************************************************************************
Registry: \??\C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\1\0
Last updated: 2020-10-05 21:32:59 UTC+0000
Value   Mru   File Name      Modified Date                  Create Date                    Access Date

------- ----- -------------- ------------------------------ ------------------------------ ------------------------------
----- ----
0       0     202010~1       2020-10-05 21:32:38 UTC+0000   2020-10-05 21:30:46 UTC+0000   2020-10-
05 21:32:38 UTC+0000   DIR                                 C:\Users\raj\Desktop\Cases\20201006030044-WIN-MJJVRJ2ONH7
***************************************************************************

***************************************************************************
Registry: \??\C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\1\0\0
Last updated: 2020-10-05 21:33:33 UTC+0000
Value   Mru   File Name      Modified Date                  Create Date                    Access Date

------- ----- -------------- ------------------------------ ------------------------------ ------------------------------
----- ----
1       2     SCREEN~1       2020-10-05 21:30:46 UTC+0000   2020-10-05 21:30:46 UTC+0000   2020-10-
05 21:30:46 UTC+0000   DIR                                 C:\Users\raj\Desktop\Cases\20201006030044-WIN-MJJVRJ2ONH7\Screenshots
0       0     Content        2020-10-05 21:30:46 UTC+0000   2020-10-05 21:30:46 UTC+0000   2020-10-
05 21:30:46 UTC+0000   DIR                                 C:\Users\raj\Desktop\Cases\20201006030044-WIN-MJJVRJ2ONH7\Content
2       1     RAM            2020-10-05 21:30:46 UTC+0000   2020-10-05 21:30:46 UTC+0000   2020-10-
05 21:30:46 UTC+0000   DIR                                 C:\Users\raj\Desktop\Cases\20201006030044-WIN-MJJVRJ2ONH7\RAM
***************************************************************************

***************************************************************************
Registry: \??\C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\0\0\1\0\0\0
Last updated: 2020-10-05 21:33:03 UTC+0000
Value   Mru   File Name      Modified Date                  Create Date                    Access Date
```

Getservicesids

This command does the work of calculating the SIDz for the services that are present on the machine. The name of the services has been taken from the registry.

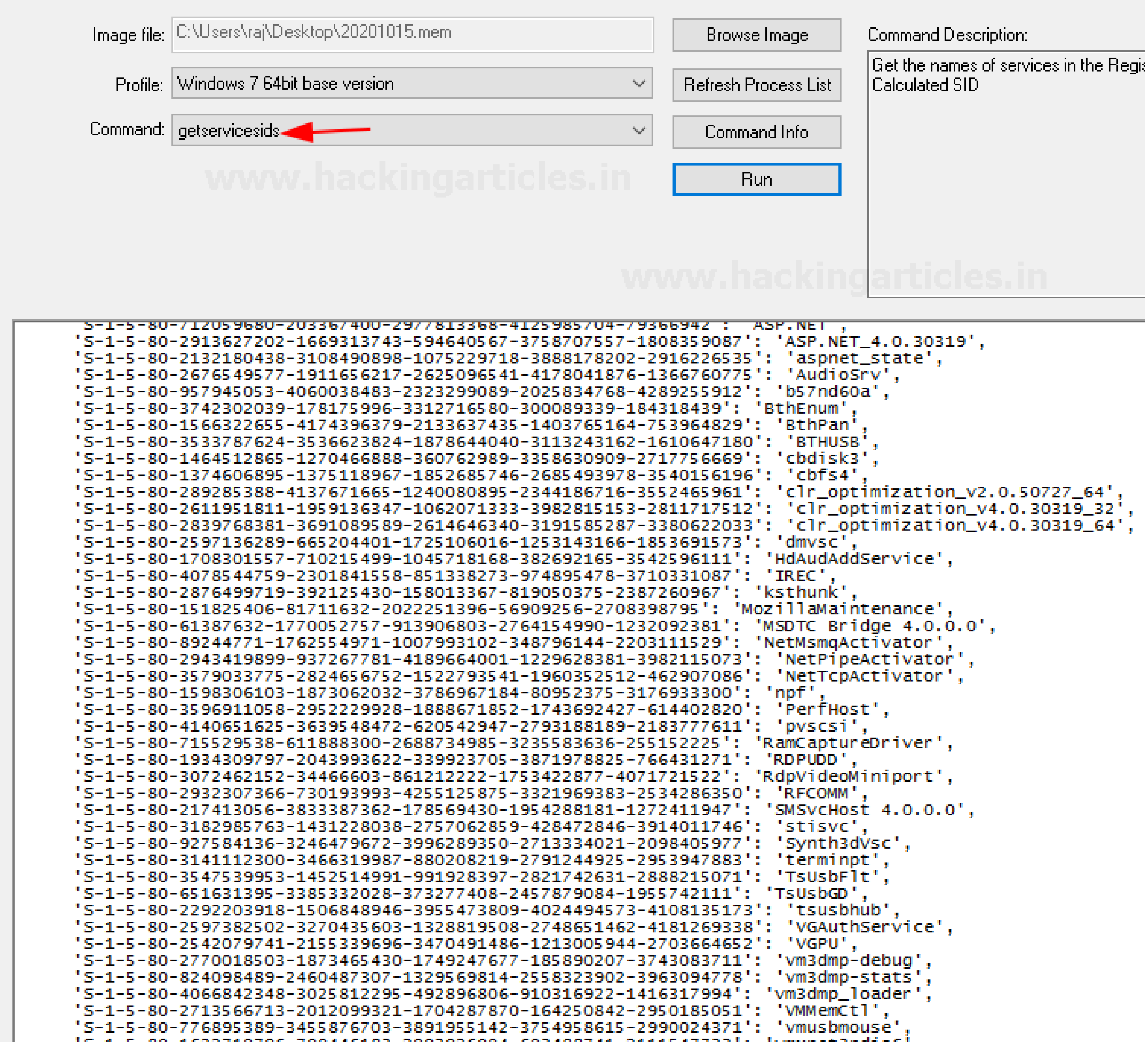


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: getservicesids

Command Description:
Get the names of services in the Regis
Calculated SID

```
'S-1-5-80-712059680-203367400-2977813368-4125985704-79366942': 'ASP.NET',
'S-1-5-80-2913627202-1669313743-594640567-3758707557-1808359087': 'ASP.NET_4.0.30319',
'S-1-5-80-2132180438-3108490898-1075229718-3888178202-2916226535': 'aspnet_state',
'S-1-5-80-2676549577-1911656217-2625096541-4178041876-1366760775': 'AudioSrv',
'S-1-5-80-957945053-4060038483-2323299089-2025834768-4289255912': 'b57nd60a',
'S-1-5-80-3742302039-178175996-3312716580-300089339-184318439': 'BthEnum',
'S-1-5-80-1566322655-4174396379-2133637435-1403765164-753964829': 'BthPan',
'S-1-5-80-3533787624-3536623824-1878644040-3113243162-1610647180': 'BTHUSB',
'S-1-5-80-1464512865-1270466888-360762989-3358630909-2717756669': 'cbdisk3',
'S-1-5-80-1374606895-1375118967-1852685746-2685493978-3540156196': 'cbfs4',
'S-1-5-80-289285388-4137671665-1240080895-2344186716-3552465961': 'clr_optimization_v2.0.50727_64',
'S-1-5-80-2611951811-1959136347-1062071333-3982815153-2811717512': 'clr_optimization_v4.0.30319_32',
'S-1-5-80-2839768381-3691089589-2614646340-3191585287-3380622033': 'clr_optimization_v4.0.30319_64',
'S-1-5-80-2597136289-665204401-1725106016-1253143166-1853691573': 'dmvsc',
'S-1-5-80-1708301557-710215499-1045718168-382692165-3542596111': 'HdAudAddService',
'S-1-5-80-4078544759-2301841558-851338273-974895478-3710331087': 'IREC',
'S-1-5-80-2876499719-392125430-158013367-819050375-2387260967': 'ksthunk',
'S-1-5-80-151825406-81711632-2022251396-56909256-2708398795': 'MozillaMaintenance',
'S-1-5-80-61387632-1770052757-913906803-2764154990-1232092381': 'MSDTC Bridge 4.0.0.0',
'S-1-5-80-89244771-1762554971-1007993102-348796144-2203111529': 'NetMsmqActivator',
'S-1-5-80-2943419899-937267781-4189664001-1229628381-3982115073': 'NetPipeActivator',
'S-1-5-80-3579033775-2824656752-1522793541-1960352512-462907086': 'NetTcpActivator',
'S-1-5-80-1598306103-1873062032-3786967184-80952375-3176933300': 'npf',
'S-1-5-80-3596911058-2952229928-1888671852-1743692427-614402820': 'PerfHost',
'S-1-5-80-4140651625-3639548472-620542947-2793188189-2183777611': 'pvscsi',
'S-1-5-80-715529538-611888300-2688734985-3235583636-255152225': 'RamCaptureDriver',
'S-1-5-80-1934309797-2043993622-339923705-3871978825-766431271': 'RDPUDD',
'S-1-5-80-3072462152-34466603-861212222-1753422877-4071721522': 'RdpVideoMiniport',
'S-1-5-80-2932307366-730193993-4255125875-3321969383-2534286350': 'RFCOMM',
'S-1-5-80-217413056-3833387362-178569430-1954288181-1272411947': 'SMSvcHost 4.0.0.0',
'S-1-5-80-3182985763-1431228038-2757062859-428472846-3914011746': 'stisvc',
'S-1-5-80-927584136-3246479672-3996289350-2713334021-2098405977': 'Synth3dVsc',
'S-1-5-80-3141112300-3466319987-880208219-2791244925-2953947883': 'terminpt',
'S-1-5-80-3547539953-1452514991-991928397-2821742631-2888215071': 'TsUsbFlt',
'S-1-5-80-651631395-3385332028-373277408-2457879084-1955742111': 'TsUsbGD',
'S-1-5-80-2292203918-1506848946-3955473809-4024494573-4108135173': 'tsusbhub',
'S-1-5-80-2597382502-3270435603-1328819508-2748651462-4181269338': 'VGAuthService',
'S-1-5-80-2542079741-2155339696-3470491486-1213005944-2703664652': 'VGPU',
'S-1-5-80-2770018503-1873465430-1749247677-185890207-3743083711': 'vm3dmp-debug',
'S-1-5-80-824098489-2460487307-1329569814-2558323902-3963094778': 'vm3dmp-stats',
'S-1-5-80-4066842348-3025812295-492896806-910316922-1416317994': 'vm3dmp_loader',
'S-1-5-80-2713566713-2012099321-1704287870-164250842-2950185051': 'VMMemCtl',
'S-1-5-80-776895389-3455876703-3891955142-3754958615-2990024371': 'vmusbmouse',
```

Dumpregistry

This plugin allows one to dump a registry hive into a disk location.

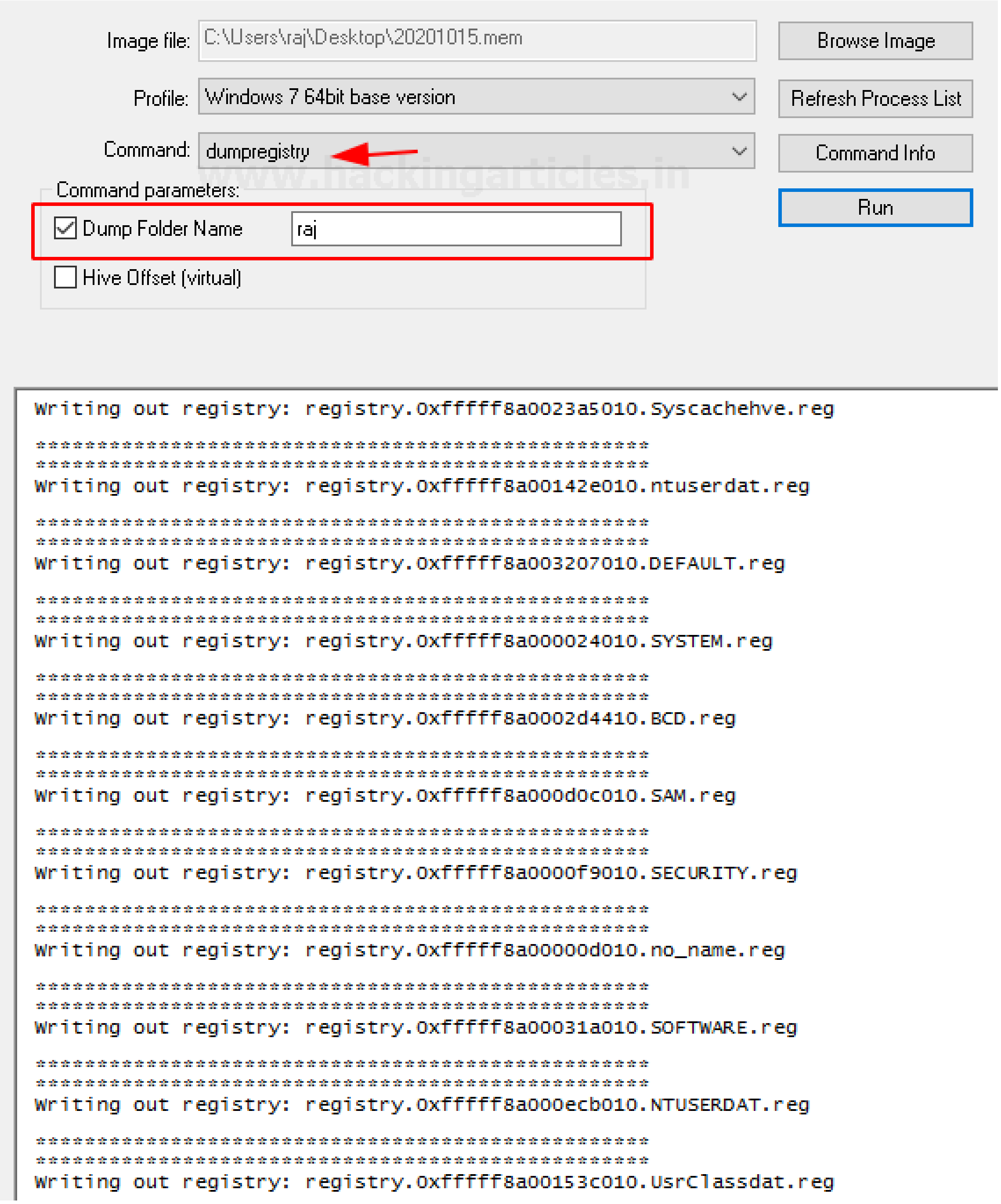


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: dumpregistry

Command parameters:

☑ Dump Folder Name raj

☐ Hive Offset (virtual)

```
Writing out registry: registry.0xfffff8a0023a5010.Syscachehve.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a00142e010.ntuserdat.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a003207010.DEFAULT.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a000024010.SYSTEM.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a0002d4410.BCD.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a000d0c010.SAM.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a0000f9010.SECURITY.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a00000d010.no_name.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a00031a010.SOFTWARE.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a000ecb010.NTUSERDAT.reg

**************************************************
**************************************************
Writing out registry: registry.0xfffff8a00153c010.UsrClassdat.reg
```

Mbrparser

This command scans and parses potential MBR from the memory dump. There are various ways to find MBR and the way of filtering it.

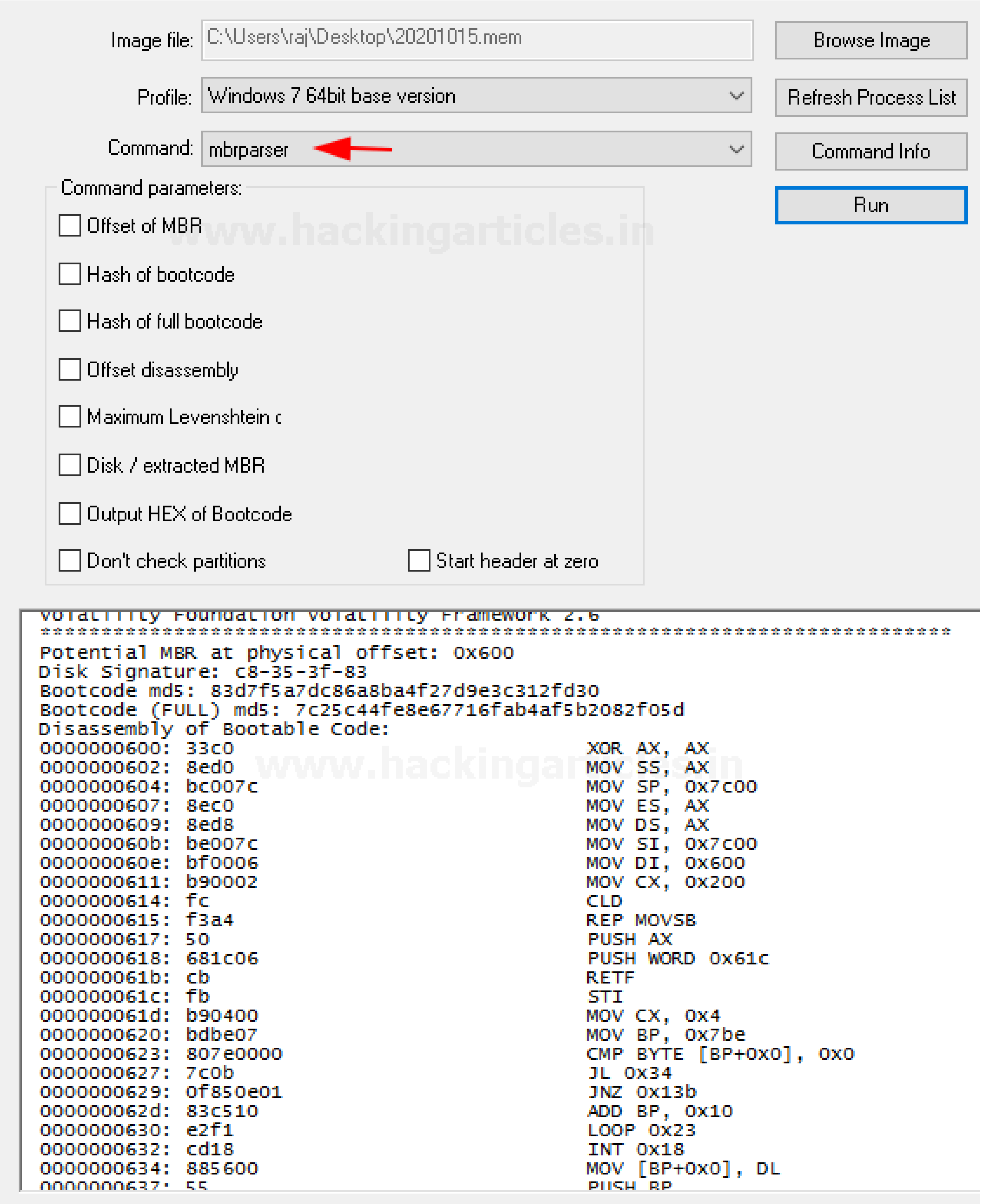


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: mbrparser

Command parameters:

□ Offset of MBR

□ Hash of bootcode

□ Hash of full bootcode

□ Offset disassembly

□ Maximum Levenshtein c

□ Disk / extracted MBR

□ Output HEX of Bootcode

□ Don't check partitions □ Start header at zero

```
Volatility Foundation Volatility Framework 2.6
***************************************************************************
Potential MBR at physical offset: 0x600
Disk Signature: c8-35-3f-83
Bootcode md5: 83d7f5a7dc86a8ba4f27d9e3c312fd30
Bootcode (FULL) md5: 7c25c44fe8e67716fab4af5b2082f05d
Disassembly of Bootable Code:
0000000600: 33c0                            XOR AX, AX
0000000602: 8ed0                            MOV SS, AX
0000000604: bc007c                          MOV SP, 0x7c00
0000000607: 8ec0                            MOV ES, AX
0000000609: 8ed8                            MOV DS, AX
000000060b: be007c                          MOV SI, 0x7c00
000000060e: bf0006                          MOV DI, 0x600
0000000611: b90002                          MOV CX, 0x200
0000000614: fc                              CLD
0000000615: f3a4                            REP MOVSB
0000000617: 50                              PUSH AX
0000000618: 681c06                          PUSH WORD 0x61c
000000061b: cb                              RETF
000000061c: fb                              STI
000000061d: b90400                          MOV CX, 0x4
0000000620: bdbe07                          MOV BP, 0x7be
0000000623: 807e0000                        CMP BYTE [BP+0x0], 0x0
0000000627: 7c0b                            JL 0x34
0000000629: 0f850e01                        JNZ 0x13b
000000062d: 83c510                          ADD BP, 0x10
0000000630: e2f1                            LOOP 0x23
0000000632: cd18                            INT 0x18
0000000634: 885600                          MOV [BP+0x0], DL
0000000637: 55                              PUSH BP
```

Mftparser

This command is used to scan the MFT entries in the memory dump and prints out the information for certain types of file attributes.

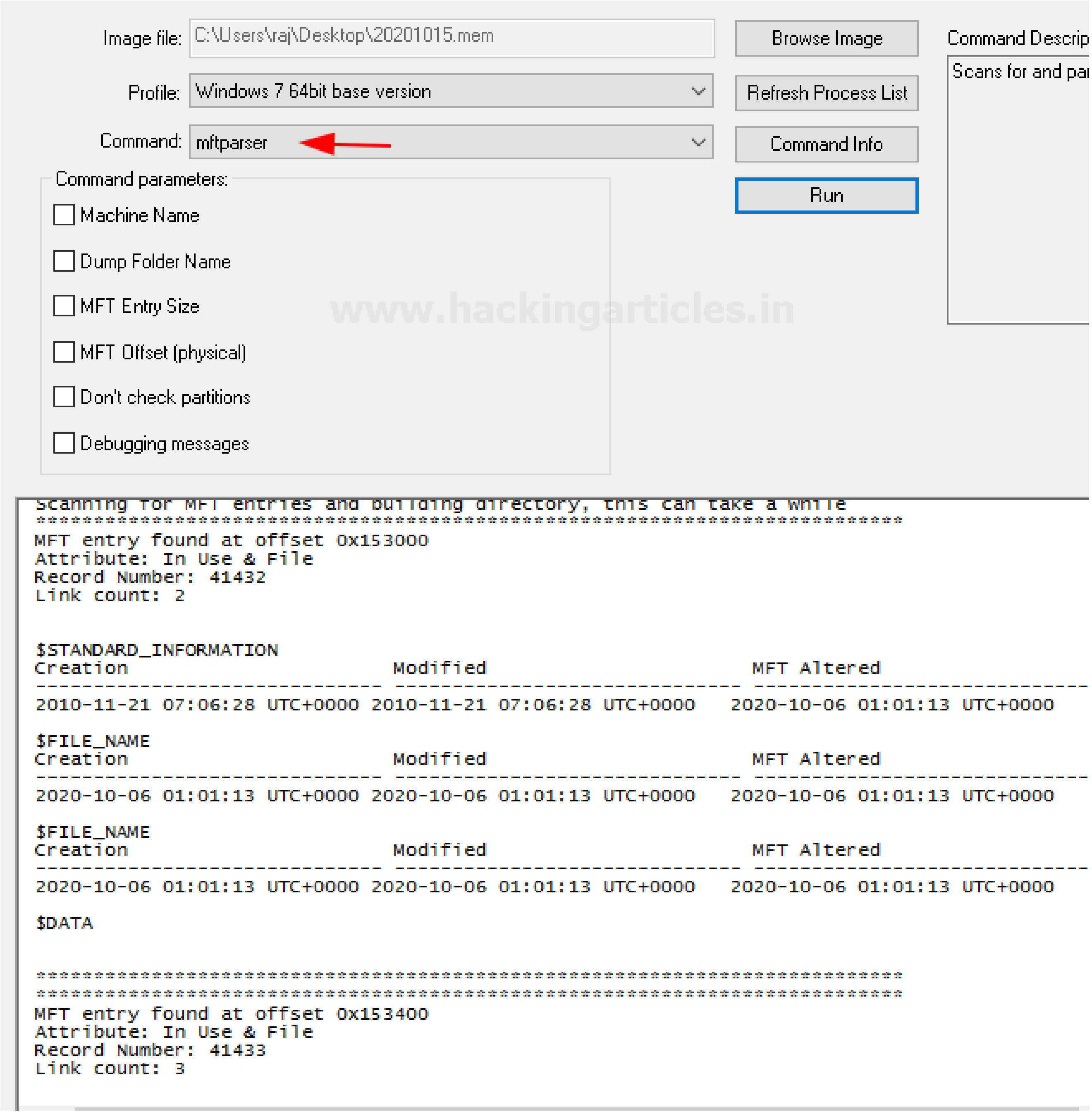


Image file: C:\Users\raj\Desktop\20201015.mem

Profile: Windows 7 64bit base version

Command: mftparser

Command parameters:

- □ Machine Name
- □ Dump Folder Name
- □ MFT Entry Size
- □ MFT Offset (physical)
- □ Don't check partitions
- □ Debugging messages

```
Scanning for MFT entries and building directory, this can take a while
***************************************************************************
MFT entry found at offset 0x153000
Attribute: In Use & File
Record Number: 41432
Link count: 2


$STANDARD_INFORMATION
Creation                       Modified                       MFT Altered
------------------------------ ------------------------------ ------------------------------
2010-11-21 07:06:28 UTC+0000 2010-11-21 07:06:28 UTC+0000   2020-10-06 01:01:13 UTC+0000

$FILE_NAME
Creation                       Modified                       MFT Altered
------------------------------ ------------------------------ ------------------------------
2020-10-06 01:01:13 UTC+0000 2020-10-06 01:01:13 UTC+0000   2020-10-06 01:01:13 UTC+0000

$FILE_NAME
Creation                       Modified                       MFT Altered
------------------------------ ------------------------------ ------------------------------
2020-10-06 01:01:13 UTC+0000 2020-10-06 01:01:13 UTC+0000   2020-10-06 01:01:13 UTC+0000

$DATA


***************************************************************************
***************************************************************************
MFT entry found at offset 0x153400
Attribute: In Use & File
Record Number: 41433
Link count: 3
```