IMAGE IDENFICATION

When we started analyzing any memory dump, we must identify the type of the image so we can use ”imageinfo” commend to identify the following things.

1- Identify the operating system
2- Identify hardware architecture (32 or 64 bit)
3- Identify service pack
3- Identify time that the sample was collected
4- Identify the DTB address

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64,
Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\MemoryForensics\MemoryDump.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a30120L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a32000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2021-07-29 17:57:58 UTC+0000
     Image local date and time : 2021-07-29 19:57:58 +0200
```

Figure 1 image identification

From the output of “imageinfo”, we can identify the suggested profile and suggested profile is very important as we can use it with other plugins.

PROCESSES CHECK

We can identify the correct profile from the previous figure 1, now we can start analyze the processes of the memory dump.

PSLIST COMMAND

To get all processes on a system, we can use “pslist” command and we can extract all processes on a system by running it on Memory Dump and get information about the following thing

1- The offset
2- Process name
3- Process ID
4- Parent process ID
5- Number of threads

6- Number of the handles
7- Data and time when process started or exited

We can see all processes on a system in the next figure and identify the previous information about every process so let us see the results in the next figure 2.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
 Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
 ------------------------------
0xfffffa800069b860 System                    4      0     92      563 ------      0 2021-07-28 21:10:24 UTC+0000
0xfffffa8003f50450 smss.exe                268      4      2       29 ------      0 2021-07-28 21:10:24 UTC+0000
0xfffffa8002479060 csrss.exe               352    344      9      489      0      0 2021-07-28 21:10:28 UTC+0000
0xfffffa8001b31060 wininit.exe             392    344      3       76      0      0 2021-07-28 21:10:28 UTC+0000
0xfffffa8002458880 csrss.exe               404    384     10      243      1      0 2021-07-28 21:10:28 UTC+0000
0xfffffa80025fe8e0 services.exe            452    392      9      237      0      0 2021-07-28 21:10:29 UTC+0000
0xfffffa8002631360 lsass.exe               460    392      7      628      0      0 2021-07-28 21:10:29 UTC+0000
0xfffffa8002649b00 lsm.exe                 468    392     10      150      0      0 2021-07-28 21:10:29 UTC+0000
0xfffffa800262ea40 winlogon.exe            496    384      5      119      1      0 2021-07-28 21:10:29 UTC+0000
0xfffffa80027c4b00 svchost.exe             620    452     11      368      0      0 2021-07-28 21:10:30 UTC+0000
0xfffffa80027e4360 svchost.exe             688    452      9      301      0      0 2021-07-28 21:10:30 UTC+0000
0xfffffa8002805b00 svchost.exe             736    452     20      488      0      0 2021-07-28 21:10:30 UTC+0000
0xfffffa8002858b00 svchost.exe             848    452     20      481      0      0 2021-07-28 21:10:31 UTC+0000
0xfffffa800289c5f0 svchost.exe             900    452     15      364      0      0 2021-07-28 21:10:31 UTC+0000
0xfffffa80028a9320 svchost.exe             944    452     41     1188      0      0 2021-07-28 21:10:31 UTC+0000
0xfffffa800296eb00 svchost.exe             984    452     18      508      0      0 2021-07-28 21:10:34 UTC+0000
0xfffffa80029d3b00 dwm.exe                1132    848      3       74      1      0 2021-07-28 21:10:34 UTC+0000
0xfffffa80029dab00 explorer.exe           1144   1124     53     1093      1      0 2021-07-28 21:10:34 UTC+0000
0xfffffa8002a11610 spoolsv.exe            1204    452     13      304      0      0 2021-07-28 21:10:35 UTC+0000
0xfffffa8002a39b00 svchost.exe            1264    452     19      329      0      0 2021-07-28 21:10:35 UTC+0000
0xfffffa8002a775f0 vm3dservice.ex         1304   1144      2       45      1      0 2021-07-28 21:10:35 UTC+0000
0xfffffa8002a434f0 vmtoolsd.exe           1312   1144      8      229      1      0 2021-07-28 21:10:35 UTC+0000
0xfffffa8002a71270 taskhost.exe           1324    452     11      276      1      0 2021-07-28 21:10:35 UTC+0000
0xfffffa8002abdb00 svchost.exe            1496    452     10      149      0      0 2021-07-28 21:10:37 UTC+0000
0xfffffa80020731d0 VGAuthService.         1632    452      3       89      0      0 2021-07-28 21:10:37 UTC+0000
0xfffffa800228b1f0 vmtoolsd.exe           1704    452     11      294      0      0 2021-07-28 21:10:38 UTC+0000
0xfffffa800225b510 WmiPrvSE.exe            844    620     10      307      0      0 2021-07-28 21:10:40 UTC+0000
0xfffffa80023a07c0 msdtc.exe              2332    452     12      147      0      0 2021-07-28 21:10:52 UTC+0000
0xfffffa800275d060 mscorsvw.exe           2184    452      5      103      0      1 2021-07-28 21:13:22 UTC+0000
0xfffffa8002a517f0 svchost.exe            2292    452      7      115      0      0 2021-07-28 21:13:22 UTC+0000
0xfffffa80039975f0 mscorsvw.exe           2084    452      5       95      0      0 2021-07-28 21:13:23 UTC+0000
```

Figure 2 list all processes

From the previous figure 2, we can identify a lot of information about every process such as the offset of the process, the name of the process, the ID of the process, the ID of parent process, the number of threads. The number of the handles and the date and time of the process when it started or exited.

Now we will show the processes that generated by “pslist” command and identify malicious process that can do malicious acts on a system and we can see the results in the following figure 3.

```
0xfffffa800276c750 sppsvc.exe             2696    452      5      155      0      0 2021-07-28 21:13:24 UTC+0000
0xfffffa80028b62b0 svchost.exe            2236    452     14      401      0      0 2021-07-28 21:13:25 UTC+0000
0xfffffa80012c6590 msiexec.exe            3492    452      5     2917      0      0 2021-07-29 07:29:17 UTC+0000
0xfffffa80025b6730 OSPPSVC.EXE            3656    452      3      150      0      0 2021-07-29 07:30:11 UTC+0000
0xfffffa8000e9a5f0 TrustedInstall         2760    452      4      132      0      0 2021-07-29 07:30:14 UTC+0000
0xfffffa8000f80b00 WmiPrvSE.exe           2416    620      5      106      0      0 2021-07-29 07:30:18 UTC+0000
0xfffffa80023a2240 SearchIndexer.         3352    452     11      622      0      0 2021-07-29 07:34:12 UTC+0000
0xfffffa80007df060 srvany.exe              660    452      2       39      0      1 2021-07-29 07:34:15 UTC+0000
0xfffffa8000f7e060 KMService.exe          3712    660      3       55      0      1 2021-07-29 07:34:15 UTC+0000
0xfffffa8000f39120 conhost.exe            2504    352      2       33      0      0 2021-07-29 07:34:15 UTC+0000
0xfffffa8000ed1250 SearchProtocol         2780   3352      7      328      0      0 2021-07-29 07:39:21 UTC+0000
0xfffffa8001b5a4d0 SearchFilterHo         3376   3352      5      126      0      0 2021-07-29 07:39:21 UTC+0000
0xfffffa8000ede1d0 audiodg.exe            3416    736      6      135      0      0 2021-07-29 07:39:29 UTC+0000
0xfffffa800191e110 taskhost.exe           2112    452      9      164      0      0 2021-07-29 17:56:01 UTC+0000
0xfffffa8001ac9060 wcryv2.exe              580    452     28      207      0      1 2021-07-29 17:57:27 UTC+0000
0xfffffa8001bce290 tasksche.exe           2328   3924      1       31      1      1 2021-07-29 17:57:30 UTC+0000
0xfffffa8000ed8b00 cmd.exe                3400    452      1       21      0      0 2021-07-29 17:57:30 UTC+0000
0xfffffa80019b7b00 tasksche.exe           3968   3400      8       81      0      1 2021-07-29 17:57:30 UTC+0000
```

Figure 3 list processes

In the figure 3, we can see the processes that generated by “pslist” command and we can see the process Wcryv2.exe which has PID (580), PPID (452), Thds (28) and Hnds (207) is stranger than legitimated processes so I will search in Google by name of the process and we can see the results in the next figure 4.

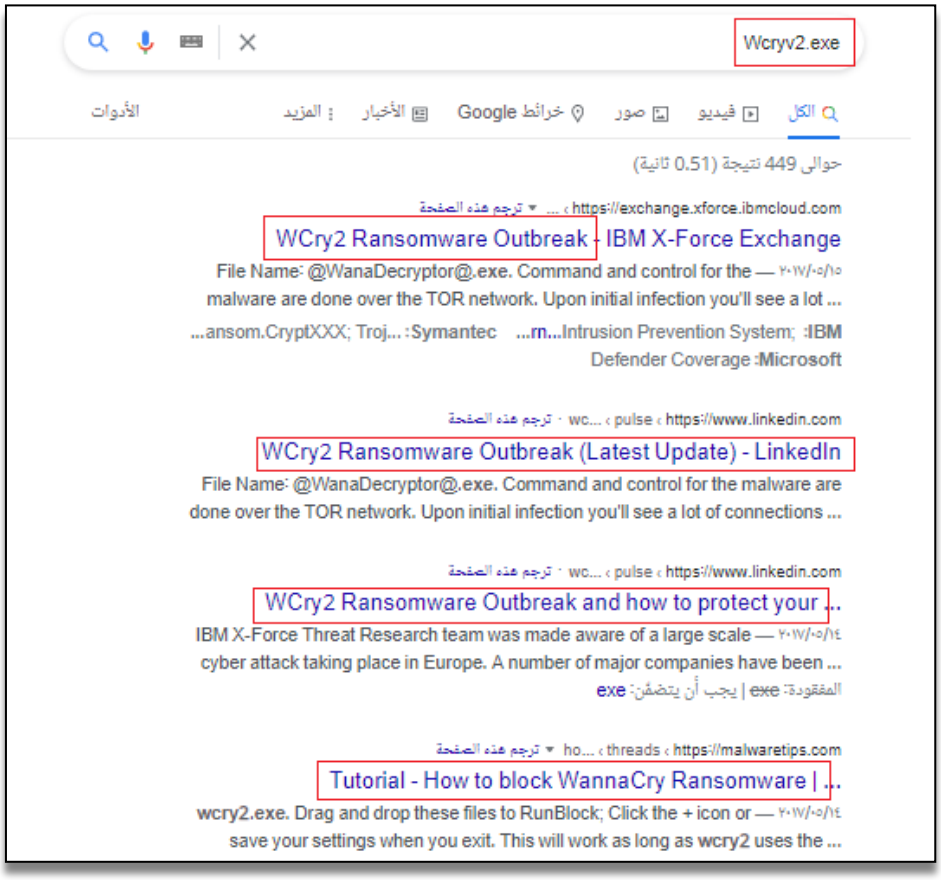
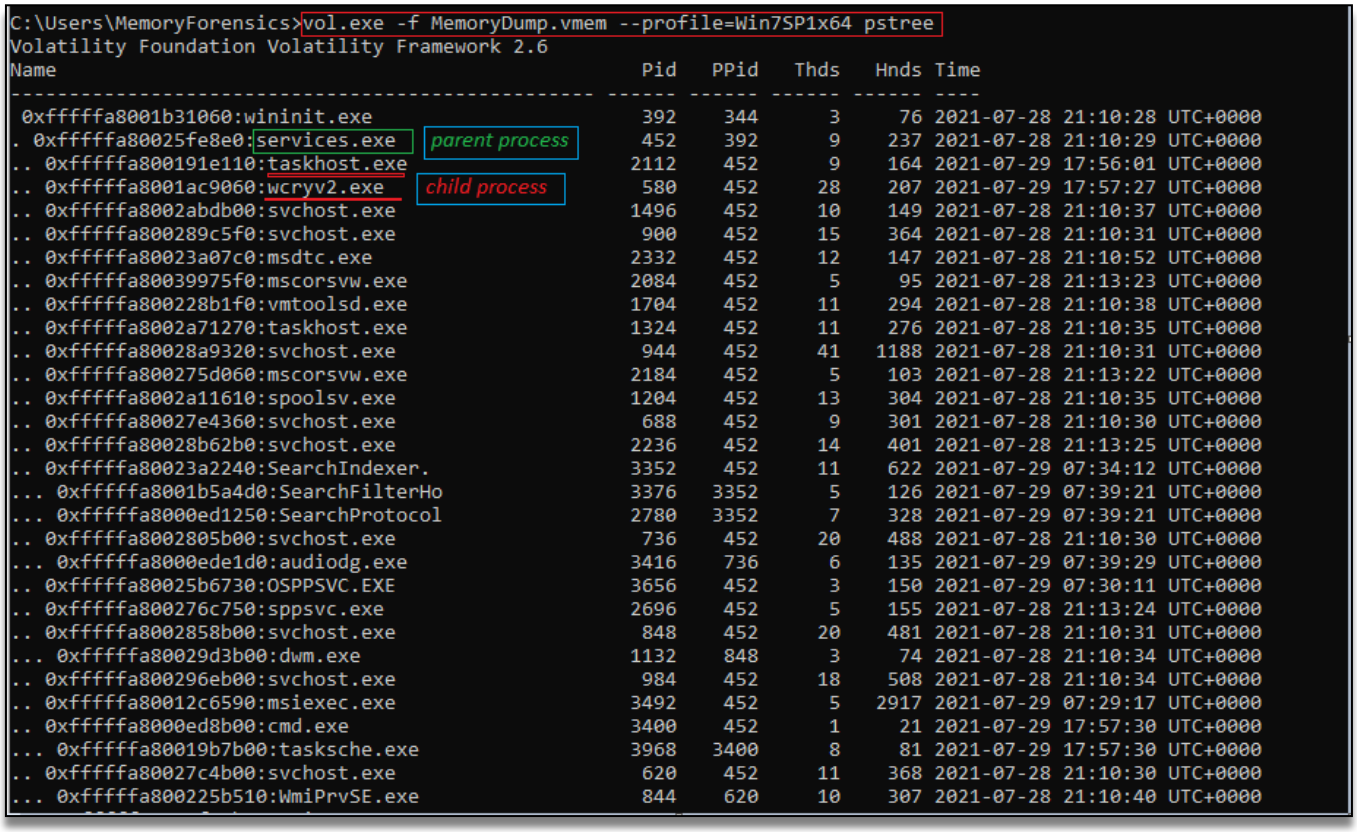


Figure 4 searching about process

From searching about the process, we can identify that the process is used by WannaCry ransomware to encrypt files on the system.

PSTREE COMMEND

When examining the processes, it is very important to know what the parent process and child process which executing under the parent process. One indicator of system compromised is identification of a process that executes outside the normal parent or child process used to inject malicious code into legitimated process like explorer.exe process so we should use "pstree" command to see parent process and child process. And we can see the results in the next figure 4.



Name	Pid	PPid	Thds	Hnds	Time
0xfffffa8001b31060:wininit.exe	392	344	3	76	2021-07-28 21:10:28 UTC+0000
. 0xfffffa80025fe8e0:services.exe	452	392	9	237	2021-07-28 21:10:29 UTC+0000
.. 0xfffffa800191e110:taskhost.exe	2112	452	9	164	2021-07-29 17:56:01 UTC+0000
.. 0xfffffa8001ac9060:wcryv2.exe	580	452	28	207	2021-07-29 17:57:27 UTC+0000
.. 0xfffffa8002abdb00:svchost.exe	1496	452	10	149	2021-07-28 21:10:37 UTC+0000
.. 0xfffffa800289c5f0:svchost.exe	900	452	15	364	2021-07-28 21:10:31 UTC+0000
.. 0xfffffa80023a07c0:msdtc.exe	2332	452	12	147	2021-07-28 21:10:52 UTC+0000
.. 0xfffffa80039975f0:mscorsvw.exe	2084	452	5	95	2021-07-28 21:13:23 UTC+0000
.. 0xfffffa800228b1f0:vmtoolsd.exe	1704	452	11	294	2021-07-28 21:10:38 UTC+0000
.. 0xfffffa8002a71270:taskhost.exe	1324	452	11	276	2021-07-28 21:10:35 UTC+0000
.. 0xfffffa80028a9320:svchost.exe	944	452	41	1188	2021-07-28 21:10:31 UTC+0000
.. 0xfffffa800275d060:mscorsvw.exe	2184	452	5	103	2021-07-28 21:13:22 UTC+0000
.. 0xfffffa8002a11610:spoolsv.exe	1204	452	13	304	2021-07-28 21:10:35 UTC+0000
.. 0xfffffa80027e4360:svchost.exe	688	452	9	301	2021-07-28 21:10:30 UTC+0000
.. 0xfffffa80028b62b0:svchost.exe	2236	452	14	401	2021-07-28 21:13:25 UTC+0000
.. 0xfffffa80023a2240:SearchIndexer.	3352	452	11	622	2021-07-29 07:34:12 UTC+0000
... 0xfffffa8001b5a4d0:SearchFilterHo	3376	3352	5	126	2021-07-29 07:39:21 UTC+0000
... 0xfffffa8000ed1250:SearchProtocol	2780	3352	7	328	2021-07-29 07:39:21 UTC+0000
.. 0xfffffa8002805b00:svchost.exe	736	452	20	488	2021-07-28 21:10:30 UTC+0000
... 0xfffffa8000ede1d0:audiodg.exe	3416	736	6	135	2021-07-29 07:39:29 UTC+0000
.. 0xfffffa80025b6730:OSPPSVC.EXE	3656	452	3	150	2021-07-29 07:30:11 UTC+0000
.. 0xfffffa800276c750:sppsvc.exe	2696	452	5	155	2021-07-28 21:13:24 UTC+0000
.. 0xfffffa8002858b00:svchost.exe	848	452	20	481	2021-07-28 21:10:31 UTC+0000
... 0xfffffa80029d3b00:dwm.exe	1132	848	3	74	2021-07-28 21:10:34 UTC+0000
.. 0xfffffa800296eb00:svchost.exe	984	452	18	508	2021-07-28 21:10:34 UTC+0000
.. 0xfffffa80012c6590:msiexec.exe	3492	452	5	2917	2021-07-29 07:29:17 UTC+0000
.. 0xfffffa8000ed8b00:cmd.exe	3400	452	1	21	2021-07-29 17:57:30 UTC+0000
... 0xfffffa80019b7b00:tasksche.exe	3968	3400	8	81	2021-07-29 17:57:30 UTC+0000
.. 0xfffffa80027c4b00:svchost.exe	620	452	11	368	2021-07-28 21:10:30 UTC+0000
... 0xfffffa800225b510:WmiPrvSE.exe	844	620	10	307	2021-07-28 21:10:40 UTC+0000

Figure 5 running pstree command

From the previous figure 5, we can take example about parent process and child process so the parent process is Services.exe which has PID (452) and child process is Wcryv.exe which has PID (580) and we know that Wcreyv.exe is malicious process that execute under Services.exe to encrypt file on a system.

DLL COMMAND

We will check the loaded DLL files that associated with the Wcreyv.exe process and this will help us to determine if malicious process has access files when it was executed on a system and we can see the files associated to Wcreyv.exe to examine the DLL files and we can see the results in the next figure 7.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 -p 580 dlllist
Volatility Foundation Volatility Framework 2.6
************************************************************************
wcryv2.exe pid:    580
Command line : C:\Users\windows_7\Desktop\wcryv2.bin\wcryv2.exe -m security
Note: use ldrmodules for listing DLLs in Wow64 processes


Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x0000000000400000           0x66b000             0xffff C:\Users\windows_7\Desktop\wcryv2.bin\wcryv2.exe
0x0000000077880000           0x19f000             0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000074970000            0x3f000                0x3 C:\Windows\SYSTEM32\wow64.dll
0x0000000074910000            0x5c000                0x1 C:\Windows\SYSTEM32\wow64win.dll
0x000000000749e0000             0x8000                0x1 C:\Windows\SYSTEM32\wow64cpu.dll
```

Figure 6 examine DLL files with process Wcreyv.exe

From the previous figure 6, we can see that process Wcreyv.exe loads the following DLL file when it was executed on a system.

- C:\Users\windows_7\Desktop\wcryv2.bin\wcryv2.exe
- C:\Windows\SYSTEM32\ntdll.dll
- C:\Windows\SYSTEM32\wow64win.dll
- C:\Windows\SYSTEM32\wow64cpu.dll

We see that process when it was started, it connected with wcryv2.exe and loaded DLL files likeas ntdll.dll, wow64.dll, wow64win.dll and wow64cpu.dll.

HANDLES COMMAND

The handles plugin can help us to view the files associated with the process and get information about registry key and we can see the handles that associated with process Wcreyv.exe that has PID (580).

We can see the results in the following Figure 7.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 -p 580 handles
Volatility Foundation Volatility Framework 2.6
Offset(V)          Pid      Handle              Access Type            Details
------------------ ------ ------------------ ------------------ ---------------- -------
0xfffff8a0026a7260    580                0x4                0x9 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffff8a0005d4760    580                0x8                0x3 Directory        KnownDlls
0xfffff8a000680ea0    580                0xc                0x3 Directory        KnownDlls32
0xfffffa8002830600    580               0x10           0x100020 File             \Device\HarddiskVolume1\Windows
0xfffff8a0024f87f0    580               0x14                0x9 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffff8a000680ea0    580               0x18                0x3 Directory        KnownDlls32
0xfffffa8003f15950    580               0x1c           0x100020 File             \Device\HarddiskVolume1\Windows\SysWOW64
0xfffff8a00197ec40    580               0x20            0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
0xfffffa8001509940    580               0x24           0x100003 Semaphore
0xfffffa80022b1480    580               0x28           0x1f0001 ALPC Port
0xfffffa80017b1840    580               0x2c           0x100003 Semaphore
0xfffffa8000f6a270    580               0x30           0x1f0001 Mutant
0xfffffa8001caa060    580               0x34           0x1f0001 Mutant
0xfffff8a002209ad0    580               0x38            0xf003f Key              MACHINE
0xfffffa8002319200    580               0x3c           0x1f0003 Event
0xfffff8a002be4060    580               0x40                0x1 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
0xfffffa80022a47c0    580               0x44              0x804 EtwRegistration
0xfffffa8002767230    580               0x48         0x21f0003 Event
0xfffffa80026bf420    580               0x4c            0xf016e WindowStation    Service-0x0-3e7$
0xfffffa80026c05b0    580               0x50            0xf00cf Desktop          Default
0xfffffa80026bf420    580               0x54            0xf016e WindowStation    Service-0x0-3e7$
0xfffff8a00752ccc0    580               0x58                0x1 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
0xfffffa80025afc80    580               0x5c              0x804 EtwRegistration
0xfffffa8002431de0    580               0x60              0x804 EtwRegistration
0xfffffa8002930070    580               0x64              0x804 EtwRegistration
0xfffffa80022c2e10    580               0x68              0x804 EtwRegistration
0xfffffa8000e50990    580               0x6c              0x804 EtwRegistration
0xfffff8a0000f0adc0    580               0x70              0x804 EtwRegistration
0xfffffa80017bff90    580               0x74              0x804 EtwRegistration
0xfffffa80077ff6b0    580               0x78              0x804 EtwRegistration
0xfffffa800282f5d0    580               0x7c           0x1f0003 Event
0xfffffa8002844060    580               0x80           0x1f0003 Event
```

Figure 7 examine handles for PID 580

We see a lot of results after running handles command and we can use amazing option to see the registry key and file associated with the process so we can started with key to identify any registry key changed with the process and we can see the results in the next Figure08.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 -p 580 handles  -t key
Volatility Foundation Volatility Framework 2.6
Offset(V)          Pid      Handle              Access Type            Details
------------------ ------ ------------------ ------------------ ---------------- -------
0xfffff8a0026a7260    580                0x4                0x9 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffff8a0024f87f0    580               0x14                0x9 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffff8a00197ec40    580               0x20            0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
0xfffff8a002209ad0    580               0x38            0xf003f Key              MACHINE
0xfffff8a002be4060    580               0x40                0x1 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
0xfffff8a00752ccc0    580               0x58                0x1 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
0xfffff8a00197ed00    580               0x9c            0xf003f Key              USER\.DEFAULT
0xfffff8a0024db580    580               0xa0            0x2001f Key              USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0xfffff8a001615e60    580               0xc0            0xf003f Key              USER
0xfffff8a0019818a0    580               0xe0                0x1 Key              USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
0xfffff8a0019d5b80    580               0xec            0x20019 Key              USER\.DEFAULT\CONTROL PANEL\INTERNATIONAL
0xfffff8a007a41930    580              0x128                0x1 Key              MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\MAIN\FEATURECONTROL
0xfffff8a001aad610    580              0x12c            0x20019 Key              MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0xfffff8a0022a0060    580              0x130            0x20019 Key              USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0xfffff8a00188a230    580              0x134            0x20019 Key              MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0xfffff8a0026a5b50    580              0x138            0x20019 Key              MACHINE\SOFTWARE\POLICIES
0xfffff8a002cb0db0    580              0x13c            0x20019 Key              USER\.DEFAULT\SOFTWARE\POLICIES
0xfffff8a001f34ad0    580              0x140            0x20019 Key              USER\.DEFAULT\SOFTWARE
0xfffff8a0073b8470    580              0x144            0x20019 Key              MACHINE\SOFTWARE\WOW6432NODE
0xfffff8a001ae5830    580              0x158            0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
0xfffff8a003c5cdc0    580              0x160            0xf003f Key              MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
0xfffff8a002b8a870    580              0x168            0x20019 Key              MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\MAIN
0xfffff8a002c2c520    580              0x18c            0x2001f Key              USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP
0xfffff8a00235f810    580              0x190            0x20019 Key              MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP

0xfffff8a0022437d0    580              0x1b8                0xf Key              USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\5.0\CACHE
```

Figure 8 show key handles

From the previous Figure 08, we can see all keys the open by the process and we can identify all handles to files in the following Figure 09.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 -p 580 handles  -t file
Volatility Foundation Volatility Framework 2.6
Offset(V)          Pid             Handle              Access Type            Details
------------------ ------ ---------------- ---------------- --------------- -------
0xfffffa8002830600    580              0x10          0x100020 File            \Device\HarddiskVolume1\Windows
0xfffffa8003f15950    580              0x1c          0x100020 File            \Device\HarddiskVolume1\Windows\SysWOW64
0xfffffa800231c5e0    580             0x118          0x12019f File            \Device\HarddiskVolume1\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\W
indows\Temporary Internet Files\counters.dat
0xfffffa800241f4b0    580             0x170          0x100080 File            \Device\Nsi
0xfffffa8002355dd0    580             0x19c          0x16019f File            \Device\Afd\Endpoint
0xfffffa8002a6eb30    580             0x1cc          0x100001 File            \Device\KsecDD
0xfffffa8001abcf20    580             0x20c          0x120089 File            \Device\HarddiskVolume1\Windows\Registration\R000000000006.clb
0xfffffa8001b41790    580             0x218          0x16019f File            \Device\Afd\Endpoint
0xfffffa8001c622f0    580             0x2a8          0x16019f File            \Device\Afd\Endpoint
0xfffffa8000f6e710    580             0x2ac          0x16019f File            \Device\Afd\Endpoint
0xfffffa8002a89300    580             0x2c0         0x212019f File            \Device\Afd\AsyncConnectHlp
0xfffffa8002839330    580             0x2cc          0x16019f File            \Device\Afd\Endpoint
0xfffffa80023ff9a0    580             0x2d4          0x16019f File            \Device\Afd\Endpoint
0xfffffa8001bffb00    580             0x304          0x16019f File            \Device\Afd\Endpoint
0xfffffa8000e55230    580             0x31c          0x16019f File            \Device\Afd\Endpoint
0xfffffa80022ff3b0    580             0x340          0x16019f File            \Device\Afd\Endpoint
0xfffffa8002a338f0    580             0x35c          0x16019f File            \Device\Afd\Endpoint
0xfffffa8000ed0b10    580             0x394          0x16019f File            \Device\Afd\Endpoint
0xfffffa8002948ac0    580             0x3b0          0x16019f File            \Device\Afd\Endpoint
```

Figure 9 identify file handles

From the previous figure 9, we can see all file handles which use the process and we will see the all keys in Memory Dump by the printkey command to see all keys in Memory Dump so we can see the results in the Figure 9.

```
C:\Users\MemoryForensics>vol.exe -f MemoryDump.vmem --profile=Win7SP1x64 printkey
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Users\windows_7\ntuser.dat
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2021-07-28 21:10:34 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) EUDC
  (S) Keyboard Layout
  (S) Network
  (S) Printers
  (S) Software
  (S) System
  (V) Volatile Environment

Values:
----------------------------
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: CMI-CreateHive{BD6FA63F-599C-4F99-99DE-A05742AA2377} (S)
Last updated: 2009-07-14 04:57:10 UTC+0000

Subkeys:
  (S) Control Panel
  (S) Environment
  (S) EUDC
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) SYSTEM
```

Figure 10 first figure to print keys in memory dump

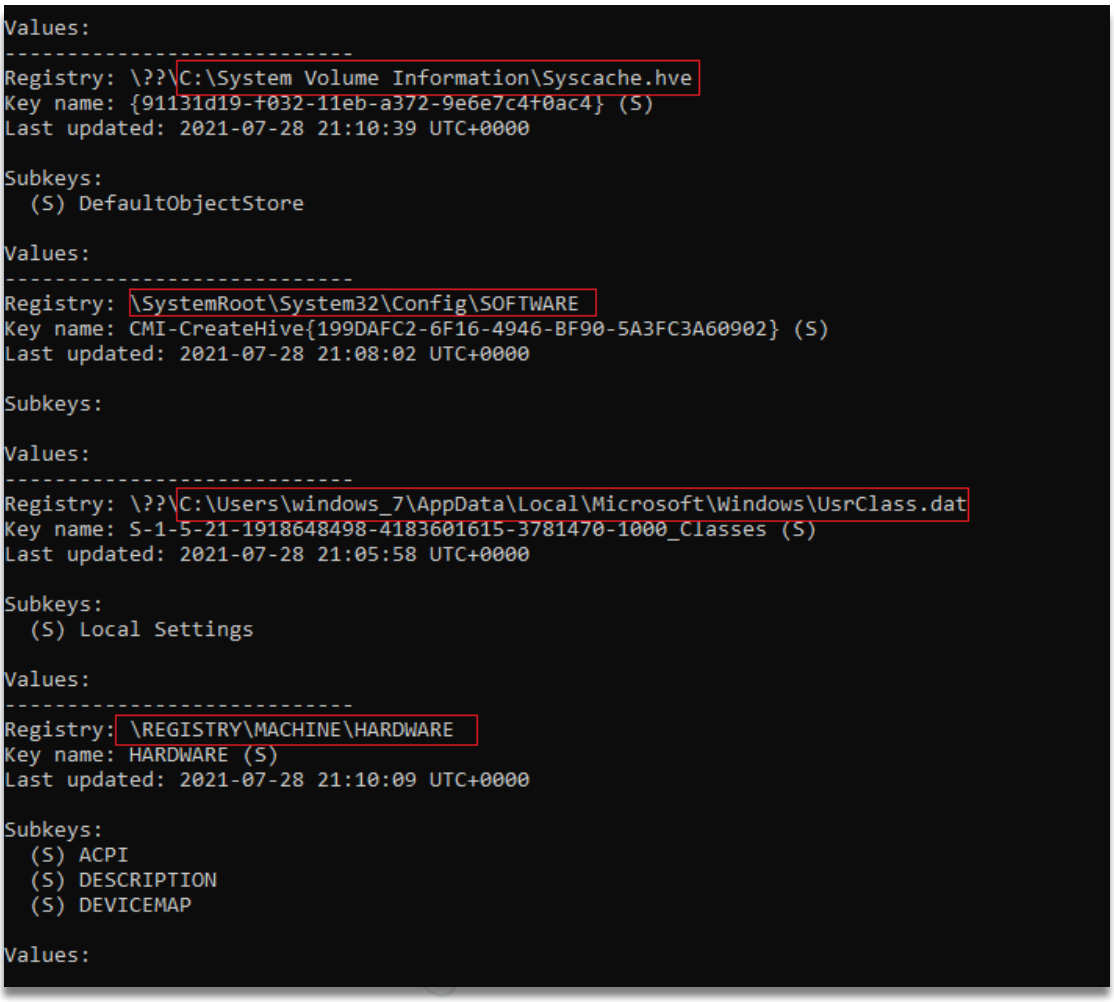


Figure 11 second figure to print keys in memory dump

From the previous figures, we can see all keys in Memory Dump