Windows Memory Forensics

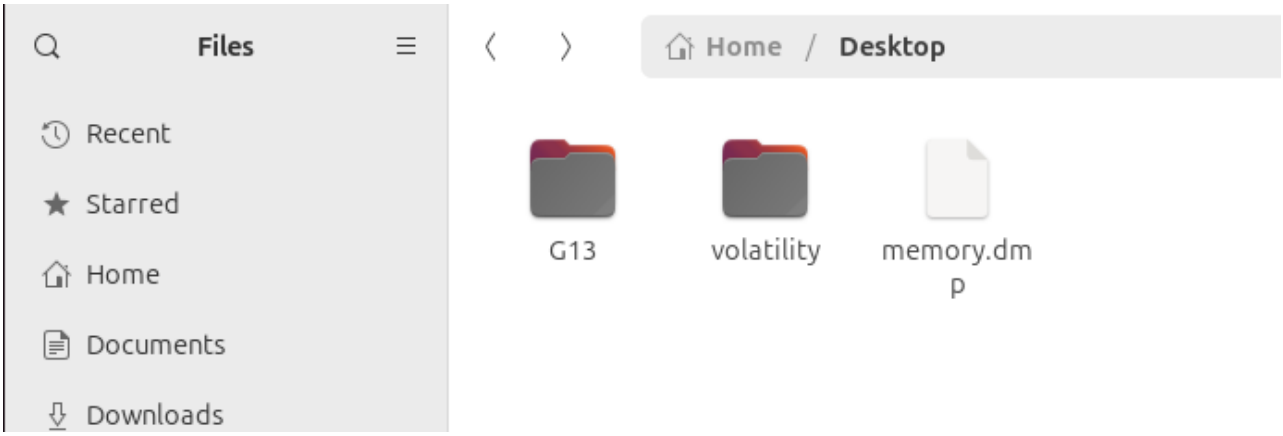
By Using Linux (Ubuntu)

Investigator:

Anas Mustafa Hashmi
Hamza Gulzar

Volatility Framework 2.6.1

We are using ***Linux (Ubuntu)*** for the memory forensics of ***G13 Dump;*** Our mission is to retrieve valuable information from this dump that can be beneficial for us as a forensic investigator.



Imageinfo: It retrieves basic information about the memory image. This information is essential for further analysis and helps in determining the appropriate profile to use with other Volatility plugins.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418,
Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/ubuntu/Desktop/memory.dmp)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000280c0a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000280dd00L
                KPCR for CPU 1 : 0xfffff880009eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2024-04-01 01:42:23 UTC+0000
     Image local date and time : 2024-04-01 03:42:23 +0200
```

This plugin in Volatility is used to gather basic information about the memory dump or image. It typically provides details such as the operating system version, service pack level, architecture (32-bit or 64-bit), and timestamps related to the memory image. This information is crucial for further analysis and understanding the context of the memory dump.

Process Analysis

pslist: This plugin lists all the active processes that are currently running in the system's memory. It provides information such as process ID, parent process ID, session ID, CPU usage, and other attributes for each process.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------
------------------------
0xfffffa80018ab040 System                    4      0     83      475 ------      0 2024-03-31 19:02:14 UTC+0000

0xfffffa8002b726a0 smss.exe                252      4      2       30 ------      0 2024-03-31 19:02:14 UTC+0000

0xfffffa80032c6060 csrss.exe               328    320      9      387      0      0 2024-03-31 19:02:14 UTC+0000

0xfffffa80018b1060 wininit.exe             376    320      3       76      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa8002bfab30 csrss.exe               388    368      8      181      1      0 2024-03-31 19:02:15 UTC+0000

0xfffffa80032ed060 winlogon.exe            424    368      4      112      1      0 2024-03-31 19:02:15 UTC+0000

0xfffffa80029f5b30 services.exe            468    376     10      199      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa8003335a10 lsass.exe               484    376      8      472      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa8003337b30 lsm.exe                 492    376     10      141      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa800339d290 svchost.exe             600    468     10      351      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa80033b6350 svchost.exe             684    468      7      259      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa80033f1920 svchost.exe             768    468     21      426      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa800341c350 svchost.exe             820    468     18      417      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa8003430b30 svchost.exe             852    468     40      962      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa8003464390 svchost.exe             936    468     13      292      0      0 2024-03-31 19:02:15 UTC+0000

0xfffffa800349ab30 svchost.exe             276    468     20      382      0      0 2024-03-31 19:02:16 UTC+0000

0xfffffa80034f4370 spoolsv.exe             924    468     13      287      0      0 2024-03-31 19:02:16 UTC+0000

0xfffffa800350b060 svchost.exe            1036    468     21      327      0      0 2024-03-31 19:02:16 UTC+0000

0xfffffa8003602b30 taskhost.exe           1256    468     12      171      1      0 2024-03-31 19:02:16 UTC+0000

0xfffffa8003650320 dwm.exe                1372    820      4       73      1      0 2024-03-31 19:02:16 UTC+0000

0xfffffa800366bb30 explorer.exe           1424   1332     29      669      1      0 2024-03-31 19:02:16 UTC+0000

0xfffffa8003717890 svchost.exe            1716    468      6      103      0      0 2024-03-31 19:02:17 UTC+0000

0xfffffa80037a5920 pythonw.exe            1892   1424      2       98      1      1 2024-03-31 19:02:18 UTC+0000

0xfffffa800383c060 SearchIndexer.         1388    468     15      591      0      0 2024-03-31 19:02:24 UTC+0000

0xfffffa800386b440 SearchProtocol         1816   1388      7      295      0      0 2024-03-31 19:02:24 UTC+0000

0xfffffa8002ba6b30 SearchFilterHo          308   1388      4       79      0      0 2024-03-31 19:02:24 UTC+0000

0xfffffa800343d650 pythonw.exe            2040   1892      0 --------      1      0 2024-03-31 19:02:33 UTC+0000   2024-
04-01 01:42:23 UTC+0000
0xfffffa800396bb30 huuhroi.exe            2300   2240     10      327      1      1 2024-04-01 01:40:11 UTC+0000
```

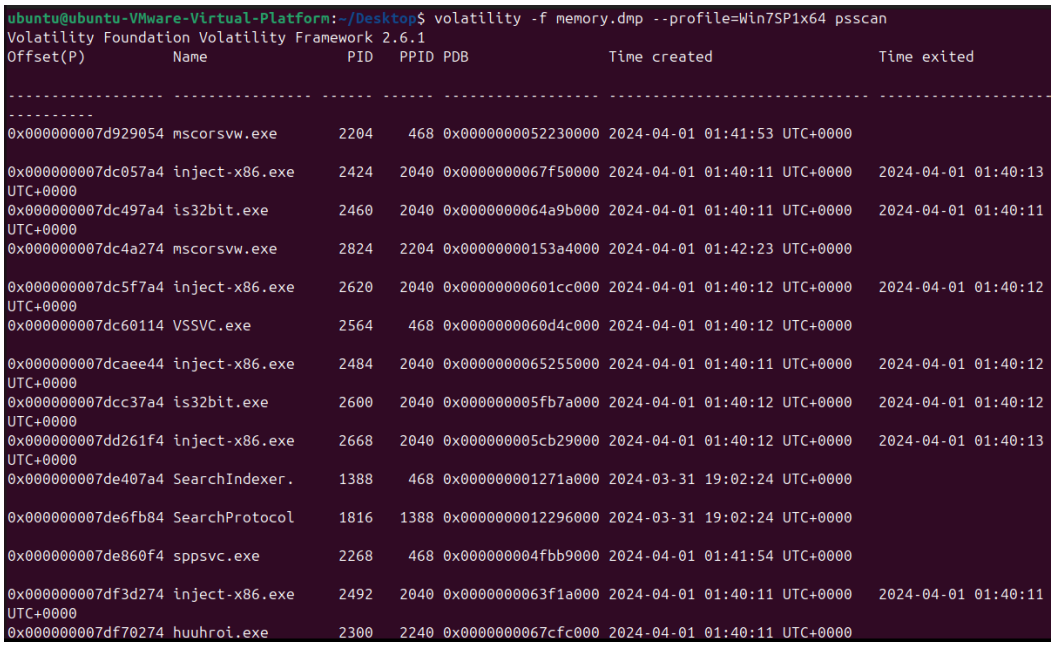
```
0xfffffa8001904060 vssadmin.exe           2444   2300      0 --------      1      0 2024-04-01 01:40:11 UTC+0000   2024-
04-01 01:40:13 UTC+0000
0xfffffa8003a5b9d0 VSSVC.exe              2564    468      7      115      0      0 2024-04-01 01:40:12 UTC+0000

0xfffffa8001afdb30 svchost.exe            2020    468     13      155      0      0 2024-04-01 01:41:53 UTC+0000

0xfffffa8001b1fb30 mscorsvw.exe            392    468      7      105      0      1 2024-04-01 01:41:53 UTC+0000

0xfffffa8003f24910 mscorsvw.exe           2204    468      8      226      0      0 2024-04-01 01:41:53 UTC+0000

0xfffffa80038819b0 sppsvc.exe             2268    468      7      153      0      0 2024-04-01 01:41:54 UTC+0000

0xfffffa8003a45b30 mscorsvw.exe           2824   2204      8      144      0      0 2024-04-01 01:42:23 UTC+0000
```

Here are some of the suspicious processes identified in the output:

1. **huuhroi.exe (PID: 2300):**
   - The process name is not recognizable as a standard Windows system process or a known legitimate application.
   - The process has a relatively high number of threads and handles, which might indicate anomalous behavior.
2. **vssadmin.exe (PID: 2444):**
   - While "vssadmin.exe" is a legitimate Windows utility, its invocation may be suspicious, especially if it is not commonly used in the context of the system.
   - The process appears to have started and exited relatively quickly, which could indicate potential malicious activity, such as attempting to manipulate Volume Shadow Copies.
3. **mscorsvw.exe (PID: 392, 2204, 2824):**
   - Multiple instances of "mscorsvw.exe" are running, which may not be typical behavior unless there are multiple .NET applications running concurrently.
   - The process has a relatively high number of threads and handles, which might indicate unusual activity.
4. **SearchIndexer.exe (PID: 1388):**
   - While "SearchIndexer.exe" is a legitimate Windows process responsible for indexing files for faster searches, its presence and behavior should be monitored, especially if it is consuming significant system resources.

5. **pythonw.exe (PID: 1892, 2040):**
    - The presence of Python-related processes may be suspicious if Python is not commonly used in the environment or if the source of the Python scripts is unknown.
    - The process with PID 2040 appears to have exited, which might warrant further investigation into its execution and associated activities.
6. **sppsvc.exe (PID: 2268):**
    - While "sppsvc.exe" is a legitimate Windows service related to software protection, its invocation may be suspicious if it occurs at unexpected times or if it exhibits unusual behavior.

psscan: Psscan lists processes, including those that have terminated but still have remnants in memory. It provides a comprehensive view of all processes that have been active on the system, even if they have since ended.



```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB               Time created                   Time exited
------------------ --------------- ------ ------ ----------------- ------------------------------ ------------------------------
----------
0x000000007d929054 mscorsvw.exe       2204    468 0x0000000052230000 2024-04-01 01:41:53 UTC+0000

0x000000007dc057a4 inject-x86.exe     2424   2040 0x0000000067f50000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:13
UTC+0000
0x000000007dc497a4 is32bit.exe        2460   2040 0x0000000064a9b000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dc4a274 mscorsvw.exe       2824   2204 0x00000000153a4000 2024-04-01 01:42:23 UTC+0000

0x000000007dc5f7a4 inject-x86.exe     2620   2040 0x00000000601cc000 2024-04-01 01:40:12 UTC+0000   2024-04-01 01:40:12
UTC+0000
0x000000007dc60114 VSSVC.exe          2564    468 0x0000000060d4c000 2024-04-01 01:40:12 UTC+0000

0x000000007dcaee44 inject-x86.exe     2484   2040 0x0000000065255000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:12
UTC+0000
0x000000007dcc37a4 is32bit.exe        2600   2040 0x000000005fb7a000 2024-04-01 01:40:12 UTC+0000   2024-04-01 01:40:12
UTC+0000
0x000000007dd261f4 inject-x86.exe     2668   2040 0x000000005cb29000 2024-04-01 01:40:12 UTC+0000   2024-04-01 01:40:13
UTC+0000
0x000000007de407a4 SearchIndexer.     1388    468 0x00000000271a000 2024-03-31 19:02:24 UTC+0000

0x000000007de6fb84 SearchProtocol     1816   1388 0x0000000012296000 2024-03-31 19:02:24 UTC+0000

0x000000007de860f4 sppsvc.exe         2268    468 0x000000004fbb9000 2024-04-01 01:41:54 UTC+0000

0x000000007df3d274 inject-x86.exe     2492   2040 0x0000000063f1a000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007df70274 huuhroi.exe        2300   2240 0x0000000067cfc000 2024-04-01 01:40:11 UTC+0000
```

```
0x000000007dfb6d74 inject-x64.exe     2164   2040 0x000000006fe97000 2024-04-01 01:40:10 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfc67a4 is32bit.exe        2248   2040 0x00000000685eb000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfc77a4 inject-x86.exe     2216   2040 0x0000000067b54000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfc8274 is32bit.exe        2200   2040 0x000000005da80000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfca274 TeslaCrypt2.ex     2240   2216 0x0000000068162000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:13
UTC+0000
0x000000007dfde274 cmd.exe            2352   2240 0x0000000067442000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:12
UTC+0000
0x000000007dfea274 inject-x86.exe     2328   2040 0x0000000067f9f000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfeb274 is32bit.exe        2308   2040 0x0000000067e4b000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007dfff274 is32bit.exe        2396   2040 0x0000000066dfd000 2024-04-01 01:40:11 UTC+0000   2024-04-01 01:40:11
UTC+0000
0x000000007e007274 taskhost.exe       1256    468 0x000000001a27c000 2024-03-31 19:02:16 UTC+0000

0x000000007e054a64 dwm.exe            1372    820 0x0000000019b8e000 2024-03-31 19:02:16 UTC+0000

0x000000007e070274 explorer.exe       1424   1332 0x000000001976c000 2024-03-31 19:02:16 UTC+0000

0x000000007e11bfd4 svchost.exe        1716    468 0x0000000017869000 2024-03-31 19:02:17 UTC+0000

0x000000007e1aa064 pythonw.exe        1892   1424 0x0000000016548000 2024-03-31 19:02:18 UTC+0000

0x000000007e220a94 svchost.exe         820    468 0x0000000017e40000 2024-03-31 19:02:15 UTC+0000

0x000000007e235274 svchost.exe         852    468 0x0000000020788000 2024-03-31 19:02:15 UTC+0000
```

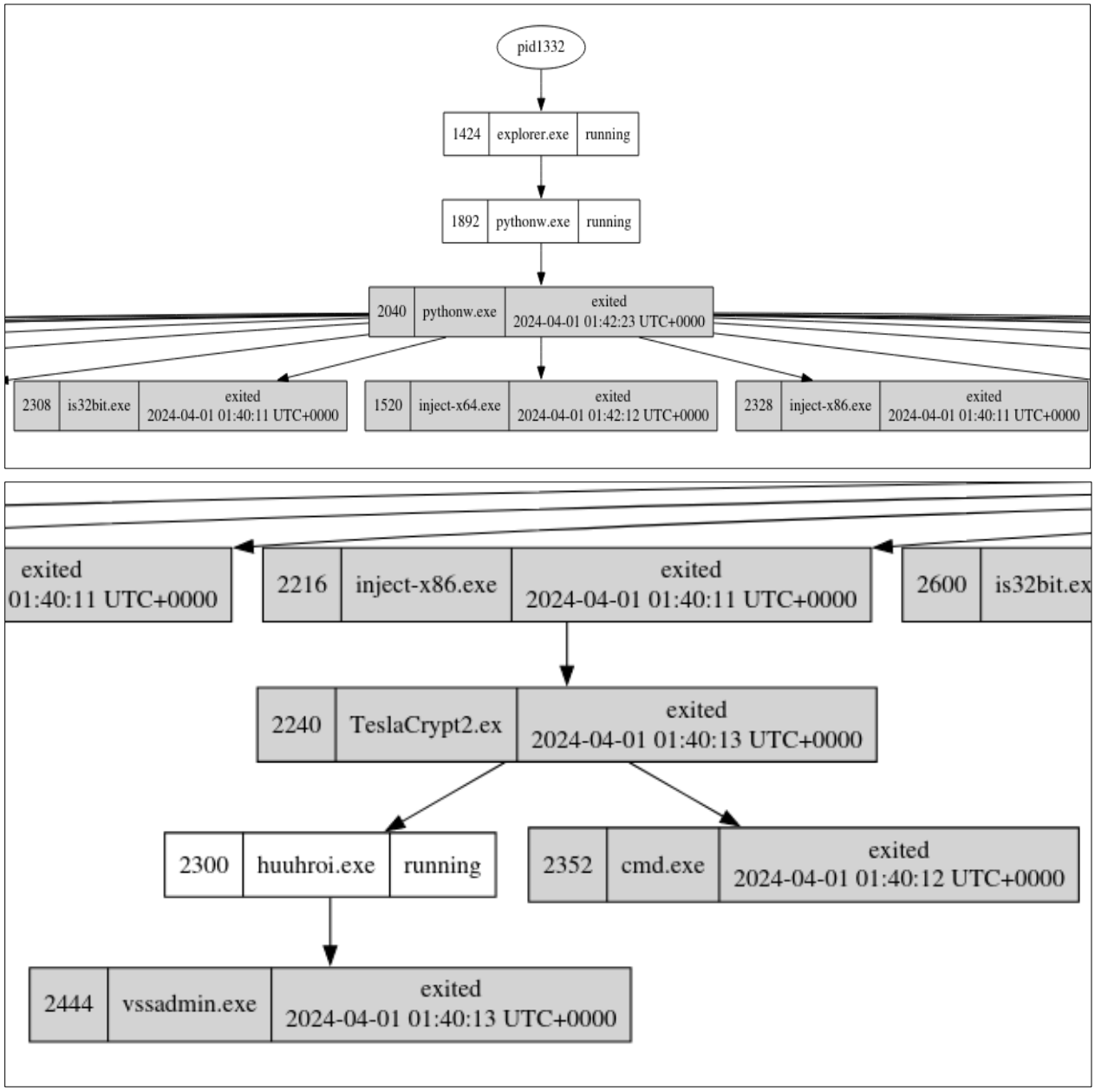
```
0x000000007e241d94 pythonw.exe        2040   1892 0x000000000e72e000 2024-03-31 19:02:33 UTC+0000   2024-04-01 01:42:23
UTC+0000
0x000000007e268ad4 svchost.exe         936    468 0x0000000020293000 2024-03-31 19:02:15 UTC+0000

0x000000007e29f274 svchost.exe         276    468 0x000000001ec1b000 2024-03-31 19:02:16 UTC+0000

0x000000007e2f8ab4 spoolsv.exe         924    468 0x000000001cda9000 2024-03-31 19:02:16 UTC+0000

0x000000007e30f7a4 svchost.exe        1036    468 0x000000001c155000 2024-03-31 19:02:16 UTC+0000

0x000000007e4ca7a4 csrss.exe           328    320 0x000000002348d000 2024-03-31 19:02:14 UTC+0000

0x000000007e4f17a4 winlogon.exe        424    368 0x0000000022585000 2024-03-31 19:02:15 UTC+0000

0x000000007e53a154 lsass.exe           484    376 0x0000000021c83000 2024-03-31 19:02:15 UTC+0000

0x000000007e53c274 lsm.exe             492    376 0x0000000021c4b000 2024-03-31 19:02:15 UTC+0000

0x000000007e5a19d4 svchost.exe         600    468 0x00000000214cc000 2024-03-31 19:02:15 UTC+0000

0x000000007e5baa94 svchost.exe         684    468 0x000000002122c000 2024-03-31 19:02:15 UTC+0000

0x000000007e5f6064 svchost.exe         768    468 0x0000000020fb6000 2024-03-31 19:02:15 UTC+0000

0x000000007ed76de4 smss.exe            252      4 0x000000002940f000 2024-03-31 19:02:14 UTC+0000

0x000000007edab274 SearchFilterHo      308   1388 0x0000000011178000 2024-03-31 19:02:24 UTC+0000

0x000000007edff274 csrss.exe           388    368 0x000000002307f000 2024-03-31 19:02:15 UTC+0000

0x000000007effa274 services.exe        468    376 0x000000002205d000 2024-03-31 19:02:15 UTC+0000
```

Here are some of the suspicious processes identified in the output:

- **inject-x86.exe (PID: 2424, 2620, 2484, 2492, 2328, 2216, 2396, 2396, 2492, 1136):** This process is injecting code into other processes, which is often indicative of malicious activity.

- **inject-x64.exe (PID: 2164, 1520, 2832):** Like inject-x86.exe, this process is injecting code into other processes, and the presence of both x86 and x64 versions suggests a sophisticated attack targeting both architectures.
- **is32bit.exe (PID: 2460, 2484, 2600, 2248, 2200, 2816):** This process may be involved in determining the bitness of the system or performing operations specific to 32-bit processes. Its repeated appearance alongside inject-x86.exe raises suspicion.
- **huuhroi.exe (PID: 2300):** The name of this process does not appear to be a standard Windows process and could be a randomly generated name by malware.
- **TeslaCrypt2.exe (PID: 2240):** This process is associated with the TeslaCrypt ransomware, which encrypts files on the system and demands payment for decryption.
- **vssadmin.exe (PID: 2444):** This process is commonly abused by ransomware to delete Volume Shadow Copies, making it harder for victims to recover their files.
- **cmd.exe (PID: 2352):** The Command Prompt is often abused by attackers for various malicious activities, including executing commands and scripts.
- **SearchIndexer.exe (PID: 1388):** While SearchIndexer.exe is a legitimate Windows process responsible for indexing files for Windows Search, its presence may be exploited by malware to disguise malicious activity.
- **mscorsvw.exe (PID: 2204, 2004, 2708, 2196, 392):** While mscorsvw.exe is a legitimate process associated with the .NET Framework, its presence alongside other suspicious processes may indicate attempts to blend in or disguise malicious activity.
- **pythonw.exe (PID: 2040, 1892):** While Python is a legitimate programming language, the presence of pythonw.exe may indicate the execution of malicious Python scripts or the use of Python-based malware.

```
ubuntu@ubuntu-001:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 psscan --output=dot --output-file=psscan.dot
Volatility Foundation Volatility Framework 2.6.1
Outputting to: psscan.dot
```



pstree: It displays process relationships in a hierarchical tree format. It helps in visualizing the parent-child relationships between processes, making it easier to understand process creation, dependencies, and potential malicious behaviors such as process spawning.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa80032c6060:csrss.exe                         328    320      9    387 2024-03-31 19:02:14 UTC+0000
 0xfffffa80018b1060:wininit.exe                       376    320      3     76 2024-03-31 19:02:15 UTC+0000
. 0xfffffa80029f5b30:services.exe                     468    376     10    199 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa80033f1920:svchost.exe                     768    468     21    426 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa8001b1fb30:mscorsvw.exe                    392    468      7    105 2024-04-01 01:41:53 UTC+0000
.. 0xfffffa800383c060:SearchIndexer.                 1388    468     15    591 2024-03-31 19:02:24 UTC+0000
... 0xfffffa800386b440:SearchProtocol                1816   1388      7    295 2024-03-31 19:02:24 UTC+0000
... 0xfffffa8002ba6b30:SearchFilterHo                 308   1388      4     79 2024-03-31 19:02:24 UTC+0000
.. 0xfffffa800350b060:svchost.exe                    1036    468     21    327 2024-03-31 19:02:16 UTC+0000
.. 0xfffffa800349ab30:svchost.exe                     276    468     20    382 2024-03-31 19:02:16 UTC+0000
.. 0xfffffa80034f4370:spoolsv.exe                     924    468     13    287 2024-03-31 19:02:16 UTC+0000
.. 0xfffffa8003f24910:mscorsvw.exe                   2204    468      8    226 2024-04-01 01:41:53 UTC+0000
... 0xfffffa8003a45b30:mscorsvw.exe                  2824   2204      8    144 2024-04-01 01:42:23 UTC+0000
.. 0xfffffa80033b6350:svchost.exe                     684    468      7    259 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa8003717890:svchost.exe                    1716    468      6    103 2024-03-31 19:02:17 UTC+0000
.. 0xfffffa800341c350:svchost.exe                     820    468     18    417 2024-03-31 19:02:15 UTC+0000
... 0xfffffa8003650320:dwm.exe                       1372    820      4     73 2024-03-31 19:02:16 UTC+0000
.. 0xfffffa8003a5b9d0:VSSVC.exe                      2564    468      7    115 2024-04-01 01:40:12 UTC+0000
.. 0xfffffa800339d290:svchost.exe                     600    468     10    351 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa80038819b0:sppsvc.exe                     2268    468      7    153 2024-04-01 01:41:54 UTC+0000
.. 0xfffffa8003602b30:taskhost.exe                   1256    468     12    171 2024-03-31 19:02:16 UTC+0000
.. 0xfffffa8003464390:svchost.exe                     936    468     13    292 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa8003430b30:svchost.exe                     852    468     40    962 2024-03-31 19:02:15 UTC+0000
.. 0xfffffa8001afdb30:svchost.exe                    2020    468     13    155 2024-04-01 01:41:53 UTC+0000
. 0xfffffa8003335a10:lsass.exe                        484    376      8    472 2024-03-31 19:02:15 UTC+0000
. 0xfffffa8003337b30:lsm.exe                          492    376     10    141 2024-03-31 19:02:15 UTC+0000
 0xfffffa8002bfab30:csrss.exe                         388    368      8    181 2024-03-31 19:02:15 UTC+0000
 0xfffffa80032ed060:winlogon.exe                      424    368      4    112 2024-03-31 19:02:15 UTC+0000
 0xfffffa800366bb30:explorer.exe                     1424   1332     29    669 2024-03-31 19:02:16 UTC+0000
```

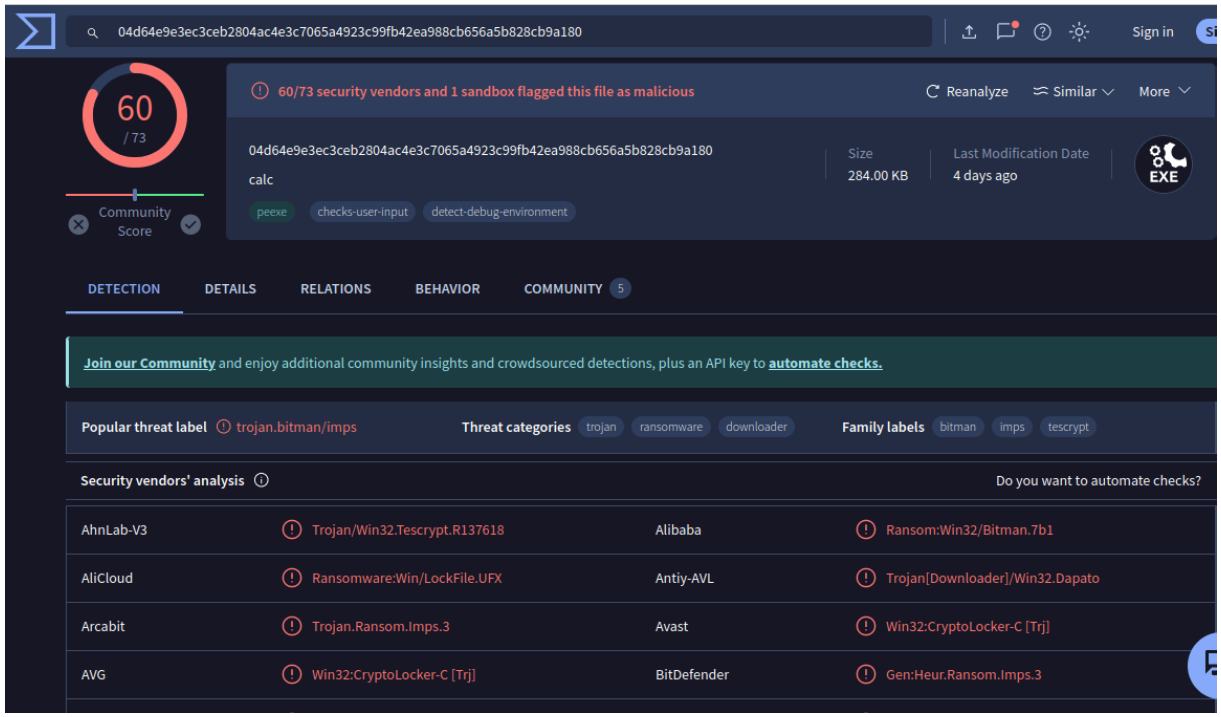
There are a few processes that might be considered suspicious or potentially malicious:

- **huuhroi.exe (PID: 2300):** This process stands out as it has an unusual name and is not a standard Windows system process. The name "huuhroi.exe" doesn't correspond to any known legitimate Windows process or application. Additionally, it's running as a child process of the system (PID: 4), which is unusual for legitimate processes.

- **vssadmin.exe (PID: 2444):** While vssadmin.exe is a legitimate Windows utility used for managing Volume Shadow Copies, it can also be abused by attackers to delete shadow copies and hinder system restoration. Its presence should be investigated further, especially if there's no legitimate reason for it to be running at that time.

After dumping the malicious executables from memory and scanning with multi-antivirus scanning engine *(VirusTotal)* confirms the dumped executable to be malicious.

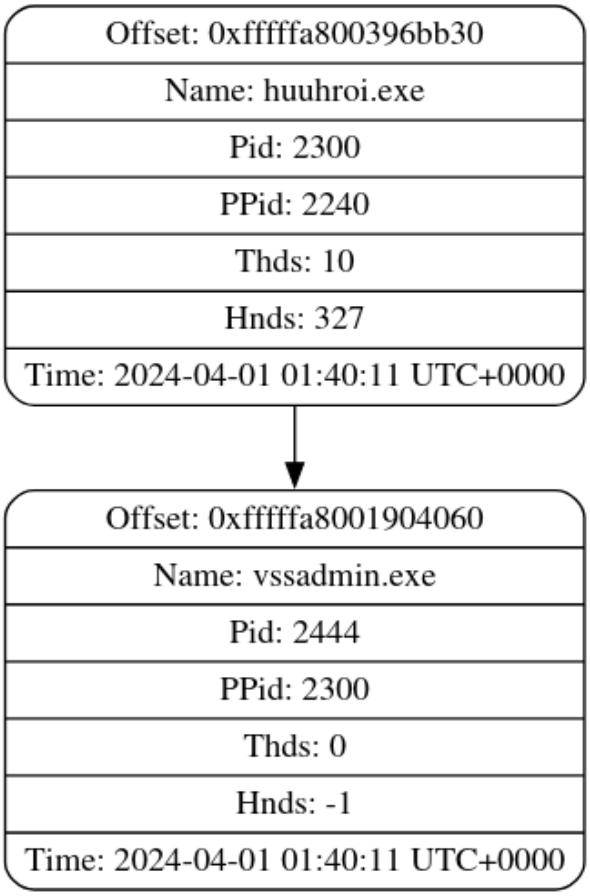
```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 procdump -p 2300 -D Dump
Volatility Foundation Volatility Framework 2.6.1
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa800396bb30 0x0000000000400000 huuhroi.exe          OK: executable.2300.exe
```



Fortinet	W32/Filecoder.EMItr	GData	Gen:Heur.Ransom.Imps.3
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.Filecoder.vb!s1
Ikarus	Trojan-Ransom.TeslaCrypt	Jiangmin	Trojan.Bitman.aqf
K7AntiVirus	Ransomware (004bcd7c1)	K7GW	Ransomware (004bcd7c1)
Kaspersky	Trojan-Ransom.Win32.Bitman.d	Kingsoft	Malware.kb.a.985
Lionic	Trojan.Win32.Bitman.tngH	Malwarebytes	Trojan.CryptoLocker
MAX	Malware (ai Score=88)	MaxSecure	Trojan.Malware.8180803.susgen
McAfee	Ransom-FYG!9F29FD1686CC	Microsoft	Ransom:Win32/Tescrypt!pz
NANO-Antivirus	Trojan.Win32.Bitman.ediseq	Palo Alto Networks	Generic.ml
Panda	Trj/Genetic.gen	QuickHeal	Trojan.GenericRI.S30114240
Rising	Ransom.Tescrypt!8.3AF (TFE:5:8o3UpX8…	Sangfor Engine Zero	Ransom.Win32.Tescrypt.Vlf1

It gives the visual representation of parent/child process relationship as we can see below.

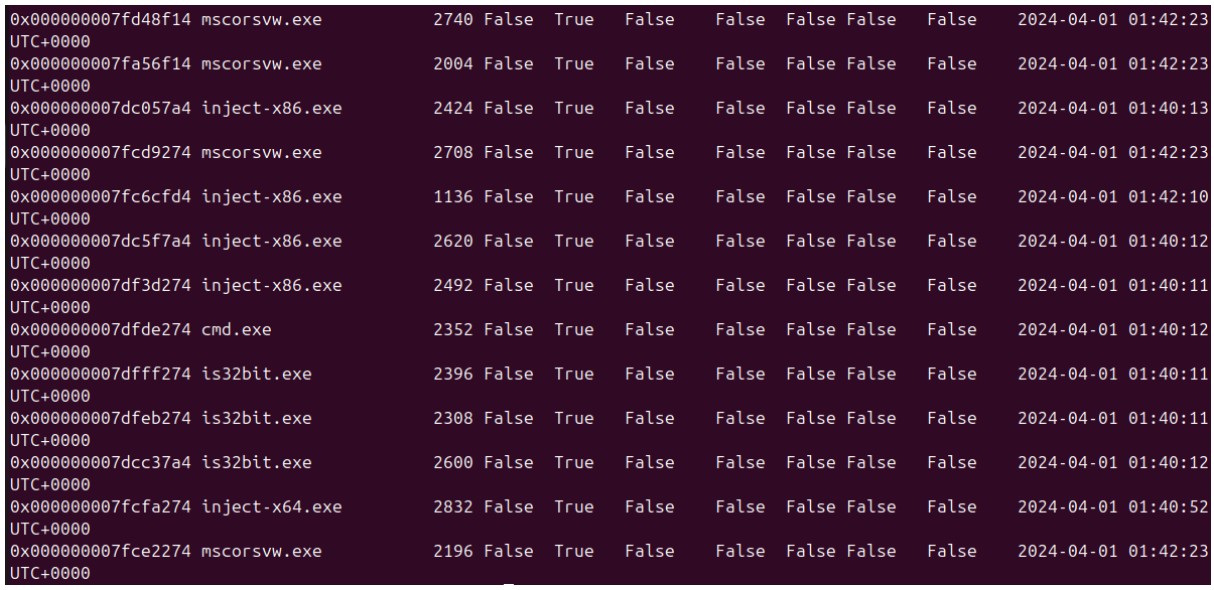
```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 pstree --output=dot --out
put-file=huuhroi.dot
Volatility Foundation Volatility Framework 2.6.1
Outputting to: huuhroi.dot
```



psxview: It provides insights into potentially hidden or malicious processes on the system, allowing further investigation and analysis to determine if any malicious activities are indeed present.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x000000007de6fb84 SearchProtocol         1816 True   True   True     True   True  True    True
0x000000007fd24274 mscorsvw.exe            392 True   True   True     True   True  True    True
0x000000007e054a64 dwm.exe                1372 True   True   True     True   True  True    True
0x000000007e007274 taskhost.exe           1256 True   True   True     True   True  True    True
0x000000007e5baa94 svchost.exe             684 True   True   True     True   True  True    True
0x000000007dc4a274 mscorsvw.exe           2824 True   True   True     True   True  True    True
0x000000007ff347a4 wininit.exe             376 True   True   True     True   True  True    True
0x000000007e5a19d4 svchost.exe             600 True   True   True     True   True  True    True
0x000000007e4f17a4 winlogon.exe            424 True   True   True     True   True  True    True
0x000000007e53c274 lsm.exe                 492 True   True   True     True   True  True    False
0x000000007e220a94 svchost.exe             820 True   True   True     True   True  True    True
0x000000007e2f8ab4 spoolsv.exe             924 True   True   True     True   True  True    True
0x000000007e070274 explorer.exe           1424 True   True   True     True   True  True    True
0x000000007de860f4 sppsvc.exe             2268 True   True   True     True   True  True    True
0x000000007e1aa064 pythonw.exe            1892 True   True   True     True   True  True    True
0x000000007e235274 svchost.exe             852 True   True   True     True   True  True    True
0x000000007d929054 mscorsvw.exe           2204 True   True   True     True   True  True    True
0x000000007de407a4 SearchIndexer.         1388 True   True   True     True   True  True    True
0x000000007e11bfd4 svchost.exe            1716 True   True   True     True   True  True    True
0x000000007effa274 services.exe            468 True   True   True     True   True  True    False
0x000000007e5f6064 svchost.exe             768 True   True   True     True   True  True    True
0x000000007dc60114 VSSVC.exe              2564 True   True   True     True   True  True    True
0x000000007e53a154 lsass.exe               484 True   True   True     True   True  True    False
0x000000007e29f274 svchost.exe             276 True   True   True     True   True  True    True
0x000000007edab274 SearchFilterHo          308 True   True   True     True   True  True    True
0x000000007e268ad4 svchost.exe             936 True   True   True     True   True  True    True
0x000000007e30f7a4 svchost.exe            1036 True   True   True     True   True  True    True
0x000000007df70274 huuhroi.exe            2300 True   True   True     True   True  True    True
```

```
0x000000007fd02274 svchost.exe            2020 True   True   True     True   True  True    True
0x000000007fec77a4 vssadmin.exe           2444 True   True   False    True   False True    False    2024-04-01 01:40:13
UTC+0000
0x000000007e4ca7a4 csrss.exe               328 True   True   True     True   False True    True
0x000000007ff6e784 System                    4 True   True   True     True   False False   False
0x000000007ed76de4 smss.exe                252 True   True   True     True   False False   False
0x000000007e241d94 pythonw.exe            2040 True   True   False    True   False True    False    2024-04-01 01:42:23
UTC+0000
0x000000007edff274 csrss.exe               388 True   True   True     True   False True    True
0x000000007dfc77a4 inject-x86.exe         2216 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dc497a4 is32bit.exe            2460 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dfca274 TeslaCrypt2.ex         2240 False  True   False    False  False False   False    2024-04-01 01:40:13
UTC+0000
0x000000007dfea274 inject-x86.exe         2328 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007fce8274 inject-x64.exe         1520 False  True   False    False  False False   False    2024-04-01 01:42:12
UTC+0000
0x000000007dfc67a4 is32bit.exe            2248 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dd261f4 inject-x86.exe         2668 False  True   False    False  False False   False    2024-04-01 01:40:13
UTC+0000
0x000000007dfc8274 is32bit.exe            2200 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007fec7274 is32bit.exe            2136 False  True   False    False  False False   False    2024-04-01 01:40:10
UTC+0000
0x000000007dfb6d74 inject-x64.exe         2164 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dcaee44 inject-x86.exe         2484 False  True   False    False  False False   False    2024-04-01 01:40:12
UTC+0000
0x000000007fceb274 is32bit.exe            2816 False  True   False    False  False False   False    2024-04-01 01:40:52
UTC+0000
```



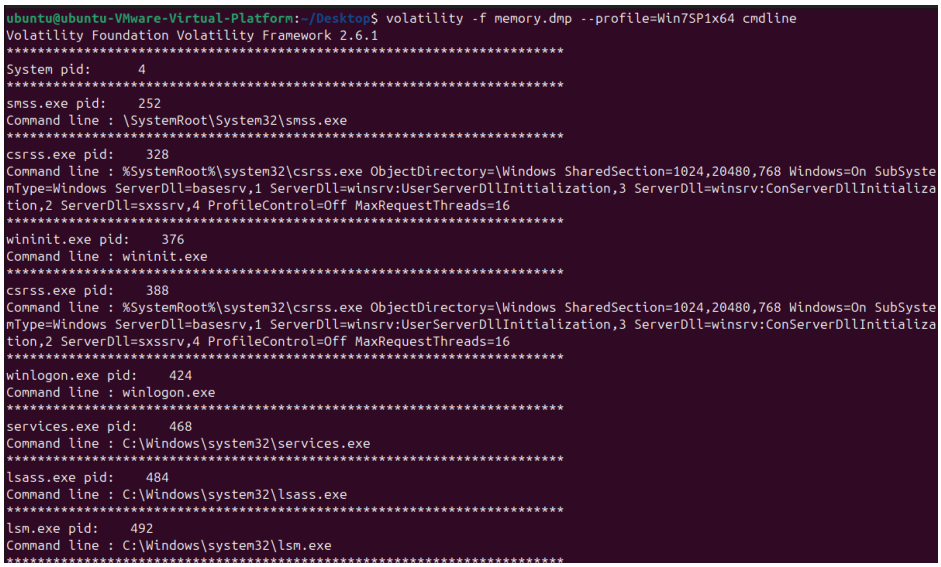
```
0x000000007fd48f14 mscorsvw.exe          2740 False  True   False    False  False False   False    2024-04-01 01:42:23
UTC+0000
0x000000007fa56f14 mscorsvw.exe          2004 False  True   False    False  False False   False    2024-04-01 01:42:23
UTC+0000
0x000000007dc057a4 inject-x86.exe        2424 False  True   False    False  False False   False    2024-04-01 01:40:13
UTC+0000
0x000000007fcd9274 mscorsvw.exe          2708 False  True   False    False  False False   False    2024-04-01 01:42:23
UTC+0000
0x000000007fc6cfd4 inject-x86.exe        1136 False  True   False    False  False False   False    2024-04-01 01:42:10
UTC+0000
0x000000007dc5f7a4 inject-x86.exe        2620 False  True   False    False  False False   False    2024-04-01 01:40:12
UTC+0000
0x000000007df3d274 inject-x86.exe        2492 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dfde274 cmd.exe               2352 False  True   False    False  False False   False    2024-04-01 01:40:12
UTC+0000
0x000000007dfff274 is32bit.exe           2396 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dfeb274 is32bit.exe           2308 False  True   False    False  False False   False    2024-04-01 01:40:11
UTC+0000
0x000000007dcc37a4 is32bit.exe           2600 False  True   False    False  False False   False    2024-04-01 01:40:12
UTC+0000
0x000000007fcfa274 inject-x64.exe        2832 False  True   False    False  False False   False    2024-04-01 01:40:52
UTC+0000
0x000000007fce2274 mscorsvw.exe          2196 False  True   False    False  False False   False    2024-04-01 01:42:23
UTC+0000
```

Here are some observations:

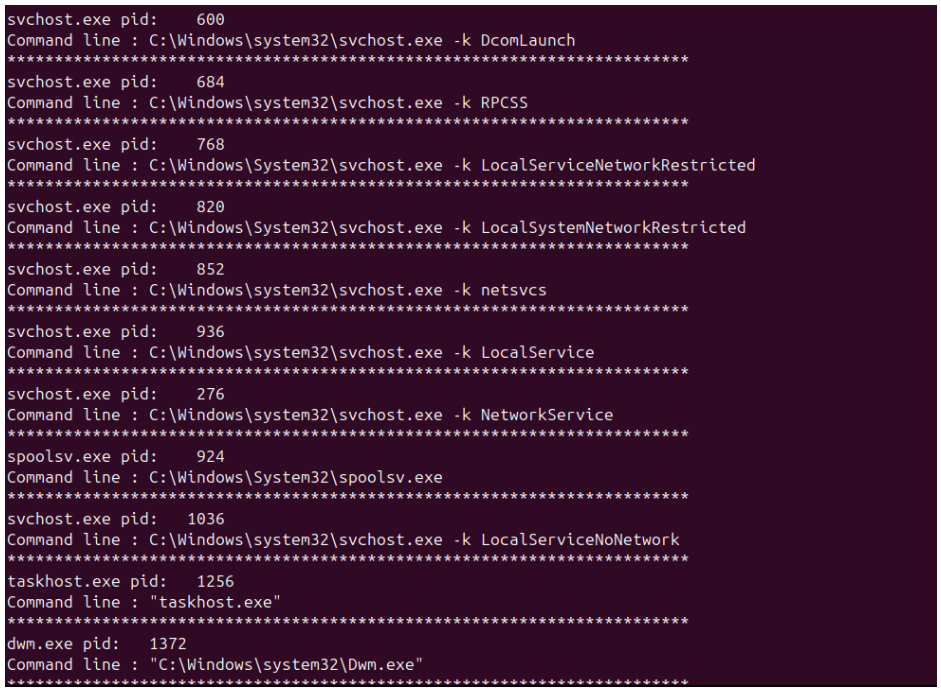
1. **Hidden Processes:**
   - **inject-x86.exe, is32bit.exe, inject-x64.exe, cmd.exe, huuhroi.exe,** and **inject-x86.exe** appear to be hidden processes. These processes have the value False under the *pslist* column, indicating that they are not visible in the standard process list.
2. **Unusual Process Names:**
   - Processes like **huuhroi.exe** and **TeslaCrypt2.exe** have unusual names, which might indicate that they are malicious or suspicious. Legitimate processes typically have recognizable names related to their function or the software they belong to.
3. **Timestamps:**
   - Some processes have recent creation or exit times, which could be suspicious, especially if they coincide with known security events or incidents.
   - For example, **vssadmin.exe** and **TeslaCrypt2.exe** have exit times recorded, which might be indicative of their activity on the system.
4. **Anomalous Behavior:**
   - Processes such as **inject-x86.exe, inject-x64.exe,** and **is32bit.exe** are known to be associated with code injection techniques often used by malware to hide their presence or execute malicious code within legitimate processes.

- Similarly, **cmd.exe** could be used for unauthorized command execution.

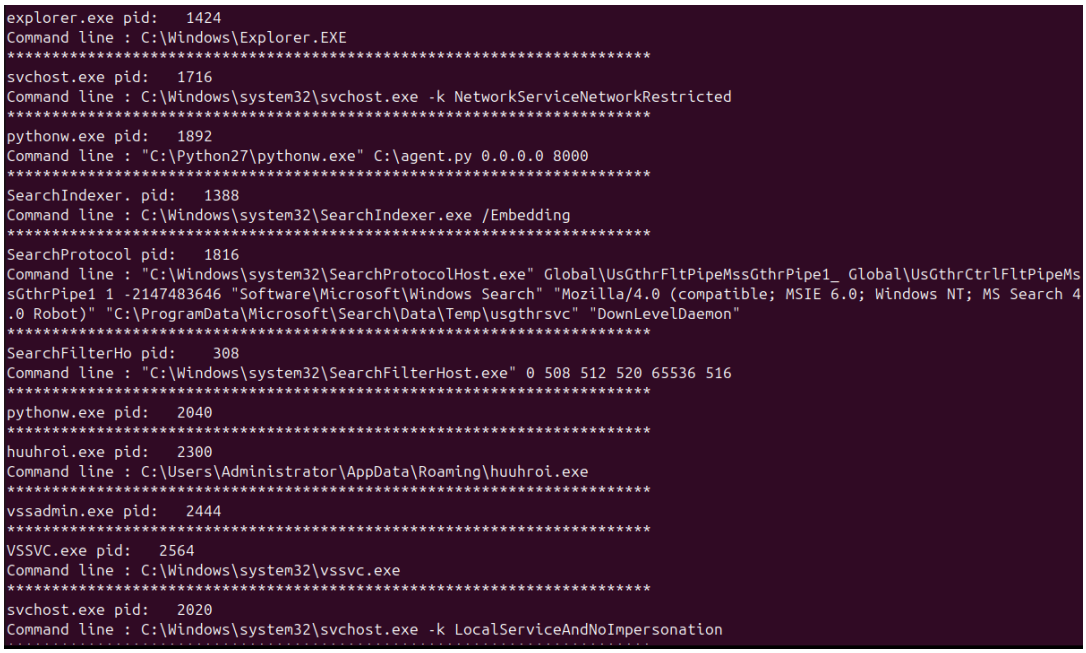
cmdline: It is used for extracting and displaying command-line arguments associated with processes found in memory dumps. It helps forensic analysts gather valuable information about the execution environment and behavior of processes at the time of memory acquisition.



```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 cmdline
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    252
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    328
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyste
mType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializa
tion,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
wininit.exe pid:    376
Command line : wininit.exe
************************************************************************
csrss.exe pid:    388
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyste
mType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializa
tion,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
winlogon.exe pid:    424
Command line : winlogon.exe
************************************************************************
services.exe pid:    468
Command line : C:\Windows\system32\services.exe
************************************************************************
lsass.exe pid:    484
Command line : C:\Windows\system32\lsass.exe
************************************************************************
lsm.exe pid:    492
Command line : C:\Windows\system32\lsm.exe
************************************************************************
```



```
svchost.exe pid:    600
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch
************************************************************************
svchost.exe pid:    684
Command line : C:\Windows\system32\svchost.exe -k RPCSS
************************************************************************
svchost.exe pid:    768
Command line : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
************************************************************************
svchost.exe pid:    820
Command line : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
************************************************************************
svchost.exe pid:    852
Command line : C:\Windows\system32\svchost.exe -k netsvcs
************************************************************************
svchost.exe pid:    936
Command line : C:\Windows\system32\svchost.exe -k LocalService
************************************************************************
svchost.exe pid:    276
Command line : C:\Windows\system32\svchost.exe -k NetworkService
************************************************************************
spoolsv.exe pid:    924
Command line : C:\Windows\System32\spoolsv.exe
************************************************************************
svchost.exe pid:   1036
Command line : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
************************************************************************
taskhost.exe pid:   1256
Command line : "taskhost.exe"
************************************************************************
dwm.exe pid:   1372
Command line : "C:\Windows\system32\Dwm.exe"
************************************************************************
```



Here are some observations:

1. **Malicious Activity:**
   - Processes such as **huuhroi.exe** and **vssadmin.exe** lack command-line arguments, which could indicate attempts to **hide their activities**. This behavior is often associated with malware trying to evade detection.

2. **Normal Activity:**
   - Normal system processes like **smss.exe, csrss.exe, wininit.exe, winlogon.exe, services.exe, lsass.exe,** and **lsm.exe** have command lines that are typical for system processes. These processes are essential for the functioning of the Windows operating system and are not indicative of malicious activity.

Kernel Modules and Drivers Analysis

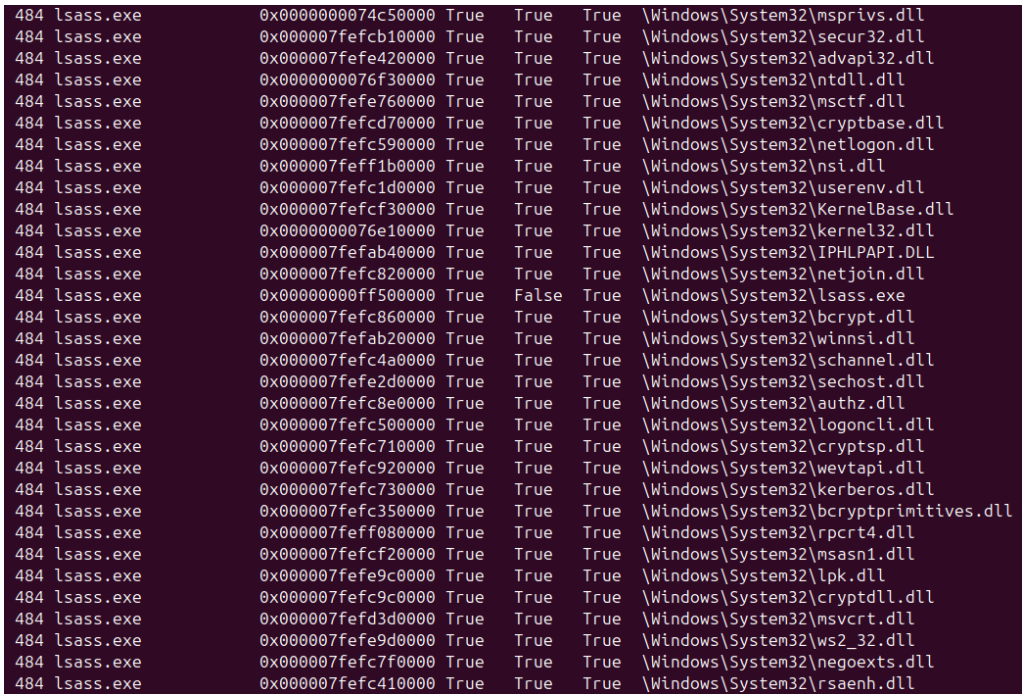
ldrmodules: They list loaded modules and their details for each process in the system. It provides information about executable modules loaded into memory, including their base address, size, and file path.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 ldrmodules
Volatility Foundation Volatility Framework 2.6.1
Pid      Process              Base               InLoad InInit InMem MappedPath
-------- -------------------- ------------------ ------ ------ ----- ----------
       4 System               0x0000000076f30000 False  False  False \Windows\System32\ntdll.dll
       4 System               0x0000000077110000 False  False  False \Windows\SysWOW64\ntdll.dll
     252 smss.exe             0x0000000048570000 True   False  True  \Windows\System32\smss.exe
     252 smss.exe             0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
     328 csrss.exe            0x00000000001a0000 False  False  False \Windows\Fonts\vgasys.fon
     328 csrss.exe            0x000000004a530000 True   False  True  \Windows\System32\csrss.exe
     328 csrss.exe            0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
     328 csrss.exe            0x000007fefd470000 True   True   True  \Windows\System32\gdi32.dll
     328 csrss.exe            0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
     328 csrss.exe            0x000007fefcd80000 True   True   True  \Windows\System32\sxs.dll
     328 csrss.exe            0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
     328 csrss.exe            0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
     328 csrss.exe            0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
     328 csrss.exe            0x000007fefcee0000 True   True   True  \Windows\System32\basesrv.dll
     328 csrss.exe            0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
     328 csrss.exe            0x000007fefe870000 True   True   True  \Windows\System32\usp10.dll
     328 csrss.exe            0x000007fefcf00000 True   True   True  \Windows\System32\csrsrv.dll
     328 csrss.exe            0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
     328 csrss.exe            0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
     376 wininit.exe          0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
     376 wininit.exe          0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
     376 wininit.exe          0x000007fefcb10000 True   True   True  \Windows\System32\secur32.dll
     376 wininit.exe          0x000007fefe760000 True   True   True  \Windows\System32\msctf.dll
     376 wininit.exe          0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
     376 wininit.exe          0x000007feff1b0000 True   True   True  \Windows\System32\nsi.dll
     376 wininit.exe          0x000007fefe9d0000 True   True   True  \Windows\System32\ws2_32.dll
     376 wininit.exe          0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
     376 wininit.exe          0x000007fefcce0000 True   True   True  \Windows\System32\sspicli.dll
```

```
     376 wininit.exe          0x000007fefe420000 True   True   True  \Windows\System32\advapi32.dll
     376 wininit.exe          0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
     376 wininit.exe          0x000007fefc6b0000 True   True   True  \Windows\System32\mswsock.dll
     376 wininit.exe          0x000007fefe2d0000 True   True   True  \Windows\System32\sechost.dll
     376 wininit.exe          0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
     376 wininit.exe          0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
     376 wininit.exe          0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
     376 wininit.exe          0x000007fefcd10000 True   True   True  \Windows\System32\apphelp.dll
     376 wininit.exe          0x00000000ff450000 True   False  True  \Windows\System32\wininit.exe
     376 wininit.exe          0x000007fefce60000 True   True   True  \Windows\System32\RpcRtRemote.dll
     376 wininit.exe          0x000007fefd470000 True   True   True  \Windows\System32\gdi32.dll
     376 wininit.exe          0x000007fefce80000 True   True   True  \Windows\System32\profapi.dll
     376 wininit.exe          0x000007fefc6a0000 True   True   True  \Windows\System32\wship6.dll
     376 wininit.exe          0x000007fefc0b0000 True   True   True  \Windows\System32\WSHTCPIP.DLL
     376 wininit.exe          0x000007fefeac0000 True   True   True  \Windows\System32\imm32.dll
     376 wininit.exe          0x000007fefc2e0000 True   True   True  \Windows\System32\credssp.dll
     376 wininit.exe          0x000007fefe870000 True   True   True  \Windows\System32\usp10.dll
     388 csrss.exe            0x00000000001a0000 False  False  False \Windows\Fonts\vgasys.fon
     388 csrss.exe            0x0000000000ed0000 False  False  False \Windows\Fonts\dosapp.fon
     388 csrss.exe            0x000000004a530000 True   False  True  \Windows\System32\csrss.exe
     388 csrss.exe            0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
     388 csrss.exe            0x0000000000ee0000 False  False  False \Windows\Fonts\cga40woa.fon
     388 csrss.exe            0x000007fefd470000 True   True   True  \Windows\System32\gdi32.dll
     388 csrss.exe            0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
     388 csrss.exe            0x000007fefcd80000 True   True   True  \Windows\System32\sxs.dll
     388 csrss.exe            0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
     388 csrss.exe            0x000007fefce90000 True   True   True  \Windows\System32\sxssrv.dll
     388 csrss.exe            0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
     388 csrss.exe            0x0000000000ec0000 False  False  False \Windows\Fonts\vgaoem.fon
     388 csrss.exe            0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
     388 csrss.exe            0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
     388 csrss.exe            0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
```

```
388 csrss.exe           0x0000000000ef0000 False  False  False \Windows\Fonts\cga80woa.fon
388 csrss.exe           0x000007fefe870000 True   True   True  \Windows\System32\usp10.dll
388 csrss.exe           0x000007fefcf00000 True   True   True  \Windows\System32\csrsrv.dll
388 csrss.exe           0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
388 csrss.exe           0x0000000000f00000 False  False  False \Windows\Fonts\ega40woa.fon
424 winlogon.exe        0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
424 winlogon.exe        0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
424 winlogon.exe        0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
424 winlogon.exe        0x000007fefe760000 True   True   True  \Windows\System32\msctf.dll
424 winlogon.exe        0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
424 winlogon.exe        0x000007fefae20000 True   True   True  \Windows\System32\slc.dll
424 winlogon.exe        0x000007fefa9f0000 True   True   True  \Windows\System32\wkscli.dll
424 winlogon.exe        0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
424 winlogon.exe        0x000007fef9be0000 True   True   True  \Windows\System32\mpr.dll
424 winlogon.exe        0x000007fefe420000 True   True   True  \Windows\System32\advapi32.dll
424 winlogon.exe        0x000007fefb630000 True   True   True  \Windows\System32\uxtheme.dll
424 winlogon.exe        0x000007fefee50000 True   True   True  \Windows\System32\ole32.dll
424 winlogon.exe        0x000007fefac80000 True   True   True  \Windows\System32\WindowsCodecs.dll
424 winlogon.exe        0x000007fefe2d0000 True   True   True  \Windows\System32\sechost.dll
424 winlogon.exe        0x00000000ff0e0000 True   False  True  \Windows\System32\winlogon.exe
424 winlogon.exe        0x000007fefc710000 True   True   True  \Windows\System32\cryptsp.dll
424 winlogon.exe        0x000007fefaa10000 True   True   True  \Windows\System32\netutils.dll
424 winlogon.exe        0x000007fefa5c0000 True   True   True  \Windows\System32\UXInit.dll
424 winlogon.exe        0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
424 winlogon.exe        0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
424 winlogon.exe        0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
424 winlogon.exe        0x000007fefc410000 True   True   True  \Windows\System32\rsaenh.dll
424 winlogon.exe        0x000007fefcd10000 True   True   True  \Windows\System32\apphelp.dll
424 winlogon.exe        0x000007fefce20000 True   True   True  \Windows\System32\winsta.dll
424 winlogon.exe        0x000007fefcce0000 True   True   True  \Windows\System32\sspicli.dll
424 winlogon.exe        0x000007fefce60000 True   True   True  \Windows\System32\RpcRtRemote.dll
424 winlogon.exe        0x000007fefd470000 True   True   True  \Windows\System32\gdi32.dll
```

```
424 winlogon.exe        0x000007fefce80000 True   True   True  \Windows\System32\profapi.dll
424 winlogon.exe        0x000007fefeac0000 True   True   True  \Windows\System32\imm32.dll
424 winlogon.exe        0x000007fefe870000 True   True   True  \Windows\System32\usp10.dll
468 services.exe        0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
468 services.exe        0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
468 services.exe        0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
468 services.exe        0x000007fefe760000 True   True   True  \Windows\System32\msctf.dll
468 services.exe        0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
468 services.exe        0x000007fefc990000 True   True   True  \Windows\System32\srvcli.dll
468 services.exe        0x000007feff1b0000 True   True   True  \Windows\System32\nsi.dll
468 services.exe        0x000007fefe9d0000 True   True   True  \Windows\System32\ws2_32.dll
468 services.exe        0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
468 services.exe        0x000007fefcce0000 True   True   True  \Windows\System32\sspicli.dll
468 services.exe        0x000007fefe420000 True   True   True  \Windows\System32\advapi32.dll
468 services.exe        0x000007fefac60000 True   True   True  \Windows\System32\wtsapi32.dll
468 services.exe        0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
468 services.exe        0x000007fefe2d0000 True   True   True  \Windows\System32\sechost.dll
468 services.exe        0x000007fefc8e0000 True   True   True  \Windows\System32\authz.dll
468 services.exe        0x000007fefcb10000 True   True   True  \Windows\System32\secur32.dll
468 services.exe        0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
468 services.exe        0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
468 services.exe        0x00000000ffa00000 True   False  True  \Windows\System32\services.exe
468 services.exe        0x000007fefcd10000 True   True   True  \Windows\System32\apphelp.dll
468 services.exe        0x000007fefce20000 True   True   True  \Windows\System32\winsta.dll
468 services.exe        0x000007fefce60000 True   True   True  \Windows\System32\RpcRtRemote.dll
468 services.exe        0x000007fefd470000 True   True   True  \Windows\System32\gdi32.dll
468 services.exe        0x000007fefce80000 True   True   True  \Windows\System32\profapi.dll
468 services.exe        0x000007fefc2a0000 True   True   True  \Windows\System32\ubpm.dll
468 services.exe        0x000007fefeac0000 True   True   True  \Windows\System32\imm32.dll
468 services.exe        0x000007fefc2e0000 True   True   True  \Windows\System32\credssp.dll
468 services.exe        0x000007fefe870000 True   True   True  \Windows\System32\usp10.dll
484 lsass.exe           0x0000000076d10000 True   True   True  \Windows\System32\user32.dll
```



```
484 lsass.exe           0x0000000074c50000 True   True   True  \Windows\System32\msprivs.dll
484 lsass.exe           0x000007fefcb10000 True   True   True  \Windows\System32\secur32.dll
484 lsass.exe           0x000007fefe420000 True   True   True  \Windows\System32\advapi32.dll
484 lsass.exe           0x0000000076f30000 True   True   True  \Windows\System32\ntdll.dll
484 lsass.exe           0x000007fefe760000 True   True   True  \Windows\System32\msctf.dll
484 lsass.exe           0x000007fefcd70000 True   True   True  \Windows\System32\cryptbase.dll
484 lsass.exe           0x000007fefc590000 True   True   True  \Windows\System32\netlogon.dll
484 lsass.exe           0x000007feff1b0000 True   True   True  \Windows\System32\nsi.dll
484 lsass.exe           0x000007fefc1d0000 True   True   True  \Windows\System32\userenv.dll
484 lsass.exe           0x000007fefcf30000 True   True   True  \Windows\System32\KernelBase.dll
484 lsass.exe           0x0000000076e10000 True   True   True  \Windows\System32\kernel32.dll
484 lsass.exe           0x000007fefab40000 True   True   True  \Windows\System32\IPHLPAPI.DLL
484 lsass.exe           0x000007fefc820000 True   True   True  \Windows\System32\netjoin.dll
484 lsass.exe           0x00000000ff500000 True   False  True  \Windows\System32\lsass.exe
484 lsass.exe           0x000007fefc860000 True   True   True  \Windows\System32\bcrypt.dll
484 lsass.exe           0x000007fefab20000 True   True   True  \Windows\System32\winnsi.dll
484 lsass.exe           0x000007fefc4a0000 True   True   True  \Windows\System32\schannel.dll
484 lsass.exe           0x000007fefe2d0000 True   True   True  \Windows\System32\sechost.dll
484 lsass.exe           0x000007fefc8e0000 True   True   True  \Windows\System32\authz.dll
484 lsass.exe           0x000007fefc500000 True   True   True  \Windows\System32\logoncli.dll
484 lsass.exe           0x000007fefc710000 True   True   True  \Windows\System32\cryptsp.dll
484 lsass.exe           0x000007fefc920000 True   True   True  \Windows\System32\wevtapi.dll
484 lsass.exe           0x000007fefc730000 True   True   True  \Windows\System32\kerberos.dll
484 lsass.exe           0x000007fefc350000 True   True   True  \Windows\System32\bcryptprimitives.dll
484 lsass.exe           0x000007feff080000 True   True   True  \Windows\System32\rpcrt4.dll
484 lsass.exe           0x000007fefcf20000 True   True   True  \Windows\System32\msasn1.dll
484 lsass.exe           0x000007fefe9c0000 True   True   True  \Windows\System32\lpk.dll
484 lsass.exe           0x000007fefc9c0000 True   True   True  \Windows\System32\cryptdll.dll
484 lsass.exe           0x000007fefd3d0000 True   True   True  \Windows\System32\msvcrt.dll
484 lsass.exe           0x000007fefe9d0000 True   True   True  \Windows\System32\ws2_32.dll
484 lsass.exe           0x000007fefc7f0000 True   True   True  \Windows\System32\negoexts.dll
484 lsass.exe           0x000007fefc410000 True   True   True  \Windows\System32\rsaenh.dll
```

Here are some observations:

1. **Malicious Activity:**
   - Process **huuhroi.exe** stands out as potentially malicious due to its absence of a mapped path. This lack of a mapped path suggests that it may not be a legitimate process and could be indicative of malware or malicious activity.
   - Another suspicious activity is the presence of multiple instances of **mscorsvw.exe** with mapped paths to directories like **\Windows\Microsoft.NET\Framework\v2.0.50727** and **\Windows\Microsoft.NET\Framework64\v2.0.50727\.** While **mscorsvw.exe** is a legitimate Microsoft process associated with .NET Framework optimization, the presence of multiple instances may indicate abnormal behavior and potentially malicious activity, especially if these processes are not typically found running concurrently.
2. **Legal Activity:**
   - System processes such as **smss.exe, csrss.exe, wininit.exe, winlogon.exe, services.exe,** and **lsass.exe** have mapped paths to

essential system directories like **\Windows\System32**, indicating their legitimacy as core Windows components.

modscan: It is designed to scan the memory dump for loaded kernel modules (drivers) and provide information about them, such as their base addresses, sizes, and file paths on disk.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 modscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                Base                             Size File
------------------ ------------------- ------------------ ------------------ ----
0x000000007d67ad60 spsys.sys           0xfffff88003b6c000            0x71000 \SystemRoot\system32\drivers\spsys.sys
0x000000007e0332e0 srv2.sys            0xfffff88002a00000             0x6b000 \SystemRoot\System32\DRIVERS\srv2.sys
0x000000007e1aae00 HIDCLASS.SYS        0xfffff88003b44000            0x19000 \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
0x000000007e1e6c80 mouhid.sys          0xfffff88003b5f000             0xd000 \SystemRoot\system32\DRIVERS\mouhid.sys
0x000000007e2858f0 lltdio.sys          0xfffff880035a5000            0x15000 \SystemRoot\system32\DRIVERS\lltdio.sys
0x000000007e28e180 rspndr.sys          0xfffff880035ba000            0x18000 \SystemRoot\system32\DRIVERS\rspndr.sys
0x000000007e31c0c0 bowser.sys          0xfffff88002747000             0x1e000 \SystemRoot\system32\DRIVERS\bowser.sys
0x000000007e32cb90 tcpipreg.sys        0xfffff88002b94000            0x12000 \SystemRoot\System32\drivers\tcpipreg.sys
0x000000007e350010 mpsdrv.sys          0xfffff88002765000            0x18000 \SystemRoot\System32\drivers\mpsdrv.sys
0x000000007e35b770 mrxsmb.sys          0xfffff8800277d000             0x2d000 \SystemRoot\system32\DRIVERS\mrxsmb.sys
0x000000007e360a20 mrxsmb10.sys        0xfffff880027aa000             0x4d000 \SystemRoot\system32\DRIVERS\mrxsmb10.sys
0x000000007e367310 mrxsmb20.sys        0xfffff88002600000             0x24000 \SystemRoot\system32\DRIVERS\mrxsmb20.sys
0x000000007e37e1a0 srv.sys             0xfffff88003a9d000            0x99000 \SystemRoot\System32\DRIVERS\srv.sys
0x000000007e3ca8c0 peauth.sys          0xfffff88002ab2000             0xa6000 \SystemRoot\system32\drivers\peauth.sys
0x000000007e3d45d0 srvnet.sys          0xfffff88002b63000            0x31000 \SystemRoot\System32\DRIVERS\srvnet.sys
0x000000007e3d4e70 secdrv.SYS          0xfffff88002b58000             0xb000 \SystemRoot\System32\Drivers\secdrv.SYS
0x000000007e428770 NDProxy.SYS         0xfffff880034de000            0x15000 \SystemRoot\System32\Drivers\NDProxy.SYS
0x000000007e445740 dump_dumpfve.sys    0xfffff88003516000            0x13000 \SystemRoot\System32\Drivers\dump_dumpfve.
sys
0x000000007e44cc60 Dxapi.sys           0xfffff88003529000             0xc000 \SystemRoot\System32\drivers\Dxapi.sys
0x000000007e450790 dump_atapi.sys      0xfffff8800350d000             0x9000 \SystemRoot\System32\Drivers\dump_atapi.sy
s
0x000000007e456370 dump_ataport.sys    0xfffff88003501000             0xc000 \SystemRoot\System32\Drivers\dump_dumpata.
sys
0x000000007e4c82a0 dxg.sys             0xfffff96000510000             0x1e000 \SystemRoot\System32\drivers\dxg.sys
0x000000007e4e1640 framebuf.dll        0xfffff960008f0000             0x9000 \SystemRoot\System32\framebuf.dll
0x000000007e4f2230 hidusb.sys          0xfffff88003b36000             0xe000 \SystemRoot\system32\DRIVERS\hidusb.sys
0x000000007e516a10 USBD.SYS            0xfffff88003b5d000             0x2000 \SystemRoot\system32\DRIVERS\USBD.SYS
0x000000007e519340 HIDPARSE.SYS        0xfffff8800356a000             0x9000 \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
0x000000007e5a22a0 luafv.sys           0xfffff88003582000            0x23000 \SystemRoot\system32\drivers\luafv.sys
0x000000007e5ffc40 HTTP.sys            0xfffff8800267e000            0xc9000 \SystemRoot\system32\drivers\HTTP.sys
0x000000007e7ee2c0 usbhub.sys          0xfffff88003484000             0x5a000 \SystemRoot\system32\DRIVERS\usbhub.sys
0x000000007ea02e30 swenum.sys          0xfffff880033fe000             0x2000 \SystemRoot\system32\DRIVERS\swenum.sys
0x000000007ea03170 CompositeBus.sys    0xfffff88003216000            0x10000 \SystemRoot\system32\DRIVERS\CompositeBus
sys
0x000000007ea1a170 AgileVpn.sys        0xfffff88003226000            0x16000 \SystemRoot\system32\DRIVERS\AgileVpn.sys
0x000000007ec3e860 win32k.sys          0xfffff96000040000           0x310000 \SystemRoot\System32\win32k.sys
0x000000007ed27700 cdrom.sys           0xfffff88001590000             0x2a000 \SystemRoot\system32\DRIVERS\cdrom.sys
0x000000007ed287a0 Beep.SYS            0xfffff880019e3000             0x7000 \SystemRoot\System32\Drivers\Beep.SYS
0x000000007ed2a1d0 Null.SYS            0xfffff880019da000             0x9000 \SystemRoot\System32\Drivers\Null.SYS
0x000000007ed2a790 vga.sys             0xfffff880019ea000             0xe000 \SystemRoot\System32\drivers\vga.sys
0x000000007ed2c970 VIDEOPRT.SYS        0xfffff880015ba000            0x25000 \SystemRoot\System32\drivers\VIDEOPRT.SYS
0x000000007ed2cf20 watchdog.sys        0xfffff88001600000            0x10000 \SystemRoot\System32\drivers\watchdog.sys
0x000000007ed2d200 rdpencdd.sys        0xfffff880015df000             0x9000 \SystemRoot\system32\drivers\rdpencdd.sys
0x000000007ed2d4f0 usbohci.sys         0xfffff8800338d000             0xb000 \SystemRoot\system32\DRIVERS\usbohci.sys
0x000000007ed2dca0 RDPCDD.sys          0xfffff88001610000             0x9000 \SystemRoot\System32\DRIVERS\RDPCDD.sys
0x000000007ed2e010 afd.sys             0xfffff88001022000            0x89000 \SystemRoot\system32\drivers\afd.sys
0x000000007ed35660 rdprefmp.sys        0xfffff880015e8000             0x9000 \SystemRoot\system32\drivers\rdprefmp.sys
0x000000007ed36bb0 Msfs.SYS            0xfffff880015f1000             0xb000 \SystemRoot\System32\Drivers\Msfs.SYS
0x000000007ed37530 Npfs.SYS            0xfffff88001400000            0x11000 \SystemRoot\System32\Drivers\Npfs.SYS
0x000000007ed386b0 tdx.sys             0xfffff88001000000            0x22000 \SystemRoot\system32\DRIVERS\tdx.sys
0x000000007ed38be0 TDI.SYS             0xfffff88001236000             0xd000 \SystemRoot\system32\DRIVERS\TDI.SYS
0x000000007ed44ba0 termdd.sys          0xfffff88002cac000            0x14000 \SystemRoot\system32\DRIVERS\termdd.sys
0x000000007ed498b0 netbt.sys           0xfffff88002c0e000            0x45000 \SystemRoot\System32\DRIVERS\netbt.sys
0x000000007ed4a350 pacer.sys           0xfffff88002c5c000            0x26000 \SystemRoot\system32\DRIVERS\pacer.sys
0x000000007ed4b8d0 wfplwf.sys          0xfffff88002c53000             0x9000 \SystemRoot\system32\DRIVERS\wfplwf.sys
0x000000007ed4d6d0 wanarp.sys          0xfffff88002c91000             0x1b000 \SystemRoot\system32\DRIVERS\wanarp.sys
0x000000007ed4fc40 rdbss.sys           0xfffff88002cc0000            0x51000 \SystemRoot\system32\DRIVERS\rdbss.sys
0x000000007ed52210 csc.sys             0xfffff88002d37000            0x83000 \SystemRoot\system32\drivers\csc.sys
0x000000007ed52970 discache.sys        0xfffff88002d28000             0xf000 \SystemRoot\System32\drivers\discache.sys
```

```
0x000000007ed55840 nsiproxy.sys         0xfffff88002d11000          0xc000 \SystemRoot\system32\drivers\nsiproxy.sys
0x000000007ed56710 mssmbios.sys         0xfffff88002d1d000          0xb000 \SystemRoot\system32\DRIVERS\mssmbios.sys
0x000000007ed60010 blbdrive.sys         0xfffff88002dd8000         0x11000 \SystemRoot\system32\DRIVERS\blbdrive.sys
0x000000007ed60760 dfsc.sys             0xfffff88002dba000          0x1e000 \SystemRoot\System32\Drivers\dfsc.sys
0x000000007ed78f20 E1G6032E.sys         0xfffff88003369000          0x24000 \SystemRoot\system32\DRIVERS\E1G6032E.sys
0x000000007ed79d40 i8042prt.sys         0xfffff8800331f000          0x1e000 \SystemRoot\system32\DRIVERS\i8042prt.sys
0x000000007ed7b5e0 kbdclass.sys         0xfffff8800333d000           0xf000 \SystemRoot\system32\DRIVERS\kbdclass.sys
0x000000007ed8e2c0 mouclass.sys         0xfffff8800334c000           0xf000 \SystemRoot\system32\DRIVERS\mouclass.sys
0x000000007ed95010 vgapnp.sys           0xfffff8800335b000           0xe000 \SystemRoot\system32\DRIVERS\vgapnp.sys
0x000000007ed9a380 crashdmp.sys         0xfffff880034f3000           0xe000 \SystemRoot\System32\Drivers\crashdmp.sys
0x000000007edad110 USBPORT.SYS          0xfffff88003398000          0x56000 \SystemRoot\system32\DRIVERS\USBPORT.SYS
0x000000007edb06d0 rdpbus.sys           0xfffff880033f3000           0xb000 \SystemRoot\system32\DRIVERS\rdpbus.sys
0x000000007ede5c60 ndistapi.sys         0xfffff88003260000           0xc000 \SystemRoot\system32\DRIVERS\ndistapi.sys
0x000000007ede6f30 ndiswan.sys          0xfffff8800326c000          0x2f000 \SystemRoot\system32\DRIVERS\ndiswan.sys
0x000000007ede9180 CmBatt.sys           0xfffff880033ee000           0x5000 \SystemRoot\system32\DRIVERS\CmBatt.sys
0x000000007edf3170 intelppm.sys         0xfffff88003200000          0x16000 \SystemRoot\system32\DRIVERS\intelppm.sys
0x000000007edf5010 raspppoe.sys         0xfffff8800329b000          0x1b000 \SystemRoot\system32\DRIVERS\raspppoe.sys
0x000000007edfb010 raspptp.sys          0xfffff880032b6000          0x21000 \SystemRoot\system32\DRIVERS\raspptp.sys
0x000000007edfd5d0 umbus.sys            0xfffff88003472000          0x12000 \SystemRoot\system32\DRIVERS\umbus.sys
0x000000007edfe010 rassstp.sys          0xfffff880032d7000          0x1a000 \SystemRoot\system32\DRIVERS\rassstp.sys
0x000000007ef91500 tunnel.sys           0xfffff880032f9000          0x26000 \SystemRoot\system32\DRIVERS\tunnel.sys
0x000000007ef989a0 netbios.sys          0xfffff88002c82000           0xf000 \SystemRoot\system32\DRIVERS\netbios.sys
0x000000007f2051e0 rasl2tp.sys          0xfffff8800323c000          0x24000 \SystemRoot\system32\DRIVERS\rasl2tp.sys
0x000000007f5ae850 ks.sys               0xfffff8800342f000          0x43000 \SystemRoot\system32\DRIVERS\ks.sys
0x000000007ff2c010 TSDDD.dll            0xfffff96000680000           0xa000 \SystemRoot\System32\TSDDD.dll
0x000000007ffa8a20 monitor.sys          0xfffff88003535000           0xe000 \SystemRoot\system32\DRIVERS\monitor.sys
0x000000007ffb60c0 ntoskrnl.exe         0xfffff8000261b000         0x5ea000 \SystemRoot\system32\ntoskrnl.exe
0x000000007ffbc690 PSHED.dll            0xfffff88000d0a000         0x14000 \SystemRoot\system32\PSHED.dll
0x000000007ffbc770 mcupdate.dll         0xfffff88000cbb000          0x4f000 \SystemRoot\system32\mcupdate_GenuineIntel
.dll
0x000000007ffbc860 kdcom.dll            0xfffff80000bad000           0xa000 \SystemRoot\system32\kdcom.dll
0x000000007ffbc940 hal.dll              0xfffff80002c05000          0x49000 \SystemRoot\system32\hal.dll
```

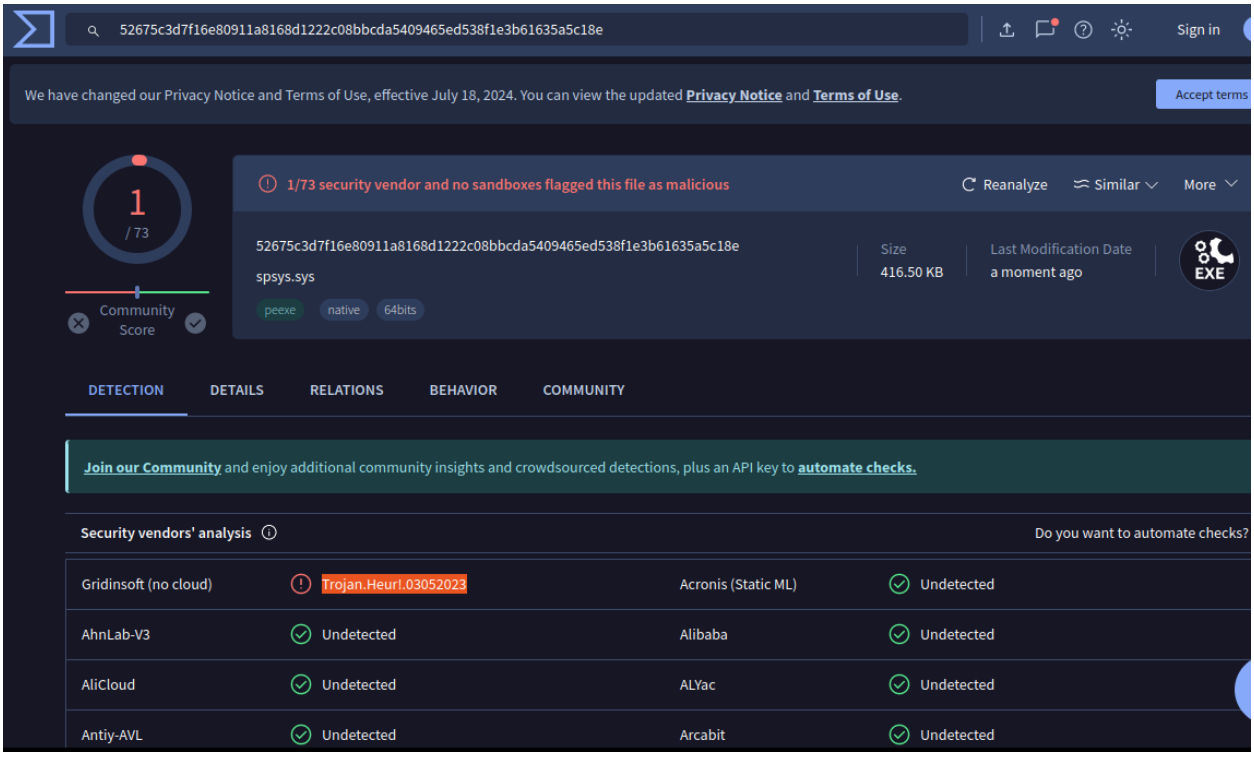
```
0x000000007ffbd010 CLFS.SYS             0xfffff88000d1e000          0x5e000 \SystemRoot\system32\CLFS.SYS
0x000000007ffbd150 mountmgr.sys         0xfffff88000c6c000          0x1a000 \SystemRoot\System32\drivers\mountmgr.sys
0x000000007ffbd240 PCIIDEX.SYS          0xfffff88000c5c000          0x10000 \SystemRoot\system32\drivers\PCIIDEX.SYS
0x000000007ffbd330 intelide.sys         0xfffff88000e77000           0x8000 \SystemRoot\system32\drivers\intelide.sys
0x000000007ffbd420 volmgrx.sys          0xfffff88000c00000          0x5c000 \SystemRoot\System32\drivers\volmgrx.sys
0x000000007ffbd510 volmgr.sys           0xfffff88000dd0000          0x15000 \SystemRoot\system32\drivers\volmgr.sys
0x000000007ffbd5f0 BATTC.SYS            0xfffff88000dc4000           0xc000 \SystemRoot\system32\DRIVERS\BATTC.SYS
0x000000007ffbd6d0 compbatt.sys         0xfffff88000ff2000           0x9000 \SystemRoot\system32\DRIVERS\compbatt.sys
0x000000007ffbd7c0 partmgr.sys          0xfffff88000daf000          0x15000 \SystemRoot\System32\drivers\partmgr.sys
0x000000007ffbd8b0 vdrvroot.sys         0xfffff88000e6a000           0xd000 \SystemRoot\system32\drivers\vdrvroot.sys
0x000000007ffbd9a0 pci.sys              0xfffff88000d7c000          0x33000 \SystemRoot\system32\drivers\pci.sys
0x000000007ffbda80 msisadrv.sys         0xfffff88000e60000           0xa000 \SystemRoot\system32\drivers\msisadrv.sys
0x000000007ffbdb70 WMILIB.SYS           0xfffff88000e57000           0x9000 \SystemRoot\system32\drivers\WMILIB.SYS
0x000000007ffbdc50 ACPI.sys             0xfffff88000e00000          0x57000 \SystemRoot\system32\drivers\ACPI.sys
0x000000007ffbdd40 WDFLDR.SYS           0xfffff88000fe3000           0xf000 \SystemRoot\system32\drivers\WDFLDR.SYS
0x000000007ffbde20 Wdf01000.sys         0xfffff88000f3f000          0xa4000 \SystemRoot\system32\drivers\Wdf01000.sys
0x000000007ffbdf20 CI.dll               0xfffff88000e7f000          0xc0000 \SystemRoot\system32\CI.dll
0x000000007ffbe010 atapi.sys            0xfffff88000c86000           0x9000 \SystemRoot\system32\drivers\atapi.sys
0x000000007ffbe0f0 spldr.sys            0xfffff880018c7000           0x8000 \SystemRoot\System32\Drivers\spldr.sys
0x000000007ffbe1d0 fwpkclnt.sys         0xfffff88001821000          0x4a000 \SystemRoot\System32\drivers\fwpkclnt.sys
0x000000007ffbe2c0 tcpip.sys            0xfffff8800161d000         0x204000 \SystemRoot\System32\drivers\tcpip.sys
0x000000007ffbe3e0 ksecpkg.sys          0xfffff88001565000          0x2b000 \SystemRoot\System32\Drivers\ksecpkg.sys
0x000000007ffbe4d0 NETIO.SYS            0xfffff88001505000          0x60000 \SystemRoot\system32\drivers\NETIO.SYS
0x000000007ffbe5c0 ndis.sys             0xfffff88001412000          0xf3000 \SystemRoot\system32\drivers\ndis.sys
0x000000007ffbe6c0 Fs_Rec.sys           0xfffff8800122c000           0xa000 \SystemRoot\System32\Drivers\Fs_Rec.sys
0x000000007ffbe7a0 pcw.sys              0xfffff8800121b000          0x11000 \SystemRoot\System32\drivers\pcw.sys
0x000000007ffbe880 cng.sys              0xfffff8800118c000          0x72000 \SystemRoot\System32\Drivers\cng.sys
0x000000007ffbe970 ksecdd.sys           0xfffff88001200000          0x1b000 \SystemRoot\System32\Drivers\ksecdd.sys
0x000000007ffbea50 msrpc.sys            0xfffff8800112e000          0x5e000 \SystemRoot\System32\Drivers\msrpc.sys
0x000000007ffbeb40 Ntfs.sys             0xfffff88001252000         0x1a3000 \SystemRoot\System32\Drivers\Ntfs.sys
0x000000007ffbec50 fileinfo.sys         0xfffff8800111a000          0x14000 \SystemRoot\system32\drivers\fileinfo.sys
0x000000007ffbed40 fltmgr.sys           0xfffff880010ce000          0x4c000 \SystemRoot\system32\drivers\fltmgr.sys
```

The potentially malicious or suspicious processes observed in the output are:

- **spsys.sys:** This process seems to have a different file path (\SystemRoot\system32\drivers\spsys.sys) compared to typical system drivers in Windows, which are usually located in \SystemRoot\System32\drivers.
- **rspndr.sys:** This process is in \SystemRoot\system32\DRIVERS, which is typical for drivers. However, its purpose and behavior may need further scrutiny.
- **secdrv.SYS:** This process is named "secdrv," which might indicate it's related to security or DRM (Digital Rights Management). Some security concerns have been associated with this driver in the past.
- **NDProxy.SYS:** The name "NDProxy" suggests it might be related to network proxy functionality, which could potentially be exploited for malicious purposes.
- **HTTP.sys:** While HTTP.sys is a legitimate Windows component responsible for processing HTTP requests, it has been targeted by attackers in the past due to its critical role in web server functionality.
- **afd.sys:** Although afd.sys is a legitimate Windows driver related to the Ancillary Function Driver for WinSock, it's worth investigating if there are any anomalies or signs of manipulation.
- **usbohci.sys:** This driver is related to USB Open Host Controller Interface. Any unusual USB activity or drivers should be investigated further, as USB devices can sometimes be used as attack vectors.
- **tcpip.sys:** While tcpip.sys is a core component of the Windows networking stack, it's worth checking for any modifications or anomalies, as network-related drivers are common targets for attackers.
- **atapi.sys:** This driver is related to ATA/ATAPI controllers. Any modifications or unusual activity related to storage drivers should be investigated thoroughly.

Let’s check **“spsys.sys”**, by submitting it to **VirusTotal** for analysis.

```
ubuntu@ubuntu-001:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 moddump -b 0xfffff88003b6c000 -D Dump
Volatility Foundation Volatility Framework 2.6.1
Module Base        Module Name          Result
------------------ -------------------- ------
0xfffff88003b6c000 spsys.sys            OK: driver.fffff88003b6c000.sys
```

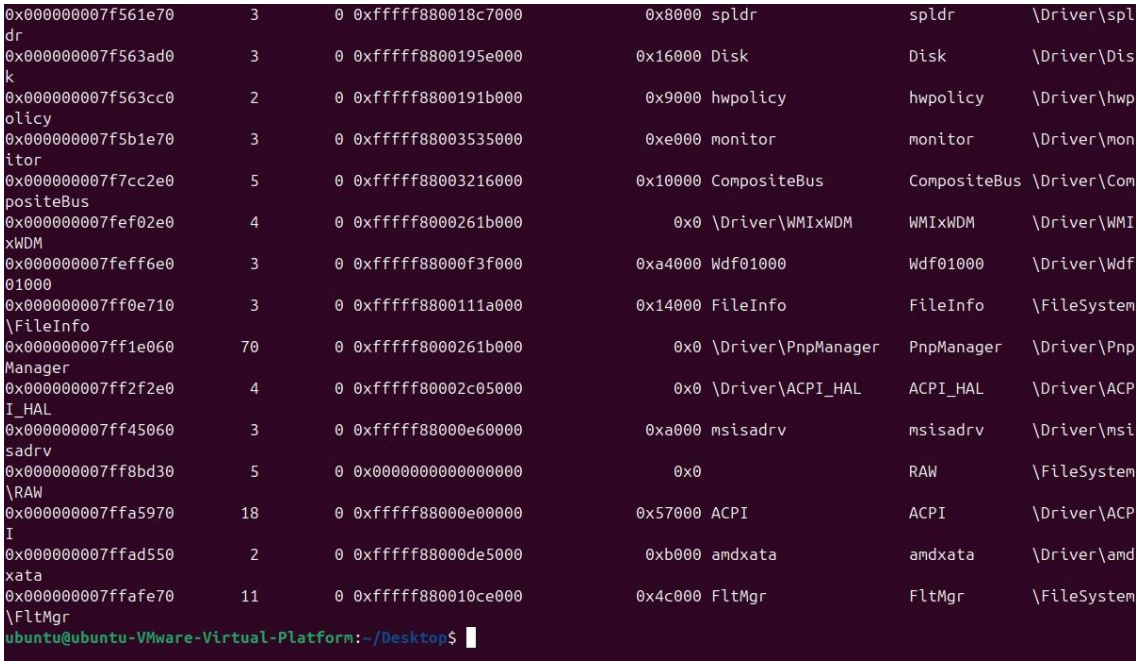


Driverscan: This plugin specifically focuses on extracting and displaying information about loaded drivers from memory dumps.

When analyzing a memory dump, understanding the drivers loaded into the system can provide valuable insights into the system's configuration, potential vulnerabilities, and signs of malicious activity. This plugin helps in this regard by parsing the memory dump and presenting information such as driver names, associated services, driver paths, and other properties.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 driverscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)              #Ptr     #Hnd Start                              Size Service Key          Name         Driver Name
------------------ -------- -------- ------------------ ------------------ -------------------- ------------ ----------
0x000000007e035840        3        0 0xfffff88002a00000            0x6b000 srv2                 srv2         \FileSystem
\srv2
0x000000007e045330        3        0 0xfffff88003a9d000            0x99000 srv                  srv          \FileSystem
\srv
0x000000007e140060        3        0 0xfffff88003b5f000             0xd000 mouhid               mouhid       \Driver\mou
hid
0x000000007e20ac80        4        0 0xfffff8800267e000            0xc9000 HTTP                 HTTP         \Driver\HTT
P
0x000000007e338bc0        3        0 0xfffff88002747000            0x1e000 bowser               bowser       \FileSystem
\bowser
0x000000007e350190        3        0 0xfffff88002765000            0x18000 mpsdrv               mpsdrv       \Driver\mps
drv
0x000000007e355de0        4        0 0xfffff8800277d000            0x2d000 mrxsmb               mrxsmb       \FileSystem
\mrxsmb
0x000000007e35b8a0        2        0 0xfffff88002b94000            0x12000 tcpipreg             tcpipreg     \Driver\tcp
ipreg
0x000000007e3652c0        2        0 0xfffff880027aa000            0x4d000 mrxsmb10             mrxsmb10     \FileSystem
\mrxsmb10
0x000000007e369e70        2        0 0xfffff88002600000            0x24000 mrxsmb20             mrxsmb20     \FileSystem
\mrxsmb20
0x000000007e3d1e70        3        0 0xfffff88002ab2000            0xa6000 PEAUTH               PEAUTH       \Driver\PEA
UTH
0x000000007e3d3100        4        0 0xfffff88002b58000             0xb000 secdrv               secdrv       \Driver\sec
drv
0x000000007e3dca90        4        0 0xfffff88002b63000            0x31000 srvnet               srvnet       \FileSystem
\srvnet
0x000000007e4285d0        3        0 0xfffff880034de000            0x15000 NDProxy              NDProxy      \Driver\NDP
roxy
```

```
0x000000007e4c47f0       13        0 0xfffff96000040000                0x0 \Driver\Win32k       Win32k       \Driver\Win
32k
0x000000007e4ecbe0        2        0 0xfffff88003582000            0x23000 luafv                luafv        \FileSystem
\luafv
0x000000007e5244e0        4        0 0xfffff88003b36000             0xe000 HidUsb               HidUsb       \Driver\Hid
Usb
0x000000007e583cb0        3        0 0xfffff880035a5000            0x15000 lltdio               lltdio       \Driver\llt
dio
0x000000007e58fd60        3        0 0xfffff880035ba000            0x18000 rspndr               rspndr       \Driver\rsp
ndr
0x000000007ea2c550        4        0 0xfffff8800338d000             0xb000 usbohci              usbohci      \Driver\usb
ohci
0x000000007ea94e70        4        0 0xfffff880033ee000             0x4500 CmBatt               CmBatt       \Driver\CmB
att
0x000000007ed27560        3        0 0xfffff88001590000            0x2a000 cdrom                cdrom        \Driver\cdr
om
0x000000007ed28060        3        0 0xfffff880019da000             0x9000 Null                 Null         \Driver\Nul
l
0x000000007ed28600        3        0 0xfffff880019e3000             0x7000 Beep                 Beep         \Driver\Bee
p
0x000000007ed2d060        3        0 0xfffff880019ea000             0xe000 VgaSave              VgaSave      \Driver\Vga
Save
0x000000007ed2db00        4        0 0xfffff88001610000             0x9000 RDPCDD               RDPCDD       \Driver\RDP
CDD
0x000000007ed34950        3        0 0xfffff880015df000             0x9000 RDPENCDD             RDPENCDD     \Driver\RDP
ENCDD
0x000000007ed35060        9        0 0xfffff88001000000            0x22000 tdx                  tdx          \Driver\tdx
0x000000007ed354c0        3        0 0xfffff880015e8000             0x9000 RDPREFMP             RDPREFMP     \Driver\RDP
REFMP
0x000000007ed36a10        3        0 0xfffff880015f1000             0xb000 Msfs                 Msfs         \FileSystem
\Msfs
0x000000007ed37390        3        0 0xfffff88001400000            0x11000 Npfs                 Npfs         \FileSystem
\Npfs
```



Here are some drivers from the output that might raise suspicion or warrant further investigation:

- **\Driver\Win32k:** This driver has an unusual name and might be worth checking for any abnormal behavior, especially considering that it's associated with the Win32k subsystem.
- **\Driver\luafv:** Similarly, the driver named "luafv" might be unfamiliar to some users. It's associated with the File System Minifilter for Virtualization, which handles file system virtualization requests. While it's not necessarily malicious, any unexpected behavior from this driver could indicate a problem.
- **\Driver\TermDD:** This driver is known to be vulnerable to exploitation in certain circumstances. Its presence might be worth investigating further, especially if there are any signs of compromise.
- **\Driver\RasSstp:** RasSstp is a driver associated with Secure Socket Tunneling Protocol (SSTP) used for VPN connections. While not inherently malicious, VPN-related drivers can sometimes be targeted by attackers for privilege escalation or bypassing network security measures.

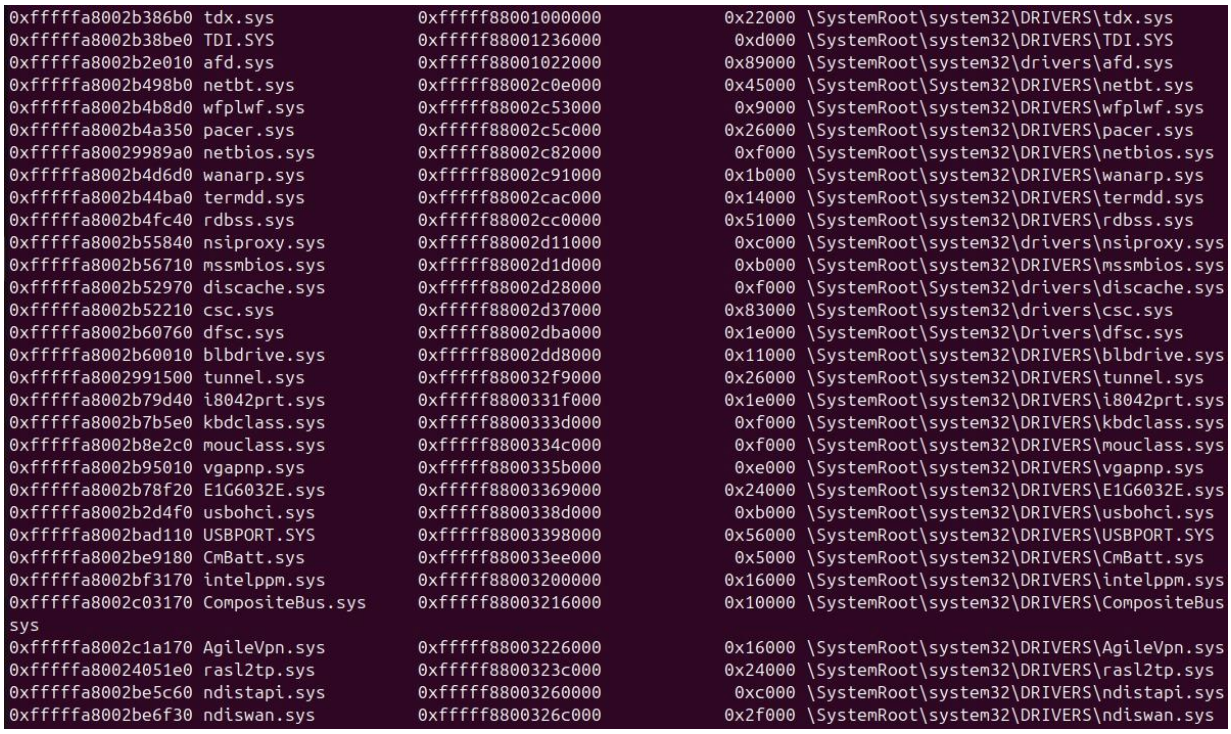
- **\Driver\NDIS:** This driver is associated with the Windows network driver interface and is crucial for network communication. However, it's worth noting that malware often attempts to tamper with network drivers to intercept or manipulate network traffic.
- **\Driver\Wdf01000:** This is the Kernel Mode Driver Framework runtime. While legitimate, it's essential to ensure that the version matches the expected one for the system and that it hasn't been tampered with.
- **\Driver\ACPI:** ACPI (Advanced Configuration and Power Interface) is a core component of modern computers, responsible for power management and hardware configuration. While not inherently suspicious, any unexpected behavior from this driver could indicate a problem.
- **\FileSystem\RAW:** The RAW file system driver might raise eyebrows as it's associated with handling raw disk access. Malware might attempt to interact with this driver to perform low-level disk operations.

These are just a few examples, but any driver with an unfamiliar name or unexpected behavior should be investigated further to ensure system integrity and security.

modules: This plugin is used to list the loaded kernel modules (drivers) in a memory dump. Kernel modules are pieces of code that can be dynamically loaded into the kernel of an operating system to extend its functionality or add support for new hardware. These modules play a crucial role in the operation of the operating system by providing various services and device access.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 modules
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                 Base                             Size File
------------------ -------------------- ---------------- ---------------- ----
0xfffffa80018370c0 ntoskrnl.exe         0xfffff8000261b000           0x5ea000 \SystemRoot\system32\ntoskrnl.exe
0xfffffa800183d940 hal.dll              0xfffff80002c05000            0x49000 \SystemRoot\system32\hal.dll
0xfffffa800183d860 kdcom.dll            0xfffff80000bad000             0xa000 \SystemRoot\system32\kdcom.dll
0xfffffa800183d770 mcupdate.dll         0xfffff88000cbb000            0x4f000 \SystemRoot\system32\mcupdate_GenuineIntel
.dll
0xfffffa800183d690 PSHED.dll            0xfffff88000d0a000            0x14000 \SystemRoot\system32\PSHED.dll
0xfffffa800183e010 CLFS.SYS             0xfffff88000d1e000             0x5e000 \SystemRoot\system32\CLFS.SYS
0xfffffa800183ef20 CI.dll               0xfffff88000e7f000             0xc0000 \SystemRoot\system32\CI.dll
0xfffffa800183ee20 Wdf01000.sys         0xfffff88000f3f000             0xa4000 \SystemRoot\system32\drivers\Wdf01000.sys
0xfffffa800183ed40 WDFLDR.SYS           0xfffff88000fe3000             0xf000 \SystemRoot\system32\drivers\WDFLDR.SYS
0xfffffa800183ec50 ACPI.sys             0xfffff88000e00000            0x57000 \SystemRoot\system32\drivers\ACPI.sys
0xfffffa800183eb70 WMILIB.SYS           0xfffff88000e57000             0x9000 \SystemRoot\system32\drivers\WMILIB.SYS
0xfffffa800183ea80 msisadrv.sys         0xfffff88000e60000             0xa000 \SystemRoot\system32\drivers\msisadrv.sys
0xfffffa800183e9a0 pci.sys              0xfffff88000d7c000            0x33000 \SystemRoot\system32\drivers\pci.sys
0xfffffa800183e8b0 vdrvroot.sys         0xfffff88000e6a000             0xd000 \SystemRoot\system32\drivers\vdrvroot.sys
0xfffffa800183e7c0 partmgr.sys          0xfffff88000daf000            0x15000 \SystemRoot\System32\drivers\partmgr.sys
0xfffffa800183e6d0 compbatt.sys         0xfffff88000ff2000             0x9000 \SystemRoot\system32\DRIVERS\compbatt.sys
0xfffffa800183e5f0 BATTC.SYS            0xfffff88000dc4000             0xc000 \SystemRoot\system32\DRIVERS\BATTC.SYS
0xfffffa800183e510 volmgr.sys           0xfffff88000dd0000            0x15000 \SystemRoot\system32\drivers\volmgr.sys
0xfffffa800183e420 volmgrx.sys          0xfffff88000c00000             0x5c000 \SystemRoot\System32\drivers\volmgrx.sys
0xfffffa800183e330 intelide.sys         0xfffff88000e77000             0x8000 \SystemRoot\system32\drivers\intelide.sys
0xfffffa800183e240 PCIIDEX.SYS          0xfffff88000c5c000            0x10000 \SystemRoot\system32\drivers\PCIIDEX.SYS
0xfffffa800183e150 mountmgr.sys         0xfffff88000c6c000             0x1a000 \SystemRoot\System32\drivers\mountmgr.sys
0xfffffa800183f010 atapi.sys            0xfffff88000c86000             0x9000 \SystemRoot\system32\drivers\atapi.sys
0xfffffa800183ff20 ataport.SYS          0xfffff88000c8f000             0x2a000 \SystemRoot\system32\drivers\ataport.SYS
0xfffffa800183fe30 amdxata.sys          0xfffff88000de5000             0xb000 \SystemRoot\system32\drivers\amdxata.sys
0xfffffa800183fd40 fltmgr.sys           0xfffff880010ce000             0x4c000 \SystemRoot\system32\drivers\fltmgr.sys
```

```
0xfffffa800183fc50 fileinfo.sys         0xfffff8800111a000            0x14000 \SystemRoot\system32\drivers\fileinfo.sys
0xfffffa800183fb40 Ntfs.sys             0xfffff88001252000            0x1a3000 \SystemRoot\System32\Drivers\Ntfs.sys
0xfffffa800183fa50 msrpc.sys            0xfffff8800112e000             0x5e000 \SystemRoot\System32\Drivers\msrpc.sys
0xfffffa800183f970 ksecdd.sys           0xfffff88001200000             0x1b000 \SystemRoot\System32\Drivers\ksecdd.sys
0xfffffa800183f880 cng.sys              0xfffff8800118c000             0x72000 \SystemRoot\System32\Drivers\cng.sys
0xfffffa800183f7a0 pcw.sys              0xfffff8800121b000             0x11000 \SystemRoot\System32\drivers\pcw.sys
0xfffffa800183f6c0 Fs_Rec.sys           0xfffff8800122c000              0xa000 \SystemRoot\System32\Drivers\Fs_Rec.sys
0xfffffa800183f5c0 ndis.sys             0xfffff88001412000             0xf3000 \SystemRoot\system32\drivers\ndis.sys
0xfffffa800183f4d0 NETIO.SYS            0xfffff88001505000             0x60000 \SystemRoot\system32\drivers\NETIO.SYS
0xfffffa800183f3e0 ksecpkg.sys          0xfffff88001565000             0x2b000 \SystemRoot\System32\Drivers\ksecpkg.sys
0xfffffa800183f2c0 tcpip.sys            0xfffff8800161d000            0x204000 \SystemRoot\System32\drivers\tcpip.sys
0xfffffa800183f1d0 fwpkclnt.sys         0xfffff88001821000             0x4a000 \SystemRoot\System32\drivers\fwpkclnt.sys
0xfffffa8001840010 vmstorfl.sys         0xfffff8800186b000             0x10000 \SystemRoot\system32\drivers\vmstorfl.sys
0xfffffa8001840f20 volsnap.sys          0xfffff8800187b000             0x4c000 \SystemRoot\system32\drivers\volsnap.sys
0xfffffa800183f0f0 spldr.sys            0xfffff880018c7000              0x8000 \SystemRoot\System32\Drivers\spldr.sys
0xfffffa8001840e30 rdyboost.sys         0xfffff880018cf000             0x3a000 \SystemRoot\System32\drivers\rdyboost.sys
0xfffffa8001840d50 mup.sys              0xfffff88001909000             0x12000 \SystemRoot\System32\Drivers\mup.sys
0xfffffa8001840c60 hwpolicy.sys         0xfffff8800191b000              0x9000 \SystemRoot\System32\drivers\hwpolicy.sys
0xfffffa8001840b80 fvevol.sys           0xfffff88001924000             0x3a000 \SystemRoot\System32\DRIVERS\fvevol.sys
0xfffffa8001840aa0 disk.sys             0xfffff8800195e000             0x16000 \SystemRoot\system32\drivers\disk.sys
0xfffffa80018409b0 CLASSPNP.SYS         0xfffff88001974000             0x30000 \SystemRoot\system32\drivers\CLASSPNP.SYS
0xfffffa8002b27700 cdrom.sys            0xfffff88001590000             0x2a000 \SystemRoot\system32\DRIVERS\cdrom.sys
0xfffffa8002b2a1d0 Null.SYS             0xfffff880019da000              0x9000 \SystemRoot\System32\Drivers\Null.SYS
0xfffffa8002b287a0 Beep.SYS             0xfffff880019e3000              0x7000 \SystemRoot\System32\Drivers\Beep.SYS
0xfffffa8002b2a790 vga.sys              0xfffff880019ea000              0xe000 \SystemRoot\System32\drivers\vga.sys
0xfffffa8002b2c970 VIDEOPRT.SYS         0xfffff880015ba000             0x25000 \SystemRoot\System32\drivers\VIDEOPRT.SYS
0xfffffa8002b2cf20 watchdog.sys         0xfffff88001600000             0x10000 \SystemRoot\System32\drivers\watchdog.sys
0xfffffa8002b2dca0 RDPCDD.sys           0xfffff88001610000              0x9000 \SystemRoot\System32\DRIVERS\RDPCDD.sys
0xfffffa8002b2d200 rdpencdd.sys         0xfffff880015df000              0x9000 \SystemRoot\system32\drivers\rdpencdd.sys
0xfffffa8002b35660 rdprefmp.sys         0xfffff880015e8000              0x9000 \SystemRoot\system32\drivers\rdprefmp.sys
0xfffffa8002b36bb0 Msfs.SYS             0xfffff880015f1000              0xb000 \SystemRoot\System32\Drivers\Msfs.SYS
0xfffffa8002b37530 Npfs.SYS             0xfffff88001400000             0x11000 \SystemRoot\System32\Drivers\Npfs.SYS
```



```
0xfffffa8002b386b0 tdx.sys             0xfffff88001000000          0x22000 \SystemRoot\system32\DRIVERS\tdx.sys
0xfffffa8002b38be0 TDI.SYS             0xfffff88001236000           0xd000 \SystemRoot\system32\DRIVERS\TDI.SYS
0xfffffa8002b2e010 afd.sys             0xfffff88001022000          0x89000 \SystemRoot\system32\drivers\afd.sys
0xfffffa8002b498b0 netbt.sys           0xfffff88002c0e000          0x45000 \SystemRoot\System32\DRIVERS\netbt.sys
0xfffffa8002b4b8d0 wfplwf.sys          0xfffff88002c53000           0x9000 \SystemRoot\system32\DRIVERS\wfplwf.sys
0xfffffa8002b4a350 pacer.sys           0xfffff88002c5c000          0x26000 \SystemRoot\system32\DRIVERS\pacer.sys
0xfffffa80029989a0 netbios.sys         0xfffff88002c82000           0xf000 \SystemRoot\system32\DRIVERS\netbios.sys
0xfffffa8002b4d6d0 wanarp.sys          0xfffff88002c91000          0x1b000 \SystemRoot\system32\DRIVERS\wanarp.sys
0xfffffa8002b44ba0 termdd.sys          0xfffff88002cac000          0x14000 \SystemRoot\system32\DRIVERS\termdd.sys
0xfffffa8002b4fc40 rdbss.sys           0xfffff88002cc0000          0x51000 \SystemRoot\system32\DRIVERS\rdbss.sys
0xfffffa8002b55840 nsiproxy.sys        0xfffff88002d11000           0xc000 \SystemRoot\system32\drivers\nsiproxy.sys
0xfffffa8002b56710 mssmbios.sys        0xfffff88002d1d000           0xb000 \SystemRoot\system32\DRIVERS\mssmbios.sys
0xfffffa8002b52970 discache.sys        0xfffff88002d28000           0xf000 \SystemRoot\System32\drivers\discache.sys
0xfffffa8002b52210 csc.sys             0xfffff88002d37000          0x83000 \SystemRoot\system32\drivers\csc.sys
0xfffffa8002b60760 dfsc.sys            0xfffff88002dba000          0x1e000 \SystemRoot\System32\Drivers\dfsc.sys
0xfffffa8002b60010 blbdrive.sys        0xfffff88002dd8000          0x11000 \SystemRoot\system32\DRIVERS\blbdrive.sys
0xfffffa8002991500 tunnel.sys          0xfffff880032f9000          0x26000 \SystemRoot\system32\DRIVERS\tunnel.sys
0xfffffa8002b79d40 i8042prt.sys        0xfffff8800331f000          0x1e000 \SystemRoot\system32\DRIVERS\i8042prt.sys
0xfffffa8002b7b5e0 kbdclass.sys        0xfffff8800333d000           0xf000 \SystemRoot\system32\DRIVERS\kbdclass.sys
0xfffffa8002b8e2c0 mouclass.sys        0xfffff8800334c000           0xf000 \SystemRoot\system32\DRIVERS\mouclass.sys
0xfffffa8002b95010 vgapnp.sys          0xfffff8800335b000           0xe000 \SystemRoot\system32\DRIVERS\vgapnp.sys
0xfffffa8002b78f20 E1G6032E.sys        0xfffff88003369000          0x24000 \SystemRoot\system32\DRIVERS\E1G6032E.sys
0xfffffa8002b2d4f0 usbohci.sys         0xfffff8800338d000           0xb000 \SystemRoot\system32\DRIVERS\usbohci.sys
0xfffffa8002bad110 USBPORT.SYS         0xfffff88003398000          0x56000 \SystemRoot\system32\DRIVERS\USBPORT.SYS
0xfffffa8002be9180 CmBatt.sys          0xfffff880033ee000           0x5000 \SystemRoot\system32\DRIVERS\CmBatt.sys
0xfffffa8002bf3170 intelppm.sys        0xfffff88003200000          0x16000 \SystemRoot\system32\DRIVERS\intelppm.sys
0xfffffa8002c03170 CompositeBus.sys    0xfffff88003216000          0x10000 \SystemRoot\system32\DRIVERS\CompositeBus
sys
0xfffffa8002c1a170 AgileVpn.sys        0xfffff88003226000          0x16000 \SystemRoot\system32\DRIVERS\AgileVpn.sys
0xfffffa80024051e0 rasl2tp.sys         0xfffff8800323c000          0x24000 \SystemRoot\system32\DRIVERS\rasl2tp.sys
0xfffffa8002be5c60 ndistapi.sys        0xfffff88003260000           0xc000 \SystemRoot\system32\DRIVERS\ndistapi.sys
0xfffffa8002be6f30 ndiswan.sys         0xfffff8800326c000          0x2f000 \SystemRoot\system32\DRIVERS\ndiswan.sys
```

```
0xfffffa8003250790 dump_atapi.sys      0xfffff8800350d000           0x9000 \SystemRoot\System32\Drivers\dump_atapi.sy
s
0xfffffa8003245740 dump_dumpfve.sys    0xfffff88003516000          0x13000 \SystemRoot\System32\Drivers\dump_dumpfve.
sys
0xfffffa8002a3e860 win32k.sys          0xfffff96000040000         0x310000 \SystemRoot\System32\win32k.sys
0xfffffa800324cc60 Dxapi.sys           0xfffff88003529000           0xc000 \SystemRoot\System32\drivers\Dxapi.sys
0xfffffa80032c82a0 dxg.sys             0xfffff96000510000          0x1e000 \SystemRoot\System32\drivers\dxg.sys
0xfffffa8001869a20 monitor.sys         0xfffff88003535000           0xe000 \SystemRoot\system32\DRIVERS\monitor.sys
0xfffffa80018ed010 TSDDD.dll           0xfffff96000680000           0xa000 \SystemRoot\System32\TSDDD.dll
0xfffffa80032e1640 framebuf.dll        0xfffff960008f0000           0x9000 \SystemRoot\System32\framebuf.dll
0xfffffa8003319340 HIDPARSE.SYS        0xfffff8800356a000           0x9000 \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
0xfffffa80033a22a0 luafv.sys           0xfffff88003582000          0x23000 \SystemRoot\system32\drivers\luafv.sys
0xfffffa80034858f0 lltdio.sys          0xfffff880035a5000          0x15000 \SystemRoot\system32\DRIVERS\lltdio.sys
0xfffffa800348e180 rspndr.sys          0xfffff880035ba000          0x18000 \SystemRoot\system32\DRIVERS\rspndr.sys
0xfffffa80033ffc40 HTTP.sys            0xfffff8800267e000          0xc9000 \SystemRoot\system32\drivers\HTTP.sys
0xfffffa800351c0c0 bowser.sys          0xfffff88002747000          0x1e000 \SystemRoot\system32\DRIVERS\bowser.sys
0xfffffa8003550010 mpsdrv.sys          0xfffff88002765000          0x18000 \SystemRoot\System32\drivers\mpsdrv.sys
0xfffffa800355b770 mrxsmb.sys          0xfffff8800277d000          0x2d000 \SystemRoot\system32\DRIVERS\mrxsmb.sys
0xfffffa8003560a20 mrxsmb10.sys        0xfffff880027aa000          0x4d000 \SystemRoot\system32\DRIVERS\mrxsmb10.sys
0xfffffa8003567310 mrxsmb20.sys        0xfffff88002600000          0x24000 \SystemRoot\system32\DRIVERS\mrxsmb20.sys
0xfffffa80035ca8c0 peauth.sys          0xfffff88002ab2000          0xa6000 \SystemRoot\system32\drivers\peauth.sys
0xfffffa80035d4e70 secdrv.SYS          0xfffff88002b58000           0xb000 \SystemRoot\System32\Drivers\secdrv.SYS
0xfffffa80035d45d0 srvnet.sys          0xfffff88002b63000          0x31000 \SystemRoot\System32\DRIVERS\srvnet.sys
0xfffffa800352cb90 tcpipreg.sys        0xfffff88002b94000          0x12000 \SystemRoot\System32\drivers\tcpipreg.sys
0xfffffa80036332e0 srv2.sys            0xfffff88002a00000          0x6b000 \SystemRoot\System32\DRIVERS\srv2.sys
0xfffffa800357e1a0 srv.sys             0xfffff88003a9d000          0x99000 \SystemRoot\System32\DRIVERS\srv.sys
0xfffffa80032f2230 hidusb.sys          0xfffff88003b36000           0xe000 \SystemRoot\system32\DRIVERS\hidusb.sys
0xfffffa80037aae00 HIDCLASS.SYS        0xfffff88003b44000          0x19000 \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
0xfffffa8003316a10 USBD.SYS            0xfffff88003b5d000           0x2000 \SystemRoot\system32\DRIVERS\USBD.SYS
0xfffffa80037e6c80 mouhid.sys          0xfffff88003b5f000           0xd000 \SystemRoot\system32\DRIVERS\mouhid.sys
0xfffffa800407ad60 spsys.sys           0xfffff88003b6c000          0x71000 \SystemRoot\system32\drivers\spsys.sys
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$
```

This plugin lists the modules (drivers) loaded into the memory of the system at the time the memory dump was taken.

Each entry in the output represents a loaded module and provides information such as the module's name, base address, size, and file path. Here's a breakdown of some of the columns:

Offset(V): This is the virtual memory offset where the module is loaded.

Name: The name of the module.

Base: The base address in memory where the module is loaded.

Size: The size of the module in memory.

File: The file path on disk where the module is located.

Dynamic Link Libraries Analysis

dlllist: lists loaded Dynamic Link Libraries (DLLs) for each process. DLLs are crucial components of Windows applications, and analyzing their presence and usage in processes can reveal dependencies, identify injected DLLs, and detect potential malware activities.

This plugin provided us a lengthy output of loaded (DLLs) for each process, uploading snapshots of every process can be a time-consuming task, so I'll just upload snapshots of two or three processes and show what forensic value we can get from it

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 dlllist
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    252
Command line : \SystemRoot\System32\smss.exe


Base                             Size          LoadCount LoadTime                       Path
-------------------- ---------- ---------- ------------------------------ ----
0x0000000048570000           0x20000             0xffff 1970-01-01 00:00:00 UTC+0000   \SystemRoot\System32\smss.exe
0x0000000076f30000           0x1a9000            0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
************************************************************************
csrss.exe pid:    328
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyste
mType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitializa
tion,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
Service Pack 1
```

There are no obvious signs of malicious activity in the above snapshot. The DLLs listed appear to be standard system DLLs and are loaded into critical system processes (smss.exe and csrss.exe).

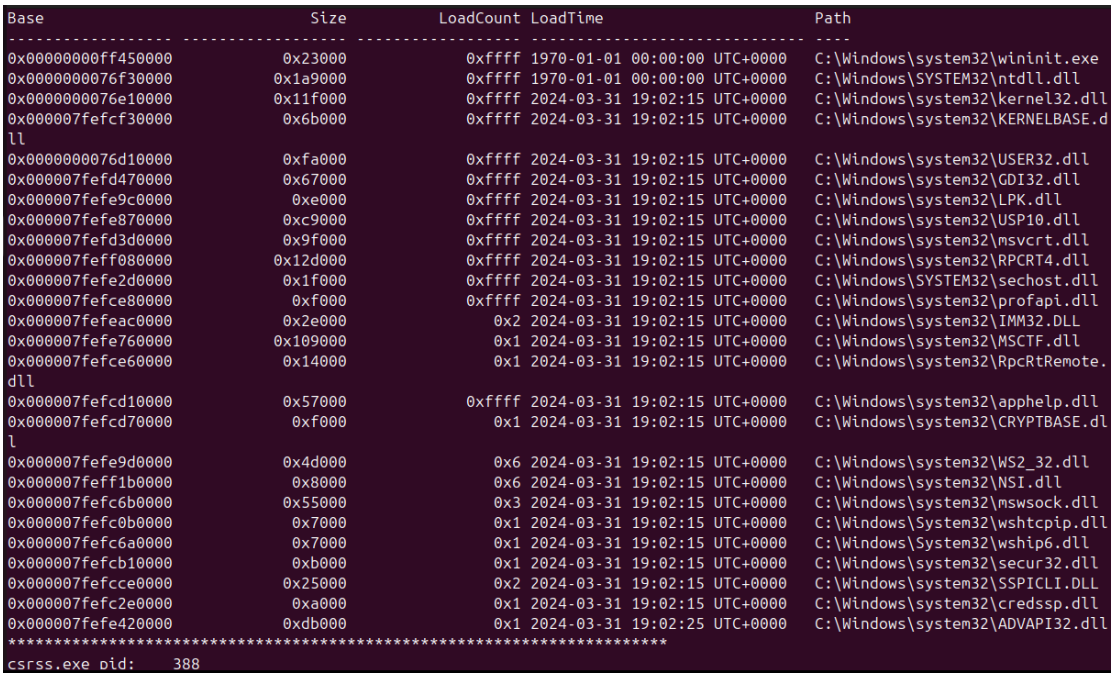
```
Base                             Size          LoadCount LoadTime                       Path
-------------------- ---------------- ---------------- ------------------------------ ----
0x000000004a530000             0x6000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\system32\csrss.exe
0x0000000076f30000             0x1a9000           0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x000007fefcf00000             0x13000            0xffff 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\CSRSRV.dll
0x000007fefcee0000             0x11000               0x4 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\basesrv.DLL
0x000007fefcea0000             0x38000               0x2 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\winsrv.DLL
0x0000000076d10000             0xfa000               0xb 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\USER32.dll
0x000007fefd470000             0x67000               0xc 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\GDI32.dll
0x0000000076e10000             0x11f000             0x45 2024-03-31 19:02:14 UTC+0000   C:\Windows\SYSTEM32\kernel32.dll
0x000007fefcf30000             0x6b000              0xdb 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\KERNELBASE.d
ll
0x000007fefe9c0000             0xe000                0x3 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\LPK.dll
0x000007fefe870000             0xc9000               0x3 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\USP10.dll
0x000007fefd3d0000             0x9f000               0x3 2024-03-31 19:02:14 UTC+0000   C:\Windows\system32\msvcrt.dll
0x000007fefce90000             0xc000                0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\sxssrv.DLL
0x000007fefcd80000             0x91000               0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\sxs.dll
0x000007feff080000             0x12d000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\RPCRT4.dll
0x000007fefcd70000             0xf000                0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\CRYPTBASE.dl
l
*******************************************************************************
wininit.exe pid:    376
Command line : wininit.exe
Service Pack 1
```

Here are some potential indicators of suspicious or malicious activity in the above snapshot:

1. **Load Time Anomalies**
   - Check for DLLs with unusual load times, especially those loaded after the system boot time (e.g., the CSRSRV.dll loaded on "2024-03-31 19:02:14 UTC+0000"). Any DLLs loaded significantly later than system processes may be worth investigating further.
   - **CSRSRV.dll**, **basesrv.DLL**, and **winsrv.DLL** were all loaded after the system's boot time, which indeed raises suspicion. These DLLs should typically load during system startup or process initialization. Loading them later might indicate that they were injected or loaded dynamically, which could be a sign of malicious activity.
   - Additionally, the presence of **CSRSRV.dll** and **winsrv.DLL** in a process like **csrss.exe** might be unusual. While these DLLs are legitimate components of the Windows subsystem, loading them at unusual times or in unexpected processes could indicate malicious activity.

- It's also worth noting that the LoadTime for these DLLs is "2024-03-31 19:02:14 UTC+0000," which matches the system's boot time, indicating they were loaded shortly after the system started.

2. **Unusual DLL Names or Locations**
   - Look for DLLs with suspicious names or loaded from unexpected locations. For example, if a DLL has a random or misspelled name or is loaded from a non-standard directory, it could be an indication of malicious activity.
3. **High Load Counts with Low Load Times**
   - DLLs with low load counts but high load times may suggest that they were dynamically loaded rather than being part of the initial system startup. Investigate these DLLs to determine if they are legitimate or potentially malicious.
4. **Mismatched Dependencies**
   - Compare the loaded DLLs against a baseline of known good DLLs for the operating system. Any discrepancies, such as missing or additional DLLs, could indicate tampering or malicious activity.
5. **Unusual Process Behavior**
   - While not evident from the provided output, analyzing process behavior alongside DLL loading can help identify suspicious activities. Look for processes exhibiting unusual behavior, such as making unexpected network connections, modifying critical system settings, or attempting to hide their presence.

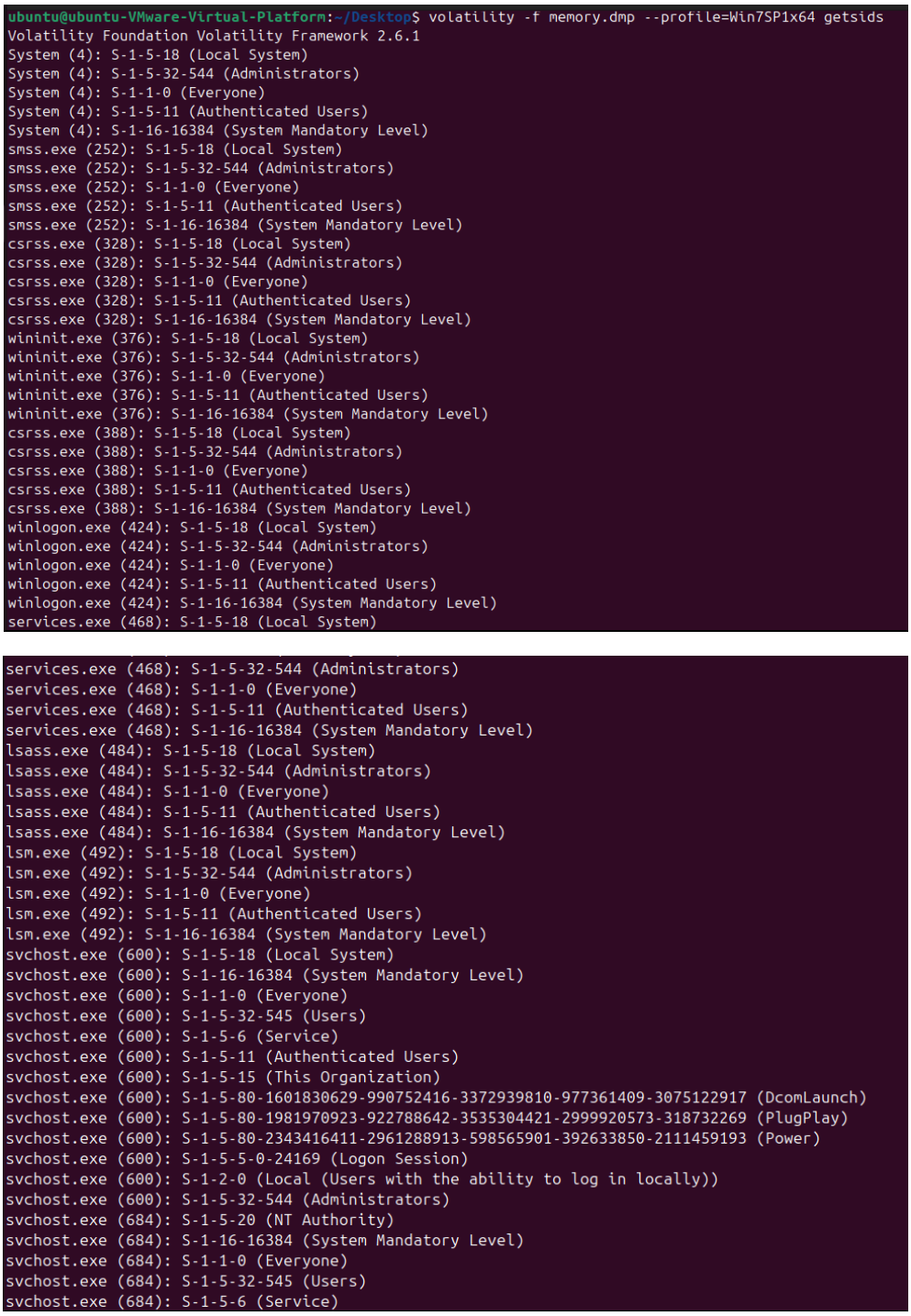


```
Base                             Size          LoadCount LoadTime                    Path
-------------------- ---------------- ---------------- --------------------------- ----
0x00000000ff450000           0x23000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\system32\wininit.exe
0x0000000076f30000           0x1a9000            0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x0000000076e10000           0x11f000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\kernel32.dll
0x000007fefcf30000            0x6b000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\KERNELBASE.d
ll
0x0000000076d10000            0xfa000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\USER32.dll
0x000007fefd470000            0x67000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\GDI32.dll
0x000007fefe9c0000             0xe000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\LPK.dll
0x000007fefe870000            0xc9000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\USP10.dll
0x000007fefd3d0000            0x9f000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\msvcrt.dll
0x000007feff080000           0x12d000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\RPCRT4.dll
0x000007fefe2d0000            0x1f000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\SYSTEM32\sechost.dll
0x000007fefce80000             0xf000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\profapi.dll
0x000007fefeac0000             0x2e000              0x2 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\IMM32.DLL
0x000007fefe760000           0x109000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\MSCTF.dll
0x000007fefce60000            0x14000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\RpcRtRemote.
dll
0x000007fefcd10000            0x57000            0xffff 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\apphelp.dll
0x000007fefcd70000             0xf000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\CRYPTBASE.dl
l
0x000007fefe9d0000            0x4d000              0x6 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\WS2_32.dll
0x000007feff1b0000             0x8000              0x6 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\NSI.dll
0x000007fefc6b0000            0x55000              0x3 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\mswsock.dll
0x000007fefc0b0000             0x7000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\System32\wshtcpip.dll
0x000007fefc6a0000             0x7000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\System32\wship6.dll
0x000007fefcb10000             0xb000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\secur32.dll
0x000007fefcce0000            0x25000              0x2 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\SSPICLI.DLL
0x000007fefc2e0000             0xa000              0x1 2024-03-31 19:02:15 UTC+0000   C:\Windows\system32\credssp.dll
0x000007fefe420000             0xdb000             0x1 2024-03-31 19:02:25 UTC+0000   C:\Windows\system32\ADVAPI32.dll
**********************************************************************
csrss.exe pid:    388
```

Here are some potential indicators of suspicious or malicious activity in the above snapshot:

- The presence of **CSRSRV.dll, basesrv.DLL, and winsrv.DLL** loaded after the system's boot time, as indicated by their LoadTime being "2024-03-31 19:02:14 UTC+0000," could be indicative of potentially malicious activity. These DLLs are typically loaded during system startup or process initialization and loading them later than expected raises suspicion.
- **CSRSRV.dll, basesrv.DLL, and winsrv.DLL** are essential system DLLs responsible for various critical functions in the Windows operating system. Their unexpected loading or loading at unusual times could suggest that they were injected or loaded dynamically, which could be a sign of malware attempting to hide its presence or manipulate system behavior.

getsids: lists Security Identifiers (SIDs) for processes. SIDs uniquely identify security principles such as users and groups in Windows. This plugin helps in identifying the security context of processes running on the system, which can aid in identifying unauthorized or suspicious activities.



No malicious or suspicious activity observed. The output mostly consists of system processes running under different user contexts, such as Local System, Administrators, Users, etc. These processes are standard for a Windows environment and are necessary for the proper functioning of the system.

Network Analysis

netscan: It enumerates network-related artifacts in memory. It helps in identifying active network connections, listening ports, and other network-related information that can be crucial for understanding network activity on the system.

```
0x7e0f3ec0         UDPv6    fe80::d092:32e5:ebb3:9bc2:60699 *:*                                 2020     svchost.exe
  2024-04-01 01:41:53 UTC+0000
0x7e169010         UDPv4    0.0.0.0:0                       *:*                                 1716     svchost.exe
  2024-03-31 19:02:17 UTC+0000
0x7e349340         UDPv4    0.0.0.0:0                       *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e349340         UDPv6    :::0                            *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e396ec0         UDPv4    192.168.56.101:1900             *:*                                 2020     svchost.exe
  2024-04-01 01:41:53 UTC+0000
0x7e3b6240         UDPv4    0.0.0.0:4500                    *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3b6240         UDPv6    :::4500                         *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3c1530         UDPv4    0.0.0.0:500                     *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3c1530         UDPv6    :::500                          *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3c39e0         UDPv4    0.0.0.0:500                     *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3c4ec0         UDPv4    0.0.0.0:4500                    *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7e3ca010         UDPv4    0.0.0.0:0                       *:*                                 852      svchost.exe
  2024-03-31 19:02:16 UTC+0000
0x7dc95910         TCPv4    192.168.56.101:139              0.0.0.0:0              LISTENING    4        System

0x7deb44f0         TCPv4    0.0.0.0:49157                   0.0.0.0:0              LISTENING    484      lsass.exe

0x7deb44f0         TCPv6    :::49157                        :::0                   LISTENING    484      lsass.exe

0x7e00ac50         TCPv4    0.0.0.0:49156                   0.0.0.0:0              LISTENING    1716     svchost.exe

0x7e00ac50         TCPv6    :::49156                        :::0                   LISTENING    1716     svchost.exe
```

```
0x7deb44f0         TCPv6    :::49157                        :::0                   LISTENING    484      lsass.exe

0x7e00ac50         TCPv4    0.0.0.0:49156                   0.0.0.0:0              LISTENING    1716     svchost.exe

0x7e00ac50         TCPv6    :::49156                        :::0                   LISTENING    1716     svchost.exe

0x7e0f77a0         TCPv4    0.0.0.0:445                     0.0.0.0:0              LISTENING    4        System

0x7e0f77a0         TCPv6    :::445                          :::0                   LISTENING    4        System

0x7e100a40         TCPv4    0.0.0.0:49155                   0.0.0.0:0              LISTENING    468      services.exe

0x7e100a40         TCPv6    :::49155                        :::0                   LISTENING    468      services.exe

0x7e1552d0         TCPv4    0.0.0.0:49156                   0.0.0.0:0              LISTENING    1716     svchost.exe

0x7e1dd180         TCPv4    0.0.0.0:8000                    0.0.0.0:0              LISTENING    1892     pythonw.exe

0x7e209ce0         TCPv4    0.0.0.0:49154                   0.0.0.0:0              LISTENING    852      svchost.exe

0x7e2e2160         TCPv4    0.0.0.0:49154                   0.0.0.0:0              LISTENING    852      svchost.exe

0x7e2e2160         TCPv6    :::49154                        :::0                   LISTENING    852      svchost.exe

0x7e39c010         TCPv4    0.0.0.0:49155                   0.0.0.0:0              LISTENING    468      services.exe

0x7dc08900         TCPv4    127.0.0.1:51334                 127.0.0.1:8000         CLOSED       2040     pythonw.exe

0x7dc0ba80         TCPv4    127.0.0.1:8000                  127.0.0.1:51335        CLOSED       1892     pythonw.exe

0x7dc8b010         TCPv4    127.0.0.1:8000                  127.0.0.1:51333        CLOSED       1892     pythonw.exe
```

Several processes are associated with potentially malicious activities:

- **svchost.exe:** This process appears multiple times, listening on various UDP and TCP ports. While svchost.exe is a legitimate system process responsible for hosting services, it is commonly targeted by malware to disguise malicious activities.
- **pythonw.exe:** This process is involved in several TCP connections, both in LISTENING and CLOSED states. While Python itself is not malicious, its presence in network connections might indicate the execution of Python-based scripts or tools for malicious purposes.
- **lsass.exe:** This process is listening on TCP port 49157, which could be a sign of LSASS (Local Security Authority Subsystem Service) exploitation. LSASS is a critical Windows system process, and its compromise can lead to credential theft and lateral movement by attackers.
- **wininit.exe:** This process is listening on TCP port 49152, which is unusual behavior for the legitimate wininit.exe process. This could potentially indicate a malicious process masquerading as wininit.exe.
- **services.exe:** This process is listening on TCP port 49155, which could indicate a malicious service or exploitation of the legitimate services.exe process.

The processes that appear to be suspicious are:

- **pythonw.exe (PID 1892)**
- **pythonw.exe (PID 2040)**

The presence of Python scripts in this context might indicate potentially malicious activity, as Python is commonly used by threat actors for various purposes, including scripting attacks and performing reconnaissance on a compromised system.

Registry Analysis

hivelist: Provides a list of the virtual and physical memory addresses where the Windows registry hives are loaded.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a006060010 0x0000000021eab010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0060f0010 0x0000000028186010 \SystemRoot\System32\Config\SAM
0xfffff8a006184410 0x0000000020f82410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00000c350 0x000000002d674350 [no name]
0xfffff8a000024010 0x000000002d4c1010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004e410 0x000000002d66f410 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000dee010 0x00000000292de010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000e66010 0x0000000029136010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001251010 0x00000000211b6010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001413010 0x000000001dd69010 \??\C:\Users\Administrator\ntuser.dat
0xfffff8a001465010 0x0000000026e0d010 \??\C:\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a001959010 0x0000000012cdd010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a0034b03e0 0x0000000023b1e3e0 \SystemRoot\System32\Config\DEFAULT
```

The forensic value of the plugin provides information about the locations and physical addresses of registry hives loaded into memory. These hives contain critical configuration and user data, which are essential for understanding system configuration and user activities.

We know that Windows password is stored on the **SAM (Security Accounts Manager)** file on Windows. This SAM file stores hashed passwords for usernames in Windows system. This file can't be accessed by any user when the Windows system is on.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a006060010 0x0000000021eab010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0060f0010 0x0000000028186010 \SystemRoot\System32\Config\SAM
0xfffff8a006184410 0x0000000020f82410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
```

hivescan: Searches through physical memory to identify and extract registry hive files, which can then be analyzed for forensic purposes.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 hivescan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)
------------------
0x0000000012cdd010
0x000000001dd69010
0x0000000020f82410
0x00000000211b6010
0x0000000021eab010
0x0000000023b1e3e0
0x0000000026e0d010
0x0000000028186010
0x0000000029136010
0x00000000292de010
0x000000002d4c1010
0x000000002d66f410
0x000000002d674350
```

The forensic value of the ***hivescan*** command contain crucial system configuration information, user profiles, and other registry data, which are essential for forensic analysis.

shimcache: is a component in Windows that stores information about executed programs, helping ensure compatibility. Forensically, analyzing ShimCache can reveal the history of executed programs, aiding in identifying suspicious or unauthorized activity on a system.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 shimcache
Volatility Foundation Volatility Framework 2.6.1
Last Modified                 Path
----------------------------- ----
2010-11-21 03:24:09 UTC+0000   \??\C:\Windows\system32\LogonUI.exe
2010-11-21 03:24:42 UTC+0000   \??\C:\Windows\System32\ieframe.dll
2009-07-14 01:39:37 UTC+0000   \??\C:\Windows\system32\SearchFilterHost.exe
2009-07-14 01:39:37 UTC+0000   \??\C:\Windows\system32\SearchProtocolHost.exe
2009-07-14 01:14:38 UTC+0000   \??\C:\Windows\SysWOW64\shutdown.exe
2009-07-14 01:14:38 UTC+0000   \??\C:\Windows\system32\shutdown.exe
2009-07-14 01:39:37 UTC+0000   \??\C:\Windows\system32\SearchIndexer.exe
2010-11-21 03:23:48 UTC+0000   \??\C:\Windows\System32\prnfldr.dll
2009-07-14 01:14:46 UTC+0000   \??\C:\Windows\SysWOW64\Wbem\wmic.exe
2010-11-21 03:23:56 UTC+0000   \??\C:\Windows\system32\mstsc.exe
2010-11-21 03:25:07 UTC+0000   \??\C:\Windows\system32\WFS.exe
2009-07-14 01:39:59 UTC+0000   \??\C:\Windows\system32\xpsrchvw.exe
2009-07-14 01:39:24 UTC+0000   \??\C:\Windows\system32\mspaint.exe
2009-07-14 01:39:41 UTC+0000   \??\C:\Windows\system32\SnippingTool.exe
2009-07-14 01:39:46 UTC+0000   \??\C:\Windows\system32\StikyNot.exe
2009-07-14 01:38:57 UTC+0000   \??\C:\Windows\system32\calc.exe
2009-07-14 01:39:06 UTC+0000   \??\C:\Windows\system32\displayswitch.exe
2009-07-14 01:39:31 UTC+0000   \??\C:\WINDOWS\SYSTEM32\RUNDLL32.EXE
2009-07-14 01:39:06 UTC+0000   \??\C:\Windows\system32\DllHost.exe
2010-11-21 03:24:15 UTC+0000   \??\C:\Windows\system32\wbem\wmiprvse.exe
2010-11-21 03:25:10 UTC+0000   \??\C:\Program Files (x86)\Windows Media Player\wmplayer.exe
2010-11-21 03:24:11 UTC+0000   \??\C:\Windows\Explorer.EXE
2010-11-21 03:25:08 UTC+0000   \??\C:\Program Files (x86)\Internet Explorer\iexplore.exe
2009-07-14 01:14:46 UTC+0000   \??\C:\Windows\System32\Wbem\wmic.exe
2013-11-10 17:24:30 UTC+0000   \??\C:\Python27\pythonw.exe
2010-11-21 03:24:02 UTC+0000   \??\C:\Windows\System32\networkexplorer.dll
2010-11-21 03:24:49 UTC+0000   \??\C:\Windows\System32\gameux.dll
2009-07-14 01:39:46 UTC+0000   \??\C:\Windows\System32\svchost.exe
```

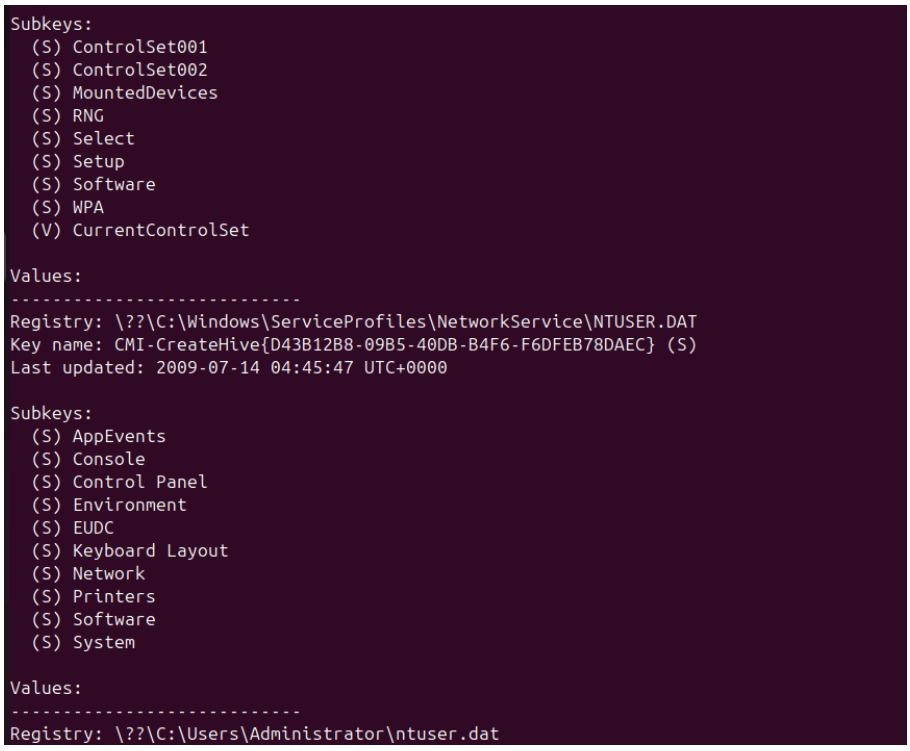
```
2010-11-21 03:23:51 UTC+0000   \??\C:\Windows\System32\ntshrui.dll
2010-11-21 03:24:41 UTC+0000   \??\C:\Windows\System32\cscui.dll
2009-07-14 01:40:36 UTC+0000   \??\C:\Windows\System32\EhStorShell.dll
2009-07-14 01:39:08 UTC+0000   \??\C:\Windows\system32\Dwm.exe
2010-11-21 03:24:28 UTC+0000   \??\C:\Windows\system32\userinit.exe
2010-11-21 03:24:08 UTC+0000   \??\C:\Windows\system32\taskhost.exe
2010-11-21 03:24:27 UTC+0000   \??\C:\Windows\System32\spoolsv.exe
2010-11-21 03:23:53 UTC+0000   \??\C:\Windows\system32\lsm.exe
2009-07-14 01:39:16 UTC+0000   \??\C:\Windows\system32\lsass.exe
2009-07-14 01:39:37 UTC+0000   \??\C:\Windows\system32\services.exe
2009-07-14 01:14:42 UTC+0000   \??\C:\Windows\SysWOW64\tasklist.exe
2009-07-14 01:14:42 UTC+0000   \??\C:\Windows\system32\tasklist.exe
2024-03-31 15:00:15 UTC+0000   \??\C:\vmcloak\click.exe
2024-03-31 18:25:15 UTC+0000   \??\C:\pillow.exe
2024-03-31 18:23:55 UTC+0000   \??\C:\pillow.exe
2009-07-14 01:39:40 UTC+0000   \??\C:\Windows\system32\shutdown.exe
2009-07-14 01:39:29 UTC+0000   \??\C:\WINDOWS\SYSTEM32\reg.exe
2013-11-10 17:24:24 UTC+0000   \??\C:\Python27\python.exe
2010-11-21 03:23:55 UTC+0000   \??\C:\Windows\system32\cmd.exe
2010-11-21 03:24:28 UTC+0000   \??\C:\Windows\syswow64\MsiExec.exe
2009-07-14 01:39:07 UTC+0000   \??\C:\Windows\system32\DrvInst.exe
2010-11-21 03:23:55 UTC+0000   \??\C:\Windows\system32\vssvc.exe
2010-11-21 03:24:15 UTC+0000   \??\C:\Windows\System32\msiexec.exe
2010-11-21 03:24:07 UTC+0000   \??\C:\Windows\system32\net1.exe
2009-07-14 01:39:25 UTC+0000   \??\C:\Windows\system32\net.exe
2009-07-14 01:39:35 UTC+0000   \??\C:\Windows\system32\sc.exe
2009-07-14 01:39:25 UTC+0000   \??\C:\Windows\System32\netsh.exe
2010-11-21 03:24:51 UTC+0000   \??\C:\Program Files\Windows Sidebar\sidebar.exe
2024-03-31 15:00:15 UTC+0000   \??\C:\vmcloak\bootstrap.bat
2009-07-14 01:39:17 UTC+0000   \??\C:\Windows\System32\mctadmin.exe
2010-11-21 03:23:51 UTC+0000   \??\C:\Windows\System32\DeviceCenter.dll
```

```
2009-07-14 01:39:12 UTC+0000   \??\C:\Windows\System32\ie4uinit.exe
2009-07-14 01:39:29 UTC+0000   \??\C:\Windows\System32\regsvr32.exe
2009-07-14 01:39:48 UTC+0000   \??\C:\Windows\System32\unregmp2.exe
2009-07-14 01:39:53 UTC+0000   \??\C:\Program Files\Windows Mail\WinMail.exe
2009-07-14 01:14:31 UTC+0000   \??\C:\Windows\SysWOW64\rundll32.exe
2010-11-21 03:25:08 UTC+0000   \??\C:\Windows\SysWOW64\ie4uinit.exe
2009-07-14 01:14:45 UTC+0000   \??\C:\Program Files (x86)\Windows Mail\WinMail.exe
2010-11-21 03:24:27 UTC+0000   \??\C:\Windows\system32\runonce.exe
2010-11-21 03:24:26 UTC+0000   \??\C:\Windows\system32\mcbuilder.exe
2010-11-21 03:24:35 UTC+0000   \??\C:\Windows\system32\winsat.exe
2009-07-14 01:39:24 UTC+0000   \??\C:\WINDOWS\SYSTEM32\MUIUNATTEND.EXE
2010-11-21 03:24:03 UTC+0000   \??\C:\Windows\servicing\TrustedInstaller.exe
2010-11-21 03:23:52 UTC+0000   \??\C:\Windows\system32\oobe\msoobe.exe
2009-07-14 01:39:26 UTC+0000   \??\C:\Windows\system32\oobe\oobeldr.exe
2010-11-21 03:24:24 UTC+0000   \??\C:\Windows\system32\oobe\windeploy.exe
2010-11-21 03:23:56 UTC+0000   \??\C:\Windows\system32\sppsvc.exe
2009-07-14 01:39:39 UTC+0000   \??\C:\WINDOWS\SYSTEM32\SETUPUGC.EXE
2009-06-10 20:39:58 UTC+0000   \??\C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
2009-06-10 21:23:09 UTC+0000   \??\C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
2010-11-21 03:24:15 UTC+0000   \??\C:\Windows\WinSxS\amd64_netfx-clrgc_b03f5f7f11d50a3a_6.1.7601.17514_none_ad7a390fa131
c970\clrgc.exe
2010-11-21 03:24:22 UTC+0000   \??\C:\Windows\bfsvc.exe
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$
```

printkey: It prints a registry key and its values. It allows for the extraction of registry key information from memory, aiding in the analysis of registry entries and configurations

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 printkey
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: [no name]
Key name: REGISTRY (S)
Last updated: 2024-03-31 19:02:10 UTC+0000

Subkeys:
  (S) A
  (S) MACHINE
  (S) USER

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: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2009-07-14 04:45:48 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

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

Values:
----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5} (S)
Last updated: 2024-03-31 19:02:10 UTC+0000
```



The forensic value of this output lies in its potential to reveal insights into system configuration, user activities, and potential security breaches.

1. **System Configuration Analysis:**
   - Identification of registry keys and sub keys provides insight into the structure and organization of the Windows registry on the analyzed system.
   - Last updated timestamps can help establish timelines of system events and changes, aiding in forensic investigations.
2. **User Activity Tracking:**
   - Examination of user-specific registry hives (??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT, ??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT, ??\C:\Users\Administrator\ntuser.dat) reveals user-specific settings, preferences, and application usage.
   - Subkeys such as AppEvents, Console, Control Panel, Environment, Printers, and Software provide insights into user interactions with system components and installed software.

3. **System Integrity Monitoring:**
    - Detection of changes to critical system hives (\SystemRoot\System32\Config) and their subkeys can indicate potential tampering or unauthorized modifications.
    - Examination of registry keys related to system startup (\REGISTRY\MACHINE\SYSTEM) and software installation (\SystemRoot\System32\Config\SOFTWARE) aids in identifying persistence mechanisms utilized by malware or unauthorized software.
4. **Security Analysis:**
    - Reviewing registry keys related to security policies (\SystemRoot\System32\Config\SECURITY) helps in assessing the integrity of security settings and identifying potential security policy violations or unauthorized changes.
    - The presence of unexpected or suspicious registry entries may indicate malicious activity, such as privilege escalation, malware persistence, or data exfiltration.
5. **Evidence of System Events:**
    - Registry entries related to boot configuration (\Device\HarddiskVolume1\Boot\BCD) and system hardware (\REGISTRY\MACHINE\HARDWARE) provide evidence of system startup processes and hardware configurations, which can be valuable for reconstructing system events and troubleshooting issues.
6. **Forensic Timeline Construction:**
    - Timestamps associated with registry key last updates enable the construction of a forensic timeline, facilitating the correlation of events and activities across the system.

shutdowntime: This plugin lies in its ability to provide investigators with crucial information regarding the system's last shutdown timestamp. This information can be valuable for various investigative purposes

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 shutdowntime
Volatility Foundation Volatility Framework 2.6.1
Registry: SYSTEM
Key Path: ControlSet001\Control\Windows
Key Last updated: 2024-03-31 19:02:04 UTC+0000
Value Name: ShutdownTime
Value: 2024-03-31 19:02:04 UTC+0000

ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$
```

This plugin offers significant forensic value by providing investigators with precise information about the last shutdown timestamp of a device. This data is pivotal in forensic investigations for several reasons.

hashdump: This plugin is used for extracting password hashes from a memory dump of a Windows system. Password hashes are cryptographic representations of user passwords stored in the system's memory or files.

When a user logs into a Windows system, their password is hashed and stored in memory for authentication purposes. The hashdump plugin scans the memory dump for these hashed passwords and extracts them, providing forensic analysts with valuable information for password cracking or authentication-related investigations.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:65447417d4368932b451883c8cd98b40:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
xhmIeJGuweOS:1000:aad3b435b51404eeaad3b435b51404ee:dcfec3adef1d3e969e1d2e85573f672b:::
```

The forensic value is:

- **Administrator:** This is the username of an account with Administrator privileges.
- **Guest:** This is the username of the built-in Guest account.
- **xhmIeJGuweOS:** This is another username present on the system.
- **SID:** Security Identifier for the respective user.
- **LM_hash:** LAN Manager hash of the user's password. (Note: LM hashes are deprecated and are not used by default on modern Windows systems.)
- **NTLM_hash:** NT LAN Manager hash of the user's password. (This is the more secure hash used for authentication on Windows systems.)

malfind: This plugin is used to find, or at least direct us toward hints of malware that may have been injected into various processes.

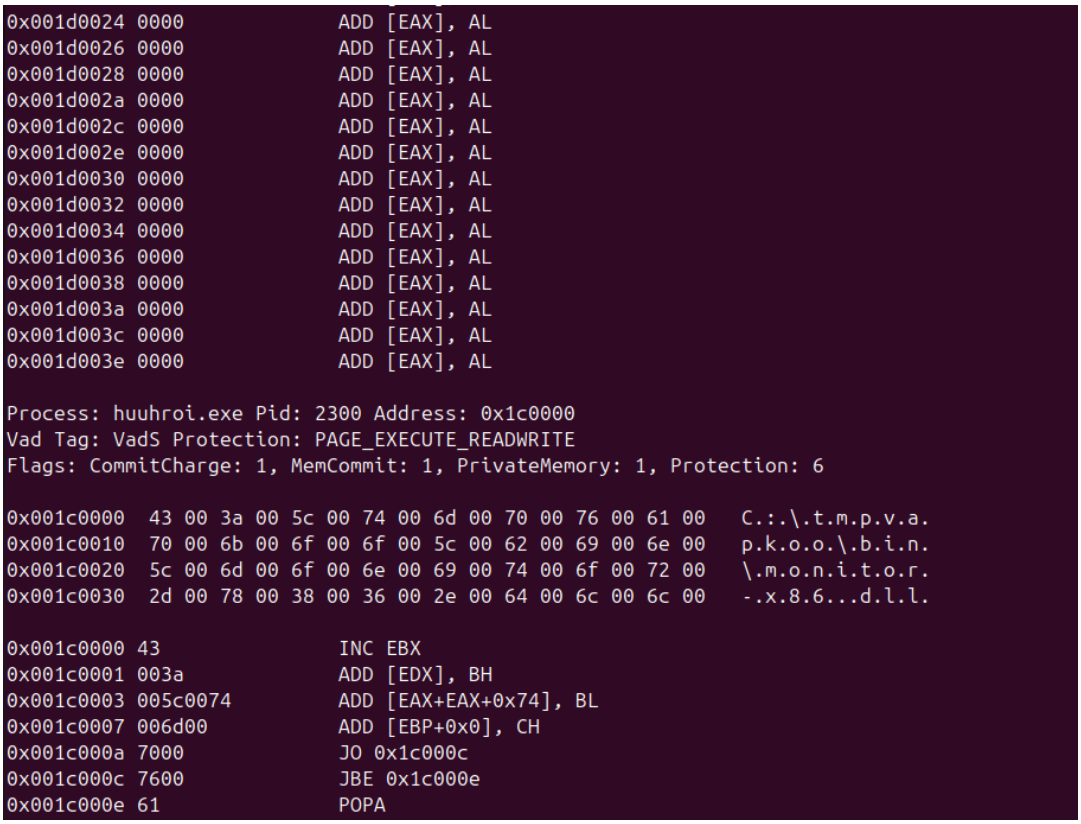
The output of malfind plugin may be very lengthy so we will apply this plugin on a specific process to extract valuable information from it.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 malfind
Volatility Foundation Volatility Framework 2.6.1
Process: lsass.exe Pid: 484 Address: 0xe0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000e0000  43 00 3a 00 5c 00 74 00 6d 00 70 00 76 00 61 00   C.:.\.t.m.p.v.a.
0x000e0010  70 00 6b 00 6f 00 6f 00 5c 00 62 00 69 00 6e 00   p.k.o.o.\.b.i.n.
0x000e0020  5c 00 6d 00 6f 00 6e 00 69 00 74 00 6f 00 72 00   \.m.o.n.i.t.o.r.
0x000e0030  2d 00 78 00 36 00 34 00 2e 00 64 00 6c 00 6c 00   -.x.6.4...d.l.l.

0x000e0000 43               INC EBX
0x000e0001 003a             ADD [EDX], BH
0x000e0003 005c0074         ADD [EAX+EAX+0x74], BL
0x000e0007 006d00           ADD [EBP+0x0], CH
0x000e000a 7000             JO 0xe000c
0x000e000c 7600             JBE 0xe000e
0x000e000e 61               POPA
0x000e000f 007000           ADD [EAX+0x0], DH
0x000e0012 6b006f           IMUL EAX, [EAX], 0x6f
0x000e0015 006f00           ADD [EDI+0x0], CH
0x000e0018 5c               POP ESP
0x000e0019 006200           ADD [EDX+0x0], AH
0x000e001c 69006e005c00     IMUL EAX, [EAX], 0x5c006e
0x000e0022 6d               INS DWORD [ES:EDI], DX
0x000e0023 006f00           ADD [EDI+0x0], CH
0x000e0026 6e               OUTS DX, BYTE [ESI]
0x000e0027 006900           ADD [ECX+0x0], CH
0x000e002a 7400             JZ 0xe002c
0x000e002c 6f               OUTS DX, DWORD [ESI]
0x000e002d 007200           ADD [EDX+0x0], DH
0x000e0030 2d00780036       SUB EAX, 0x36007800
0x000e0035 003400           ADD [EAX+EAX], DH
```

We get a very long output. To be more specific we can use -p flag to analyze a specific PID. As we have discovered previously (pslist plugin), **huuhroi.exe** is assigned to PID 2300.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 malfind -p 2300
Volatility Foundation Volatility Framework 2.6.1
Process: huuhroi.exe Pid: 2300 Address: 0x200000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00200000  b8 20 00 00 00 33 c9 8d 54 24 04 64 ff 15 c0 00   .....3..T$.d....
0x00200010  00 00 83 c4 04 c2 18 00 00 00 00 00 00 00 00 00   ................
0x00200020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00200030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x00200000 b820000000       MOV EAX, 0x20
0x00200005 33c9             XOR ECX, ECX
0x00200007 8d542404         LEA EDX, [ESP+0x4]
0x0020000b 64ff15c0000000   CALL DWORD [FS:0xc0]
0x00200012 83c404           ADD ESP, 0x4
0x00200015 c21800           RET 0x18
0x00200018 0000             ADD [EAX], AL
0x0020001a 0000             ADD [EAX], AL
0x0020001c 0000             ADD [EAX], AL
0x0020001e 0000             ADD [EAX], AL
0x00200020 0000             ADD [EAX], AL
0x00200022 0000             ADD [EAX], AL
0x00200024 0000             ADD [EAX], AL
0x00200026 0000             ADD [EAX], AL
0x00200028 0000             ADD [EAX], AL
0x0020002a 0000             ADD [EAX], AL
0x0020002c 0000             ADD [EAX], AL
0x0020002e 0000             ADD [EAX], AL
0x00200030 0000             ADD [EAX], AL
0x00200032 0000             ADD [EAX], AL
0x00200034 0000             ADD [EAX], AL
```

```
0x00200036 0000             ADD [EAX], AL
0x00200038 0000             ADD [EAX], AL
0x0020003a 0000             ADD [EAX], AL
0x0020003c 0000             ADD [EAX], AL
0x0020003e 0000             ADD [EAX], AL

Process: huuhroi.exe Pid: 2300 Address: 0x1d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x001d0000  3a c4 14 77 cd db 16 77 40 00 42 00 00 00 1c 00   :..w...w@.B.....
0x001d0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x001d0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x001d0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x001d0000 3ac4             CMP AL, AH
0x001d0002 1477             ADC AL, 0x77
0x001d0004 cddb             INT 0xdb
0x001d0006 16               PUSH SS
0x001d0007 7740             JA 0x1d0049
0x001d0009 004200           ADD [EDX+0x0], AL
0x001d000c 0000             ADD [EAX], AL
0x001d000e 1c00             SBB AL, 0x0
0x001d0010 0000             ADD [EAX], AL
0x001d0012 0000             ADD [EAX], AL
0x001d0014 0000             ADD [EAX], AL
0x001d0016 0000             ADD [EAX], AL
0x001d0018 0000             ADD [EAX], AL
0x001d001a 0000             ADD [EAX], AL
0x001d001c 0000             ADD [EAX], AL
0x001d001e 0000             ADD [EAX], AL
0x001d0020 0000             ADD [EAX], AL
```

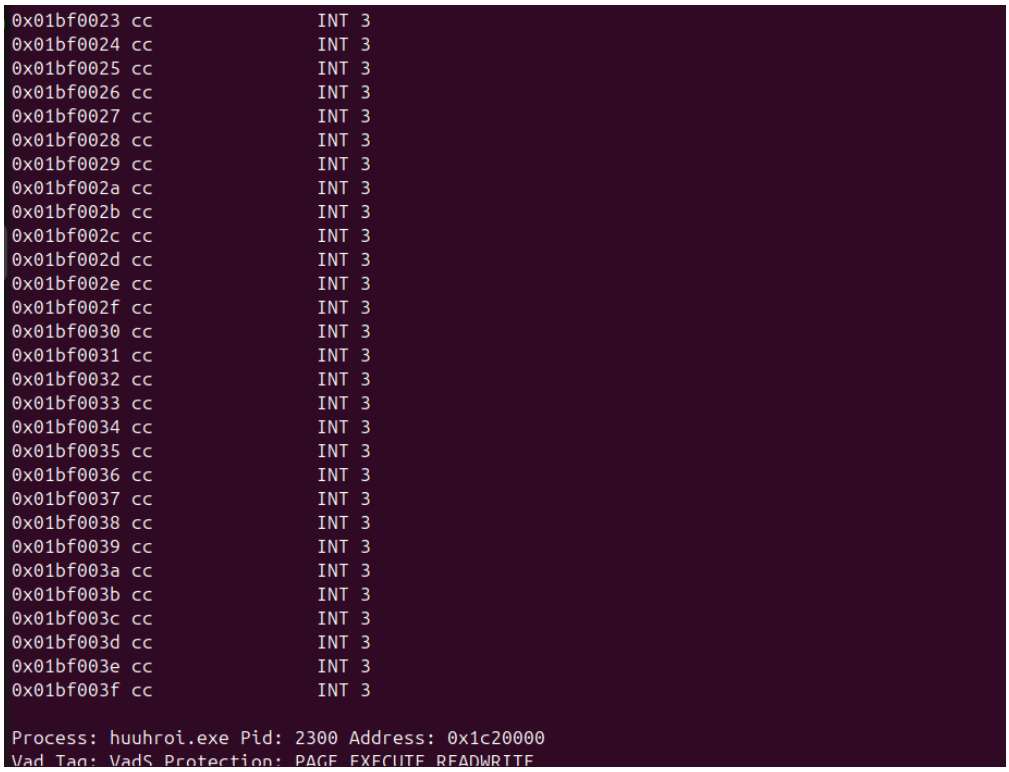


```
0x001d0024 0000             ADD [EAX], AL
0x001d0026 0000             ADD [EAX], AL
0x001d0028 0000             ADD [EAX], AL
0x001d002a 0000             ADD [EAX], AL
0x001d002c 0000             ADD [EAX], AL
0x001d002e 0000             ADD [EAX], AL
0x001d0030 0000             ADD [EAX], AL
0x001d0032 0000             ADD [EAX], AL
0x001d0034 0000             ADD [EAX], AL
0x001d0036 0000             ADD [EAX], AL
0x001d0038 0000             ADD [EAX], AL
0x001d003a 0000             ADD [EAX], AL
0x001d003c 0000             ADD [EAX], AL
0x001d003e 0000             ADD [EAX], AL

Process: huuhroi.exe Pid: 2300 Address: 0x1c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x001c0000  43 00 3a 00 5c 00 74 00 6d 00 70 00 76 00 61 00   C.:.\.t.m.p.v.a.
0x001c0010  70 00 6b 00 6f 00 6f 00 5c 00 62 00 69 00 6e 00   p.k.o.o.\.b.i.n.
0x001c0020  5c 00 6d 00 6f 00 6e 00 69 00 74 00 6f 00 72 00   \.m.o.n.i.t.o.r.
0x001c0030  2d 00 78 00 38 00 36 00 2e 00 64 00 6c 00 6c 00   -.x.8.6...d.l.l.

0x001c0000 43               INC EBX
0x001c0001 003a             ADD [EDX], BH
0x001c0003 005c0074         ADD [EAX+EAX+0x74], BL
0x001c0007 006d00           ADD [EBP+0x0], CH
0x001c000a 7000             JO 0x1c000c
0x001c000c 7600             JBE 0x1c000e
0x001c000e 61               POPA
```

```
0x001c000f 007000           ADD [EAX+0x0], DH
0x001c0012 6b006f           IMUL EAX, [EAX], 0x6f
0x001c0015 006f00           ADD [EDI+0x0], CH
0x001c0018 5c               POP ESP
0x001c0019 006200           ADD [EDX+0x0], AH
0x001c001c 69006e005c00     IMUL EAX, [EAX], 0x5c006e
0x001c0022 6d               INS DWORD [ES:EDI], DX
0x001c0023 006f00           ADD [EDI+0x0], CH
0x001c0026 6e               OUTS DX, BYTE [ESI]
0x001c0027 006900           ADD [ECX+0x0], CH
0x001c002a 7400             JZ 0x1c002c
0x001c002c 6f               OUTS DX, DWORD [ESI]
0x001c002d 007200           ADD [EDX+0x0], DH
0x001c0030 2d00780038       SUB EAX, 0x38007800
0x001c0035 0036             ADD [ESI], DH
0x001c0037 002e             ADD [ESI], CH
0x001c0039 0064006c         ADD [EAX+EAX+0x6c], AH
0x001c003d 00               DB 0x0
0x001c003e 6c               INS BYTE [ES:EDI], DX
0x001c003f 00               DB 0x0

Process: huuhroi.exe Pid: 2300 Address: 0x1e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x001e0000  55 89 e5 83 ec 28 c7 45 f4 00 00 00 00 8b 45 08   U....(.E......E.
0x001e0010  8b 00 8b 55 08 8d 4a 08 8d 55 f0 89 54 24 0c 89   ...U..J..U..T$..
0x001e0020  4c 24 08 c7 44 24 04 00 00 00 00 c7 04 24 00 00   L$..D$.......$..
0x001e0030  00 00 ff d0 83 ec 10 85 c0 79 0b 8b 45 08 8b 40   .........y..E..@

0x001e0000 55               PUSH EBP
0x001e0001 89e5             MOV EBP, ESP
```

```
0x001e0003 83ec28           SUB ESP, 0x28
0x001e0006 c745f400000000   MOV DWORD [EBP-0xc], 0x0
0x001e000d 8b4508           MOV EAX, [EBP+0x8]
0x001e0010 8b00             MOV EAX, [EAX]
0x001e0012 8b5508           MOV EDX, [EBP+0x8]
0x001e0015 8d4a08           LEA ECX, [EDX+0x8]
0x001e0018 8d55f0           LEA EDX, [EBP-0x10]
0x001e001b 8954240c         MOV [ESP+0xc], EDX
0x001e001f 894c2408         MOV [ESP+0x8], ECX
0x001e0023 c744240400000000 MOV DWORD [ESP+0x4], 0x0
0x001e002b c7042400000000   MOV DWORD [ESP], 0x0
0x001e0032 ffd0             CALL EAX
0x001e0034 83ec10           SUB ESP, 0x10
0x001e0037 85c0             TEST EAX, EAX
0x001e0039 790b             JNS 0x1e0046
0x001e003b 8b4508           MOV EAX, [EBP+0x8]
0x001e003e 8b               DB 0x8b
0x001e003f 40               INC EAX

Process: huuhroi.exe Pid: 2300 Address: 0x1bf0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
```

```
Flags: CommitCharge: 8, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01bf0000  6a 10 68 d0 1a a3 76 e9 57 4d e3 74 cc cc cc cc   j.h...v.WM.t....
0x01bf0010  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc   ................
0x01bf0020  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc   ................
0x01bf0030  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc   ................

0x01bf0000 6a10             PUSH 0x10
0x01bf0002 68d01aa376       PUSH DWORD 0x76a31ad0
0x01bf0007 e9574de374       JMP 0x76a24d63
0x01bf000c cc               INT 3
0x01bf000d cc               INT 3
0x01bf000e cc               INT 3
0x01bf000f cc               INT 3
0x01bf0010 cc               INT 3
0x01bf0011 cc               INT 3
0x01bf0012 cc               INT 3
0x01bf0013 cc               INT 3
0x01bf0014 cc               INT 3
0x01bf0015 cc               INT 3
0x01bf0016 cc               INT 3
0x01bf0017 cc               INT 3
0x01bf0018 cc               INT 3
0x01bf0019 cc               INT 3
0x01bf001a cc               INT 3
0x01bf001b cc               INT 3
0x01bf001c cc               INT 3
0x01bf001d cc               INT 3
```



Several potential suspicious or malicious activities can be observed:

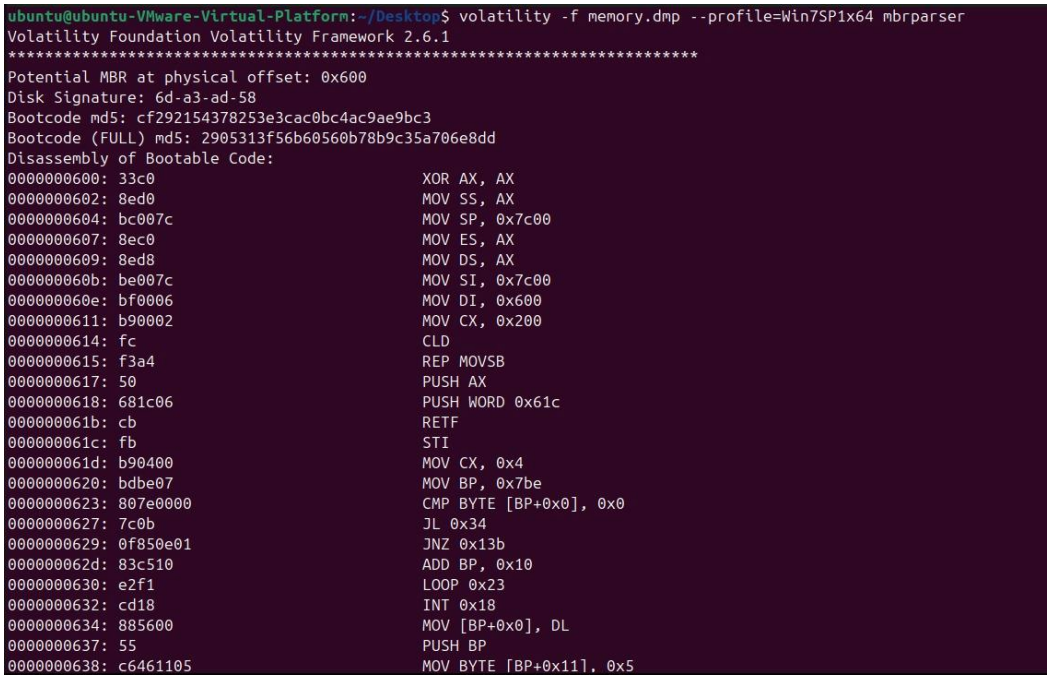
- **Code Injection:** The presence of memory regions marked as PAGE_EXECUTE_READWRITE within the process huuhroi.exe suggests code injection. This means that executable code has been written into a writable memory region, which is often indicative of malicious activity.
- **Encoded or Obfuscated Code:** Some of the assembly instructions appear to be encoded or obfuscated, which is a common technique used by malware to evade detection. For example, the repetitive ADD [EAX], AL instructions in certain memory regions could be part of obfuscation or padding to hide the actual malicious code.
- **Jump Instructions:** The presence of JMP (Jump) instructions to suspicious memory locations indicates control flow redirection, which could be a sign of code execution hijacking or exploitation attempts.
- **INT 3 Instructions:** The presence of INT 3 instructions at certain memory locations suggests the use of debug breakpoints, which could indicate debugging or analysis evasion attempts. Malware often uses such instructions to hinder reverse engineering efforts.

- **Replication or NOP Sleds:** Repetitive sequences of NOP (No Operation) instructions (NOP sleds) or redundant ADD instructions in memory regions may indicate attempts to create space for injected code or to confuse static analysis tools.
- **Non-Printable Characters:** Some memory regions contain non-printable characters or unintelligible data, which could indicate encrypted or packed code that is intended to conceal its true purpose.
- **Unusual Memory Allocation Patterns:** The allocation of memory regions with excessive Commit Charge and Private Memory flags may indicate abnormal memory usage patterns, potentially associated with malware attempting to hide its presence or evade detection.

The combination of writable and executable memory regions, along with the presence of encoded or obfuscated code, control flow redirection, debug instructions, and unusual memory allocation patterns, suggests that the **process huuhroi.exe** may have been compromised or infected by malicious code.

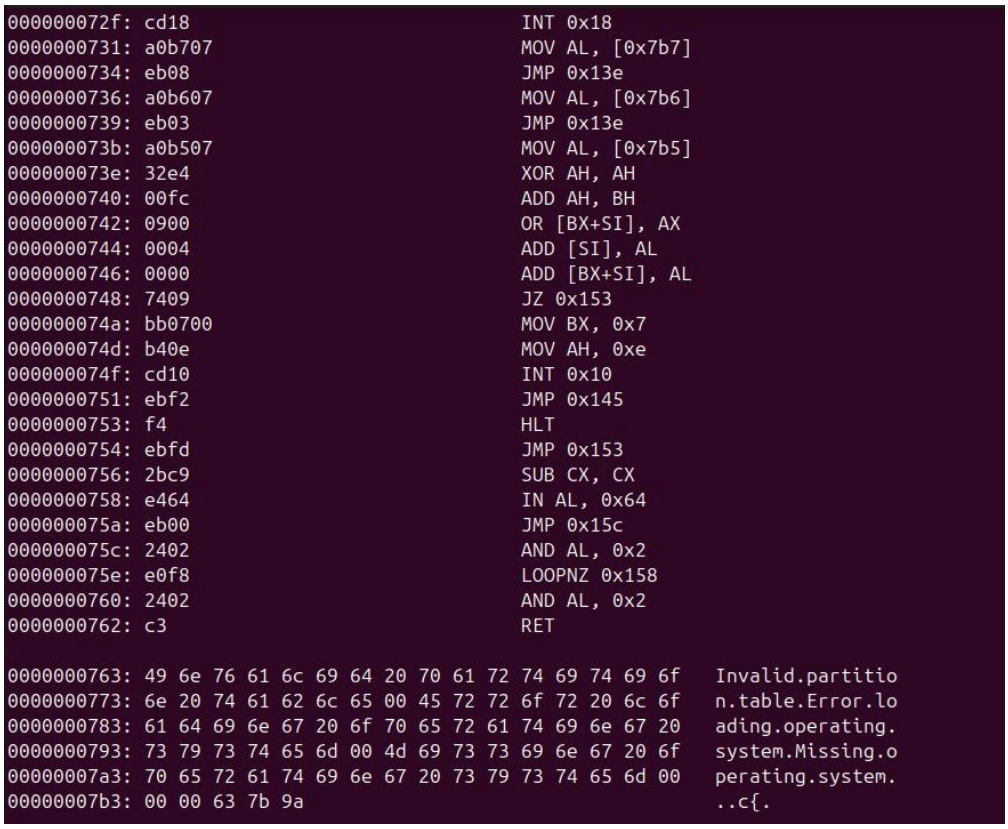
Hard Disk Analysis

mbrparser: This plugin is used for analyzing the Master Boot Record (MBR) of a disk image. The MBR is the first sector of a storage device and contains crucial information for bootstrapping an operating system.



```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 mbrparser
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
Potential MBR at physical offset: 0x600
Disk Signature: 6d-a3-ad-58
Bootcode md5: cf292154378253e3cac0bc4ac9ae9bc3
Bootcode (FULL) md5: 2905313f56b60560b78b9c35a706e8dd
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
0000000638: c6461105                    MOV BYTE [BP+0x11], 0x5
```

```
000000063c: c6461000                    MOV BYTE [BP+0x10], 0x0
0000000640: b441                        MOV AH, 0x41
0000000642: bbaa55                      MOV BX, 0x55aa
0000000645: cd13                        INT 0x13
0000000647: 5d                          POP BP
0000000648: 720f                        JB 0x59
000000064a: 81fb55aa                    CMP BX, 0xaa55
000000064e: 7509                        JNZ 0x59
0000000650: f7c10100                    TEST CX, 0x1
0000000654: 7403                        JZ 0x59
0000000656: fe4610                      INC BYTE [BP+0x10]
0000000659: 6660                        PUSHA
000000065b: 807e1000                    CMP BYTE [BP+0x10], 0x0
000000065f: 7426                        JZ 0x87
0000000661: 666800000000                PUSH DWORD 0x0
0000000667: 66ff7608                    PUSH DWORD [BP+0x8]
000000066b: 680000                      PUSH WORD 0x0
000000066e: 68007c                      PUSH WORD 0x7c00
0000000671: 680100                      PUSH WORD 0x1
0000000674: 681000                      PUSH WORD 0x10
0000000677: b442                        MOV AH, 0x42
0000000679: 8a5600                      MOV DL, [BP+0x0]
000000067c: 8bf4                        MOV SI, SP
000000067e: cd13                        INT 0x13
0000000680: 9f                          LAHF
0000000681: 83c410                      ADD SP, 0x10
0000000684: 9e                          SAHF
0000000685: eb14                        JMP 0x9b
0000000687: b80102                      MOV AX, 0x201
000000068a: bb007c                      MOV BX, 0x7c00
000000068d: 8a5600                      MOV DL, [BP+0x0]
0000000690: 8a7601                      MOV DH, [BP+0x1]
```



```
000000072f: cd18                            INT 0x18
0000000731: a0b707                          MOV AL, [0x7b7]
0000000734: eb08                            JMP 0x13e
0000000736: a0b607                          MOV AL, [0x7b6]
0000000739: eb03                            JMP 0x13e
000000073b: a0b507                          MOV AL, [0x7b5]
000000073e: 32e4                            XOR AH, AH
0000000740: 00fc                            ADD AH, BH
0000000742: 0900                            OR [BX+SI], AX
0000000744: 0004                            ADD [SI], AL
0000000746: 0000                            ADD [BX+SI], AL
0000000748: 7409                            JZ 0x153
000000074a: bb0700                          MOV BX, 0x7
000000074d: b40e                            MOV AH, 0xe
000000074f: cd10                            INT 0x10
0000000751: ebf2                            JMP 0x145
0000000753: f4                              HLT
0000000754: ebfd                            JMP 0x153
0000000756: 2bc9                            SUB CX, CX
0000000758: e464                            IN AL, 0x64
000000075a: eb00                            JMP 0x15c
000000075c: 2402                            AND AL, 0x2
000000075e: e0f8                            LOOPNZ 0x158
0000000760: 2402                            AND AL, 0x2
0000000762: c3                              RET

0000000763: 49 6e 76 61 6c 69 64 20 70 61 72 74 69 74 69 6f   Invalid.partitio
0000000773: 6e 20 74 61 62 6c 65 00 45 72 72 6f 72 20 6c 6f   n.table.Error.lo
0000000783: 61 64 69 6e 67 20 6f 70 65 72 61 74 69 6e 67 20   ading.operating.
0000000793: 73 79 73 74 65 6d 00 4d 69 73 73 69 6e 67 20 6f   system.Missing.o
00000007a3: 70 65 72 61 74 69 6e 67 20 73 79 73 74 65 6d 00   perating.system.
00000007b3: 00 00 63 7b 9a                                    ..c{.
```

```
===== Partition Table #1 =====
Boot flag: 0x80 (Bootable)
Partition type: 0x7 (NTFS)
Starting Sector (LBA): 0x800 (2048)
Starting CHS: Cylinder: 0 Head: 32 Sector: 33
Ending CHS: Cylinder: 38 Head: 94 Sector: 56
Size in sectors: 0x96000 (614400)

===== Partition Table #2 =====
Boot flag: 0x1
Partition type: 0x7 (NTFS)
Starting Sector (LBA): 0x96800 (616448)
Starting CHS: Cylinder: 38 Head: 5 Sector: 57
Ending CHS: Cylinder: 1023 Head: 254 Sector: 63
Size in sectors: 0x1ff69000 (536252416)

===== Partition Table #3 =====
Boot flag: 0x0
Partition type: 0x0 (Empty)
Starting Sector (LBA): 0x0 (0)
Starting CHS: Cylinder: 0 Head: 0 Sector: 0
Ending CHS: Cylinder: 0 Head: 0 Sector: 0
Size in sectors: 0x0 (0)

===== Partition Table #4 =====
Boot flag: 0x0
Partition type: 0x0 (Empty)
Starting Sector (LBA): 0x0 (0)
Starting CHS: Cylinder: 0 Head: 0 Sector: 0
Ending CHS: Cylinder: 0 Head: 0 Sector: 0
Size in sectors: 0x0 (0)
```

Potential MBR at physical offset: This indicates the physical offset where the potential MBR was found in the memory dump.

- **Disk Signature:** This is the signature of the disk.
- **Bootcode md5:** MD5 hash of the boot code.
- **Bootcode (FULL) md5:** MD5 hash of the full boot code.
- **Disassembly of Bootable Code:** Disassembly of the bootable code found in the MBR, showing the assembly instructions.

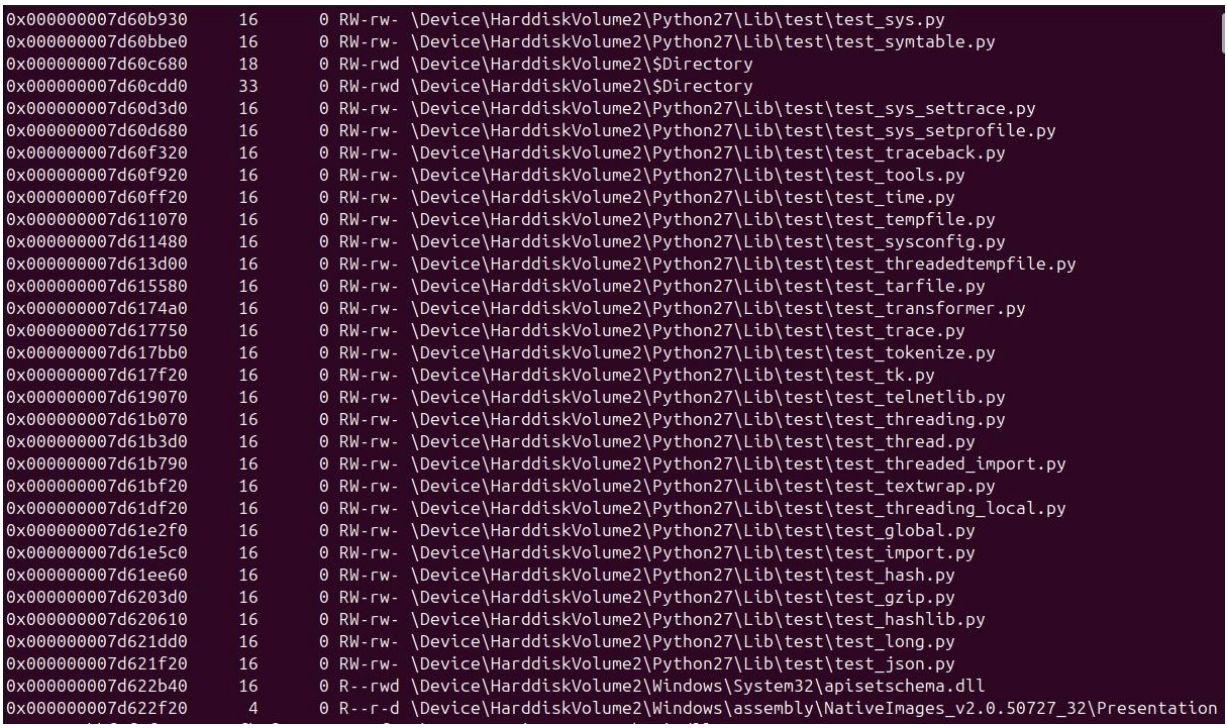
After disassembling the bootable code, the output provides information about the partitions:

- **Partition Table #1 to #4:** Information about each partition in the MBR, including the boot flag, partition type, starting sector, starting CHS (Cylinder, Head, Sector), ending CHS, and size in sectors.

File and Memory Analysis

filescan: This plugin is used for scanning and listing file objects that are present in the memory of a Windows system.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~/Desktop$ volatility -f memory.dmp --profile=Win7SP1x64 filescan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)           #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x00000000059f9660      6      0 R--r-d \Device\HarddiskVolume2\Windows\assembly\NativeImages_v2.0.50727_64\ehshell\d1dc
67c666bc15291be843bd67cd2a2e\ehshell.ni.dllshell.dll
0x00000000059fb290      5      0 R--r-d \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dl
l
0x00000000059fb5b0     12      0 R--r-d \Device\HarddiskVolume2\Windows\assembly\NativeImages_v2.0.50727_32\Accessibilit
y\9859a6e0562f64eacfb8ad76f260a2d6\Accessibility.ni.dll
0x00000000059fbcd0      9      0 R--r-d \Device\HarddiskVolume2\Program Files\Windows Defender\MpSvc.dll
0x000000007d600810     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_optparse.py
0x000000007d600d90     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_os.py
0x000000007d601070     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_nis.py
0x000000007d6017e0     17      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot2\edb.log
0x000000007d601930     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_new.py
0x000000007d601f20     16      0 RW-rw- \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v2.0.50727\ASP.NETWebA
dminFiles\Images\ASPdotNET_logo.jpg
0x000000007d6028e0     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_StringIO.py
0x000000007d602e60     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_strop.py
0x000000007d603680     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_string.py
0x000000007d603a70     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_stringprep.py
0x000000007d604640     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_operator.py
0x000000007d604cd0     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_openpty.py
0x000000007d6059a0     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_old_mailbox.py
0x000000007d605bb0     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_ntpath.py
0x000000007d606070     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_shelve.py
0x000000007d6066b0     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_SimpleHTTPServer.py
0x000000007d607350     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_sgmllib.py
0x000000007d608970     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_opcodes.py
0x000000007d608d10     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_pep263.py
0x000000007d60ab10     12      0 R--r-d \Device\HarddiskVolume2\Windows\SysWOW64\wtsapi32.dll
0x000000007d60b930     16      0 RW-rw- \Device\HarddiskVolume2\Python27\Lib\test\test_sys.py
```



In Windows Operating System, file objects represent files that are currently open or being used by processes. These file objects contain information such as the **file name, file handle, file attributes**, and other **metadata** associated with the file.

Conclusion

By carefully examining the Windows memory dump with Volatility plugins on Ubuntu Linux, we've gained a deep understanding of the system's operations and potential security risks. We looked at many aspects like processes, network activities, DLL files, registry entries, drivers, and more.

We found some important things. For example, we spotted suspicious processes and strange network connections that could indicate security problems. Also, we checked out DLL files and registry entries for any signs of tampering or unauthorized changes.

We also dove into the system's core, looking for any hidden threats or unusual activities in the kernel. And when we analyzed files, we found evidence of possible malware and how it might have been trying to sneak around the system.

Our investigation didn't stop there. We went further, digging into the behavior of potential malware, trying to understand how it works and how it might try to avoid detection. And by looking at the history of the hard disk, we found clues about past actions and attempts to delete or hide files.

All of this tells us a lot about the system's health and security. It's clear that we need to stay vigilant and keep up with the latest threats. By learning from this investigation and working together with others in the field, we can better protect ourselves against cyber threats in the future.