Assignment: Memory and Volatility Lab

Keegan R. Heaton

University of Advancing Technology

CFR - 101 Computer Forensic Essentials

Aaron Rodriguez

3/12/2024

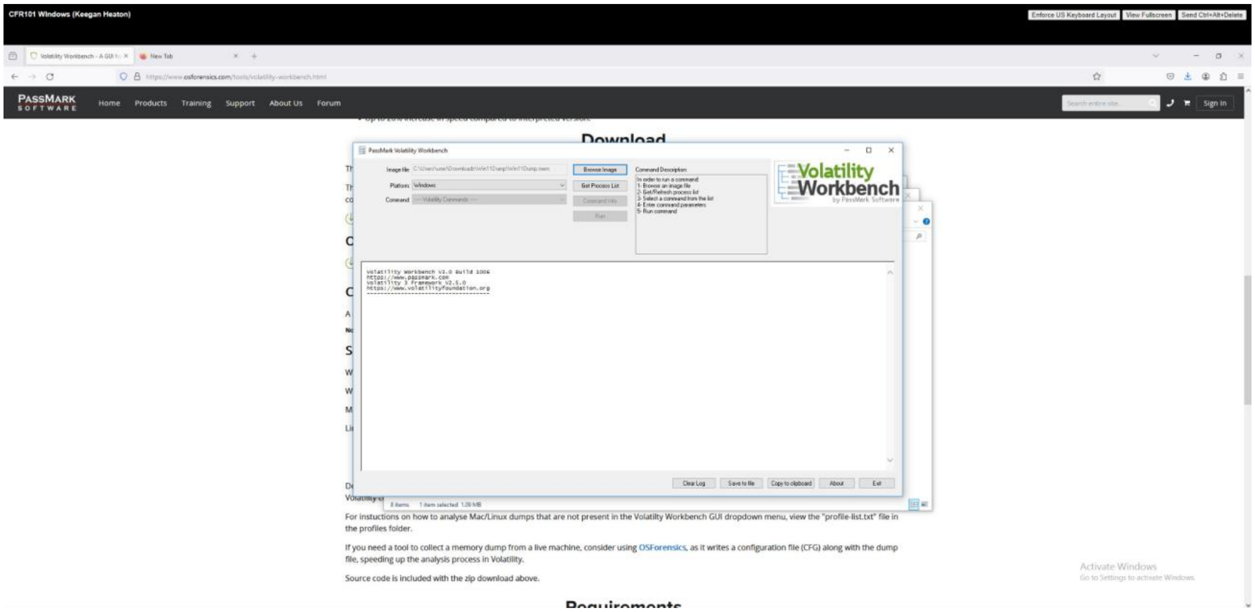


Image file: C:\Users\user\Downloads\Win11Dump\Win11Dump.mem
Platform: Windows
Command: --- Volatility Commands ---

Command Description:
In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command

```
Volatility Workbench v3.0 Build 1006
https://www.passmark.com
Volatility 3 Framework v2.5.0
https://www.volatilityfoundation.org
------------------------------------
```

For instructions on how to analyse Mac/Linux dumps that are not present in the Volatilty Workbench GUI dropdown menu, view the "profile-list.txt" file in the profiles folder.

If you need a tool to collect a memory dump from a live machine, consider using OSForensics, as it writes a configuration file (CFG) along with the dump file, speeding up the analysis process in Volatility.

Source code is included with the zip download above.

1.

a. Using Volatility workbench and a sampled Windows 10 dump, I scanned the dump using Volatility. Due to memory constraints, I only did the windows 10 dump and not all three dumps.

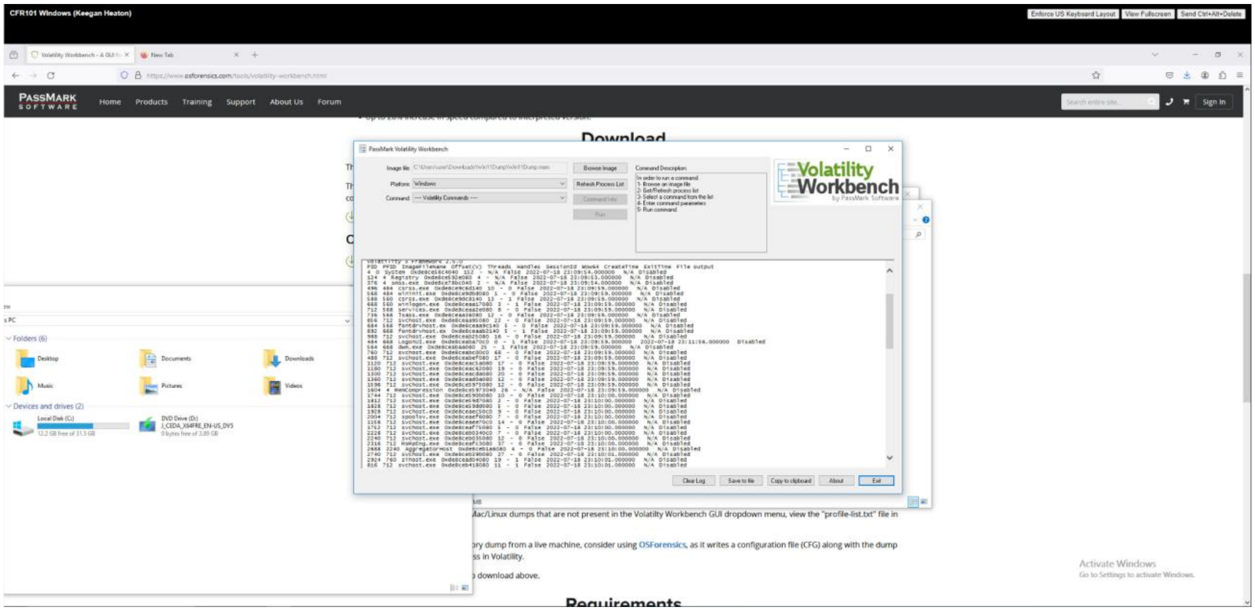


Image file: C:\Users\user\Downloads\Win11Dump\Win11Dump.mem
Platform: Windows
Command: --- Volatility Commands ---

Command Description:
In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command

```
Volatility 3 Framework 2.5.0
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
4  0  System  0xde8ce58c4040  152  -  N/A  False  2022-07-18 23:09:54.000000   N/A  Disabled
124  4  Registry  0xde8ce592e080  4  -  N/A  False  2022-07-18 23:09:53.000000   N/A  Disabled
376  4  smss.exe  0xde8ce78bc040  2  -  N/A  False  2022-07-18 23:09:54.000000   N/A  Disabled
496  484  csrss.exe  0xde8ce9c6d140  10  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
568  484  wininit.exe  0xde8ce9dbd080  1  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
580  560  csrss.exe  0xde8ce9dc8140  13  -  1  False  2022-07-18 23:09:59.000000   N/A  Disabled
668  560  winlogon.exe  0xde8ceaa17080  3  -  1  False  2022-07-18 23:09:59.000000   N/A  Disabled
712  568  services.exe  0xde8ceaa2e080  8  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
736  568  lsass.exe  0xde8ceaa36080  12  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
856  712  svchost.exe  0xde8ceaa95080  22  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
884  568  fontdrvhost.ex  0xde8ceaa9c140  5  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
892  668  fontdrvhost.ex  0xde8ceaab2140  5  -  1  False  2022-07-18 23:09:59.000000   N/A  Disabled
988  712  svchost.exe  0xde8ceab25080  16  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
484  668  LogonUI.exe  0xde8ceaba70c0  0  -  1  False  2022-07-18 23:09:59.000000   2022-07-18 23:11:56.000000   Disabled
564  668  dwm.exe  0xde8ceabaa080  25  -  1  False  2022-07-18 23:09:59.000000   N/A  Disabled
760  712  svchost.exe  0xde8ceabc00c0  68  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
488  712  svchost.exe  0xde8ceabef080  17  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1120  712  svchost.exe  0xde8ceac5a080  17  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1180  712  svchost.exe  0xde8ceac62080  19  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1300  712  svchost.exe  0xde8ceacda080  20  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1360  712  svchost.exe  0xde8cead0a080  12  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1596  712  svchost.exe  0xde8ce5975080  12  -  0  False  2022-07-18 23:09:59.000000   N/A  Disabled
1604  4  MemCompression  0xde8ce5973040  26  -  N/A  False  2022-07-18 23:09:59.000000   N/A  Disabled
1744  712  svchost.exe  0xde8ce590b080  10  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
1812  712  svchost.exe  0xde8ce69d7080  3  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
1828  712  svchost.exe  0xde8ce59dd080  5  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
1928  712  svchost.exe  0xde8ceaec50c0  9  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2004  712  spoolsv.exe  0xde8ceaef6080  7  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
1156  712  svchost.exe  0xde8ceaee70c0  14  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
1762  712  svchost.exe  0xde8ceaf75080  6  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2228  712  svchost.exe  0xde8ceb0340c0  7  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2240  712  svchost.exe  0xde8ceb035080  12  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2316  712  MsMpEng.exe  0xde8ceafc3080  37  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2688  2240  AggregatorHost  0xde8ceb1a6080  4  -  0  False  2022-07-18 23:10:00.000000   N/A  Disabled
2740  712  svchost.exe  0xde8ceb39b080  27  -  0  False  2022-07-18 23:10:01.000000   N/A  Disabled
2924  760  sihost.exe  0xde8cead04080  19  -  1  False  2022-07-18 23:10:01.000000   N/A  Disabled
816  712  svchost.exe  0xde8ceb418080  11  -  1  False  2022-07-18 23:10:01.000000   N/A  Disabled
```

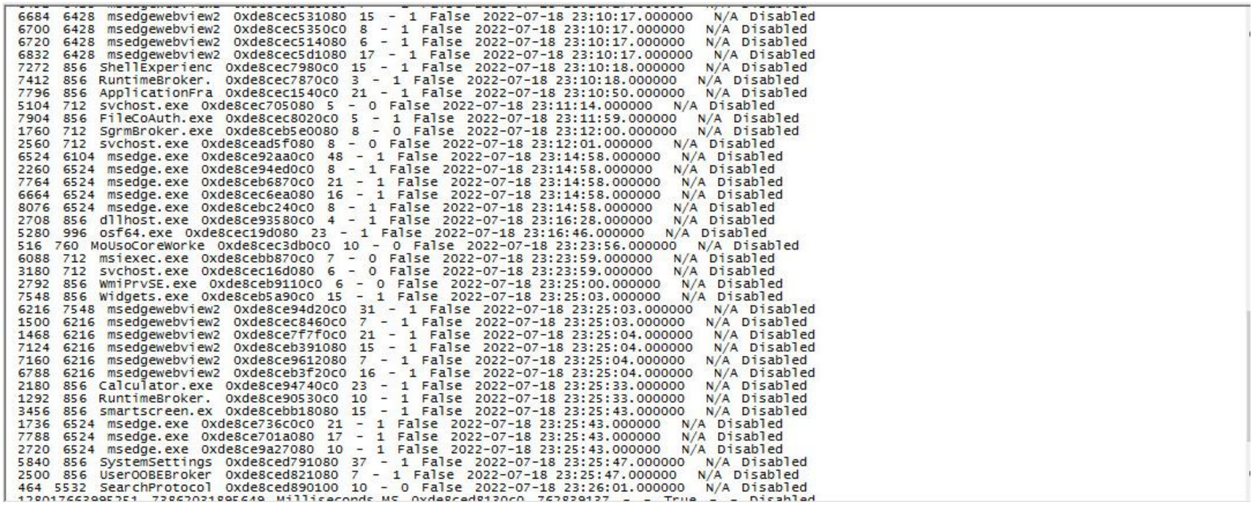
Mac/Linux dumps that are not present in the Volatilty Workbench GUI dropdown menu, view the "profile-list.txt" file in

ory dump from a live machine, consider using OSForensics, as it writes a configuration file (CFG) along with the dump ss in Volatility.

download above.

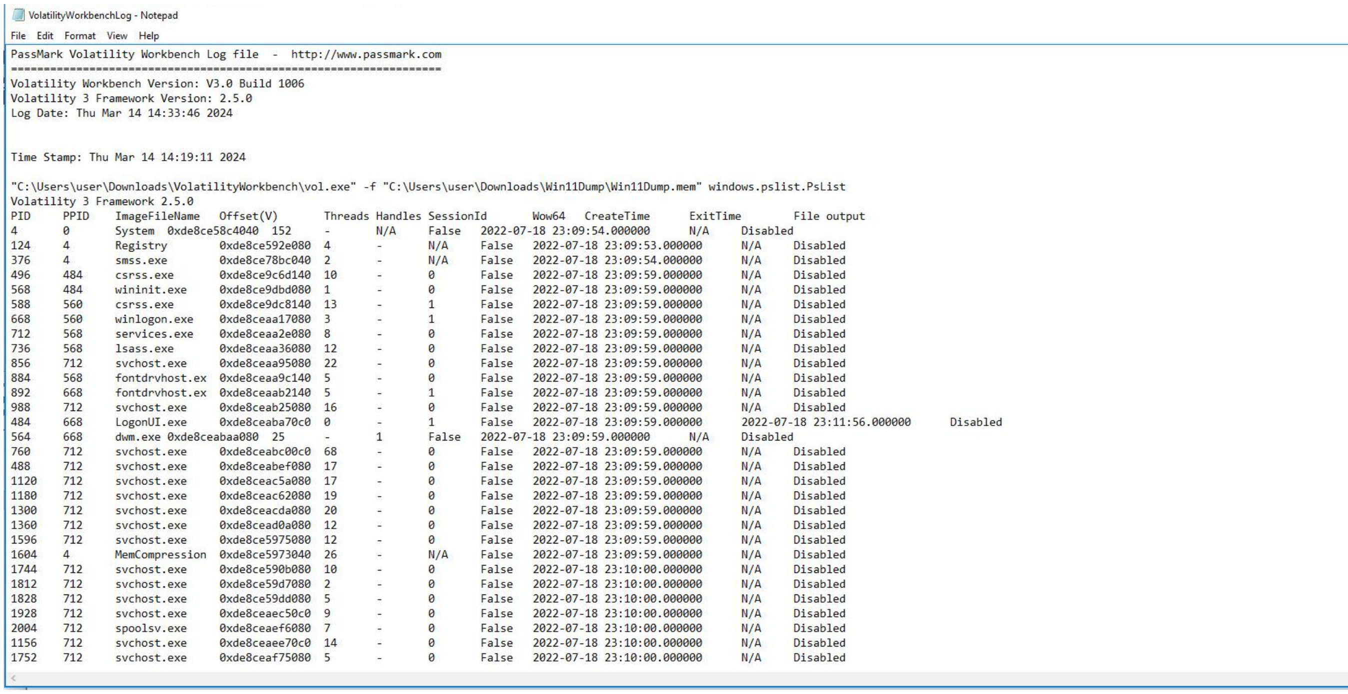
2.

a. Once Volatility starts processing the process list, it takes about 10-15 minutes to complete. This screenshot shows the process list Volatility created of the Windows 10 dump. The list shows all open items and processes recorded.

3. 

```
6684  6428  msedgewebview2  0xde8cec531080  15  -  1  False  2022-07-18 23:10:17.000000   N/A  Disabled
6700  6428  msedgewebview2  0xde8cec5350c0  8  -  1  False  2022-07-18 23:10:17.000000   N/A  Disabled
6720  6428  msedgewebview2  0xde8cec514080  6  -  1  False  2022-07-18 23:10:17.000000   N/A  Disabled
6832  6428  msedgewebview2  0xde8cec5d1080  17  -  1  False  2022-07-18 23:10:17.000000   N/A  Disabled
7272  856  ShellExperienc  0xde8cec7980c0  15  -  1  False  2022-07-18 23:10:18.000000   N/A  Disabled
7412  856  RuntimeBroker.  0xde8cec7870c0  3  -  1  False  2022-07-18 23:10:18.000000   N/A  Disabled
7796  856  ApplicationFra  0xde8cec1540c0  21  -  1  False  2022-07-18 23:10:50.000000   N/A  Disabled
5104  712  svchost.exe  0xde8cec705080  5  -  0  False  2022-07-18 23:11:14.000000   N/A  Disabled
7904  856  FileCoAuth.exe  0xde8cec8020c0  5  -  1  False  2022-07-18 23:11:59.000000   N/A  Disabled
1760  712  SgrmBroker.exe  0xde8ceb5e0080  8  -  0  False  2022-07-18 23:12:00.000000   N/A  Disabled
2560  712  svchost.exe  0xde8cead5f080  8  -  0  False  2022-07-18 23:12:01.000000   N/A  Disabled
6524  6104  msedge.exe  0xde8ce92aa0c0  48  -  1  False  2022-07-18 23:14:58.000000   N/A  Disabled
2260  6524  msedge.exe  0xde8ce94ed0c0  8  -  1  False  2022-07-18 23:14:58.000000   N/A  Disabled
7764  6524  msedge.exe  0xde8ceb6870c0  21  -  1  False  2022-07-18 23:14:58.000000   N/A  Disabled
6664  6524  msedge.exe  0xde8cec6ea080  16  -  1  False  2022-07-18 23:14:58.000000   N/A  Disabled
8076  6524  msedge.exe  0xde8cebc240c0  8  -  1  False  2022-07-18 23:14:58.000000   N/A  Disabled
2708  856  dllhost.exe  0xde8ce93580c0  4  -  1  False  2022-07-18 23:16:28.000000   N/A  Disabled
5280  996  osf64.exe  0xde8cec19d080  23  -  1  False  2022-07-18 23:16:46.000000   N/A  Disabled
516  760  MoUsoCoreWorke  0xde8cec3db0c0  10  -  0  False  2022-07-18 23:23:56.000000   N/A  Disabled
6088  712  msiexec.exe  0xde8cebb870c0  7  -  0  False  2022-07-18 23:23:59.000000   N/A  Disabled
3180  712  svchost.exe  0xde8cec16d080  6  -  0  False  2022-07-18 23:23:59.000000   N/A  Disabled
2792  856  WmiPrvSE.exe  0xde8ceb9110c0  6  -  0  False  2022-07-18 23:25:00.000000   N/A  Disabled
7548  856  Widgets.exe  0xde8ceb5a90c0  15  -  1  False  2022-07-18 23:25:03.000000   N/A  Disabled
6216  7548  msedgewebview2  0xde8ce94d20c0  31  -  1  False  2022-07-18 23:25:03.000000   N/A  Disabled
1500  6216  msedgewebview2  0xde8cec8460c0  7  -  1  False  2022-07-18 23:25:03.000000   N/A  Disabled
1468  6216  msedgewebview2  0xde8ce7f7f0c0  21  -  1  False  2022-07-18 23:25:04.000000   N/A  Disabled
7124  6216  msedgewebview2  0xde8ceb391080  15  -  1  False  2022-07-18 23:25:04.000000   N/A  Disabled
7160  6216  msedgewebview2  0xde8ce9612080  7  -  1  False  2022-07-18 23:25:04.000000   N/A  Disabled
6788  6216  msedgewebview2  0xde8ceb3f20c0  16  -  1  False  2022-07-18 23:25:04.000000   N/A  Disabled
2180  856  Calculator.exe  0xde8ce94740c0  23  -  1  False  2022-07-18 23:25:33.000000   N/A  Disabled
1292  856  RuntimeBroker.  0xde8ce90530c0  10  -  1  False  2022-07-18 23:25:33.000000   N/A  Disabled
3456  856  smartscreen.ex  0xde8cebb18080  15  -  1  False  2022-07-18 23:25:43.000000   N/A  Disabled
1736  6524  msedge.exe  0xde8ce736c0c0  21  -  1  False  2022-07-18 23:25:43.000000   N/A  Disabled
7788  6524  msedge.exe  0xde8ce701a080  17  -  1  False  2022-07-18 23:25:43.000000   N/A  Disabled
2720  6524  msedge.exe  0xde8ce9a27080  10  -  1  False  2022-07-18 23:25:43.000000   N/A  Disabled
5840  856  SystemSettings  0xde8ced791080  37  -  1  False  2022-07-18 23:25:47.000000   N/A  Disabled
2500  856  UserOOBEBroker  0xde8ced821080  7  -  1  False  2022-07-18 23:25:47.000000   N/A  Disabled
464  5532  SearchProtocol  0xde8ced890100  10  -  0  False  2022-07-18 23:26:01.000000   N/A  Disabled
```

   a. This screenshot shows more of the process list. From the information available, A majority of the processes were coming from the Microsoft Edge Browser.

4. 

```
PassMark Volatility Workbench Log file  -  http://www.passmark.com
=====================================================================
Volatility Workbench Version: V3.0 Build 1006
Volatility 3 Framework Version: 2.5.0
Log Date: Thu Mar 14 14:33:46 2024


Time Stamp: Thu Mar 14 14:19:11 2024

"C:\Users\user\Downloads\VolatilityWorkbench\vol.exe" -f "C:\Users\user\Downloads\Win11Dump\Win11Dump.mem" windows.pslist.PsList
Volatility 3 Framework 2.5.0
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output
4       0       System  0xde8ce58c4040  152     -       N/A     False   2022-07-18 23:09:54.000000      N/A     Disabled
124     4       Registry        0xde8ce592e080  4       -       N/A     False   2022-07-18 23:09:53.000000      N/A     Disabled
376     4       smss.exe        0xde8ce78bc040  2       -       N/A     False   2022-07-18 23:09:54.000000      N/A     Disabled
496     484     csrss.exe       0xde8ce9c6d140  10      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
568     484     wininit.exe     0xde8ce9dbd080  1       -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
588     560     csrss.exe       0xde8ce9dc8140  13      -       1       False   2022-07-18 23:09:59.000000      N/A     Disabled
668     560     winlogon.exe    0xde8ceaa17080  3       -       1       False   2022-07-18 23:09:59.000000      N/A     Disabled
712     568     services.exe    0xde8ceaa2e080  8       -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
736     568     lsass.exe       0xde8ceaa36080  12      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
856     712     svchost.exe     0xde8ceaa95080  22      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
884     568     fontdrvhost.ex  0xde8ceaa9c140  5       -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
892     668     fontdrvhost.ex  0xde8ceaab2140  5       -       1       False   2022-07-18 23:09:59.000000      N/A     Disabled
988     712     svchost.exe     0xde8ceab25080  16      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
484     668     LogonUI.exe     0xde8ceaba70c0  0       -       1       False   2022-07-18 23:09:59.000000      2022-07-18 23:11:56.000000      Disabled
564     668     dwm.exe 0xde8ceabaa080  25      -       1       False   2022-07-18 23:09:59.000000      N/A     Disabled
760     712     svchost.exe     0xde8ceabc00c0  68      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
488     712     svchost.exe     0xde8ceabef080  17      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1120    712     svchost.exe     0xde8ceac5a080  17      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1180    712     svchost.exe     0xde8ceac62080  19      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1300    712     svchost.exe     0xde8ceacda080  20      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1360    712     svchost.exe     0xde8cead0a080  12      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1596    712     svchost.exe     0xde8ce5975080  12      -       0       False   2022-07-18 23:09:59.000000      N/A     Disabled
1604    4       MemCompression  0xde8ce5973040  26      -       N/A     False   2022-07-18 23:09:59.000000      N/A     Disabled
1744    712     svchost.exe     0xde8ce590b080  10      -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
1812    712     svchost.exe     0xde8ce59d7080  2       -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
1828    712     svchost.exe     0xde8ce59dd080  5       -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
1928    712     svchost.exe     0xde8ceaec50c0  9       -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
2004    712     spoolsv.exe     0xde8ceaef6080  7       -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
1156    712     svchost.exe     0xde8ceaee70c0  14      -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
1752    712     svchost.exe     0xde8ceaf75080  5       -       0       False   2022-07-18 23:10:00.000000      N/A     Disabled
```

   a. This Screenshot shows the categories of information. The PID, PPID, ImageFileName, Offset, Threads, Handles, SessionID, Wow64, CreateTime, ExitTime, File output are all categories available.