Time Stamp: Fri Mar 26 23:02:47 2021

"C:\Users\rgrdo\Downloads\VolatilityWorkbench\vol.exe" -f "F:\DQ lab 4 take 2.mem" windows.pslist.PsList

Volatility 3 Framework 1.1.0-beta.1

PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime

4 0 System 0x968fa54a2300 272 - N/A False 2021-03-21 00:24:26.000000 N/A

144 4 Registry 0x968fa56e1040 4 - N/A False 2021-03-21 00:24:14.000000 N/A

716 4 smss.exe 0x968fbef08040 2 - N/A False 2021-03-21 00:24:26.000000 N/A

804 788 csrss.exe 0x968fbe98e140 14 - 0 False 2021-03-21 00:24:26.000000 N/A

936 788 wininit.exe 0x968fbfe950c0 1 - 0 False 2021-03-21 00:24:30.000000 N/A

944 928 csrss.exe 0x968fc124b140 14 - 1 False 2021-03-21 00:24:30.000000 N/A

1008 936 services.exe 0x968fc1270180 6 - 0 False 2021-03-21 00:24:30.000000 N/A

104 936 lsass.exe 0x968fc10d3080 6 - 0 False 2021-03-21 00:24:30.000000 N/A

120 1008 svchost.exe 0x968fc13ef380 1 - 0 False 2021-03-21 00:24:31.000000 N/A

1048 1008 svchost.exe 0x968fc13f1340 16 - 0 False 2021-03-21 00:24:31.000000 N/A

1072 1008 WUDFHost.exe 0x968fc1ad3240 10 - 0 False 2021-03-21 00:24:31.000000 N/A

1080 936 fontdrvhost.ex 0x968fc1ad5240 5 - 0 False 2021-03-21 00:24:31.000000 N/A

1184 1008 WUDFHost.exe 0x968fbee27080 13 - 0 False 2021-03-21 00:24:31.000000 N/A

1224 1008 svchost.exe 0x968fc1b5f3c0 12 - 0 False 2021-03-21 00:24:31.000000 N/A

1284 1008 svchost.exe 0x968fc1ba9380 3 - 0 False 2021-03-21 00:24:31.000000 N/A

1368 928 winlogon.exe 0x968fc1bd9080 3 - 1 False 2021-03-21 00:24:31.000000 N/A

1424 1368 fontdrvhost.ex 0x968fc1bf3240 5 - 1 False 2021-03-21 00:24:31.000000 N/A

1500 1368 LogonUI.exe 0x968fbf0211c0 0 - 1 False 2021-03-21 00:24:31.000000 2021-03-21 00:24:59.000000

1508 1368 dwm.exe 0x968fbf00f100 12 - 1 False 2021-03-21 00:24:31.000000 N/A

1588 1008 svchost.exe 0x968fc1cf8400 2 - 0 False 2021-03-21 00:24:31.000000 N/A

1596 1008 svchost.exe 0x968fc1cf9080 2 - 0 False 2021-03-21 00:24:31.000000 N/A

1604 1008 svchost.exe 0x968fc1d25400 7 - 0 False 2021-03-21 00:24:31.000000 N/A

1704 1008 svchost.exe 0x968fc1d48380 6 - 0 False 2021-03-21 00:24:31.000000 N/A

1712 1008 svchost.exe 0x968fc1d4a400 1 - 0 False 2021-03-21 00:24:31.000000 N/A

1840 1008 svchost.exe 0x968fc1d7d3c0 2 - 0 False 2021-03-21 00:24:31.000000 N/A

1860 1008 svchost.exe 0x968fc1d7f380 7 - 0 False 2021-03-21 00:24:31.000000 N/A

1868 1008 svchost.exe 0x968fc1d81380 5 - 0 False 2021-03-21 00:24:31.000000 N/A

1988 1008 svchost.exe 0x968fc1e1d080 2 - 0 False 2021-03-21 00:24:31.000000 N/A

8 1008 svchost.exe 0x968fc1e86400 6 - 0 False 2021-03-21 00:24:31.000000 N/A

932 1008 svchost.exe 0x968fc1e89080 2 - 0 False 2021-03-21 00:24:31.000000 N/A

2096 1008 svchost.exe 0x968fc1e99380 4 - 0 False 2021-03-21 00:24:31.000000 N/A

2144 1008 UshUpgradeServ 0x968fc1eec380 2 - 0 False 2021-03-21 00:24:31.000000 N/A

2232 1008 atiesrxx.exe 0x968fc1fa3080 4 - 0 False 2021-03-21 00:24:31.000000 N/A

2240 1008 svchost.exe 0x968fc1fa5400 7 - 0 False 2021-03-21 00:24:31.000000 N/A

2360 1008 svchost.exe 0x968fc1fc9400 1 - 0 False 2021-03-21 00:24:31.000000 N/A

2420 1008 svchost.exe 0x968fc20053c0 4 - 0 False 2021-03-21 00:24:31.000000 N/A

2516 1008 svchost.exe 0x968fc20a1380 8 - 0 False 2021-03-21 00:24:31.000000 N/A

2524 2420 dasHost.exe 0x968fc20a4080 11 - 0 False 2021-03-21 00:24:31.000000 N/A

2568 1008 svchost.exe 0x968fc20bd3c0 1 - 0 False 2021-03-21 00:24:31.000000 N/A

2604 1008 svchost.exe 0x968fc20bf400 5 - 0 False 2021-03-21 00:24:31.000000 N/A

2688 1008 svchost.exe 0x968fc2106400 7 - 0 False 2021-03-21 00:24:31.000000 N/A

2744 1008 svchost.exe 0x968fc216c400 10 - 0 False 2021-03-21 00:24:31.000000 N/A

2820 1008 svchost.exe 0x968fc21ae400 10 - 0 False 2021-03-21 00:24:31.000000 N/A

2888 1008 svchost.exe 0x968fc22153c0 2 - 0 False 2021-03-21 00:24:31.000000 N/A

3040 1008 WUDFHost.exe 0x968fc226b080 5 - 0 False 2021-03-21 00:24:32.000000 N/A

2476 1008 svchost.exe 0x968fc22e90c0 0 - 0 False 2021-03-21 00:24:32.000000 2021-03-21 00:25:40.000000

3112 1008 WUDFHost.exe 0x968fc22f8080 5 - 0 False 2021-03-21 00:24:32.000000 N/A

3168 1008 svchost.exe 0x968fc239a080 4 - 0 False 2021-03-21 00:24:32.000000 N/A

3176 1008 svchost.exe 0x968fc239c380 3 - 0 False 2021-03-21 00:24:32.000000 N/A

3184 1008 svchost.exe 0x968fc239b080 4 - 0 False 2021-03-21 00:24:32.000000 N/A

3192 2232 atieclxx.exe 0x968fc23a3440 8 - 1 False 2021-03-21 00:24:32.000000 N/A

3276 4 MemCompression 0x968fc22f6480 46 - N/A False 2021-03-21 00:24:32.000000 N/A

3324 1008 svchost.exe 0x968fc248d340 2 - 0 False 2021-03-21 00:24:32.000000 N/A

3352 1008 svchost.exe 0x968fc24230c0 6 - 0 False 2021-03-21 00:24:32.000000 N/A

3360 1008 svchost.exe 0x968fc23da080 4 - 0 False 2021-03-21 00:24:32.000000 N/A

3408 1008 igfxCUIService 0x968fc24c1080 2 - 0 False 2021-03-21 00:24:32.000000 N/A

3460 1008 svchost.exe 0x968fc24b4080 2 - 0 False 2021-03-21 00:24:32.000000 N/A

3468 1008 svchost.exe 0x968fc24b9400 4 - 0 False 2021-03-21 00:24:32.000000 N/A

3560 1008 svchost.exe 0x968fc24da080 2 - 0 False 2021-03-21 00:24:32.000000 N/A

3744 2096 sihost.exe 0x968fc25db0c0 10 - 1 False 2021-03-21 00:24:32.000000 N/A

3788 1008 svchost.exe 0x968fc25e5080 10 - 1 False 2021-03-21 00:24:32.000000 N/A

3852 1008 svchost.exe 0x968fc2e30440 2 - 0 False 2021-03-21 00:24:32.000000 N/A

3900 1008 svchost.exe 0x968fc2e3e400 8 - 0 False 2021-03-21 00:24:32.000000 N/A

3936 2420 dasHost.exe 0x968fc2e4d3c0 1 - 0 False 2021-03-21 00:24:32.000000 N/A

4020 1008 svchost.exe 0x968fc2eac3c0 6 - 1 False 2021-03-21 00:24:32.000000 N/A

3620 1008 svchost.exe 0x968fc2ee0380 19 - 0 False 2021-03-21 00:24:32.000000 N/A

4008 1008 svchost.exe 0x968fc2ee2400 7 - 0 False 2021-03-21 00:24:32.000000 N/A

4028 1008 svchost.exe 0x968fc2ee4400 14 - 0 False 2021-03-21 00:24:32.000000 N/A

4128 1860 taskhostw.exe 0x968fc2eec080 8 - 1 False 2021-03-21 00:24:32.000000 N/A

4260 1008 svchost.exe 0x968fc2f89380 6 - 0 False 2021-03-21 00:24:32.000000 N/A

4420 1008 svchost.exe 0x968fc40af3c0 3 - 0 False 2021-03-21 00:24:32.000000 N/A

4524 1008 svchost.exe 0x968fc40d8080 14 - 0 False 2021-03-21 00:24:32.000000 N/A

4548 4420 ctfmon.exe 0x968fc40d9080 11 - 1 False 2021-03-21 00:24:32.000000 N/A

4568 1008 svchost.exe 0x968fc40da080 6 - 0 False 2021-03-21 00:24:32.000000 N/A

4728 1008 svchost.exe 0x968fc4107380 4 - 0 False 2021-03-21 00:24:32.000000 N/A

4824 1008 svchost.exe 0x968fc41a73c0 12 - 0 False 2021-03-21 00:24:32.000000 N/A

4940 1008 spoolsv.exe 0x968fc41f0340 12 - 0 False 2021-03-21 00:24:32.000000 N/A

5052 1008 HostStorageSer 0x968fc429f380 2 - 0 False 2021-03-21 00:24:32.000000 N/A

5064 1008 HostControlSer 0x968fc42cb380 1 - 0 False 2021-03-21 00:24:32.000000 N/A

4976 1008 svchost.exe 0x968fc431e380 8 - 0 False 2021-03-21 00:24:32.000000 N/A

5132 1008 svchost.exe 0x968fc4320400 10 - 0 False 2021-03-21 00:24:32.000000 N/A

5212 1008 svchost.exe 0x968fc434d400 3 - 0 False 2021-03-21 00:24:32.000000 N/A

5564 1008 AdminService.e 0x968fc44da080 3 - 0 False 2021-03-21 00:24:33.000000 N/A

5580 1008 svchost.exe 0x968fc4390080 11 - 0 False 2021-03-21 00:24:33.000000 N/A

5592 1008 esif\_uf.exe 0x968fc4395080 3 - 0 False 2021-03-21 00:24:33.000000 N/A

5648 1008 svchost.exe 0x968fc44f9400 5 - 0 False 2021-03-21 00:24:33.000000 N/A

5656 1008 svchost.exe 0x968fc44fb380 5 - 0 False 2021-03-21 00:24:33.000000 N/A

5664 1008 IntelCpHDCPSvc 0x968fc44fc080 4 - 0 False 2021-03-21 00:24:33.000000 N/A

5672 1008 svchost.exe 0x968fc44fa080 18 - 0 False 2021-03-21 00:24:33.000000 N/A

5684 1008 dpoMonitorSvc. 0x968fc448c080 6 - 0 False 2021-03-21 00:24:33.000000 N/A

5696 1008 HidMonitorSvc. 0x968fc44f0080 2 - 0 False 2021-03-21 00:24:33.000000 N/A

5704 1008 LMS.exe 0x968fc44fe400 4 - 0 True 2021-03-21 00:24:33.000000 N/A

5720 1008 svchost.exe 0x968fc44e0400 1 - 0 False 2021-03-21 00:24:33.000000 N/A

5732 1008 dpoTelemetrySv 0x968fc44e1080 7 - 0 False 2021-03-21 00:24:33.000000 N/A

5740 1008 svchost.exe 0x968fc4598400 1 - 0 False 2021-03-21 00:24:33.000000 N/A

5748 1008 poaTaServ.exe 0x968fc459a380 3 - 0 False 2021-03-21 00:24:33.000000 N/A

5768 1008 QcomWlanSrvx64 0x968fc44f8080 3 - 0 False 2021-03-21 00:24:33.000000 N/A

5780 1008 poaSmSrv.exe 0x968fc4597080 2 - 0 False 2021-03-21 00:24:33.000000 N/A

5788 1008 svchost.exe 0x968fc459d080 6 - 0 False 2021-03-21 00:24:33.000000 N/A

5804 1008 poaService.exe 0x968fc459c380 8 - 0 False 2021-03-21 00:24:33.000000 N/A

5816 1008 RstMwService.e 0x968fc459f4c0 6 - 0 False 2021-03-21 00:24:33.000000 N/A

5828 1008 svchost.exe 0x968fc4599080 3 - 0 False 2021-03-21 00:24:33.000000 N/A

5844 1008 SwiService.exe 0x968fc459b080 14 - 0 False 2021-03-21 00:24:33.000000 N/A

5860 1008 WavesSysSvc64. 0x968fc459e080 2 - 0 False 2021-03-21 00:24:33.000000 N/A

5896 1008 RtkAudUService 0x968fc45aa380 9 - 0 False 2021-03-21 00:24:33.000000 N/A

5908 1008 svchost.exe 0x968fc45ab080 8 - 0 False 2021-03-21 00:24:33.000000 N/A

5920 1008 MsMpEng.exe 0x968fc45ae440 52 - 0 False 2021-03-21 00:24:33.000000 N/A

6096 1008 svchost.exe 0x968fc461e380 4 - 0 False 2021-03-21 00:24:33.000000 N/A

6396 1008 jhi\_service.ex 0x968fc46a3340 2 - 0 False 2021-03-21 00:24:33.000000 N/A

6408 1008 svchost.exe 0x968fc4659400 2 - 0 False 2021-03-21 00:24:33.000000 N/A

6596 1008 svchost.exe 0x968fc48aa340 12 - 0 False 2021-03-21 00:24:33.000000 N/A

6648 1008 svchost.exe 0x968fc48bd400 8 - 0 False 2021-03-21 00:24:33.000000 N/A

6868 1008 IntelCpHeciSvc 0x968fc494b080 4 - 0 False 2021-03-21 00:24:33.000000 N/A

7840 1368 userinit.exe 0x968fc2eef080 0 - 1 False 2021-03-21 00:24:34.000000 2021-03-21 00:24:57.000000

7896 7840 explorer.exe 0x968fc4f4a080 78 - 1 False 2021-03-21 00:24:34.000000 N/A

8028 1008 svchost.exe 0x968fa5b1e400 7 - 0 False 2021-03-21 00:24:34.000000 N/A

1700 1048 WmiPrvSE.exe 0x968fa5a25380 7 - 0 False 2021-03-21 00:24:34.000000 N/A

7564 1008 svchost.exe 0x968fa5a450c0 4 - 1 False 2021-03-21 00:24:34.000000 N/A

8360 5696 Apoint.exe 0x968fa5a9a0c0 6 - 1 False 2021-03-21 00:24:34.000000 N/A

8652 1008 svchost.exe 0x968fc504a340 15 - 0 False 2021-03-21 00:24:34.000000 N/A

8716 1008 svchost.exe 0x968fc50aa400 8 - 0 False 2021-03-21 00:24:34.000000 N/A

8724 1008 svchost.exe 0x968fc50ac380 2 - 0 False 2021-03-21 00:24:34.000000 N/A

8832 1008 svchost.exe 0x968fc50482c0 2 - 0 False 2021-03-21 00:24:35.000000 N/A

8856 8360 ApMsgFwd.exe 0x968fc50ed080 2 - 1 False 2021-03-21 00:24:35.000000 N/A

8864 1008 svchost.exe 0x968fc50ef080 7 - 0 False 2021-03-21 00:24:35.000000 N/A

9084 8360 ApRemote.exe 0x968fc516f080 1 - 1 False 2021-03-21 00:24:35.000000 N/A

9108 8360 hidfind.exe 0x968fc5166080 1 - 1 False 2021-03-21 00:24:35.000000 N/A

9160 4192 RadeonSettings 0x968fc51e80c0 11 - 1 False 2021-03-21 00:24:35.000000 N/A

8404 1008 NisSrv.exe 0x968fc2edc080 7 - 0 False 2021-03-21 00:24:35.000000 N/A

8492 9072 ApntEx.exe 0x968fc52c3080 2 - 1 False 2021-03-21 00:24:35.000000 N/A

4100 8492 conhost.exe 0x968fc531f080 3 - 1 False 2021-03-21 00:24:35.000000 N/A

9256 1048 StartMenuExper 0x968fbe7f3080 11 - 1 False 2021-03-21 00:24:35.000000 N/A

9572 1008 svchost.exe 0x968fc5536080 5 - 0 False 2021-03-21 00:24:35.000000 N/A

9612 1048 RuntimeBroker. 0x968fc5308080 4 - 1 False 2021-03-21 00:24:35.000000 N/A

9784 1048 SearchUI.exe 0x968fc1eef080 63 - 1 False 2021-03-21 00:24:35.000000 N/A

9792 1008 SearchIndexer. 0x968fc5795380 30 - 0 False 2021-03-21 00:24:35.000000 N/A

10132 1048 RuntimeBroker. 0x968fc5875080 26 - 1 False 2021-03-21 00:24:36.000000 N/A

10052 5896 RtkAudUService 0x968fc5abb3c0 5 - 1 False 2021-03-21 00:24:36.000000 N/A

10356 1048 unsecapp.exe 0x968fc5aef380 3 - 1 False 2021-03-21 00:24:36.000000 N/A

10556 1048 SettingSyncHos 0x968fc5b450c0 12 - 1 False 2021-03-21 00:24:36.000000 N/A

10948 1048 LockApp.exe 0x968fc4a0b080 11 - 1 False 2021-03-21 00:24:36.000000 N/A

11076 1048 RuntimeBroker. 0x968fc5d3b080 5 - 1 False 2021-03-21 00:24:37.000000 N/A

11232 1048 RemindersServe 0x968fc5f36080 9 - 1 False 2021-03-21 00:24:38.000000 N/A

5504 1048 YourPhone.exe 0x968fc5f40240 13 - 1 False 2021-03-21 00:24:38.000000 N/A

11456 1048 RuntimeBroker. 0x968fc579a0c0 3 - 1 False 2021-03-21 00:24:39.000000 N/A

11780 3848 GoogleCrashHan 0x968fc63c6080 3 - 0 True 2021-03-21 00:24:40.000000 N/A

11792 3848 GoogleCrashHan 0x968fc63cc480 3 - 0 False 2021-03-21 00:24:40.000000 N/A

12152 1048 RuntimeBroker. 0x968fc4676080 1 - 1 False 2021-03-21 00:24:41.000000 N/A

12140 7896 SecurityHealth 0x968fc1fc72c0 1 - 1 False 2021-03-21 00:24:46.000000 N/A

11952 1008 SecurityHealth 0x968fc6433380 7 - 0 False 2021-03-21 00:24:46.000000 N/A

11828 7896 RtkAudUService 0x968fc6438080 7 - 1 False 2021-03-21 00:24:47.000000 N/A

12096 7896 WavesSvc64.exe 0x968fc6628080 4 - 1 False 2021-03-21 00:24:48.000000 N/A

5712 7896 DisplayLinkTra 0x968fc6625080 2 - 1 False 2021-03-21 00:24:48.000000 N/A

6104 7896 OneDrive.exe 0x968fc5915080 28 - 1 True 2021-03-21 00:24:50.000000 N/A

10700 7896 chrome.exe 0x968fc6724080 30 - 1 False 2021-03-21 00:24:53.000000 N/A

9716 10700 chrome.exe 0x968fc67f6380 7 - 1 False 2021-03-21 00:24:53.000000 N/A

5408 10700 chrome.exe 0x968fc6213080 16 - 1 False 2021-03-21 00:24:53.000000 N/A

9956 10700 chrome.exe 0x968fc6880080 12 - 1 False 2021-03-21 00:24:54.000000 N/A

12292 10700 chrome.exe 0x968fc68970c0 8 - 1 False 2021-03-21 00:24:54.000000 N/A

12440 10700 chrome.exe 0x968fc696f080 16 - 1 False 2021-03-21 00:24:54.000000 N/A

12460 10700 chrome.exe 0x968fc69ef080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

12468 10700 chrome.exe 0x968fc69e6080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

12508 10700 chrome.exe 0x968fc6a0d080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

12548 10700 chrome.exe 0x968fc6a07080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

12612 10700 chrome.exe 0x968fc6a21080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

12720 10700 chrome.exe 0x968fc6a22080 15 - 1 False 2021-03-21 00:24:54.000000 N/A

2380 1008 svchost.exe 0x968fc1ede080 2 - 0 False 2021-03-21 00:25:06.000000 N/A

11768 1048 SystemSettings 0x968fc5b61080 0 - 1 False 2021-03-21 00:25:20.000000 2021-03-21 00:25:37.000000

11372 1048 ApplicationFra 0x968fc6121080 2 - 1 False 2021-03-21 00:25:20.000000 N/A

11376 1008 svchost.exe 0x968fc56b9080 2 - 1 False 2021-03-21 00:25:21.000000 N/A

3488 1008 svchost.exe 0x968fc63af380 3 - 0 False 2021-03-21 00:25:21.000000 N/A

13796 10700 chrome.exe 0x968fc6a024c0 8 - 1 False 2021-03-21 00:25:40.000000 N/A

3236 1048 WinStore.App.e 0x968fc6ef1080 20 - 1 False 2021-03-21 00:25:41.000000 N/A

3552 1048 RuntimeBroker. 0x968fc730c0c0 3 - 1 False 2021-03-21 00:25:41.000000 N/A

4268 1008 svchost.exe 0x968fc5bdf380 0 - 0 False 2021-03-21 00:25:42.000000 2021-03-21 00:30:47.000000

6032 1008 svchost.exe 0x968fc78f8080 3 - 0 False 2021-03-21 00:25:43.000000 N/A

13216 11944 IAStorIcon.exe 0x968fc7b440c0 5 - 1 False 2021-03-21 00:25:47.000000 N/A

2936 1048 dllhost.exe 0x968fc71eb080 5 - 1 False 2021-03-21 00:26:11.000000 N/A

5252 1008 svchost.exe 0x968fc6f84080 6 - 1 False 2021-03-21 00:26:32.000000 N/A

12044 1008 svchost.exe 0x968fc7f56080 7 - 0 False 2021-03-21 00:26:33.000000 N/A

6116 1008 DDVRulesProces 0x968fc79fb080 6 - 0 False 2021-03-21 00:26:33.000000 N/A

12336 1008 Dell.D3.WinSvc 0x968fc1e222c0 118 - 0 False 2021-03-21 00:26:33.000000 N/A

13724 1008 ServiceShell.e 0x968fc7035080 52 - 0 False 2021-03-21 00:26:33.000000 N/A

13612 1008 dllhost.exe 0x968fc7bf8080 10 - 0 False 2021-03-21 00:26:34.000000 N/A

13172 1008 msdtc.exe 0x968fc7b70080 9 - 0 False 2021-03-21 00:26:34.000000 N/A

13144 1008 svchost.exe 0x968fc8054080 9 - 0 False 2021-03-21 00:26:36.000000 N/A

5260 1008 svchost.exe 0x968fc6f4b080 3 - 0 False 2021-03-21 00:26:36.000000 N/A

10416 1008 IAStorDataMgrS 0x968fc8055080 7 - 0 False 2021-03-21 00:26:36.000000 N/A

1764 1008 SgrmBroker.exe 0x968fc783f340 3 - 0 False 2021-03-21 00:26:36.000000 N/A

10568 1008 svchost.exe 0x968fc718a380 8 - 0 False 2021-03-21 00:26:37.000000 N/A

12424 1008 DDVDataCollect 0x968fc6fde3c0 7 - 0 False 2021-03-21 00:26:37.000000 N/A

4808 1008 DDVCollectorSv 0x968fc7f7b080 2 - 0 False 2021-03-21 00:26:37.000000 N/A

14448 8436 DellPoaEvents. 0x968fc88bf4c0 6 - 1 True 2021-03-21 00:26:49.000000 N/A

14572 1048 unsecapp.exe 0x968fc6430080 3 - 1 False 2021-03-21 00:26:50.000000 N/A

14884 12424 atiw.exe 0x968fc62d5480 3 - 1 False 2021-03-21 00:26:59.000000 N/A

4576 1008 svchost.exe 0x968fc7ad1080 0 - 0 False 2021-03-21 00:27:31.000000 2021-03-21 00:27:37.000000

13200 1008 svchost.exe 0x968fc80440c0 0 - 0 False 2021-03-21 00:28:14.000000 2021-03-21 00:29:07.000000

7276 1008 svchost.exe 0x968fc83230c0 0 - 0 False 2021-03-21 00:31:49.000000 2021-03-21 00:32:44.000000

1300 1048 CompPkgSrv.exe 0x968fc79f2080 1 - 1 False 2021-03-21 00:33:11.000000 N/A

9948 7896 rundll32.exe 0x968fc98dc2c0 1 - 1 False 2021-03-21 00:33:21.000000 N/A

14276 8188 VirtualBoxVM.e 0x968fca388080 0 - 1 False 2021-03-21 01:03:03.000000 2021-03-21 02:51:13.000000

288 1368 LogonUI.exe 0x968fc51a3080 0 - 1 False 2021-03-21 01:35:26.000000 2021-03-21 02:50:50.000000

9356 1368 LogonUI.exe 0x968fc9b41080 0 - 1 False 2021-03-21 02:51:38.000000 2021-03-21 03:12:34.000000

8372 1008 svchost.exe 0x968fc6e70080 0 - 0 False 2021-03-21 03:12:41.000000 2021-03-21 03:13:28.000000

8924 1008 svchost.exe 0x968fca955080 0 - 0 False 2021-03-21 03:21:21.000000 2021-03-21 03:22:59.000000

6296 1048 ShellExperienc 0x968fcc0840c0 18 - 1 False 2021-03-21 03:21:22.000000 N/A

6576 1048 RuntimeBroker. 0x968fca220080 3 - 1 False 2021-03-21 03:21:22.000000 N/A

1892 1048 FileCoAuth.exe 0x968fcbbcd4c0 2 - 1 True 2021-03-21 03:22:42.000000 N/A

8564 1368 LogonUI.exe 0x968fc25e2080 0 - 1 False 2021-03-21 03:54:22.000000 2021-03-26 21:25:13.000000

4348 1008 svchost.exe 0x968fca8e9480 3 - 0 False 2021-03-26 21:24:37.000000 N/A

9708 1008 svchost.exe 0x968fc54e5080 0 - 0 False 2021-03-26 21:24:38.000000 2021-03-26 21:26:17.000000

16768 1008 svchost.exe 0x968fcc4d4400 0 - 0 False 2021-03-26 21:24:43.000000 2021-03-26 21:29:47.000000

11304 1008 WUDFHost.exe 0x968fccd64080 10 - 0 False 2021-03-26 21:24:43.000000 N/A

18248 1008 tbtsvc.exe 0x968fcccdc080 3 - 0 True 2021-03-26 21:24:47.000000 N/A

8952 1008 WUDFHost.exe 0x968fcd415080 6 - 0 False 2021-03-26 21:24:47.000000 N/A

5852 17284 Thunderbolt.ex 0x968fcd43b080 8 - 1 True 2021-03-26 21:24:47.000000 N/A

3348 1048 unsecapp.exe 0x968fcd38a080 3 - 0 False 2021-03-26 21:24:47.000000 N/A

2680 10700 chrome.exe 0x968fd5a2e080 15 - 1 False 2021-03-26 21:24:54.000000 N/A

3984 1008 svchost.exe 0x968fbf173080 1 - 0 False 2021-03-26 21:25:25.000000 N/A

18732 10700 chrome.exe 0x968fbe6c14c0 15 - 1 False 2021-03-26 21:27:18.000000 N/A

11132 7896 SnippingTool.e 0x968fc7957080 12 - 1 False 2021-03-26 21:34:27.000000 N/A

18888 7896 EDD.exe 0x968fc7b24080 1 - 1 True 2021-03-26 21:37:34.000000 N/A

14912 18888 conhost.exe 0x968fc5307080 3 - 1 False 2021-03-26 21:37:34.000000 N/A

11212 10700 chrome.exe 0x968fc97ec080 16 - 1 False 2021-03-26 21:38:46.000000 N/A

3628 10700 chrome.exe 0x968fc462c080 17 - 1 False 2021-03-26 21:39:00.000000 N/A

9404 12424 atiw.exe 0x968fc60a0080 0 - 1 False 2021-03-26 21:39:38.000000 2021-03-26 21:39:39.000000

10368 12424 atiw.exe 0x968fc6f7c080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

13268 12424 atiw.exe 0x968fcd411080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

1192 12424 atiw.exe 0x968fcc0b9080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

7128 12424 atiw.exe 0x968fcadec080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

14664 12424 atiw.exe 0x968fcd3d9080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

8552 12424 atiw.exe 0x968fa8e570c0 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:39.000000

7796 12424 atiw.exe 0x968fc50e4080 0 - 1 False 2021-03-26 21:39:39.000000 2021-03-26 21:39:40.000000

8672 12424 atiw.exe 0x968fc94c9080 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

12068 12424 atiw.exe 0x968fc5894340 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

15908 12424 atiw.exe 0x968fc7b14300 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

7920 12424 atiw.exe 0x968fc5ab9080 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

9728 12424 atiw.exe 0x968fcbfd8300 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

9620 12424 atiw.exe 0x968fc2e522c0 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

14948 12424 atiw.exe 0x968fc5d9b2c0 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

13008 12424 atiw.exe 0x968fcd3cc080 0 - 1 False 2021-03-26 21:39:40.000000 2021-03-26 21:39:40.000000

4632 1008 svchost.exe 0x968fc7027080 20 - 0 False 2021-03-26 21:39:47.000000 N/A

10424 1048 WmiPrvSE.exe 0x968fd5a18380 5 - 0 False 2021-03-26 21:39:55.000000 N/A

18196 10700 chrome.exe 0x968fc71e5080 15 - 1 False 2021-03-26 21:39:58.000000 N/A

16840 10700 chrome.exe 0x968fbeb0f080 15 - 1 False 2021-03-26 21:41:03.000000 N/A

17560 7896 notepad.exe 0x968fcc287080 1 - 1 False 2021-03-26 21:41:39.000000 N/A

14964 7896 notepad.exe 0x968fc8158480 1 - 1 False 2021-03-26 21:42:30.000000 N/A

16344 7896 cmd.exe 0x968fc7ed8080 1 - 1 False 2021-03-26 21:45:24.000000 N/A

2988 16344 conhost.exe 0x968fca94a080 3 - 1 False 2021-03-26 21:45:24.000000 N/A

14108 7896 FTK Imager.exe 0x968fca281080 14 - 1 True 2021-03-26 21:50:13.000000 N/A

4296 1048 Microsoft.Phot 0x968fca8ee080 18 - 1 False 2021-03-26 21:57:19.000000 N/A

16236 1048 RuntimeBroker. 0x968fca3a5080 5 - 1 False 2021-03-26 21:57:20.000000 N/A

11724 1008 svchost.exe 0x968fc6b3f080 0 - 0 False 2021-03-26 22:09:44.000000 2021-03-26 22:14:44.000000

3404 1048 backgroundTask 0x968fccccf080 0 - 1 False 2021-03-26 22:12:33.000000 2021-03-26 22:13:42.000000

9452 1008 svchost.exe 0x968fc6f78080 4 - 0 False 2021-03-26 22:24:33.000000 N/A

13884 1048 WmiPrvSE.exe 0x968fc1f7c080 4 - 0 False 2021-03-26 22:24:37.000000 N/A

19012 1008 svchost.exe 0x968fcc4df080 2 - 0 False 2021-03-26 22:26:21.000000 N/A

15364 1008 svchost.exe 0x968fccda9080 0 - 0 False 2021-03-26 22:26:22.000000 2021-03-26 22:27:11.000000

15892 1008 svchost.exe 0x968fc6f25080 4 - 0 False 2021-03-26 22:38:48.000000 N/A

17264 1008 WmiApSrv.exe 0x968fc99d0080 8 - 0 False 2021-03-26 22:39:33.000000 N/A

Time Stamp: Fri Mar 26 23:08:24 2021

\*\*\*\*\*\*\* End of command output \*\*\*\*\*\*

Time Stamp: Fri Mar 26 23:10:27 2021

"C:\Users\rgrdo\Downloads\VolatilityWorkbench\vol.exe" -f "F:\DQ lab 4 take 2.mem" windows.cmdline.CmdLine

Volatility 3 Framework 1.1.0-beta.1

PID Process Args

4 System Required memory at 0x20 is not valid (process exited?)

144 Registry Required memory at 0x20 is not valid (process exited?)

716 smss.exe \SystemRoot\System32\smss.exe

804 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

936 wininit.exe wininit.exe

944 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

1008 services.exe C:\WINDOWS\system32\services.exe

104 lsass.exe C:\WINDOWS\system32\lsass.exe

120 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s PlugPlay

1048 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p

1072 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-adb738e5-a71a-467c-9e6c-03800134159a -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-9aeef1cc-71dc-475e-a140-ace8b2295f86 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-4792743e-e61d-405c-9abc-91b1e44b6b9f -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fabb32b6-0091-4b92-886a-3ce149e5d7a2 -LifetimeId:ce5437a4-d7d8-42d5-a6fa-f084bda5d75b -DeviceGroupId: -HostArg:0

1080 fontdrvhost.ex "fontdrvhost.exe"

1184 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-5b76eafd-cff0-4196-8dd9-5a10665db245 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-0a5e29b5-fe1b-42de-86cd-cfe38225f515 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-c307da21-8736-43d8-9320-a8c1c76159c6 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-ea135e00-d871-4745-9d08-33b68b64b3f3 -LifetimeId:0f2be83d-8ae5-4f22-b662-483ed31afbca -DeviceGroupId: -HostArg:0

1224 svchost.exe C:\WINDOWS\system32\svchost.exe -k RPCSS -p

1284 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM

1368 winlogon.exe winlogon.exe

1424 fontdrvhost.ex "fontdrvhost.exe"

1500 LogonUI.exe Required memory at 0xfb5dbc2020 is not valid (process exited?)

1508 dwm.exe "dwm.exe"

1588 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService

1596 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s BthAvctpSvc

1604 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s bthserv

1704 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService

1712 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc

1840 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DisplayEnhancementService

1860 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule

1868 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s hidserv

1988 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc

8 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s SmsRouter

932 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p

2096 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UserManager

2144 UshUpgradeServ "C:\WINDOWS\System32\UshUpgradeService.exe"

2232 atiesrxx.exe C:\WINDOWS\System32\DriverStore\FileRepository\u0330240.inf\_amd64\_dc7b29de95493557\B330101\atiesrxx.exe

2240 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog

2360 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc

2420 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService

2516 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s lfsvc

2524 dasHost.exe dashost.exe {6d027cae-d19f-4d04-89483e82e448ec73}

2568 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi

2604 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

2688 svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s NlaSvc

2744 svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache

2820 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalService -p -s netprofm

2888 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p

3040 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-8ae5b4c0-32c5-412a-a728-c448ed0a4c7d -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-e024e836-4292-4225-b436-6de6a60243ac -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-14cb6e74-0d53-47ce-bc69-96e7beaa55b4 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-52baf1d5-9622-4caf-baef-f7b89394e6e5 -LifetimeId:895eb7c4-a0c8-439b-bcf9-64c2ab617824 -DeviceGroupId:WudfDefaultDevicePoolPriorityHigh -HostArg:0

2476 svchost.exe Required memory at 0x41ab83d020 is not valid (process exited?)

3112 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-45c79de7-b898-4249-9969-6aff97d11607 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-6e73db4b-586f-4738-83b4-1ee9a2081405 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-c0ea9def-45cc-47a1-917a-1ff67cc81f23 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-5a46c468-ac2e-462b-8050-3ab52620267d -LifetimeId:ea560cd9-f3a6-4e80-976e-3b684c0a6fe9 -DeviceGroupId:WudfDefaultDevicePool -HostArg:0

3168 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain

3176 svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes

3184 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem

3192 atieclxx.exe atieclxx

3276 MemCompression Required memory at 0x20 is not valid (process exited?)

3324 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s SENS

3352 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -s CertPropSvc

3360 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -s SCardSvr

3408 igfxCUIService C:\WINDOWS\System32\DriverStore\FileRepository\cui\_dc\_comp.inf\_amd64\_82f69cea8b2d928f\igfxCUIService.exe

3460 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder

3468 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s FontCache

3560 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCtnrSvc

3744 sihost.exe sihost.exe

3788 svchost.exe C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc

3852 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc

3900 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p

3936 dasHost.exe dashost.exe {c650c79b-55be-4dcd-9a0ef9219cd1f164}

4020 svchost.exe C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService

3620 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s WwanSvc

4008 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p

4028 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p

4128 taskhostw.exe taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}

4260 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s TokenBroker

4420 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService

4524 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

4548 ctfmon.exe "ctfmon.exe"

4568 svchost.exe C:\WINDOWS\system32\svchost.exe -k appmodel -p -s StateRepository

4728 svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s ShellHWDetection

4824 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc

4940 spoolsv.exe C:\WINDOWS\System32\spoolsv.exe

5052 HostStorageSer "C:\WINDOWS\System32\HostStorageService.exe"

5064 HostControlSer "C:\WINDOWS\System32\HostControlService.exe"

4976 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Winmgmt

5132 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p

5212 svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s LanmanWorkstation

5564 AdminService.e C:\WINDOWS\System32\drivers\AdminService.exe

5580 svchost.exe C:\WINDOWS\System32\svchost.exe -k utcsvc -p

5592 esif\_uf.exe C:\WINDOWS\System32\Intel\DPTF\esif\_uf.exe

5648 svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s CryptSvc

5656 svchost.exe C:\WINDOWS\System32\svchost.exe -k NetSvcs -p -s iphlpsvc

5664 IntelCpHDCPSvc C:\WINDOWS\System32\DriverStore\FileRepository\iigd\_dc\_base.inf\_amd64\_5183d512e3aa272e\IntelCpHDCPSvc.exe

5672 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork -p -s DPS

5684 dpoMonitorSvc. "C:\Program Files\Dell\PPO\dpoMonitorSvc.exe"

5696 HidMonitorSvc. C:\WINDOWS\system32\DellTPad\HidMonitorSvc.exe

5704 LMS.exe "C:\WINDOWS\Intel\Intel(R) Management Engine Components\LMS\LMS.exe"

5720 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s fdPHost

5732 dpoTelemetrySv "C:\Program Files\Dell\PPO\Telemetry\dpoTelemetrySvc.exe"

5740 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s SstpSvc

5748 poaTaServ.exe "C:\Program Files\Dell\PPO\poaTaServ.exe"

5768 QcomWlanSrvx64 C:\WINDOWS\System32\drivers\QcomWlanSrvx64.exe

5780 poaSmSrv.exe "C:\Program Files\Dell\PPO\poaSmSrv.exe"

5788 svchost.exe C:\WINDOWS\system32\svchost.exe -k imgsvc

5804 poaService.exe "C:\Program Files\Dell\PPO\poaService.exe"

5816 RstMwService.e C:\WINDOWS\System32\DriverStore\FileRepository\iastorac.inf\_amd64\_d778d9f2df7418ce\RstMwService.exe

5828 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks

5844 SwiService.exe "C:\Program Files\Sierra Wireless Inc\Utils\SWIService.exe"

5860 WavesSysSvc64. C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo75de.inf\_amd64\_5ff36f834a6d461a\WavesSysSvc64.exe

5896 RtkAudUService "C:\WINDOWS\System32\RtkAudUService64.exe"

5908 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s WpnService

5920 MsMpEng.exe "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2102.4-0\MsMpEng.exe"

6096 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s LanmanServer

6396 jhi\_service.ex C:\WINDOWS\System32\jhi\_service.exe

6408 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalService -p -s WdiServiceHost

6596 svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs

6648 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s FDResPub

6868 IntelCpHeciSvc C:\WINDOWS\System32\DriverStore\FileRepository\iigd\_dc\_base.inf\_amd64\_5183d512e3aa272e\IntelCpHeciSvc.exe

7840 userinit.exe Required memory at 0x49425b8020 is not valid (process exited?)

7896 explorer.exe C:\WINDOWS\Explorer.EXE

8028 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s CDPSvc

1700 WmiPrvSE.exe C:\WINDOWS\system32\wbem\wmiprvse.exe

7564 svchost.exe C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc

8360 Apoint.exe "C:\WINDOWS\system32\DellTPad\Apoint.exe"

8652 svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s BITS

8716 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV

8724 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Appinfo

8832 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc

8856 ApMsgFwd.exe "C:\WINDOWS\system32\DellTPad\ApMsgFwd.exe" -s{05FA8492-C047-4207-BE65-780D8591C113}

8864 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc

9084 ApRemote.exe "C:\WINDOWS\system32\DellTPad\ApRemote.exe"

9108 hidfind.exe "C:\WINDOWS\system32\DellTPad\HidFind.exe"

9160 RadeonSettings "C:\Program Files\AMD\CNext\CNext\RadeonSettings.exe" atlogon

8404 NisSrv.exe "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2102.4-0\NisSrv.exe"

8492 ApntEx.exe "Apntex.exe"

4100 conhost.exe \??\C:\WINDOWS\system32\conhost.exe 0x4

9256 StartMenuExper "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost\_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca

9572 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalService -p -s LicenseManager

9612 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

9784 SearchUI.exe "C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca

9792 SearchIndexer. C:\WINDOWS\system32\SearchIndexer.exe /Embedding

10132 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

10052 RtkAudUService "C:\WINDOWS\System32\RtkAudUService64.exe" -admin

10356 unsecapp.exe C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding

10556 SettingSyncHos C:\WINDOWS\system32\SettingSyncHost.exe -Embedding

10948 LockApp.exe "C:\Windows\SystemApps\Microsoft.LockApp\_cw5n1h2txyewy\LockApp.exe" -ServerName:WindowsDefaultLockScreen.AppX7y4nbzq37zn4ks9k7amqjywdat7d3j2z.mca

11076 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

11232 RemindersServe "C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\RemindersServer.exe" -ServerName:RemindersServer

5504 YourPhone.exe "C:\Program Files\WindowsApps\Microsoft.YourPhone\_1.21022.139.0\_x64\_\_8wekyb3d8bbwe\YourPhone.exe" -ServerName:App.AppX9yct9q388jvt4h7y0gn06smzkxcsnt8m.mca

11456 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

11780 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.36.72\GoogleCrashHandler.exe"

11792 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.36.72\GoogleCrashHandler64.exe"

12152 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

12140 SecurityHealth "C:\Windows\System32\SecurityHealthSystray.exe"

11952 SecurityHealth C:\WINDOWS\system32\SecurityHealthService.exe

11828 RtkAudUService "C:\Windows\System32\RtkAudUService64.exe" -background

12096 WavesSvc64.exe "C:\Windows\System32\DriverStore\FileRepository\wavesapo75de.inf\_amd64\_5ff36f834a6d461a\WavesSvc64.exe" -Jack

5712 DisplayLinkTra "C:\Program Files\DisplayLink Core Software\DisplayLinkTrayApp.exe" -basicMode

6104 OneDrive.exe "C:\Users\rgrdo\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

10700 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --no-startup-window /prefetch:5

9716 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\rgrdo\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\rgrdo\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\rgrdo\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=89.0.4389.90 --initial-client-data=0xe8,0xec,0xf0,0xc4,0xf4,0x7ffa76704f50,0x7ffa76704f60,0x7ffa76704f70

5408 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --gpu-preferences=SAAAAAAAAADgAAAwAAAAAAAAAAAAAAAAAABgAAAAAAAoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB4AAAAAAAAAHgAAAAAAAAAKAAAAAQAAAAgAAAAAAAAACgAAAAAAAAAMAAAAAAAAAA4AAAAAAAAABAAAAAAAAAAAAAAAAUAAAAQAAAAAAAAAAAAAAAGAAAAEAAAAAAAAAABAAAABQAAABAAAAAAAAAAAQAAAAYAAAAIAAAAAAAAAAgAAAAAAAAA --mojo-platform-channel-handle=1680 /prefetch:2

9956 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --service-sandbox-type=network --mojo-platform-channel-handle=1988 /prefetch:8

12292 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --service-sandbox-type=utility --mojo-platform-channel-handle=2328 /prefetch:8

12440 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=5 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3036 /prefetch:1

12460 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=6 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3500 /prefetch:1

12468 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=7 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3784 /prefetch:1

12508 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=8 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3772 /prefetch:1

12548 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=9 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3732 /prefetch:1

12612 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=11 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=4256 /prefetch:1

12720 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=12 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=3840 /prefetch:1

2380 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s Netman

11768 SystemSettings Required memory at 0x5df0f6020 is not valid (process exited?)

11372 ApplicationFra C:\WINDOWS\system32\ApplicationFrameHost.exe -Embedding

11376 svchost.exe C:\WINDOWS\system32\svchost.exe -k DevicesFlow -s DevicesFlowUserSvc

3488 svchost.exe C:\WINDOWS\system32\svchost.exe -k WbioSvcGroup -s WbioSrvc

13796 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=3156 /prefetch:8

3236 WinStore.App.e "C:\Program Files\WindowsApps\Microsoft.WindowsStore\_12011.1001.1.0\_x64\_\_8wekyb3d8bbwe\WinStore.App.exe" -ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca

3552 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

4268 svchost.exe Required memory at 0xa2e5c2f020 is not valid (process exited?)

6032 svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs -p

13216 IAStorIcon.exe "C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe"

2936 dllhost.exe C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}

5252 svchost.exe C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup

12044 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc

6116 DDVRulesProces "C:\Program Files\Dell\DellDataVault\DDVRulesProcessor.exe"

12336 Dell.D3.WinSvc "C:\Program Files (x86)\Dell Digital Delivery Services\Dell.D3.WinSvc.exe"

13724 ServiceShell.e "C:\Program Files (x86)\Dell\UpdateService\ServiceShell.exe"

13612 dllhost.exe C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}

13172 msdtc.exe C:\WINDOWS\System32\msdtc.exe

13144 svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s DoSvc

5260 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc

10416 IAStorDataMgrS "C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe"

1764 SgrmBroker.exe C:\WINDOWS\system32\SgrmBroker.exe

10568 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UsoSvc

12424 DDVDataCollect "C:\Program Files\Dell\DellDataVault\DDVDataCollector.exe"

4808 DDVCollectorSv "C:\Program Files\Dell\DellDataVault\DDVCollectorSvcApi.exe"

14448 DellPoaEvents. "C:\Program Files\Dell\PPO\DellPoaEvents\DellPoaEvents.exe"

14572 unsecapp.exe C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding

14884 atiw.exe "C:\Program Files\Dell\DellDataVault\atiw.exe" -p 1 -continuous

4576 svchost.exe Required memory at 0x7adcc75020 is not valid (process exited?)

13200 svchost.exe Required memory at 0xdfbcc99020 is not valid (process exited?)

7276 svchost.exe Required memory at 0x95b6f2d020 is not valid (process exited?)

1300 CompPkgSrv.exe C:\Windows\System32\CompPkgSrv.exe -Embedding

9948 rundll32.exe "C:\WINDOWS\system32\rundll32.exe" -localserver 22d8c27b-47a1-48d1-ad08-7da7abd79617

14276 VirtualBoxVM.e Required memory at 0xd8b020 is not valid (process exited?)

288 LogonUI.exe Required memory at 0xdba26a7020 is not valid (process exited?)

9356 LogonUI.exe Required memory at 0xfb04125020 is not valid (process exited?)

8372 svchost.exe Required memory at 0x3cfdaa2020 is not valid (process exited?)

8924 svchost.exe Required memory at 0x7efa75e020 is not valid (process exited?)

6296 ShellExperienc "C:\Windows\SystemApps\ShellExperienceHost\_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca

6576 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

1892 FileCoAuth.exe "C:\Users\rgrdo\AppData\Local\Microsoft\OneDrive\21.030.0211.0002\FileCoAuth.exe" -Embedding

8564 LogonUI.exe Required memory at 0x5dd0ed7020 is not valid (process exited?)

4348 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts

9708 svchost.exe Required memory at 0x44b1fa1020 is not valid (process exited?)

16768 svchost.exe Required memory at 0xcb786cc020 is not valid (process exited?)

11304 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-21f85b5b-5e8d-46af-821f-13cea10c00b3 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-14b7fa9a-a98a-44cc-be81-84a6e48e383a -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-d139ae74-fac9-4a52-9d39-e4c02cc2523d -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-800a3c82-dc10-4120-b116-052a6e3c70b8 -LifetimeId:ece4ef6f-66e1-4c66-a7f1-5c0c43d9ac07 -DeviceGroupId: -HostArg:0

18248 tbtsvc.exe "C:\Program Files (x86)\Intel\Thunderbolt Software\tbtsvc.exe"

8952 WUDFHost.exe "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-4577e332-1759-459c-a1ad-ec3cfeda92e2 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-55762eb7-7e79-46dc-b0b8-3b9be3a70928 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-de3163de-39ba-4778-a6a8-a9481ea28888 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-a8272099-9861-4ae0-913f-812277913f74 -LifetimeId:6febfb2e-6cd5-4866-9a53-57eeb47c674b -DeviceGroupId:WpdFsGroup -HostArg:0

5852 Thunderbolt.ex Thunderbolt.exe CONDITIONALLY\_STARTED SILENT

3348 unsecapp.exe C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding

2680 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --extension-process --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=200 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=4924 /prefetch:1

3984 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s PhoneSvc

18732 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=224 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=5140 /prefetch:1

11132 SnippingTool.e "C:\WINDOWS\system32\SnippingTool.exe"

18888 EDD.exe "C:\Users\rgrdo\Desktop\EDD.exe"

14912 conhost.exe \??\C:\WINDOWS\system32\conhost.exe 0x4

11212 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=238 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=7476 /prefetch:1

3628 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=246 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=6916 /prefetch:1

9404 atiw.exe Required memory at 0xd094fde020 is not valid (process exited?)

10368 atiw.exe Required memory at 0x52ee2db020 is not valid (process exited?)

13268 atiw.exe Required memory at 0x4e12808020 is not valid (process exited?)

1192 atiw.exe Required memory at 0x2999f32020 is not valid (process exited?)

7128 atiw.exe Required memory at 0x2305ae4020 is not valid (process exited?)

14664 atiw.exe Required memory at 0xf523ab4020 is not valid (process exited?)

8552 atiw.exe Required memory at 0xfcfd8df020 is not valid (process exited?)

7796 atiw.exe Required memory at 0xba3f940020 is not valid (process exited?)

8672 atiw.exe Required memory at 0x8ee61ac020 is not valid (process exited?)

12068 atiw.exe Required memory at 0x12a8c52020 is not valid (process exited?)

15908 atiw.exe Required memory at 0xc368ef0020 is not valid (process exited?)

7920 atiw.exe Required memory at 0x70769d1020 is not valid (process exited?)

9728 atiw.exe Required memory at 0xf18f603020 is not valid (process exited?)

9620 atiw.exe Required memory at 0x3f57a84020 is not valid (process exited?)

14948 atiw.exe Required memory at 0x57a7513020 is not valid (process exited?)

13008 atiw.exe Required memory at 0xd155833020 is not valid (process exited?)

4632 svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s TapiSrv

10424 WmiPrvSE.exe C:\WINDOWS\system32\wbem\wmiprvse.exe

18196 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=249 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=6952 /prefetch:1

16840 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1644,17741171101667519690,17340551837078391470,131072 --lang=en-US --origin-trial-disabled-features=SecurePaymentConfirmation --device-scale-factor=1.25 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=251 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=9884 /prefetch:1

17560 notepad.exe "C:\WINDOWS\system32\notepad.exe"

14964 notepad.exe "C:\WINDOWS\system32\notepad.exe"

16344 cmd.exe "C:\WINDOWS\system32\cmd.exe"

2988 conhost.exe \??\C:\WINDOWS\system32\conhost.exe 0x4

14108 FTK Imager.exe "D:\AccessDataFTK\FTK Imager\FTK Imager.exe"

4296 Microsoft.Phot Required memory at 0x200149b768c8 is not valid (incomplete layer memory\_layer?)

16236 RuntimeBroker. C:\Windows\System32\RuntimeBroker.exe -Embedding

11724 svchost.exe Required memory at 0xdda4cb020 is not valid (process exited?)

3404 backgroundTask Required memory at 0xeaec0a9020 is not valid (process exited?)

9452 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s DsSvc

13884 WmiPrvSE.exe C:\WINDOWS\system32\wbem\wmiprvse.exe

19012 svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost

15364 svchost.exe Required memory at 0xa0cdbdf020 is not valid (process exited?)

15892 svchost.exe C:\WINDOWS\system32\svchost.exe -k appmodel -p -s camsvc

17264 WmiApSrv.exe Required memory at 0x9024948b48 is not valid (process exited?)

Time Stamp: Fri Mar 26 23:12:16 2021

\*\*\*\*\*\*\* End of command output \*\*\*\*\*\*

Time Stamp: Fri Mar 26 23:13:40 2021

"C:\Users\rgrdo\Downloads\VolatilityWorkbench\vol.exe" -f "F:\DQ lab 4 take 2.mem" windows.cmdline.CmdLine --pid 16344

Volatility 3 Framework 1.1.0-beta.1

PID Process Args

16344 cmd.exe "C:\WINDOWS\system32\cmd.exe"

Time Stamp: Fri Mar 26 23:15:28 2021

\*\*\*\*\*\*\* End of command output \*\*\*\*\*\*

Time Stamp: Fri Mar 26 23:19:22 2021

"C:\Users\rgrdo\Downloads\VolatilityWorkbench\vol.exe" -f "F:\DQ lab 4 take 2.mem" windows.filescan.FileScan

Volatility 3 Framework 1.1.0-beta.1

Offset Name

Traceback (most recent call last):

File "vol.py", line 10, in <module>

File "volatility\cli\\_\_init\_\_.py", line 508, in main

File "volatility\cli\\_\_init\_\_.py", line 306, in run

File "volatility\cli\text\_renderer.py", line 179, in render

File "volatility\framework\renderers\\_\_init\_\_.py", line 215, in populate

File "volatility\cli\text\_renderer.py", line 174, in visitor

File "d:\python\python38-32\lib\encodings\cp1252.py", line 19, in encode

UnicodeEncodeError: 'charmap' codec can't encode characters in position 15-17: character maps to <undefined>

[32320] Failed to execute script vol

Time Stamp: Fri Mar 26 23:23:24 2021

\*\*\*\*\*\*\* End of command output \*\*\*\*\*\*