Task 2-A Step 4:

Volatility Foundation Volatility Framework 2.6

Name Pid PPid Thds Hnds Time

-------------------------------------------------- ------ ------ ------ ------ ----

0xfffffa8003cdd040:System 4 0 93 632 2015-10-12 03:56:54 UTC+0000

. 0xfffffa80051df9d0:smss.exe 300 4 2 29 2015-10-12 03:56:54 UTC+0000

.. 0xfffffa8006014710:smss.exe 676 300 0 ------ 2015-10-12 03:56:57 UTC+0000

... 0xfffffa8003db4140:csrss.exe 696 676 11 634 2015-10-12 03:56:57 UTC+0000

.... 0xfffffa80049ebb10:conhost.exe 3240 696 1 34 2015-10-12 03:57:25 UTC+0000

.... 0xfffffa800646c060:conhost.exe 3504 696 2 51 2015-10-12 11:36:03 UTC+0000

... 0xfffffa8005d5c8f0:winlogon.exe 744 676 3 114 2015-10-12 03:56:57 UTC+0000

.... 0xfffffa80067ccb10:userinit.exe 1452 744 0 ------ 2015-10-12 03:57:02 UTC+0000

..... 0xfffffa80067f3060:explorer.exe 2056 1452 32 996 2015-10-12 03:57:02 UTC+0000

...... 0xfffffa8004632060:wordpad.exe 4740 2056 4 140 2015-10-12 11:35:41 UTC+0000

...... 0xfffffa8006939b10:chrome.exe 3564 2056 31 765 2015-10-12 11:34:25 UTC+0000

....... 0xfffffa80067e2060:chrome.exe 3120 3564 8 167 2015-10-12 11:34:38 UTC+0000

....... 0xfffffa8004639060:chrome.exe 4316 3564 5 166 2015-10-12 11:34:26 UTC+0000

...... 0xfffffa8006b26b10:iexplore.exe 768 2056 16 542 2015-10-12 11:34:42 UTC+0000

....... 0xfffffa80068cb060:iexplore.exe 4352 768 53 879 2015-10-12 11:34:43 UTC+0000

....... 0xfffffa8006c6e060:iexplore.exe 3684 768 31 711 2015-10-12 11:35:03 UTC+0000

...... 0xfffffa8006960360:runonce.exe 2424 2056 0 ------ 2015-10-12 03:57:04 UTC+0000

....... 0xfffffa8006972b10:avgui.exe 2472 2424 23 562 2015-10-12 03:57:04 UTC+0000

........ 0xfffffa8004f35060:ctfmon.exe 2956 2472 2 86 2015-10-12 03:57:07 UTC+0000

....... 0xfffffa800696db10:jusched.exe 2508 2424 5 322 2015-10-12 03:57:04 UTC+0000

....... 0xfffffa8006967b10:avguix.exe 2492 2424 23 352 2015-10-12 03:57:04 UTC+0000

....... 0xfffffa80069719e0:vprot.exe 2500 2424 36 564 2015-10-12 03:57:04 UTC+0000

........ 0xfffffa8004995b10:avgcefrend.exe 3272 2500 10 187 2015-10-12 03:57:12 UTC+0000

...... 0xfffffa8006fb5270:FTK Imager.exe 3460 2056 14 375 2015-10-12 11:41:01 UTC+0000

...... 0xfffffa80069dab10:AcroRd32.exe 4368 2056 10 213 2015-10-12 11:05:26 UTC+0000

....... 0xfffffa80042a1b10:AcroRd32.exe 3780 4368 7 318 2015-10-12 11:05:26 UTC+0000

...... 0xfffffa8006956b10:vmtoolsd.exe 2416 2056 6 276 2015-10-12 03:57:04 UTC+0000

...... 0xfffffa800691eb10:cmd.exe 3320 2056 1 24 2015-10-12 11:36:03 UTC+0000

Task 2-A Step 8:

Volatility Foundation Volatility Framework 2.6

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CommandProcess: conhost.exe Pid: 3240

CommandHistory: 0xa2350 Application: TPAutoConnect.exe Flags: Allocated

CommandCount: 0 LastAdded: -1 LastDisplayed: -1

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CommandProcess: conhost.exe Pid: 3504

CommandHistory: 0x2f21a0 Application: cmd.exe Flags: Allocated, Reset

CommandCount: 15 LastAdded: 14 LastDisplayed: 14

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 @ 0x2f0cd0: cd\

Cmd #1 @ 0x2e7810: cd "Program Files (x86)"

Cmd #2 @ 0x2e57e0: cd mandiant

Cmd #3 @ 0x2f0b10: dir

Cmd #4 @ 0x2e5800: cd Memoryze

Cmd #5 @ 0x2f6540: dir

Cmd #6 @ 0x2f6590: f:

Cmd #7 @ 0x2f65a0: cls

Cmd #8 @ 0x2e5820: cd x64

Cmd #9 @ 0x2f65b0: dir

Cmd #10 @ 0x2e7850: memorydd.bat -output E:\

Cmd #11 @ 0x2f65c0: dir

Cmd #12 @ 0x2f1a00: memorydd.bat -o E:\

Cmd #13 @ 0x2e7890: memorydd.bat -output F:\

Cmd #14 @ 0x2f1a30: memorydd.bat -o F:\