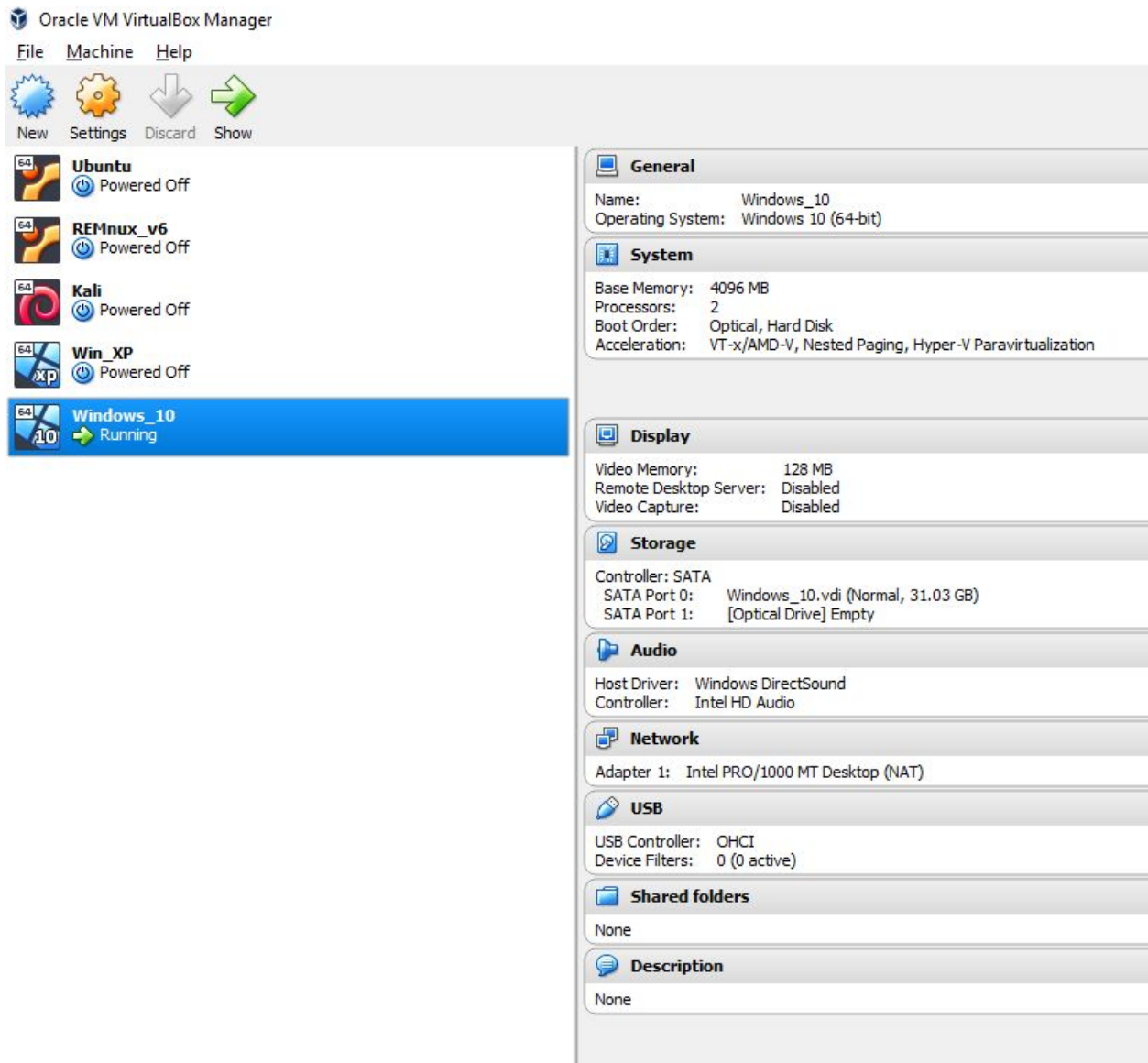
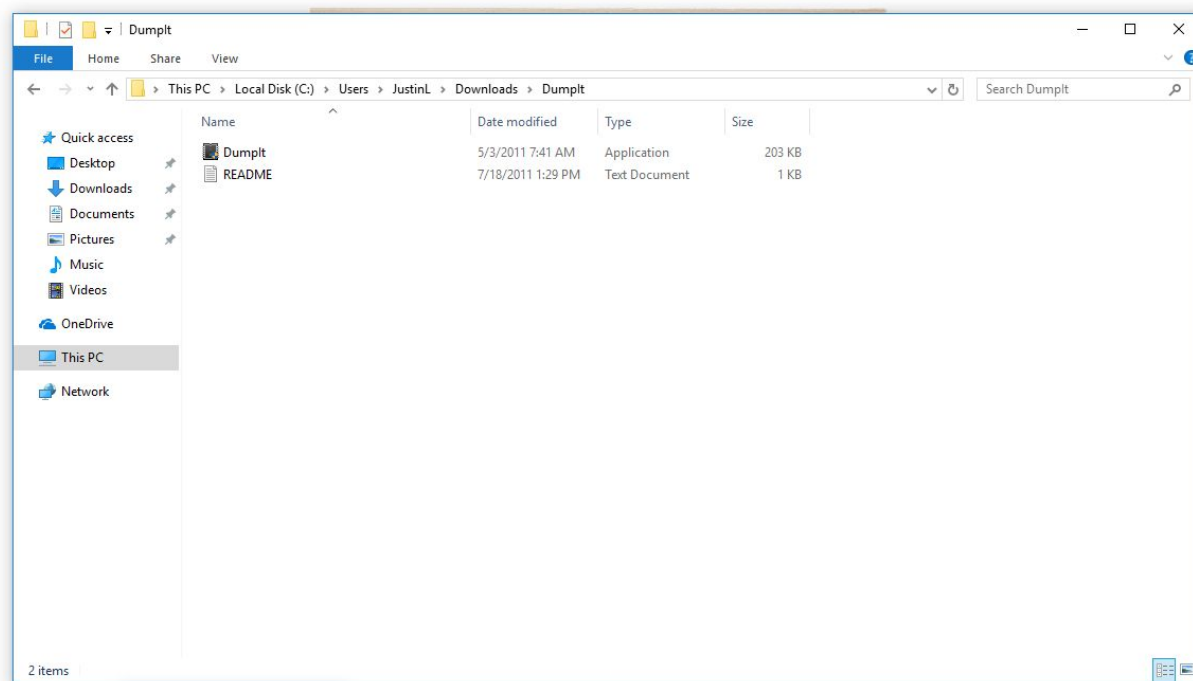


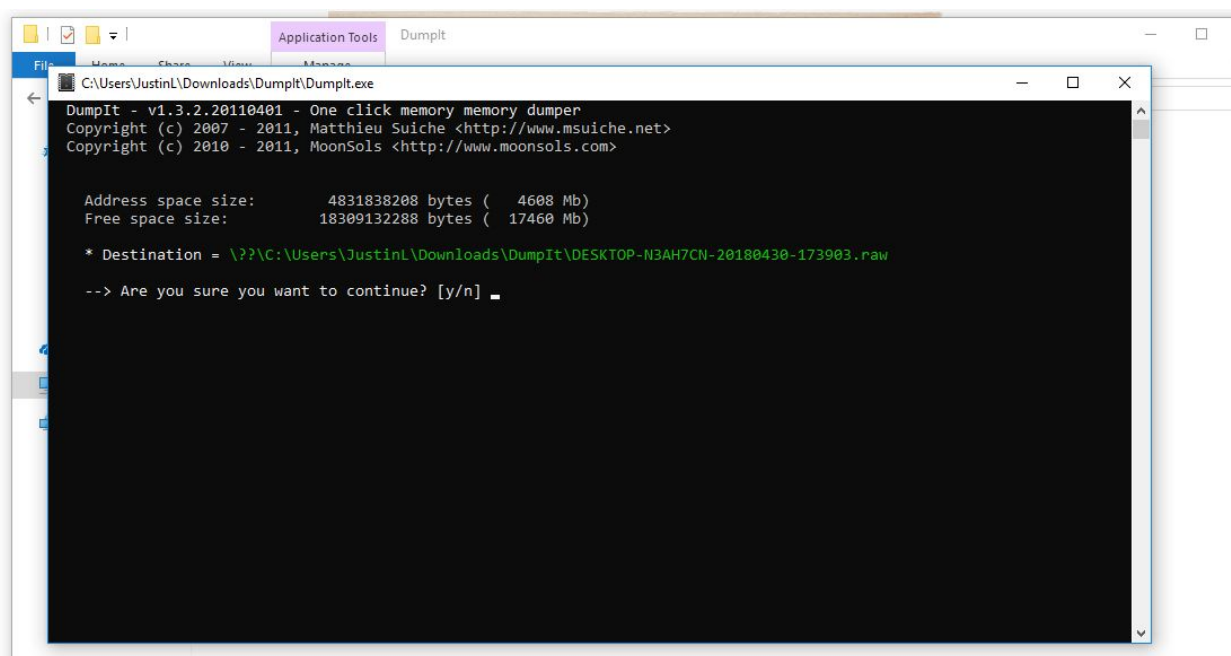
I am using a Windows 10 virtual machine for this assignment.

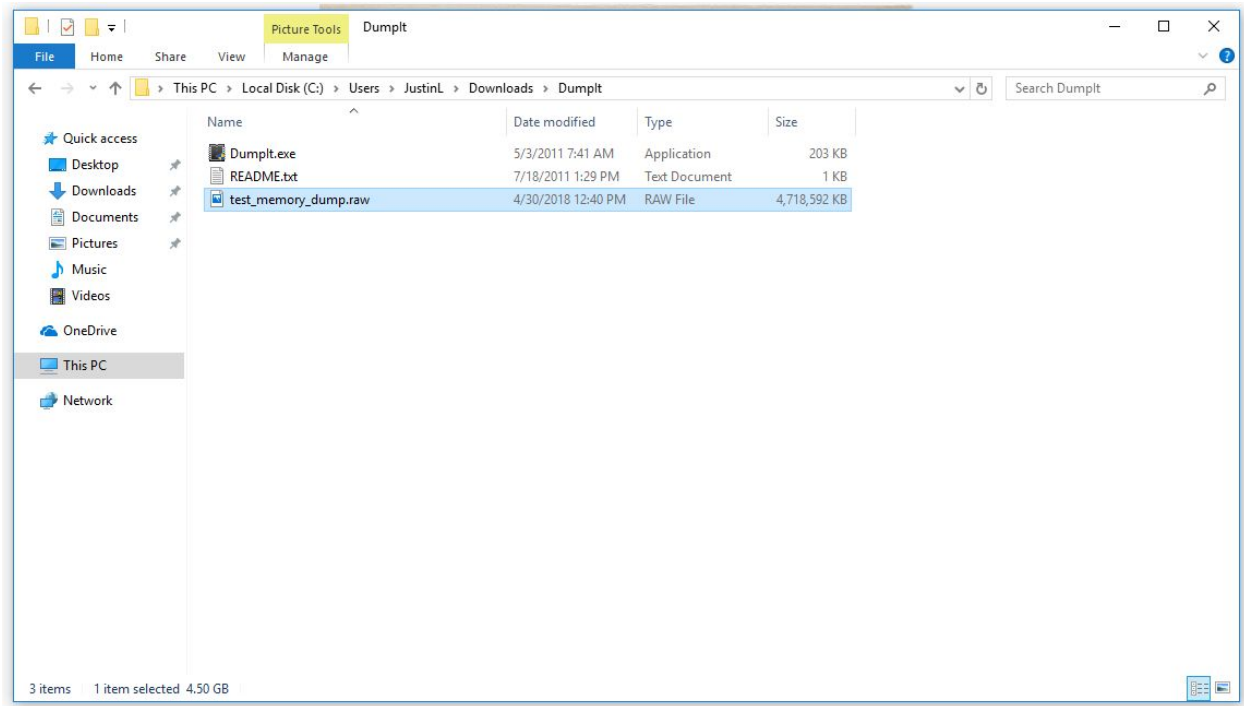


The first thing I did was download DumpIt for memory analysis on the VM.



I then did a test of *DumpIt* to make sure it was working correctly.





I decided to download the win-rootkit because I am on a Windows VM.

https://github.com/varshapaidi/Kernel_Rootkit

<https://github.com/karol-gruszczek/win-rootkit>

<https://github.com/hanj4096/wukong>

No description, website, or topics provided.

13 commits2 branches0 releases1 contributor

Branch: masterNew pull requestFind fileClone or download

karol-gruszczek Update README.mdLatest commit 4f3f546 on Feb 21, 2016

src	Fixed .gitmodules	2 years ago
vs-project	Added dll injection	2 years ago
.gitignore	added visual studio project	2 years ago
.gitmodules	Fixed .gitmodules	2 years ago
Makefile	Updated makefile	2 years ago
README.md	Update README.md	2 years ago

README.md

Windows rootkit

Rootkit for hiding processes and files, designed for windows platform

Requirements

- g++
- make

Setup

I had to download MinGW so that I could have the G++ compiler and *make* on my Windows VM. Then I compiled using *make*.

```
Command Prompt
Microsoft Windows [Version 10.0.16299.371]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\JustinL>cd Downloads

C:\Users\JustinL\Downloads>cd win-rootkit

C:\Users\JustinL\Downloads\win-rootkit>make
g++ -Wall --std=c++11 -static-libgcc -static-libstdc++ -c src/main.cpp -o src/main.o
g++ -Wall --std=c++11 -static-libgcc -static-libstdc++ -c src/dll_injector.cpp -o src/dll_injector.o
g++ -Wall --std=c++11 -static-libgcc -static-libstdc++ src/main.o src/dll_injector.o -o rootkit.exe -Wl,-subsystem,windows
g++ -Wall --std=c++11 -static-libgcc -static-libstdc++ src/test.cpp -o test.exe
g++ -Wall --std=c++11 -c src/dllmain.cpp -o src/dllmain.o -DBUILDING_EXAMPLE_DLL
g++ -Wall --std=c++11 -c src/hook.cpp -o src/hook.o -DBUILDING_EXAMPLE_DLL
g++ -Wall --std=c++11 src/dllmain.o src/hook.o -shared -o win-rootkit.dll

C:\Users\JustinL\Downloads\win-rootkit>dir
Volume in drive C has no label.
Volume Serial Number is 7691-FA48

Directory of C:\Users\JustinL\Downloads\win-rootkit

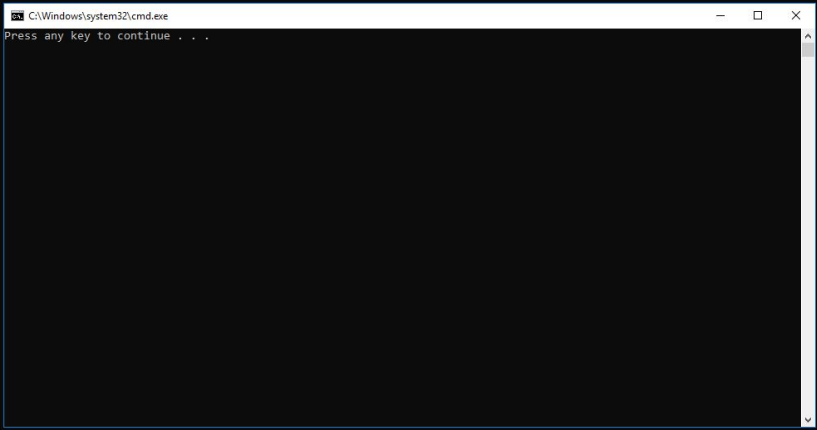
04/30/2018  01:38 PM  <DIR>          .
04/30/2018  01:38 PM  <DIR>          ..
04/30/2018  01:25 PM                313 .gitignore
04/30/2018  01:25 PM                82 .gitmodules
04/30/2018  01:25 PM             1,129 Makefile
04/30/2018  01:25 PM                272 README.md
04/30/2018  01:38 PM       2,358,195 rootkit.exe
04/30/2018  01:38 PM  <DIR>          src
04/30/2018  01:38 PM       2,138,767 test.exe
04/30/2018  01:26 PM  <DIR>          vs-project
04/30/2018  01:25 PM  <DIR>          win-rootkit-master
04/30/2018  01:38 PM       30,959 win-rootkit.dll
               7 File(s)      4,529,717 bytes
               5 Dir(s)    10,843,336,704 bytes free

C:\Users\JustinL\Downloads\win-rootkit>
```

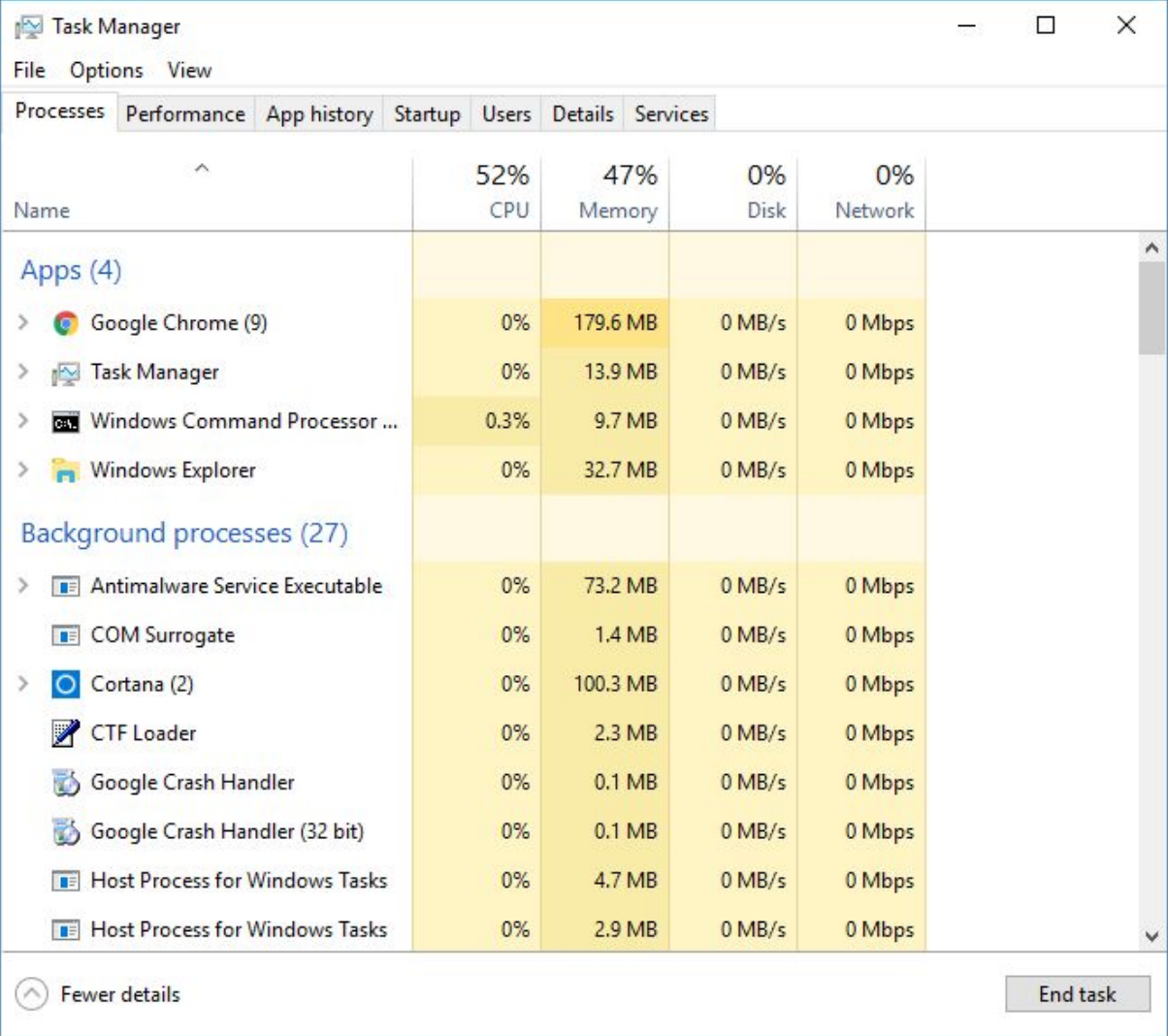
You will notice that the *rootkit.exe* executable was generated, along with *test.exe*.

I executed *rootkit.exe* and received the following:

```
C:\Users\JustinL\Downloads\win-rootkit>rootkit.exe
C:\Users\JustinL\Downloads\win-rootkit>
```



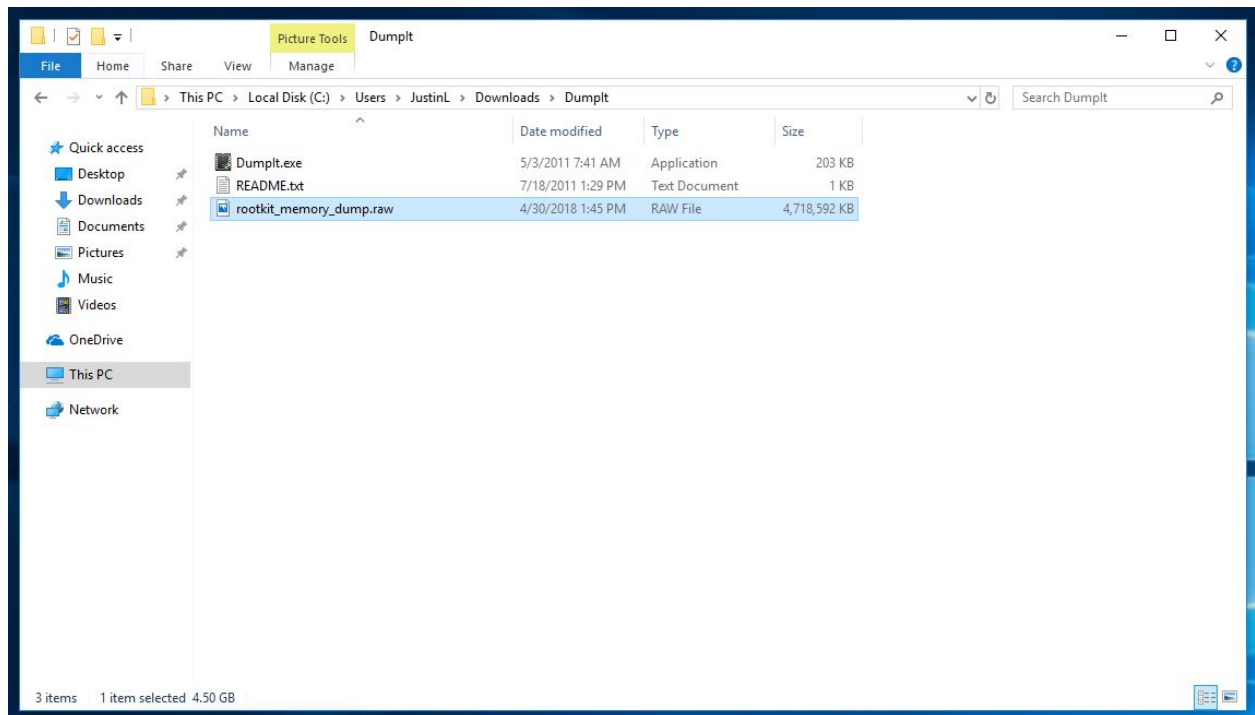
I noticed that the CPU usage was high (using Task Manager).



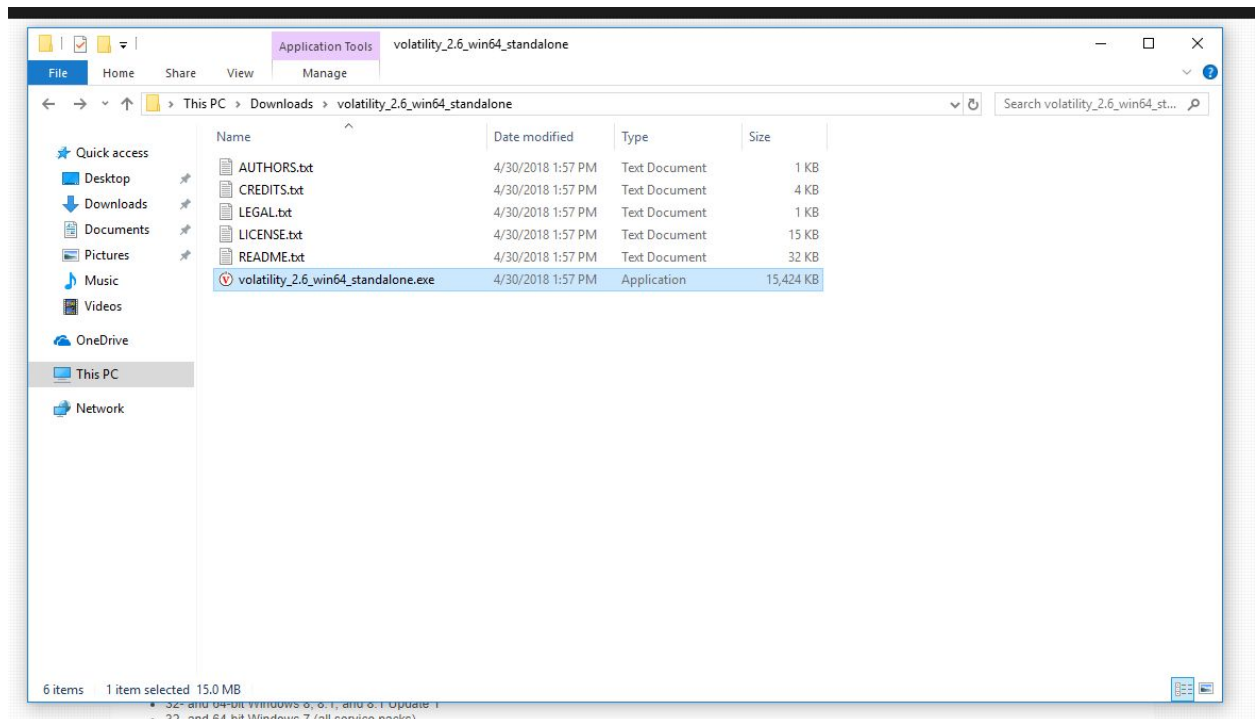
The screenshot shows the Windows Task Manager application with the 'Performance' tab selected. The 'CPU' section is highlighted, showing a usage of 52%. Below this, a table lists running processes categorized into 'Apps (4)' and 'Background processes (27)'. The table columns are Name, CPU, Memory, Disk, and Network. Google Chrome (9) is the highest memory consumer at 179.6 MB. Task Manager itself uses 13.9 MB. Windows Explorer uses 32.7 MB. Among background processes, Cortana (2) uses 100.3 MB, and Antimalware Service Executable uses 73.2 MB. The bottom of the window shows a 'Fewer details' button and an 'End task' button.

Name	CPU	Memory	Disk	Network
Apps (4)				
> Google Chrome (9)	0%	179.6 MB	0 MB/s	0 Mbps
> Task Manager	0%	13.9 MB	0 MB/s	0 Mbps
> Windows Command Processor ...	0.3%	9.7 MB	0 MB/s	0 Mbps
> Windows Explorer	0%	32.7 MB	0 MB/s	0 Mbps
Background processes (27)				
> Antimalware Service Executable	0%	73.2 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.4 MB	0 MB/s	0 Mbps
> Cortana (2)	0%	100.3 MB	0 MB/s	0 Mbps
CTF Loader	0%	2.3 MB	0 MB/s	0 Mbps
Google Crash Handler	0%	0.1 MB	0 MB/s	0 Mbps
Google Crash Handler (32 bit)	0%	0.1 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	4.7 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	2.9 MB	0 MB/s	0 Mbps

Next, I performed a memory dump using *Dumplt*.



I downloaded the Volatility Framework to perform the next step of the assignment, which is to analyze the memory dump from *Dumplt*.



I first utilized the *imageinfo* flag with *volatility*.

I ran the *pslist* on the rootkit memory dump. The results are below. You will notice that the process names have been omitted and the reason is still unknown.

```
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>volatility.exe -f rootkit_memory_dump.raw --profile=Win10x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)      Name      PID      PPID      Thds      Hnds      Sess      Wow64      Start      Exit
-----
0xffffffff302abec8338      4      0 28...4      0 -----      0 -
0xffffffff302ad685578     312      0 29...2      0 -----      0 -
0xffffffff302ad5df578     408      0 29...2      0 -----      0 -
0xffffffff302aee59078     472      0 29...0      0 -----      0 -
0xffffffff302ad8e0078     480     252 29...6      0 -----      0 -
0xffffffff302ad5cd138     496      0 29...8      0 -----      0 -
0xffffffff302aee86078     572     344 29...0      0 -----      0 -
0xffffffff302ad97a078     592      0 29...0      0 -----      0 -
0xffffffff302aef9578     624      0 29...4      0 -----      0 -
0xffffffff302aee7278     720      0 29...2      0 -----      0 -
0xffffffff302aef1078     744     216 29...0      0 -----      0 -
0xffffffff302aef6078     752     132 29...6      0 -----      0 -
0xffffffff302aee9c578     764     300 29...8      0 -----      0 -
0xffffffff302aef4a338     848      0 29...8      0 -----      0 -
0xffffffff302aef6a578     900     272 29...8      0 -----      0 -
0xffffffff302aef75578        60     252 29...2      0 -----      0 -
0xffffffff302aef4578     348     252 29...6      0 -----      0 -
0xffffffff302aef7578     360     256 29...4      0 -----      0 -
0xffffffff302af29c578     540     252 29...4      0 -----      0 -
0xffffffff302af2942b8    1000     252 29...8      0 -----      0 -
0xffffffff302af262578    1056     148 29...6      0 -----      0 -
0xffffffff302af2b5578    1072     264 29...2      0 -----      0 -
0xffffffff302af2f7578    1168     252 29...2      0 -----      0 -
0xffffffff302af2f9578    1176     256 29...8      0 -----      0 -
0xffffffff302af2fd578    1200     260 29...8      0 -----      0 -
0xffffffff302af306578    1208     252 29...8      0 -----      0 -
0xffffffff302af30c578    1280     264 29...4      0 -----      0 -
0xffffffff302af391038    1364        0 29...8      0 -----      0 -
0xffffffff302af3c4578    1380     260 29...2      0 -----      0 -
0xffffffff302af591578    1440     260 29...8      0 -----      0 -
0xffffffff302af5c5578    1460     252 29...0      0 -----      0 -
0xffffffff302af5a6578    1468     252 29...4      0 -----      0 -
0xffffffff302af5d3578    1524     240 29...4      0 -----      0 -
0xffffffff302af5f0578    1536     204 29...0      0 -----      0 -
0xffffffff302af687578    1716     252 29...2      0 -----      0 -
0xffffffff302af6f3578    1880     252 29...6      0 -----      0 -
0xffffffff302af6ff338    1920     268 29...8      0 -----      0 -
0xffffffff302af760578    1996     252 29...6      0 -----      0 -
0xffffffff302af742578    1136     252 29...4      0 -----      0 -
0xffffffff302af775578    1532     252 29...4      0 -----      0 -
0xffffffff302af7b0578    2084     252 29...0      0 -----      0 -
0xffffffff302af816578    2224     252 29...2      0 -----      0 -
0xffffffff302af7fd578    2232     136 29...6      0 -----      0 -
```

The *psscan* was executed next.

```
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>volatility.exe -f rootkit_memory_dump.raw --profile=Win10x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Name          PID  PPID  PDB          Time created          Time exited
-----
0x0000ab80000c8340      29...4      0 0x00000000001aa000 2018-04-30 17:53:13 UTC+0000
0x0000ab80000de580 pu?svchost. 28...8 592 0x0000000051950000 2018-04-30 17:53:25 UTC+0000
0x0000ab80000f1080 ?s?svchost. 28...0 592 0x0000000051c50000 2018-04-30 17:53:25 UTC+0000
0x0000ab80000f8080 ???svchost. 28...2 592 0x0000000051c00000 2018-04-30 17:53:25 UTC+0000
0x0000ab80000fa080 ???svchost. 29...4 592 0x0000000051e40000 2018-04-30 17:53:25 UTC+0000
0x0000ab8000105080 ?Sc?svchost. 28...8 592 0x0000000051b10000 2018-04-30 17:53:25 UTC+0000
0x0000ab800013d080 ?G?chrome.e 29...4 1416 0x00000000ae700000 2018-04-30 18:06:21 UTC+0000
0x0000bc0e0651b1be 85...7 71...5 0x0000020c1f00020
0x0000bc0e0655b216 o 32...3 18...8 0xc1d8ffffff00000
0x0000bc0e0af6b1be 0 41...4 0x5180ffffff00000
0x0000e302abec8340      29...4      0 0x00000000001aa000 2018-04-30 17:53:13 UTC+0000
0x0000e302abede580 pu?svchost. 28...8 592 0x0000000051950000 2018-04-30 17:53:25 UTC+0000
0x0000e302abef1080 ?s?svchost. 28...0 592 0x0000000051c50000 2018-04-30 17:53:25 UTC+0000
0x0000e302abef8080 ???svchost. 28...2 592 0x0000000051c00000 2018-04-30 17:53:25 UTC+0000
0x0000e302abefa080 ???svchost. 29...4 592 0x0000000051e40000 2018-04-30 17:53:25 UTC+0000
0x0000e302abf05080 ?Sc?svchost. 28...8 592 0x0000000051b10000 2018-04-30 17:53:25 UTC+0000
0x0000e302abfd3080 ?G?chrome.e 29...4 1416 0x00000000ae700000 2018-04-30 18:06:21 UTC+0000
0x0000e302ac0b4580 ?svchost. 29...6 592 0x0000000069f10000 2018-04-30 17:53:27 UTC+0000
0x0000e302ac526080 ^?svchost. 29...2 5760 0x0000000045a00000 2018-04-30 18:43:51 UTC+0000
0x0000e302ac586580 ^s?TiWorker 29...4 764 0x00000000ce600000 2018-04-30 18:22:43 UTC+0000
0x0000e302ac588580 ?svchost. 28...8 592 0x000000009bb00000 2018-04-30 18:22:43 UTC+0000
0x0000e302ac6f7580 ?cmd.exe 29...8 4292 0x0000000083800000 2018-04-30 18:38:33 UTC+0000
0x0000e302acf46080 P^M?chrome.e 29...2 1416 0x0000000057d00000 2018-04-30 18:40:30 UTC+0000
0x0000e302acff5580      29...4      592 0x00000000b9500000 2018-04-30 17:55:39 UTC+0000
0x0000e302ad2fd080 ???chrome.e 29...0 1416 0x0000000016f00000 2018-04-30 18:05:28 UTC+0000
0x0000e302ad42d580 ???chrome.e 29...6 1416 0x00000000c6e00000 2018-04-30 18:05:19 UTC+0000
0x0000e302ad5cd140 @R?csrss.ex 29...4 472 0x0000000023600000 2018-04-30 17:53:22 UTC+0000
0x0000e302ad5df580 ???csrss.ex 29...4 400 0x0000000020d00000 2018-04-30 17:53:22 UTC+0000
0x0000e302ad5e4080 ^Z?svchost. 29...8 592 0x00000000b5a00000 2018-04-30 18:33:59 UTC+0000
0x0000e302ad685580 ?h?smss.exe 29...8 4 0x00000000102100000 2018-04-30 17:53:13 UTC+0000
0x0000e302ad739580 ?k?chrome.e 29...2 1416 0x000000005ee00000 2018-04-30 18:06:23 UTC+0000
0x0000e302ad79a580 p?chrome.e 29...8 1416 0x000000004f900000 2018-04-30 18:05:19 UTC+0000
0x0000e302ad8e0080 ???wininit. 29...2 400 0x000000001f100000 2018-04-30 17:53:22 UTC+0000
0x0000e302ad97a080 ?services 29...0 480 0x000000001bb00000 2018-04-30 17:53:22 UTC+0000
0x0000e302ad97e580 ?w?services 29...4 592 0x00000000b5f00000 2018-04-30 17:55:38 UTC+0000
0x0000e302ae388580 ?chrome.e 28...4 1416 0x000000004da00000 2018-04-30 18:06:21 UTC+0000
0x0000e302ae716580 ?RuntimeB 29...8 764 0x0000000010a800000 2018-04-30 18:12:54 UTC+0000
0x0000e302ae82b580 ?RuntimeB 29...8 764 0x00000000b7900000 2018-04-30 18:12:57 UTC+0000
0x0000e302ae870080 ^D?RuntimeB 28...0 764 0x000000007bb00000 2018-04-30 18:17:19 UTC+0000
0x0000e302ae890580 %?SkypeHos 29...6 764 0x0000000007500000 2018-04-30 18:17:18 UTC+0000
0x0000e302ae8e0580 0???svchost. 28...2 592 0x00000000c5401000 2018-04-30 18:38:32 UTC+0000
0x0000e302ae908580 ?dllhost. 29...2 764 0x0000000050300000 2018-04-30 18:12:56 UTC+0000
0x0000e302ae930580 @???svchost. 29...8 592 0x0000000043c00000 2018-04-30 18:35:06 UTC+0000
0x0000e302ae9de580 ^H?svchost. 29...0 592 0x00000000a4b00000 2018-04-30 18:05:10 UTC+0000
0x0000e302aeaf9580 ?lsass.ex 29...2 480 0x0000000022200000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee59080      29...2      312 0x0000000020a00000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee80580 @N?svchost. 29...4 592 0x0000000052210000 2018-04-30 17:53:25 UTC+0000
0x0000e302aee86080 <n?winlogon 29...6 472 0x000000001c200000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee9c580 ???svchost. 29...4 592 0x000000001ee00000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee7280 PU?svchost. 29...6 592 0x0000000021800000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee1080 ???fontdrvh 29...6 572 0x0000000020e00000 2018-04-30 17:53:22 UTC+0000
0x0000e302aee6080 ?fontdrvh 29...6 480 0x0000000021000000 2018-04-30 17:53:22 UTC+0000
```

This time, the names of the processes are displayed. The rootkit is supposed to hide certain processes, although which process is hidden is not given from the Github page. Some of the processes here don't have names. For example, process ID '0' and '592' are nameless, along with '4', '572', and '764'. Review the image below to see the other nameless processes.

0x0000e302af3394c0	???	28...4	1990	0x0000000000000000	2018-04-30	18:43:50	UTC+0000
0x0000e302af391040		29...6	4	0x00000000040110000	2018-04-30	17:53:23	UTC+0000
0x0000e302af3c4580	???	29...2	592	0x00000000040030000	2018-04-30	17:53:23	UTC+0000
0x0000e302af41b080	p??	29...8	764	0x00000000086700000	2018-04-30	18:29:56	UTC+0000
0x0000e302af4a6580	???	29...8	2732	0x00000000047800000	2018-04-30	18:44:04	UTC+0000
0x0000e302af591580	???	29...4	592	0x00000000040200000	2018-04-30	17:53:24	UTC+0000
0x0000e302af5a6580	???	29...8	592	0x00000000040a50000	2018-04-30	17:53:24	UTC+0000
0x0000e302af5c5580	0??	29...8	592	0x00000000040a10000	2018-04-30	17:53:24	UTC+0000
0x0000e302af5d3580	0??	29...2	592	0x00000000041010000	2018-04-30	17:53:24	UTC+0000
0x0000e302af5f0580	@??	29...8	592	0x00000000041110000	2018-04-30	17:53:24	UTC+0000
0x0000e302af687580	???	29...6	592	0x00000000042800000	2018-04-30	17:53:24	UTC+0000
0x0000e302af6f3580	xm??	29...2	592	0x00000000044b20000	2018-04-30	17:53:24	UTC+0000
0x0000e302af6ff340	???	29...0	592	0x00000000045300000	2018-04-30	17:53:24	UTC+0000
0x0000e302af742580	p??	29...6	592	0x00000000048300000	2018-04-30	17:53:24	UTC+0000
0x0000e302af7b0580	???	29...0	592	0x00000000047720000	2018-04-30	17:53:24	UTC+0000
0x0000e302af775580	0??	29...0	592	0x00000000048820000	2018-04-30	17:53:24	UTC+0000
0x0000e302af79b080	???	29...4	592	0x0000000008bb00000	2018-04-30	18:03:38	UTC+0000
0x0000e302af8d5580	???	29...2	592	0x0000000004b100000	2018-04-30	17:53:24	UTC+0000
0x0000e302af7fd580	???	29...0	592	0x0000000004c720000	2018-04-30	17:53:25	UTC+0000
0x0000e302af816580	???	29...2	592	0x0000000004c700000	2018-04-30	17:53:25	UTC+0000
0x0000e302af819580	???	29...4	592	0x0000000004c900000	2018-04-30	17:53:25	UTC+0000
0x0000e302af85e580	???	28...4	592	0x0000000004d910000	2018-04-30	17:53:25	UTC+0000
0x0000e302af8bd580	???	29...8	592	0x00000000023700000	2018-04-30	17:53:25	UTC+0000
0x0000e302af8d5580	???	29...0	592	0x00000000052760000	2018-04-30	17:53:25	UTC+0000
0x0000e302af931580	???	29...8	592	0x00000000054410000	2018-04-30	17:53:25	UTC+0000
0x0000e302af961580	???	28...4	592	0x00000000055300000	2018-04-30	17:53:25	UTC+0000
0x0000e302afa5f580	???	29...4	1880	0x00000000093600000	2018-04-30	17:53:48	UTC+0000
0x0000e302afa68580	???	29...2	592	0x00000000079800000	2018-04-30	17:53:36	UTC+0000
0x0000e302afb3d580	???	29...4	592	0x000000000cc900000	2018-04-30	17:59:25	UTC+0000
0x0000e302afc28580	???	29...0	592	0x00000000092100000	2018-04-30	17:53:48	UTC+0000
0x0000e302afc48340	???	29...2	592	0x0000000007f400000	2018-04-30	17:53:48	UTC+0000
0x0000e302afc4e580	???	29...8	592	0x00000000022d00000	2018-04-30	17:53:48	UTC+0000
0x0000e302afc7c580	???	29...6	1468	0x00000000021f00000	2018-04-30	17:53:48	UTC+0000
0x0000e302afc98580	???	29...4	592	0x00000000020000000	2018-04-30	17:53:48	UTC+0000
0x0000e302afce1080	p??	29...8	592	0x0000000001d700000	2018-04-30	17:53:48	UTC+0000
0x0000e302afd0f380	???	29...2	4104	0x00000000093300000	2018-04-30	17:53:48	UTC+0000
0x0000e302afd4e340	???	29...4	572	0x0000000004f500000	2018-04-30	17:53:48	UTC+0000
0x0000e302afd71080	???	29...0	1416	0x00000000076f00000	2018-04-30	18:05:19	UTC+0000
0x0000e302afd77580	p??	29...6	4248	0x00000000068500000	2018-04-30	17:53:48	UTC+0000
0x0000e302afdc4580	P??	29...6	592	0x00000000084700000	2018-04-30	17:53:49	UTC+0000
0x0000e302afeb1580	???	29...8	592	0x0000000009d640000	2018-04-30	17:53:50	UTC+0000
0x0000e302afef0580	???	29...8	592	0x00000000097000000	2018-04-30	17:53:50	UTC+0000
0x0000e302aff91580	???	29...6	4292	0x0000000006a300000	2018-04-30	18:41:32	UTC+0000
0x0000e302affc2080	???	29...4	4292	0x00000000106900000	2018-04-30	18:05:19	UTC+0000
0x0000e302b0070580	???	29...0	592	0x00000000100e00000	2018-04-30	17:55:38	UTC+0000
0x0000e302b0091580	0??	29...4	764	0x000000000b2400000	2018-04-30	17:53:56	UTC+0000
0x0000e302b00ce580	I??	29...2	1468	0x000000000a4f00000	2018-04-30	18:04:40	UTC+0000
0x0000e302b00d7080	???	29...2	4292	0x000000000d7000000	2018-04-30	17:54:08	UTC+0000
0x0000e302b010a340	@??	29...4	4024	0x00000000087e00000	2018-04-30	18:38:33	UTC+0000
0x0000e302b0216580	???	29...6	4292	0x000000000bec00000	2018-04-30	17:54:08	UTC+0000
0x0000e302b0290580	???	29...2	764	0x000000000a6800000	2018-04-30	17:53:57	UTC+0000
0x0000e302b02d9580	???	29...0	764	0x0000000005c000000	2018-04-30	18:12:53	UTC+0000
0x0000e302b0343500	???	29...6	572	0x00000000034100000	2018-04-30	18:05:13	UTC+0000
0x0000e302b049d3c0	???	29...8	3948	0x000000000ab200000	2018-04-30	17:54:00	UTC+0000

Process '572' looks very suspicious from the above analysis. It is shown to have three different names.

I did also execute *files*can and *handles* with volatility but I was unable to get results.

```
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>volatility.exe -f rootkit_memory_dump.raw --profile=Win10x64 filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)      #Ptr    #Hnd Access Name
-----
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>volatility.exe -f rootkit_memory_dump.raw --profile=Win10x64 handles
Volatility Foundation Volatility Framework 2.6
Offset(V)      Pid      Handle      Access Type      Details
-----
C:\Users\JustinL\Downloads\volatility_2.6_win64_standalone>
```