# ENPM687 – Digital Forensics and Incidence Responses

# Assignment – 2

*Author – Syed Mohammad Ibrahim*

*UMD ID:* *iamibi*

*UID: 118428369*

*Email:* [*iamibi@umd.edu*](mailto:iamibi@umd.edu)

1. What was going on at the time the memory dump was taken? (What programs appeared to be running at the time the image was taken and what do you suspect about what was happening.)

A. The following programs were running when the memory dump was taken

|  |
| --- |
| $ ./volatility\_2.6\_win64\_standalone.exe -f Homework/hw2.mem --profile=Win7SP1x64 psscan  Volatility Foundation Volatility Framework 2.6  Offset(P) Name PID PPID PDB Time created Time exited  ------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------  0x000000007d6751d0 GoogleCrashHan 2564 2484 0x0000000064ba2000 2017-06-19 19:39:43 UTC+0000  0x000000007d675700 GoogleCrashHan 2556 2484 0x000000005f01a000 2017-06-19 19:39:43 UTC+0000  0x000000007d6d0b30 TPAutoConnect. 2916 1852 0x0000000061963000 2017-06-19 19:39:49 UTC+0000  0x000000007d6d3060 conhost.exe 2924 404 0x00000000618aa000 2017-06-19 19:39:49 UTC+0000  0x000000007d6fa270 WmiPrvSE.exe 3012 620 0x000000005ab51000 2017-06-19 19:39:57 UTC+0000  0x000000007d8e77c0 WmiPrvSE.exe 1704 620 0x00000000761cf000 2017-06-19 19:39:37 UTC+0000  0x000000007d8f0060 FTK Imager.exe 3368 2148 0x0000000034f2a000 2017-06-19 19:42:30 UTC+0000  0x000000007d9d3060 vmtoolsd.exe 2300 2148 0x0000000072936000 2017-06-19 19:39:41 UTC+0000  0x000000007d9f0b30 SearchIndexer. 2712 488 0x00000000658dd000 2017-06-19 19:39:47 UTC+0000  0x000000007da28a30 svchost.exe 524 488 0x00000000127b9000 2017-06-19 19:39:33 UTC+0000  0x000000007da35b30 svchost.exe 1068 488 0x0000000006608000 2017-06-19 19:39:34 UTC+0000  0x000000007daa0480 spoolsv.exe 1160 488 0x0000000007757000 2017-06-19 19:39:34 UTC+0000  0x000000007dae0b30 svchost.exe 1196 488 0x000000000ed3b000 2017-06-19 19:39:35 UTC+0000  0x000000007db3b800 ManagementAgen 1428 488 0x000000000d5fa000 2017-06-19 19:39:35 UTC+0000  0x000000007db5d1d0 svchost.exe 860 488 0x0000000042173000 2017-06-19 19:41:09 UTC+0000  0x000000007db8c990 VGAuthService. 1372 488 0x000000000cfad000 2017-06-19 19:39:35 UTC+0000  0x000000007dbc8a60 vmtoolsd.exe 1400 488 0x000000000d573000 2017-06-19 19:39:35 UTC+0000  0x000000007dc07060 SearchFilterHo 3804 2712 0x0000000000d67000 2017-06-19 19:42:47 UTC+0000  0x000000007dc23060 taskeng.exe 2112 932 0x000000006f2de000 2017-06-19 19:39:40 UTC+0000  0x000000007dc38340 dllhost.exe 1956 488 0x000000007aaea000 2017-06-19 19:39:39 UTC+0000  0x000000007dc42910 vmacthlp.exe 688 488 0x000000000e104000 2017-06-19 19:39:32 UTC+0000  0x000000007dc5f890 svchost.exe 720 488 0x000000000e70e000 2017-06-19 19:39:32 UTC+0000  0x000000007dc9bb30 svchost.exe 772 488 0x000000000ea95000 2017-06-19 19:39:32 UTC+0000  0x000000007dc9f060 dwm.exe 2136 880 0x000000007542c000 2017-06-19 19:39:40 UTC+0000  0x000000007dccbb30 svchost.exe 3544 488 0x0000000054556000 2017-06-19 19:41:37 UTC+0000  0x000000007dd0a340 msdtc.exe 1248 488 0x000000007b7f3000 2017-06-19 19:39:39 UTC+0000  0x000000007dd2cb30 svchost.exe 880 488 0x0000000012b65000 2017-06-19 19:39:33 UTC+0000  0x000000007dd3a360 explorer.exe 2148 2124 0x000000006ebdd000 2017-06-19 19:39:40 UTC+0000  0x000000007dd70b30 svchost.exe 932 488 0x000000001276c000 2017-06-19 19:39:33 UTC+0000  0x000000007dd9db30 audiodg.exe 992 772 0x00000000133f7000 2017-06-19 19:39:33 UTC+0000  0x000000007de05b30 lsass.exe 496 392 0x0000000010eda000 2017-06-19 19:39:32 UTC+0000  0x000000007de0ab30 lsm.exe 504 392 0x0000000016a22000 2017-06-19 19:39:32 UTC+0000  0x000000007dfbc060 TPAutoConnSvc. 1852 488 0x000000007639c000 2017-06-19 19:39:39 UTC+0000  0x000000007dfc4060 svchost.exe 1824 488 0x0000000075095000 2017-06-19 19:39:39 UTC+0000  0x000000007dfddb30 svchost.exe 620 488 0x000000000e103000 2017-06-19 19:39:32 UTC+0000  0x000000007e07cb30 wininit.exe 392 332 0x000000001138c000 2017-06-19 19:39:31 UTC+0000  0x000000007e0fc220 csrss.exe 404 384 0x0000000011f54000 2017-06-19 19:39:31 UTC+0000  0x000000007e16db30 taskhost.exe 2060 488 0x0000000071f8b000 2017-06-19 19:39:40 UTC+0000  0x000000007e195830 winlogon.exe 452 384 0x000000001199a000 2017-06-19 19:39:31 UTC+0000  0x000000007e19fb30 services.exe 488 392 0x0000000017fb9000 2017-06-19 19:39:32 UTC+0000  0x000000007e3b7060 csrss.exe 340 332 0x0000000011446000 2017-06-19 19:39:31 UTC+0000  0x000000007ea0d7e0 smss.exe 260 4 0x00000000201b3000 2017-06-19 19:39:30 UTC+0000  0x000000007efa1b30 SearchProtocol 2844 2712 0x0000000062ca9000 2017-06-19 19:39:47 UTC+0000  0x000000007f300060 obiwan.exe 3624 2148 0x0000000009921000 2017-06-19 19:42:38 UTC+0000  0x000000007f301b30 chrome.exe 1652 2148 0x0000000045eaf000 2017-06-19 19:41:09 UTC+0000 2017-06-19 19:41:31 UTC+0000  0x000000007fb35b30 conhost.exe 3596 404 0x000000006b19c000 2017-06-19 19:42:38 UTC+0000  0x000000007fdbc340 obiwan.exe 3292 3624 0x0000000064715000 2017-06-19 19:42:38 UTC+0000  0x000000007fe81720 WmiApSrv.exe 2976 488 0x0000000001707000 2017-06-19 19:42:01 UTC+0000  0x000000007feda680 sppsvc.exe 3452 488 0x000000005090f000 2017-06-19 19:41:37 UTC+0000  0x000000007ff6d9e0 System 4 0 0x0000000000187000 2017-06-19 19:39:30 UTC+0000 |

The above processes suggest that the user was browsing internet on chrome browser. There was another unknown service running called obiwan.exe.

2. Can you extract the malware for further analysis? What command(s) did you run? What commands did you try that were not successful and what did those commands output?

A. Yes, I was able to identify the malware process called obiwan.exe and the malware was successfully extracted using the command.

|  |
| --- |
| $ ./volatility\_2.6\_win64\_standalone.exe -f Homework/hw2.mem --profile=Win7SP1x64 dumpfiles -r obiwan.exe --name obiwan.exe --dump-dir=Homework/.  Volatility Foundation Volatility Framework 2.6  ImageSectionObject 0xfffffa8003c27070 3624 \Device\HarddiskVolume1\Users\ENPM687\Documents\obiwan.exe  DataSectionObject 0xfffffa8003c27070 3624 \Device\HarddiskVolume1\Users\ENPM687\Documents\obiwan.exe |

However, in the process of getting to this point of extraction I had executed few other commands which were unsuccessful like:

* “./volatility\_2.6\_win64\_standalone.exe -f Homework/hw2.mem --profile=Win7SP1x64 dumpfiles -Q 0xfffffa8002500060 –name obiwan.exe –dump-dir=Homework/” This command was executed in the hopes of extracting the malware from the memory offset.

3. What’s the malware file name?

A. obiwan.exe

4. What’s is the MD5 hash for it (It’s not real malware, I promise.)

A. be72a4c90c4bee65742eebf556f040f3 \*Homework/file.3624.0xfffffa80040f9c80.obiwan.exe.img

5. Write a short description of what plugins you used and what you found interesting from a forensic analysis perspective(including the answers to the 4 questions above).

A. I used the imageinfo, psscan, pstree, dumpfiles, netscan plugins as part of my analysis.

- imageinfo – used for identifying the signature of the memory and potentially the operating system architecture

- psscan – for all the running processes at the time of memory snapshot along with terminated processes

- pstree – for identifying a parent and child process of malware

- dumfiles – for dumping the malicious binary from memory

- netscan – To get the network calls going in and out of the system. A snapshot is provided below. Helped in identifying Command-and-Control Server of the malicious file.

|  |
| --- |
| $ ./volatility\_2.6\_win64\_standalone.exe -f Homework/hw2.mem --profile=Win7SP1x64 netscan  Volatility Foundation Volatility Framework 2.6  Offset(P) Proto Local Address Foreign Address State Pid Owner Created  0x7d618ec0 UDPv4 0.0.0.0:0 \*:\* 1068 svchost.exe 2017-06-19 19:39:43 UTC+0000  0x7d618ec0 UDPv6 :::0 \*:\* 1068 svchost.exe 2017-06-19 19:39:43 UTC+0000  0x7d67bec0 UDPv4 0.0.0.0:5355 \*:\* 1068 svchost.exe 2017-06-19 19:39:43 UTC+0000  0x7d67bec0 UDPv6 :::5355 \*:\* 1068 svchost.exe 2017-06-19 19:39:43 UTC+0000  0x7d818860 UDPv4 192.168.2.132:137 \*:\* 4 System 2017-06-19 19:39:36 UTC+0000  0x7d81dec0 UDPv4 192.168.2.132:138 \*:\* 4 System 2017-06-19 19:39:36 UTC+0000  0x7d642910 TCPv4 0.0.0.0:49156 0.0.0.0:0 LISTENING 496 lsass.exe  0x7d642910 TCPv6 :::49156 :::0 LISTENING 496 lsass.exe  0x7d642b80 TCPv4 0.0.0.0:49156 0.0.0.0:0 LISTENING 496 lsass.exe  0x7d814680 TCPv4 192.168.2.132:139 0.0.0.0:0 LISTENING 4 System  0x7d854e70 TCPv4 0.0.0.0:49155 0.0.0.0:0 LISTENING 488 services.exe  0x7d854e70 TCPv6 :::49155 :::0 LISTENING 488 services.exe  0x7d85c860 TCPv4 0.0.0.0:49155 0.0.0.0:0 LISTENING 488 services.exe  0x7d85def0 TCPv4 0.0.0.0:445 0.0.0.0:0 LISTENING 4 System  0x7d85def0 TCPv6 :::445 :::0 LISTENING 4 System  0x7da3d850 UDPv4 0.0.0.0:5355 \*:\* 1068 svchost.exe 2017-06-19 19:39:43 UTC+0000  0x7da8fad0 TCPv4 0.0.0.0:49154 0.0.0.0:0 LISTENING 932 svchost.exe  0x7da8fad0 TCPv6 :::49154 :::0 LISTENING 932 svchost.exe  0x7da90ef0 TCPv4 0.0.0.0:49154 0.0.0.0:0 LISTENING 932 svchost.exe  0x7dc7cdc0 TCPv4 0.0.0.0:135 0.0.0.0:0 LISTENING 720 svchost.exe  0x7dc7cdc0 TCPv6 :::135 :::0 LISTENING 720 svchost.exe  0x7dc7ead0 TCPv4 0.0.0.0:135 0.0.0.0:0 LISTENING 720 svchost.exe  0x7dc9d9f0 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 392 wininit.exe  0x7dca0830 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENING 392 wininit.exe  0x7dca0830 TCPv6 :::49152 :::0 LISTENING 392 wininit.exe  0x7dd34ce0 TCPv4 0.0.0.0:49153 0.0.0.0:0 LISTENING 772 svchost.exe  0x7dd35ad0 TCPv4 0.0.0.0:49153 0.0.0.0:0 LISTENING 772 svchost.exe  0x7dd35ad0 TCPv6 :::49153 :::0 LISTENING 772 svchost.exe  0x7dc9acf0 TCPv6 -:0 98f8:a503:80fa:ffff:98f8:a503:80fa:ffff:0 CLOSED 1 @?\☻????  0x7dd52c30 TCPv4 -:0 56.187.169.3:0 CLOSED 1 @?\☻????  0x7e1e8cf0 TCPv4 192.168.2.132:49321 54.230.19.247:443 CLOSE\_WAIT 3292 obiwan.exe  0x7ebabac0 UDPv6 fe80::cde2:40e2:3528:dd69:1900 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fa01d00 UDPv4 127.0.0.1:1900 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fa052f0 UDPv4 192.168.2.132:1900 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fa05ec0 UDPv6 ::1:1900 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fa74a80 UDPv6 ::1:52537 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fcceec0 UDPv4 127.0.0.1:52538 \*:\* 860 svchost.exe 2017-06-19 19:41:37 UTC+0000  0x7fa41680 TCPv4 -:0 56.11.183.3:0 CLOSED 1652 chrome.exe  0x7fa47010 TCPv4 192.168.2.132:49318 54.230.19.105:443 CLOSED 3292 obiwan.exe  0x7fa55cf0 TCPv6 -:0 380b:b703:80fa:ffff:380b:b703:80fa:ffff:0 CLOSED 1652 chrome.exe  0x7fa658b0 TCPv4 192.168.2.132:49290 23.13.165.231:80 ESTABLISHED 1068 svchost.exe  0x7fa852e0 TCPv4 192.168.2.132:49308 54.230.19.32:443 CLOSE\_WAIT 3292 obiwan.exe  0x7fc779f0 TCPv4 192.168.2.132:49289 72.21.91.29:80 ESTABLISHED 1068 svchost.exe  0x7fcd8cf0 TCPv4 -:49161 172.217.8.3:443 CLOSED 1652 chrome.exe  0x7fdb6010 TCPv4 -:49160 172.217.8.13:443 CLOSED 1652 chrome.exe  0x7fdd9ca0 TCPv4 -:49165 172.217.8.3:443 CLOSED 1652 chrome.exe |