# ENPM687 – Digital Forensics and Incidence Responses

# Assignment – 6

*Author – Syed Mohammad Ibrahim*

*UMD ID: iamibi*

*UID: 118428369*

*Email: iamibi@umd.edu*

## Brief Summary of Information

The investigation involved examining example1.pcap file which contained network calls to a potential command-and-control center to fetch exploit(s). One file that was recovered from the pcap file was obiwan.exe which further was able to make network calls.

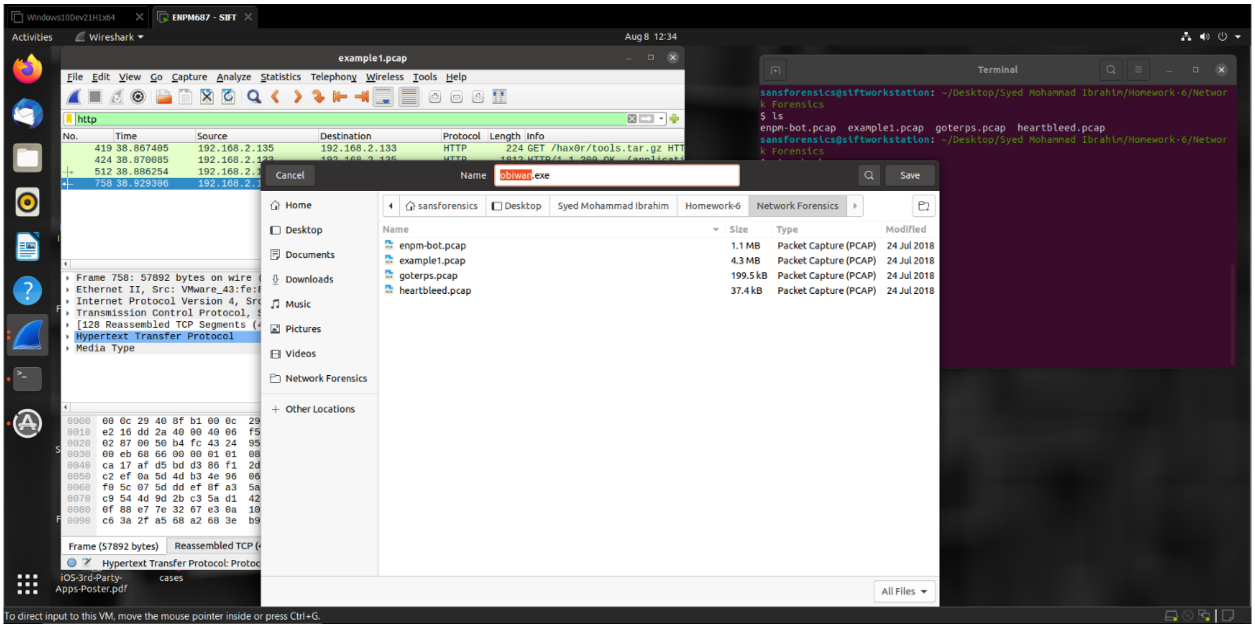
## Tools Used

- Wireshark
  - Used for analyzing the pcap file, extracting the HTTP object and analyzing the binary file network calls.
  - Assumptions – The tool is going to display all the network calls that were made on the machine within the specified time from the system the pcap is taken from.

## Repository

The following steps were performed, and the findings were reported:

1. The pcap file was opened up in Wireshark. After applying the “http” filter, there were two calls made to a remote server which could potentially be a command-and-control server.
2. The objects were retrieved from Wireshark using “Export Object” option and selecting the HTTP > obiwan.exe



example1.pcap

http

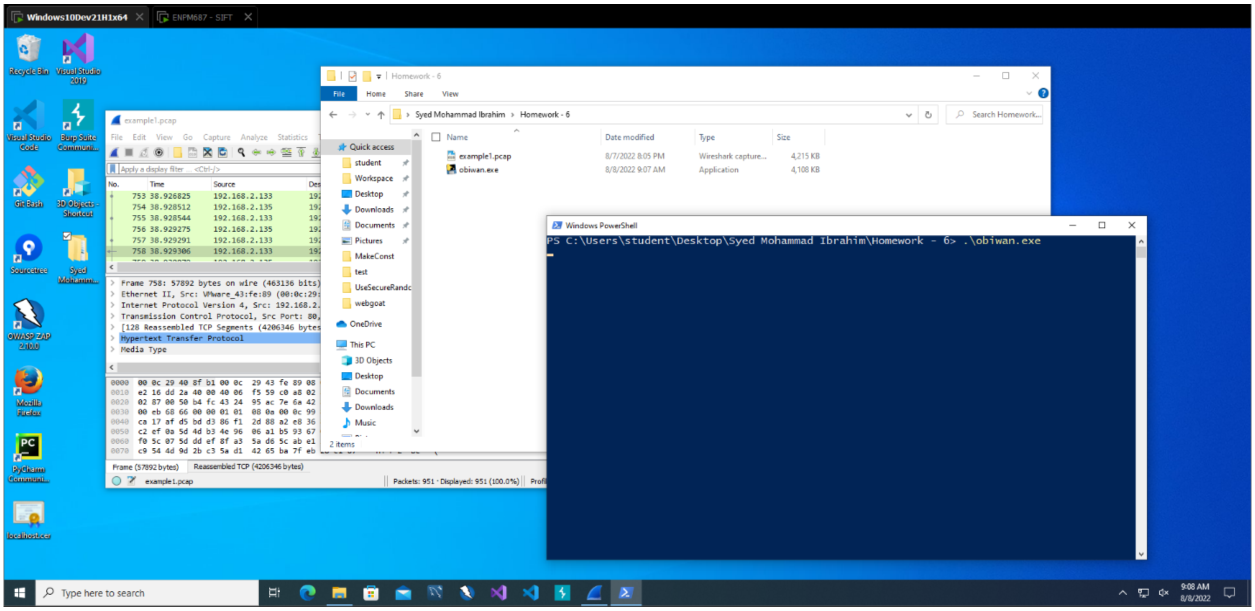
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 419 | 38.867405 | 192.168.2.135 | 192.168.2.133 | HTTP | 224 | GET /hax0r/tools.tar.gz HTT |

Name: obiwan.exe

| Name | Size | Type | Modified |
|---|---|---|---|
| enpm-bot.pcap | 1.1 MB | Packet Capture (PCAP) | 24 Jul 2018 |
| example1.pcap | 4.3 MB | Packet Capture (PCAP) | 24 Jul 2018 |
| goterps.pcap | 199.5 kB | Packet Capture (PCAP) | 24 Jul 2018 |
| heartbleed.pcap | 37.4 kB | Packet Capture (PCAP) | 24 Jul 2018 |

```
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/Homework-6/Networ
k Forensics
$ ls
enpm-bot.pcap  example1.pcap  goterps.pcap  heartbleed.pcap
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/Homework-6/Networ
k Forensics
```

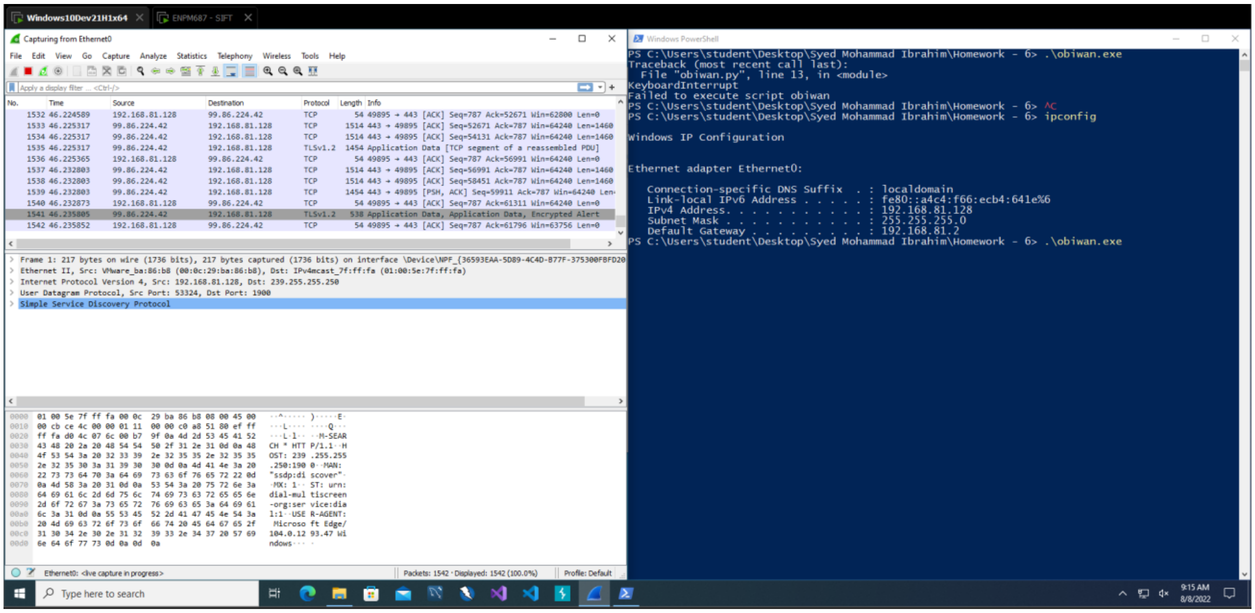
3. This obiwan.exe was then executed in an isolated windows environment inside a virtual machine to make sure that the host system is not accessible and proper forensics can be performed.



| Name | Date modified | Type | Size |
|---|---|---|---|
| example1.pcap | 8/7/2022 8:05 PM | Wireshark capture... | 4,215 KB |
| obiwan.exe | 8/8/2022 9:07 AM | Application | 4,108 KB |

```
PS C:\Users\student\Desktop\Syed Mohammad Ibrahim\Homework - 6> .\obiwan.exe
```

4. Before executing the binary, the Wireshark capture mode was turned on to capture all the network traffic that will be going in and out from the binary.



Windows10Dev21H1x64
ENPM687 - SIFT
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Windows PowerShell
Type here to search

```
No.  Time       Source          Destination     Protocol Length Info
1532 46.224589  192.168.81.128  99.86.224.42    TCP        54 49895 → 443 [ACK] Seq=787 Ack=52671 Win=62800 Len=0
1533 46.225317  99.86.224.42    192.168.81.128  TCP      1514 443 → 49895 [ACK] Seq=52671 Ack=787 Win=64240 Len=1460
1534 46.225317  99.86.224.42    192.168.81.128  TCP      1514 443 → 49895 [ACK] Seq=54131 Ack=787 Win=64240 Len=1460
1535 46.225317  99.86.224.42    192.168.81.128  TLSv1.2  1454 Application Data [TCP segment of a reassembled PDU]
1536 46.225365  192.168.81.128  99.86.224.42    TCP        54 49895 → 443 [ACK] Seq=787 Ack=56991 Win=64240 Len=0
1537 46.232803  99.86.224.42    192.168.81.128  TCP      1514 443 → 49895 [ACK] Seq=56991 Ack=787 Win=64240 Len=1460
1538 46.232803  99.86.224.42    192.168.81.128  TCP      1514 443 → 49895 [ACK] Seq=58451 Ack=787 Win=64240 Len=1460
1539 46.232803  99.86.224.42    192.168.81.128  TCP      1454 443 → 49895 [PSH, ACK] Seq=59911 Ack=787 Win=64240 Len=
1540 46.232873  192.168.81.128  99.86.224.42    TCP        54 49895 → 443 [ACK] Seq=787 Ack=61311 Win=64240 Len=0
1541 46.235805  99.86.224.42    192.168.81.128  TLSv1.2   538 Application Data, Application Data, Encrypted Alert
1542 46.235852  192.168.81.128  99.86.224.42    TCP        54 49895 → 443 [ACK] Seq=787 Ack=61796 Win=63756 Len=0
```

```
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{36593EAA-5D89-4C4D-B77F-375300FBFD20
> Ethernet II, Src: VMware_ba:86:b8 (00:0c:29:ba:86:b8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.81.128, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53324, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 00 0c  29 ba 86 b8 08 00 45 00   ··^····· )·····E·
0010  00 cb ce 4c 00 00 01 11  00 00 c0 a8 51 80 ef ff   ···L···· ····Q···
0020  ff fa d0 4c 07 6c 00 b7  9f 0a 4d 2d 53 45 41 52   ···L·l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 4d 69 63 72 6f 73 6f  66 74 20 45 64 67 65 2f    Microso ft Edge/
00c0  31 30 34 2e 30 2e 31 32  39 33 2e 34 37 20 57 69   104.0.12 93.47 Wi
00d0  6e 64 6f 77 73 0d 0a 0d  0a                        ndows··· ·
```

Ethernet0: <live capture in progress>

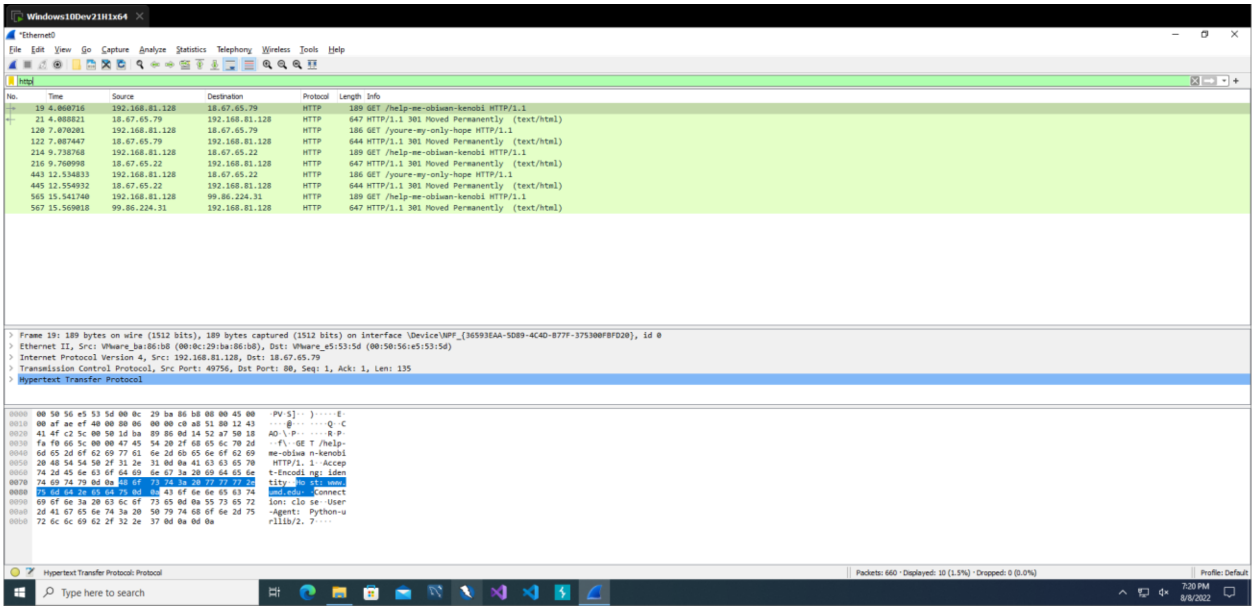
Packets: 1542 · Displayed: 1542 (100.0%)

Profile: Default

```
PS C:\Users\student\Desktop\Syed Mohammad Ibrahim\Homework - 6> .\obiwan.exe
Traceback (most recent call last):
  File "obiwan.py", line 13, in <module>
KeyboardInterrupt
Failed to execute script obiwan
PS C:\Users\student\Desktop\Syed Mohammad Ibrahim\Homework - 6> ^C
PS C:\Users\student\Desktop\Syed Mohammad Ibrahim\Homework - 6> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a4c4:f66:ecb4:641e%6
   IPv4 Address. . . . . . . . . . . : 192.168.81.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.81.2
PS C:\Users\student\Desktop\Syed Mohammad Ibrahim\Homework - 6> .\obiwan.exe
```

9:15 AM
8/8/2022

5. After examining the network calls, it was evident that there were some messages being passed by obiwan.exe to the remote server and a response was received as message.



Windows10Dev21H1x64
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Type here to search

```
No.  Time       Source          Destination     Protocol Length Info
  19 4.060716   192.168.81.128  18.67.65.79     HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
  21 4.088821   18.67.65.79     192.168.81.128  HTTP     647 HTTP/1.1 301 Moved Permanently  (text/html)
 120 7.070201   192.168.81.128  18.67.65.79     HTTP     186 GET /youre-my-only-hope HTTP/1.1
 122 7.087447   18.67.65.79     192.168.81.128  HTTP     644 HTTP/1.1 301 Moved Permanently  (text/html)
 214 9.738768   192.168.81.128  18.67.65.22     HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
 216 9.760998   18.67.65.22     192.168.81.128  HTTP     647 HTTP/1.1 301 Moved Permanently  (text/html)
 443 12.534833  192.168.81.128  18.67.65.22     HTTP     186 GET /youre-my-only-hope HTTP/1.1
 445 12.554932  18.67.65.22     192.168.81.128  HTTP     644 HTTP/1.1 301 Moved Permanently  (text/html)
 565 15.541740  192.168.81.128  99.86.224.31    HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
 567 15.569018  99.86.224.31    192.168.81.128  HTTP     647 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 19: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF_{36593EAA-5D89-4C4D-B77F-375300FBFD20}, id 0
> Ethernet II, Src: VMware_ba:86:b8 (00:0c:29:ba:86:b8), Dst: VMware_e5:53:5d (00:50:56:e5:53:5d)
> Internet Protocol Version 4, Src: 192.168.81.128, Dst: 18.67.65.79
> Transmission Control Protocol, Src Port: 49756, Dst Port: 80, Seq: 1, Ack: 1, Len: 135
> Hypertext Transfer Protocol
```

```
0000  00 50 56 e5 53 5d 00 0c  29 ba 86 b8 08 00 45 00   ·PV·S]·· )·····E·
0010  00 af ae ef 40 00 80 06  00 00 c0 a8 51 80 12 43   ····@··· ····Q··C
0020  41 4f c2 5c 00 50 1d ba  89 86 0d 14 52 a7 50 18   AO·\·P·· ····R·P·
0030  fa f0 66 5c 00 00 47 45  54 20 2f 68 65 6c 70 2d   ··f\··GE T /help-
0040  6d 65 2d 6f 62 69 77 61  6e 2d 6b 65 6e 6f 62 69   me-obiwa n-kenobi
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 41 63 63 65 70    HTTP/1. 1··Accep
0060  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 69 64 65 6e   t-Encodi ng: iden
0070  74 69 74 79 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   tity··Ho st: www.
0080  75 6d 64 2e 65 64 75 0d  0a 43 6f 6e 6e 65 63 74   umd.edu· ·Connect
0090  69 6f 6e 3a 20 63 6c 6f  73 65 0d 0a 55 73 65 72   ion: clo se··User
00a0  2d 41 67 65 6e 74 3a 20  50 79 74 68 6f 6e 2d 75   -Agent:  Python-u
00b0  72 6c 6c 69 62 2f 32 2e  37 0d 0a 0d 0a            rllib/2. 7····
```

Hypertext Transfer Protocol: Protocol

Packets: 660 · Displayed: 10 (1.5%) · Dropped: 0 (0.0%)

Profile: Default

7:20 PM
8/8/2022

## Recommendations and Next Steps

- Make sure to keep the anti-malware system is up to date.
- A whitelist network blocking should be done.