# ENPM687 – Digital Forensics and Incidence Responses

# Assignment – 6

*Author – Syed Mohammad Ibrahim*

*UMD ID:* *iamibi*

*UID: 118428369*

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

Graphical user interface, text

Description automatically generated

1. 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.

A screenshot of a computer

Description automatically generated

1. 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.

A screenshot of a computer

Description automatically generated with medium confidence

1. 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.

Graphical user interface, text, application

Description automatically generated

## Recommendations and Next Steps

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