Execution:

First Method of Exfiltration: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol.

Create data

A screenshot of a computer

Description automatically generated with medium confidence

^creating the .txt data to obfuscate/hide in plain text.

Hiding data:

Graphical user interface, text, application

Description automatically generated

^choosing a jpg image in order to obfuscate the secrete txt file

Text

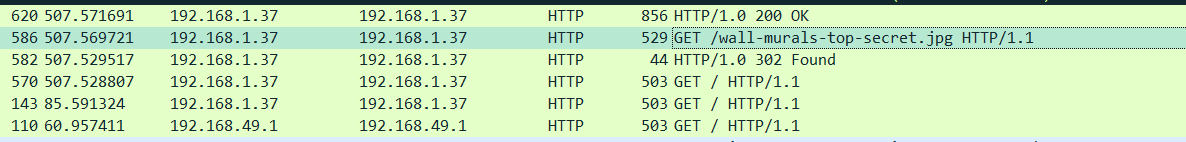
Description automatically generated

^obfuscating the data

A picture containing graphical user interface

Description automatically generated

^Downloading the obfuscated data across the network in the environment.



^proof of obfuscation of data in Wireshark where it showed the jpg that was actually hiding the txt data to be obtained across the network^

Graphical user interface, text, application, email

Description automatically generated

^exporting the obfuscated data

Text

Description automatically generated

^image downloaded

Conclusion: Using the method Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol, I have obfuscated the hidden/confidential text data into a random jpg file in order to hide the fact that extremely sensitive data was actually being moved from one environment to another, as shown with the Wireshark pcap file screenshot where the jpg file was being seen through the network and not the txt file -which is the actual confidential data being exfiltrated across the network- itself. Methods used were steganography, with serve file for transporting across the network itself and having the obfuscation exfiltration method being accomplished at the end.