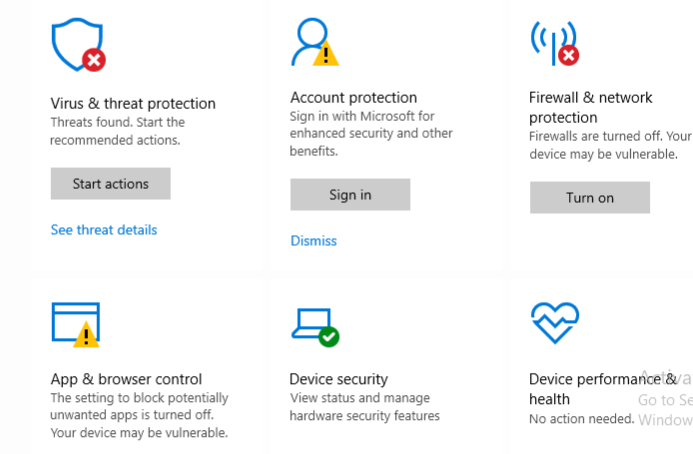
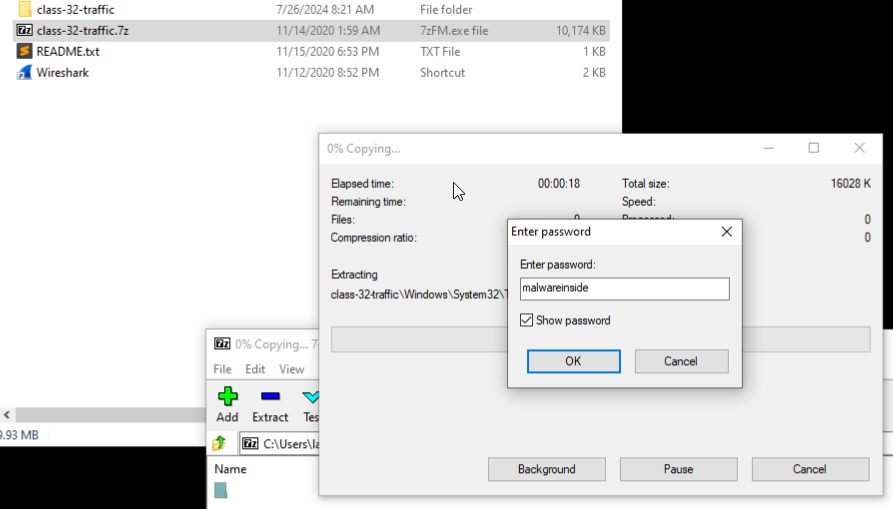
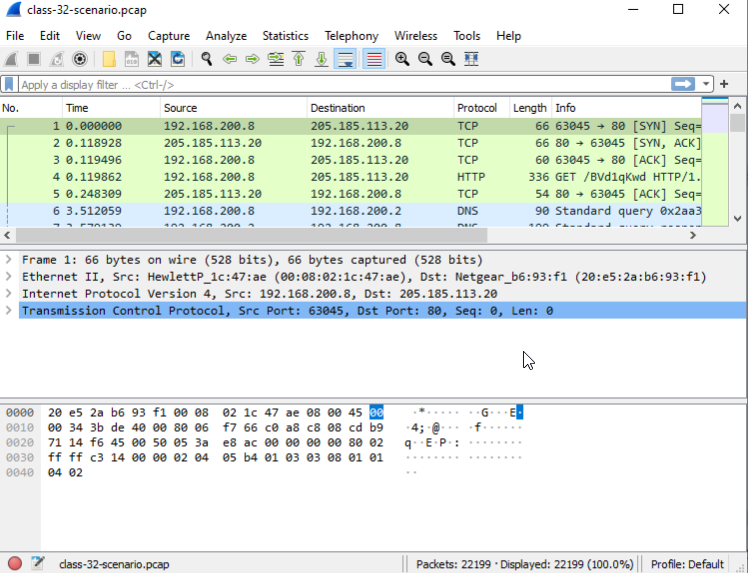
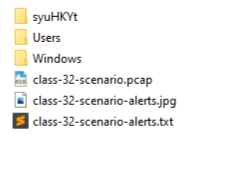
Hélio Ferreira 25/07/2024

# **Lab: Malware Traffic Analysis with Wireshark**

### **Part 1: Staging**

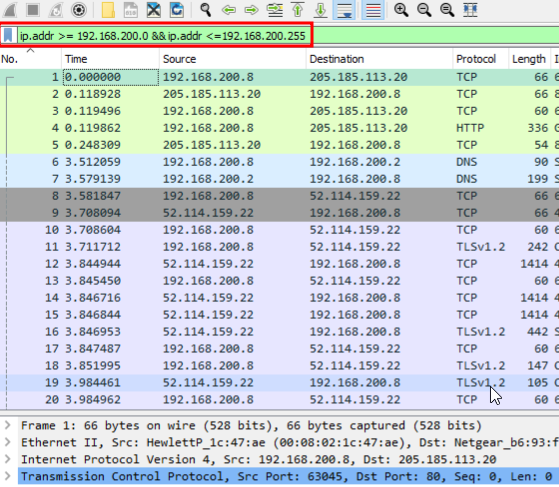
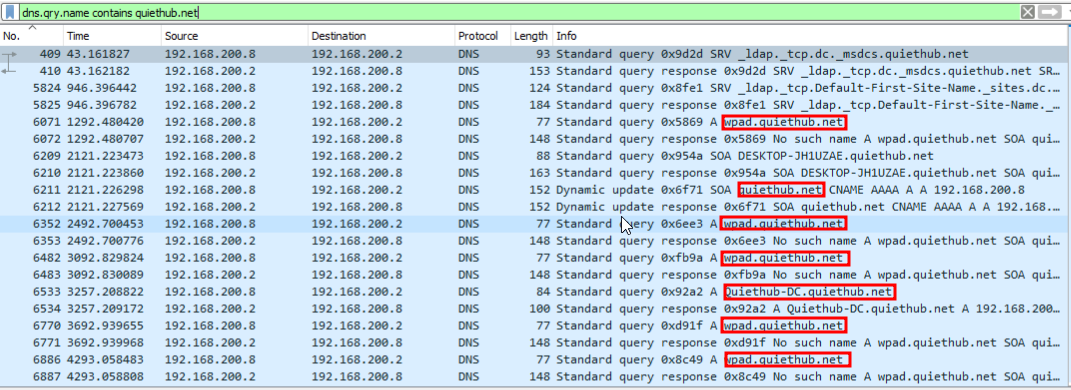
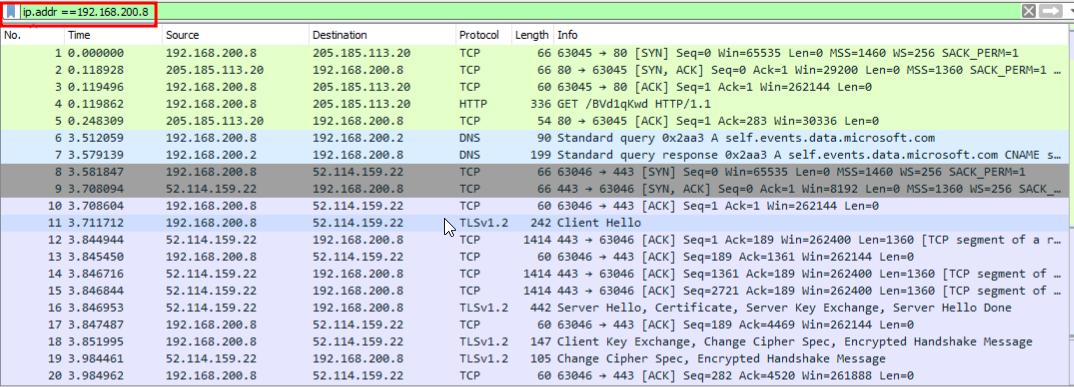
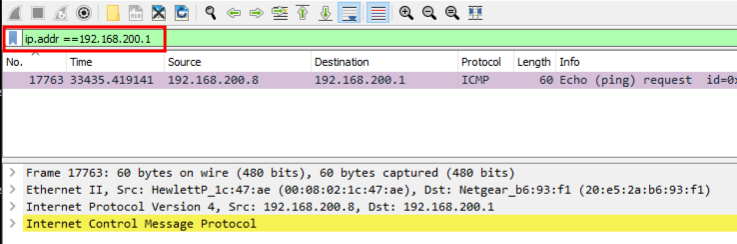
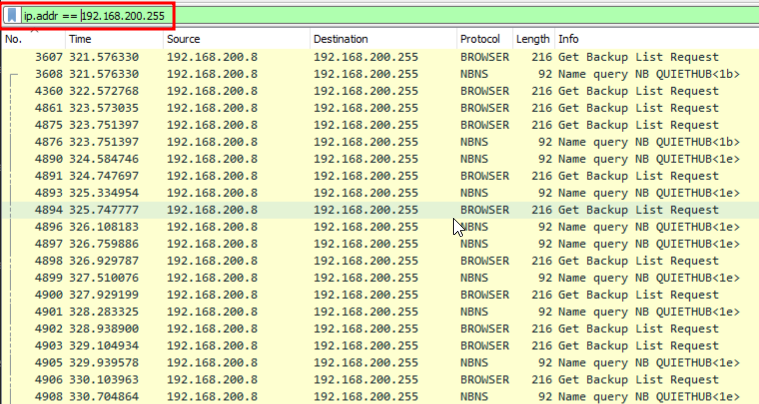
Time to figure out what really took place based on the evidence we have available.

* Disable Windows Defender Antivirus in FLARE VM
* Open the evidence package named “class-32-traffic.7z” on your FLARE VM desktop using password “malwareinside” to open.  
    
  

*WARNING: Part of this package contains live malware. Ensure that you download this into a sandboxed VM that is isolated from the host PC and the rest of your network. You have been warned.*

### **Part 2: Malware Traffic Analysis**

Refer to this information about the environment:

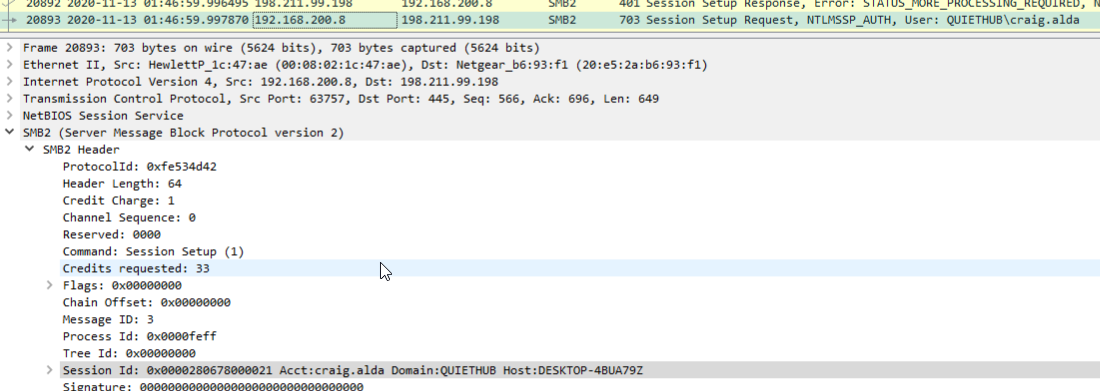
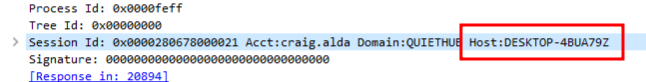
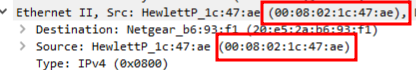
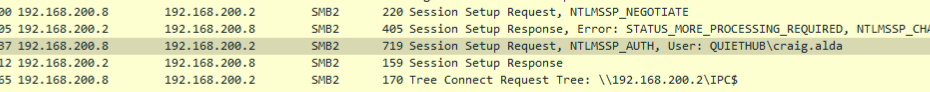
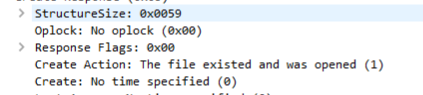
* LAN segment range: 192.168.200.0/24 (192.168.200.0 through 192.168.200.255)  
  
* Domain: quiethub.net  
  
* Domain controller: 192.168.200.8 - Quiethub-DC  
  
* LAN segment gateway: 192.168.200.1
* LAN segment broadcast address: 192.168.200.255  
  

Evaluate the evidence; use the tools you’ve learned thus far to piece together the details of what took place. In order to complete this lab, you’ll need to use critical thinking and careful analysis to reconstruct the events that took place.

*Forensic analysis of data files can be tedious, dry, tiresome, and even frustrating! If you ever get stuck, start with the most obvious signals and let those clues guide your next steps. Ask yourself: “Did the evidence lead me here?” If the answer is no, go back to the beginning and rethink your approach.*

### **Part 3: Reporting**

Write an incident report based on your findings. Include the following components:

* Executive Summary
  + Include when, who, and what happened.  
      
    WHEN  
      
      
    WHO  
      
      
    WHAT HAPPENED  
      
    It was possible to analyze and understand that there is an attempt to compromise the systems by a threat actor, one of the ways was the analysis carried out on an entire network and on several ports, the threat actor was able to access the system and exfiltrate data.
* Details
  + Include details of the victim such as hostname, IP address, MAC address, Windows user account name.  
      
    Hostname  
      
    IP Adress  
      
    MAC Adress  
      
    Windows User Account Name   
    
* Indicators of Compromise (IOCs)
  + Include SHA256 hashes and details of the malware and/or artifacts, IP addresses, domains and URLs associated with the infection.  
      
    

*Take care not to accidentally transmit malware. All artifacts should remain on your FLARE VM.*