Network Traffic Analysis with Wireshark – Yonase Project

Introduction:

For this project, I captured and analysed my system's network activity using Wireshark. Finding any abnormal traffic that would point to unauthorised connections or malicious activity was the aim. I was able to find other dubious IP addresses through filtering and analysis that were linked to malware and other risks, as confirmed by security tools like VirusTotal.

Setup and Tools:

- **Wireshark**: Network protocol analyser used to capture and inspect the traffic on my local network.
- **VirusTotal**: Online service used to check suspicious IP addresses against security vendor databases for known threats.

Steps:

1. **Installed Wireshark** on my Windows machine and recorded network traffic for a specific duration to capture a range of connections.
2. **Filtered traffic** using specific filters to identify unusual and potentially malicious activity. The filters used include:
    - `tcp.flags.syn == 1 and tcp.flags.ack == 0` (to find SYN packets initiating a connection).
    - `tcp.flags.syn == 1` (to locate connection initiation attempts in general).
3. Analysed the filtered traffic to identify suspicious IP addresses.
4. Cross-referenced the suspicious IPs found using **VirusTotal** to verify their reputation and determine if they are associated with any known malware.

Findings:

Malicious IPs Identified:

Through my analysis, I identified several suspicious IP addresses, all of which were flagged by multiple security vendors on VirusTotal for being associated with malware.

1. **139.45.197.238**
    - Flagged by Lumu and Dr.Web as being associated with malware.
    - Additional detections by SOCradar.
2. **139.45.197.248**
    - Flagged by Lumu and Dr.Web as being associated with malware.
3. **139.45.197.236**
    - Flagged by Lumu, Dr.Web, and SOCradar as being associated with various malware strains.

These IP addresses share the same prefix, indicating that they might be part of a broader malicious campaign originating from a similar source.

New Finding:

During additional filtering (`tcp.flags.syn == 1`), I found another IP address that raised suspicion:

- **204.79.197.203**: According to VirusTotal, this IP is flagged as a **criminal IP**. This indicates an additional malicious connection attempt.

Analysis of Findings:

The identified IP addresses initiated **SYN packets**, which is the first step in establishing a TCP connection. This suggests that the malicious actors were trying to initiate a connection with my system, potentially to exploit vulnerabilities or compromise it.

VirusTotal Analysis:

Each suspicious IP address was checked on VirusTotal. The following table summarizes the results:

IP Address	VirusTotal Findings
139.45.197.238	Lumu, Dr.Web, SOCradar - Malware-associated
139.45.197.248	Lumu, Dr.Web - Malware-associated
139.45.197.236	Lumu, Dr.Web, SOCradar - Malware-associated

204.79.197.203	Flagged as a **Criminal IP** by security vendors

System Health Check:

After detecting the suspicious IP addresses, I conducted a full **antivirus scan** of my system to determine if any malware had compromised my machine. According to the scan results, there were no active infections. This suggests that despite attempts to establish malicious connections, there was no successful infiltration.

Here is the final version of your document with the updated content and screenshots:

Network Traffic Analysis with Wireshark

Introduction

For this project, I captured and analyzed my system's network activity using Wireshark. The goal was to identify any abnormal traffic that might indicate unauthorized connections or malicious activity. By filtering and analyzing the captured traffic, I was able to find suspicious IP addresses associated with malware, as confirmed by security tools like VirusTotal.

Setup and Tools

- **Wireshark**: Network protocol analyzer used to capture and inspect the traffic on my local network.
- **VirusTotal**: Online service used to check suspicious IP addresses against security vendor databases for known threats.

Steps

5. Installed Wireshark on my Windows machine and recorded network traffic for a specific duration to capture a range of connections.

6. Filtered traffic using specific filters to identify unusual and potentially malicious activity. The filters used include:
    - `tcp.flags.syn == 1 and tcp.flags.ack == 0` (to find SYN packets initiating a connection).
    - `tcp.flags.syn == 1` (to locate connection initiation attempts in general).
7. Analyzed the filtered traffic to identify suspicious IP addresses.
8. Cross-referenced the suspicious IPs found using VirusTotal to verify their reputation and determine if they are associated with any known malware.

Findings

Malicious IPs Identified

Through my analysis, I identified several suspicious IP addresses, all of which were flagged by multiple security vendors on VirusTotal for being associated with malware:

- **139.45.197.238**: Flagged by Lumu and Dr.Web as being associated with malware. Additional detections by SOCradar.
- **139.45.197.248**: Flagged by Lumu and Dr.Web as being associated with malware.
- **139.45.197.236**: Flagged by Lumu, Dr.Web, and SOCradar as being associated with various malware strains.

These IP addresses share the same prefix, indicating that they might be part of a broader malicious campaign originating from a similar source.

New Finding

During additional filtering using `tcp.flags.syn == 1`, I found another IP address that raised suspicion:

- **204.79.197.203**: According to VirusTotal, this IP is flagged as a criminal IP. This indicates an additional malicious connection attempt.

Analysis of Findings

The identified IP addresses initiated SYN packets, which is the first step in establishing a TCP connection. This suggests that malicious actors were attempting to initiate a connection with my system, potentially to exploit vulnerabilities or compromise it.

VirusTotal Analysis

Each suspicious IP address was checked on VirusTotal. The following table summarizes the results:

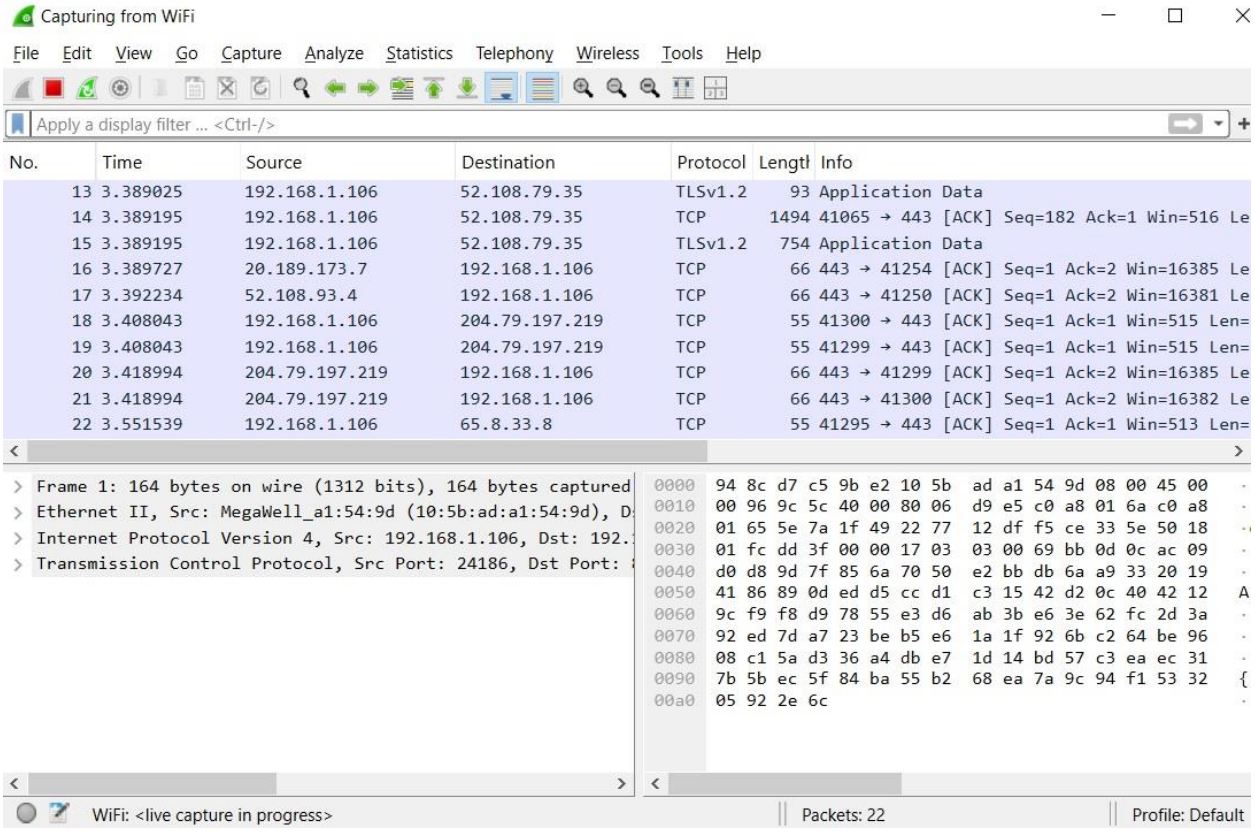
IP Address	VirusTotal Findings
139.45.197.238	Lumu, Dr.Web, SOCradar - Malware-associated
139.45.197.248	Lumu, Dr.Web - Malware-associated
139.45.197.236	Lumu, Dr.Web, SOCradar - Malware-associated
204.79.197.203	Flagged as a Criminal IP by security vendors

System Health Check

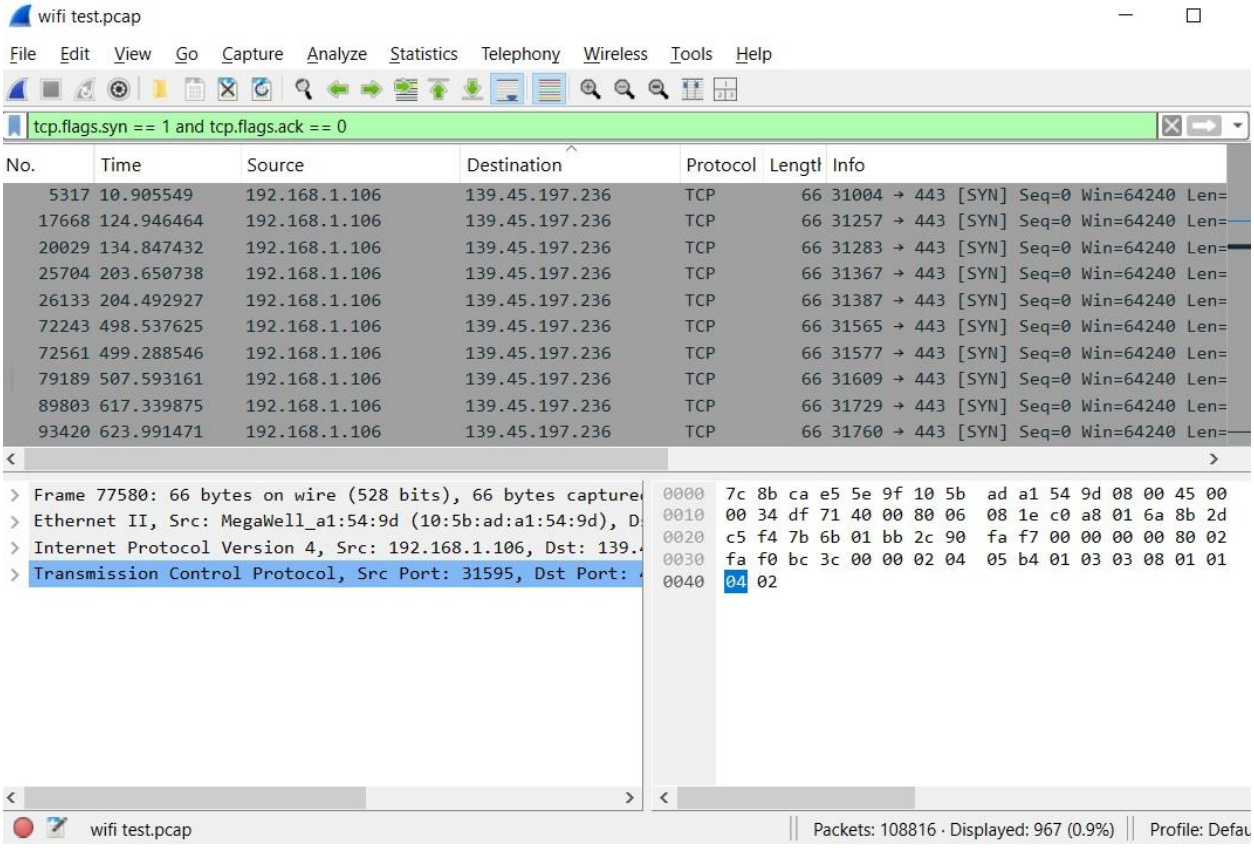
After detecting the suspicious IP addresses, I conducted a full antivirus scan of my system to determine if any malware had compromised my machine. According to the scan results, there were no active infections. This suggests that despite attempts to establish malicious connections, there was no successful infiltration.

Screenshots

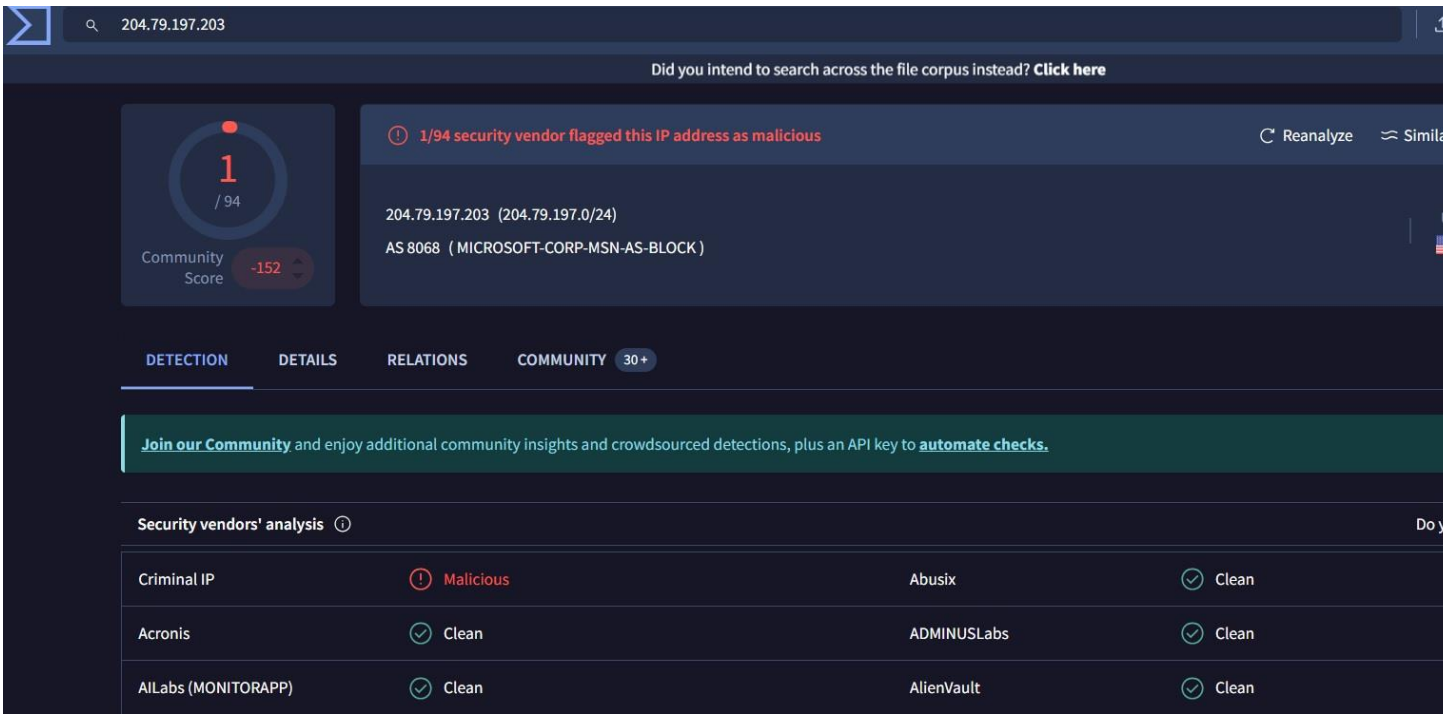
Screenshot 1: Wireshark Capturing Live Traffic



Screenshot 2: SYN Packet Filter Results



Screenshot 3: VirusTotal Analysis for IP 204.79.197.203



Conclusion:

I was able to identify multiple suspicious IP addresses trying to connect to my system from the Wireshark analysis. VirusTotal confirmed that these IPs were connected to known malware and criminal activity. However, thanks to active system defences, my machine remained uncompromised.

This exercise highlights how crucial it is to regularly monitor network traffic and understanding connection attempts . It also demonstrates the value of leveraging tools like Wireshark and VirusTotal in order to stay ahead of potential security risks.