**MOHAMAD ALMASRI** **101167438**

# *DIGITAL FORENSICS&INCID. RESP - COMP 4071*

## Homework Lab 2

First, I started my VMware.

Inside VMware, I turned on my VPN.

Then, I took a screenshot of everything.

After that, I downloaded 5 malware samples from box.com.

I opened Wireshark and ran it using my VPN connection.

Next, I ran the 5 malware files as administrator.

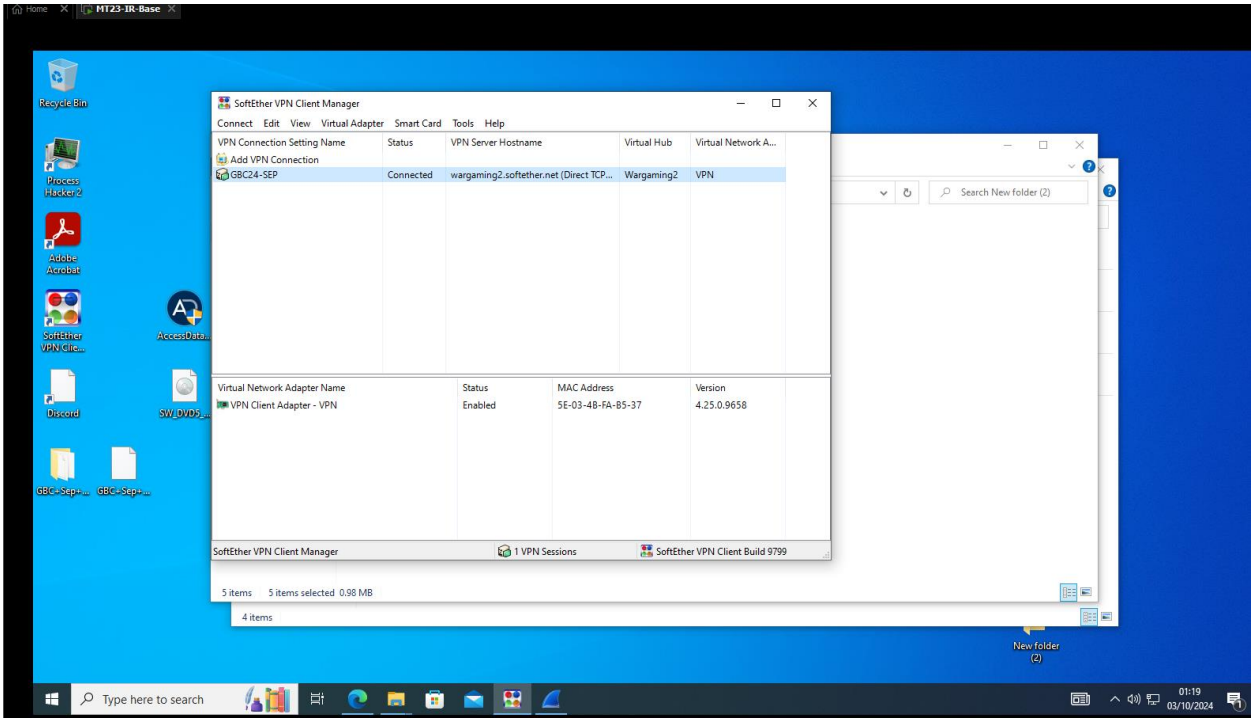
I waited for about 5 minutes.

Then, I stopped Wireshark to stop the capture.

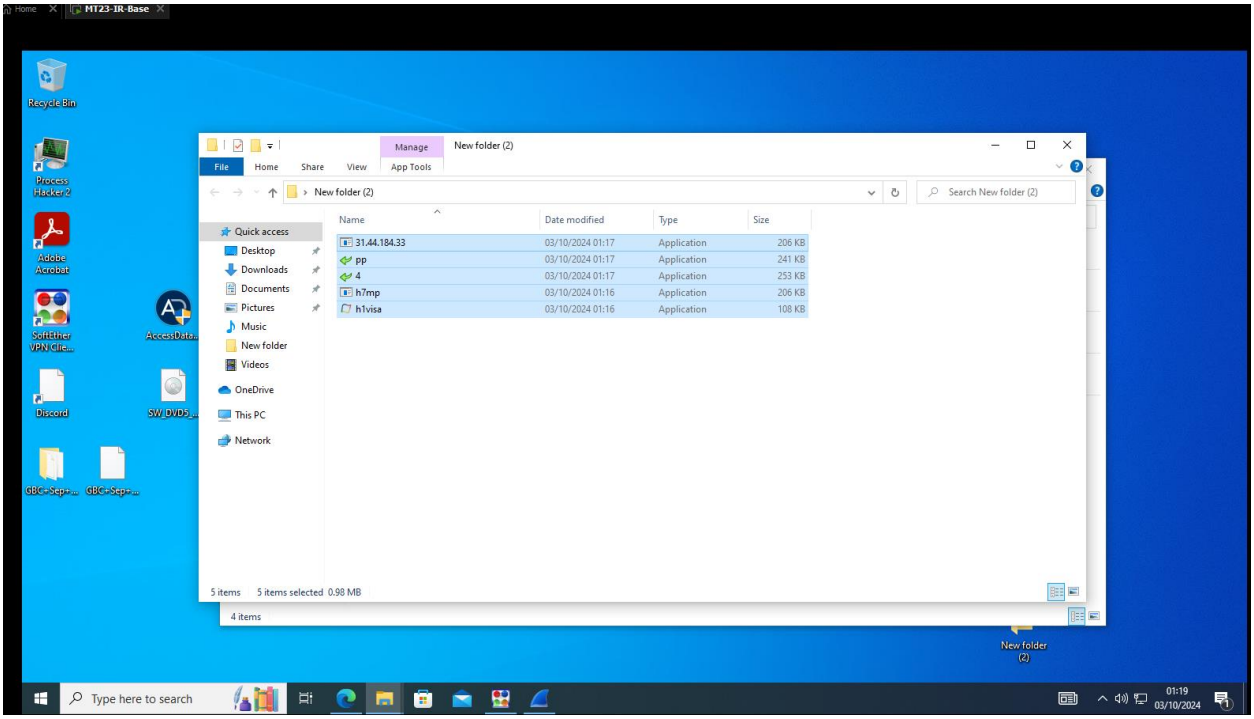
After that, I saved the capture file as a backup.

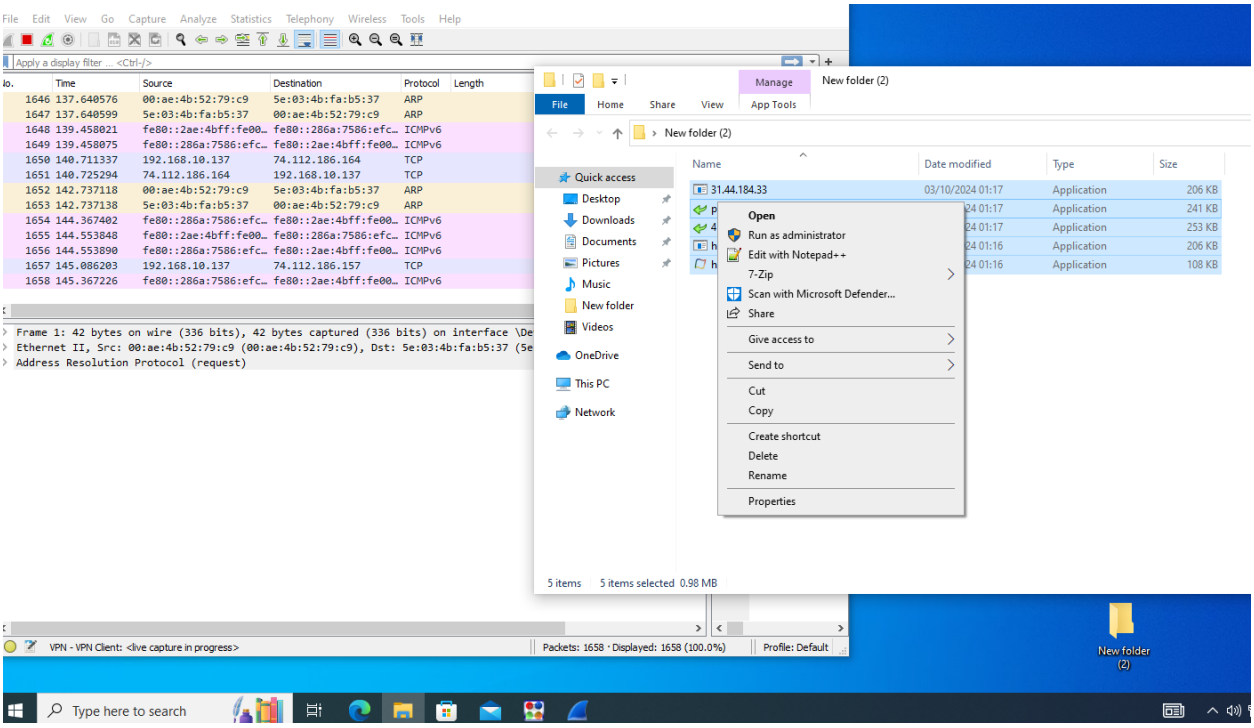
Finally, I used a snapshot reverse to clean my machine.

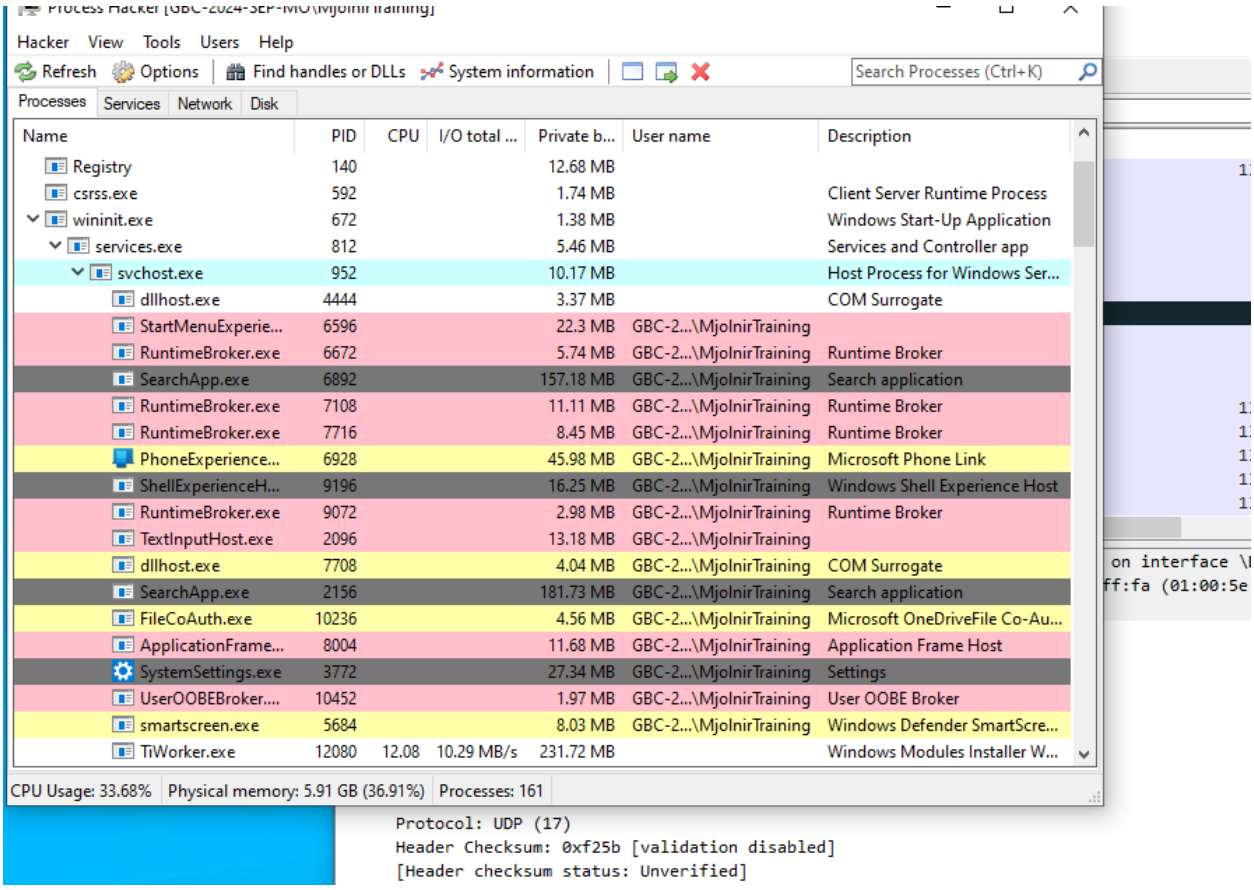
# MOHAMAD ALMASRI 101167438



# MOHAMAD ALMASRI 101167438



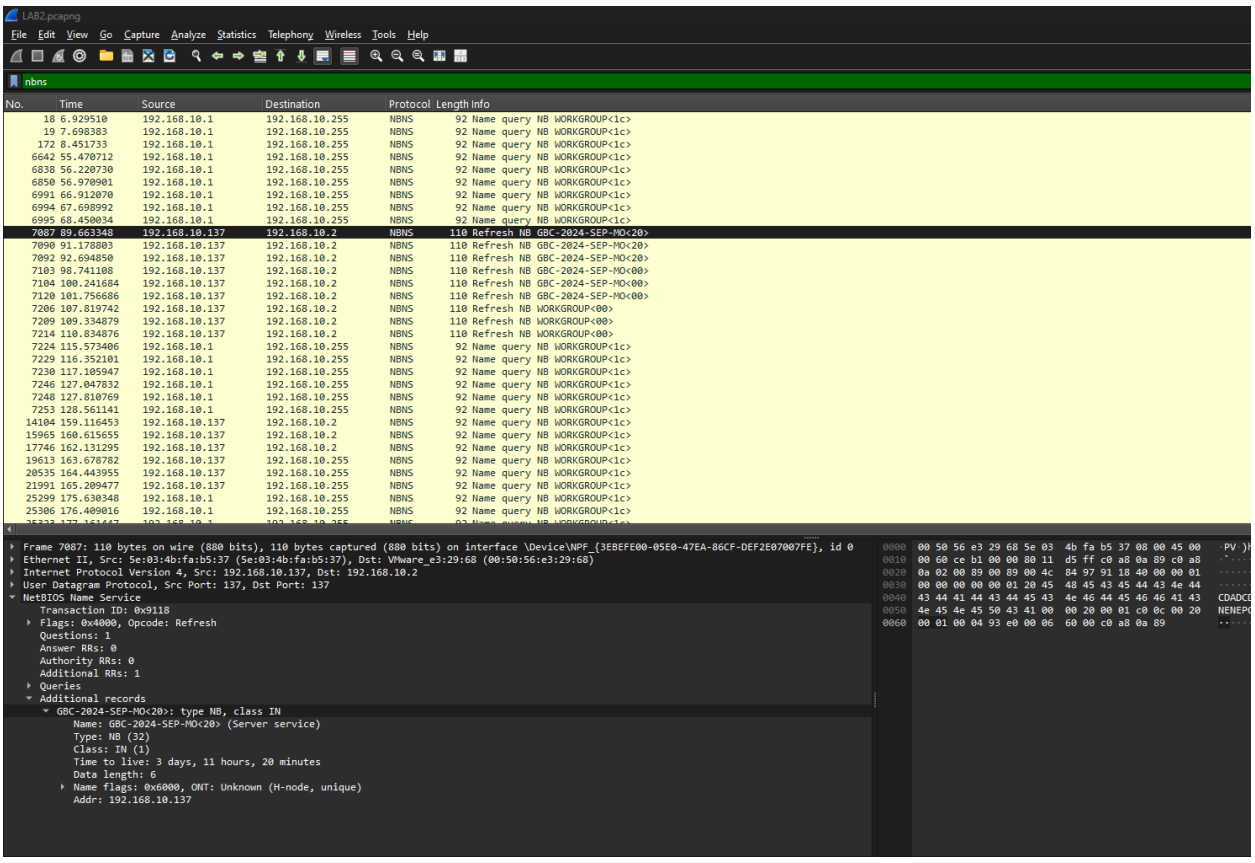





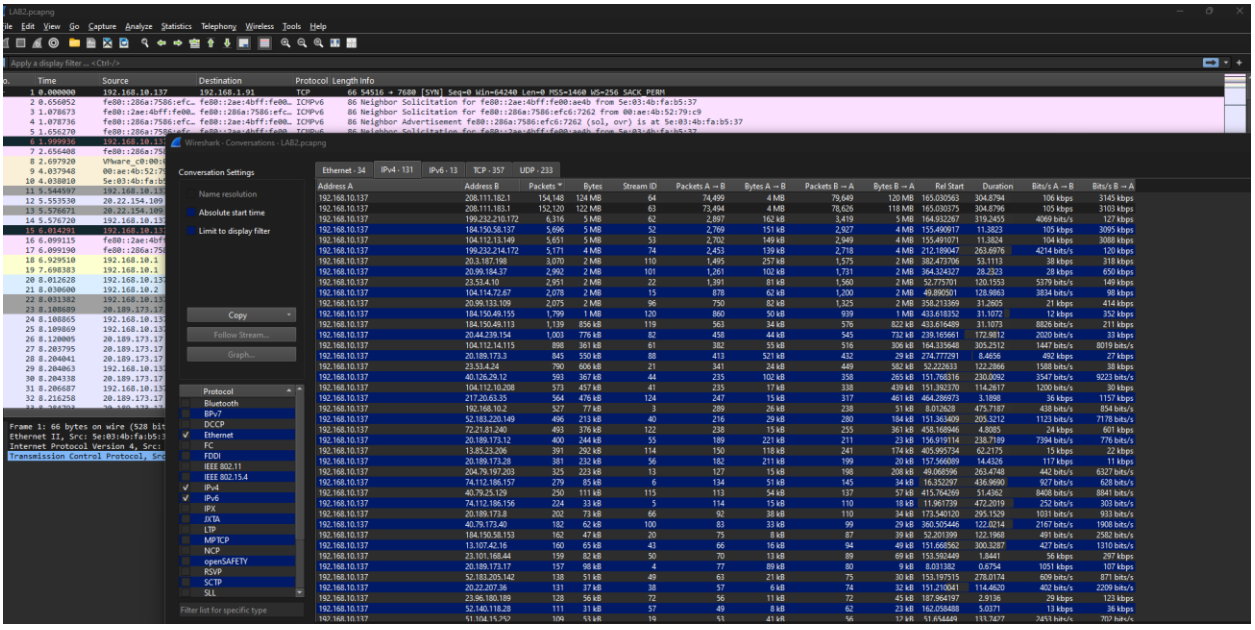

Instructions

1. What is the hostname of the infected device?
   GBC-2024-SEP-MO<20>: type NB, class IN

   I used nbns (NetBIOS Name Service) in Wireshark. After starting the capture, I looked for nbsn traffic, which helps resolve network names. Under the Queries section, I saw the name request for the device, which gave me the hostname. Specifically, I found the hostname in the Additional Records section




2. What is the IP of the infected device? 192.168.10.137



HTTP Requests: The infected gadget with IP 192.168.10.137 is making frequent suspicious HTTP requests. GET queries to purportedly random or encoded URLs are included in these requests; these requests may also indicate communication with a command-and-manage (C2) server or the download of harmful payloads. Certain URLs (such as "lowedcertstl.Cab") also point to untrusted or confusing certificates that may be used in malware or infection techniques. High Volume of Traffic: As you can see from the "Statistics" page, 192.168.10.137 gets charged for a significant amount of traffic to multiple destinations, which may be a sign of unusual interest. A possible malware contamination can be inferred from the number of connections, bytes exchanged, and length of some of the streams, since these kinds of site visits are frequently linked to C2 communications, malware updates, or data exfiltration. Destination IPs: Some of the requests' vacation spot addresses are suspect, including a handful that are associated with well-known CDN (Content Delivery Network) providers. Malware authors may utilize these addresses to conceal their traffic or use trustworthy infrastructure to disseminate

3. Identify all malware(s) with their VT links and VT score:

To find malware collectively with its VirusTotal (VT) URLs and ratings, take the followin movements:

Apply the HTTP Filter: In Wireshark, begin by applying the clear out http. With the resource of this clear out, you'll be able to separate out all HTTP traffic and give attention to web-based conversation, which often includes report downloads and server interactions

Find Suspicious IPs: Keep a watch out for any IP addresses showing peculiar or suspiciou activity, which include repeated connections, encoded URLs, or connections to uncommo domains. This is probably a sign of viable malware activities, like interacting with a command-and-manage (C2) site or downloading documents which might be dangerous..

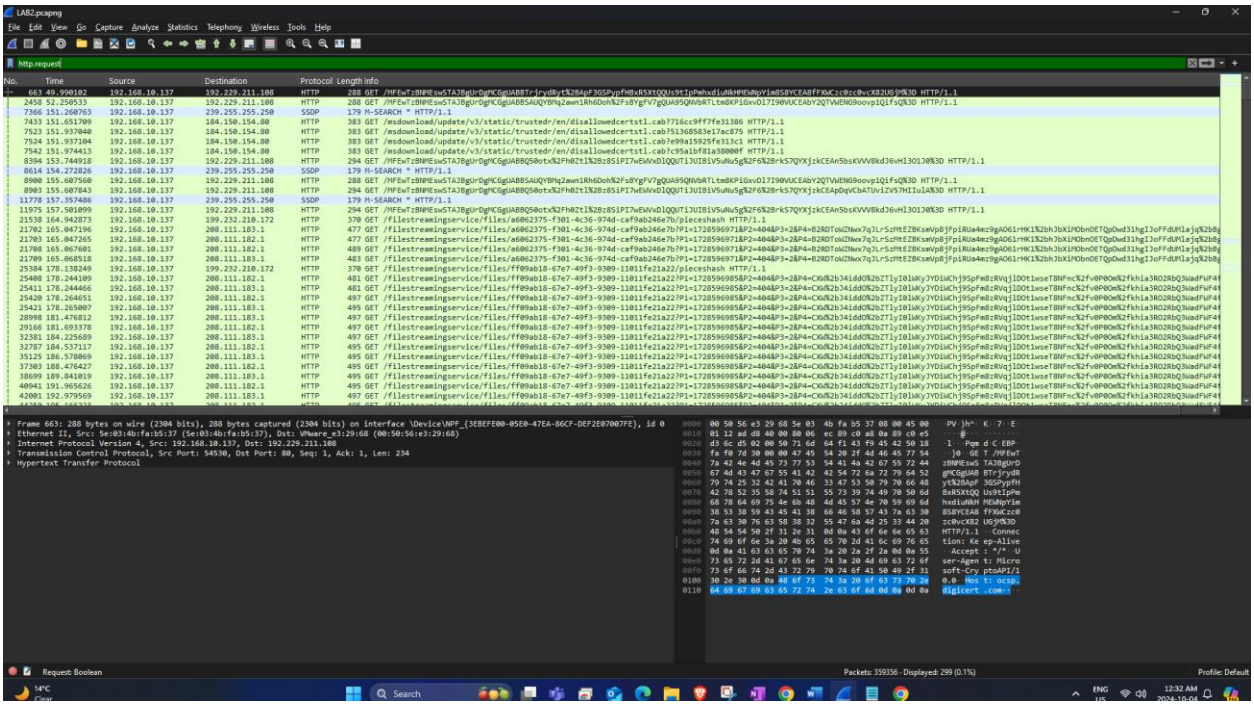
Click on "Follow TCP Stream" from the context menu when you see a suspicious IP address. This will allow you to follow the HTTP stream. This displays all of the tool and server communication. A report that might be malware may be seen to be downloading.

Acquire the File: Note the URL or report name if you locate a file in the stream. This

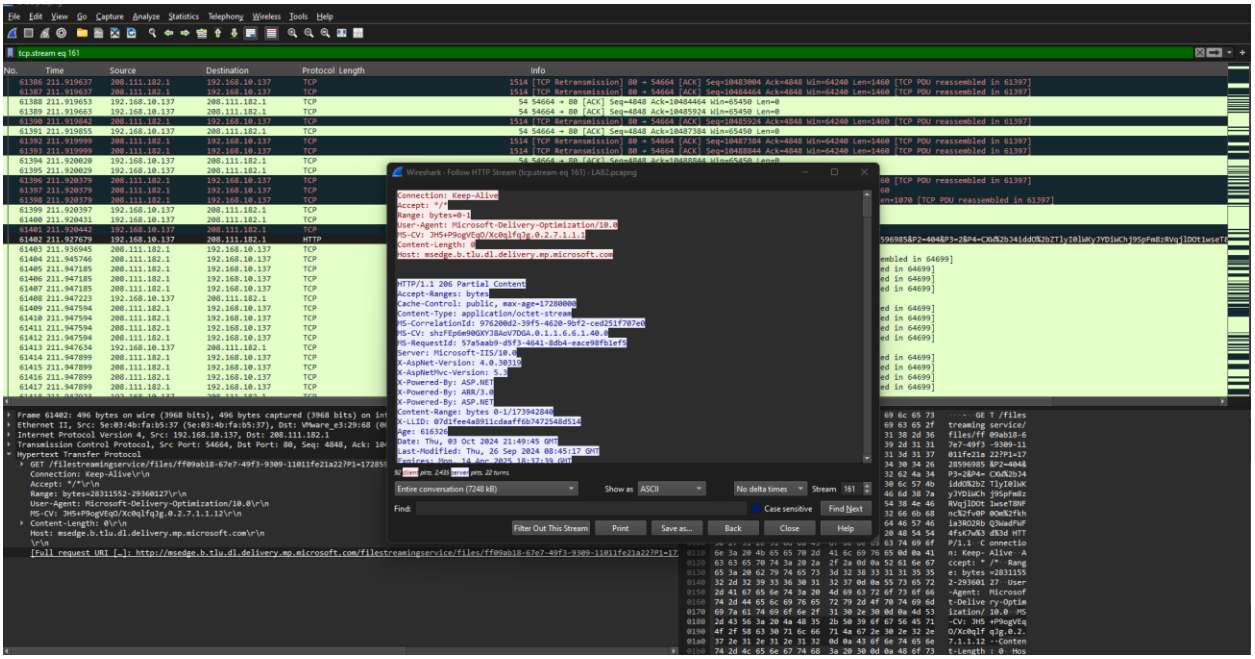
report can be taken out and examined.

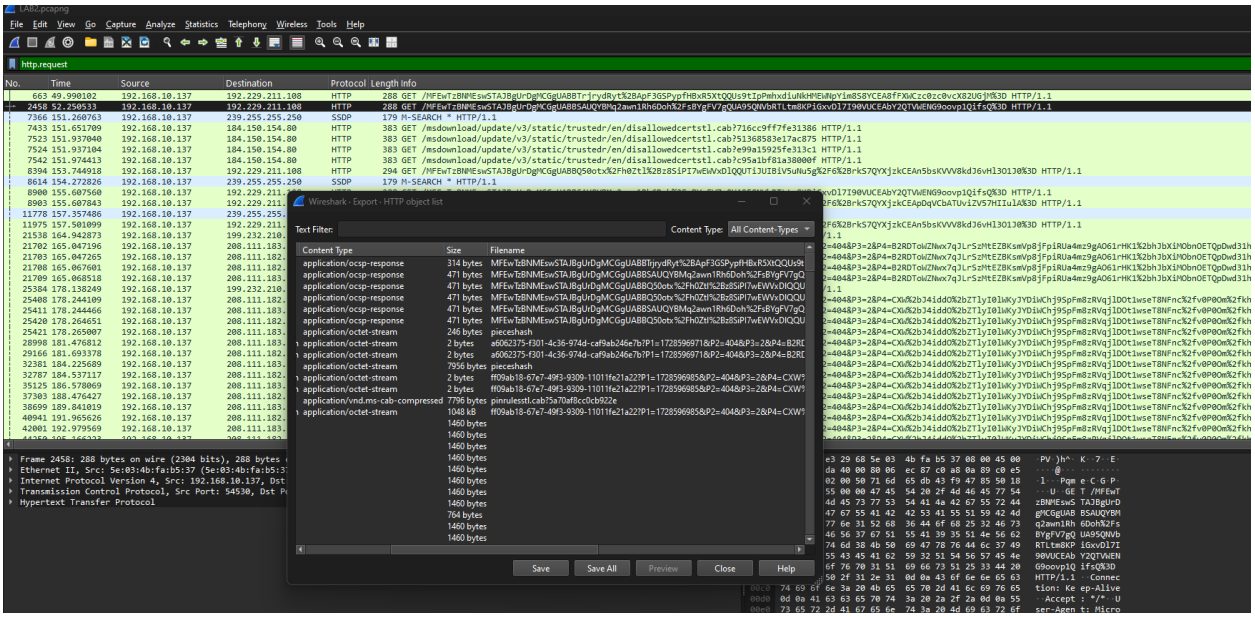
Add the document or paste the URL to VirusTotal.Com after visiting the website. It will b
examined by VirusTotal using a variety of antivirus programs.

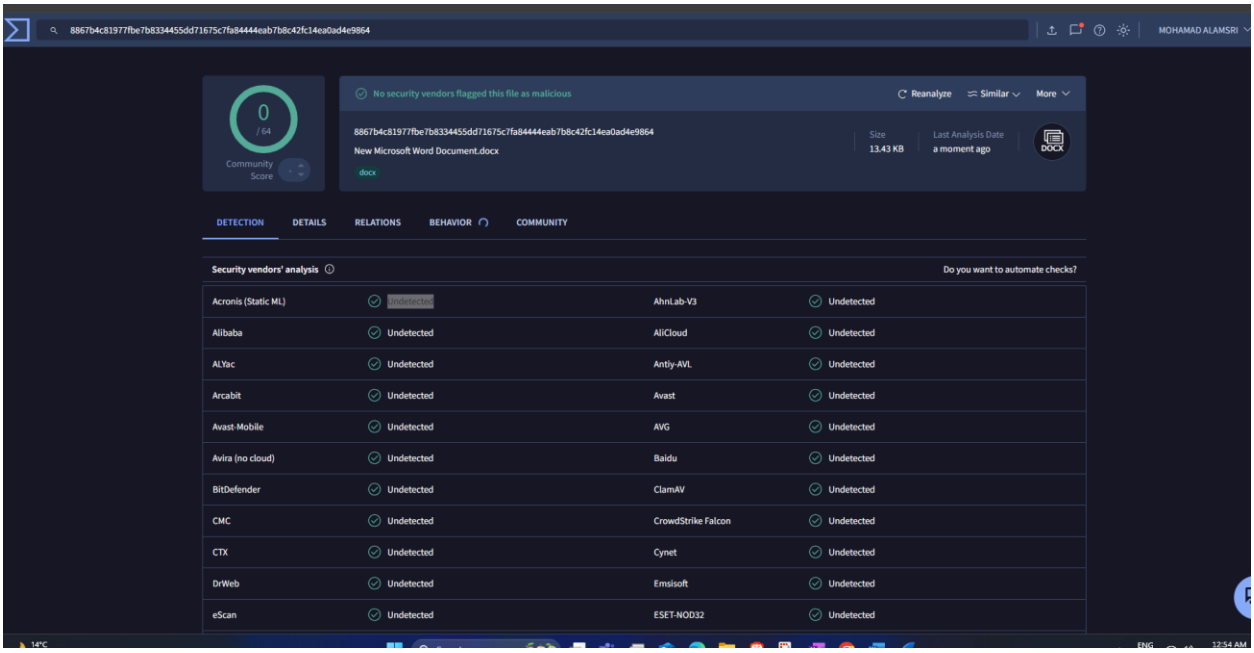
Find the VT Link and Score: VirusTotal will provide a record containing a link and a VT
score that indicates the quantity of antivirus programs that deemed the file to be harmful.



**MOHAMAD ALMASRI** **101167438**





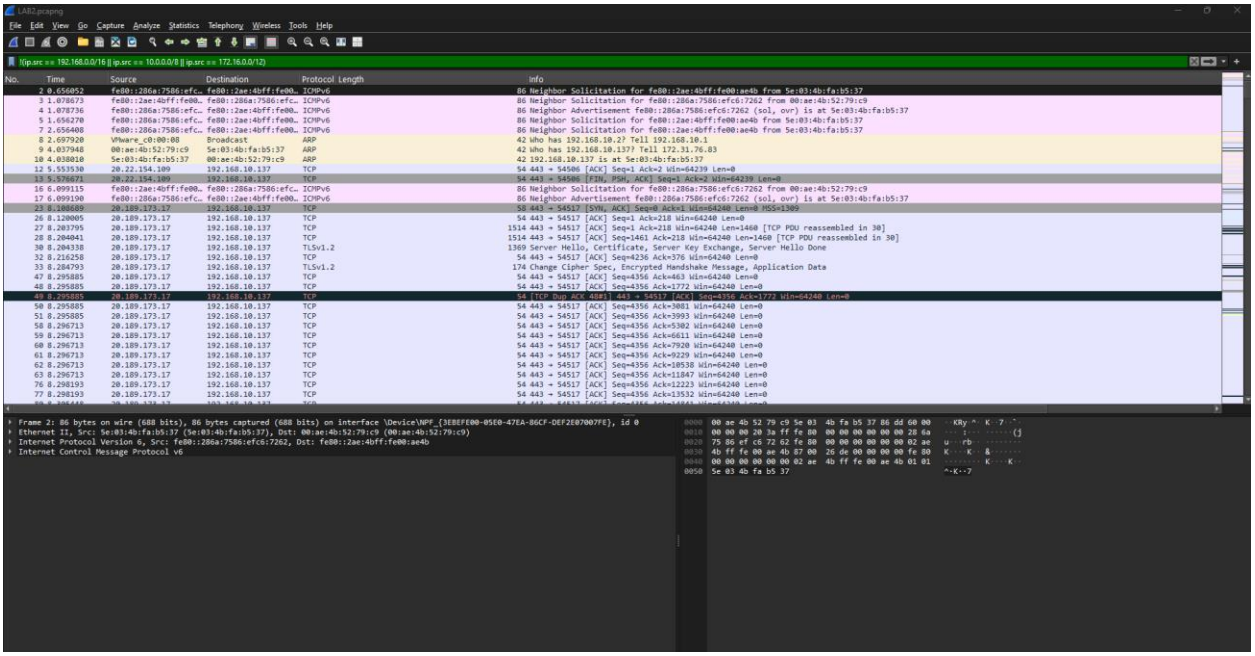


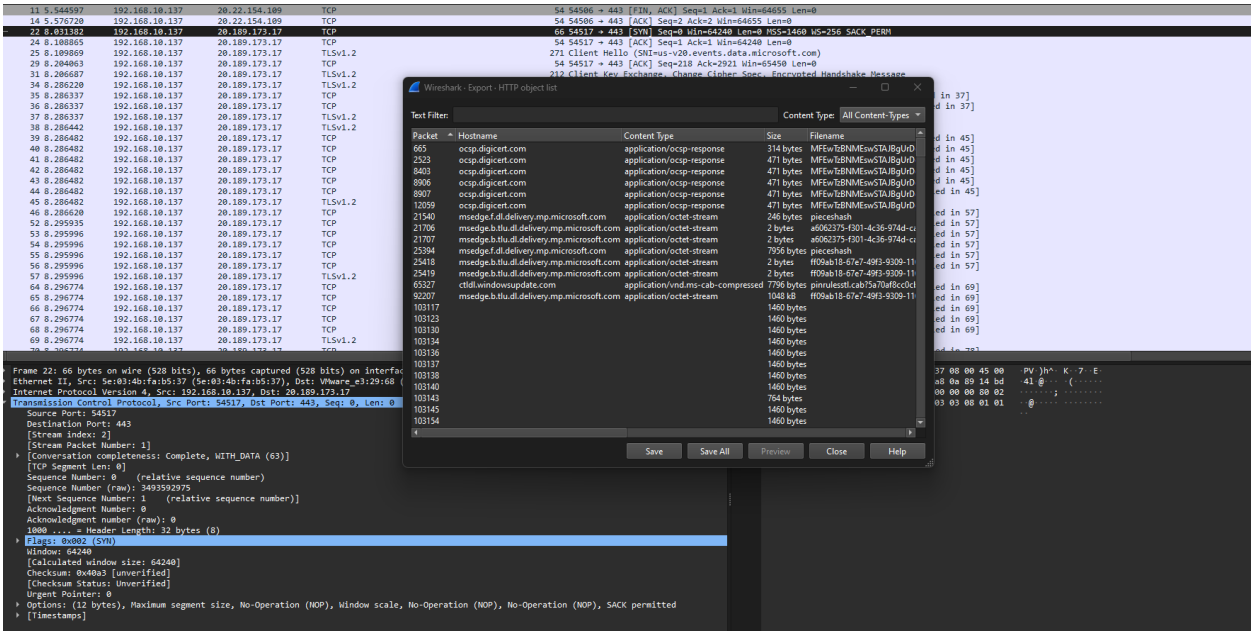

4. Identify all remote hosts which are malicious

To get a list of every external IP that has communicated with your device, navigate to Statistics > Conversations and select the IPv4 or IPv6 tab.

Take the suspicious IP addresses and determine if they are marked as malicious by visiting websites such as VirusTotal or IPVoid.

This procedure has the advantage of determining whether your device is corresponding with any risky or unidentified distant servers that might be involved in a malware infection or hack.





5. Identify all netflow for malicious traffic

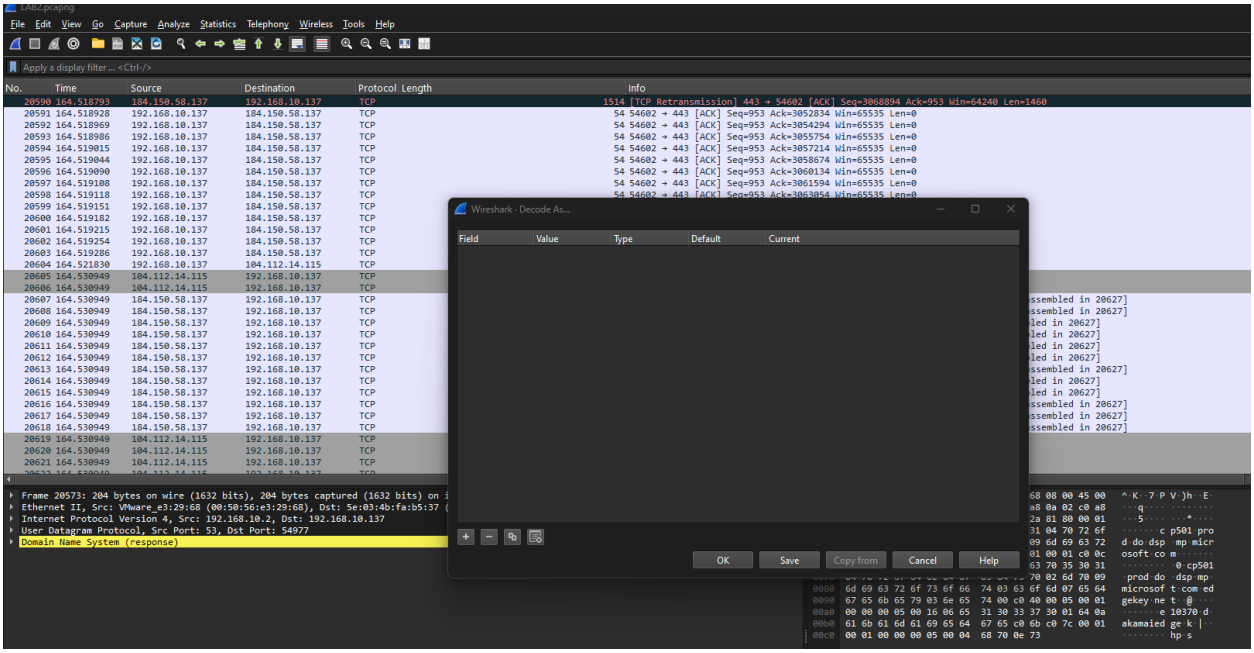
   Select menu option Analyze->Decode As:

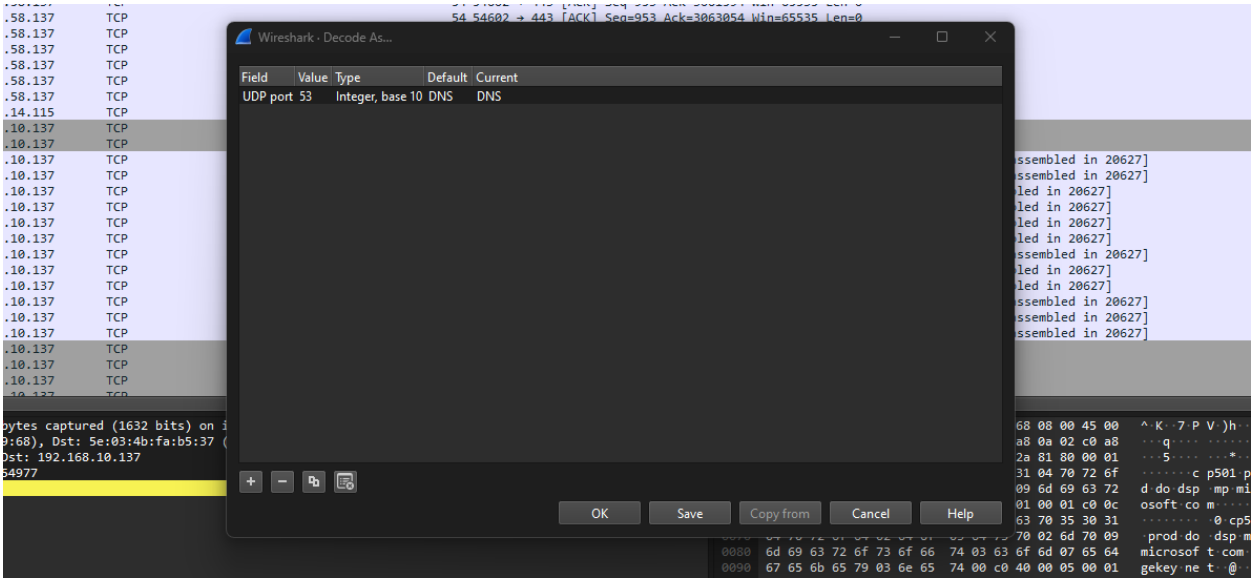
   Select '+' in lower left corner to add an entry to the 'Decode As' window

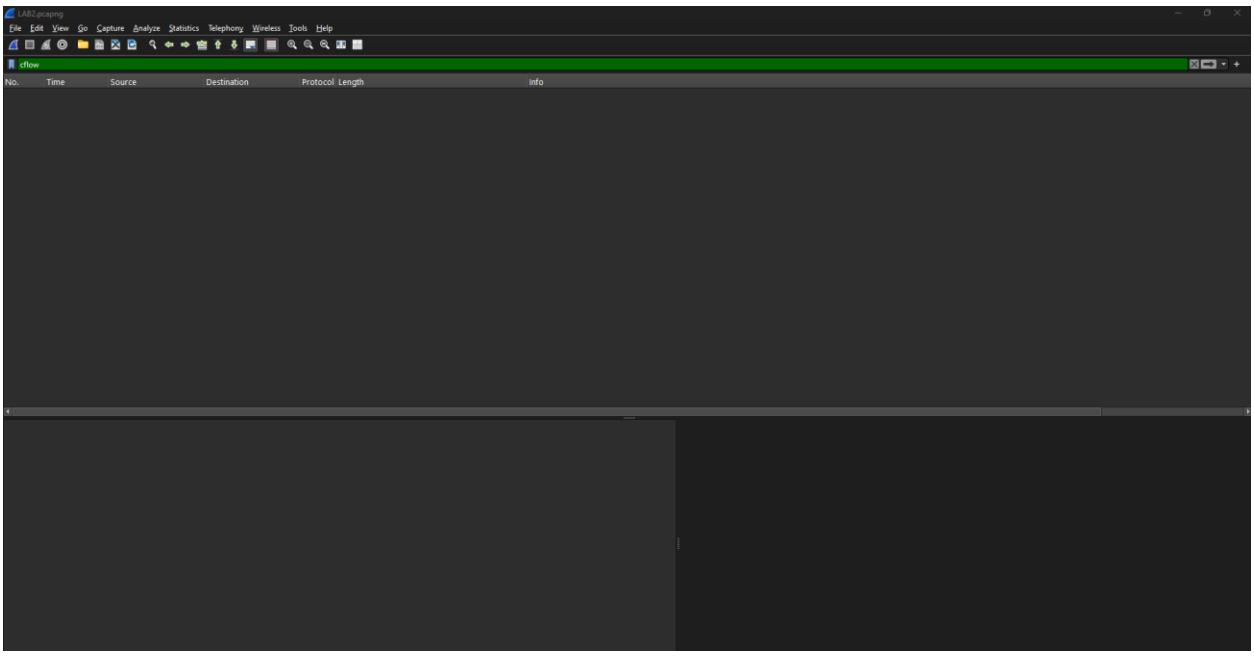
   Select 'none' in the 'current' column then choose 'cflow' from the list:

   Select 'OK' to save the selection. Note flow packets are subsequently denoted as CFLOW in the protocol column:

After this, NetFlow packets will appear as cflow in the protocol column. However, no relevant NetFlow traffic was found in the capture.

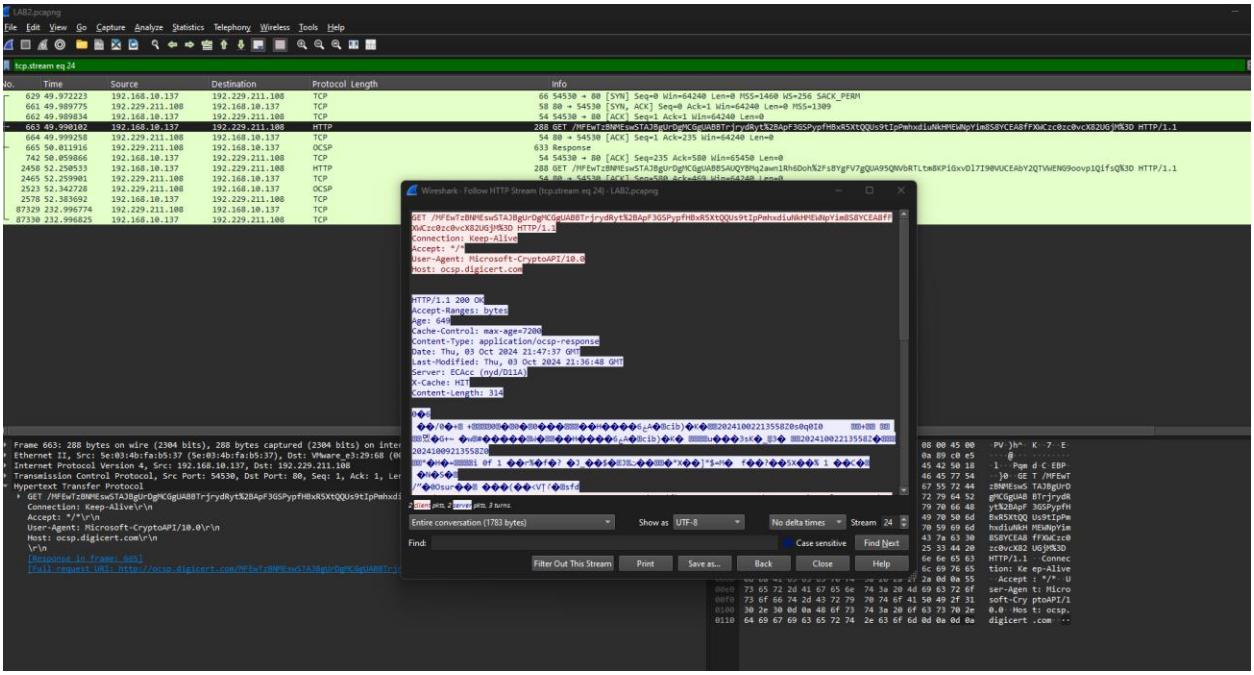


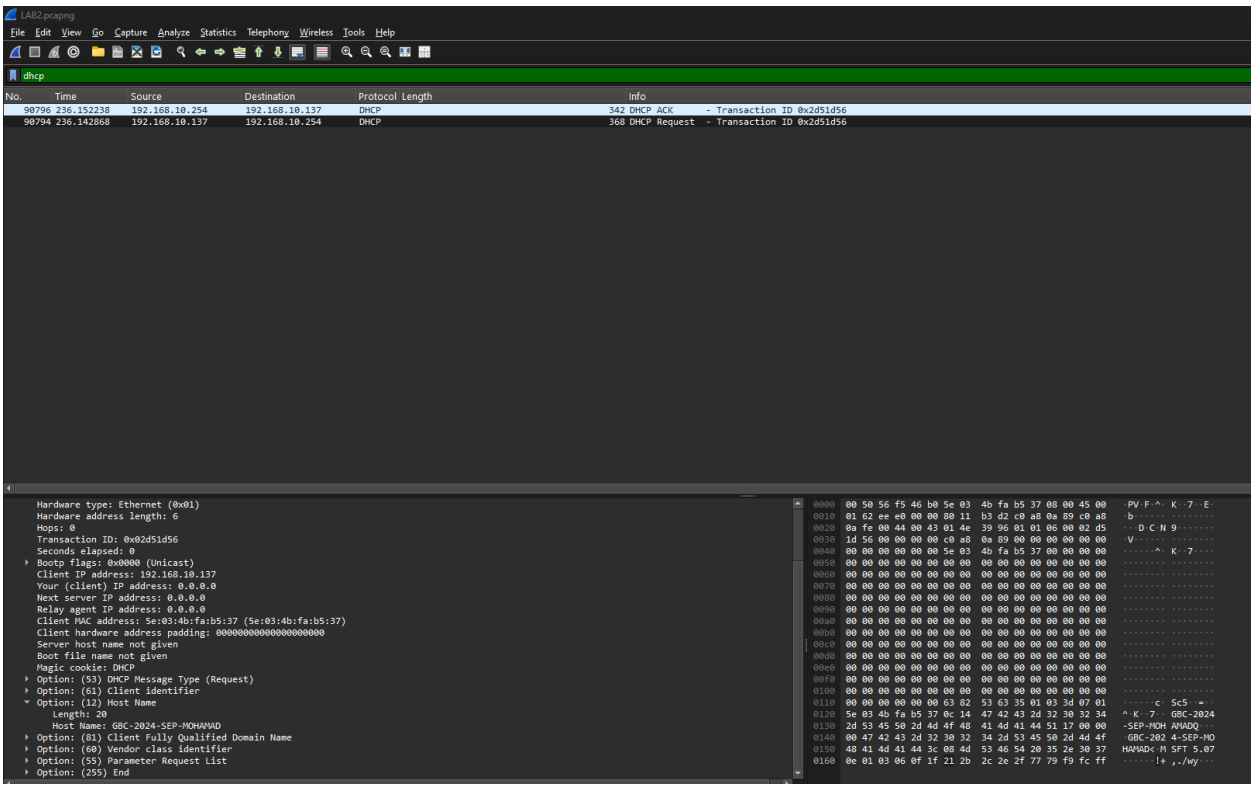





6. Identify usernames :

User-Agent: Microsoft-CryptoAPI/10.0

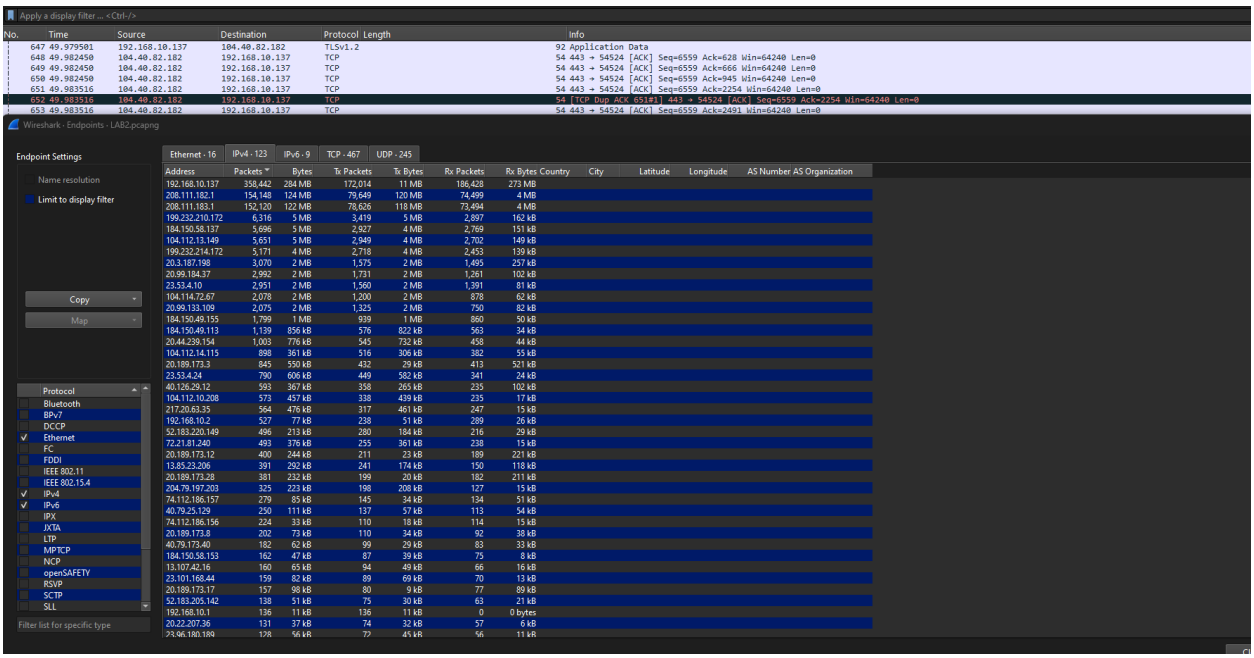





7. Identify who else is on the network

To identify who else is on the network, follow these steps:

- Go to Statistics: In Wireshark, click on the "Statistics" menu at the top.
- Select Endpoints: Choose "Endpoints" from the drop-down menu. This will show you a li of all devices (endpoints) that have communicated on the network during the capture.
- View the List: The list will display IP addresses, MAC addresses, and other details about each device connected to the network.




8. What are the HTTP and DNS requests:

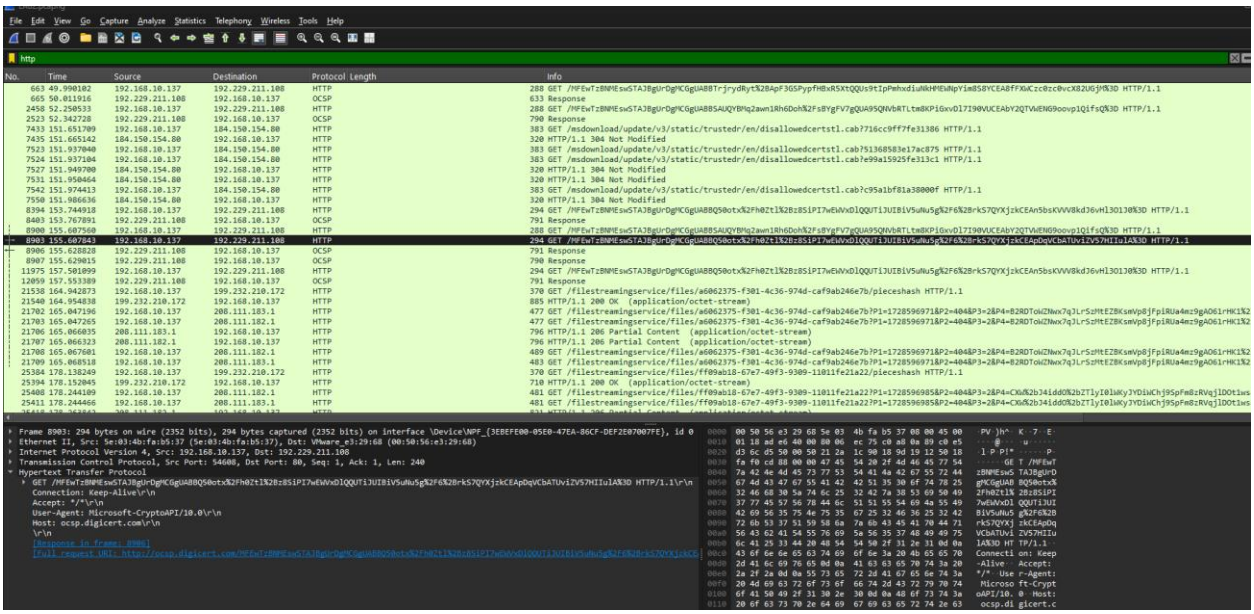
**HTTP requests** are used when a computer (client) talks to a website's server to ask for something or send information. Different types of requests do different things:

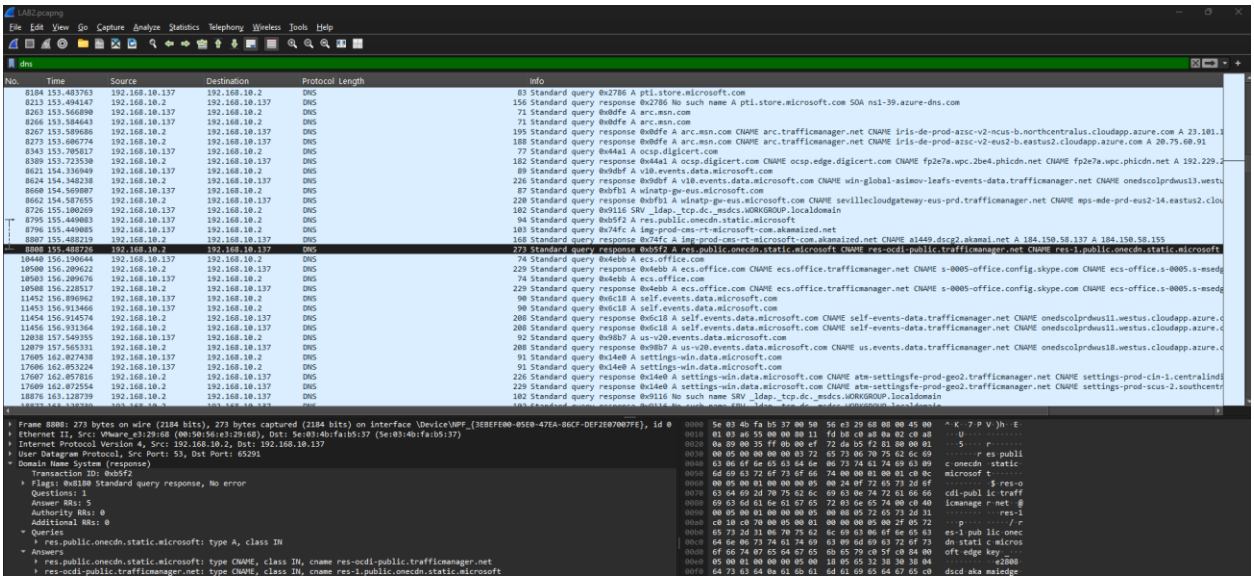
- **GET**: Used to get (retrieve) a webpage or file.
- **POST**: Used to send data, like when you fill out a form.
- **PUT**: Used to update something, like a file or information.
- **DELETE**: Used to remove something from the server.
- **PATCH**: Used to update just part of something.

**DNS requests** are like asking a phonebook for a phone number. When you type a website's name (like google.com) in your browser, your computer doesn't know where tha is right away. So, it sends a **DNS request** to find the **IP address** (like the phone number) for that website.

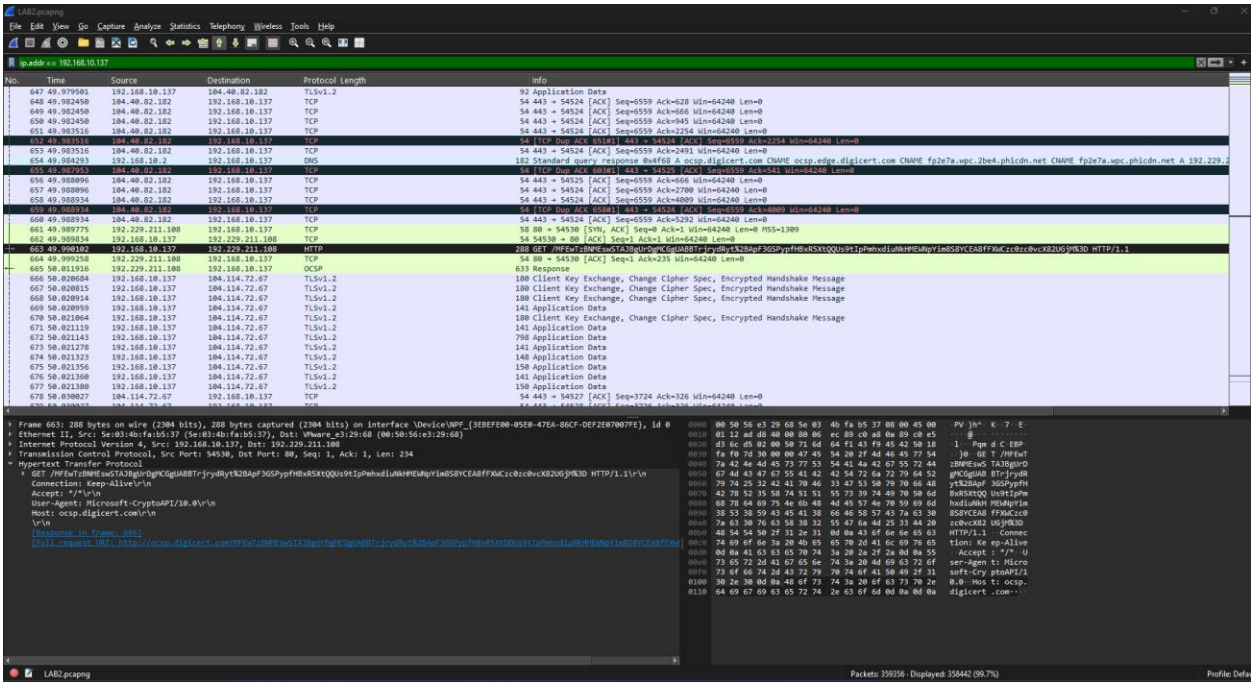
The **DNS server** then replies with the IP address, and your computer uses that to connect to the website.

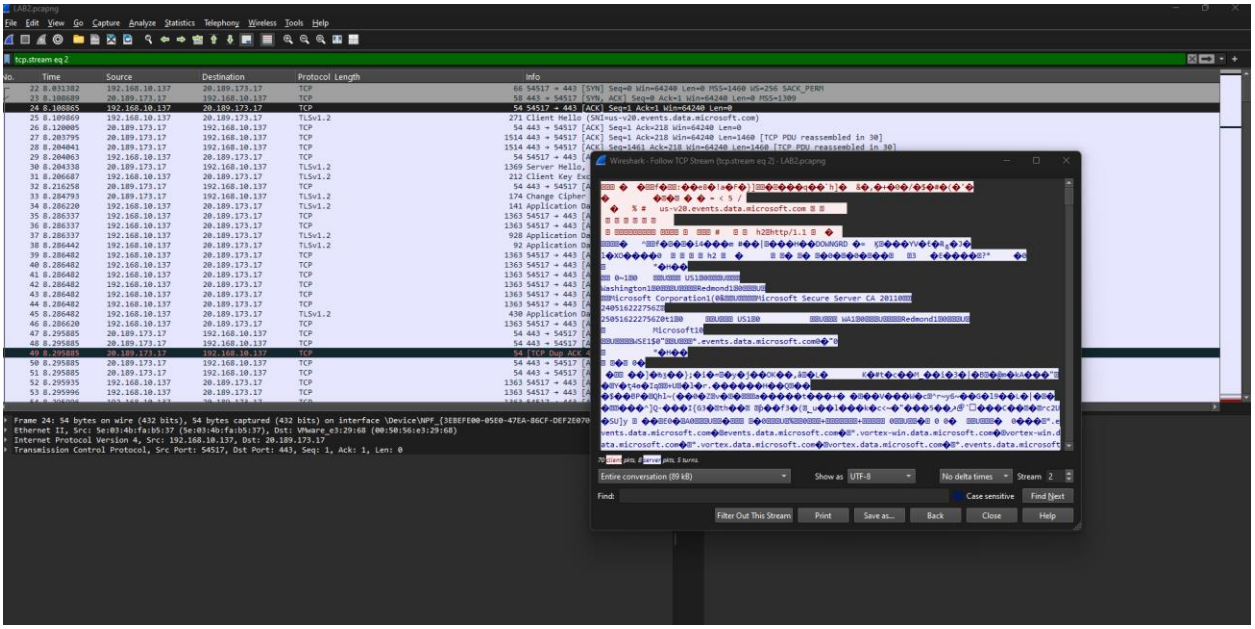
In short, DNS requests help your computer find the right address for websites so you can visit them.

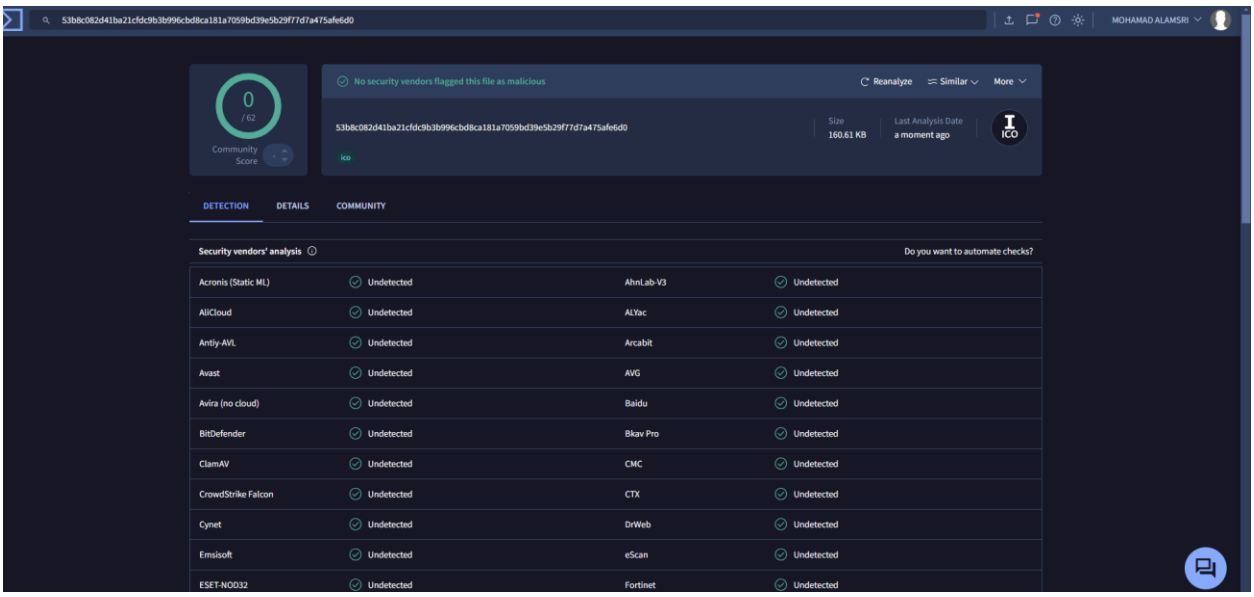




9. Identify which malware connected to which remote host








10. In a minimum of 1500 words, explain what was captured in the pcap chronologically. You explanation must include full screen screenshots with labels on them.

This is an independent activity, do not work in groups to solve the answer. Everyone needs to ru their own malware, and do their own analysis.