While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.

Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed… by you!

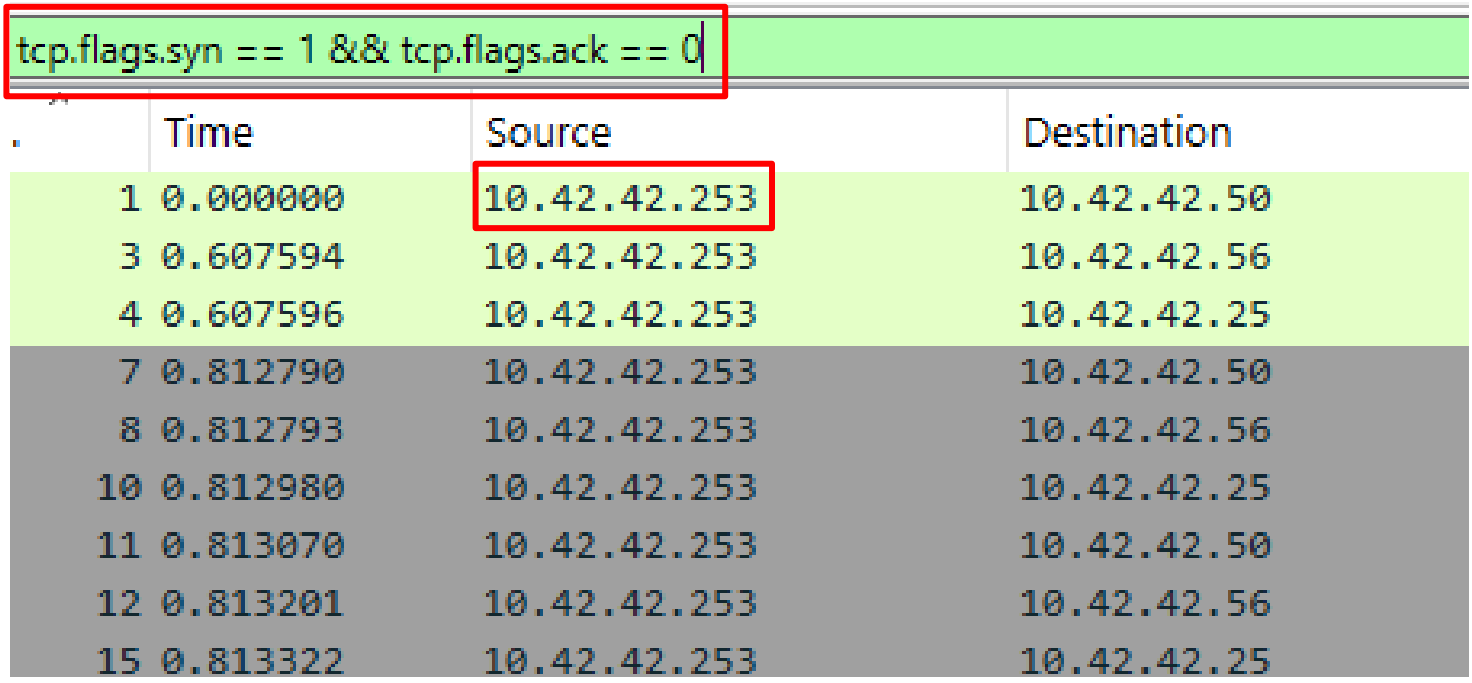
The .pcap evidence I attached to this assignment and in files directory. You must include image evidence and/or file path for every question. Each question is worth 16.66 points.

As the network forensic investigator, your mission is to answer the following questions:

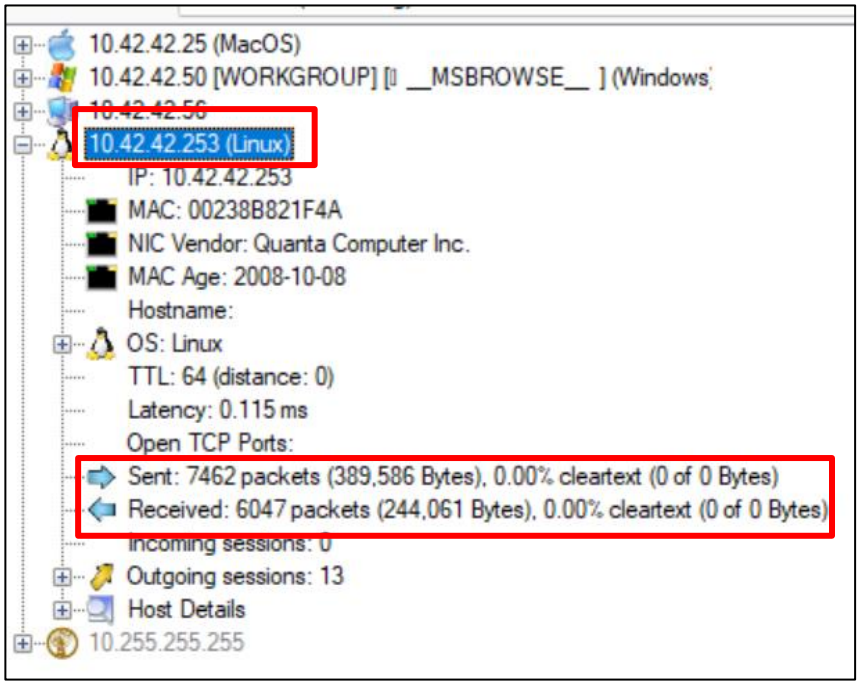
1. **What was the IP address of Mr. X's scanner?**

Answer: 10.42.42.253

- Mr. X is scanning the network to gather information, and each scanning attempt originates from his IP address. To identify his scanner, we need to locate the source of the scan traffic. Since most scans involve sending many packets to various ports on target machines, the scanner's IP address will be the source IP in those packets.
- Filter for SYN packets using **tcp.flags.syn == 1 && tcp.flags.ack == 0**. SYN packets are used to initiate TCP connections. Port scans often consist of large numbers of SYN packets sent to different destinations, as Mr. X is trying to discover open ports.
- Analyze the Source IP field in the results. The IP address that appears most frequently as the source in these packets is likely Mr. X's scanner.



- **Verify with Network Miner:**

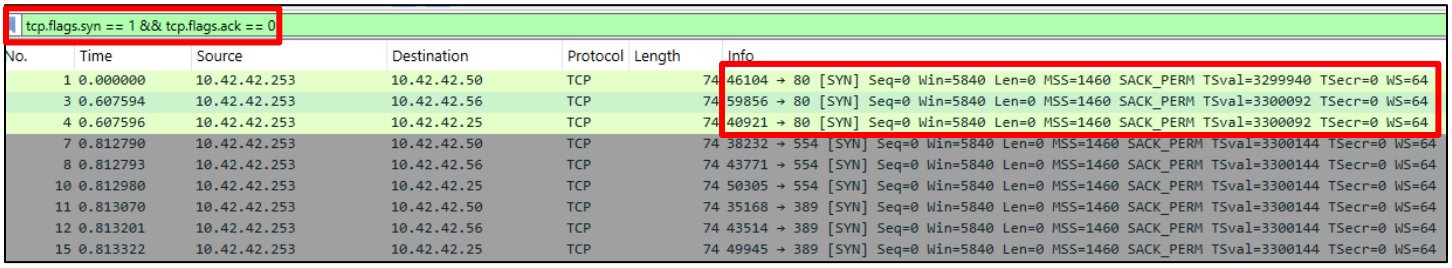


2. For the FIRST port scan that Mr. X conducted, what type of port scan was it? (Note: the scan consisted of many thousands of packets.) Pick one:

- **TCP SYN**
- **TCP ACK**
- **UDP**
- **TCP Connect**
- **TCP XMAS**
- **TCP RST**

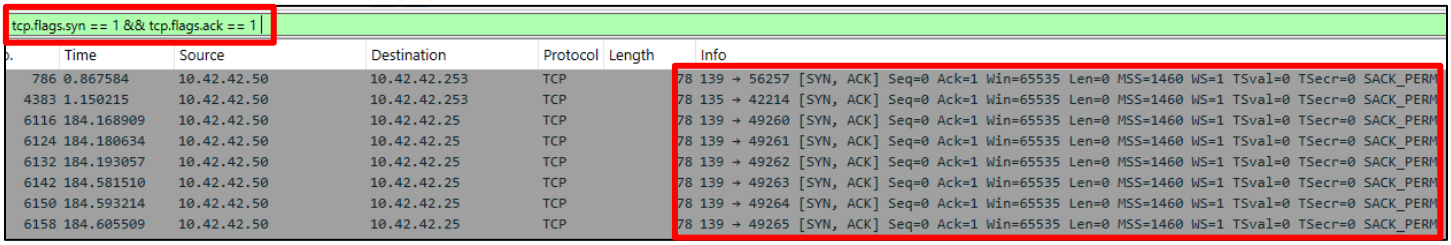
Answer: TCP Connect

Method:
Filter for SYN packets:

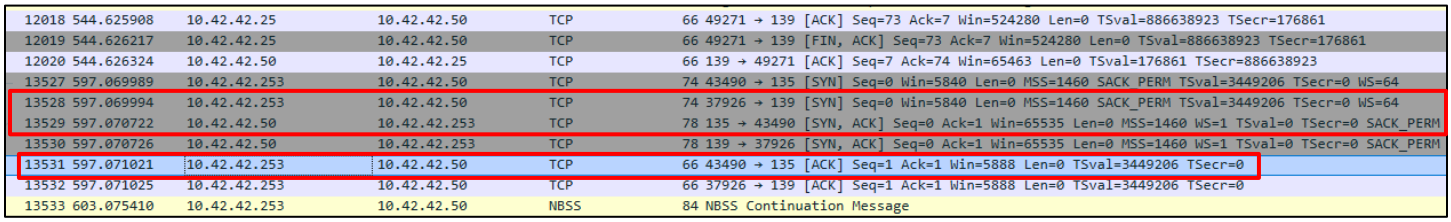


Initially, the packet capture analysis suggests a **TCP SYN** scan, as the closed port behavior is identical for both **TCP SYN** and **TCP Connect** scans. In the capture, we observe **SYN** packets being sent from the scanner **(10.42.42.253)** to the targets **(e.g., 10.42.42.50 and 10.42.42.56),** with the targets responding with **RST, ACK** packets, indicating that the ports are closed. This type of response, **SYN → RST, ACK**, is the same for both **TCP SYN** scans and **TCP** Connect scans when the ports are closed.

Filter for SYN-ACK responses:



Completing the Handshake:



However, upon closer examination, the **TCP Connect scan** completes the three-way handshake for open ports, which differentiates it from a **TCP SYN scan**. In a **TCP SYN scan**, the connection is terminated with an **RST** after receiving a **SYN-ACK** from an open port, without completing the handshake. But in a **TCP Connect scan**, the scanner sends an **ACK** to complete the handshake, establishing a full connection.

Thus, since the three-way handshake is completed for open ports, confirming a full connection, we can conclude that Mr. X performed a **TCP Connect scan**.

3. What were the IP addresses of the targets Mr. X discovered?

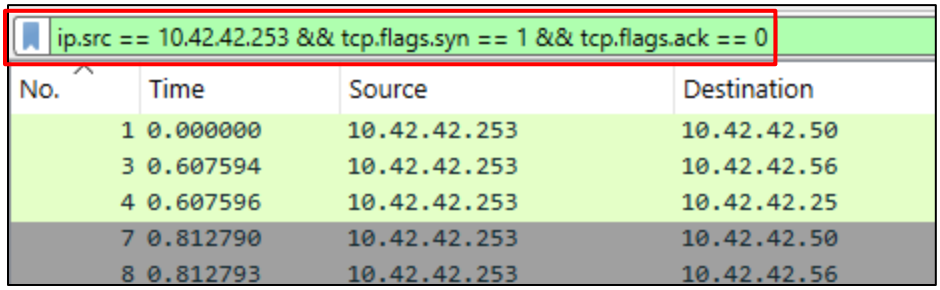
Answer: 10.42.42.25, 10.42.42.50 and 10.42.42.56

Method:

To answer this, we need to analyze the **targets** Mr. X scanned and interacted with during his reconnaissance. This involves identifying which IP addresses responded to Mr. X's scanning activity, particularly with SYN-ACK responses, indicating open ports.

Step 1: Filter SYN Packets Sent by Mr. X

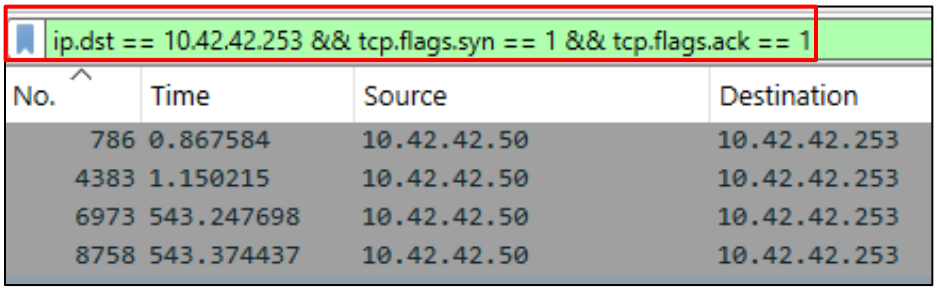
Since we already know Mr. X's IP address (10.42.42.253), the first step is to filter all **SYN packets** he sent during the scan. This will give us a list of all the IP addresses he attempted to connect to. Apply this filter to show all SYN packets Mr. X sent:



Step 2: Filter SYN-ACK Responses from Target IPs

To identify the IP addresses of the systems that responded to Mr. X's scan, you need to check for SYN-ACK packets sent to Mr. X. A SYN-ACK response indicates that the target's port is open and responding to the scan.

Apply this filter to display SYN-ACK responses sent to Mr. X:



Conclusion:

The IP addresses of the targets Mr. X discovered are: **10.42.42.25, 10.42.42.50** and **10.42.42.56**

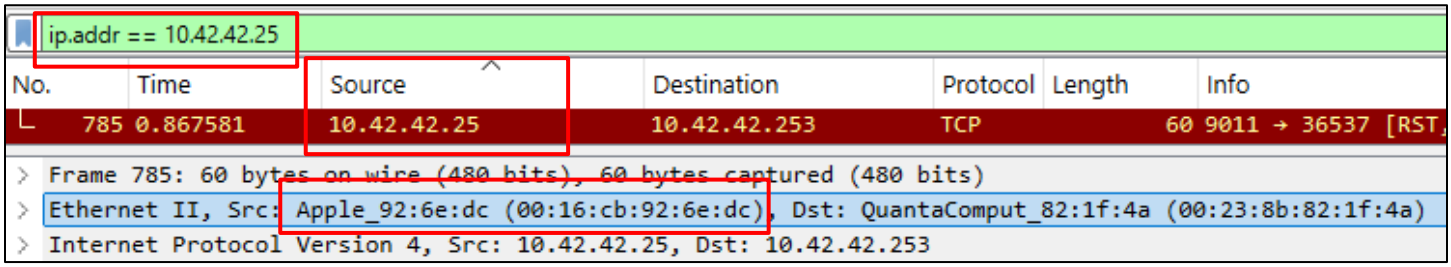
Even though only **10.42.42.50** responded with an acknowledgment (ACK), Mr. X sent SYN packets to all three, meaning they were all discovered as potential targets during the scan.

4. What was the MAC address of the Apple system he found?

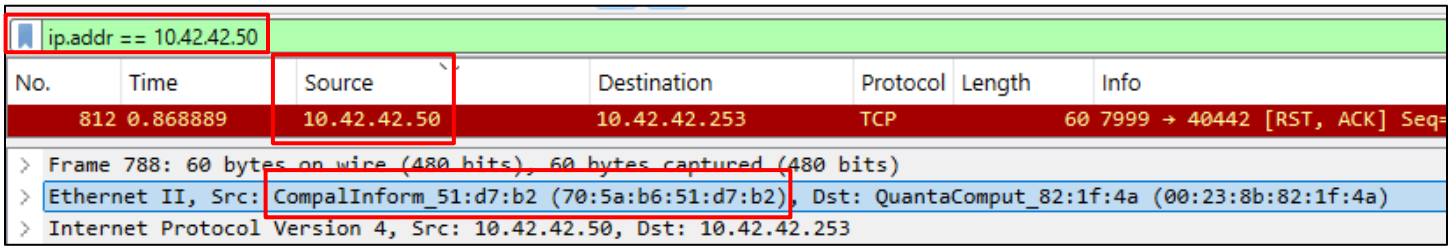
Answer: IP Address: 10.42.42.25 and Mac Address: (00: 16 : cb : 92 : 6e : dc)
Method:

Checking discovered IP Address packets and finding devices:

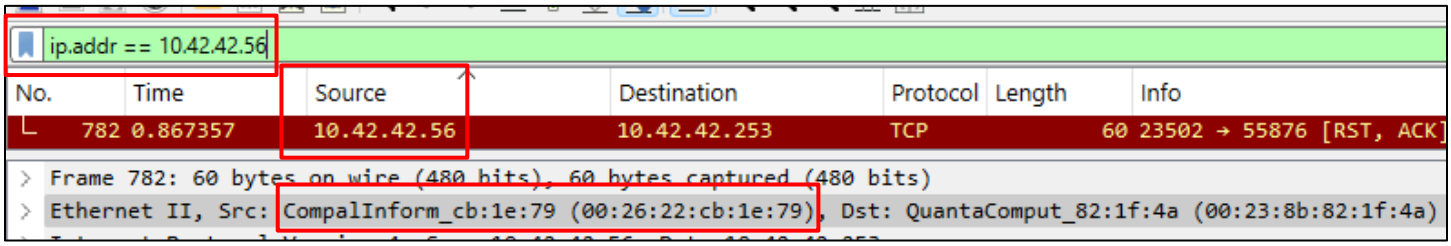
IP Address: 10.42.42.25



IP Address: 10.42.42.50



IP Address: 10.42.42. 56

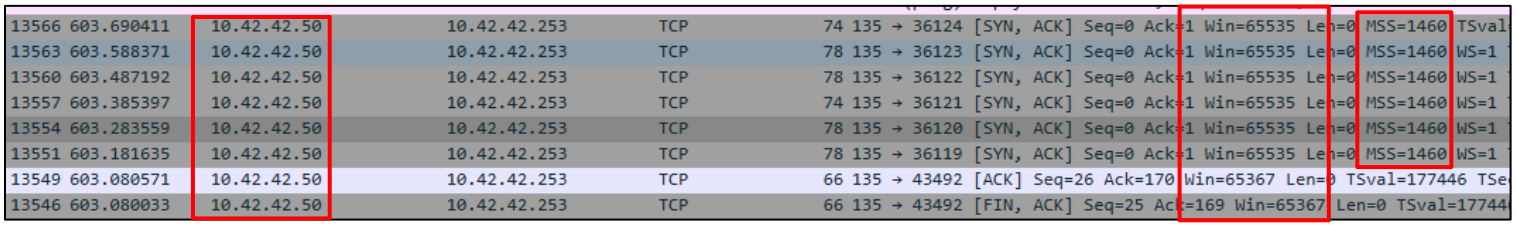


5. What was the IP address of the Windows system he found?

Answer: 10.42.42.50

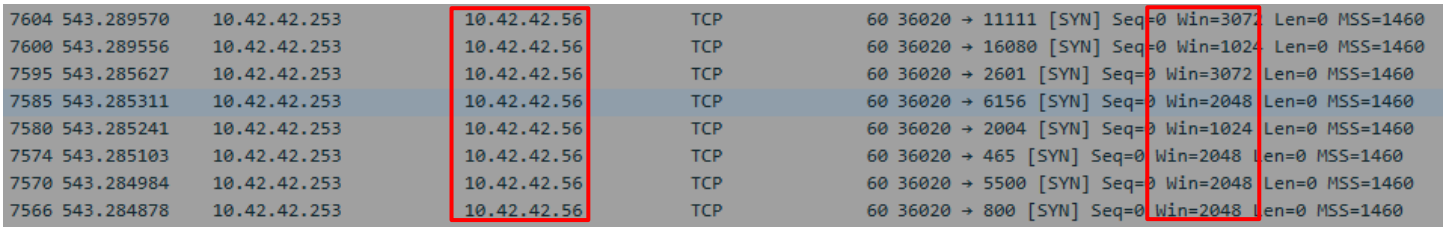
Method:

We are checking the Headers of packets:
IP Address: 10.42.42.50



- **Window Size (65535)** for the packets from **10.42.42.50**.
- The packets are **TCP SYN/ACK** and **ACK**, indicating responses to connection requests from **10.42.42.50**.
- **Window Scaling (WS) = 1**, commonly seen in Windows configurations.
- **65367** is a relatively large window size, very close to **65535**, which is commonly seen in Windows configurations. The difference could be due to slight adjustments in the network conditions, but it's still within the range associated with Windows machines.
- **TCP window size changes dynamically** as data is transmitted, which explains why it might slightly decrease from the initial **65535** to **65367** in the middle of the connection. This is normal behavior and does not change the classification of the operating system.

IP Address: 10.42.42.56



In this image, the IP **10.42.42.56** is involved in multiple TCP connections with **10.42.42.253**. The window sizes shown in the packets are significantly smaller, and there are multiple values:
Window Sizes (Win): **3072** / **2048** /**1024**
These window sizes are quite small and deviate from what we typically see in Windows systems, which usually have larger default window sizes (like 65535 or 65367, as seen previously). Instead, these smaller window sizes are characteristic of **Linux/Unix-based** systems or non-Windows devices, where lower initial window sizes can sometimes be observed depending on system configuration and network optimization.

- **10.42.42.50**: Likely **Windows** based on the larger window sizes (65535, 65367).
- **10.42.42.56**: Likely **Linux/Unix-based** based on the smaller window sizes (5840, 3072, 2048, 1024).

6. What TCP ports were open on the Windows system? (Please list the decimal numbers from lowest to highest.)

Answer:

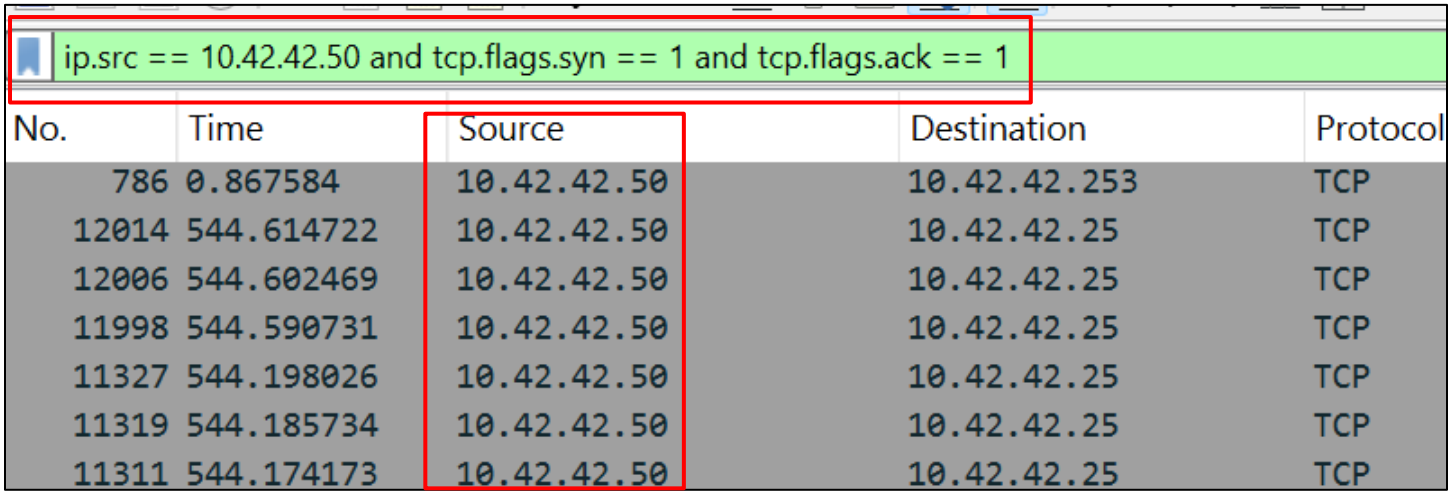
135

139

Method:

To identify open ports, you need to focus on the **SYN-ACK** packets sent by 10.42.42.50, which indicate that the server at this IP is responding to connection requests (indicating the ports are open).

- **ip.src == 10.42.42.50**: Filters packets where the source IP is 10.42.42.50.
- **tcp.flags.syn == 1**: Ensures that the packet is part of the TCP handshake (SYN flag is set).
- **tcp.flags.ack == 1**: Ensures that the ACK flag is also set, which is typical for a SYN-ACK response.

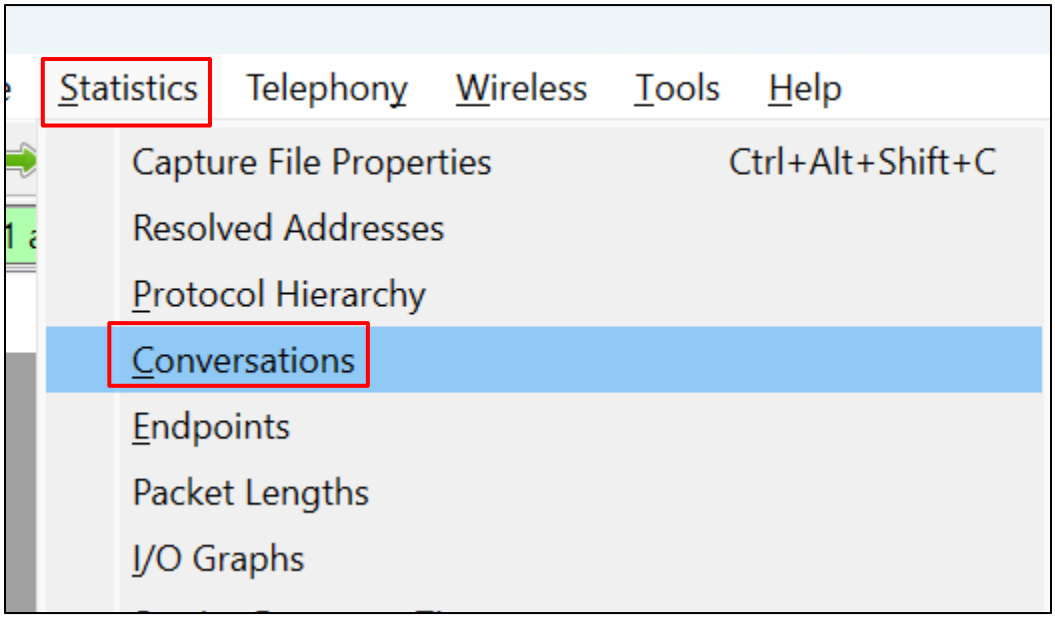


The filter is designed to identify TCP three-way handshakes, which are a crucial part of establishing a TCP connection.

After this, we can simply Statistics > Conversations.

In the TCP tab, look for the IP address `10.42.42.50` under the "Address A" or "Address B" columns.

This will give you a list of conversations, and you can identify the destination ports involved in these conversations.



Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 27 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	B
10.42.42.25	49260	10.42.42.50	139	1	78 bytes	3378	8	12.50%	0	
10.42.42.25	49261	10.42.42.50	139	1	78 bytes	3379	8	12.50%	0	
10.42.42.25	49262	10.42.42.50	139	1	78 bytes	3380	8	12.50%	0	
10.42.42.25	49263	10.42.42.50	139	1	78 bytes	3381	8	12.50%	0	
10.42.42.25	49264	10.42.42.50	139	1	78 bytes	3382	8	12.50%	0	
10.42.42.25	49265	10.42.42.50	139	1	78 bytes	3383	8	12.50%	0	
10.42.42.25	49266	10.42.42.50	139	1	78 bytes	5990	8	12.50%	0	
10.42.42.25	49267	10.42.42.50	139	1	78 bytes	5991	8	12.50%	0	
10.42.42.25	49268	10.42.42.50	139	1	78 bytes	5992	8	12.50%	0	
10.42.42.25	49269	10.42.42.50	139	1	78 bytes	6404	8	12.50%	0	
10.42.42.25	49270	10.42.42.50	139	1	78 bytes	6405	8	12.50%	0	
10.42.42.25	49271	10.42.42.50	139	1	78 bytes	6406	8	12.50%	0	
10.42.42.253	36020	10.42.42.50	139	1	60 bytes	3780	3	33.33%	0	
10.42.42.253	36020	10.42.42.50	135	1	60 bytes	4708	3	33.33%	0	
10.42.42.253	36119	10.42.42.50	135	1	78 bytes	7416	3	33.33%	0	

Ports 135 and 139 on 10.42.42.50 are confirmed open, as SYN-ACK packets were detected, indicating active services on these ports.