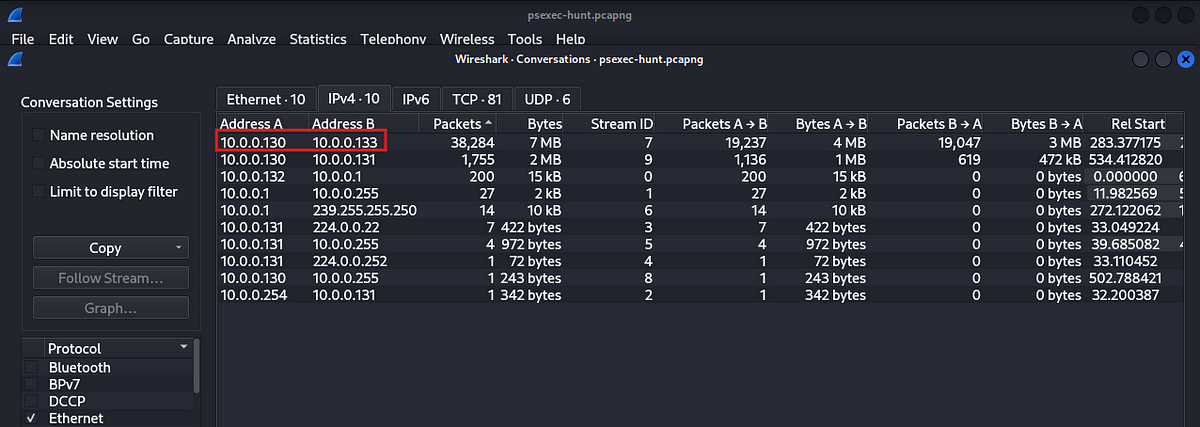
### **PsExec Hunt — Cyberdefenders**

Scenario: An alert from the Intrusion Detection System (IDS) flagged suspicious lateral movement activity involving PsExec. This indicates potential unauthorized access and movement across the network. As a SOC Analyst, your task is to investigate the provided PCAP file to trace the attacker’s activities. Identify their entry point, the machines targeted, the extent of the breach, and any critical indicators that reveal their tactics and objectives within the compromised environment.

Tasks:

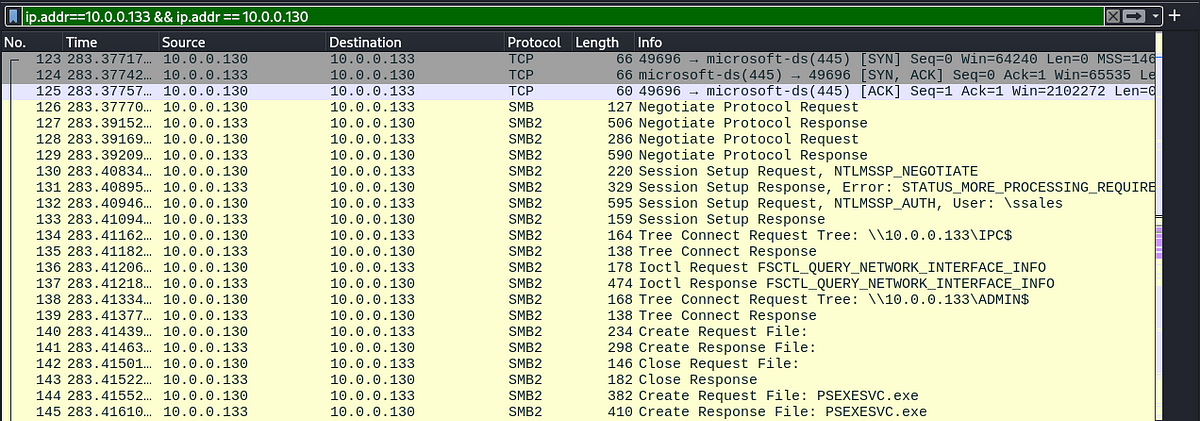
1. To effectively trace the attacker’s activities within our network, can you identify the IP address of the machine from which the attacker initially gained access?

Let us check the conversation statistics to see any unusual amount of traffic being sent. Statistics -> Conversations -> IPv4



We can see that two IP addresses are contributing the most traffic, let us examine them more closely.

Filter: ip.addr == 10.0.0.130 && ip.addr == 10.0.0.133

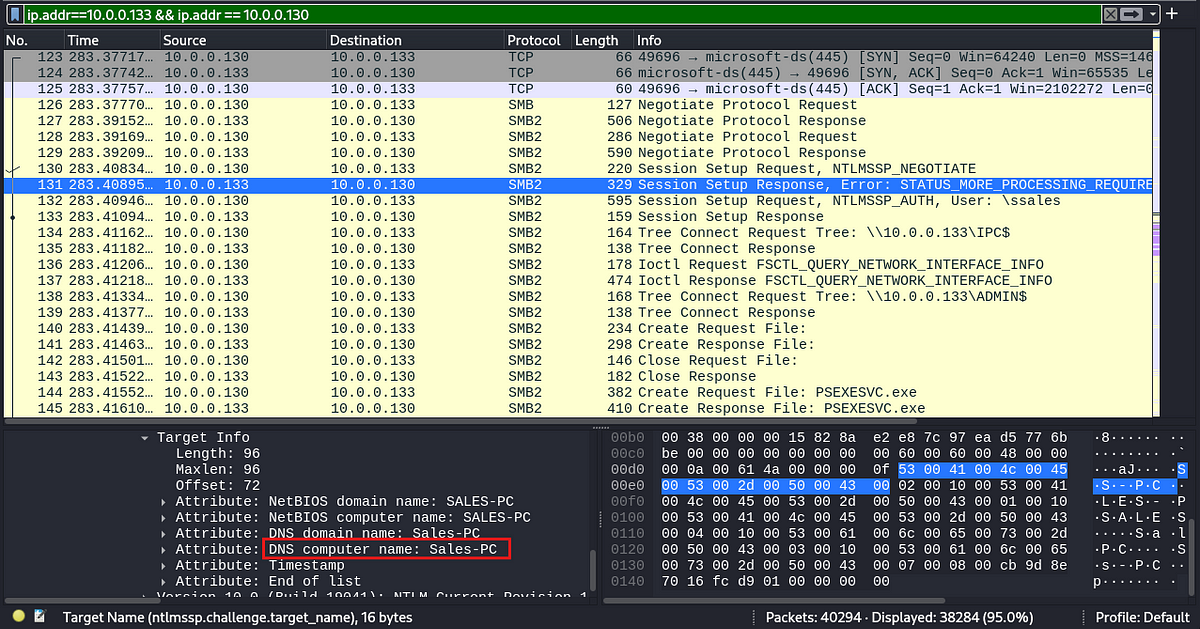


We, can see that the IP address 10.0.0.130 connected to the IP address 10.0.0.133 and created a file called PSEXESVC.EXE which is the service component of the PSEXEC utility.

Answer: 10.0.0.130

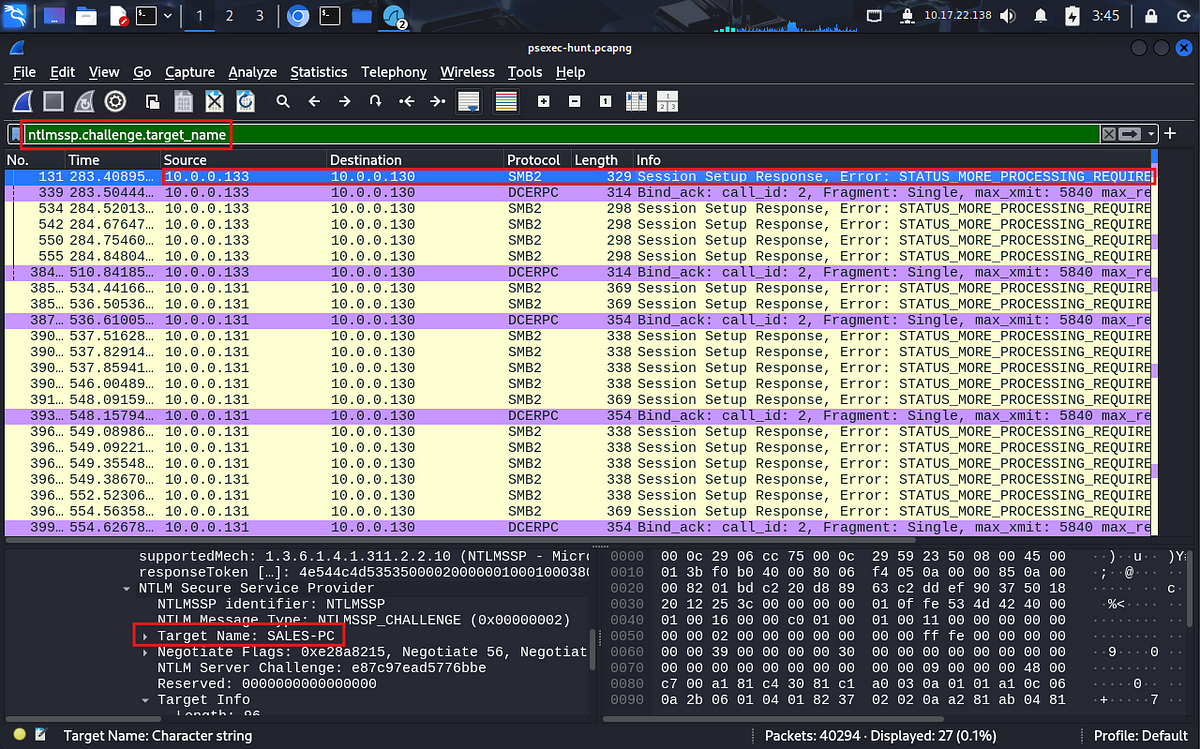
2. To fully understand the extent of the breach, can you determine the machine’s hostname to which the attacker first pivoted?

In the above screenshot, we can see session setup requests from the attacker IP, if we check the details of these packets, we can fing the hostname of the attacker.



Alternatively, we can search specifically for NTLMSSP(NT LAN Manager Security Support Provider) which is commonly used in Windows environments for challenge-response authentication. This protocol authenticates the users accessing the network resources. In NTLMSSP challenge response the client will share the information in order to authenticate them. So we will be able to look for the details about the sender in a challenge response packet.

Filter: ntlmssp.challenge.target\_name

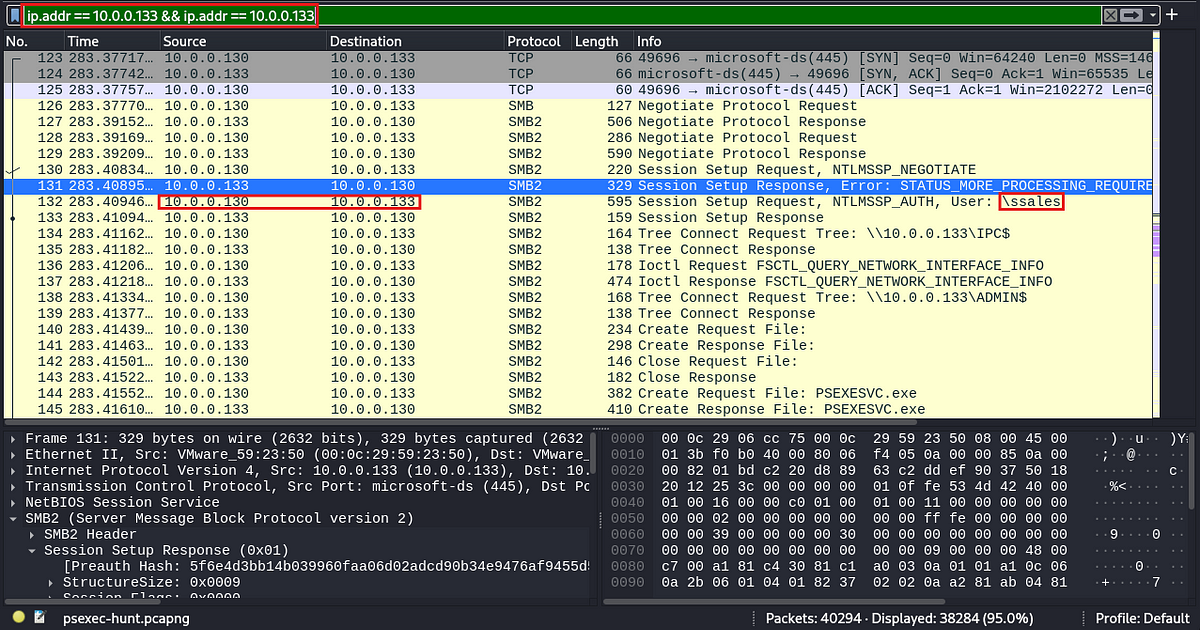


Answer: SALES -PC

3. Knowing the username of the account the attacker used for authentication will give us insights into the extent of the breach. What is the username utilized by the attacker for authentication?

Let us go back to the previous filter

ip.addr == 10.0.0.133 && ip.addr == 10.0.0.130

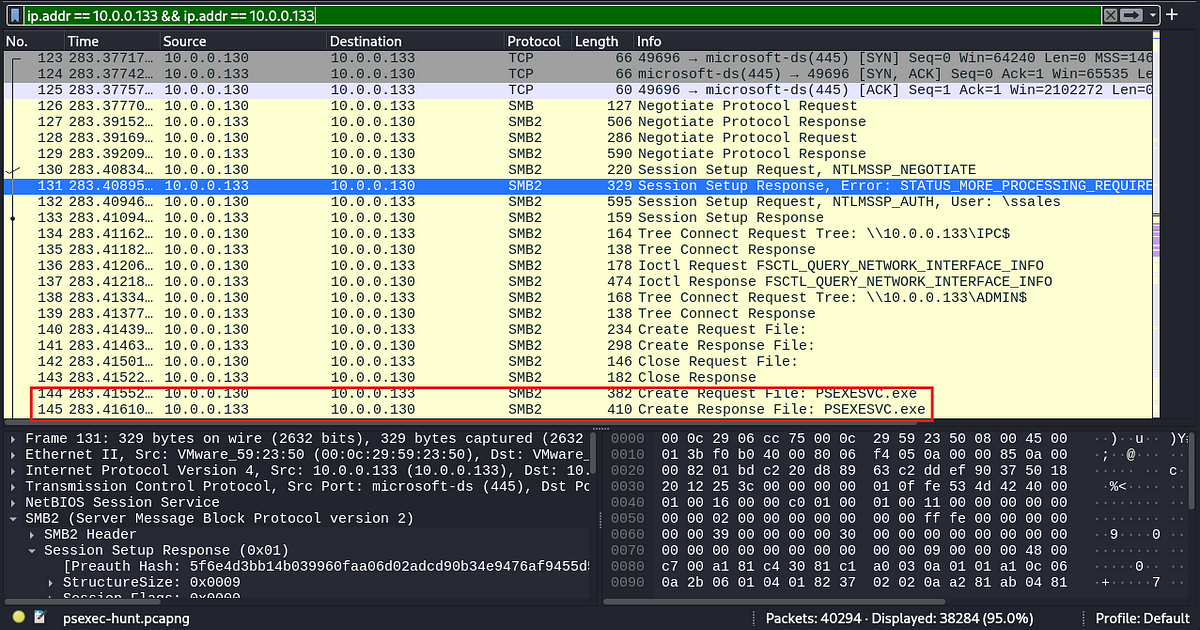


We can see above that the attacker, requested access with the username ssales

Answer: ssales

4. After figuring out how the attacker moved within our network, we need to know what they did on the target machine. What’s the name of the service executable the attacker set up on the target?

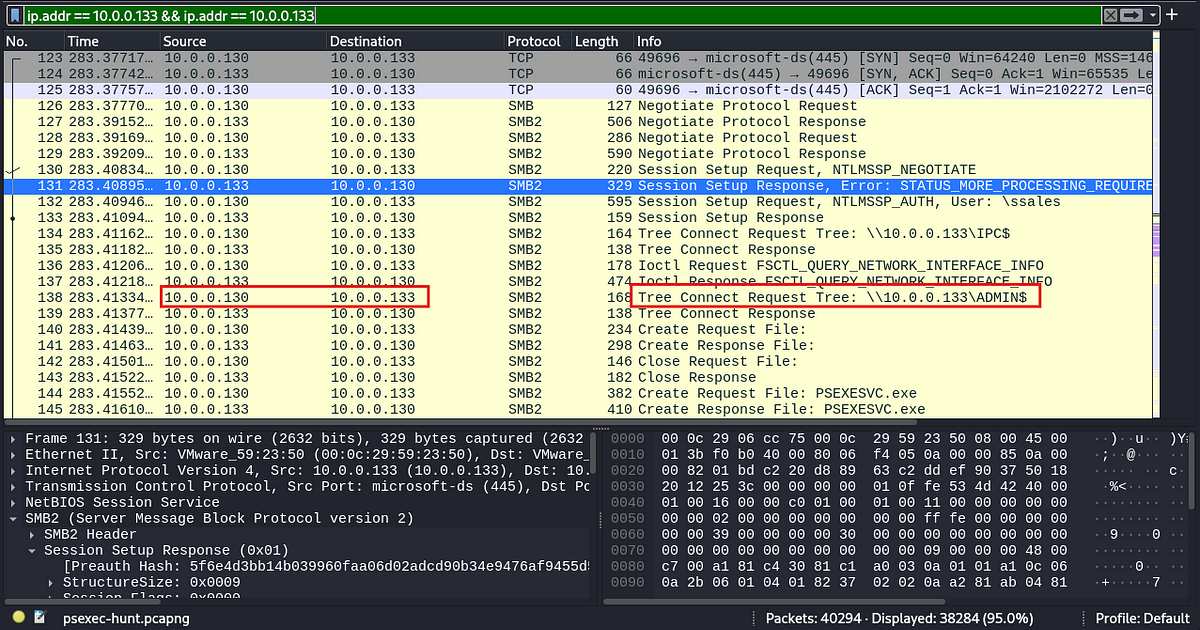
Few packets later the attacker requested to create a file called PSEXESVC.exe, which I explained earlier



Answer: PSEXESVC

5. We need to know how the attacker installed the service on the compromised machine to understand the attacker’s lateral movement tactics. This can help identify other affected systems. Which network share was used by PsExec to install the service on the target machine?

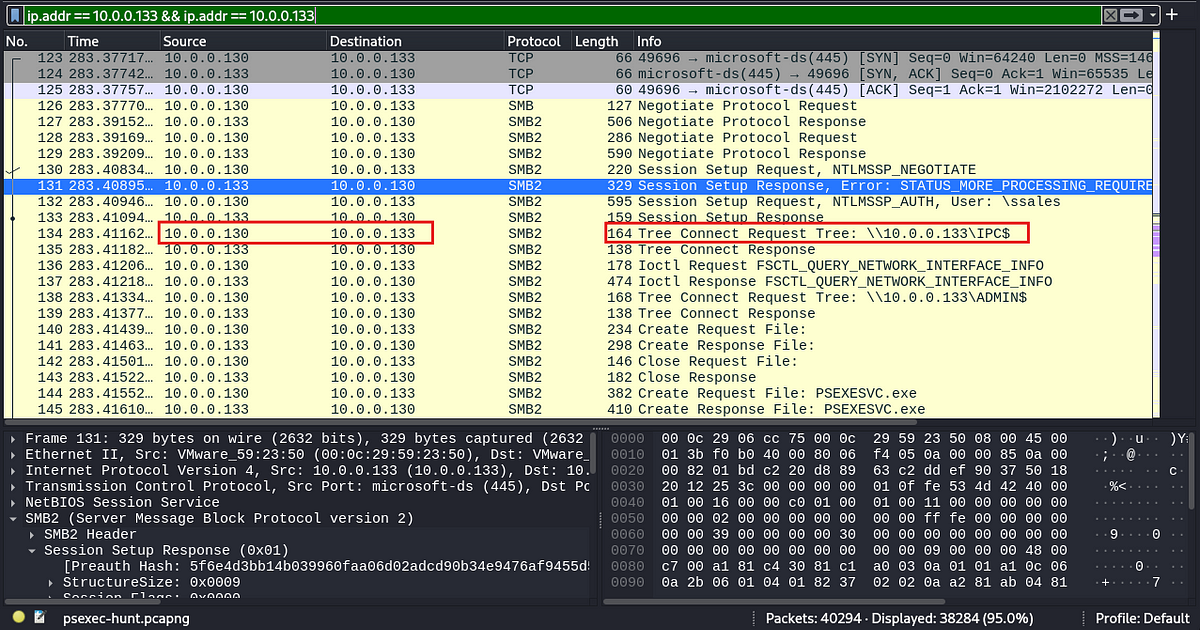
This can also be seen in the above screenshot, the attacker has requested for a tree connect on ADMIN$ which is a special share which will grant admin privileges to the server’s file system



Answer: ADMIN$

6. We must identify the network share used to communicate between the two machines. Which network share did PsExec use for communication?

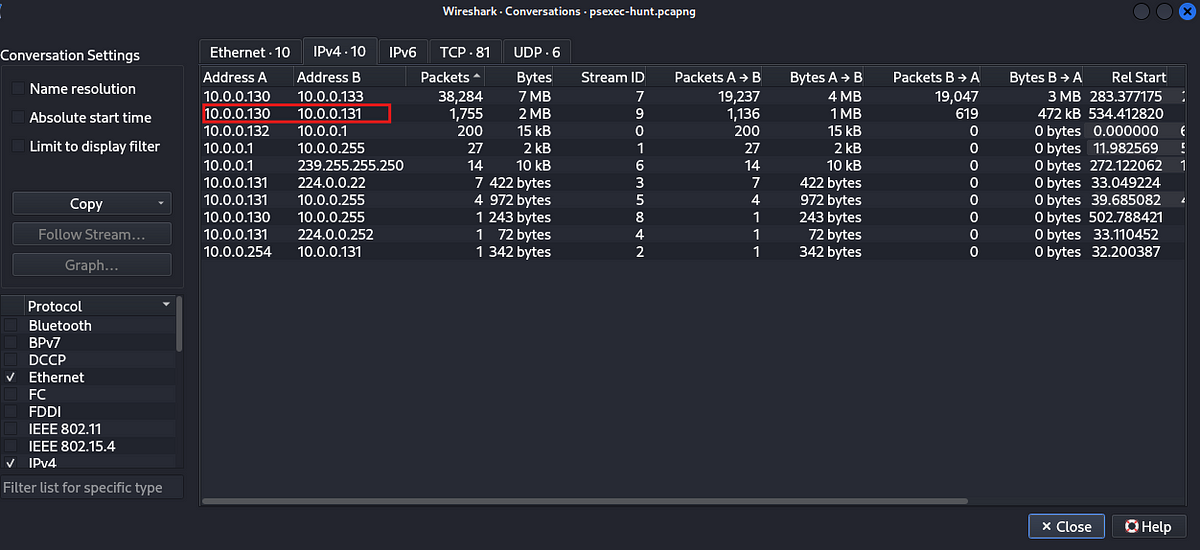
Few lines above this packet, we can see a tree connect request to IPC$. IPC stands for Inter-Process Communication, this is a special share which will allow two processes to communicate witheach other.



Answer: IPC$

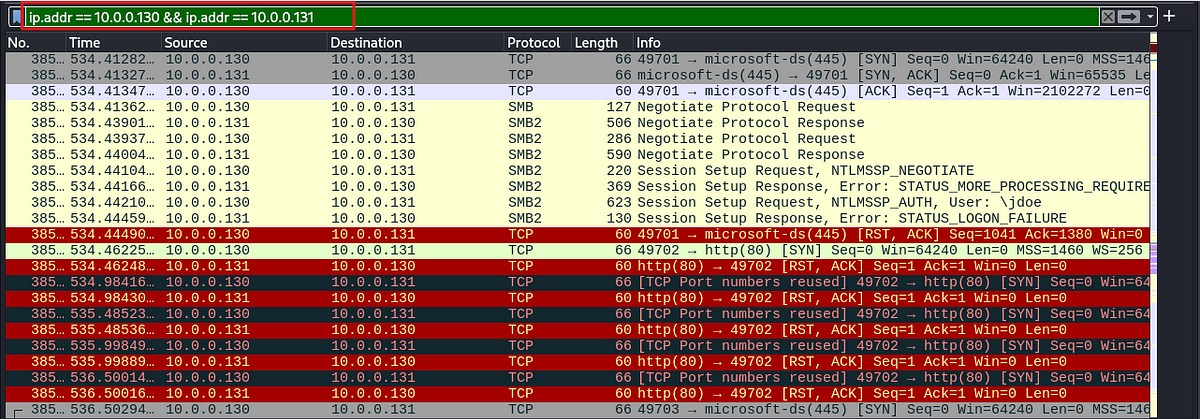
7. Now that we have a clearer picture of the attacker’s activities on the compromised machine, it’s important to identify any further lateral movement. What is the hostname of the second machine the attacker targeted to pivot within our network?

In the conversations tab, the attacker IP had the aecond most conversations with the IP 10.0.0.131

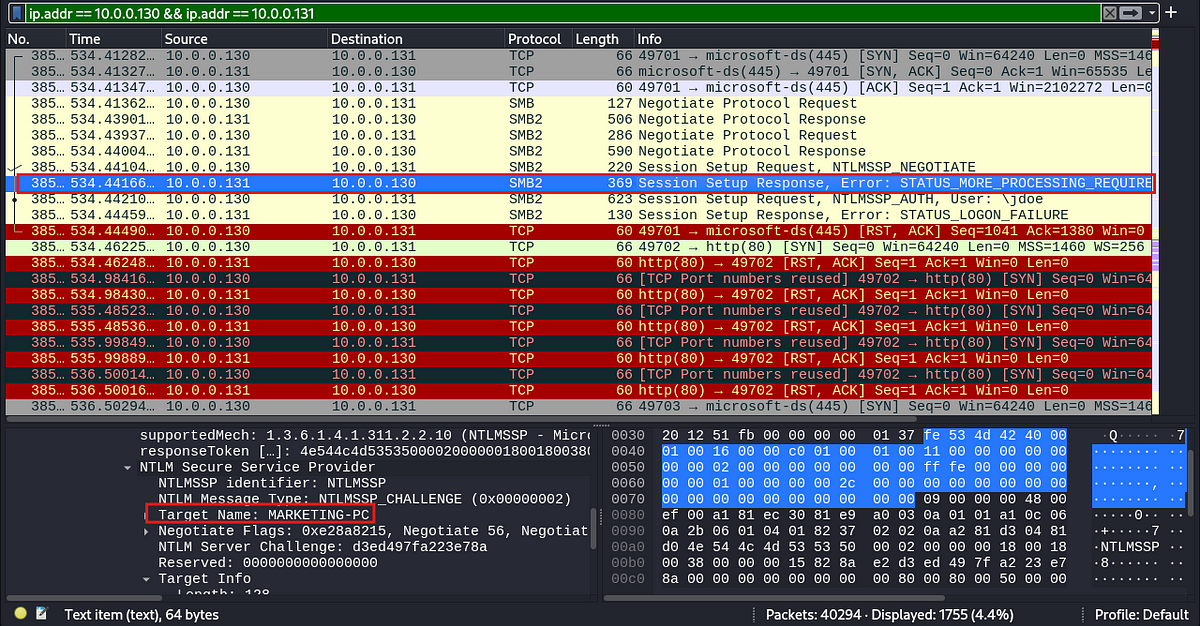


Let us check the conversation between these two IP’s

Filter : ip.addr == 10.0.0.130 && ip.addr == 10.0.0.131



Now, let us check the NTLMSSP newgotioation packets to see the name of this system.



Answer: MARKETING\_PC

This is the end of the walkthrough.