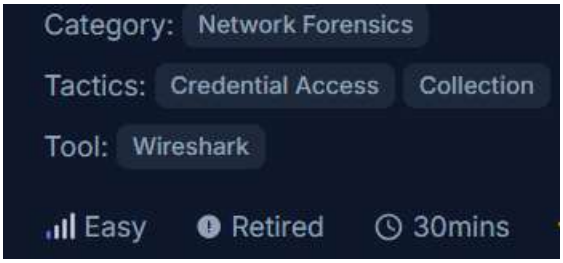
PoisonedCredentials Lab

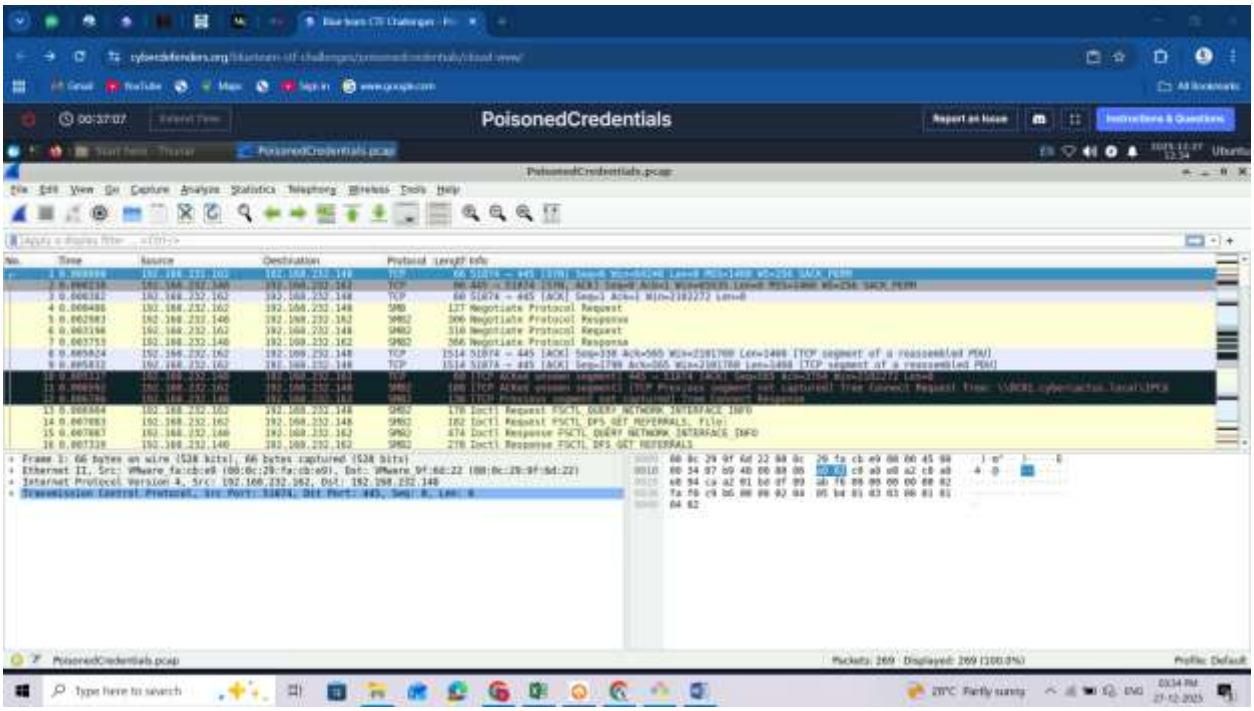
Analyze network traffic for LLMNR/NBT-NS poisoning attacks using Wireshark to identify the rogue machine, compromised accounts, and affected systems.



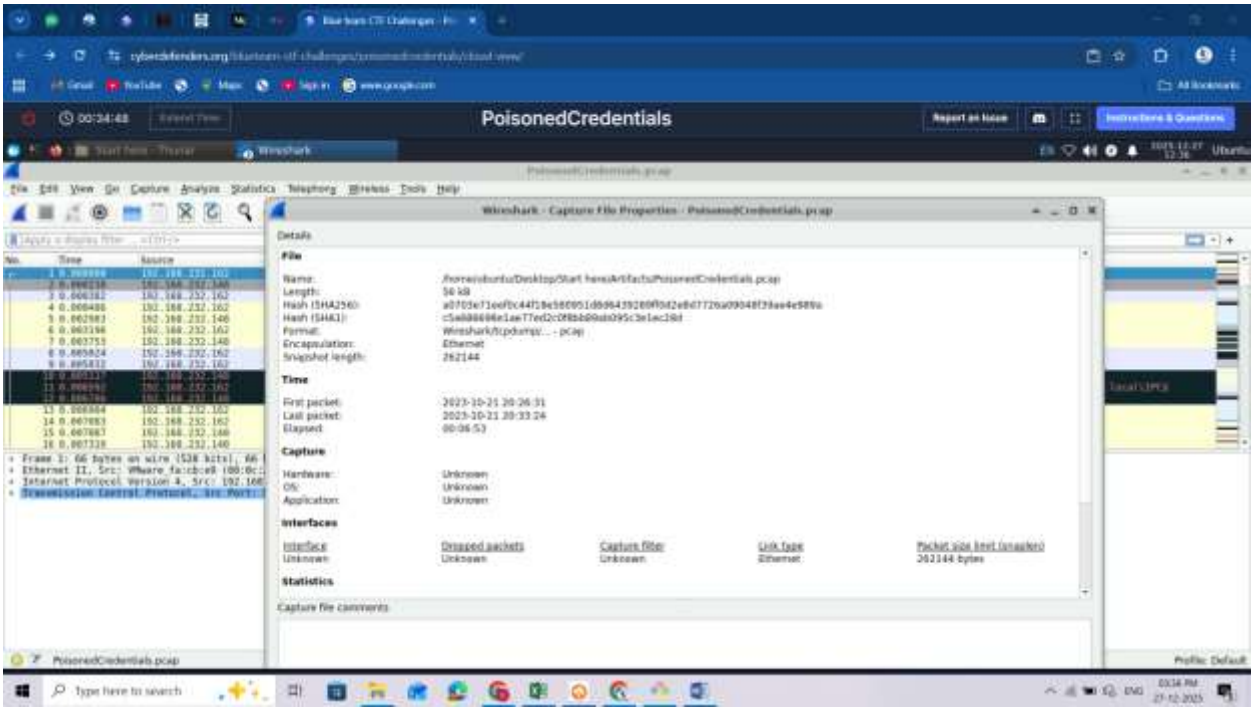
Scenario

Your organization's security team has detected a surge in suspicious network activity. There are concerns that LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) poisoning attacks may be occurring within your network. These attacks are known for exploiting these protocols to intercept network traffic and potentially compromise user credentials. Your task is to investigate the network logs and examine captured network traffic.

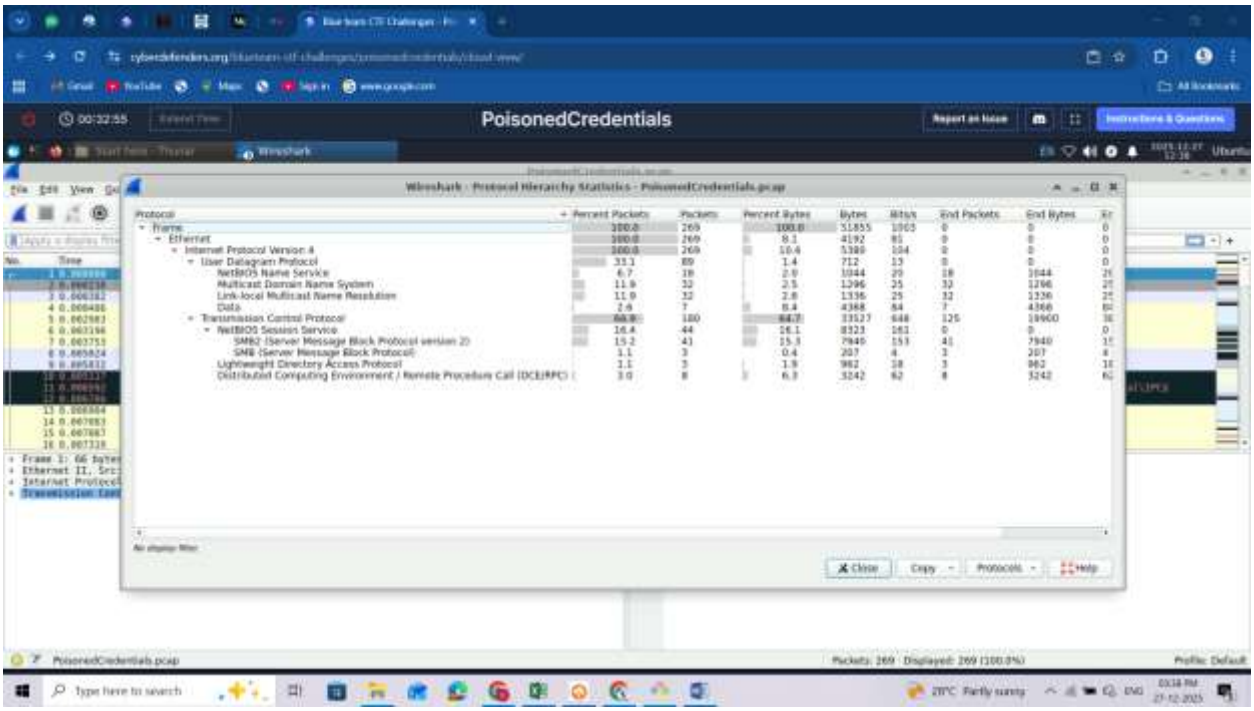
1. Open Wireshark from the folder provided on the desktop and load the pcap file



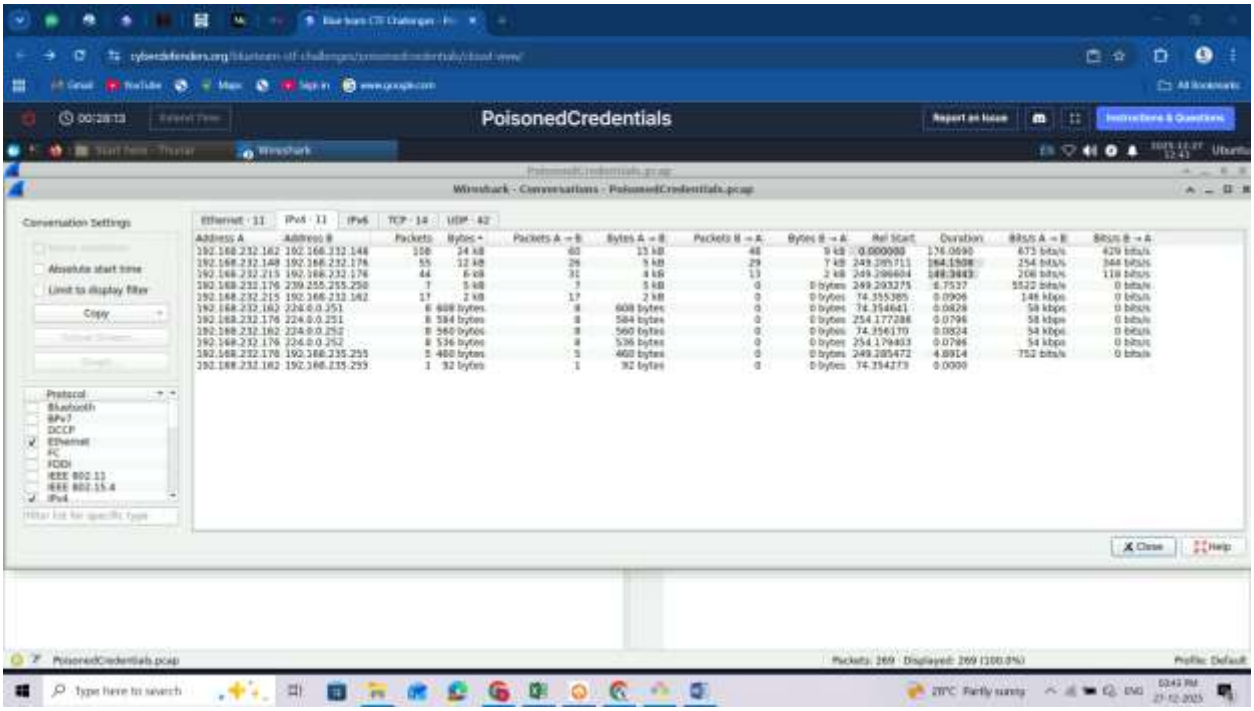
Check the pcap file properties: On the top Click on **Statistics** then click on **Capture file Properties**



Check the Protocols that exist in the PCAP file: **Statistics -> Protocol Hierarchy Statistics**

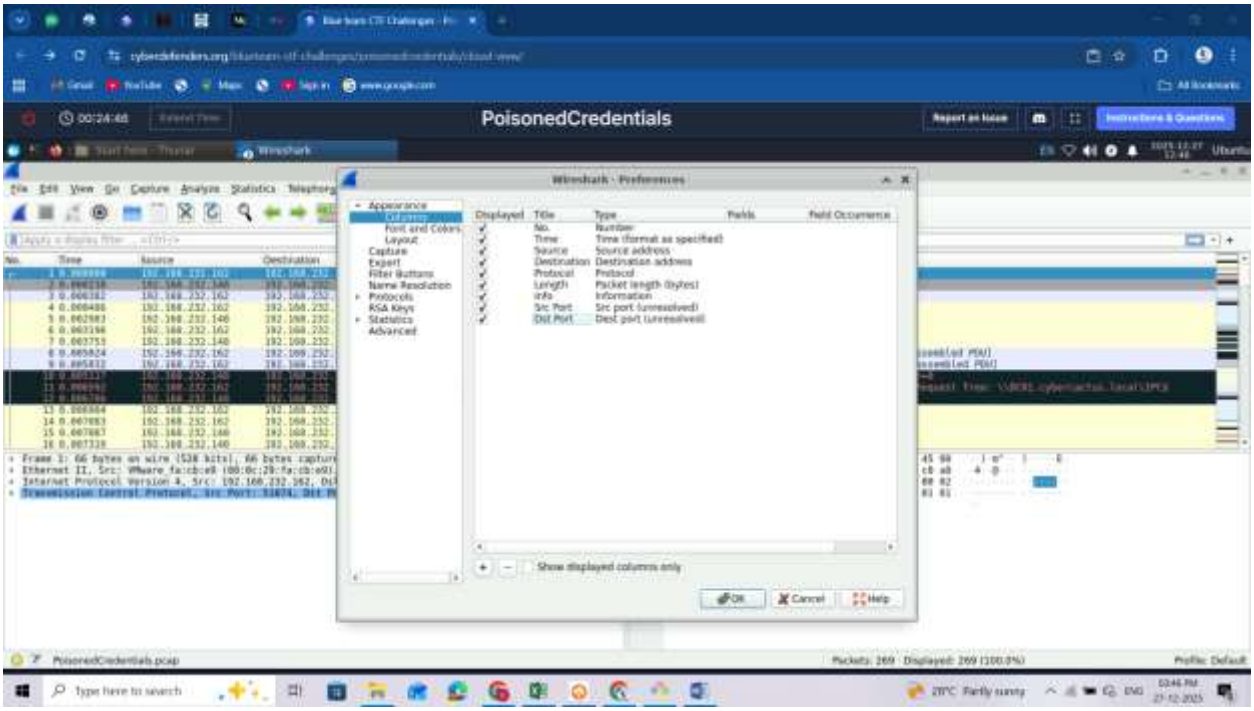


Check the Conversations: **statistics->conversations:** sort by bytes: top bytes at the top and the conversations currently btn endpoints.we will understand further in the section why the 1st endpoints have the largest convos.

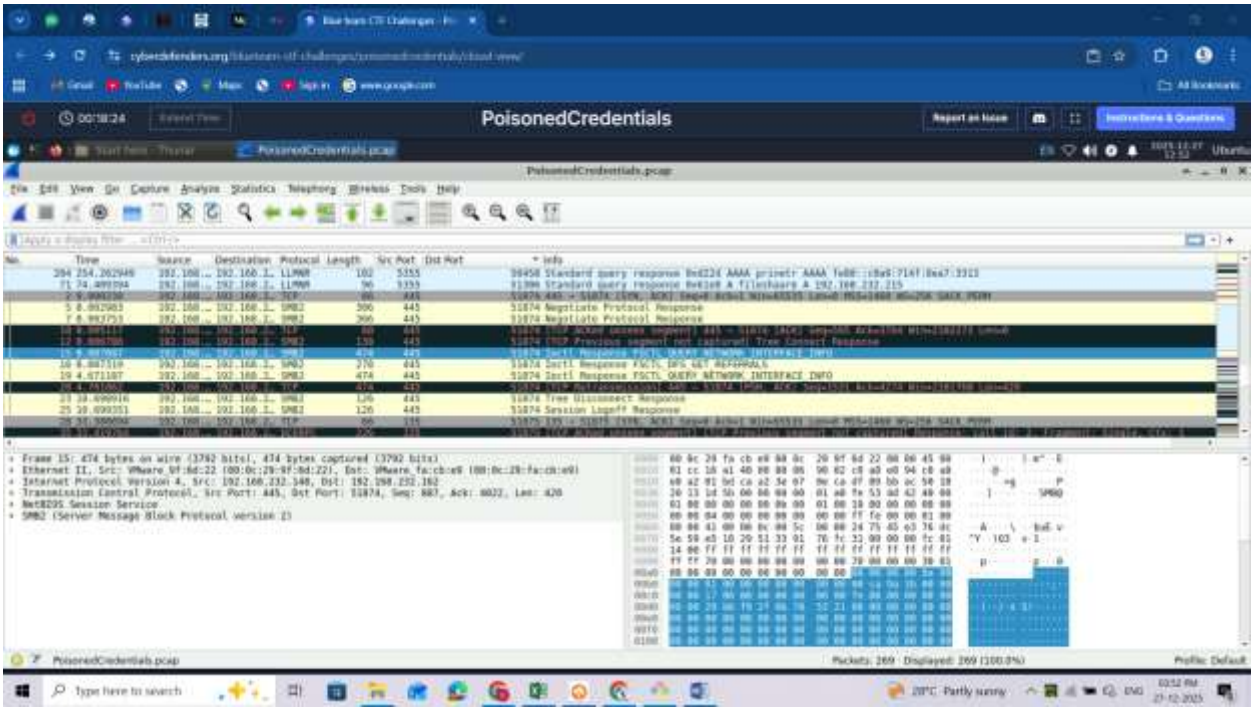


Add your preferences: Click on **Edit -> Preferences -> Columns -> click the + SIGN -> add dst and src port -> Click OK**

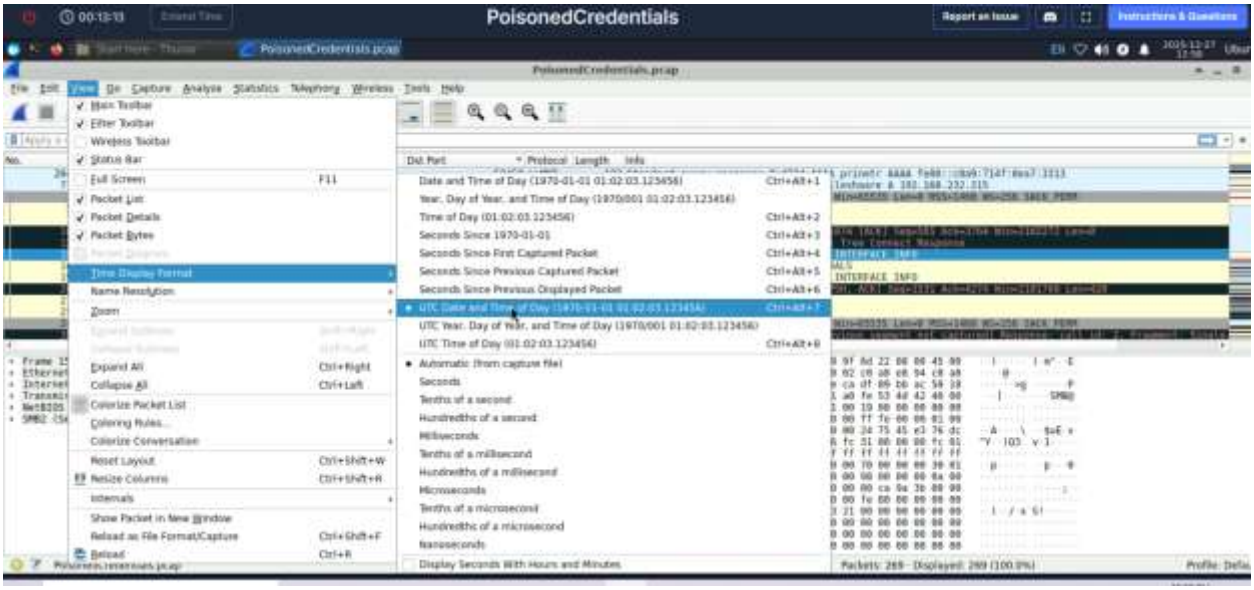
These will help you see the src and dst port at a glance within your capture view.



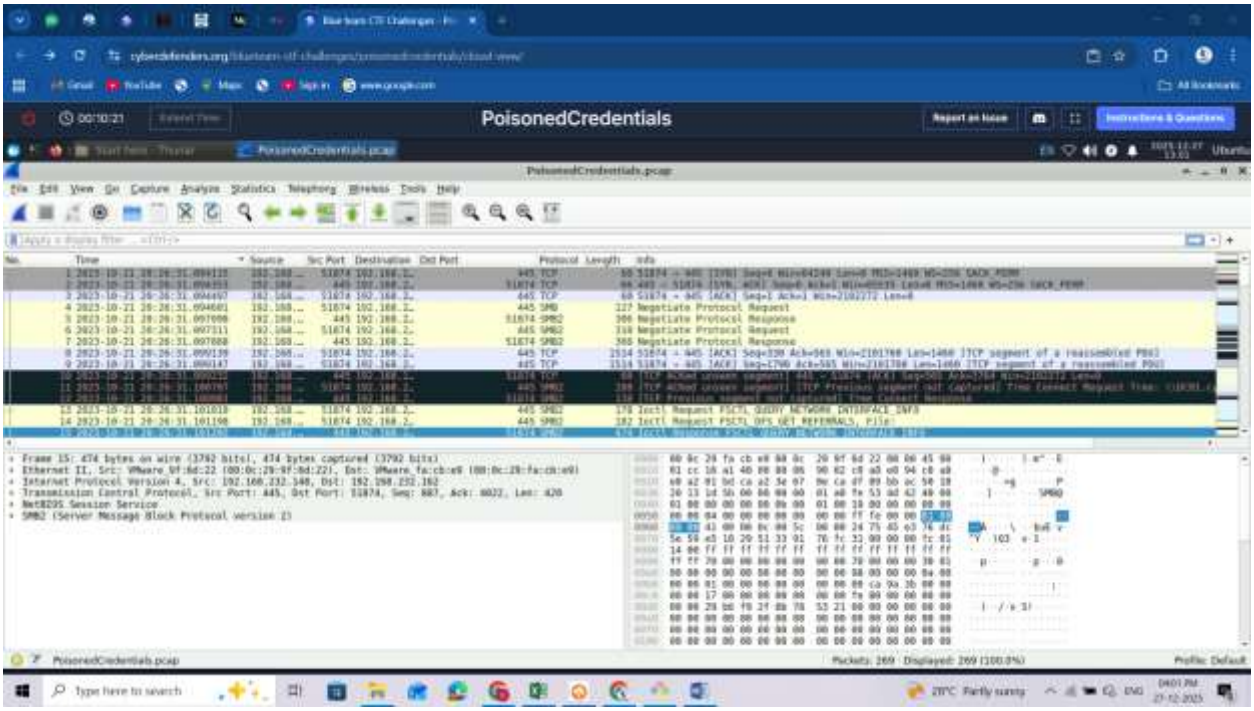
They should now be added on your table on the far right hand side, you might be unable to see them so you minimize each column to move them closer:



You can change your time display to preferred format suitable for you, in my case I used **UTC Date and Time of day** display though lengthy is a lot presentable.



You can also sort your packet properly by clicking on no. column

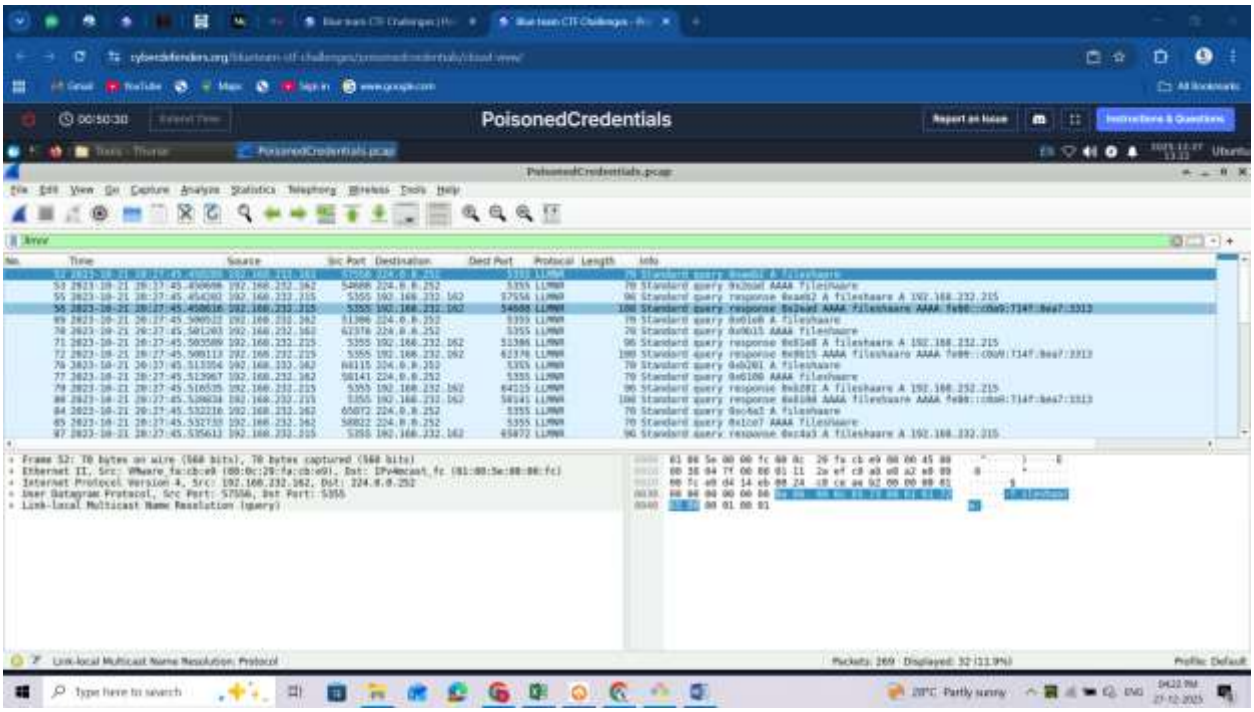


Start your analysis:

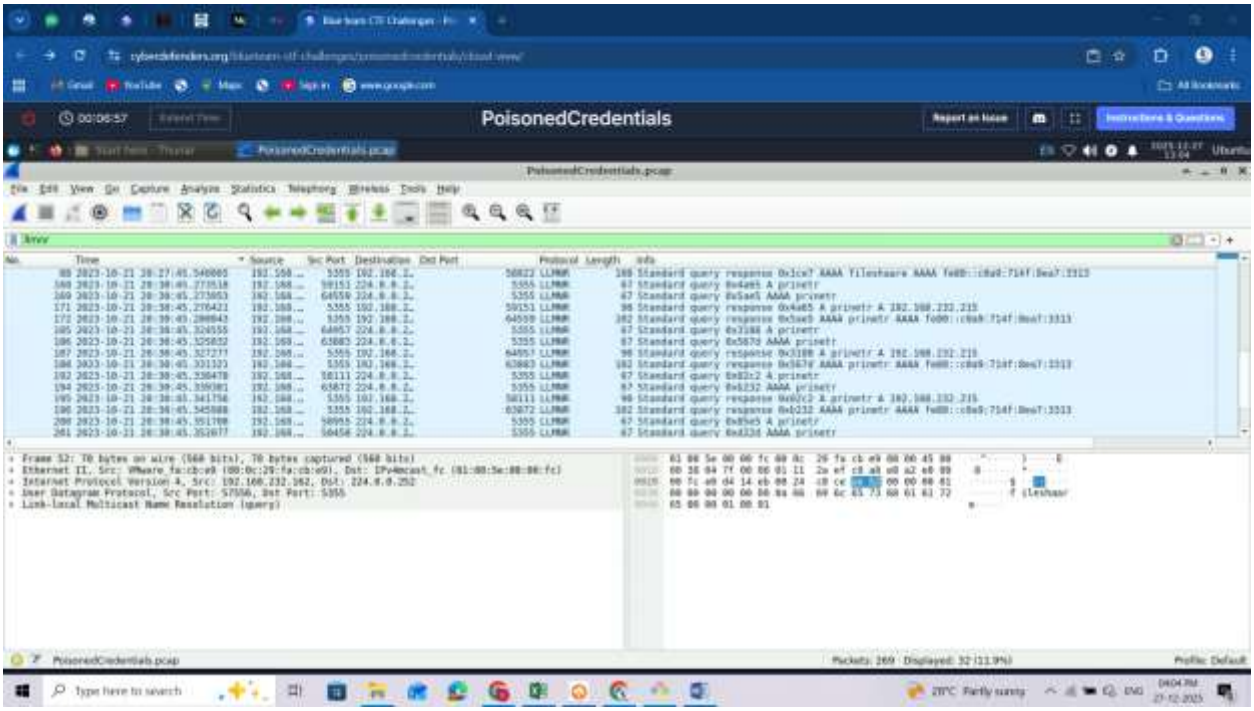
Filter with llmnr protocol:

It starts from 52,

We see a fileshaare misspelt probably for fileshare and there is a communication btn the endpoint of 192.168.232.21. and .162: **llmnr poisoning**

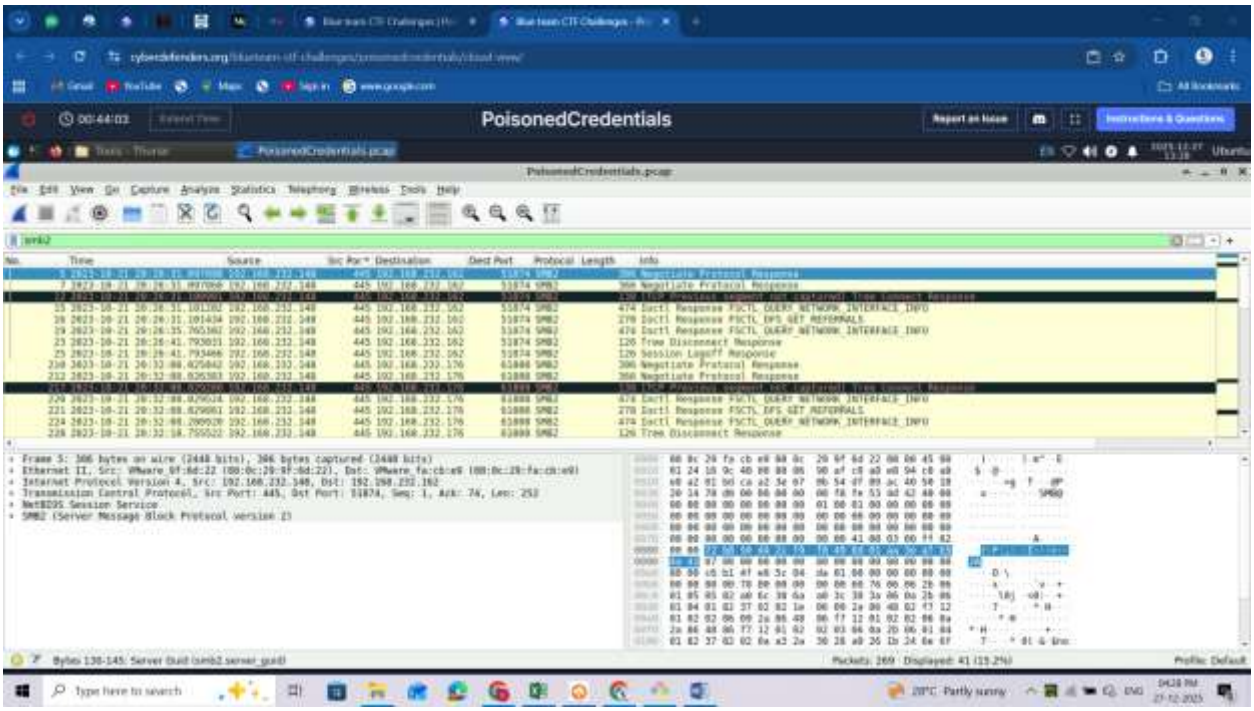


There is another communication btn .176 and .215 and there is a misspelling of printer probably for printer: **llmnr poisoning**



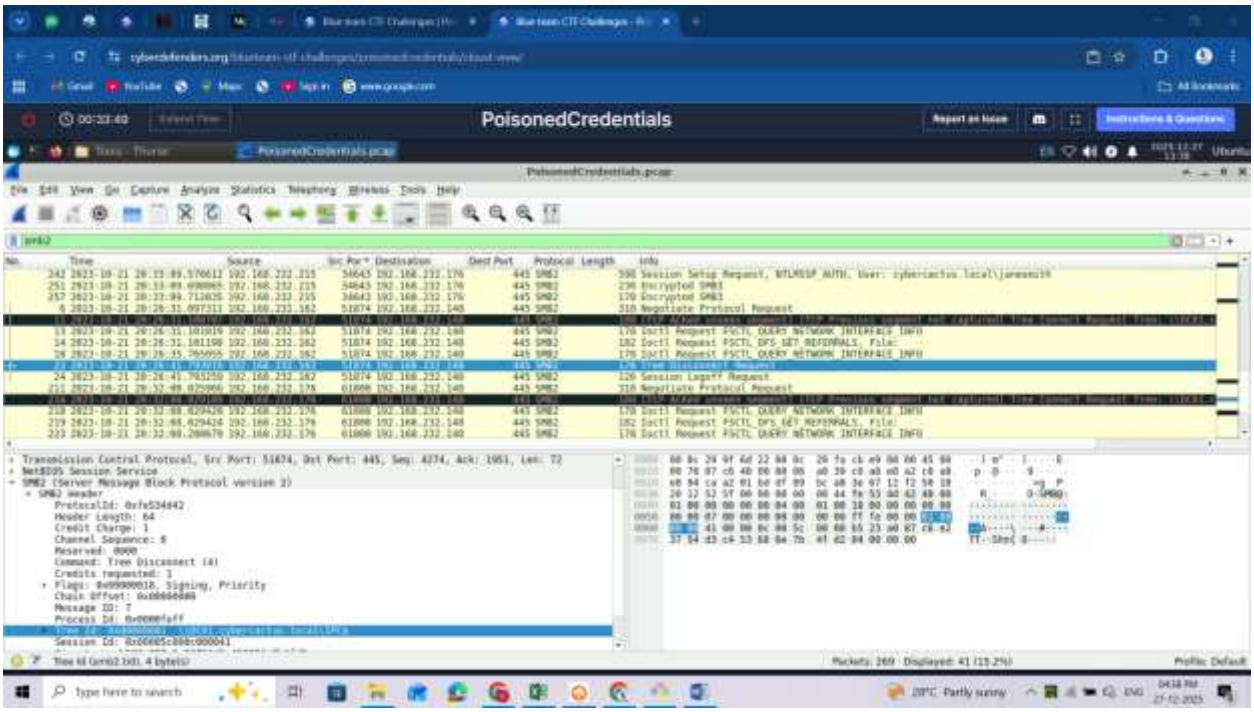
Filter with: **smb2**

we can see a communication btn .148 and .162



Tree Disconnect Request:

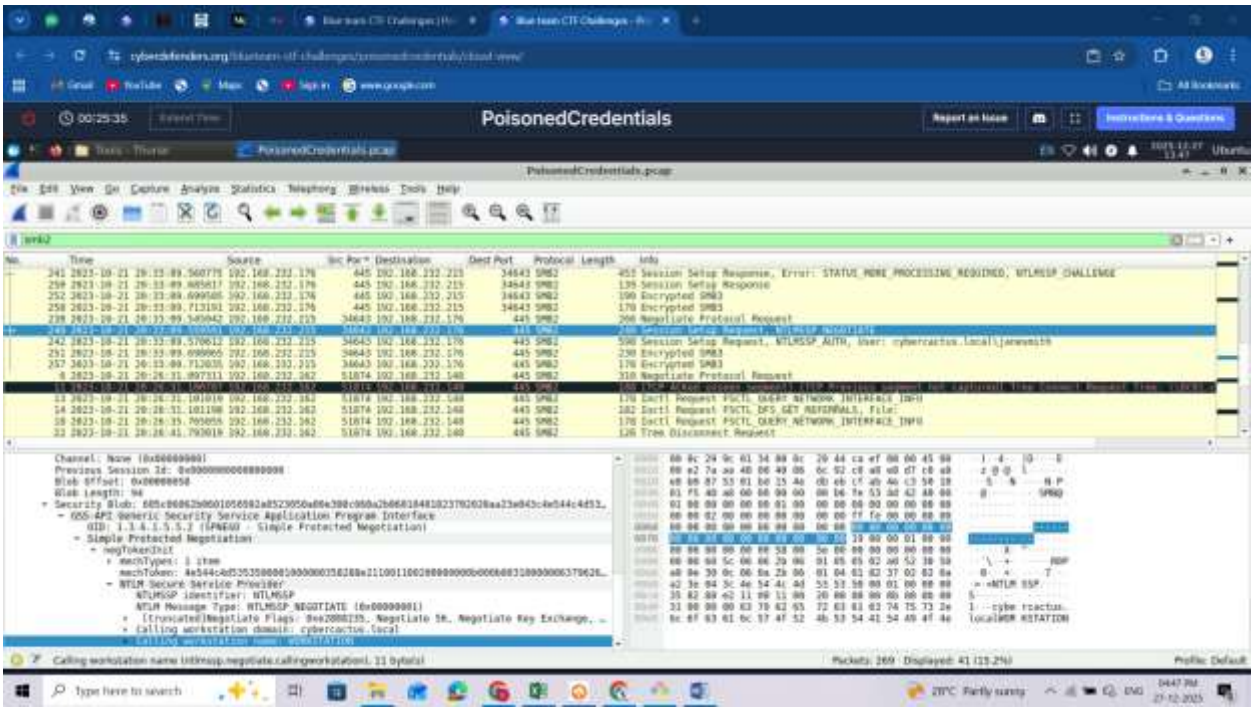
expand the **SMB2 -> SMB2 header**
We can see what the IP: 192.168.232.148 resolves to: Tree Id: DC01.cybercactus.local\ we are able to see the endpoint hostname (DC01) and domainname (cybercactus) and the share that was requested(IPC$). This share is used for intercommunication btn endpoints/services



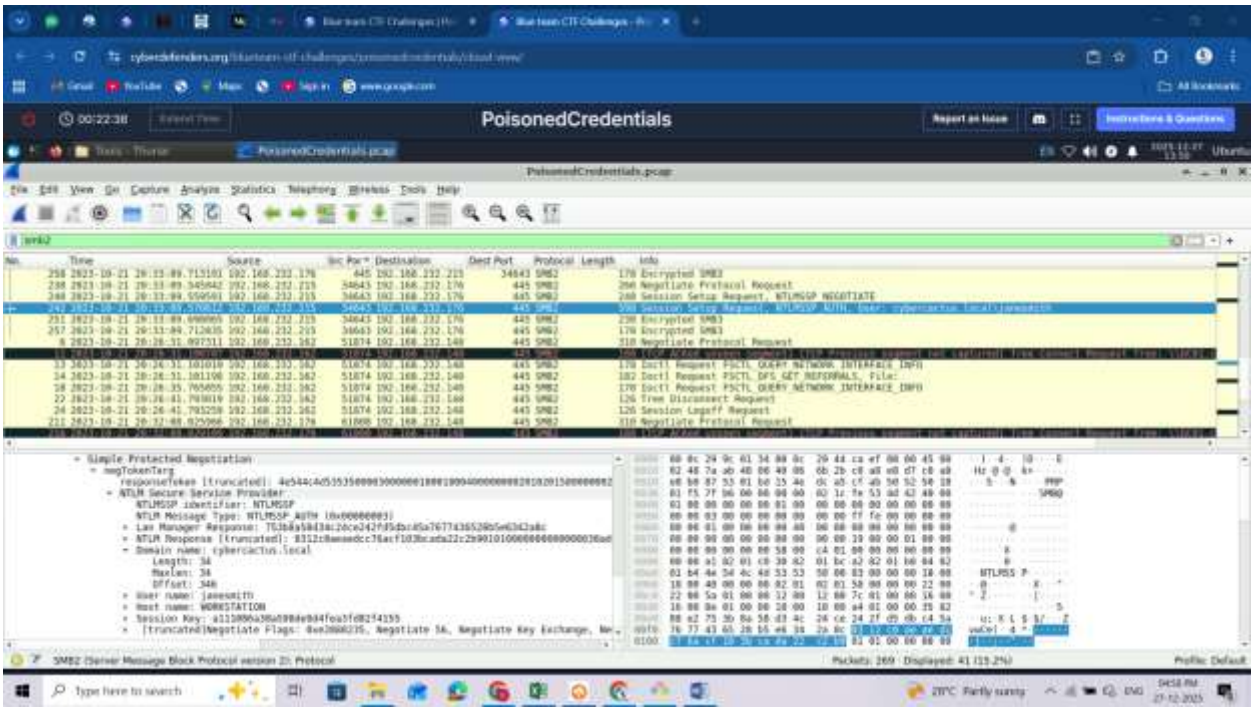
Session Setup Request

.215: Probably the attacker, earlier it deceived .162 that the 2 incorrect filenames exist and live under **.215** and now **.215** is making a request to **.176**

Expand SMB2 Header -> Session setup request -> Security blob -> continue exoanding to NTLM secure service provider; you will see the calling workstation name: WORSTATION; thus the source W.S name. The .215 ip resolves to the hostname of workstation. It id on the same domain.

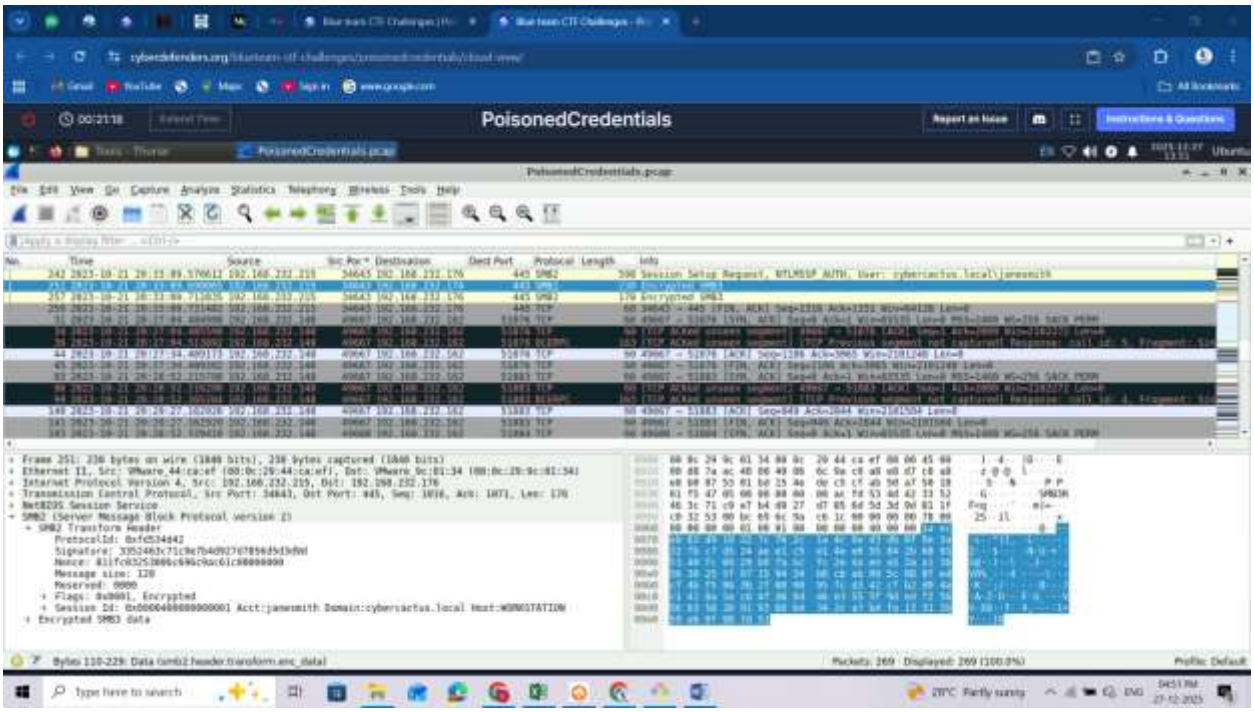


Let’s look on packet 242: we get to see more information including the username



If we check on Encrypted SMB3 pkt 251:

We can see: session ID, acct and the host.

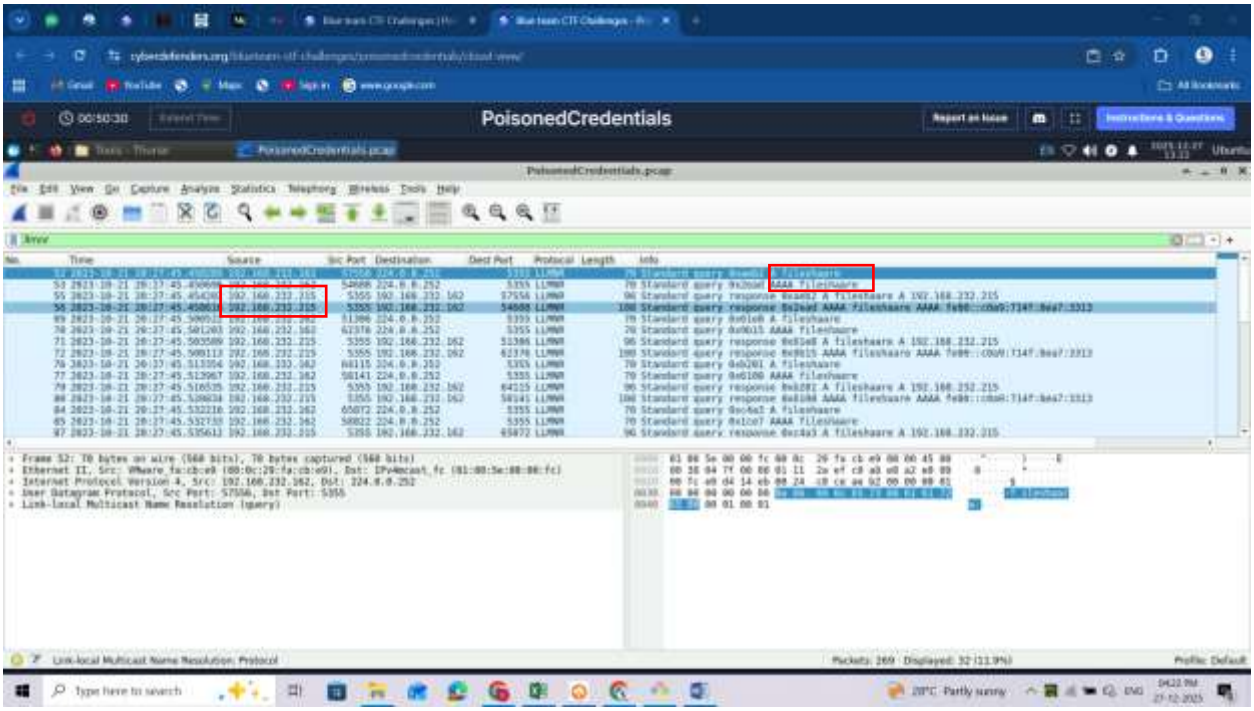


QUESTIONS

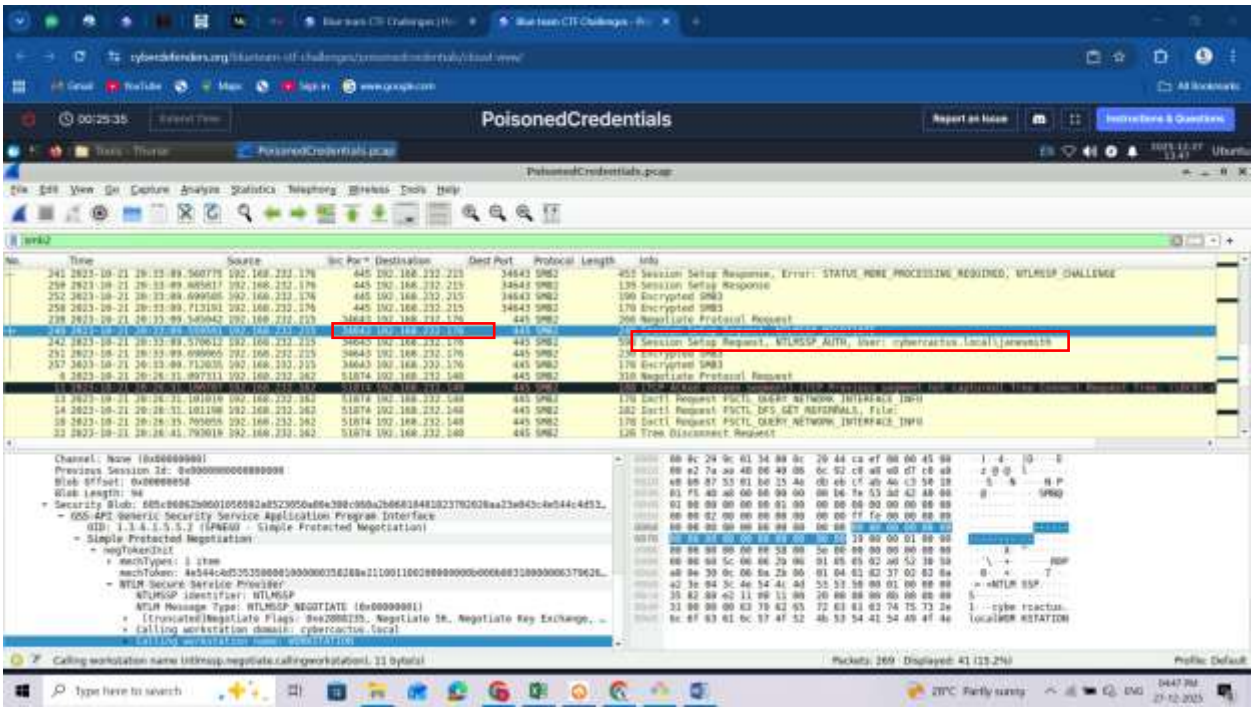
1. In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify

the specific mistyped query made by the machine with the IP address 192.168.232.162? **fileshaare**

2. We are investigating a network security incident. To conduct a thorough investigation, We need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity? **192.168.232.215**



3. As part of our investigation, identifying all affected machines is essential. What is the IP address of the second machine that received poisoned responses from the rogue machine? **192.168.232.176**
4. We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised? **Janesmith**



5. As part of our investigation, we aim to understand the extent of the attacker's activities. What is the hostname of the machine that the attacker accessed via SMB? **ACCOUNTINGPC**