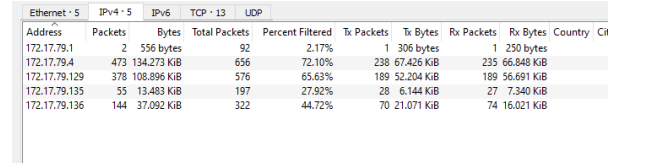
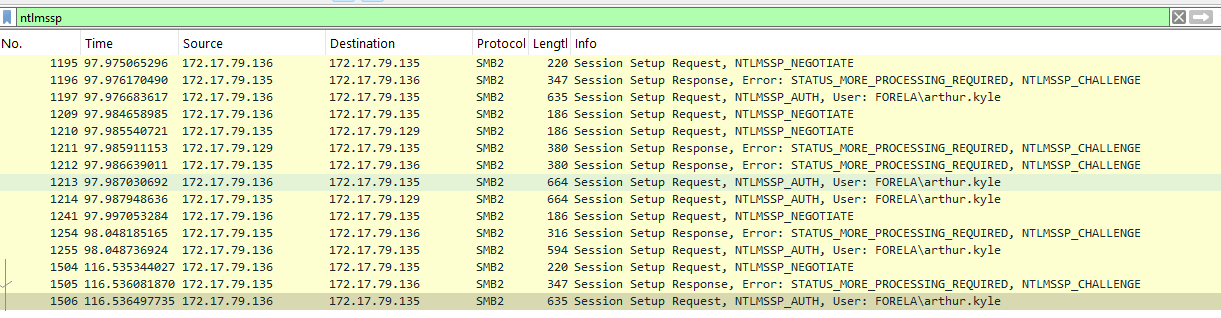
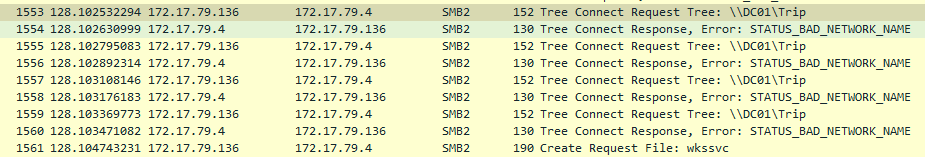
What is PCAP? : PCAP files are data files created using a program. These files contain packet data of a network and are used to analyze the network characteristics. They also contribute to controlling the network traffic and determining network status. Using PCAP files, teams can attend to detect network problems and resolve data communications using various programs. Security teams can use a network packet capture tool to identify, analyze, inspect, and monitor network traffic. Unusual traffic spikes can be due to a faulty application or a security breach. The packet capture tool allows IT teams to identify the root cause of the issues by tracking network packets.   
  
**Let's start by opening the PCAP file in Wireshark. Going over Statistics-> Endpoints we can see top most IP Addresses.**  


Analysis : Q1 What is the IP Address for Forela-Wkstn001?   
**Hint : Filter for nbns protocol to find the relevant IP Address.**

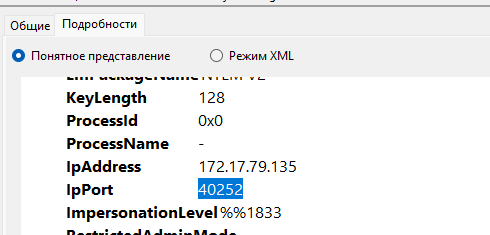
Q2 What is the IP Address for Forela-Wkstn002?   
**Hint : Filter for nbns protocol to find the relevant IP Address**.  
  
Q3 What is the username of the account whose hash was stolen by attacker?   
**Hint : Filter for ntlmssp protocol in wireshark OR Filter for 4624 event ID and Look for an odd looking logon event.**

****

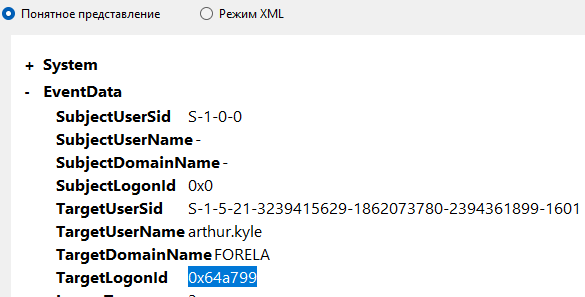
Q5 Shortly after entering the wrong path and triggering the relay attack, the user tried again and entered the intended path. What was this fileshare path which victim tried navigating to?   
**Hint : Filter for smb2 traffic in wireshark. Search for keywords "Tree connect Request Tree" in packet details. Now look for any file share path which seems like a legit path a day to day user might visit.**

****

Q6 What is the source port used to logon to target workstation using the compromised account?   
**Hint : In provided Event logs, filter for event ID 4624 and look for a event where Security ID is NULL and logon type is 3.The logon process value will be NtlmSSP and authentication package value is NTLM. Then look for Source Port value in event details.**

****

Q7 What is the Logon ID for the malicious session?   
**Hint : In the same event, look for LOGON ID Value**

****

Q8 The detection was based on the mismatch of hostname and the assigned IP Address.What is the workstation name and the source IP Address from which the malicious logon occur?   
**Hint : We already found all the IP Addresses for all the devices in the network. In the specified event ID 4624 , find both the workstation and IP from network information section. The workstation name is false as its assigned IP will not be the one you see in the event log.**

Q9 When did the malicious logon happened. Please make sure the timestamp is in UTC?   
**Hint : Look in details tab for the UTC Time**

Q10 What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?Look for the answer in Provided Event logs.   
**Hint : Look for event ID 5140 and see the share name accessed. We can corelate this event with the malicious session via the Logon ID we found before**