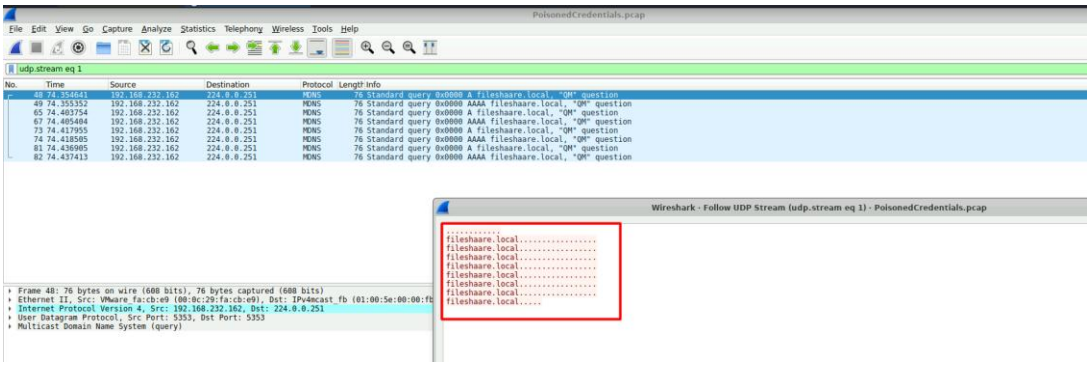
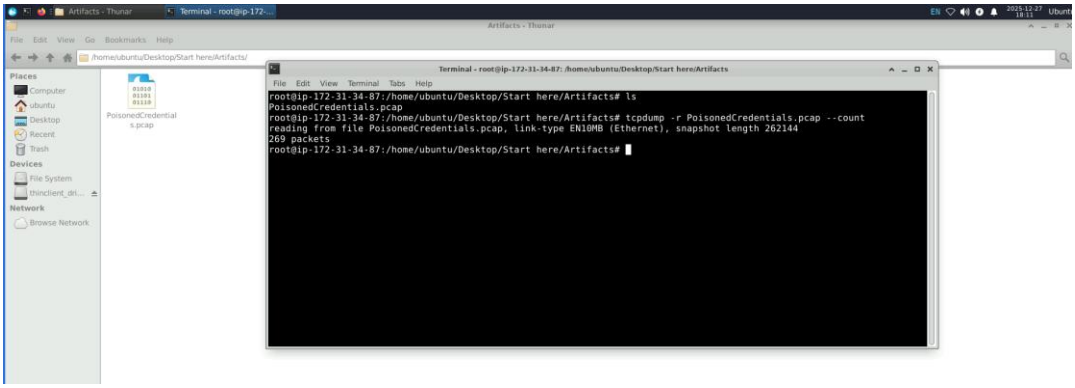
Reference: https://cyberdefenders.org/blueteam-ctf-challenges/poisonedcredentials/

Start the VM and analyze the PCAP file.

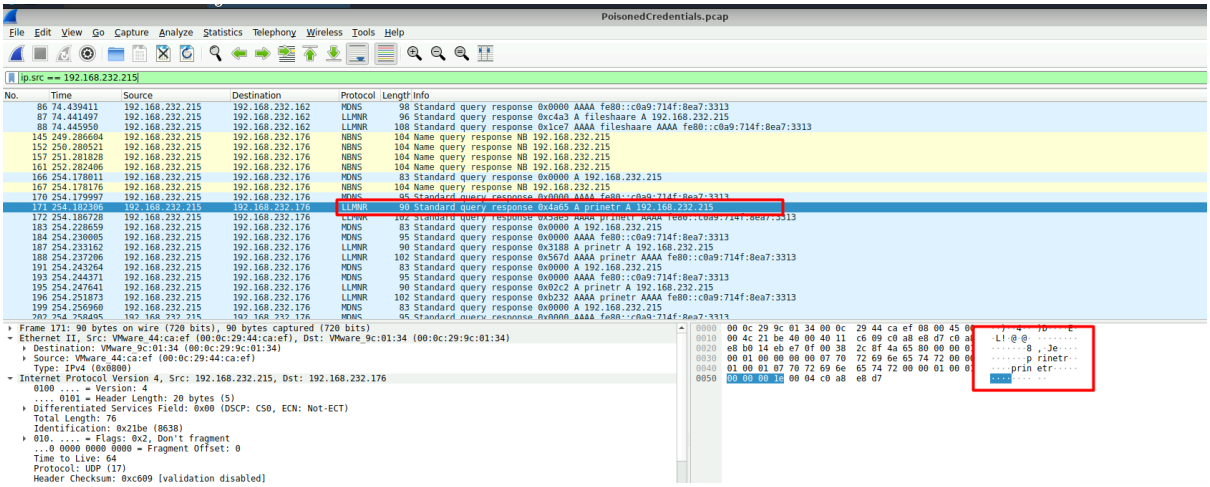
1. In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?
   fileshaare



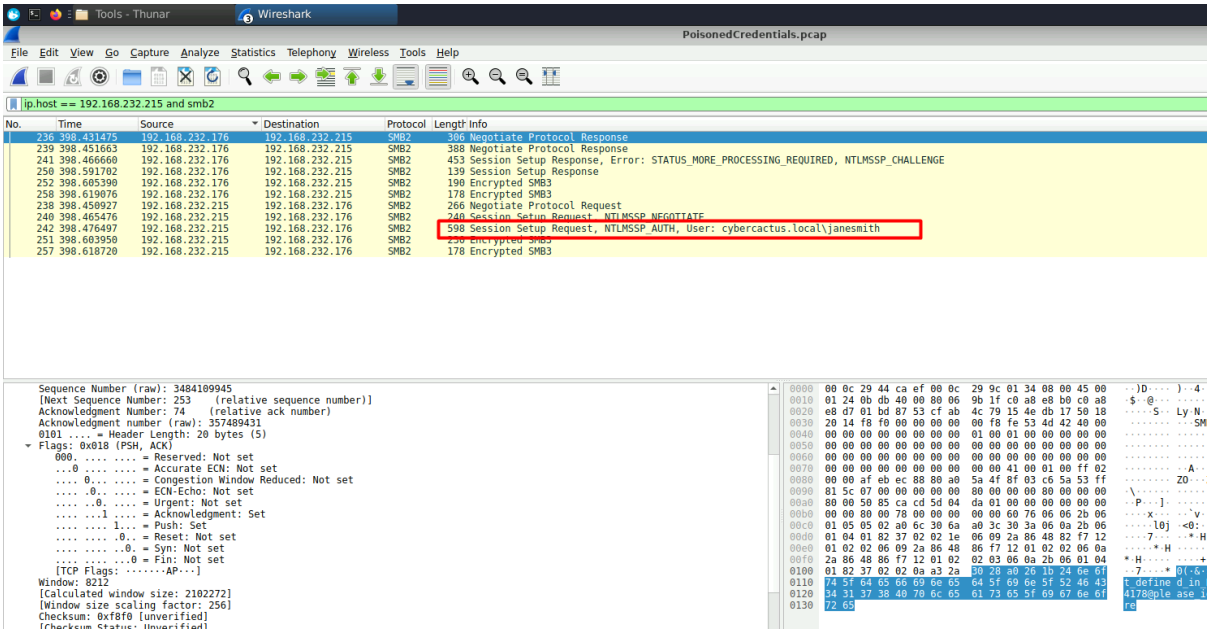
2. We are investigating a network security incident. To conduct a thorough investigation, We need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity? ***192.168.232.215***



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***