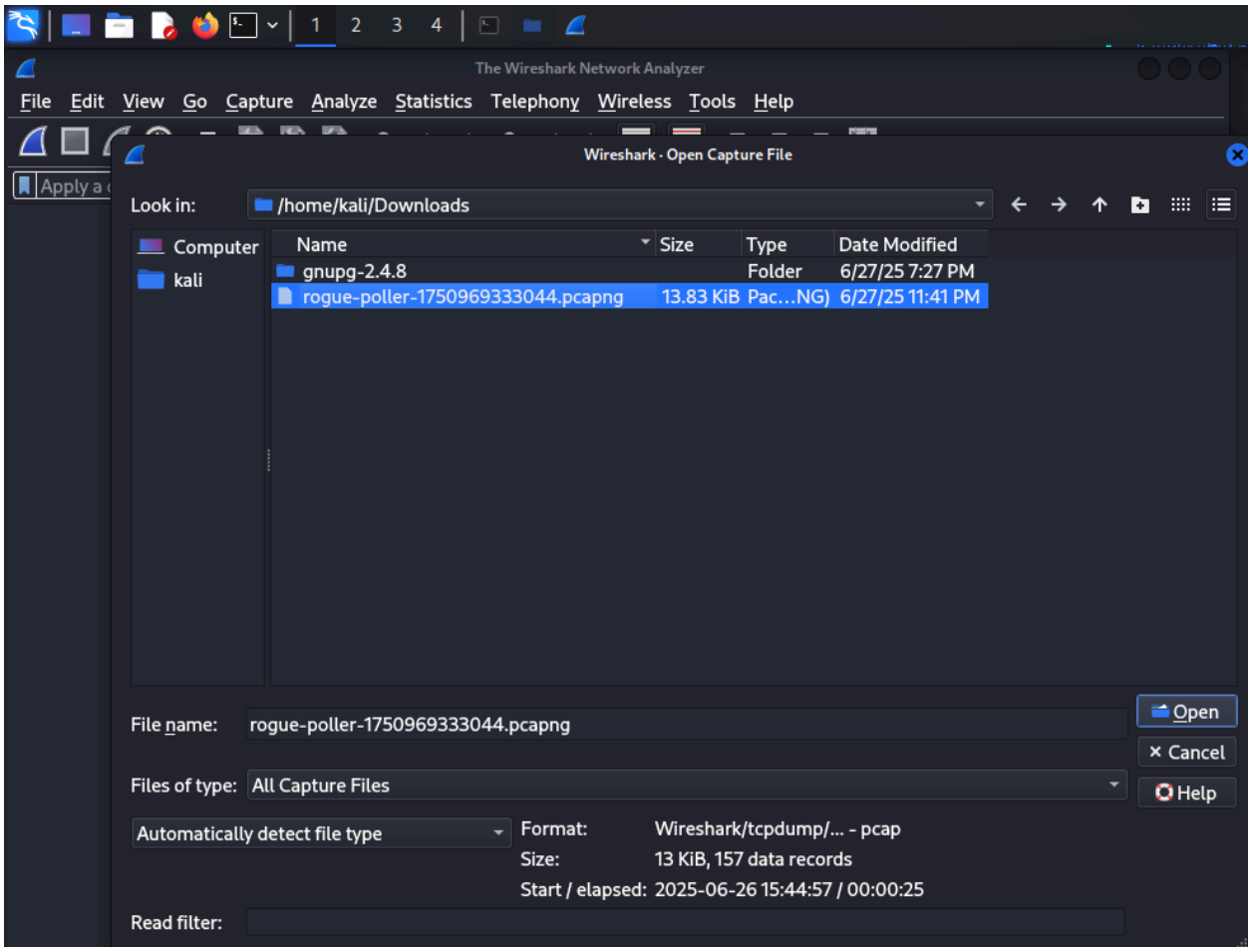
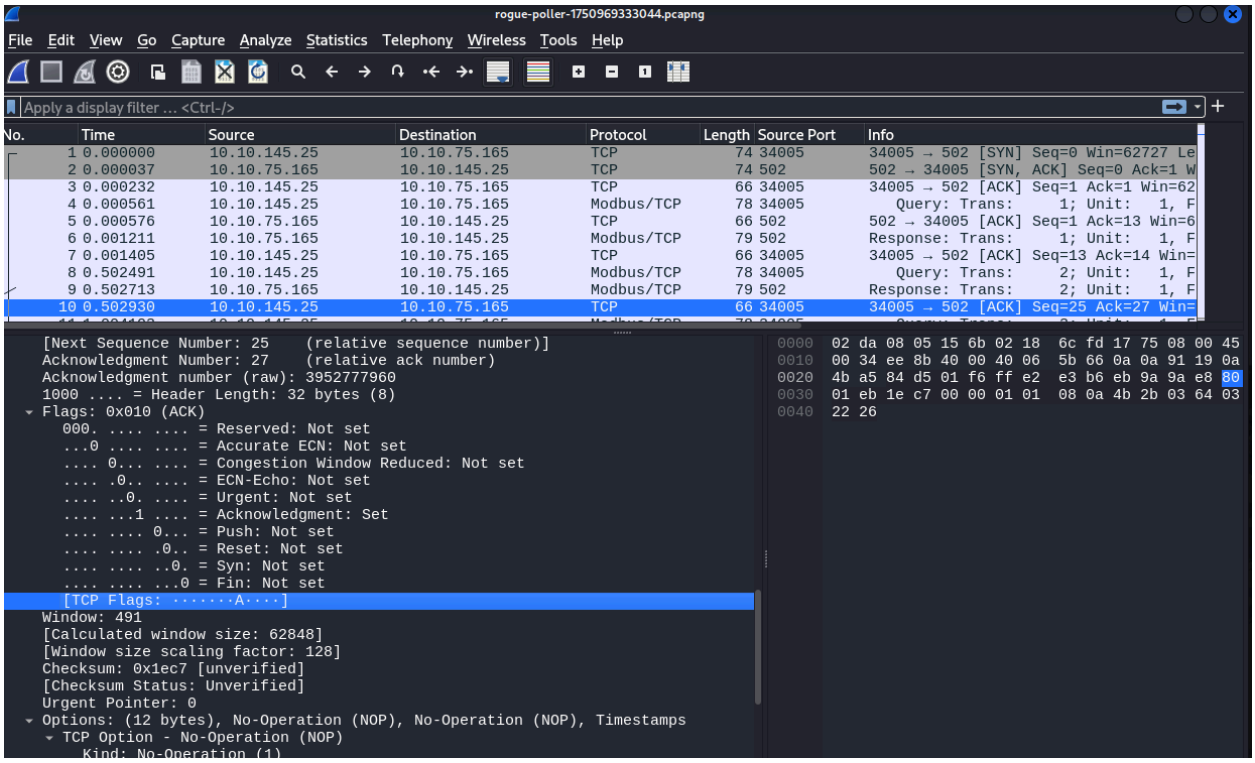
Task 22: Rogue Poller

This task was an intriguing one! It turned out to be much simpler than I initially thought and what I believe is the best beginner-friendly challenge in this CTF. Here are the steps and write-up for solving this challenge.

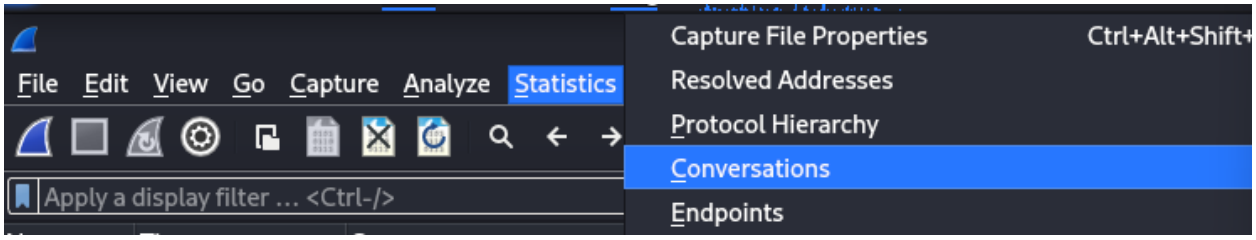
1. Download the .pcapng file from the THM Industry Intrusion room (https://tryhackme.com/room/industrial-intrusion). Or download the file from my github.
2. Boot up Wireshark. Personally, I was using Kali Linux on my VM which had Wireshark pre-installed.
3. Inside Wireshark, click on File > Open, then navigate to the downloaded .pcapng file and open it.



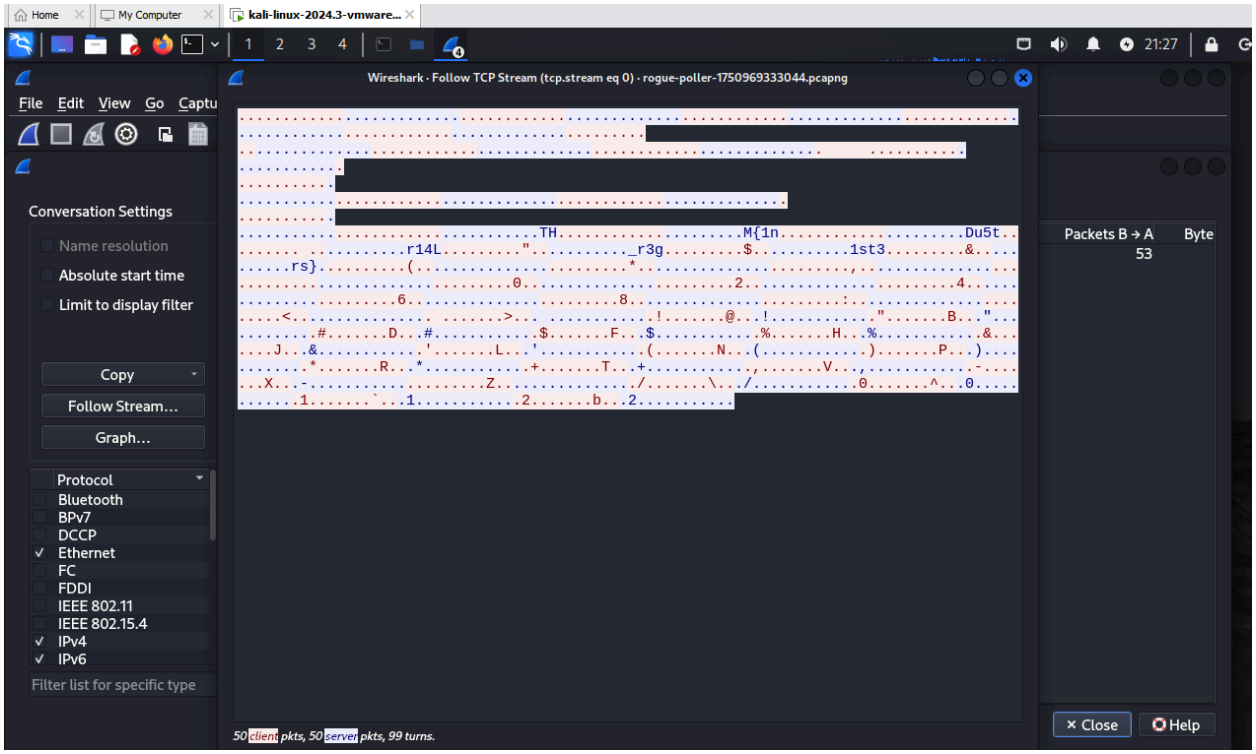
4. Looking at the traffic between TCP and Modbus was overwhelming at first, and delving into the contents of a packet did not expressly reveal anything at first.



5. After inputting various filters resulting in little result. I decided to go into Statistics > Conversations.



6. Clicking on the TCP tab, we are able to follow the Stream to get a much clearer picture of what we are looking at.



7. Clean up the dots and miscellaneous symbols and you will have your flag!
   THM{1nDu5tr14L_r3g1st3rs}

   Don't worry about leaving out the underscore, I left it out when I first submitted the flag and THM was nice enough to still count it. Happy Hacking!

   - Coy