Lab8 Network analysis and forensics

CSCI 4406_60L – Computer Networks Lab
Joshua Ludolf

Using the 6 pcap files in the attached folder, pick and answer 10 questions from the file below. For each answer, you are supposed to justify and support your answer (e.g. with a screenshot, statement, etc.).

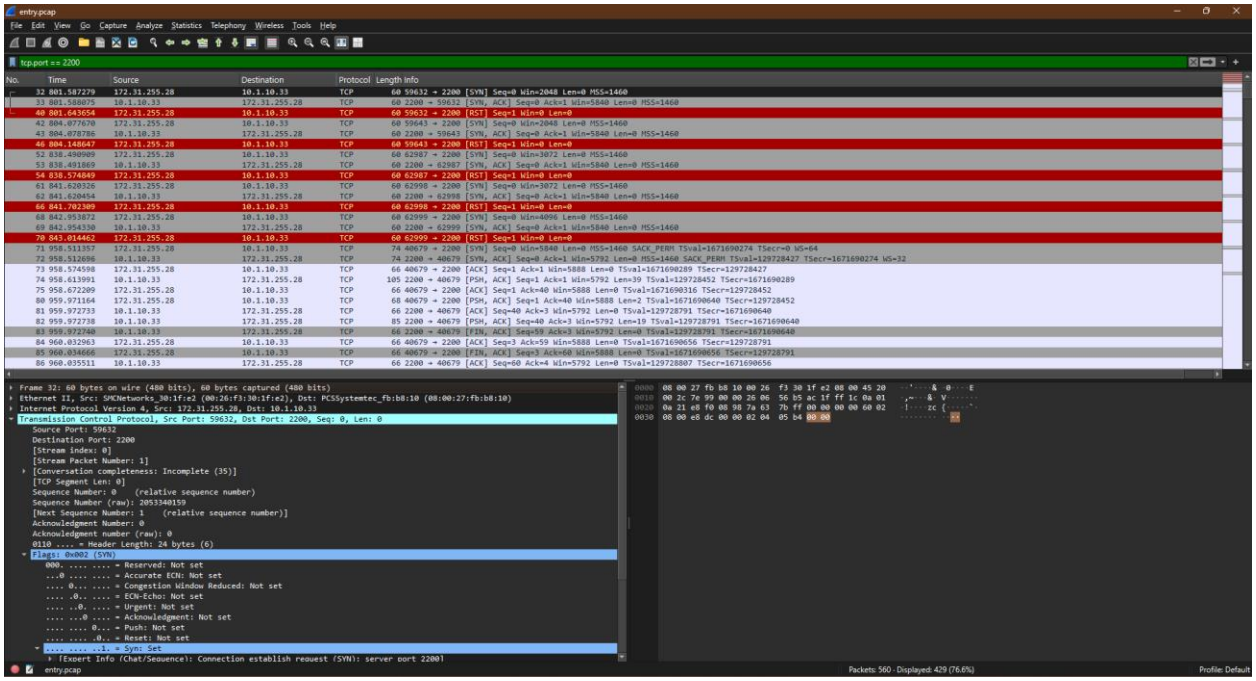
A small utility in an unnamed locale has a small SCADA test environment setup. The staff at this utility have installed a DSL line to enable remote access to this system. Unfortunately, the utility staff did not adequately consider the security implications of doing this, leaving the test environment open to attack from the internet.

After experiencing odd behavior on this system, the lead engineer began looking at system logs and network traffic in an attempt to troubleshoot the issue. He discovered what appeared to be unauthorized access into the system. You have been called in to examine this evidence and help determine what has occurred.

Your task, should you choose to accept it, is to examine these evidentiary artifacts to determine what has happened, and provide answers to the following questions.

Before you begin, please download and install Wireshark (1.4.6 or later), and then download the following ZIP file (containing 6 packet capture files) for analysis:
February 2012 Cyber Quest PCAP's
Section 1: Initial recon and entry

Artifacts
Packet capture - entry.pcap
Question 1
Marks: 1
What service appears to be running on port 2200?
Choose one answer.
- Industrial Control Interface
- Rockwell Automation PPTP
- Inter Carrier Interface
- Secure Shell



I first checked port 2200 to see what was running on it. I used the filter “tcp.port == 2200” in Wireshark to find the packets that deal with that specific TCP port. I couldn’t tell too much from this data alone. I had a strange suspicion that it was SSH because SSH uses port 22 by default. I had a feeling they used the extra 2 0’s at the end to make it trickier to see.

Question 2
Marks: 1
It appears that after running a scan, the attackers made connections to each of the open ports. Which of the following tools was most likely used to establish those connections? Choose one answer.

- Nessus
- SSH
- Telnet
- Netcat

Netcat was most likely used to establish connections to each of the open ports. Netcat is a versatile networking utility that can read and write data across network connections using the TCP/IP protocol. It's often referred to as the "Swiss Army Knife" for network administrators and hackers because of its ability to establish connections and perform various tasks on different ports.

Question 3
Marks: 1
Which IP address had port 2200 open?

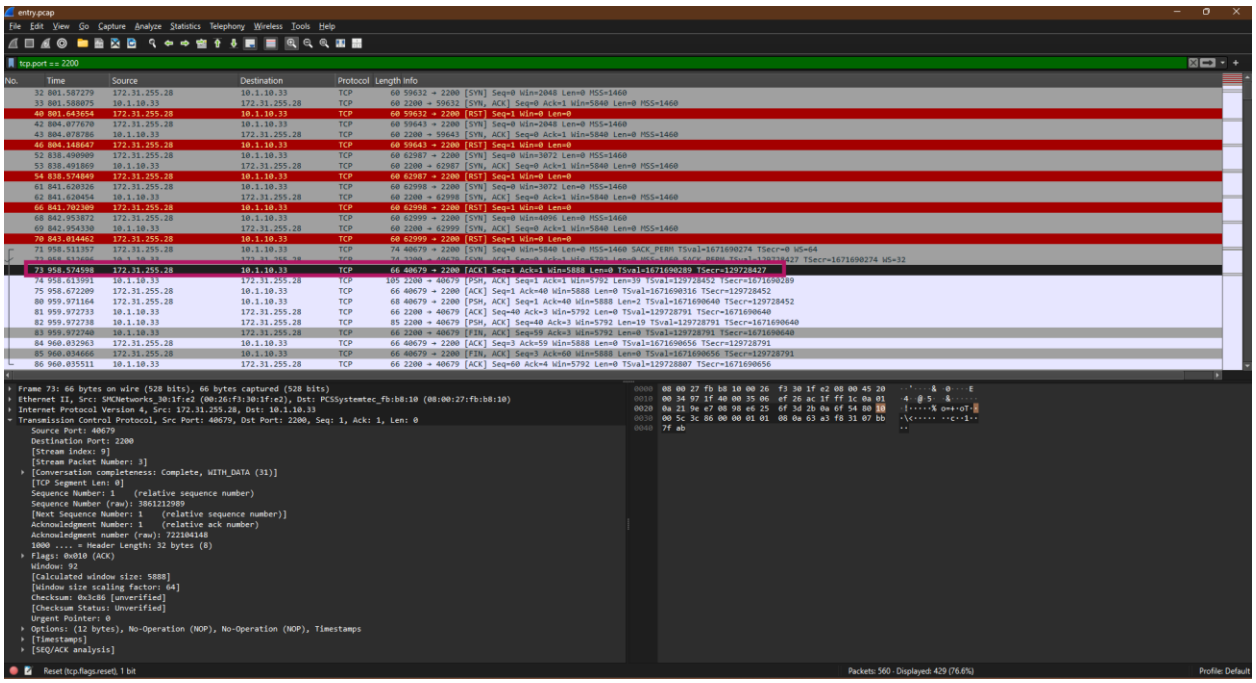
Choose one answer.

10.1.10.33

10.1.10.60

10.1.10.20

10.1.10.130



I used the same filter as before, “tcp.port == 2200” to filter out the data. I noticed most of the SYN packets never got responses back. This is visible by the red data packets and those packets have RST responses, which means Reset. One SYN packet did get a response, the request server sent a SYN packet and the receiving server responded with anACK packet. This means the port is open and is responding to requests. I boxed that packet in magenta.

Question 4

Marks: 1

Which version of SSH was the attacker using?

Choose one answer.

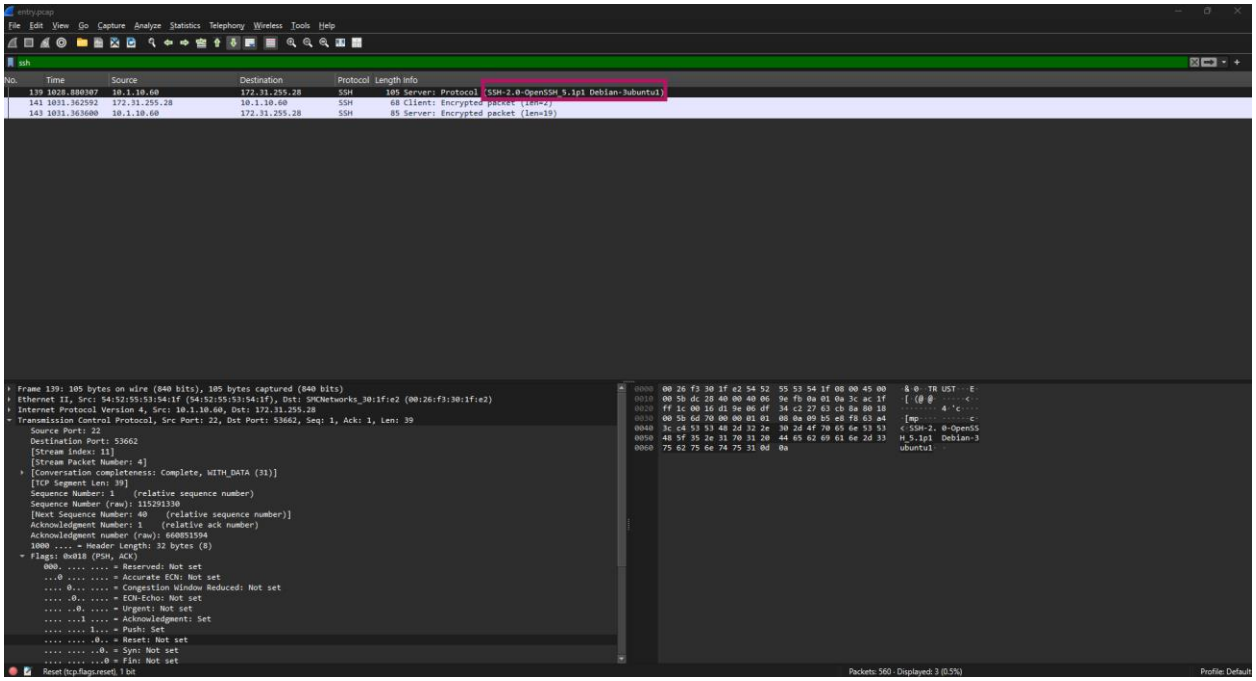
WinSSH

PuTTY

OpenSSH 5.3p1

OpenSSH 5.2

None of the above its OpenSSH 5.1p1

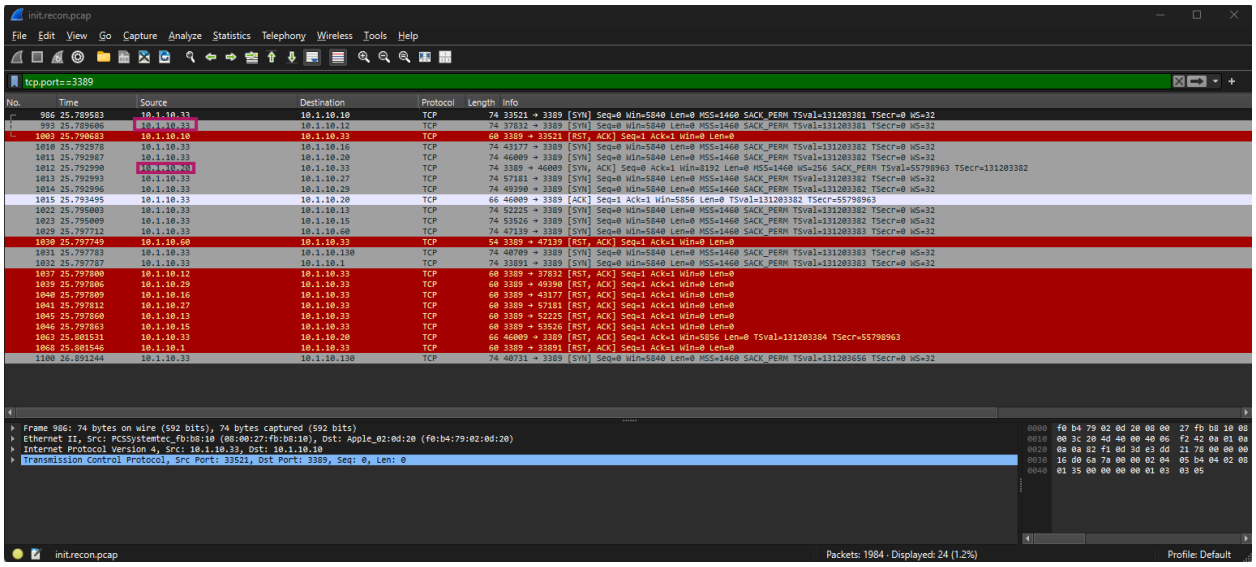


I used “SSH” as the filter in Wireshark. The protocol for SSH is now filtered and only the packets using that protocol will show up. You can see the answer is in the first packet. The first pack has information, and it reads out “SSH2.0-OpenSSH_5.1p1” so I concluded it’s using OpenSSH 5.1p1.

Section 2: Initial Recon

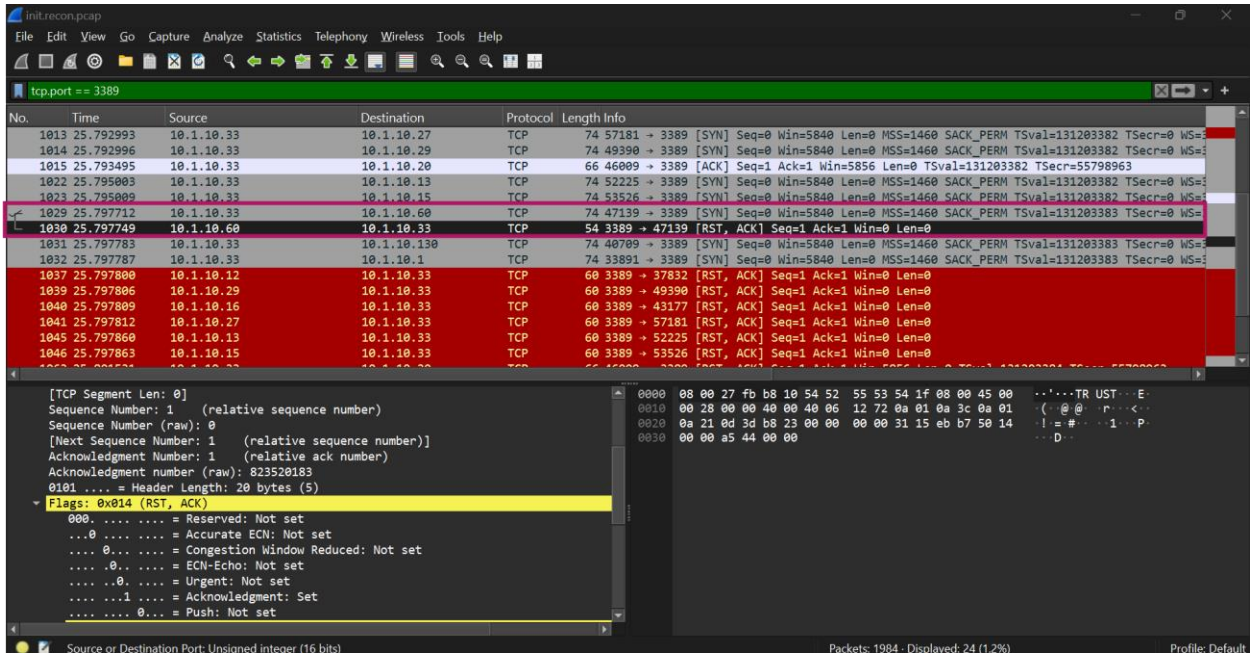
Artifacts
Packet capture: init.recon.pcap
Question 5
Marks: 1
Which of the following IP addresses appear to be the same type of device?
Choose one answer.
- 10.1.10.13 and 10.1.10.29
- 10.1.10.20 and 10.1.10.29
- 10.1.10.15 and 10.1.10.13
- 10.1.10.20 and 10.1.10.130

Question 6
Marks: 1
How many IP addresses had port 3389 open?
Choose one answer.
- 1
- 2
- 3
- 4



Question 7
Marks: 1
Which of the following IP addresses appears to be running a Human Machine Interface (HMI)?
Choose one answer.

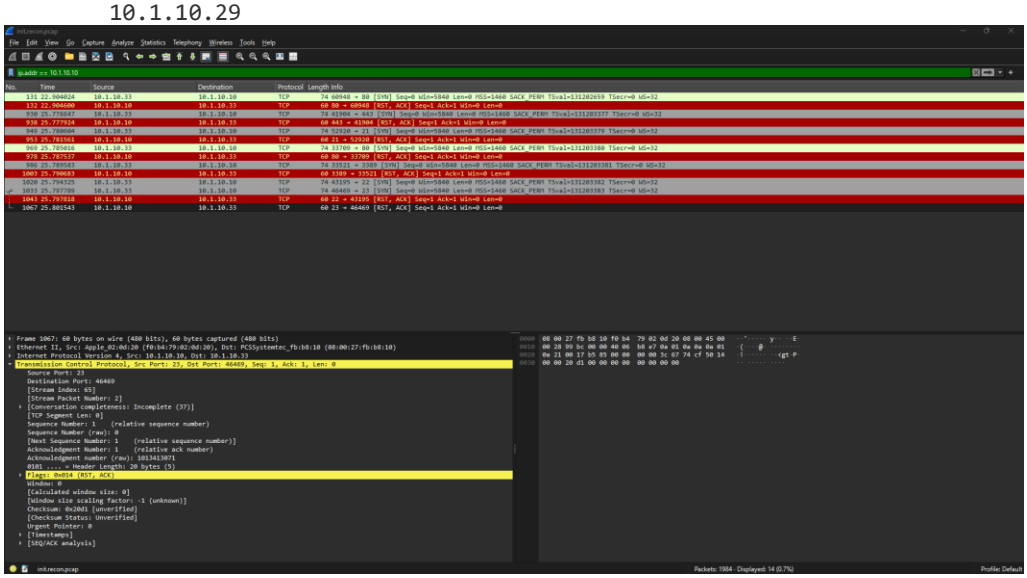
10.1.10.60
10.1.10.130
10.1.10.29
10.1.10.20



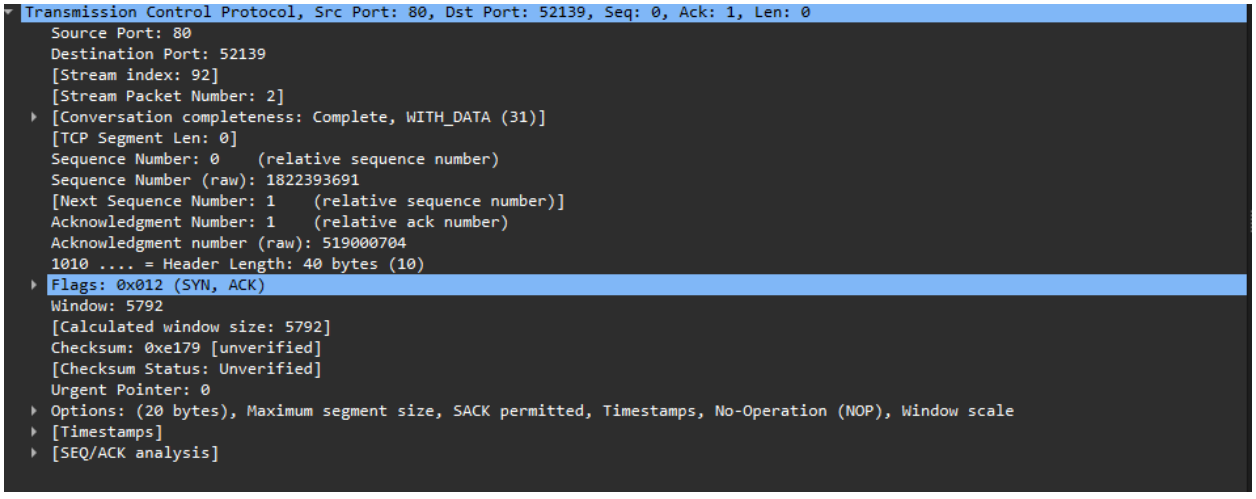
Using Wireshark, I applied the following filter: tcp.port == 3389 , to isolate RDP traffic and then analyze the IP addresses involved. The IP address that shows regular RDP traffic and possibly interacts with other industrial devices is likely running an HMI.

Question 8
Marks: 1
Which of the following IP addresses did NOT have port 23 open?
Choose one answer.

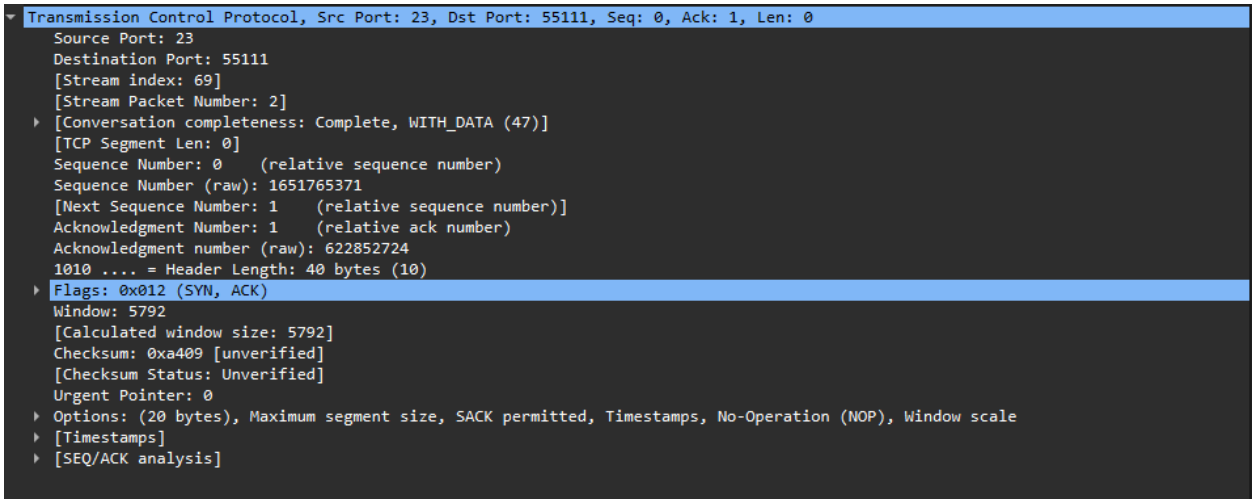
10.1.10.10
10.1.10.27
10.1.10.16
10.1.10.29



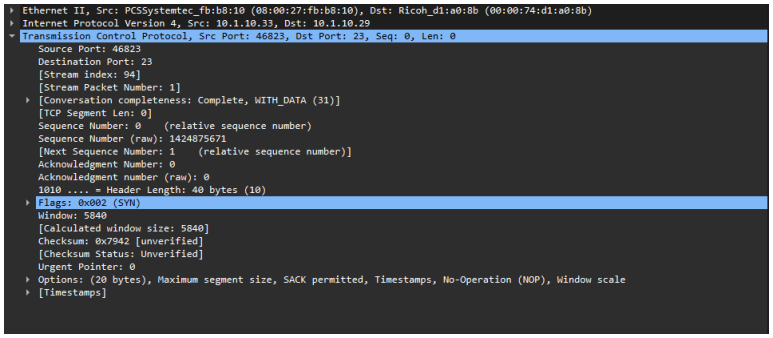
First, I checked out the .10 ip address. I used the filter "tcp.port == 23" to filter out all data that had that port. I saw the .10 address sent back a RST flag. This means that the port was closed and didn't allow data to get past it. I will go ahead and check the other ports to make sure.



.27 ip address sent back a SYN packet, meaning it allowed the requests and port 23 is open.



.16 did the same thing, so port 23 on it is open as well.



.33 also did the same thing, so port 23 is open on it as well.

Question 9
Marks: 1
Which of the following ports was not included in the scan of the internal network?
Choose one answer.
- TCP 3389
- TCP 80
- TCP 23
- TCP 2200

Question 10
Marks: 1
Approximately how long did the port scan take to complete?
Choose one answer.
- 27.1 seconds
- 4.0 seconds
- 3.5 seconds
- 17.1 seconds

Section 3: SCADA Protocols

Artifacts
Packet capture: HMI2PLC.pcap
Question 11
Marks: 1
Which of the following best describes the nature of the communications between .20 and .130?

Choose one answer.
- Each device sends data as needed based on operational events.
- The .130 device sends data at regular intervals
- The .20 device requests data at regular intervals
- Both devices exchange data at regular intervals

Question 12
Marks: 1
A number of packets from .20 to .130 appear to have a counter. Which of the following represents the packet offset location of the counter?
Choose one answer.
- 0x73
- 0x26
- 0x42
- 0x2a

Question 13
Marks: 1
Which of the following protocols appears to be in use between the two devices?
Choose one answer.
- Ethernet over IP
- Common Instrumentation Protocol
- Modbus
- Ethernet Industrial Protocol

Section 4: PLC web recon

Artifacts
Packet Capture: web_recon.pcap

Question 14
Marks: 1
What username was successfully used to access pages on the webserver on .130?
Choose one answer.
- admin
- ml1100
- root
- guest

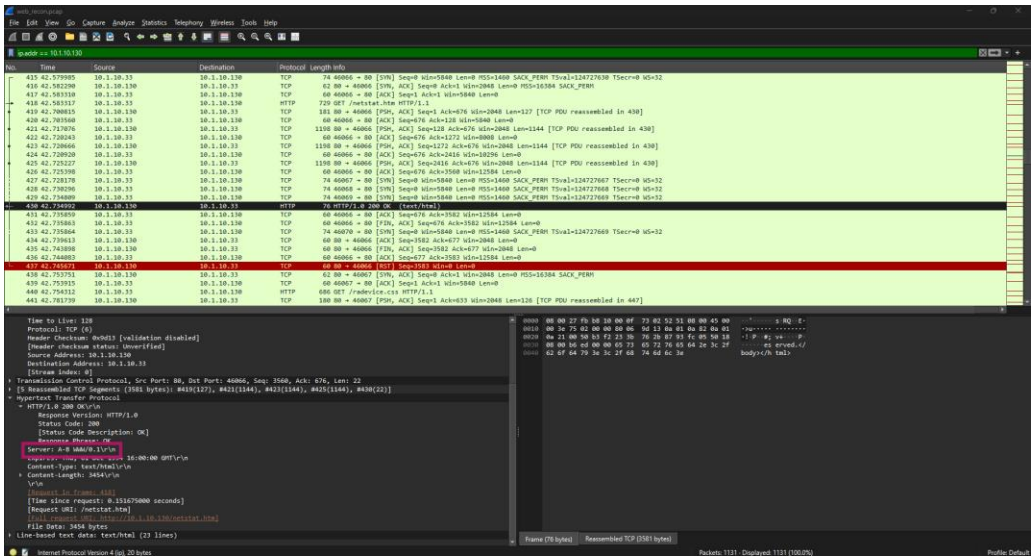
I did a follow TCP stream and searched. I found this. The Authorization Username is guest as shown in the screenshot above.

Question 15
Marks: 1
What was the URI that returned an embedded reference to an ActiveX control?
Choose one answer.
- /navtree.htm
- /dataview.htm

/control.htm
/newdata.htm

Question 16
Marks: 1
Which URL request first resulted in an authentication request?
Choose one answer.
/dataview.htm
/redirect.htm
/navtree.htm
/home.htm

Question 17
Marks: 1
What webserver appears to be running on the .130 device?
Choose one answer.
Apache 2.2.19
A-B WWW/0.1
Firefox/3.6.24
1763-L16BWA B/9.00



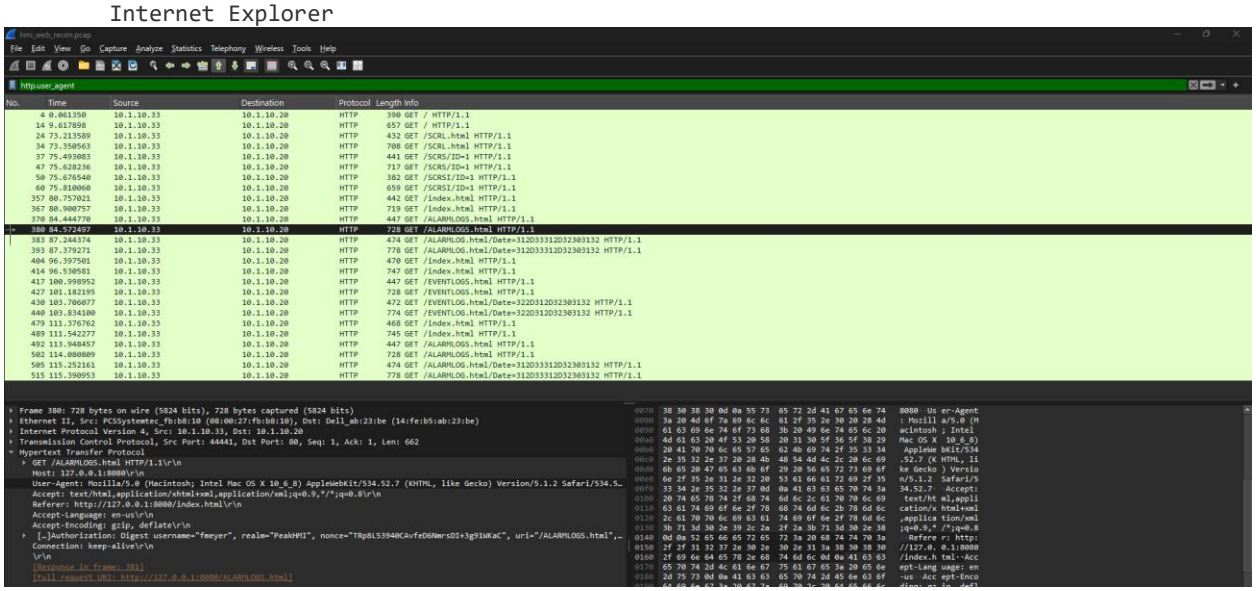
I looked for the first packet that had a get request. I then looked for the response. I looked under the HTTP respond in packet 414 which was a get request. I looked for the "Server" header tag and found "Server: A-B WWW/0.1"

Question 18
Marks: 1
What tool do the attackers appear to be using to probe the webserver on .130?
Choose one answer.
Firefox
wget
Nessus
OpenVAS

Section 5: HMI web recon

Artifact
Packet Capture: hmi_web_recon.pcap

Question 19
Marks: 1
What browser did the attackers use to access the HMI?
Choose one answer.
- Safari
- Chrome
- Firefox
- Internet Explorer

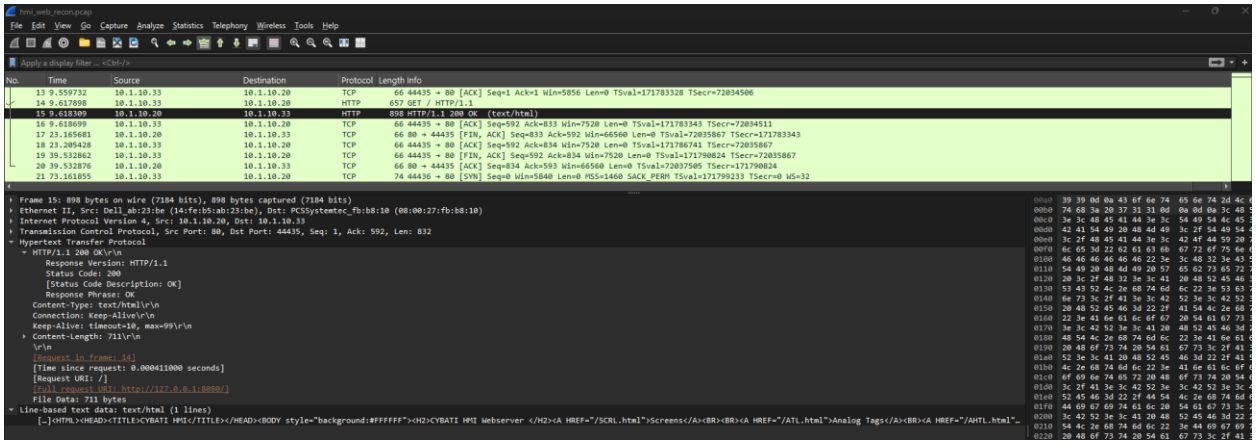


I did a quick search using a Wireshark filter. I used "http.user_agent" and I checked the first packet. I noticed that the help box says it's a Chat/Sequence. I wasn't sure if this meant chat box, but I assumed it did. Because HMI stands for Human Machine Interface, and that means anything that a machine and human use to communicate, I assume this is the answer. Safari is listed as the user-Agent, so that's the answer.

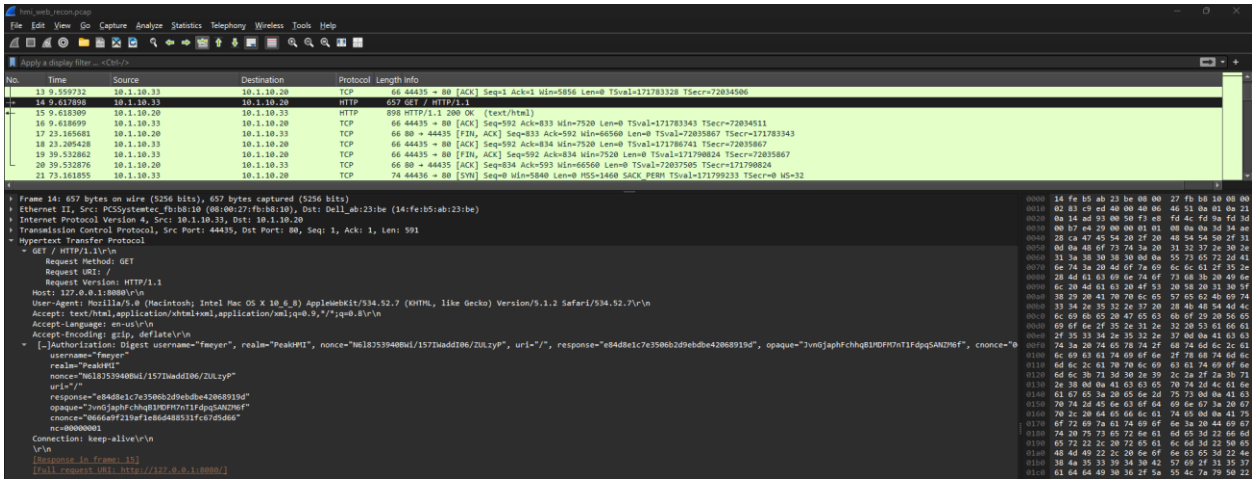
Question 20
Marks: 1
The operating system that appears to be running on the attacker's machine appears to differ from the OS running on 10.1.10.33. Based on the information in the packet capture, what is the most likely explanation?
Choose one answer.
- The attackers are tunneling X11 over an SSH connection
- The attackers are spoofing their source address.
- The attackers set up a tunnel for port 80 over an SSH connection
- The attackers set up a PPTP server on the 10.1.10.33 box

Question 21
Marks: 1
Which of the following passwords was most likely used to authenticate to the HMI webserver?
Choose one answer.
- L3tmein
- password

fm3y3r-hmi
hmiviewonly



I looked for the first HTTP Get method, but this packet says, Denied. I checked the next one a saw a few different things. First, the next packet says Authentication Authorized.



This packet says the authorized user is “fmeyer”. I looked for a little while and couldn’t find a direct answer to the password. But the options for the passwords are: L3tmein, password, fm3y3r-hmi, and hmiviewonly. The only password that makes sense here is, fm3y3r-hmi since the username used was fmeyer. And the password and username are very similar.

Question 22
Marks: 1
One of the pages viewed by the attackers contains logs showing logon times. This log appears to have captured their activity on the HMI webserver. Based on this, which U.S. timezone does the HMI appear to be in? [Note: assume the packet capture timestamps were stored in UTC, and are adjusted by Wireshark to reflect your local timezone]
Choose one answer.
- Pacific
- Mountain
- Eastern
- Central

Question 23

Marks: 1
Based on the times from the logfile in the previous question, which of the following most closely represents the time differential between the HMI webserver and the device performing the packet captures?
Choose one answer.
- 3 seconds
- 9 seconds
- 13 seconds
- 51 seconds

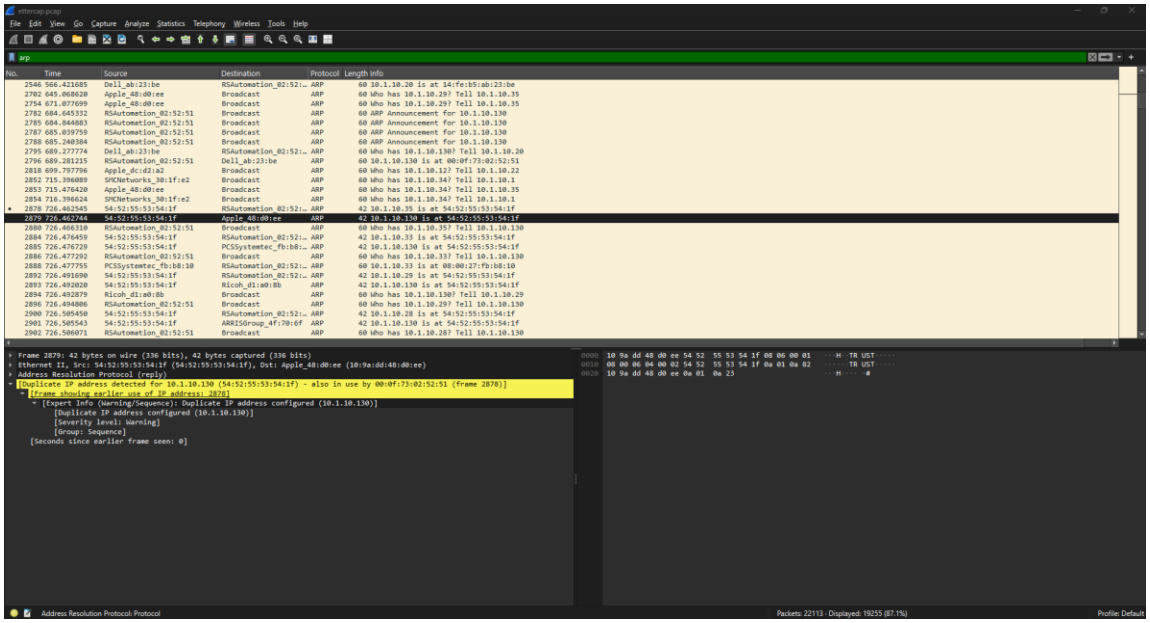
Section 6: Attempted Man-in-the-Middle attack on PLC and HMI

Artifact
Packet Capture: ettercap.pcap
Question 24
Marks: 1
The previously mentioned page that showed logon times also contained logs of other events. Based on this page, what event occurred on the HMI on Feb 1 at 3:24:50PM?
Choose one answer.
- A log file rotation
- A user login
- An HMI restart
- A watchdog timer event

Question 25
Marks: 1
Assume that a watchdog timer event indicates a loss of communication between the HMI and the PLC. Based on the packet captures, what is the most likely cause of the communications loss?
Choose one answer.
- The switch began dropping packets due to a MAC table overflow
- A port scan caused the PLC to reboot
- A forged bootp reply changed the PLC’s IP address
- ARP spoofing disrupted communications

Question 26
Marks: 1
Assume that a watchdog timer event indicates a loss of communication between the HMI and the PLC. Which packet most likely first caused the communications failure?
Choose one answer.
- 2922
- 2878
- 2920
- 2879

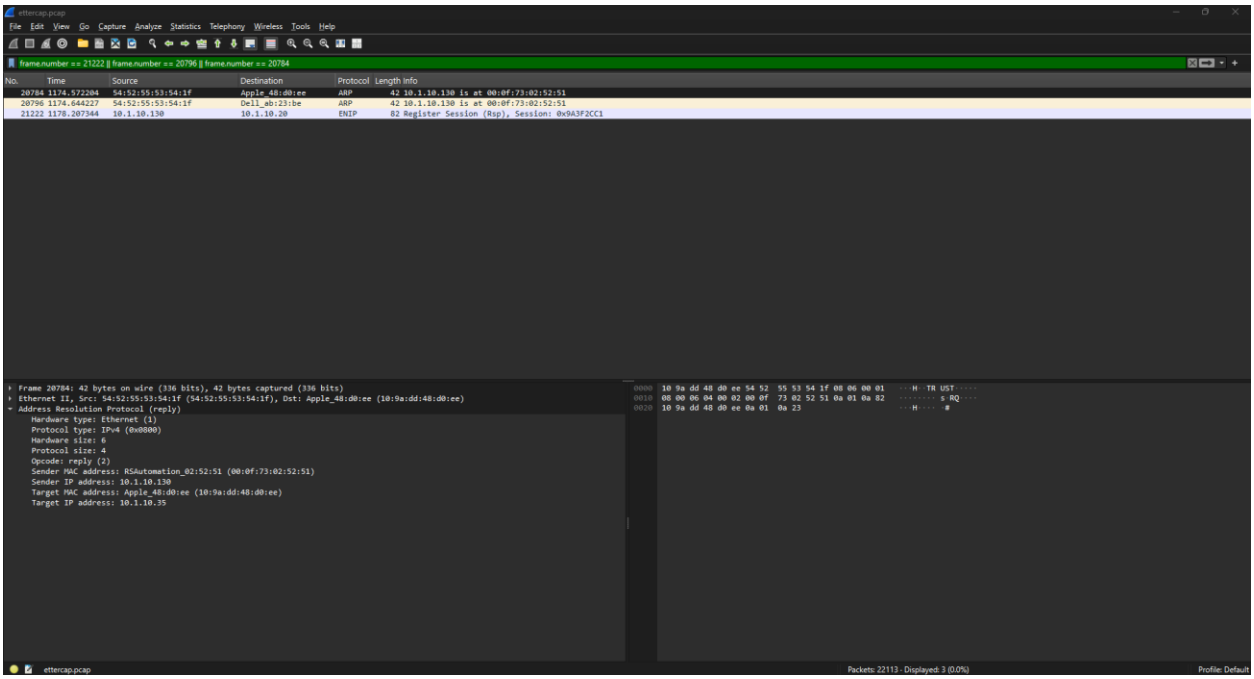
Question 27
Marks: 1
What appears to be the MAC address of the device which performed the ARP spoofing?
Choose one answer.
- 00:0f:73:02:52:51
- 54:52:55:53:54:1f
- 08:00:27:fb:b8:10
- 14:fe:b5:ab:23:be



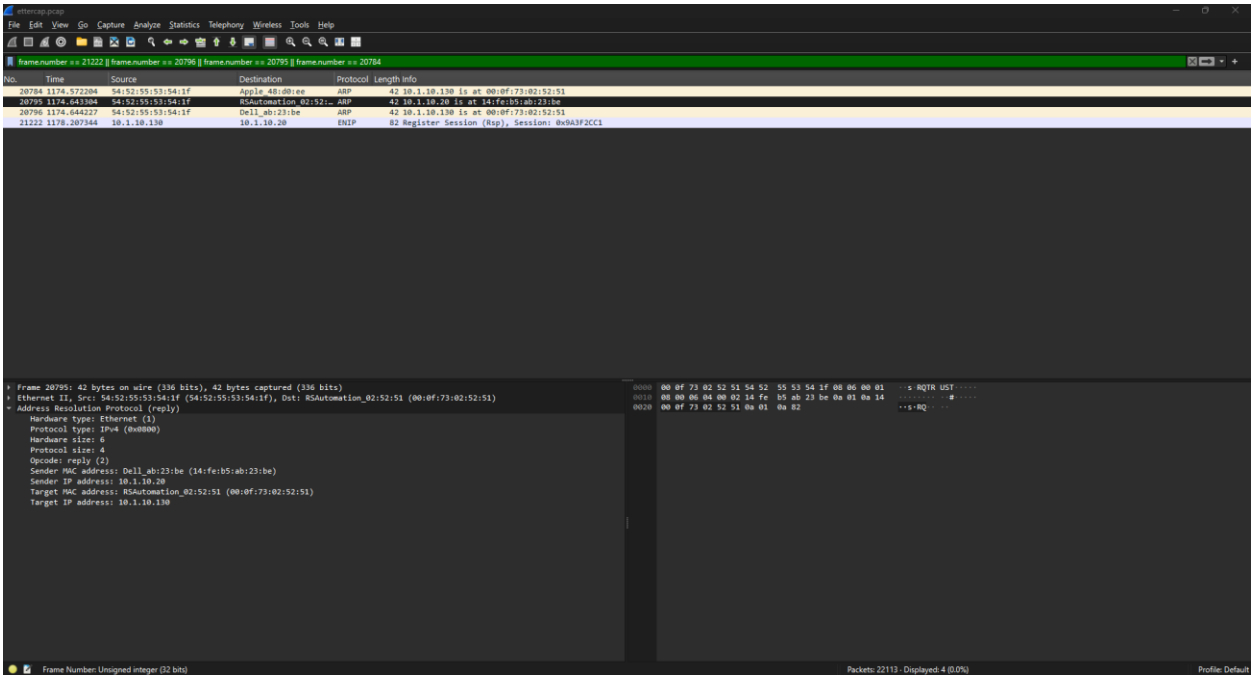
I searched for ARP to find the device using spoofing. After searching for a while, I found a packet that stated “Duplicate IP Address” and said it was also in use by another device on the network.

```
Question 28
Marks: 1
What event allowed the PLC and HMI connection to be restored?
Choose one answer.
        The HMI sent an ARP request and the response overwrote the spoofed ARP
        The spoofed ARP timed out
        The PLC sent a gratuitous ARP that overwrote the spoofed ARP
        The attackers spoofed an ARP packet with the correct settings
Question 29
Marks: 1
Which packet allowed communications between the HMI and PLC to be restored?
Choose one answer.
        21222
        20796
        20795
        20784
```

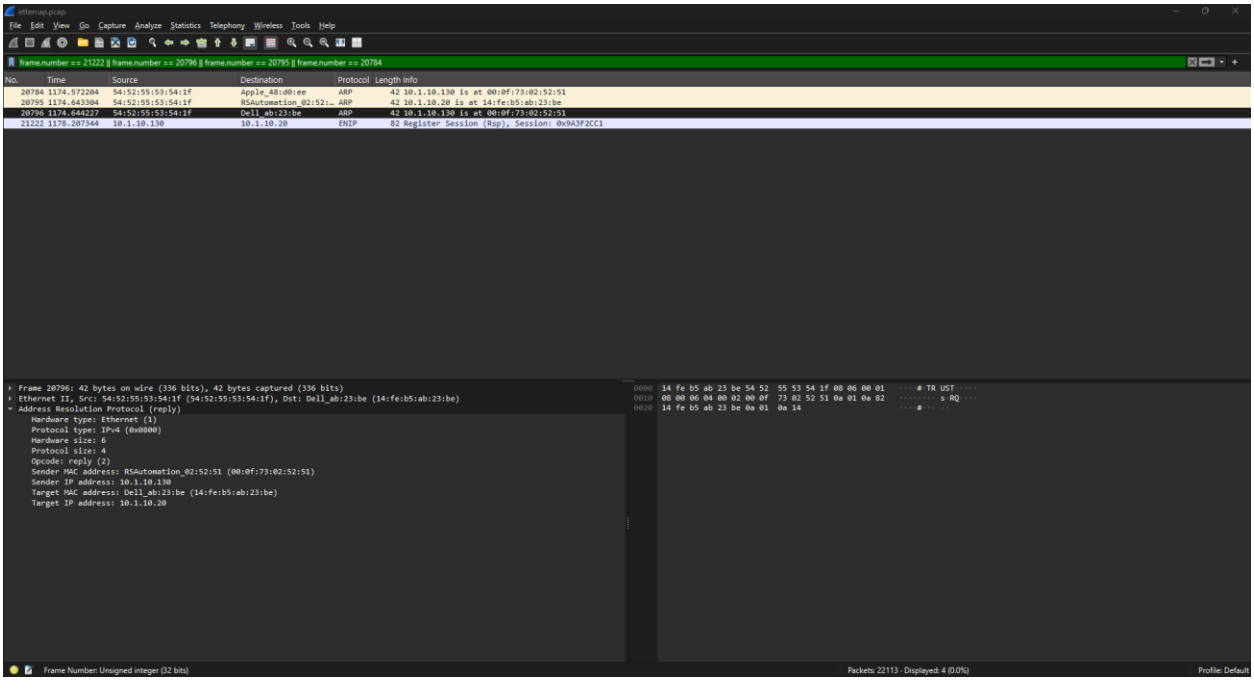
First I did a packet search. I used this Wireshark filter: “frame.number == 21222 || frame.number == 20796 || frame.number == 20795 || frame.number == 20784”. I’m filtering all the packets that are included in the possible answers. Packet 21222 is the only packet that looks different than the other 3. First, packet 21222 is a ENIP protocol vs the other 3 are using ARP.



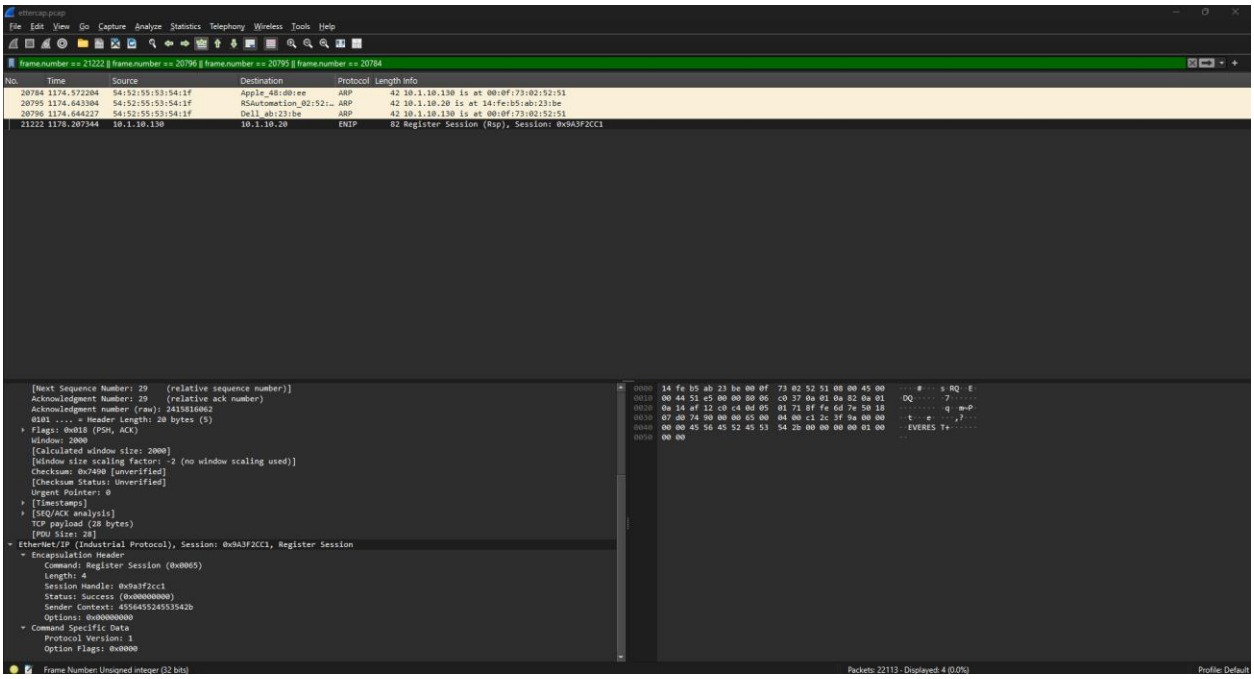
The first packet, 20784 is a ARP packet.



The second packet, 20795 is also an ARP packet.



The third packet, 20796 is a ARP packet.



But the last packet, 21222 is very different. It's using the ENIP protocol. And it's trying to register a session. It's using Ethernet/IP to connect. My guess is this is the chatbot trying to reestablish a connection to the client.