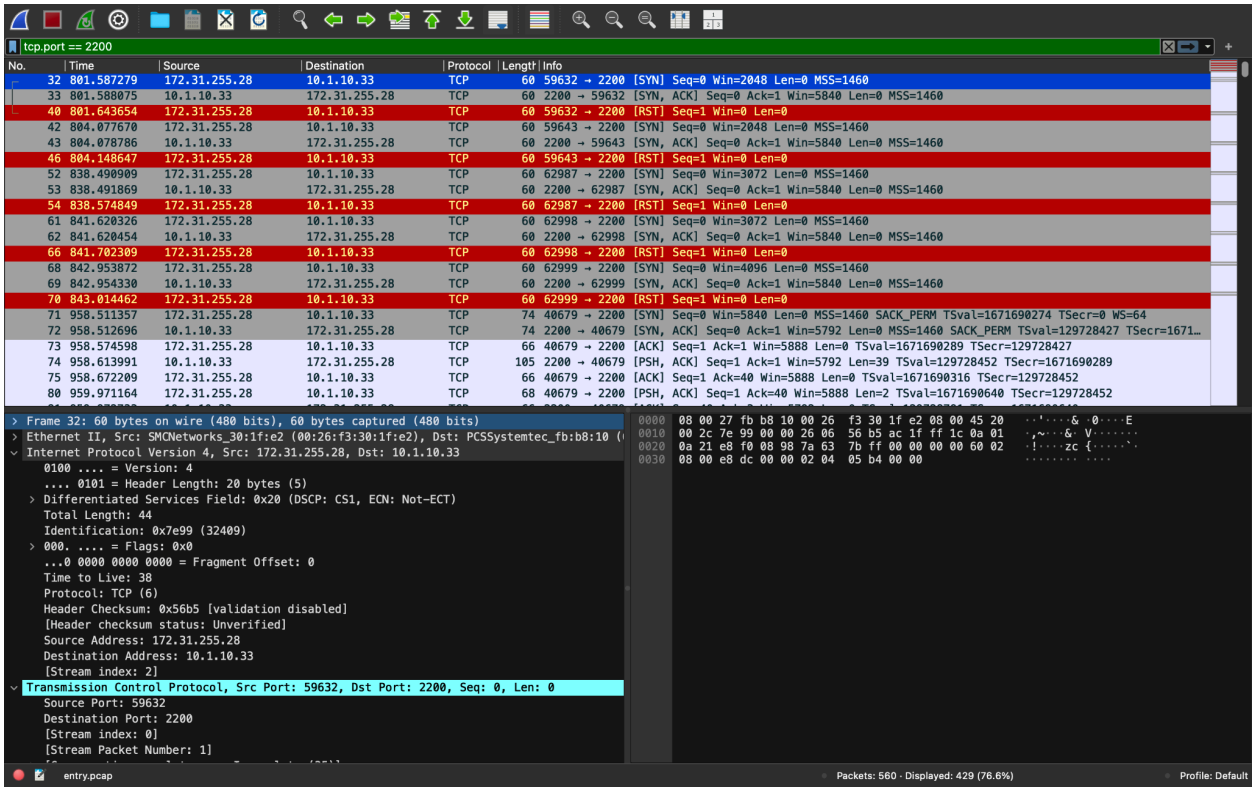
Samantha Jackson
CSCI4406
11-03-2024

Lab 8 - Network Forensics

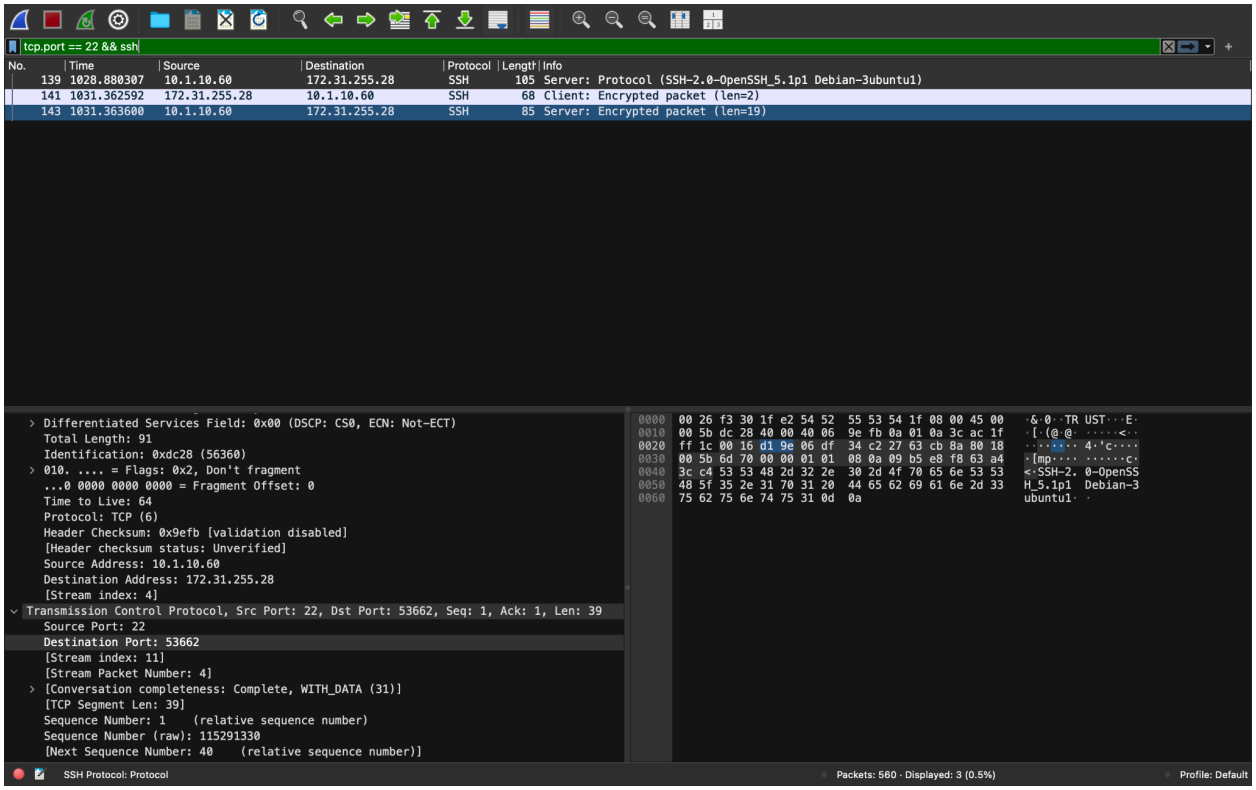
Question 1

What service appears to be running on port 2200?
Choose one answer.

- Industrial Control Interface
- Rockwell Automation PPTP
- Inter Carrier Interface
- Secure Shell



I checked port 2200 to see what protocol was running on it using the filter ‘tcp.port == 2200’ to see what packets were running on that particular port. Typically SSH uses TCP as a transport protocol with a well known port for SSH traffic being on 22. It’s possible that it could not be though and filtering by ssh reveals nothing but so does every other filter protocol.



When checking SSH protocols on port 22 you can see the destination of the request is 172.31.255.28 which is the same source as the TCP protocols on port 2200. All of these SSH protocols link directly into the TCP protocols. I can assume they are reliant on SSH.

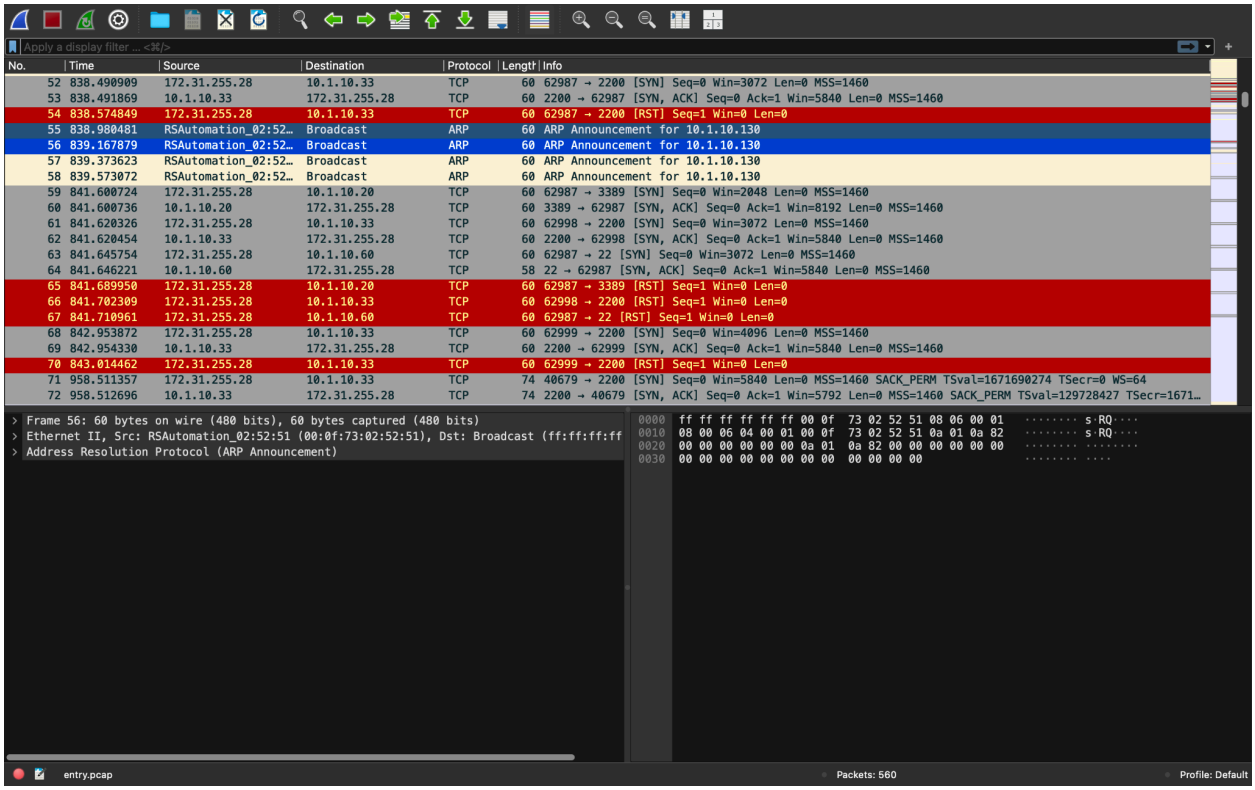
Question 2

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

My answer is going to make a lot of conjectures so just bear with me. Looking through the packets in entry.pcap you see a lot of TCP checks. This is indicative of the attackers searching for a network vulnerability. Network Port Scanners The SYN scanner in Nessus has a similar signature to what we see in the Wireshark file. You can see multiple SYN packets being sent to determine if the ports are open. If they are, the attackers received a SYN-ACK reply. You can also see that some of these connections are sending RST reset flags meaning that the server does not recognize the packets. Essentially a denial of service. After getting these scans we can assume the attacker knows the open ports for Netcat is a good option as it is specifically made for port interactions. Especially with tools like Reverse Shell which make this process straightforward.


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Lengtl Info
52 838.490909 172.31.255.28 10.1.10.33 TCP 60 62987 → 2200 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
53 838.491869 10.1.10.33 172.31.255.28 TCP 60 2200 → 62987 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
54 838.574849 172.31.255.28 10.1.10.33 TCP 60 62987 → 2200 [RST] Seq=1 Win=0 Len=0
55 838.980481 RSAutomation_02:52… Broadcast ARP 60 ARP Announcement for 10.1.10.130
56 839.167879 RSAutomation_02:52… Broadcast ARP 60 ARP Announcement for 10.1.10.130
57 839.373623 RSAutomation_02:52… Broadcast ARP 60 ARP Announcement for 10.1.10.130
58 839.573072 RSAutomation_02:52… Broadcast ARP 60 ARP Announcement for 10.1.10.130
59 841.600724 172.31.255.28 10.1.10.20 TCP 60 62987 → 3389 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
60 841.600736 10.1.10.20 172.31.255.28 TCP 60 3389 → 62987 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
61 841.620326 172.31.255.28 10.1.10.33 TCP 60 62998 → 2200 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
62 841.620454 10.1.10.33 172.31.255.28 TCP 60 2200 → 62998 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
63 841.645754 172.31.255.28 10.1.10.60 TCP 60 62987 → 22 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
64 841.646221 10.1.10.60 172.31.255.28 TCP 58 22 → 62987 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
65 841.689950 172.31.255.28 10.1.10.20 TCP 60 62987 → 3389 [RST] Seq=1 Win=0 Len=0
66 841.702309 172.31.255.28 10.1.10.33 TCP 60 62998 → 2200 [RST] Seq=1 Win=0 Len=0
67 841.710961 172.31.255.28 10.1.10.60 TCP 60 62987 → 22 [RST] Seq=1 Win=0 Len=0
68 842.953872 172.31.255.28 10.1.10.33 TCP 60 62999 → 2200 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
69 842.954330 10.1.10.33 172.31.255.28 TCP 60 2200 → 62999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
70 843.014462 172.31.255.28 10.1.10.33 TCP 60 62999 → 2200 [RST] Seq=1 Win=0 Len=0
71 958.511357 172.31.255.28 10.1.10.33 TCP 74 40679 → 2200 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=1671690274 TSecr=0 WS=64
72 958.512696 10.1.10.33 172.31.255.28 TCP 74 2200 → 40679 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=129728427 TSecr=1671…
Frame 56: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: RSAutomation_02:52:51 (00:0f:73:02:52:51), Dst: Broadcast (ff:ff:ff:ff
Address Resolution Protocol (ARP Announcement)
0000 ff ff ff ff ff ff 00 0f 73 02 52 51 08 06 00 01 ····· s·RQ····
0010 08 00 06 04 00 01 00 0f 73 02 52 51 0a 01 0a 82 ····· s·RQ····
0020 00 00 00 00 00 00 0a 01 0a 82 00 00 00 00 00 00 ····· ·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 ····· ····
entry.pcap
Packets: 560
Profile: Default

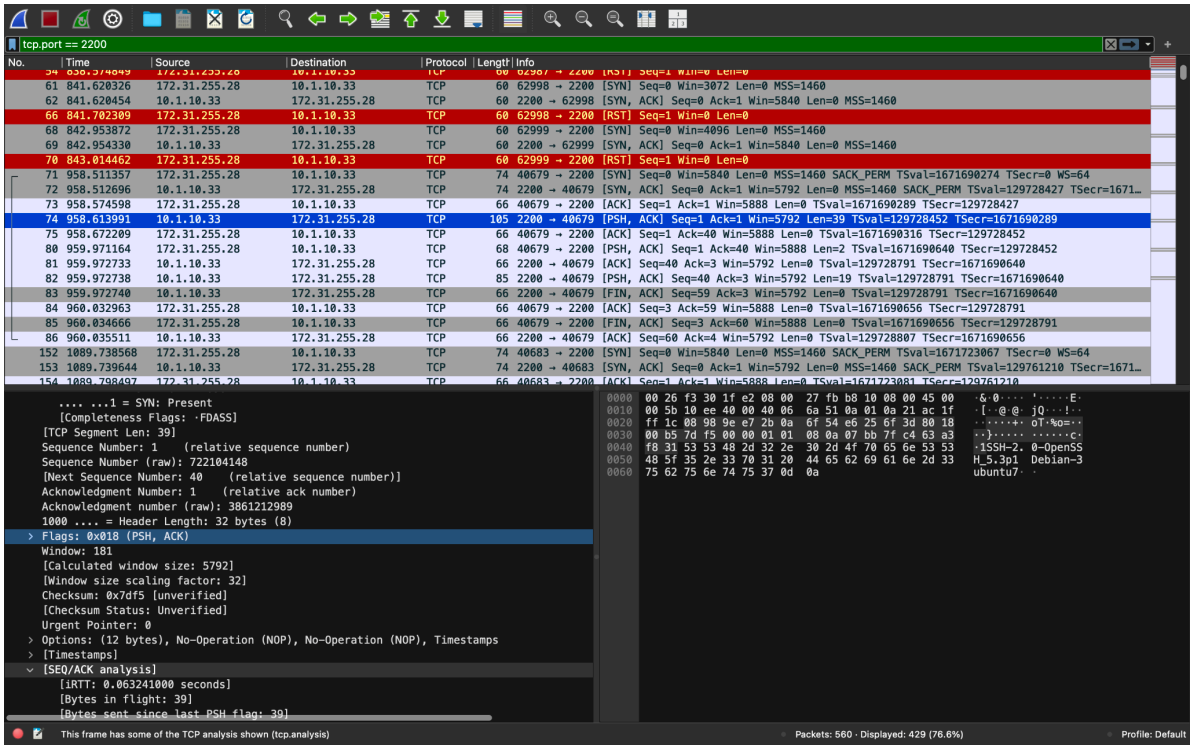
Question 3

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

This question is pretty straightforward. We're just going to check TCP connections on port 2200. You can see any instance with port 2200 open has a source IP of 10.1.10.33. Thus 10.1.10.33 has port 2200 open.



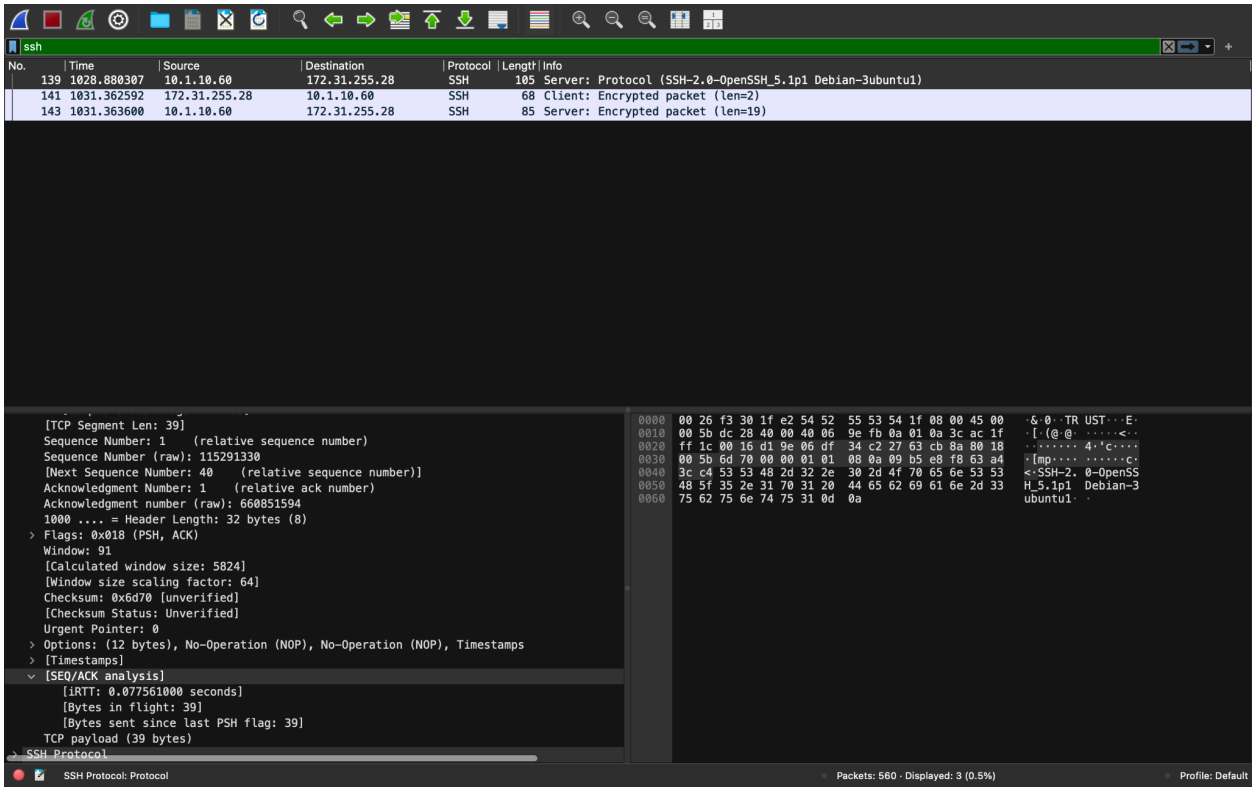
Question 4

Which version of SSH was the attacker using?

Choose one answer. OpenSSH 5.1p1

- WinSSH
- PuTTY
- OpenSSH 5.3p1
- OpenSSH 5.2

We can determine what version of SSH the attacker was using by checking the ssh filter. You can see that on packet 139 the attacker is using OpenSSH 5.1p1.



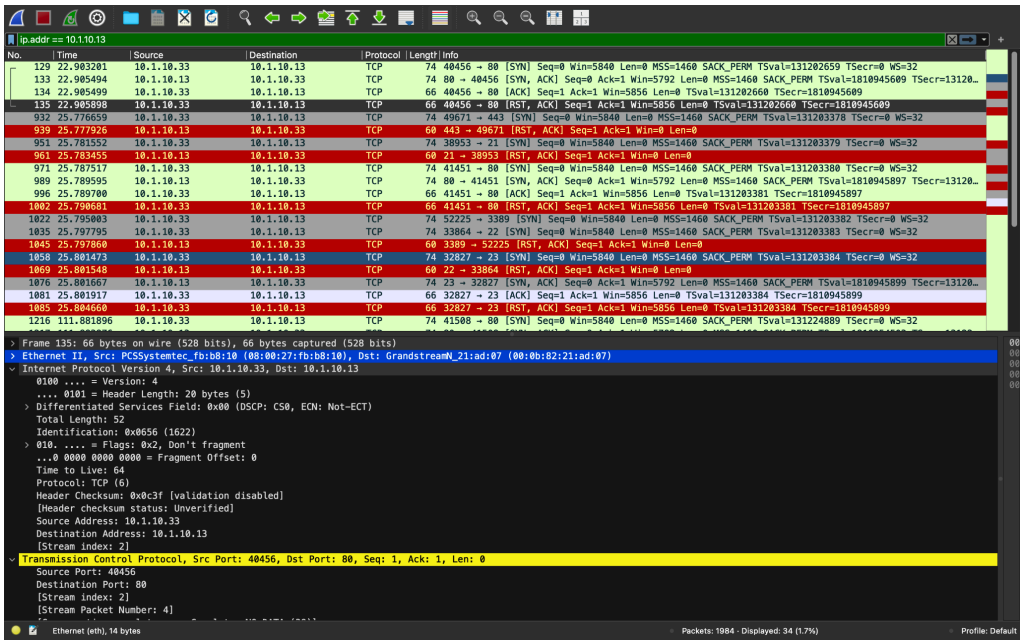
Question 5

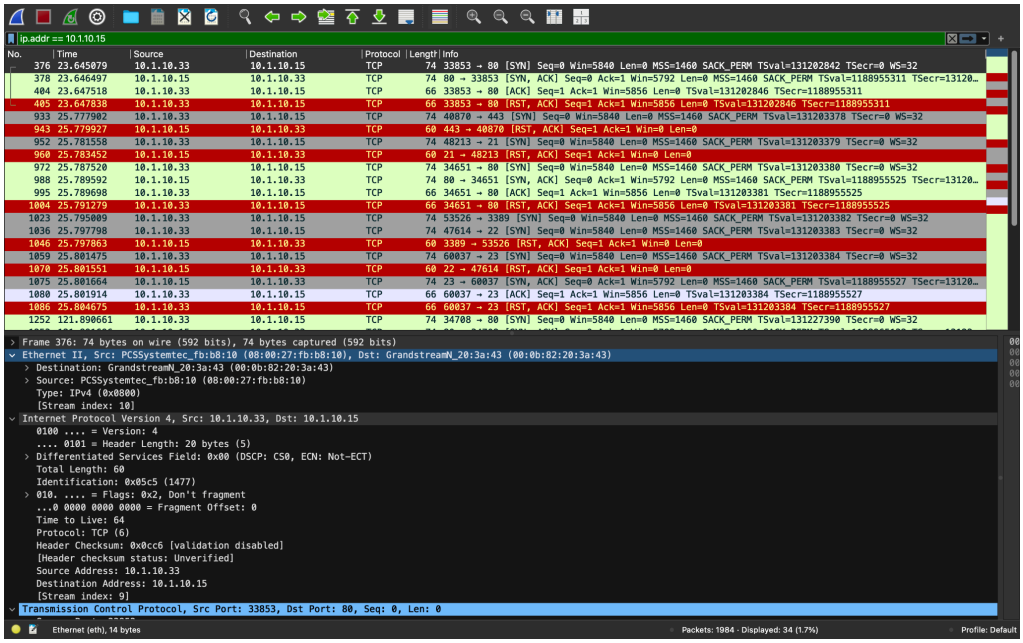
Which of the following IP addresses appear to be the same type of device?

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

We can determine whether or not the IP Addresses are on the same kind of device based on the destination. In this case we can see both 10.1.10.15 and 10.1.10.13 are running on a GrandstreamN device.





Question 6

How many IP addresses had port 3389 open?

Choose one answer. 9

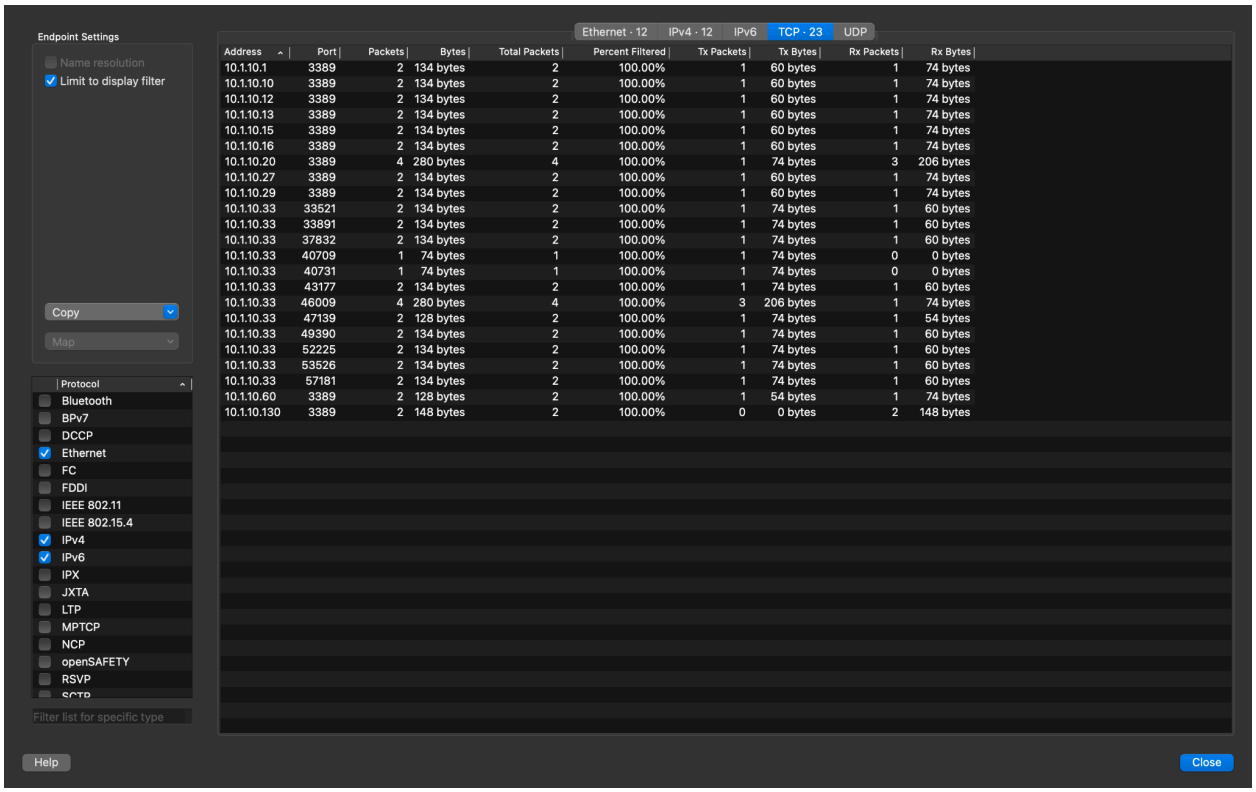
1

2

3

4

We can determine the IP addresses associated with port 3389 by doing a filter for ‘tcp.port == 3389’. After that we can go to Statistics > Endpoints. We get this result.



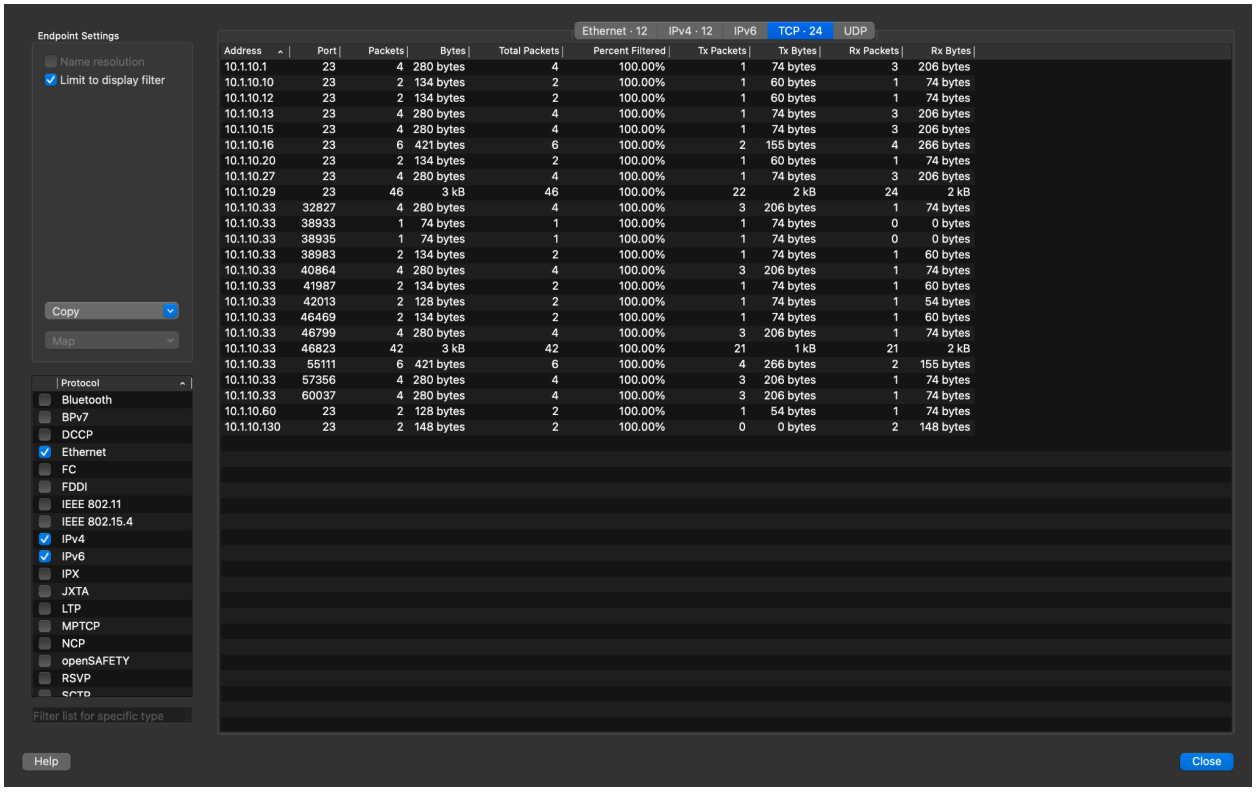
You can see that IP addresses: 10.1.10.1, 10.1.10.10, 10.1.10.12, 10.1.10.13, 10.1.10.15, 10.1.10.16, 10.1.10.20, 10.1.10.27, and 10.1.10.29 had port 3389 open at some point. Meaning that nine ports had port 3389 open.

Question 8

Which of the following IP addresses did NOT have port 23 open?
Choose one answer. None

- 10.1.10.10
- 10.1.10.27
- 10.1.10.16
- 10.1.10.29

We can determine which of the following IP addresses did not have port 23 open in the same way we solved question six. We'll do a filter for 'tcp.port == 23'. Then we'll go to Statistics > Endpoints. Ultimately all of these IP addresses had port 23 open at some point.



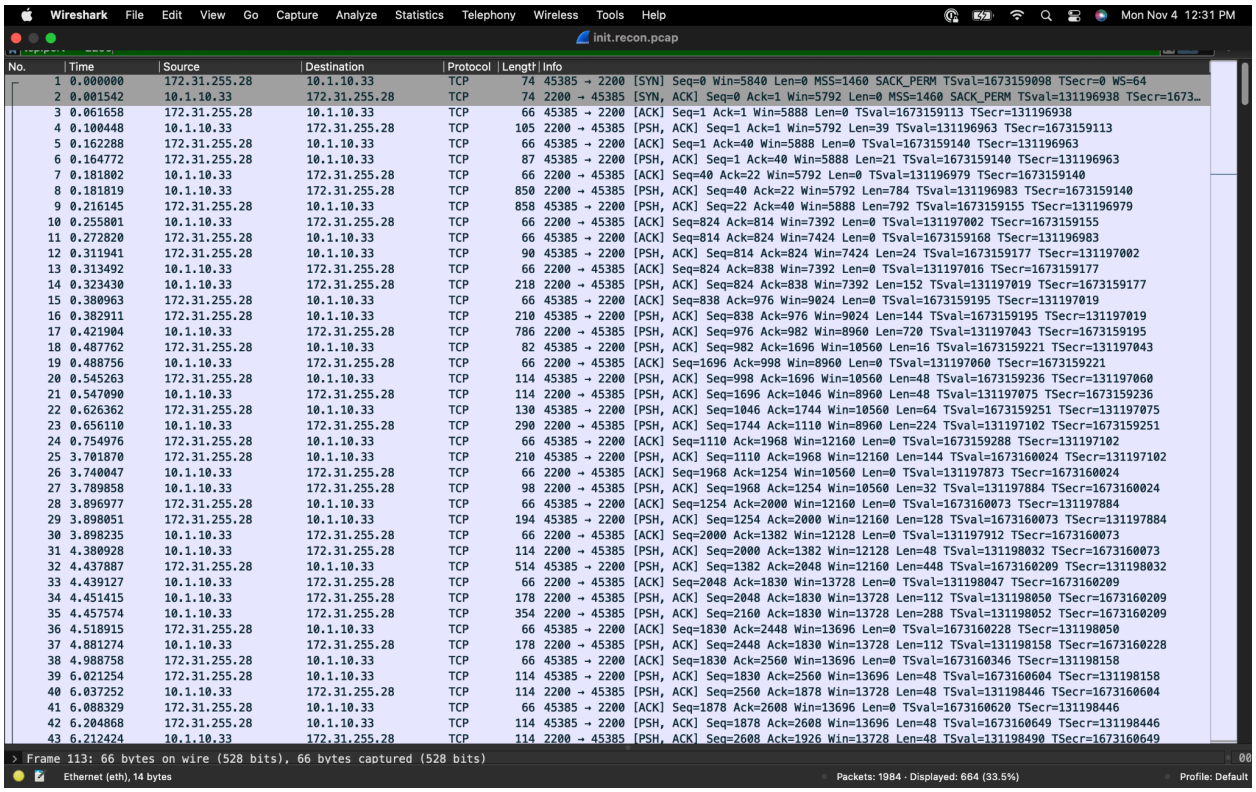
Address	Port	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.1.10.1	23	4	280 bytes	4	100.00%	1	74 bytes	3	206 bytes
10.1.10.10	23	2	134 bytes	2	100.00%	1	60 bytes	1	74 bytes
10.1.10.12	23	2	134 bytes	2	100.00%	1	60 bytes	1	74 bytes
10.1.10.13	23	4	280 bytes	4	100.00%	1	74 bytes	3	206 bytes
10.1.10.15	23	4	280 bytes	4	100.00%	1	74 bytes	3	206 bytes
10.1.10.16	23	6	421 bytes	6	100.00%	2	155 bytes	4	266 bytes
10.1.10.20	23	2	134 bytes	2	100.00%	1	60 bytes	1	74 bytes
10.1.10.27	23	4	280 bytes	4	100.00%	1	74 bytes	3	206 bytes
10.1.10.29	23	46	3 kB	46	100.00%	22	2 kB	24	2 kB
10.1.10.33	32827	4	280 bytes	4	100.00%	3	206 bytes	1	74 bytes
10.1.10.33	38933	1	74 bytes	1	100.00%	1	74 bytes	0	0 bytes
10.1.10.33	38935	1	74 bytes	1	100.00%	1	74 bytes	0	0 bytes
10.1.10.33	38983	2	134 bytes	2	100.00%	1	74 bytes	1	60 bytes
10.1.10.33	40864	4	280 bytes	4	100.00%	3	206 bytes	1	74 bytes
10.1.10.33	41987	2	134 bytes	2	100.00%	1	74 bytes	1	60 bytes
10.1.10.33	42013	2	128 bytes	2	100.00%	1	74 bytes	1	54 bytes
10.1.10.33	46469	2	134 bytes	2	100.00%	1	74 bytes	1	60 bytes
10.1.10.33	46799	4	280 bytes	4	100.00%	3	206 bytes	1	74 bytes
10.1.10.33	46823	42	3 kB	42	100.00%	21	1 kB	21	2 kB
10.1.10.33	55111	6	421 bytes	6	100.00%	4	266 bytes	2	155 bytes
10.1.10.33	57356	4	280 bytes	4	100.00%	3	206 bytes	1	74 bytes
10.1.10.33	60037	4	280 bytes	4	100.00%	3	206 bytes	1	74 bytes
10.1.10.60	23	2	128 bytes	2	100.00%	1	54 bytes	1	74 bytes
10.1.10.130	23	2	148 bytes	2	100.00%	0	0 bytes	2	148 bytes

Question 9

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

A common motif in this .pcap file is that any ports that have been scanned on the internal network have a packet with a RST, ACK modifier. TCP 2200 does not have any RST, ACK packets. This means that the port wasn't interacted with internally.

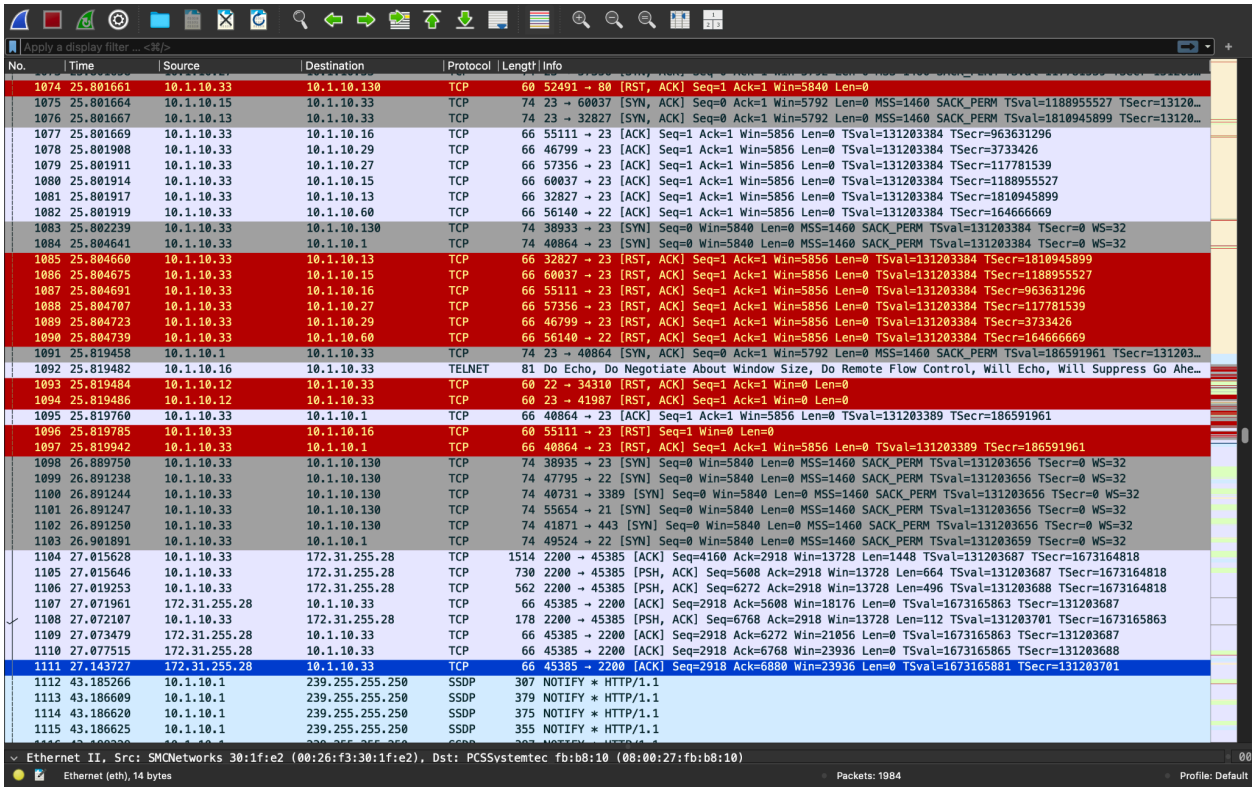


Question 10

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

We can see how long the port scans took to complete by seeing the time the TCP packets end and the SSDP protocols begin. In this case the packet at 1111 indicates the end of the scan at 27.134 seconds.



Question 17

What web server 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

By using HTTP stream on .130 we can determine what webserver is running on the .130 device. We'll use the filter "http.request.method == "GET"" then we'll go to Analyze > Follow > HTTP. Then we get this result: Firefox/3.6.24 for the user's web server.