Name of Student:- Mohit Ajaykumar Dhabuwala

Course: CYFI - 620 Investigation Technique – 1

AIM: While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.

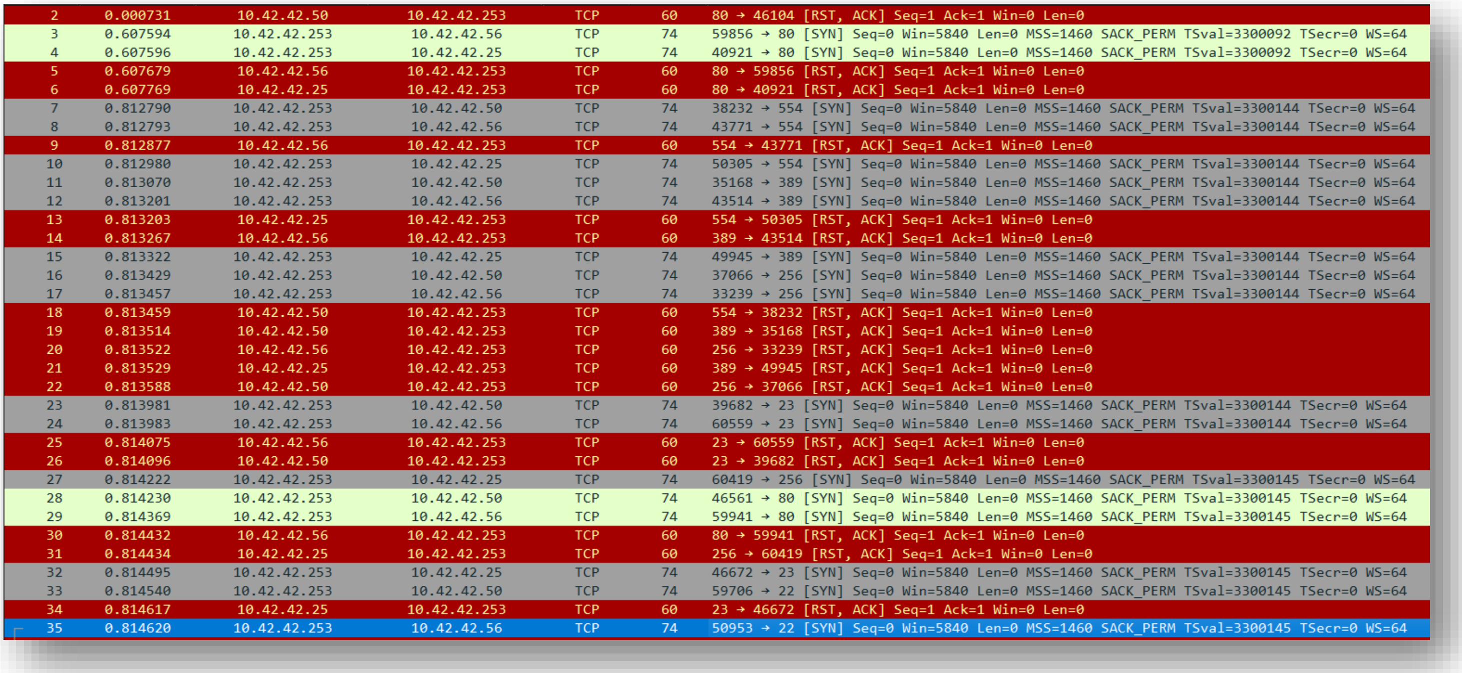
Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed… by you!

The .pcap evidence I attached to this assignment and in files directory. You must include image evidence and/or file path for every question. Each question is worth 16.66 points.

As the network forensic investigator, your mission is to answer the following question

1. What was the IP address of Mr. X's scanner?

Answer: The IP address of Me. X's scanner is "**10.42.42.253.**" This can be noted as there are 1000's of SYN packets originating from **10.42.42.253**, attempting to connect to 10.42.42.25 on different ports. There are no corresponding SYN-ACK packets in response to the SYN packets. On the contrary, the destination IP was sending **[RST, ACK]** packet which that destination IP 10.42.42.25 is either not responding or is blocking these connection attempts.



```
 2  0.000731  10.42.42.50   10.42.42.253  TCP  60  80 → 46104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 3  0.607594  10.42.42.253  10.42.42.56   TCP  74  59856 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300092 TSecr=0 WS=64
 4  0.607596  10.42.42.253  10.42.42.25   TCP  74  40921 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300092 TSecr=0 WS=64
 5  0.607679  10.42.42.56   10.42.42.253  TCP  60  80 → 59856 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 6  0.607769  10.42.42.25   10.42.42.253  TCP  60  80 → 40921 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 7  0.812790  10.42.42.253  10.42.42.50   TCP  74  38232 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
 8  0.812793  10.42.42.253  10.42.42.56   TCP  74  43771 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
 9  0.812877  10.42.42.56   10.42.42.253  TCP  60  554 → 43771 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10  0.812980  10.42.42.253  10.42.42.25   TCP  74  50305 → 554 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
11  0.813070  10.42.42.253  10.42.42.50   TCP  74  35168 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
12  0.813201  10.42.42.253  10.42.42.56   TCP  74  43514 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
13  0.813203  10.42.42.25   10.42.42.253  TCP  60  554 → 50305 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14  0.813267  10.42.42.56   10.42.42.253  TCP  60  389 → 43514 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15  0.813322  10.42.42.253  10.42.42.25   TCP  74  49945 → 389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
16  0.813429  10.42.42.253  10.42.42.50   TCP  74  37066 → 256 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
17  0.813457  10.42.42.253  10.42.42.56   TCP  74  33239 → 256 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
18  0.813459  10.42.42.50   10.42.42.253  TCP  60  554 → 38232 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19  0.813514  10.42.42.50   10.42.42.253  TCP  60  389 → 35168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20  0.813522  10.42.42.56   10.42.42.253  TCP  60  256 → 33239 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21  0.813529  10.42.42.25   10.42.42.253  TCP  60  389 → 49945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22  0.813588  10.42.42.50   10.42.42.253  TCP  60  256 → 37066 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23  0.813981  10.42.42.253  10.42.42.50   TCP  74  39682 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
24  0.813983  10.42.42.253  10.42.42.56   TCP  74  60559 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300144 TSecr=0 WS=64
25  0.814075  10.42.42.56   10.42.42.253  TCP  60  23 → 60559 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26  0.814096  10.42.42.50   10.42.42.253  TCP  60  23 → 39682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27  0.814222  10.42.42.253  10.42.42.25   TCP  74  60419 → 256 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
28  0.814230  10.42.42.253  10.42.42.50   TCP  74  46561 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
29  0.814369  10.42.42.253  10.42.42.56   TCP  74  59941 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
30  0.814432  10.42.42.56   10.42.42.253  TCP  60  80 → 59941 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31  0.814434  10.42.42.25   10.42.42.253  TCP  60  256 → 60419 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32  0.814495  10.42.42.253  10.42.42.25   TCP  74  46672 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
33  0.814540  10.42.42.253  10.42.42.50   TCP  74  59706 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
34  0.814617  10.42.42.25   10.42.42.253  TCP  60  23 → 46672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35  0.814620  10.42.42.253  10.42.42.56   TCP  74  50953 → 22 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300145 TSecr=0 WS=64
```

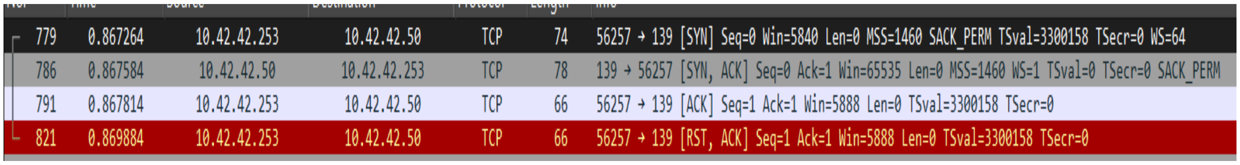
If we look at the packets from the first packet down, we can see that a single IP (10.42.42.253) is continuously sending packets with SYN flags to perform a port scan.

2. For the FIRST port scan that Mr. X conducted, C? (Note: the scan consisted of many thousands of packets.) Pick one:

- TCP SYN
- TCP ACK
- UDP
- TCP Connect
- TCP XMAS
- TCP RST

Answer: For the FIRST port scan that Mr. X conducted, what type of port scan was "**TCP CONNECT**".

The captured packets were filtered for those whose destination IP was 10.42.42.253 with the SYN and ACK flags turned on. Such packets reflect an established TCP connection during the scanning. On following the TCP stream, a sequence is clearly seen as shown in the figure below.

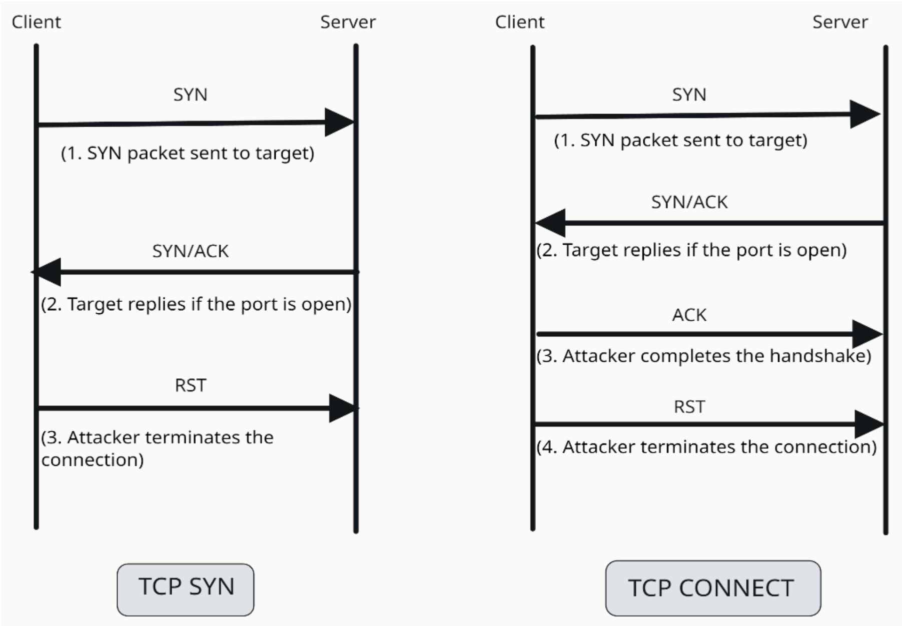


```
779  0.867264  10.42.42.253  10.42.42.50   TCP  74  56257 → 139 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3300158 TSecr=0 WS=64
786  0.867584  10.42.42.50   10.42.42.253  TCP  78  139 → 56257 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
791  0.867814  10.42.42.253  10.42.42.50   TCP  66  56257 → 139 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3300158 TSecr=0
821  0.869884  10.42.42.253  10.42.42.50   TCP  66  56257 → 139 [RST, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3300158 TSecr=0
```

The IP belonging to Mr. X sends a SYN packet towards the target IP, **10.42.42.50** (numbered 779); to connect. The packet received from **10.42.42.50** (number 786) responds with a SYN-ACK, showing the target port to be open and accepting the connection. Mr. X completes the TCP three-way handshake by sending an ACK packet, thus establishing the connection.

After the connection is established, the target at **10.42.42.50** sends a packet of **RST-ACK** to terminate the connection, which means this is the end of the communication session.

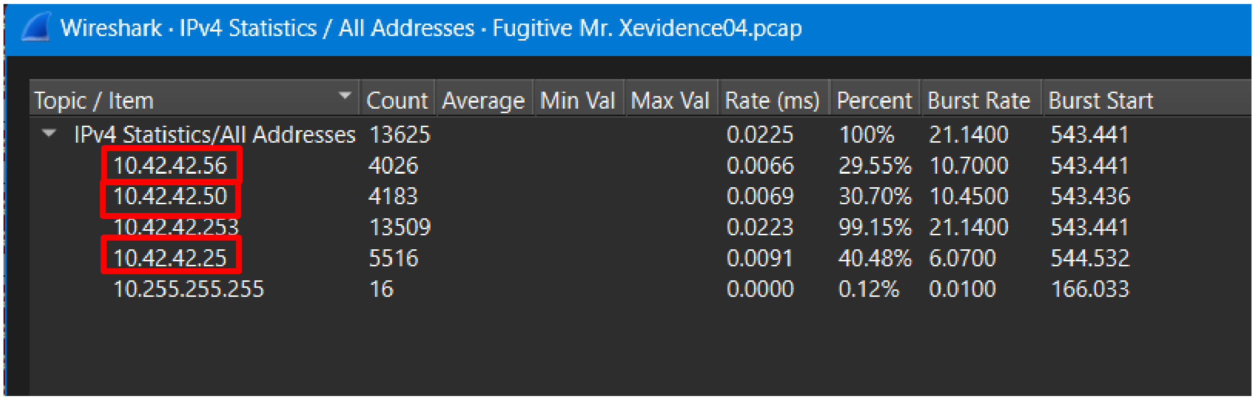
This behavior helps to identify the use of two possible scanning techniques: **TCP Connect** and **TCP SYN Scan**. In a **TCP SYN Scan**, the attacker sends a SYN packet and waits briefly for a SYN-ACK in response, which would indicate the port is open, without completing the handshake. Unlike TCP SYN scan, a TCP Connect scan goes all the way, completing the entire three-way handshake process to establish a full TCP connection with the target port. This means it sends a SYN packet, waits for a SYN-ACK response, and then sends a final ACK to confirm the connection.


Client
Server
SYN
(1. SYN packet sent to target)
SYN/ACK
(2. Target replies if the port is open)
RST
(3. Attacker terminates the connection)
TCP SYN
Client
Server
SYN
(1. SYN packet sent to target)
SYN/ACK
(2. Target replies if the port is open)
ACK
(3. Attacker completes the handshake)
RST
(4. Attacker terminates the connection)
TCP CONNECT

Thus, the sequence of events represents a “TCP CONNECT Scan”, where Mr. X completes a handshake to successfully connect to the target before the connection gets reset.

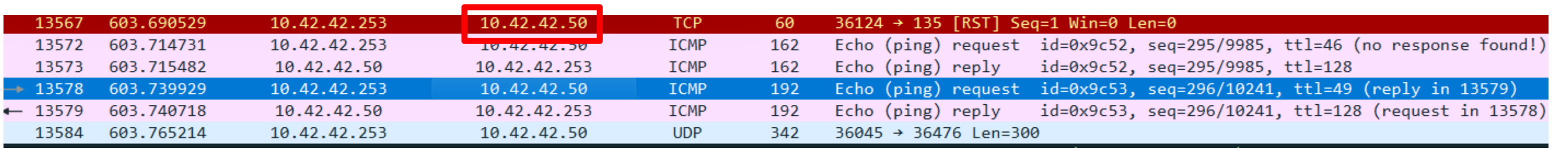
3. What were the IP addresses of the targets Mr. X discovered?

Answer: The IP addresses that Mr. X discovered are: **10.42.42.25 (apple device)**, **10.42.42.50 (windows device)**, and **10.42.42.56 (unidentified)**. It can be found in the menu statistics->IPv4 Statistics -> All Addresses

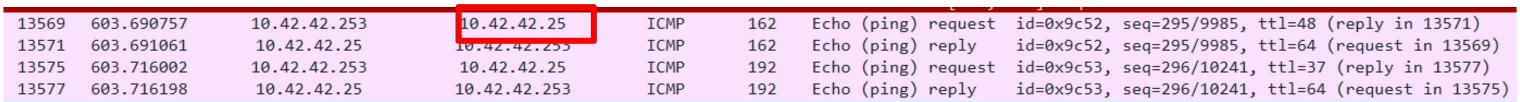


Wireshark · IPv4 Statistics / All Addresses · Fugitive Mr. Xevidence04.pcap

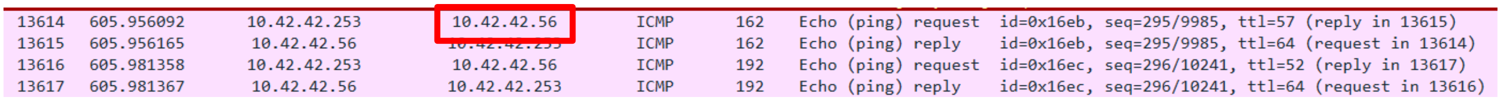
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	13625				0.0225	100%	21.1400	543.441
10.42.42.56	4026				0.0066	29.55%	10.7000	543.441
10.42.42.50	4183				0.0069	30.70%	10.4500	543.436
10.42.42.253	13509				0.0223	99.15%	21.1400	543.441
10.42.42.25	5516				0.0091	40.48%	6.0700	544.532
10.255.255.255	16				0.0000	0.12%	0.0100	166.033



```
13567  603.690529  10.42.42.253  10.42.42.50   TCP    60  36124 → 135 [RST] Seq=1 Win=0 Len=0
13572  603.714731  10.42.42.253  10.42.42.50   ICMP  162  Echo (ping) request  id=0x9c52, seq=295/9985, ttl=46 (no response found!)
13573  603.715482  10.42.42.50   10.42.42.253  ICMP  162  Echo (ping) reply    id=0x9c52, seq=295/9985, ttl=128
13578  603.739929  10.42.42.253  10.42.42.50   ICMP  192  Echo (ping) request  id=0x9c53, seq=296/10241, ttl=49 (reply in 13579)
13579  603.740718  10.42.42.50   10.42.42.253  ICMP  192  Echo (ping) reply    id=0x9c53, seq=296/10241, ttl=128 (request in 13578)
13584  603.765214  10.42.42.253  10.42.42.50   UDP   342  36045 → 36476 Len=300
```



```
13569  603.690757  10.42.42.253  10.42.42.25   ICMP  162  Echo (ping) request  id=0x9c52, seq=295/9985, ttl=48 (reply in 13571)
13571  603.691061  10.42.42.25   10.42.42.253  ICMP  162  Echo (ping) reply    id=0x9c52, seq=295/9985, ttl=64 (request in 13569)
13575  603.716002  10.42.42.253  10.42.42.25   ICMP  192  Echo (ping) request  id=0x9c53, seq=296/10241, ttl=37 (reply in 13577)
13577  603.716198  10.42.42.25   10.42.42.253  ICMP  192  Echo (ping) reply    id=0x9c53, seq=296/10241, ttl=64 (request in 13575)
```

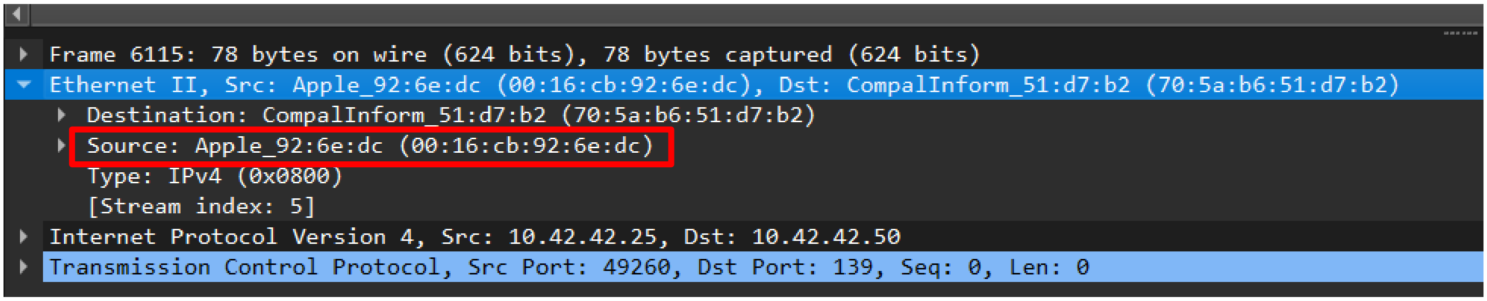


```
13614  605.956092  10.42.42.253  10.42.42.56   ICMP  162  Echo (ping) request  id=0x16eb, seq=295/9985, ttl=57 (reply in 13615)
13615  605.956165  10.42.42.56   10.42.42.253  ICMP  162  Echo (ping) reply    id=0x16eb, seq=295/9985, ttl=64 (request in 13614)
13616  605.981358  10.42.42.253  10.42.42.56   ICMP  192  Echo (ping) request  id=0x16ec, seq=296/10241, ttl=52 (reply in 13617)
13617  605.981367  10.42.42.56   10.42.42.253  ICMP  192  Echo (ping) reply    id=0x16ec, seq=296/10241, ttl=64 (request in 13616)
```

These images suggest that Mr. X has tried to communicate with this devices during his attempt to find the open ports.

4. What was the MAC address of the Apple system he found?

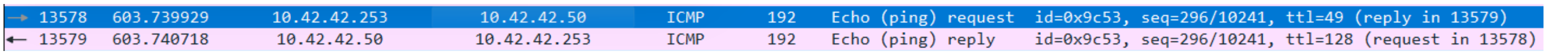
Answer: The MAC address of the Apple system found by Mr. X is "**00:16:CB:92:6E:DC**". There are 2 evidence to support my finding that this IP is for the apple device. The first one is the device name/ID that is "**Apple_92:6e:dc**"



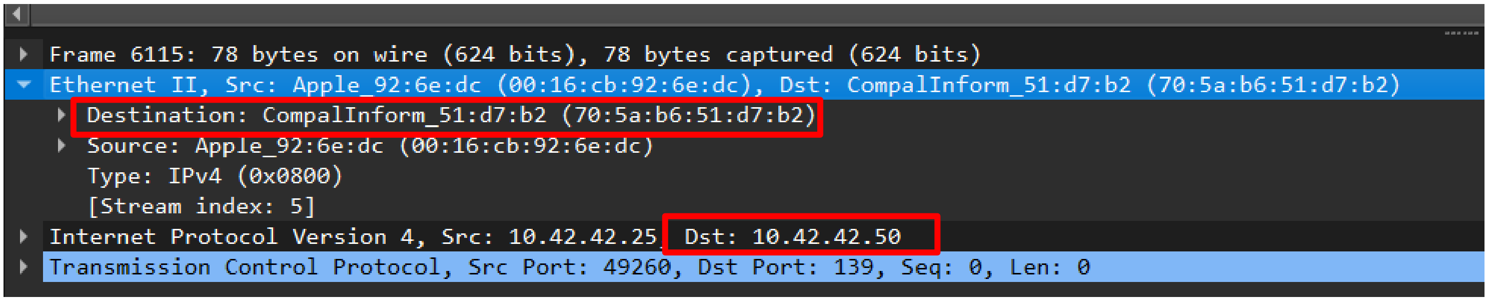
```
▸ Frame 6115: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▾ Ethernet II, Src: Apple_92:6e:dc (00:16:cb:92:6e:dc), Dst: CompalInform_51:d7:b2 (70:5a:b6:51:d7:b2)
   ▸ Destination: CompalInform_51:d7:b2 (70:5a:b6:51:d7:b2)
   ▸ Source: Apple_92:6e:dc (00:16:cb:92:6e:dc)
     Type: IPv4 (0x0800)
     [Stream index: 5]
▸ Internet Protocol Version 4, Src: 10.42.42.25, Dst: 10.42.42.50
▸ Transmission Control Protocol, Src Port: 49260, Dst Port: 139, Seq: 0, Len: 0
```

5. What was the IP address of the Windows system he found?

Answer: The IP address of the Windows system found by Mr. X is "**10.42.42.50.**" **(packet 13578 and 13579)**This IP address corresponds to Windows machine as the 10.42.42.50 replied with a TTL of 128 which indicates that this is the default TTL value. This suggests the reply was likely sent from a Windows machine since Windows typically sets TTL to 128.



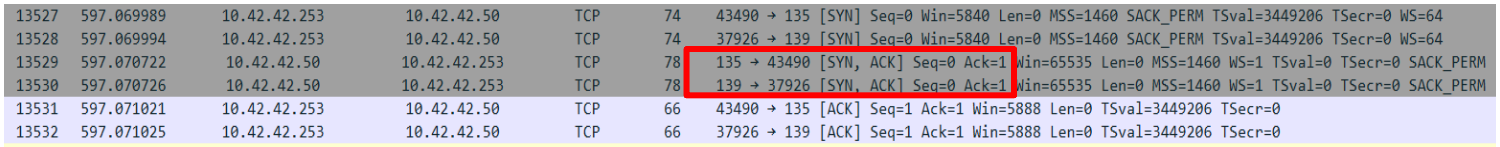
```
→ 13578   603.739929   10.42.42.253   10.42.42.50    ICMP   192   Echo (ping) request   id=0x9c53, seq=296/10241, ttl=49 (reply in 13579)
← 13579   603.740718   10.42.42.50    10.42.42.253   ICMP   192   Echo (ping) reply     id=0x9c53, seq=296/10241, ttl=128 (request in 13578)
```



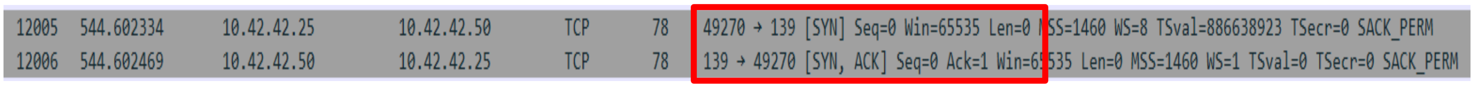
```
▸ Frame 6115: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▾ Ethernet II, Src: Apple_92:6e:dc (00:16:cb:92:6e:dc), Dst: CompalInform_51:d7:b2 (70:5a:b6:51:d7:b2)
   ▸ Destination: CompalInform_51:d7:b2 (70:5a:b6:51:d7:b2)
   ▸ Source: Apple_92:6e:dc (00:16:cb:92:6e:dc)
     Type: IPv4 (0x0800)
     [Stream index: 5]
▸ Internet Protocol Version 4, Src: 10.42.42.25 Dst: 10.42.42.50
▸ Transmission Control Protocol, Src Port: 49260, Dst Port: 139, Seq: 0, Len: 0
```

6. What TCP ports were open on the Windows system? (Please list the decimal numbers from lowest to highest.)

Answer: The TCP ports **135 (packet 13529)** and **139 (packet 12005)** are open on the Windows system with the IP address “10.42.42.50.” This is confirmed by receiving a [SYN ACK] packet for both ports, where the TCP packet shows "seq = 0" and "ack = 1," indicating the second step of the TCP three-way handshake.



```
13527  597.069989   10.42.42.253   10.42.42.50    TCP   74   43490 → 135 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3449206 TSecr=0 WS=64
13528  597.069994   10.42.42.253   10.42.42.50    TCP   74   37926 → 139 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3449206 TSecr=0 WS=64
13529  597.070722   10.42.42.50    10.42.42.253   TCP   78   135 → 43490 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
13530  597.070726   10.42.42.50    10.42.42.253   TCP   78   139 → 37926 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
13531  597.071021   10.42.42.253   10.42.42.50    TCP   66   43490 → 135 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3449206 TSecr=0
13532  597.071025   10.42.42.253   10.42.42.50    TCP   66   37926 → 139 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=3449206 TSecr=0
```



```
12005  544.602334   10.42.42.25    10.42.42.50    TCP   78   49270 → 139 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=886638923 TSecr=0 SACK_PERM
12006  544.602469   10.42.42.50    10.42.42.25    TCP   78   139 → 49270 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
```