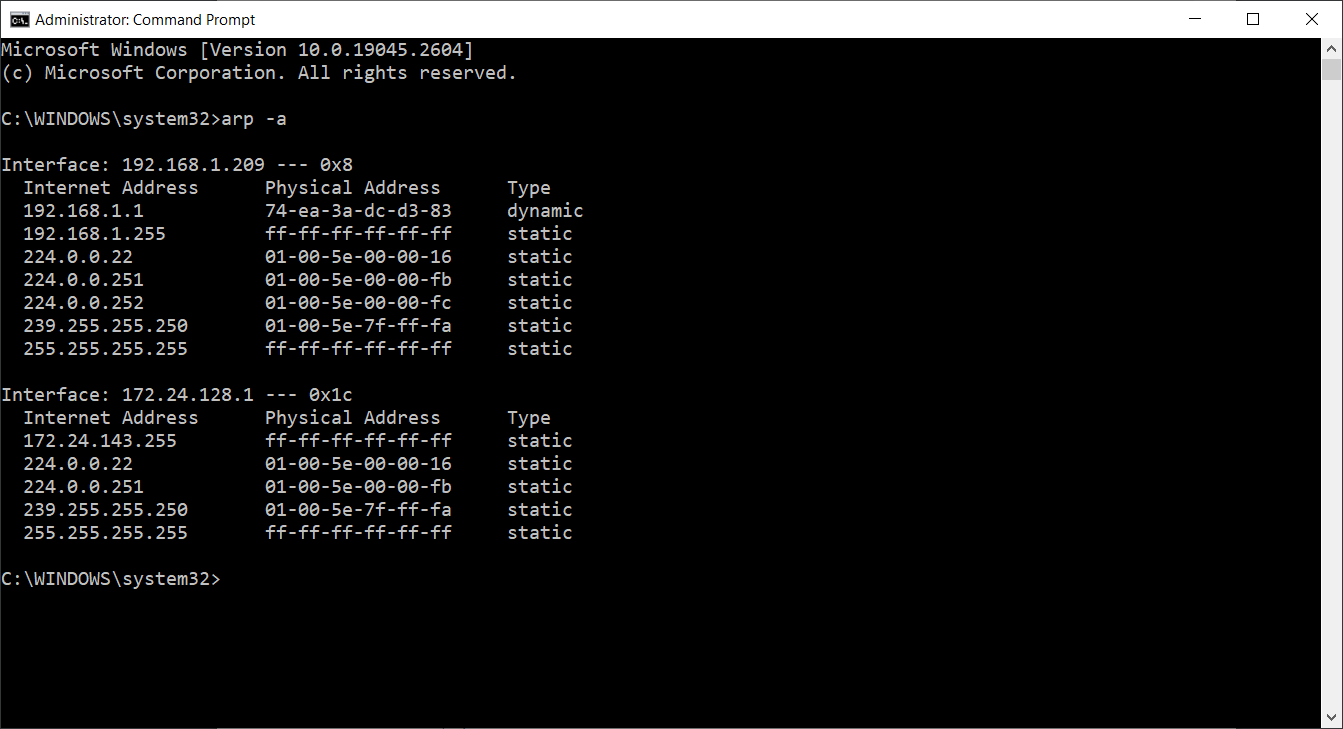
Exercise 1 – Basic network stuff.

Use the arp command and paste the output from the arp table on your system:



Use the route command and paste the output from the routing table on your system:

Table for IPv4:

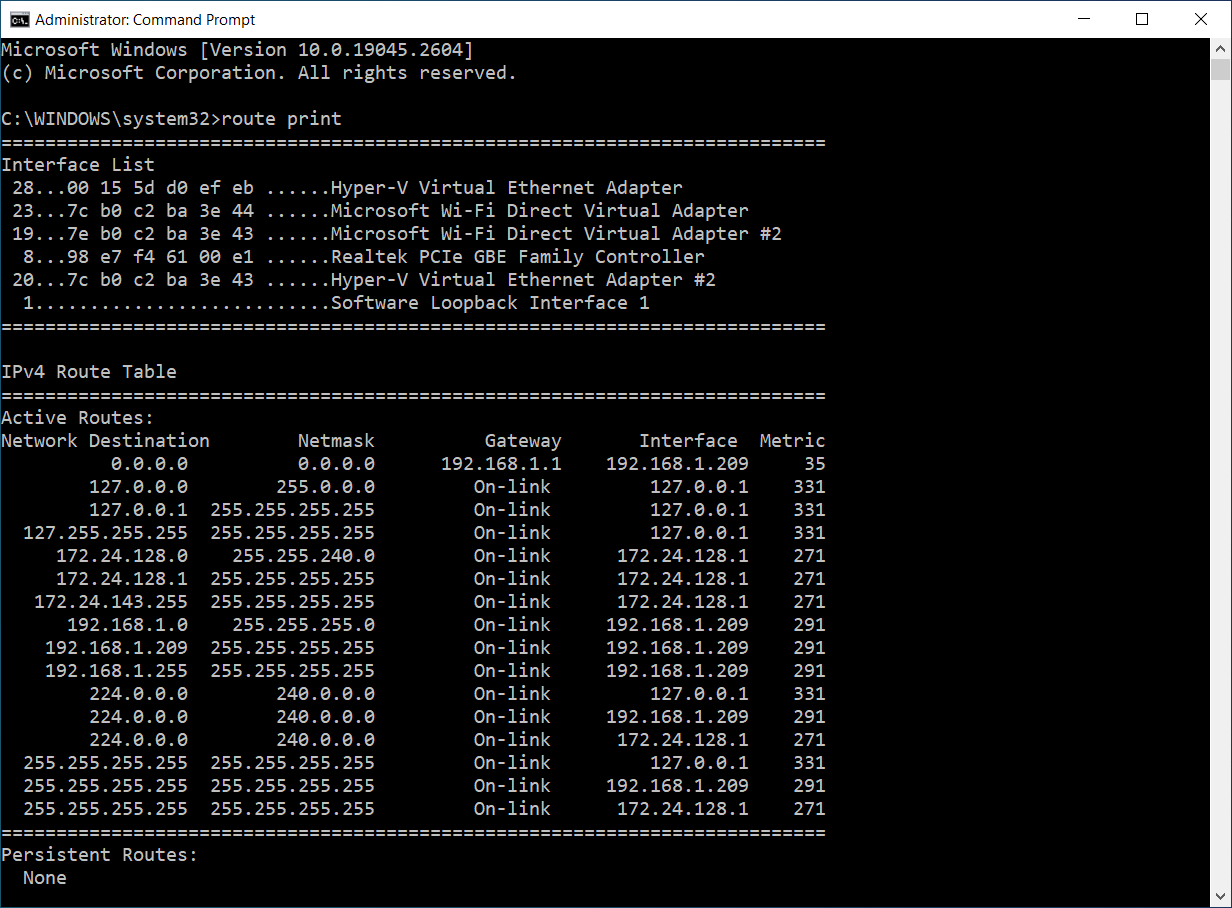
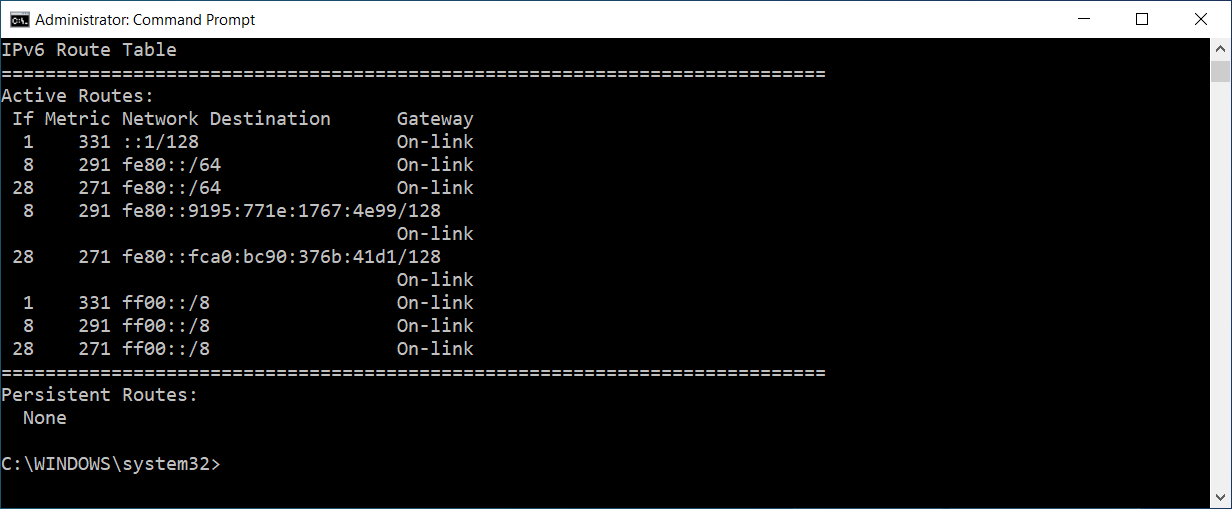
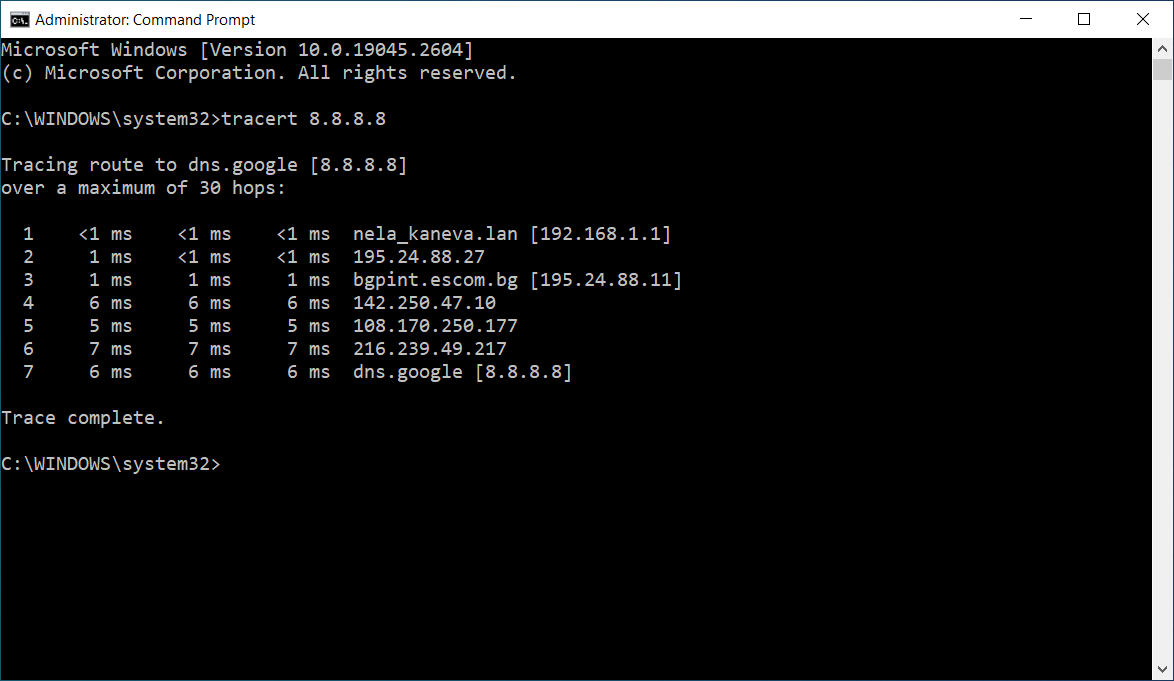


Table for IPv6:



Use the traceroute command on your system and observe the hops to Google’s DNS, 8.8.8.8. Paste the full output from the command bellow showing all the hops from your system to 8.8.8.8.



Why would you need to use the ping command?

Answer: To check if a machine has internet access and can communicate with other computers or network devices.

Write down the TCP/UDP ports of the most commonly used services bellow in the form of TCP[PORT] or UDP[PORT]. As an example, the first two answers have been filled in:

• HTTP – TCP80

• SNMP – UDP161

• HTTPS – TCP443 and UDP443

• DNS client – UDPP53

• DNS zone transfer – TCP53

• SMTP – TCP25

• SSH – TCP22

• FTP – TCP21

• Telnet – TCP23

• MSSQL - TCP**1433**, **4022**, **135**, **1434**, and UDP**1434**

• MySQL – TCP3306

• PostreSQL – TCP5432

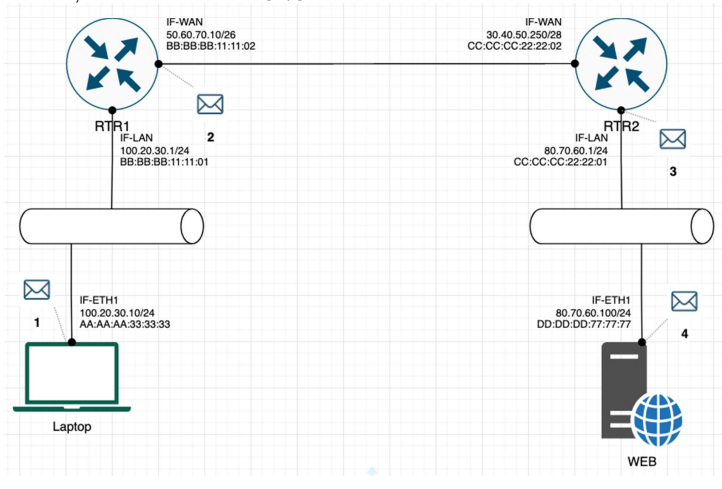
• RDP (Remote Desktop Protocol) – TCP3389 and UDP3389

• NTP – UDP123

• NFS – UDP2049

Exercise 2 – TCP/IP Basics.

The letter symbol ✉, represents the IP packet as it travels across the network. In the example shown, the laptop attempts to communicate with the web server in question. During its travel the packet will be forwarded across the network nodes and will eventually end up across six network interfaces before it reaches the web server. Each packet as part of the TCP/IP Stack contains fields for the source and destination MAC Address, IP Address and the TCP/UDP Port.



For each of the packet locations shown, 1 to 4 write down the source and destination MAC addresses of the packet as it travels across the network interfaces.

1. The laptop initiates communication with the web server and prepares a packet. What would the packet look like at this stage?

♣ SRC IP: laptop's ip address / or 100.20.30.10/24

♣ DST IP: web server's ip address / or 80.70.60.100/24

♣ SRC MAC: AA:AA:AA:33:33:33

♣ DST MAC: BB:BB:BB:11:11:01

1. RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IFWAN. What would the packet look like at this stage?

♣ SRC IP: laptop's ip address / or 100.20.30.10/24

♣ DST IP: web server's ip address / or 80.70.60.100/24

♣ SRC MAC: BB:BB:BB:11:11:01

♣ DST MAC: CC:CC:CC:22:22:01

1. RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IFLAN. What would the packet look like at this stage?

♣ SRC IP: laptop's ip address / or 100.20.30.10/24

♣ DST IP: web server's ip address / or 80.70.60.100/24

♣ SRC MAC: CC:CC:CC:22:22:01

♣ DST MAC: DD:DD:DD:77:77:77

1. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?

♣ SRC IP: web server's ip address / or 80.70.60.100/24

♣ DST IP: laptop's ip address / or 100.20.30.10/24

♣ SRC MAC: DD:DD:DD:77:77:77

♣ DST MAC: CC:CC:CC:22:22:01

Since we are talking about web traffic (www) in the example, which transport layer protocol will most probably be used?

* TCP
* UDP

If we do a traffic analysis with a network packet monitoring tool like WireShark, what can we expect to see for the source and destination ports when the laptop sends the packet?

• SRC PORT: A random port number from the range 49152 to 65535  
• DST PORT: Port 80 for HTTP, Port 443 for HTTPS

Similarly, and vice versa, what can we expect to see as destination ports when the Web server sends a response packet back?

• SRC PORT: Port 80 for HTTP, Port 443 for HTTPS  
• DST PORT: Same port number as in the original request

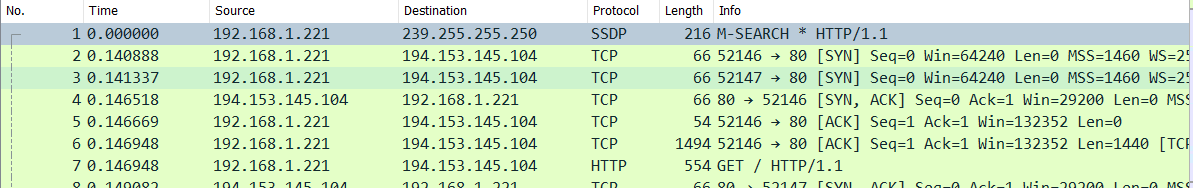
How many broadcast domains are there in the exhibit shown? – 4

Exercise 3 – Traffic analysis and identifying the OSI layers of the network packets.

Prerequisite: Search online and get familiar with the TCP’s three-way handshake. Learn how to capture the three way handshake using Wireshark. Install Wireshark on your computer and use it to capture traffic against a website or a server or your choice. It is recommended that you capture traffic against a simple website. Name and the IP address of the website you plan to capture traffic:

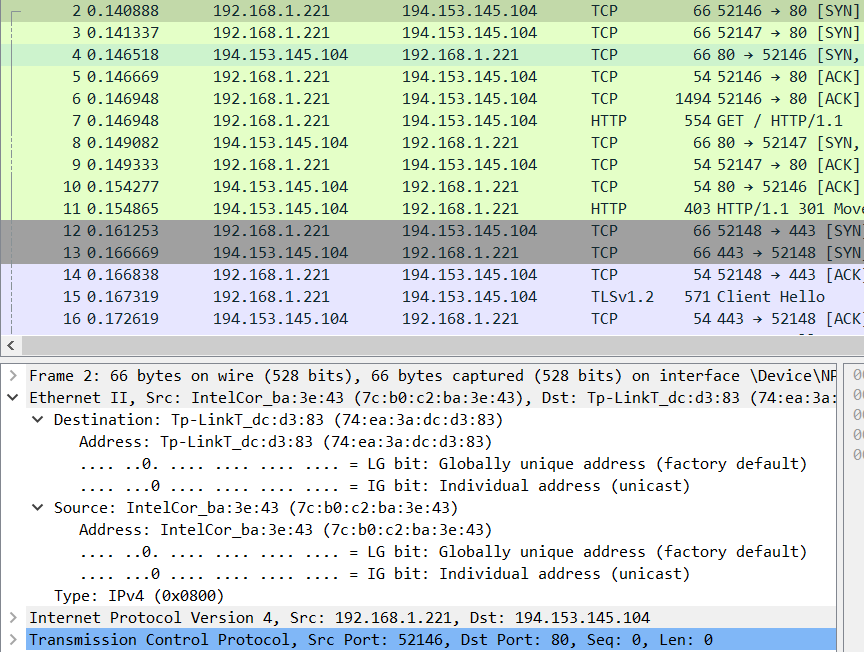
Analyze the TCP’s three-way handshake and using screenshots from the Wireshark window answer the questions bellow:

1. What is the source IP (of the initiating host): 192.168.1.221  
2. What is the destination IP? (target website): 194.153.145.104



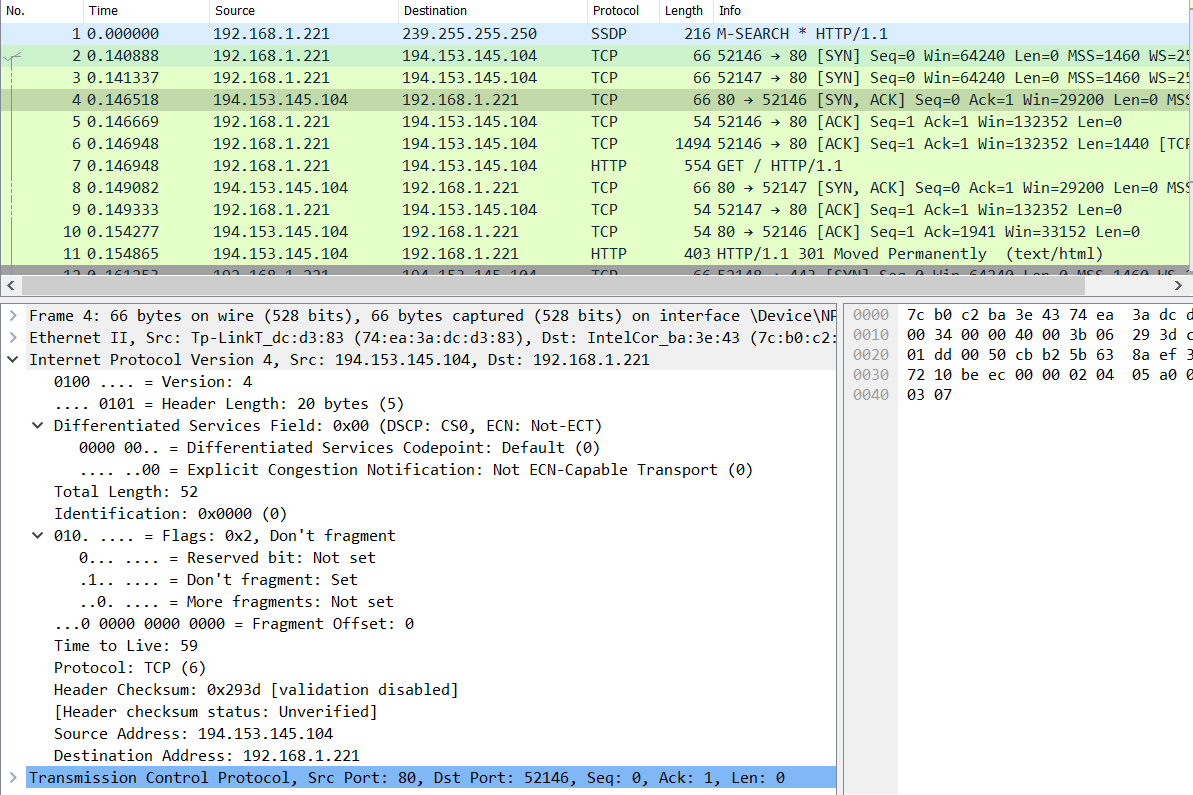
Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:

For this, we expand Ethernet II, Src while the SYN packet is selected:



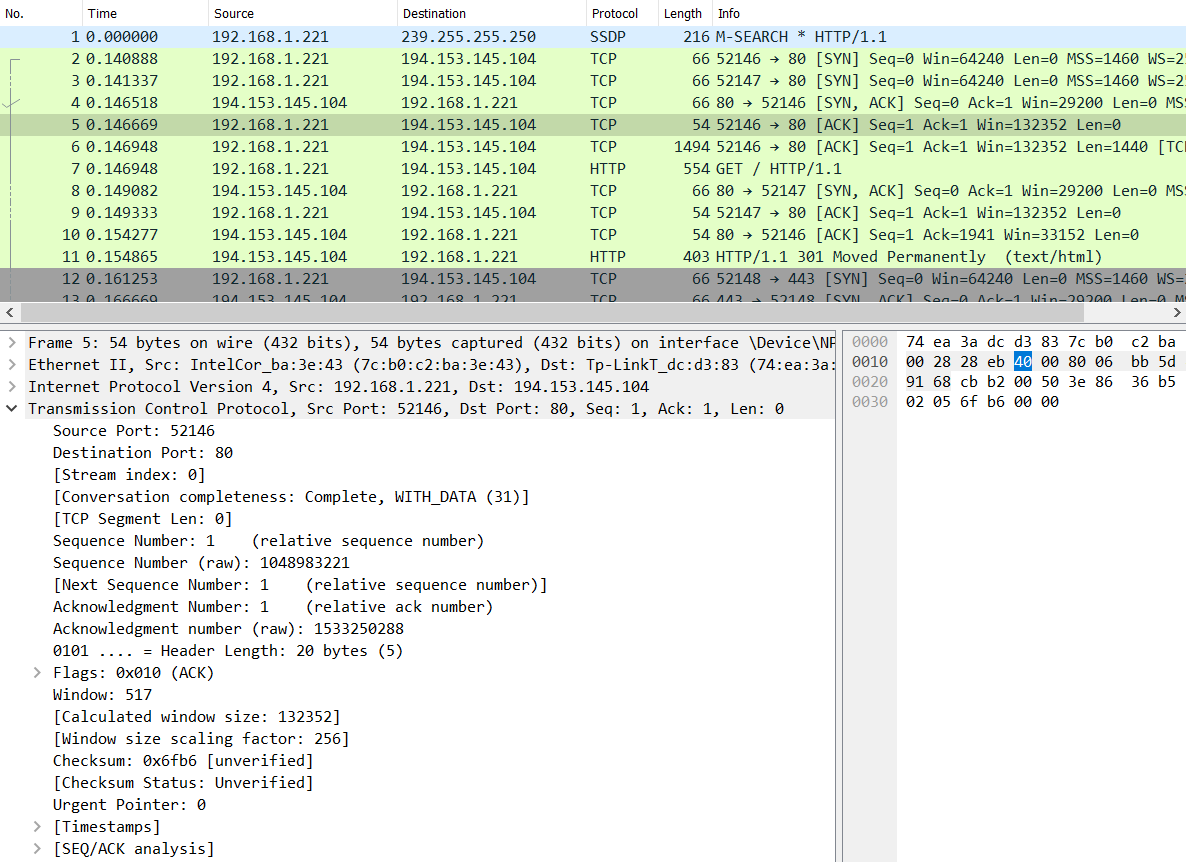
Identify the Network Layer 3 section of the SYN/ACK packet and paste a screenshot from it:

For this, we expand Internet Protocol Version 4 while the SYN/ACK packet is selected:



Identify the Transport Layer 4 section of the ACK packet and paste a screenshot from it bellow:

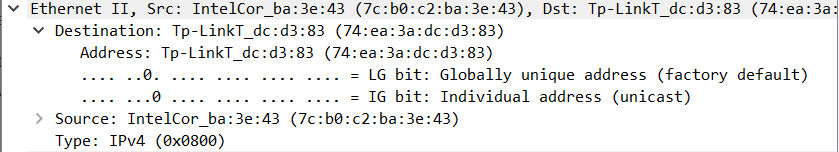
For this, we expand Transmission Control Protocol while the ACK packet is selected:



Look closely at the L2 section of the three-way handshake packet details. Each of them shows the source and destination MAC address of the packets.

Who is the owner of the destination MAC address of the SYN packet?

Here, we select the SYN packet and check in Layer 2 again (Ethernet II, Src). We can see that in Destination part, it shows this MAC address – 74:ea:3a:dc:d3:83.



To check the owner, we can use an online look up tool and we get the following result:

