SFA Homework #8
Elizabeth Ivanova

Exercise 1.

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

```
elizabeth.ivanova@Elizabeths-MacBook-Air ~ % arp -a
? (192.168.100.1) at bc:76:c5:2e:1a:62 on en0 ifscope [ethernet]
? (192.168.100.29) at 62:b1:e5:e:79:a7 on en0 ifscope [ethernet]
? (192.168.100.30) at 3e:d1:df:47:82:c0 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

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

```
elizabeth.ivanova@Elizabeths-MacBook-Air ~ % netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags           Netif Expire
default            192.168.100.1      UGScg             en0
127                127.0.0.1          UCS               lo0
127.0.0.1          127.0.0.1          UH                lo0
169.254            link#6             UCS               en0      !
192.168.100        link#6             UCS               en0      !
192.168.100.1/32   link#6             UCS               en0      !
192.168.100.1      bc:76:c5:2e:1a:62  UHLWIir           en0   1165
192.168.100.24/32  link#6             UCS               en0      !
192.168.100.29     62:b1:e5:e:79:a7   UHLWIi            en0    922
192.168.100.30     3e:d1:df:47:82:c0  UHLWI             en0    981
224.0.0/4          link#6             UmCS              en0      !
224.0.0.251        1:0:5e:0:0:fb      UHmLWI            en0
239.255.255.250    1:0:5e:7f:ff:fa    UHmLWI            en0
255.255.255.255/32 link#6             UCS               en0      !

Internet6:
```

➔ Netstat is the command to show routes on a MacOS. -r is to show the routes, and -n is to not resolve IP addresses to hostnames.

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.

```
ff02::%utun4/32                        fe80::40de:8bfb:f3ce:5ece%utun4 UmCI
    utun4
elizabeth.ivanova@Elizabeths-MacBook-Air ~ % traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
 1  192.168.100.1 (192.168.100.1)  3.241 ms  3.523 ms  2.843 ms
 2  78-83-112-2.spectrumnet.bg (78.83.112.2)  6.537 ms  15.541 ms  11.513 ms
 3  * * *
 4  92.247.143.226 (92.247.143.226)  6.392 ms  6.302 ms  6.276 ms
 5  * * *
 6  dns.google (8.8.8.8)  12.353 ms  6.066 ms  5.736 ms
```

Why would you need to use the ping command? Answer:

The ping command can test whether some host is reachable across an IP network. Ping also measures the time of the packet to be sent from source to destination and back, and reports losses.

Ping google:

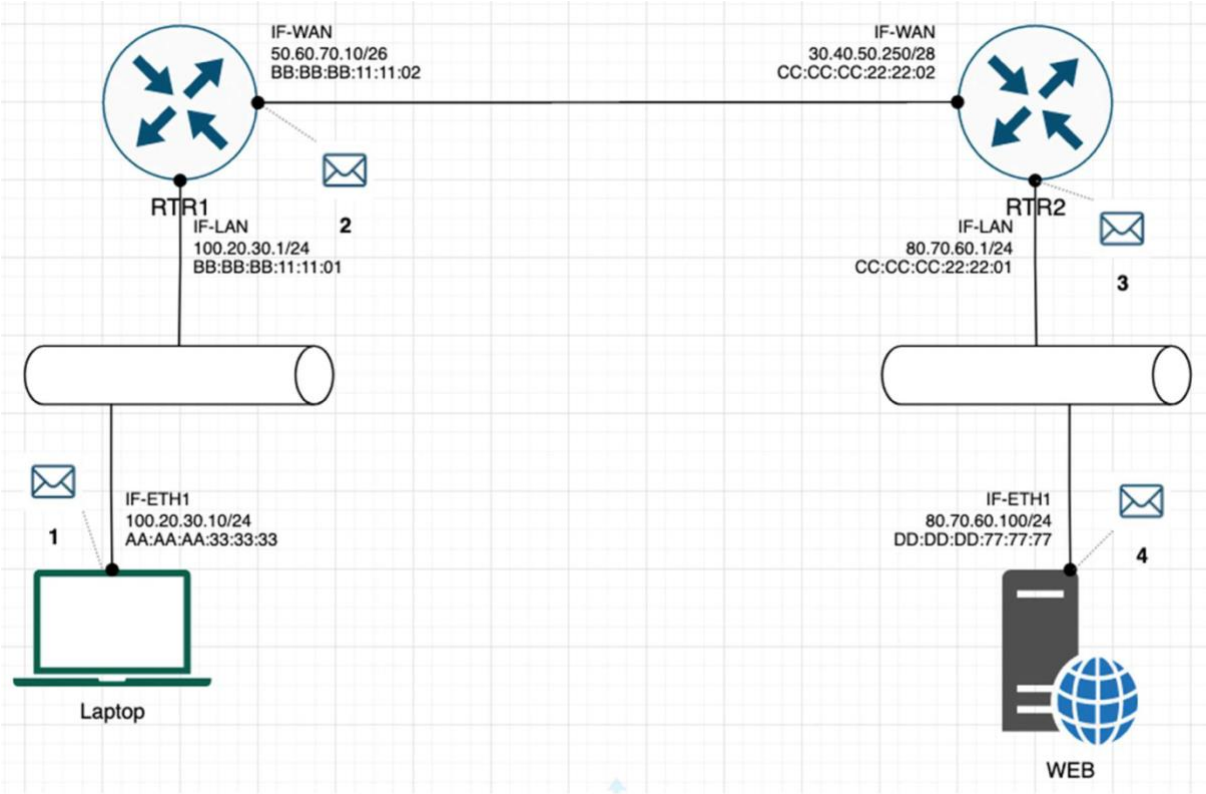
```
elizabeth.ivanova@Elizabeths-MacBook-Air ~ % ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=60 time=11.449 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=60 time=12.143 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=12.098 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=60 time=29.487 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=60 time=12.089 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=60 time=11.627 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=60 time=18.650 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=60 time=11.975 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=60 time=5.748 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=60 time=11.917 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=60 time=11.652 ms
^C
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.748/13.530/29.487/5.752 ms
```

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
- DNS client – UDP53
- DNS zone transfer – TCP53
- SMTP – TCP25
- SSH – TCP22
- FTP – TCP21
- Telnet - TCP23
- MSSQL – TCP1433
- MySQL – TCP3306
- PostgreSQL – TCP5432
- RDP (Remote Desktop Protocol) – TCP3389
- NTP – UDP123
- NFS – TCP2049

Exercise 2.

Refer to the exhibit and answer the questions below. 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 – 100.20.30.10/24
    - DST IP – 80.70.60.100/24
    - SRC MAC - AA:AA:AA:33:33:33
    - DST MAC – BB:BB:BB:11:11:01

2. RTR1 receives the packet on its IF-LAN interface, prepares it accordingly and forwards it out its IF-WAN. What would the packet look like at this stage?
    - SRC IP – 100.20.30.10/24
    - DST IP - 80.70.60.100/24
    - SRC MAC - BB:BB:BB:11:11:02
    - DST MAC – CC:CC:CC:22:22:02

3. RTR2 receives the packet on its IF-WAN interface, prepares it accordingly and forwards it out via IF-LAN. What would the packet look like at this stage?
    - SRC IP - 100.20.30.10/24
    - DST IP - 80.70.60.100/24

- SRC MAC – CC:CC:CC:22:22:01
- DST MAC – DD:DD:DD:77:77:77

4. The web server receives the packet and prepares a response packet back. What would the packet look like at this stage?
    - SRC IP - 80.70.60.100/24
    - DST IP - 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 – because it is highly reliable and packets are received in the correct order.

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: 1024 and up

DST PORT: 443

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

SRC PORT: 443

DST PORT: 1024 and up

How many broadcast domains are there in the exhibit shown? _____2

Exercise 3.

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:

matrixcalc.org

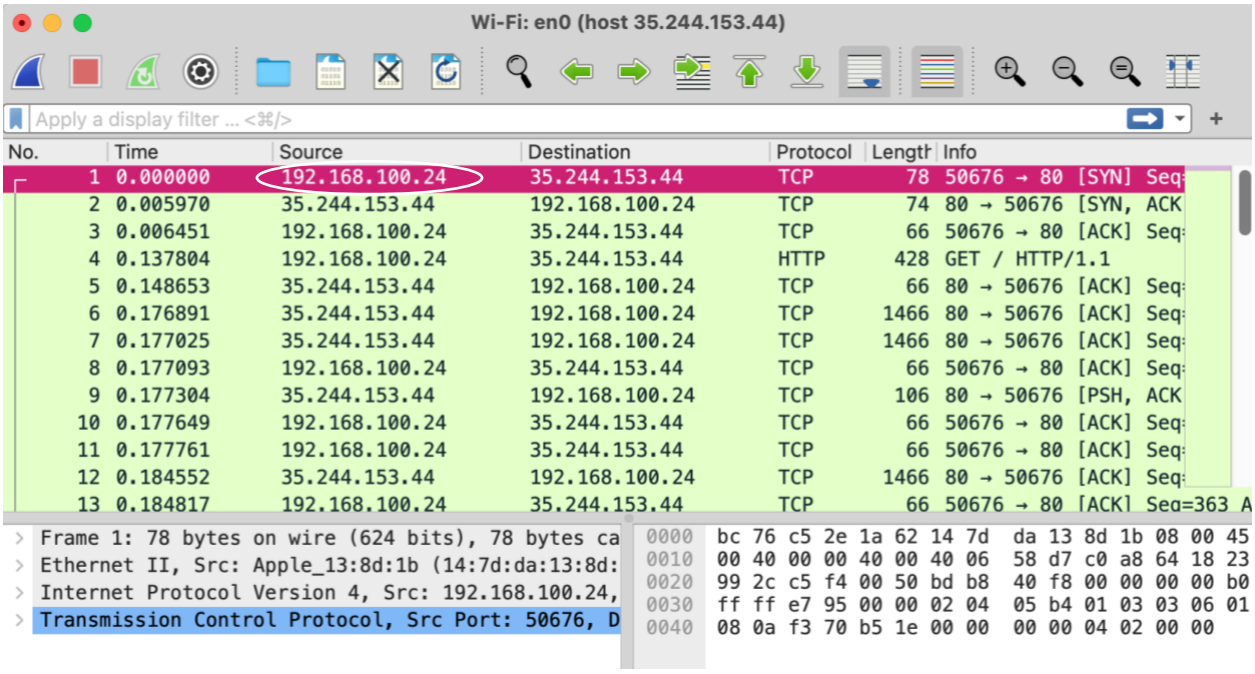
35.244.153.44

```
elizabeth.ivanova@Elizabeths-MacBook-Air ~ % ping matrixcalc.org
PING matrixcalc.org (35.244.153.44): 56 data bytes
64 bytes from 35.244.153.44: icmp_seq=0 ttl=119 time=5.904 ms
64 bytes from 35.244.153.44: icmp_seq=1 ttl=119 time=12.453 ms
64 bytes from 35.244.153.44: icmp_seq=2 ttl=119 time=6.579 ms
64 bytes from 35.244.153.44: icmp_seq=3 ttl=119 time=6.464 ms
64 bytes from 35.244.153.44: icmp_seq=4 ttl=119 time=6.308 ms
^C
--- matrixcalc.org ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 5.904/7.542/12.453/2.466 ms
```

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

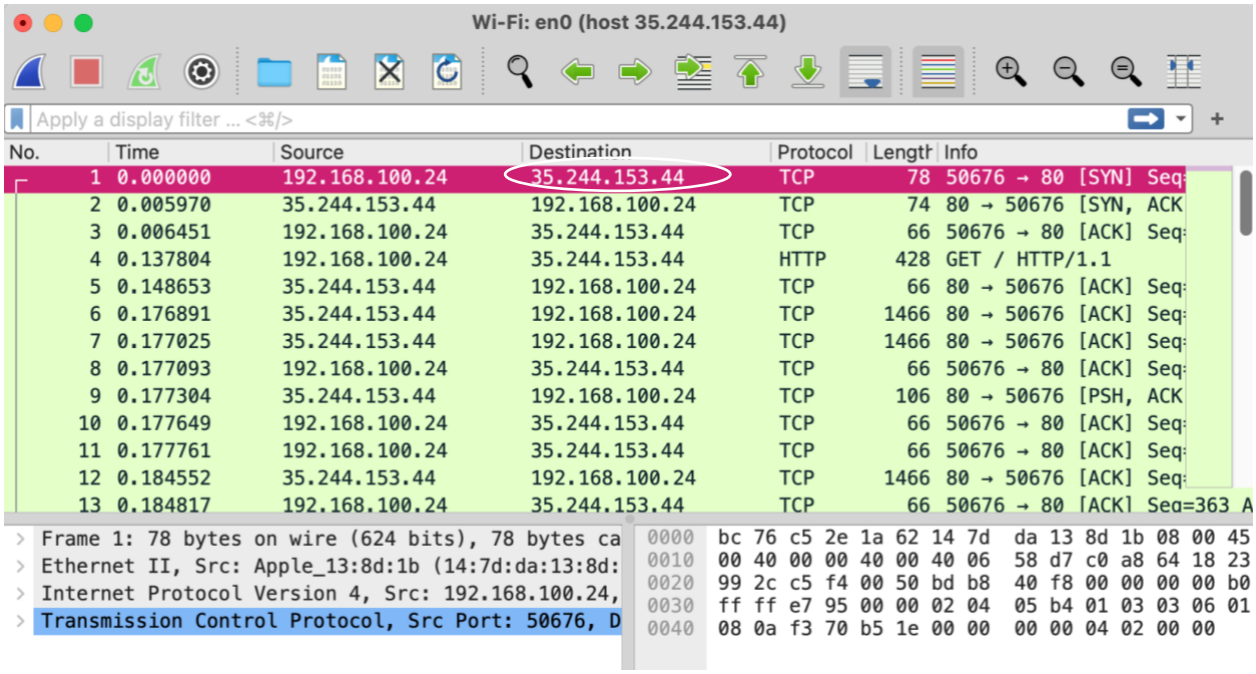
1. What is the source IP (of the initiating host):

The source IP address is my laptop's IP address: 192.168.100.24

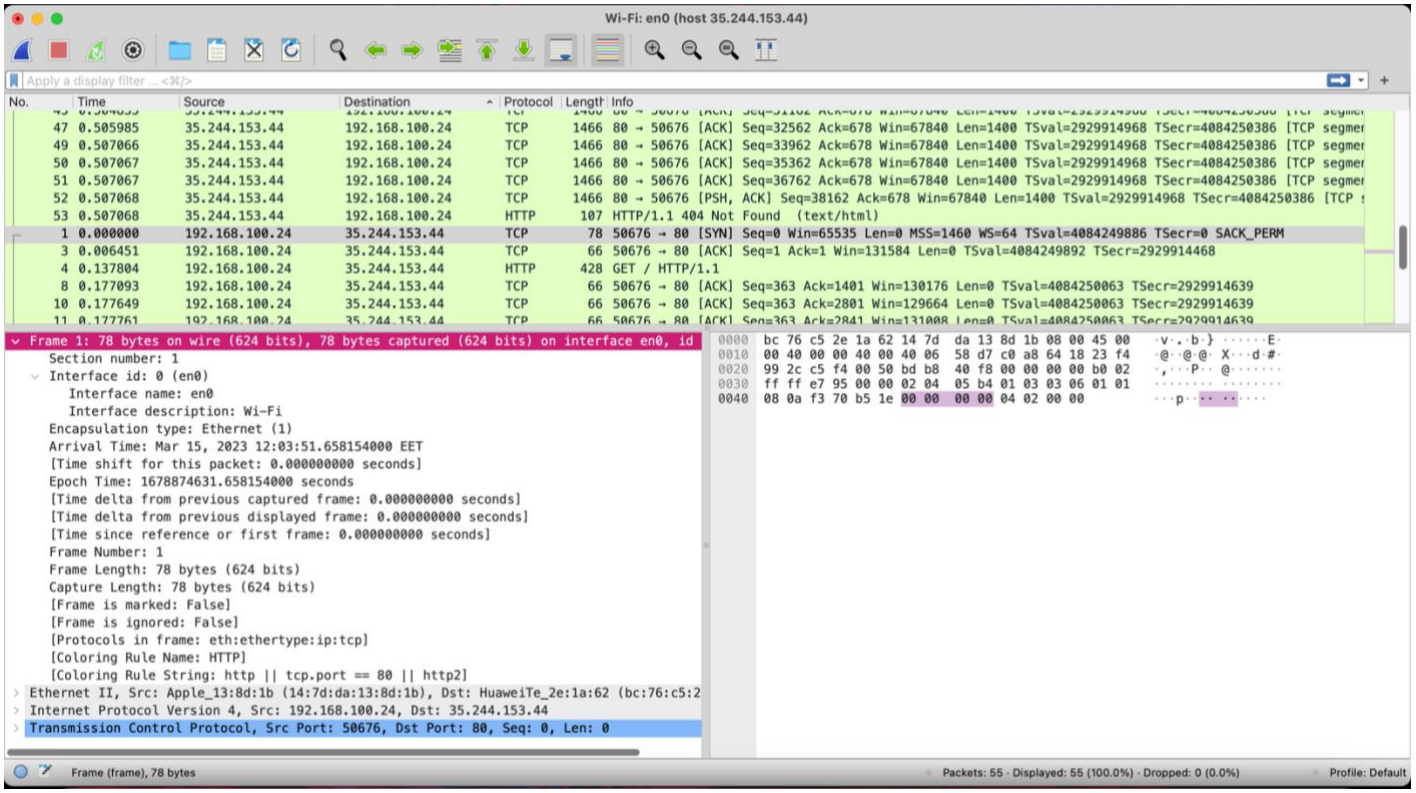


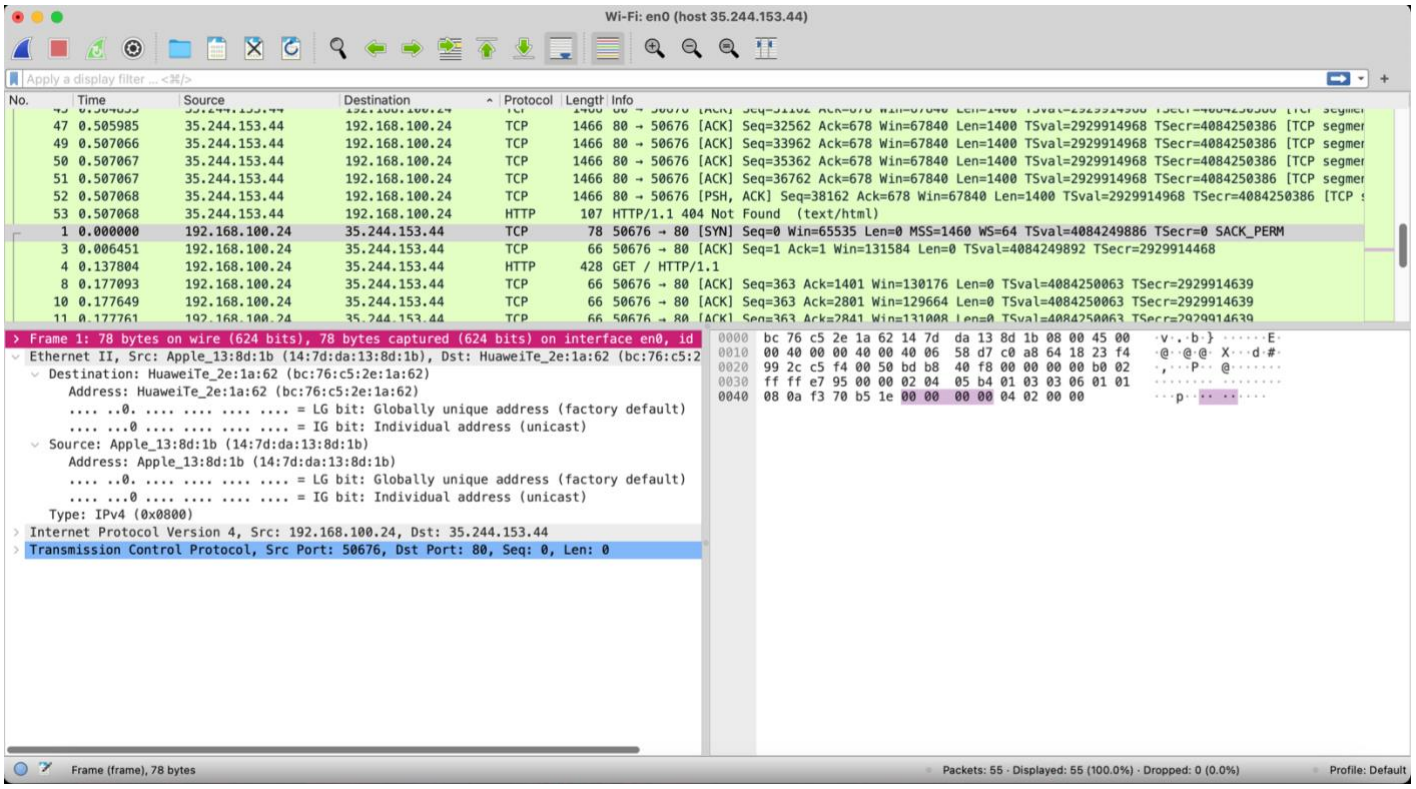
2. What is the destination IP? (target website):

The destination IP address is the target website IP address: 35.244.153.44

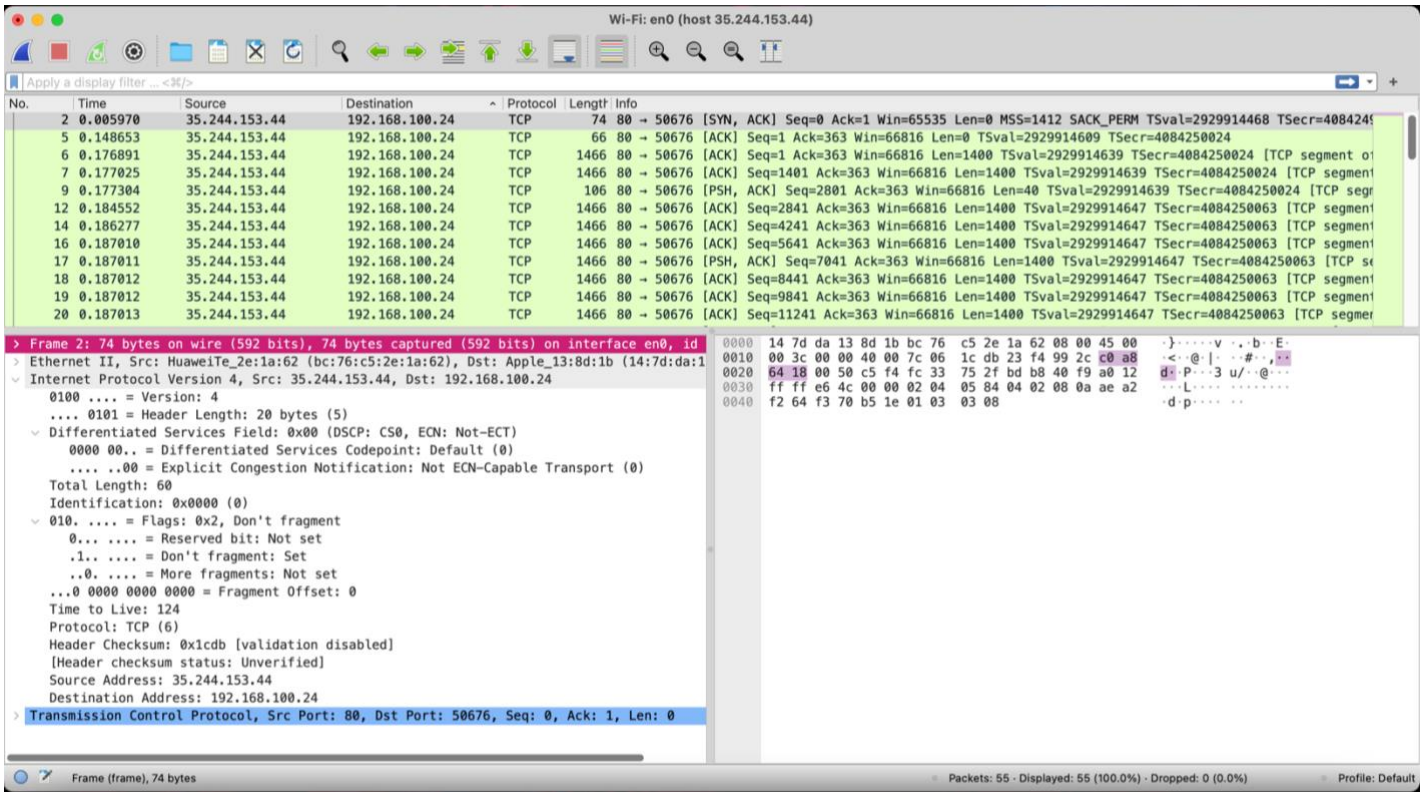


Identify the Network Interface (Layer 1 & 2) section of the SYN packet and paste a screenshot from it:

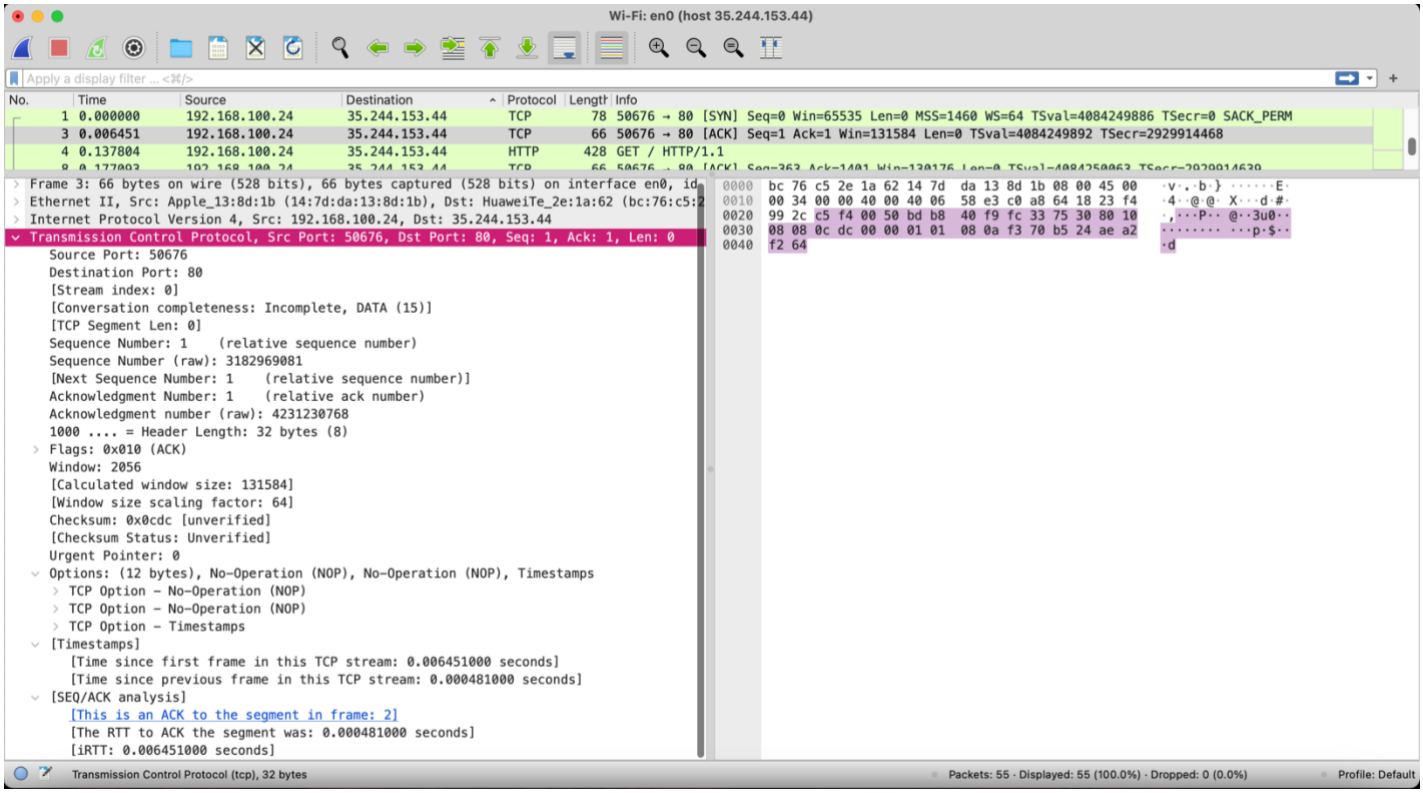

Wi-Fi: en0 (host 35.244.153.44)
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
47 0.505985 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=32562 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
49 0.507066 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=33962 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
50 0.507067 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=35362 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
51 0.507067 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=36762 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
52 0.507068 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [PSH, ACK] Seq=38162 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP
53 0.507068 35.244.153.44 192.168.100.24 HTTP 107 HTTP/1.1 404 Not Found (text/html)
1 0.000000 192.168.100.24 35.244.153.44 TCP 78 50676 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4084249886 TSecr=0 SACK_PERM
3 0.006451 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=4084249892 TSecr=2929914468
4 0.137804 192.168.100.24 35.244.153.44 HTTP 428 GET / HTTP/1.1
8 0.177093 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=363 Ack=1401 Win=130176 Len=0 TSval=4084250063 TSecr=2929914639
10 0.177649 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=363 Ack=2801 Win=129664 Len=0 TSval=4084250063 TSecr=2929914639
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id
Section number: 1
Interface id: 0 (en0)
Interface name: en0
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Mar 15, 2023 12:03:51.658154000 EET
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1678874631.658154000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 78 bytes (624 bits)
Capture Length: 78 bytes (624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Apple_13:8d:1b (14:7d:da:13:8d:1b), Dst: HuaweiTe_2e:1a:62 (bc:76:c5:2
Internet Protocol Version 4, Src: 192.168.100.24, Dst: 35.244.153.44
Transmission Control Protocol, Src Port: 50676, Dst Port: 80, Seq: 0, Len: 0
0000 bc 76 c5 2e 1a 62 14 7d da 13 8d 1b 08 00 45 00
0010 00 40 00 00 40 00 40 06 58 d7 c0 a8 64 18 23 f4
0020 99 2c c5 f4 00 50 bd b8 40 f8 00 00 00 00 b0 02
0030 ff ff e7 95 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a f3 70 b5 1e 00 00 00 00 04 02 00 00
Frame (frame), 78 bytes
Packets: 55 · Displayed: 55 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


Wi-Fi: en0 (host 35.244.153.44)
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
47 0.505985 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=32562 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
49 0.507066 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=33962 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
50 0.507067 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=35362 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
51 0.507067 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [ACK] Seq=36762 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP segmer
52 0.507068 35.244.153.44 192.168.100.24 TCP 1466 80 → 50676 [PSH, ACK] Seq=38162 Ack=678 Win=67840 Len=1400 TSval=2929914968 TSecr=4084250386 [TCP
53 0.507068 35.244.153.44 192.168.100.24 HTTP 107 HTTP/1.1 404 Not Found (text/html)
1 0.000000 192.168.100.24 35.244.153.44 TCP 78 50676 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4084249886 TSecr=0 SACK_PERM
3 0.006451 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=4084249892 TSecr=2929914468
4 0.137804 192.168.100.24 35.244.153.44 HTTP 428 GET / HTTP/1.1
8 0.177093 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=363 Ack=1401 Win=130176 Len=0 TSval=4084250063 TSecr=2929914639
10 0.177649 192.168.100.24 35.244.153.44 TCP 66 50676 → 80 [ACK] Seq=363 Ack=2801 Win=129664 Len=0 TSval=4084250063 TSecr=2929914639
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id
Ethernet II, Src: Apple_13:8d:1b (14:7d:da:13:8d:1b), Dst: HuaweiTe_2e:1a:62 (bc:76:c5:2
Destination: HuaweiTe_2e:1a:62 (bc:76:c5:2e:1a:62)
Address: HuaweiTe_2e:1a:62 (bc:76:c5:2e:1a:62)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Apple_13:8d:1b (14:7d:da:13:8d:1b)
Address: Apple_13:8d:1b (14:7d:da:13:8d:1b)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.100.24, Dst: 35.244.153.44
Transmission Control Protocol, Src Port: 50676, Dst Port: 80, Seq: 0, Len: 0
0000 bc 76 c5 2e 1a 62 14 7d da 13 8d 1b 08 00 45 00
0010 00 40 00 00 40 00 40 06 58 d7 c0 a8 64 18 23 f4
0020 99 2c c5 f4 00 50 bd b8 40 f8 00 00 00 00 b0 02
0030 ff ff e7 95 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a f3 70 b5 1e 00 00 00 00 04 02 00 00
Frame (frame), 78 bytes
Packets: 55 · Displayed: 55 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

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



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



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?