Analyzing Network Traffic with Wireshark (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 01

Student:	Email:
Jalen Salgado	jsalgado1915@gmail.com

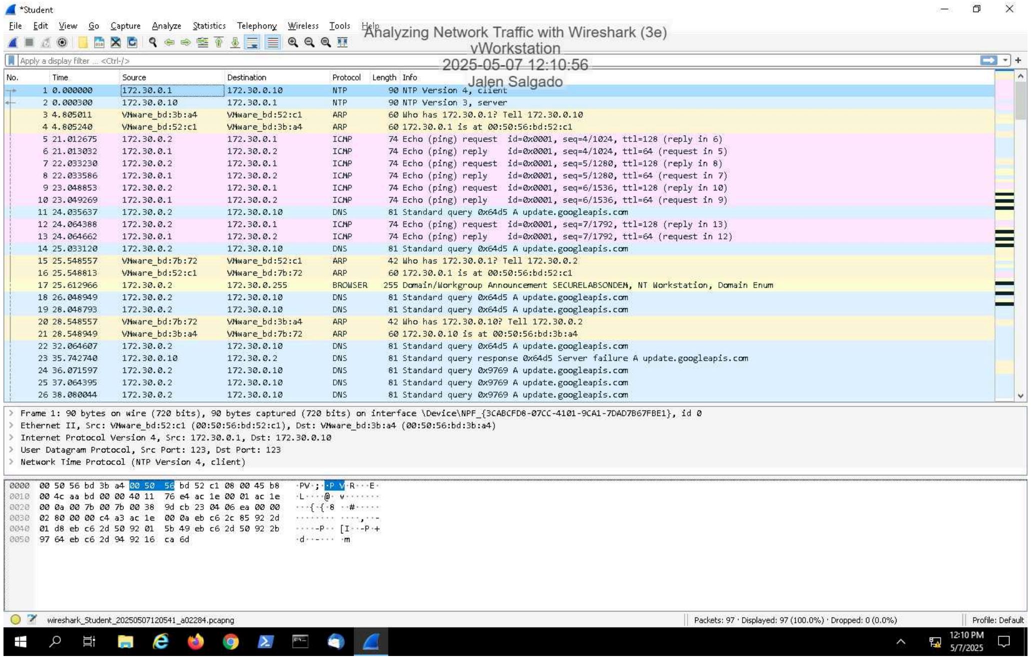
Time on Task:	Progress:
1 hour, 51 minutes	100%

Report Generated: Saturday, July 26, 2025 at 2:11 PM

Section 1: Hands-On Demonstration

Part 1: Explore Wireshark

13. **Make a screen capture** showing **the fields related to time**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:10:56
Jalen Salgado
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source             Destination        Protocol  Length Info
   1 0.000000   172.30.0.1         172.30.0.10        NTP         90 NTP Version 4, client
   2 0.000300   172.30.0.10        172.30.0.1         NTP         90 NTP Version 3, server
   3 4.805011   VMware_bd:3b:a4    VMware_bd:52:c1    ARP         60 Who has 172.30.0.1? Tell 172.30.0.10
   4 4.805240   VMware_bd:52:c1    VMware_bd:3b:a4    ARP         60 172.30.0.1 is at 00:50:56:bd:52:c1
   5 21.012675  172.30.0.2         172.30.0.1         ICMP        74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 6)
   6 21.013032  172.30.0.1         172.30.0.2         ICMP        74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=64 (request in 5)
   7 22.033230  172.30.0.2         172.30.0.1         ICMP        74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 8)
   8 22.033586  172.30.0.1         172.30.0.2         ICMP        74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=64 (request in 7)
   9 23.048853  172.30.0.2         172.30.0.1         ICMP        74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 10)
  10 23.049269  172.30.0.1         172.30.0.2         ICMP        74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=64 (request in 9)
  11 24.035637  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x64d5 A update.googleapis.com
  12 24.064388  172.30.0.2         172.30.0.1         ICMP        74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 13)
  13 24.064662  172.30.0.1         172.30.0.2         ICMP        74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=64 (request in 12)
  14 25.033120  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x64d5 A update.googleapis.com
  15 25.548557  VMware_bd:7b:72    VMware_bd:52:c1    ARP         42 Who has 172.30.0.1? Tell 172.30.0.2
  16 25.548813  VMware_bd:52:c1    VMware_bd:7b:72    ARP         60 172.30.0.1 is at 00:50:56:bd:52:c1
  17 25.612966  172.30.0.2         172.30.0.255       BROWSER    255 Domain/Workgroup Announcement SECURELABSONDEM, NT Workstation, Domain Enum
  18 26.048949  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x64d5 A update.googleapis.com
  19 28.048793  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x64d5 A update.googleapis.com
  20 28.548557  VMware_bd:7b:72    VMware_bd:3b:a4    ARP         42 Who has 172.30.0.10? Tell 172.30.0.2
  21 28.548949  VMware_bd:3b:a4    VMware_bd:7b:72    ARP         60 172.30.0.10 is at 00:50:56:bd:3b:a4
  22 32.064607  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x64d5 A update.googleapis.com
  23 35.742740  172.30.0.10        172.30.0.2         DNS         81 Standard query response 0x64d5 Server failure A update.googleapis.com
  24 36.071597  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x9769 A update.googleapis.com
  25 37.064395  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x9769 A update.googleapis.com
  26 38.080044  172.30.0.2         172.30.0.10        DNS         81 Standard query 0x9769 A update.googleapis.com
```

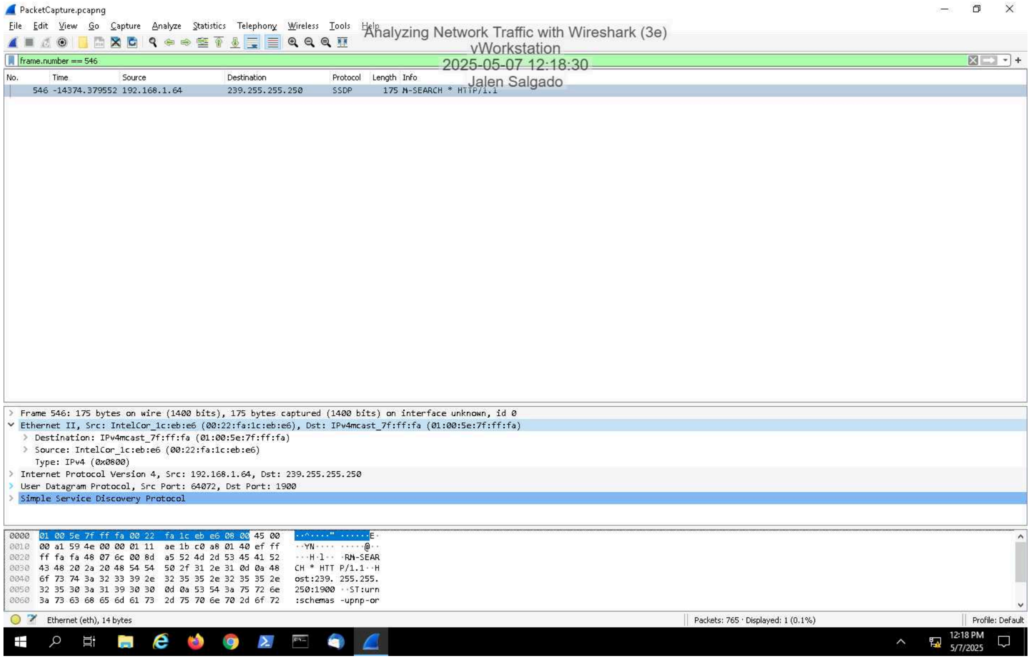
```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{3CABCFD8-07CC-4101-9CA1-7DAD7B67FBE1}, id 0
> Ethernet II, Src: VMware_bd:52:c1 (00:50:56:bd:52:c1), Dst: VMware_bd:3b:a4 (00:50:56:bd:3b:a4)
> Internet Protocol Version 4, Src: 172.30.0.1, Dst: 172.30.0.10
> User Datagram Protocol, Src Port: 123, Dst Port: 123
> Network Time Protocol (NTP Version 4, client)
```

```
0000  00 50 56 bd 3b a4 00 50  56 bd 52 c1 08 00 45 b8   ·PV·;··P V·R···E·
0010  00 4c aa bd 00 00 40 11  76 e4 ac 1e 00 01 ac 1e   ·L····@· v·······
0020  00 0a 00 7b 00 7b 00 38  9d cb 23 04 06 ea 00 00   ···{·{·8 ··#·····
0030  02 80 00 00 c4 a3 ac 1e  00 0a eb c6 2c 85 92 2d   ········ ····,··-
0040  01 d8 eb c6 2d 50 92 01  5b 49 eb c6 2d 50 92 2b   ····-P·· [I··-P·+
0050  97 64 eb c6 2d 94 92 16  ca 6d                     ·d··-··· ·m
```

wireshark_Student_20250507120541_a02284.pcapng | Packets: 97 · Displayed: 97 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Part 2: Analyze Wireshark Capture Information

7. **Make a screen capture** showing the **complete hexadecimal representation for the source and destination Media Access Control (MAC) addresses in Packet 546**.



frame.number == 546

```
No.    Time           Source         Destination       Protocol  Length Info
   546 -14374.379552 192.168.1.64   239.255.255.250   SSDP        175 M-SEARCH * HTTP/1.1
```

```
> Frame 546: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface unknown, id 0
v Ethernet II, Src: IntelCor_1c:eb:e6 (00:22:fa:1c:eb:e6), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Source: IntelCor_1c:eb:e6 (00:22:fa:1c:eb:e6)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.64, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 64072, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 00 22  fa 1c eb e6 08 00 45 00   ··^····" ······E·
0010  00 a1 59 4e 00 00 01 11  ae 1b c0 a8 01 40 ef ff   ··YN···· ·····@··
0020  ff fa fa 48 07 6c 00 8d  a5 52 4d 2d 53 45 41 52   ···H·l·· ·RM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
0050  32 35 30 3a 31 39 30 30  0d 0a 53 54 3a 75 72 6e   250:1900 ··ST:urn
0060  3a 73 63 68 65 6d 61 73  2d 75 70 6e 70 2d 6f 72   :schemas -upnp-or
```

8. **Record** the **code assigned by the IEEE to Intel for use in identifying Intel Core network interfaces in Packet 546**.

00:22:fa

9. **Record** the **MAC address used for IPv4 multicast in Packet 546**.

01:00:5e:7f:ff:fa

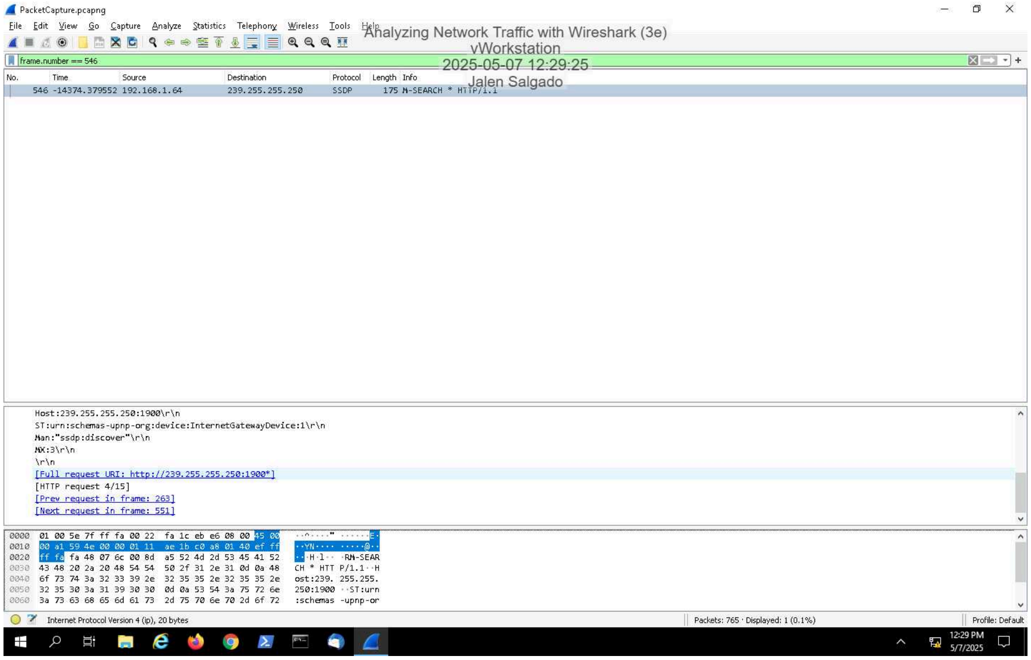
12. **Record** the **version of the Internet Protocol being used in Packet 546**.

Internet protocol version 4

13. **Record** the **source IP address in Packet 546**.

192.168.1.64

19. **Make a screen capture** showing the **related frame numbers for Packet 546**.



PacketCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:29:25
Jalen Salgado

frame.number == 546

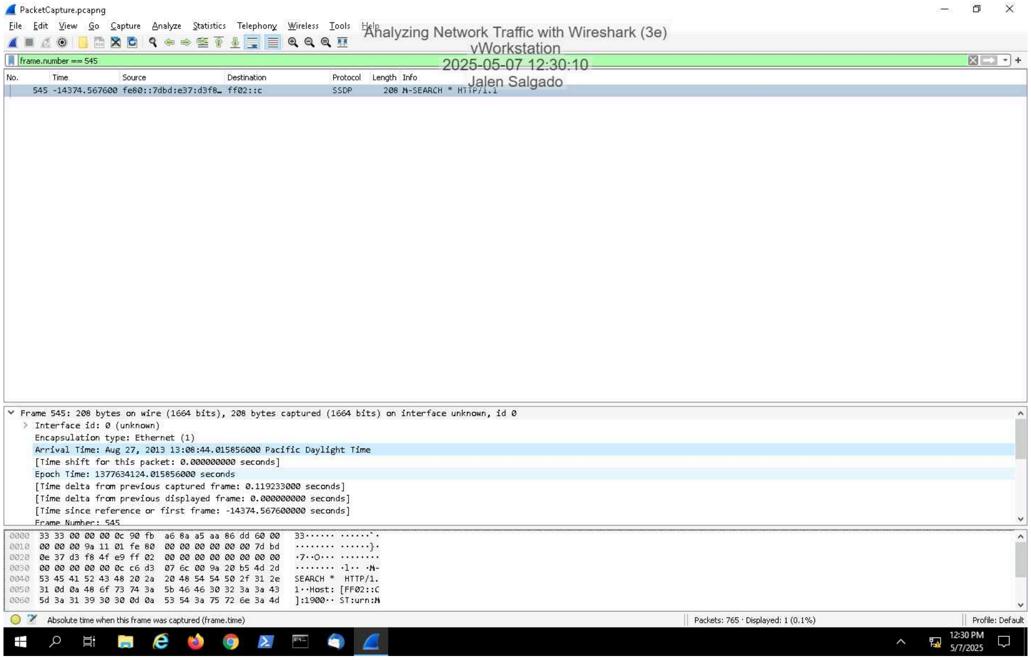
```
No.   Time           Source        Destination      Protocol  Length  Info
  546 -14374.379552  192.168.1.64  239.255.255.250  SSDP         175  M-SEARCH * HTTP/1.1
```

```
Host:239.255.255.250:1900\r\n
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
Man:"ssdp:discover"\r\n
MX:3\r\n
\r\n
[Full request URI: http://239.255.255.250:1900*]
[HTTP request 4/15]
[Prev request in frame: 263]
[Next request in frame: 551]
```

```
0000  01 00 5e 7f ff fa 00 22  fa 1c eb e6 08 00 45 00   ··^····" ······E·
0010  00 a1 59 4e 00 00 01 11  ae 1b c0 a8 01 40 ef ff   ··YN···· ·····@··
0020  ff fa fa 48 07 6c 00 8d  a5 52 4d 2d 53 45 41 52   ···H·l·· ·RM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
0050  32 35 30 3a 31 39 30 30  0d 0a 53 54 3a 75 72 6e   250:1900 ··ST:urn
0060  3a 73 63 68 65 6d 61 73  2d 75 70 6e 70 2d 6f 72   :schemas -upnp-or
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 765 · Displayed: 1 (0.1%) | Profile: Default

- **Make a screen capture** showing the **complete hexadecimal representation for the source and destination Media Access Control (MAC) addresses in Packet 545**.


PacketCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:30:10
Jalen Salgado
12:30 PM
5/7/2025

frame.number == 545

```
No.  Time          Source                  Destination  Protocol  Length  Info
545 -14374.567600  fe80::7dbd:e37:d3f8…    ff02::c      SSDP        208   M-SEARCH * HTTP/1.1
```

```
Frame 545: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface unknown, id 0
  > Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 27, 2013 13:08:44.015856000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1377634124.015856000 seconds
    [Time delta from previous captured frame: 0.119233000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: -14374.567600000 seconds]
    Frame Number: 545
```

```
0000  33 33 00 00 00 0c 90 fb  a6 8a a5 aa 86 dd 60 00   33······ ······`·
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 7d bd   ········ ······}·
0020  0e 37 d3 f8 4f e9 ff 02  00 00 00 00 00 00 00 00   ·7··O··· ········
0030  00 00 00 00 00 0c c6 d3  07 6c 00 9a 20 b5 4d 2d   ········ ·l·· ·M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  5b 46 46 30 32 3a 3a 43   1··Host: [FF02::C
0060  5d 3a 31 39 30 30 0d 0a  53 54 3a 75 72 6e 3a 4d   ]:1900·· ST:urn:M
```

Absolute time when this frame was captured (frame.time) | Packets: 765 · Displayed: 1 (0.1%) | Profile: Default

- **Record** the **IEEE-assigned manufacturer's unique ID in Packet 545**.

90:fb:a6

- **Record** the **MAC address used for multicast in Packet 545**.

33:33:00:00:00:0c

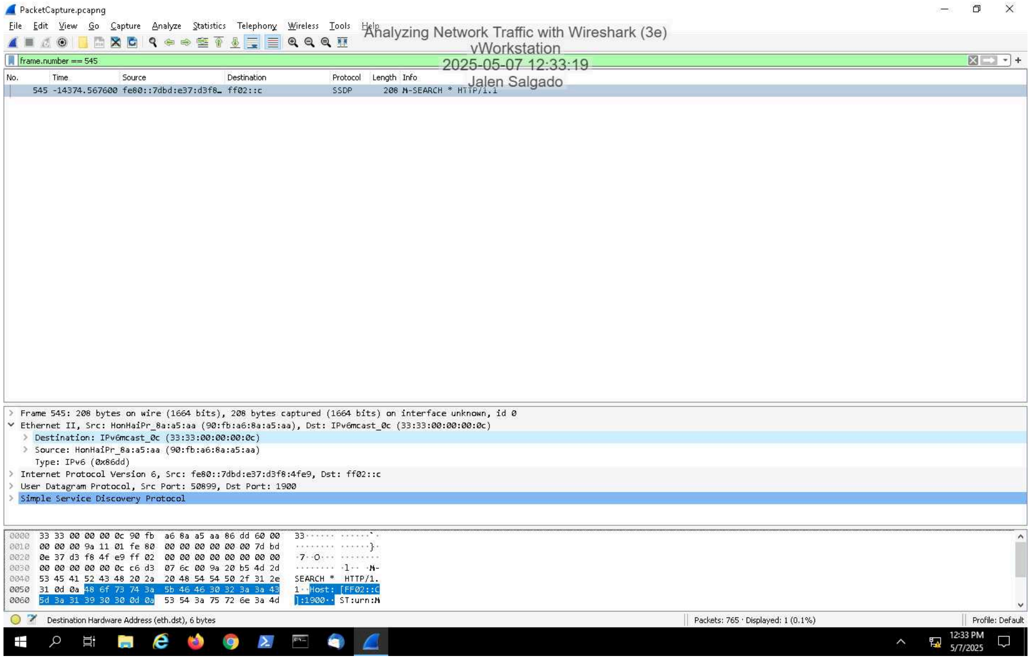
- **Record** the **version of the Internet Protocol being used in Packet 545**.

IPv6

- **Record** the **source IP address in Packet 545**.

fe80::7dbd:e37d:3f8:4fe9

- **Make a screen capture** showing the **related frame numbers for Packet 545**.


PacketCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:33:19
Jalen Salgado

frame.number == 545

```
No.   Time           Source                Destination  Protocol  Length  Info
  545 -14374.567600  fe80::7dbd:e37:d3f8…  ff02::c      SSDP         208  M-SEARCH * HTTP/1.1
```

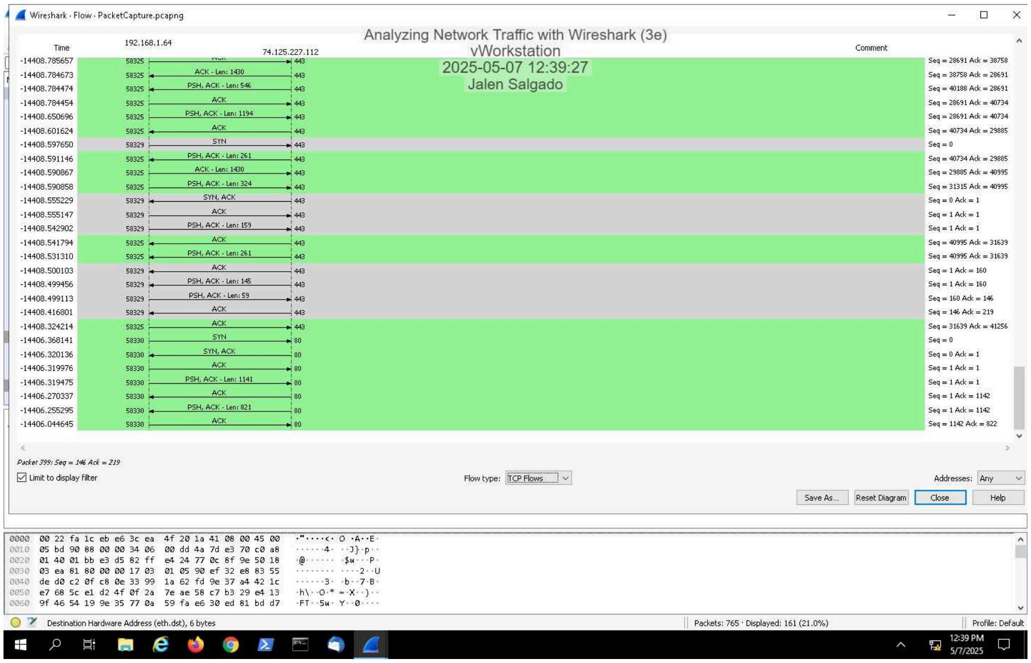
```
> Frame 545: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface unknown, id 0
v Ethernet II, Src: HonHaiPr_8a:a5:aa (90:fb:a6:8a:a5:aa), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
  > Destination: IPv6mcast_0c (33:33:00:00:00:0c)
  > Source: HonHaiPr_8a:a5:aa (90:fb:a6:8a:a5:aa)
    Type: IPv6 (0x86dd)
> Internet Protocol Version 6, Src: fe80::7dbd:e37:d3f8:4fe9, Dst: ff02::c
> User Datagram Protocol, Src Port: 50899, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  33 33 00 00 00 0c 90 fb  a6 8a a5 aa 86 dd 60 00   33······ ······`·
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 7d bd   ········ ······}·
0020  0e 37 d3 f8 4f e9 ff 02  00 00 00 00 00 00 00 00   ·7··O··· ········
0030  00 00 00 00 00 0c c6 d3  07 6c 00 9a 20 b5 4d 2d   ········ ·l·· ·M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  5b 46 46 30 32 3a 3a 43   1··Host: [FF02::C
0060  5d 3a 31 39 30 30 0d 0a  53 54 3a 75 72 6e 3a 4d   ]:1900·· ST:urn:M
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 765 · Displayed: 1 (0.1%) | Profile: Default

12:33 PM
5/7/2025

36. **Make a screen capture** showing the **time** (found in the Time column on the left) **that each step of the handshake occurred**.



Wireshark · Flow · PacketCapture.pcapng

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:39:27
Jalen Salgado

Time	192.168.1.64		74.125.227.112	Comment
-14408.785657	58325	ACK →	443	Seq = 28691 Ack = 38758
-14408.784673	58325	← ACK - Len: 1430	443	Seq = 38758 Ack = 28691
-14408.784474	58325	← PSH, ACK - Len: 546	443	Seq = 40188 Ack = 28691
-14408.784454	58325	ACK →	443	Seq = 28691 Ack = 40734
-14408.650696	58325	PSH, ACK - Len: 1194 →	443	Seq = 28691 Ack = 40734
-14408.601624	58325	← ACK	443	Seq = 40734 Ack = 29885
-14408.597650	58329	SYN →	443	Seq = 0
-14408.591146	58325	← PSH, ACK - Len: 261	443	Seq = 40734 Ack = 29885
-14408.590867	58325	ACK - Len: 1430 →	443	Seq = 29885 Ack = 40995
-14408.590858	58325	PSH, ACK - Len: 324 →	443	Seq = 31315 Ack = 40995
-14408.555229	58329	← SYN, ACK	443	Seq = 0 Ack = 1
-14408.555147	58329	ACK →	443	Seq = 1 Ack = 1
-14408.542902	58329	PSH, ACK - Len: 159 →	443	Seq = 1 Ack = 1
-14408.541794	58325	← ACK	443	Seq = 40995 Ack = 31639
-14408.531310	58325	← PSH, ACK - Len: 261	443	Seq = 40995 Ack = 31639
-14408.500103	58329	← ACK	443	Seq = 1 Ack = 160
-14408.499456	58329	← PSH, ACK - Len: 145	443	Seq = 1 Ack = 160
-14408.499113	58329	PSH, ACK - Len: 59 →	443	Seq = 160 Ack = 146
-14408.416801	58329	← ACK	443	Seq = 146 Ack = 219
-14408.324214	58325	ACK →	443	Seq = 31639 Ack = 41256
-14406.368141	58330	SYN →	80	Seq = 0
-14406.320136	58330	← SYN, ACK	80	Seq = 0 Ack = 1
-14406.319976	58330	ACK →	80	Seq = 1 Ack = 1
-14406.319475	58330	PSH, ACK - Len: 1141 →	80	Seq = 1 Ack = 1
-14406.270337	58330	← ACK	80	Seq = 1 Ack = 1142
-14406.255295	58330	← PSH, ACK - Len: 821	80	Seq = 1 Ack = 1142
-14406.044645	58330	ACK →	80	Seq = 1142 Ack = 822

Packet 399: Seq = 146 Ack = 219

☑ Limit to display filter

Flow type: TCP Flows

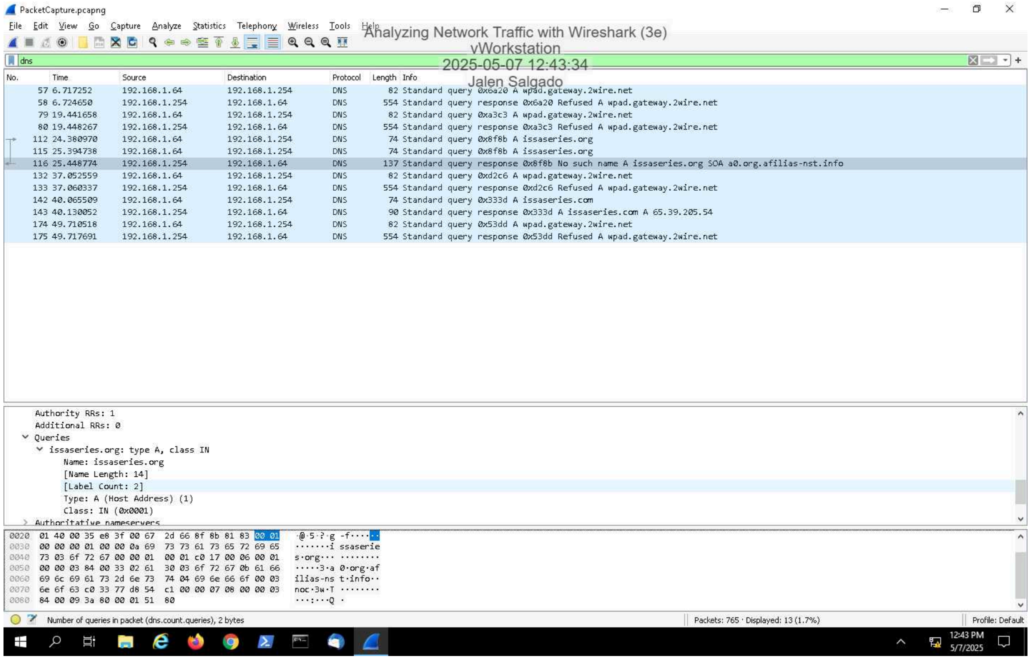
Addresses: Any

```
0000  00 22 fa 1c eb e6 3c ea  4f 20 1a 41 08 00 45 00   ·"····<· O ·A··E·
0010  05 bd 90 88 00 00 34 06  00 dd 4a 7d e3 70 c0 a8   ······4·  ··J}·p··
0020  01 40 01 bb e3 d5 82 ff  e4 24 77 0c 8f 9e 50 18   ·@······  ·$w···P·
0030  03 ea 81 80 00 00 17 03  01 05 90 ef 32 e8 83 55   ········  ····2··U
0040  de d0 c2 0f c8 0e 33 99  1a 62 fd 9e 37 a4 42 1c   ······3·  ·b··7·B·
0050  e7 68 5c e1 d2 4f 0f 2a  7e ae 58 c7 b3 29 e4 13   ·h\··O·*  ~·X··)··
0060  9f 46 54 19 9e 35 77 0a  59 fa e6 30 ed 81 bd d7   ·FT··5w·  Y··0····
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 765 · Displayed: 161 (21.0%) | Profile: Default

12:39 PM
5/7/2025

45. **Make a screen capture** showing the **response to the issaseries.org query**.



PacketCapture.pcapng

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:43:34
Jalen Salgado

dns

No.	Time	Source	Destination	Protocol	Length	Info
57	6.717252	192.168.1.64	192.168.1.254	DNS	82	Standard query 0x6a20 A wpad.gateway.2wire.net
58	6.724650	192.168.1.254	192.168.1.64	DNS	554	Standard query response 0x6a20 Refused A wpad.gateway.2wire.net
79	19.441658	192.168.1.64	192.168.1.254	DNS	82	Standard query 0xa3c3 A wpad.gateway.2wire.net
80	19.448267	192.168.1.254	192.168.1.64	DNS	554	Standard query response 0xa3c3 Refused A wpad.gateway.2wire.net
112	24.380970	192.168.1.64	192.168.1.254	DNS	74	Standard query 0x8f8b A issaseries.org
115	25.394738	192.168.1.64	192.168.1.254	DNS	74	Standard query 0x8f8b A issaseries.org
116	25.448774	192.168.1.254	192.168.1.64	DNS	137	Standard query response 0x8f8b No such name A issaseries.org SOA a0.org.afilias-nst.info
132	37.052559	192.168.1.64	192.168.1.254	DNS	82	Standard query 0xd2c6 A wpad.gateway.2wire.net
133	37.060337	192.168.1.254	192.168.1.64	DNS	554	Standard query response 0xd2c6 Refused A wpad.gateway.2wire.net
142	40.065509	192.168.1.64	192.168.1.254	DNS	74	Standard query 0x333d A issaseries.com
143	40.130052	192.168.1.254	192.168.1.64	DNS	90	Standard query response 0x333d A issaseries.com A 65.39.205.54
174	49.710518	192.168.1.64	192.168.1.254	DNS	82	Standard query 0x53dd A wpad.gateway.2wire.net
175	49.717691	192.168.1.254	192.168.1.64	DNS	554	Standard query response 0x53dd Refused A wpad.gateway.2wire.net

```
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v issaseries.org: type A, class IN
        Name: issaseries.org
        [Name Length: 14]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Authoritative nameservers
```

```
0020  01 40 00 35 e8 3f 00 67  2d 66 8f 8b 81 83 00 01   ·@·5·?·g -f······
0030  00 00 00 01 00 00 0a 69  73 73 61 73 65 72 69 65   ·······i ssaserie
0040  73 03 6f 72 67 00 00 01  00 01 c0 17 00 06 00 01   s·org··· ········
0050  00 00 03 84 00 33 02 61  30 03 6f 72 67 0b 61 66   ·····3·a 0·org·af
0060  69 6c 69 61 73 2d 6e 73  74 04 69 6e 66 6f 00 03   ilias-ns t·info··
0070  6e 6f 63 c0 33 77 d8 54  c1 00 00 07 08 00 00 03   noc·3w·T ········
0080  84 00 09 3a 80 00 01 51  80                        ···:···Q ·
```

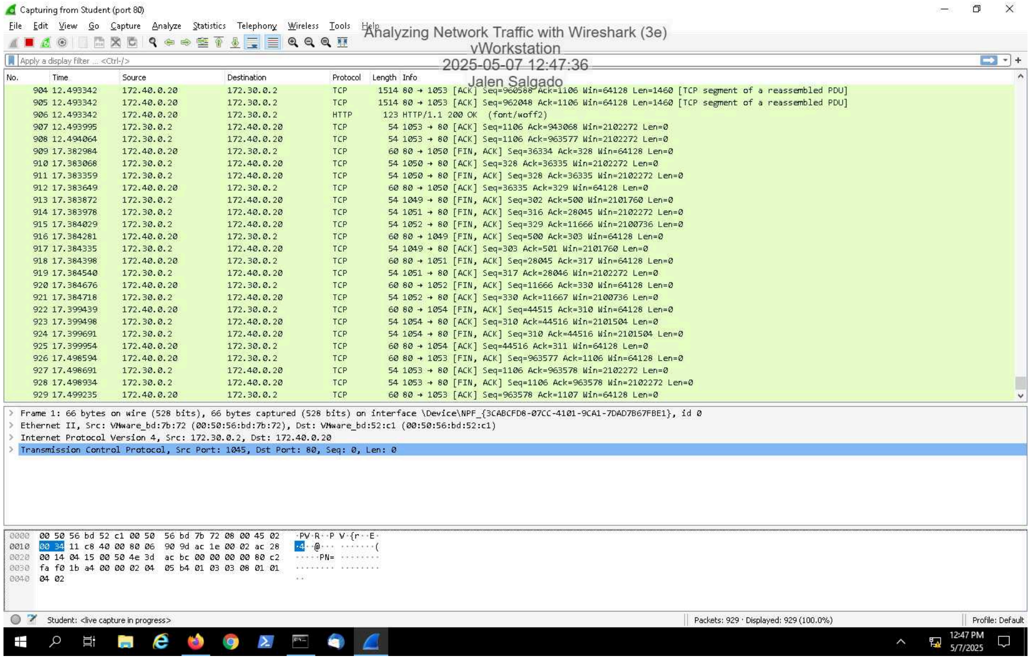
Number of queries in packet (dns.count.queries), 2 bytes | Packets: 765 · Displayed: 13 (1.7%) | Profile: Default

12:43 PM
5/7/2025

Section 2: Applied Learning

Part 1: Explore Wireshark

12. **Make a screen capture** showing the **http traffic**.



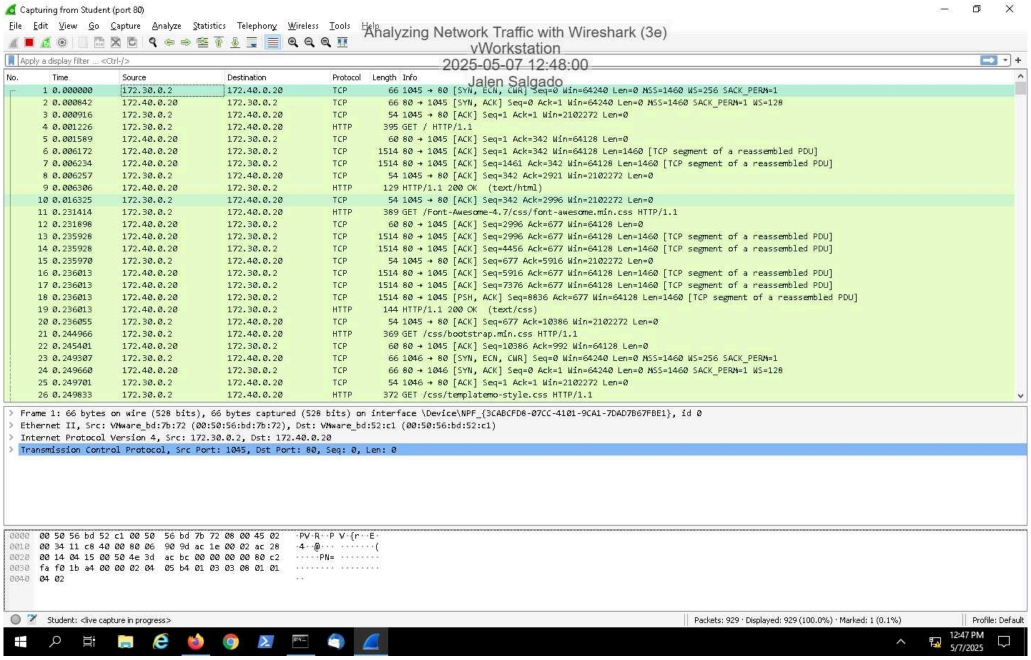
Capturing from Student (port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:47:36
Jalen Salgado

```
No.  Time       Source       Destination  Protocol Length Info
 904 12.493342  172.40.0.20  172.30.0.2   TCP      1514 80 → 1053 [ACK] Seq=960588 Ack=1106 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 905 12.493342  172.40.0.20  172.30.0.2   TCP      1514 80 → 1053 [ACK] Seq=962048 Ack=1106 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
 906 12.493342  172.40.0.20  172.30.0.2   HTTP      123 HTTP/1.1 200 OK  (font/woff2)
 907 12.493995  172.30.0.2   172.40.0.20  TCP        54 1053 → 80 [ACK] Seq=1106 Ack=943068 Win=2102272 Len=0
 908 12.494064  172.30.0.2   172.40.0.20  TCP        54 1053 → 80 [ACK] Seq=1106 Ack=963577 Win=2102272 Len=0
 909 17.382984  172.40.0.20  172.30.0.2   TCP        60 80 → 1050 [FIN, ACK] Seq=36334 Ack=328 Win=64128 Len=0
 910 17.383068  172.30.0.2   172.40.0.20  TCP        54 1050 → 80 [ACK] Seq=328 Ack=36335 Win=2102272 Len=0
 911 17.383359  172.30.0.2   172.40.0.20  TCP        54 1050 → 80 [FIN, ACK] Seq=328 Ack=36335 Win=2102272 Len=0
 912 17.383649  172.40.0.20  172.30.0.2   TCP        60 80 → 1050 [ACK] Seq=36335 Ack=329 Win=64128 Len=0
 913 17.383872  172.30.0.2   172.40.0.20  TCP        54 1049 → 80 [FIN, ACK] Seq=302 Ack=500 Win=2101760 Len=0
 914 17.383978  172.30.0.2   172.40.0.20  TCP        54 1051 → 80 [FIN, ACK] Seq=316 Ack=28045 Win=2102272 Len=0
 915 17.384029  172.30.0.2   172.40.0.20  TCP        54 1052 → 80 [FIN, ACK] Seq=329 Ack=11666 Win=2100736 Len=0
 916 17.384281  172.40.0.20  172.30.0.2   TCP        60 80 → 1049 [FIN, ACK] Seq=500 Ack=303 Win=64128 Len=0
 917 17.384335  172.30.0.2   172.40.0.20  TCP        54 1049 → 80 [ACK] Seq=303 Ack=501 Win=2101760 Len=0
 918 17.384398  172.40.0.20  172.30.0.2   TCP        60 80 → 1051 [FIN, ACK] Seq=28045 Ack=317 Win=64128 Len=0
 919 17.384540  172.30.0.2   172.40.0.20  TCP        54 1051 → 80 [ACK] Seq=317 Ack=28046 Win=2102272 Len=0
 920 17.384676  172.40.0.20  172.30.0.2   TCP        60 80 → 1052 [FIN, ACK] Seq=11666 Ack=330 Win=64128 Len=0
 921 17.384718  172.30.0.2   172.40.0.20  TCP        54 1052 → 80 [ACK] Seq=330 Ack=11667 Win=2100736 Len=0
 922 17.399439  172.40.0.20  172.30.0.2   TCP        60 80 → 1054 [FIN, ACK] Seq=44515 Ack=310 Win=64128 Len=0
 923 17.399498  172.30.0.2   172.40.0.20  TCP        54 1054 → 80 [ACK] Seq=310 Ack=44516 Win=2101504 Len=0
 924 17.399691  172.30.0.2   172.40.0.20  TCP        54 1054 → 80 [FIN, ACK] Seq=310 Ack=44516 Win=2101504 Len=0
 925 17.399954  172.40.0.20  172.30.0.2   TCP        60 80 → 1054 [ACK] Seq=44516 Ack=311 Win=64128 Len=0
 926 17.498594  172.40.0.20  172.30.0.2   TCP        60 80 → 1053 [FIN, ACK] Seq=963577 Ack=1106 Win=64128 Len=0
 927 17.498691  172.30.0.2   172.40.0.20  TCP        54 1053 → 80 [ACK] Seq=1106 Ack=963578 Win=2102272 Len=0
 928 17.498934  172.30.0.2   172.40.0.20  TCP        54 1053 → 80 [FIN, ACK] Seq=1106 Ack=963578 Win=2102272 Len=0
 929 17.499235  172.40.0.20  172.30.0.2   TCP        60 80 → 1053 [ACK] Seq=963578 Ack=1107 Win=64128 Len=0

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3CABCFD8-07CC-4101-9CA1-7DAD7B67FBE1}, id 0
> Ethernet II, Src: VMware_bd:7b:72 (00:50:56:bd:7b:72), Dst: VMware_bd:52:c1 (00:50:56:bd:52:c1)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
> Transmission Control Protocol, Src Port: 1045, Dst Port: 80, Seq: 0, Len: 0

0000  00 50 56 bd 52 c1 00 50  56 bd 7b 72 08 00 45 02   ·PV·R··P V·{r··E·
0010  00 34 11 c8 40 00 80 06  90 9d ac 1e 00 02 ac 28   ·4··@··· ·······(
0020  00 14 04 15 00 50 4e 3d  ac bc 00 00 00 00 80 c2   ·····PN= ········
0030  fa f0 1b a4 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··

Student: <live capture in progress>          Packets: 929 · Displayed: 929 (100.0%)          Profile: Default
```

15. **Make a screen capture** showing the **fields related to time**.



Capturing from Student (port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:48:00
Jalen Salgado

```
No.  Time      Source       Destination  Protocol Length Info
   1 0.000000  172.30.0.2   172.40.0.20  TCP        66 1045 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2 0.000842  172.40.0.20  172.30.0.2   TCP        66 80 → 1045 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
   3 0.000916  172.30.0.2   172.40.0.20  TCP        54 1045 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
   4 0.001226  172.30.0.2   172.40.0.20  HTTP      395 GET / HTTP/1.1
   5 0.001589  172.40.0.20  172.30.0.2   TCP        60 80 → 1045 [ACK] Seq=1 Ack=342 Win=64128 Len=0
   6 0.006172  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=1 Ack=342 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
   7 0.006234  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=1461 Ack=342 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
   8 0.006257  172.30.0.2   172.40.0.20  TCP        54 1045 → 80 [ACK] Seq=342 Ack=2921 Win=2102272 Len=0
   9 0.006306  172.40.0.20  172.30.0.2   HTTP      129 HTTP/1.1 200 OK  (text/html)
  10 0.016325  172.30.0.2   172.40.0.20  TCP        54 1045 → 80 [ACK] Seq=342 Ack=2996 Win=2102272 Len=0
  11 0.231414  172.30.0.2   172.40.0.20  HTTP      389 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP/1.1
  12 0.231898  172.40.0.20  172.30.0.2   TCP        60 80 → 1045 [ACK] Seq=2996 Ack=677 Win=64128 Len=0
  13 0.235928  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=2996 Ack=677 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  14 0.235928  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=4456 Ack=677 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  15 0.235970  172.30.0.2   172.40.0.20  TCP        54 1045 → 80 [ACK] Seq=677 Ack=5916 Win=2102272 Len=0
  16 0.236013  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=5916 Ack=677 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  17 0.236013  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [ACK] Seq=7376 Ack=677 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  18 0.236013  172.40.0.20  172.30.0.2   TCP      1514 80 → 1045 [PSH, ACK] Seq=8836 Ack=677 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  19 0.236013  172.40.0.20  172.30.0.2   HTTP      144 HTTP/1.1 200 OK  (text/css)
  20 0.236055  172.30.0.2   172.40.0.20  TCP        54 1045 → 80 [ACK] Seq=677 Ack=10386 Win=2102272 Len=0
  21 0.244966  172.30.0.2   172.40.0.20  HTTP      369 GET /css/bootstrap.min.css HTTP/1.1
  22 0.245401  172.40.0.20  172.30.0.2   TCP        60 80 → 1045 [ACK] Seq=10386 Ack=992 Win=64128 Len=0
  23 0.249307  172.30.0.2   172.40.0.20  TCP        66 1046 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  24 0.249660  172.40.0.20  172.30.0.2   TCP        66 80 → 1046 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
  25 0.249701  172.30.0.2   172.40.0.20  TCP        54 1046 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
  26 0.249833  172.30.0.2   172.40.0.20  HTTP      372 GET /css/templatemo-style.css HTTP/1.1

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3CABCFD8-07CC-4101-9CA1-7DAD7B67FBE1}, id 0
> Ethernet II, Src: VMware_bd:7b:72 (00:50:56:bd:7b:72), Dst: VMware_bd:52:c1 (00:50:56:bd:52:c1)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
> Transmission Control Protocol, Src Port: 1045, Dst Port: 80, Seq: 0, Len: 0

0000  00 50 56 bd 52 c1 00 50  56 bd 7b 72 08 00 45 02   ·PV·R··P V·{r··E·
0010  00 34 11 c8 40 00 80 06  90 9d ac 1e 00 02 ac 28   ·4··@··· ·······(
0020  00 14 04 15 00 50 4e 3d  ac bc 00 00 00 00 80 c2   ·····PN= ········
0030  fa f0 1b a4 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··

Student: <live capture in progress>          Packets: 929 · Displayed: 929 (100.0%) · Marked: 1 (0.1%)          Profile: Default
```

Part 2: Analyze Wireshark Capture Information

5. **Record** the **number of bytes captured and the bytes on the wire**.

237 on wire and 237 captured

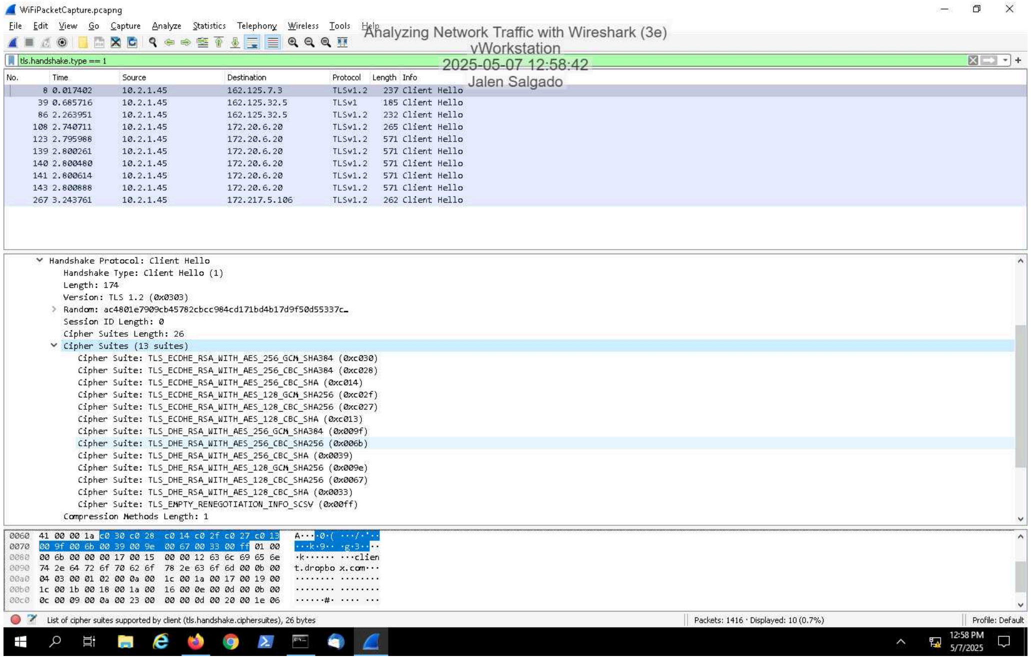
7. **Record** the **manufacturer of the destination device**.

ASUSTekC_a3:ae:f8

10. **Record** the **source IP address**.

Version 4 SRC 10.2.1.45 Dst: 162.125.7.3

16. **Make a screen capture** showing the **entire list of cipher suites**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 12:58:42
Jalen Salgado

tls.handshake.type == 1

```
No.   Time      Source      Destination     Protocol  Length Info
    8 0.017402  10.2.1.45   162.125.7.3     TLSv1.2   237 Client Hello
   39 0.685716  10.2.1.45   162.125.32.5    TLSv1     185 Client Hello
   86 2.263951  10.2.1.45   162.125.32.5    TLSv1.2   232 Client Hello
  108 2.740711  10.2.1.45   172.20.6.20     TLSv1.2   265 Client Hello
  123 2.795988  10.2.1.45   172.20.6.20     TLSv1.2   571 Client Hello
  139 2.800261  10.2.1.45   172.20.6.20     TLSv1.2   571 Client Hello
  140 2.800480  10.2.1.45   172.20.6.20     TLSv1.2   571 Client Hello
  141 2.800614  10.2.1.45   172.20.6.20     TLSv1.2   571 Client Hello
  143 2.800888  10.2.1.45   172.20.6.20     TLSv1.2   571 Client Hello
  267 3.243761  10.2.1.45   172.217.5.106   TLSv1.2   262 Client Hello
```

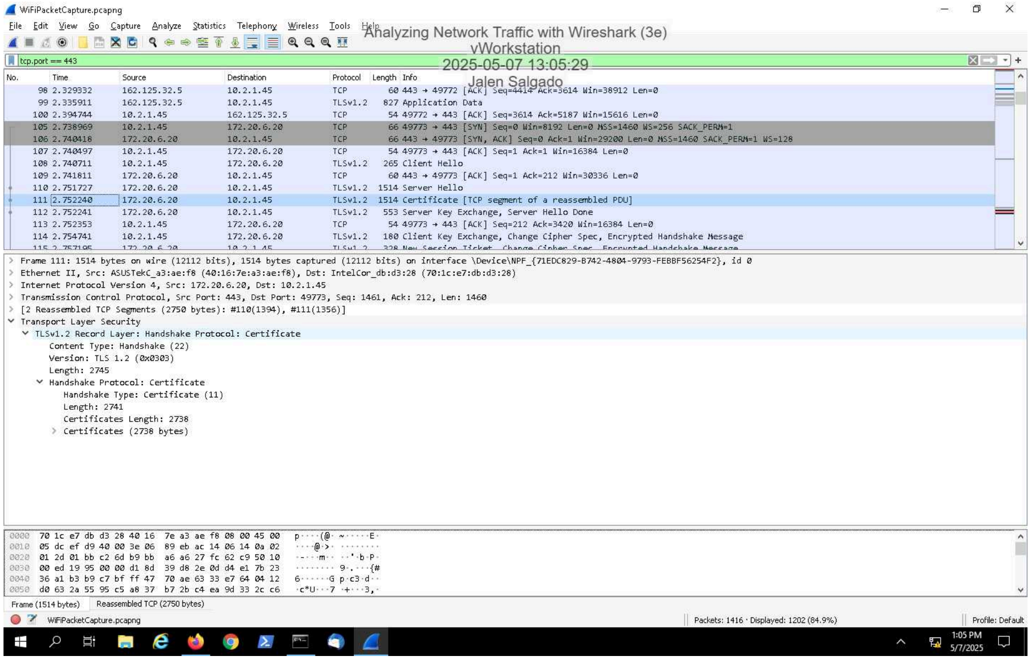
```
  v Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 174
      Version: TLS 1.2 (0x0303)
    > Random: ac4801e7909cb45782cbcc984cd171bd4b17d9f50d55337c…
      Session ID Length: 0
      Cipher Suites Length: 26
    v Cipher Suites (13 suites)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
      Compression Methods Length: 1
```

```
0060  41 00 00 1a c0 30 c0 28  c0 14 c0 2f c0 27 c0 13   A···0·( ···/·'··
0070  00 9f 00 6b 00 39 00 9e  00 67 00 33 00 ff 01 00   ···k·9·· ·g·3····
0080  00 6b 00 00 00 17 00 15  00 00 12 63 6c 69 65 6e   ·k······ ···clien
0090  74 2e 64 72 6f 70 62 6f  78 2e 63 6f 6d 00 0b 00   t.dropbo x.com···
00a0  04 03 00 01 02 00 0a 00  1c 00 1a 00 17 00 19 00   ········ ········
00b0  1c 00 1b 00 18 00 1a 00  16 00 0e 00 0d 00 0b 00   ········ ········
00c0  0c 00 09 00 0a 00 23 00  00 00 0d 00 20 00 1e 06   ······#· ···· ···
```

List of cipher suites supported by client (tls.handshake.ciphersuites), 26 bytes | Packets: 1416 · Displayed: 10 (0.7%) | Profile: Default

12:58 PM
5/7/2025

21. **Make a screen capture** showing the **issuer of the certificate**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:05:29
Jalen Salgado

tcp.port == 443

```
No.   Time      Source         Destination    Protocol Length Info
   98 2.329332  162.125.32.5   10.2.1.45      TCP        60 443 → 49772 [ACK] Seq=4414 Ack=3614 Win=38912 Len=0
   99 2.335911  162.125.32.5   10.2.1.45      TLSv1.2   827 Application Data
  100 2.394744  10.2.1.45      162.125.32.5   TCP        54 49772 → 443 [ACK] Seq=3614 Ack=5187 Win=15616 Len=0
  105 2.738969  10.2.1.45      172.20.6.20    TCP        66 49773 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  106 2.740418  172.20.6.20    10.2.1.45      TCP        66 443 → 49773 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  107 2.740497  10.2.1.45      172.20.6.20    TCP        54 49773 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0
  108 2.740711  10.2.1.45      172.20.6.20    TLSv1.2   265 Client Hello
  109 2.741811  172.20.6.20    10.2.1.45      TCP        60 443 → 49773 [ACK] Seq=1 Ack=212 Win=30336 Len=0
  110 2.751727  172.20.6.20    10.2.1.45      TLSv1.2  1514 Server Hello
  111 2.752240  172.20.6.20    10.2.1.45      TLSv1.2  1514 Certificate [TCP segment of a reassembled PDU]
  112 2.752241  172.20.6.20    10.2.1.45      TLSv1.2   553 Server Key Exchange, Server Hello Done
  113 2.752353  10.2.1.45      172.20.6.20    TCP        54 49773 → 443 [ACK] Seq=212 Ack=3420 Win=16384 Len=0
  114 2.754741  10.2.1.45      172.20.6.20    TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  115 2.757195  172.20.6.20    10.2.1.45      TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
```

```
> Frame 111: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{71EDC829-B742-4804-9793-FEBBF56254F2}, id 0
> Ethernet II, Src: ASUSTekC_a3:ae:f8 (40:16:7e:a3:ae:f8), Dst: IntelCor_db:d3:28 (70:1c:e7:db:d3:28)
> Internet Protocol Version 4, Src: 172.20.6.20, Dst: 10.2.1.45
> Transmission Control Protocol, Src Port: 443, Dst Port: 49773, Seq: 1461, Ack: 212, Len: 1460
> [2 Reassembled TCP Segments (2750 bytes): #110(1394), #111(1356)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2745
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2741
        Certificates Length: 2738
      > Certificates (2738 bytes)
```

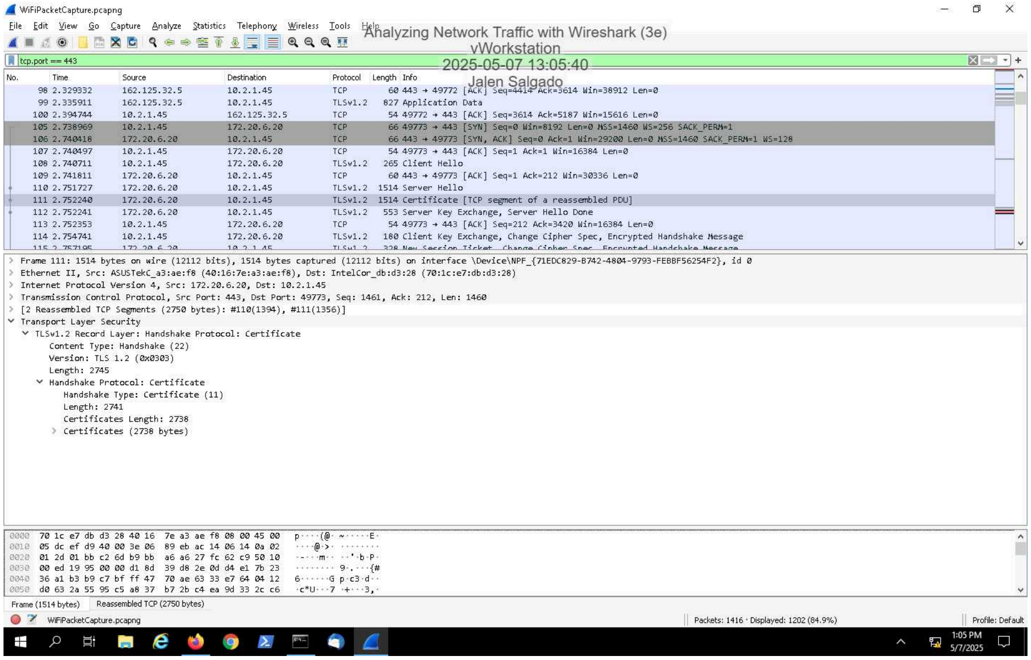
```
0000  70 1c e7 db d3 28 40 16  7e a3 ae f8 08 00 45 00   p····(@· ~·····E·
0010  05 dc ef d9 40 00 3e 06  89 eb ac 14 06 14 0a 02   ····@·>· ········
0020  01 2d 01 bb c2 6d b9 bb  a6 a6 27 fc 62 c9 50 10   ·-···m·· ··'·b·P·
0030  00 ed 19 95 00 00 d1 8d  39 d8 2e 0d d4 e1 7b 23   ········ 9·.···{#
0040  36 a1 b3 b9 c7 bf ff 47  70 ae 63 33 e7 64 04 12   6······G p·c3·d··
0050  d0 63 2a 55 95 c5 a8 37  b7 2b c4 ea 9d 33 2c c6   ·c*U···7 ·+···3,·
```

Frame (1514 bytes) | Reassembled TCP (2750 bytes)

WiFiPacketCapture.pcapng | Packets: 1416 · Displayed: 1202 (84.9%) | Profile: Default

1:05 PM
5/7/2025

24. **Make a screen capture** showing the **details of the certificate**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:05:40
Jalen Salgado

tcp.port == 443

```
No.   Time      Source         Destination    Protocol Length Info
   98 2.329332  162.125.32.5   10.2.1.45      TCP        60 443 → 49772 [ACK] Seq=4414 Ack=3614 Win=38912 Len=0
   99 2.335911  162.125.32.5   10.2.1.45      TLSv1.2   827 Application Data
  100 2.394744  10.2.1.45      162.125.32.5   TCP        54 49772 → 443 [ACK] Seq=3614 Ack=5187 Win=15616 Len=0
  105 2.738969  10.2.1.45      172.20.6.20    TCP        66 49773 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  106 2.740418  172.20.6.20    10.2.1.45      TCP        66 443 → 49773 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  107 2.740497  10.2.1.45      172.20.6.20    TCP        54 49773 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0
  108 2.740711  10.2.1.45      172.20.6.20    TLSv1.2   265 Client Hello
  109 2.741811  172.20.6.20    10.2.1.45      TCP        60 443 → 49773 [ACK] Seq=1 Ack=212 Win=30336 Len=0
  110 2.751727  172.20.6.20    10.2.1.45      TLSv1.2  1514 Server Hello
  111 2.752240  172.20.6.20    10.2.1.45      TLSv1.2  1514 Certificate [TCP segment of a reassembled PDU]
  112 2.752241  172.20.6.20    10.2.1.45      TLSv1.2   553 Server Key Exchange, Server Hello Done
  113 2.752353  10.2.1.45      172.20.6.20    TCP        54 49773 → 443 [ACK] Seq=212 Ack=3420 Win=16384 Len=0
  114 2.754741  10.2.1.45      172.20.6.20    TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  115 2.757195  172.20.6.20    10.2.1.45      TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
```

```
> Frame 111: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{71EDC829-B742-4804-9793-FEBBF56254F2}, id 0
> Ethernet II, Src: ASUSTekC_a3:ae:f8 (40:16:7e:a3:ae:f8), Dst: IntelCor_db:d3:28 (70:1c:e7:db:d3:28)
> Internet Protocol Version 4, Src: 172.20.6.20, Dst: 10.2.1.45
> Transmission Control Protocol, Src Port: 443, Dst Port: 49773, Seq: 1461, Ack: 212, Len: 1460
> [2 Reassembled TCP Segments (2750 bytes): #110(1394), #111(1356)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2745
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2741
        Certificates Length: 2738
      > Certificates (2738 bytes)
```

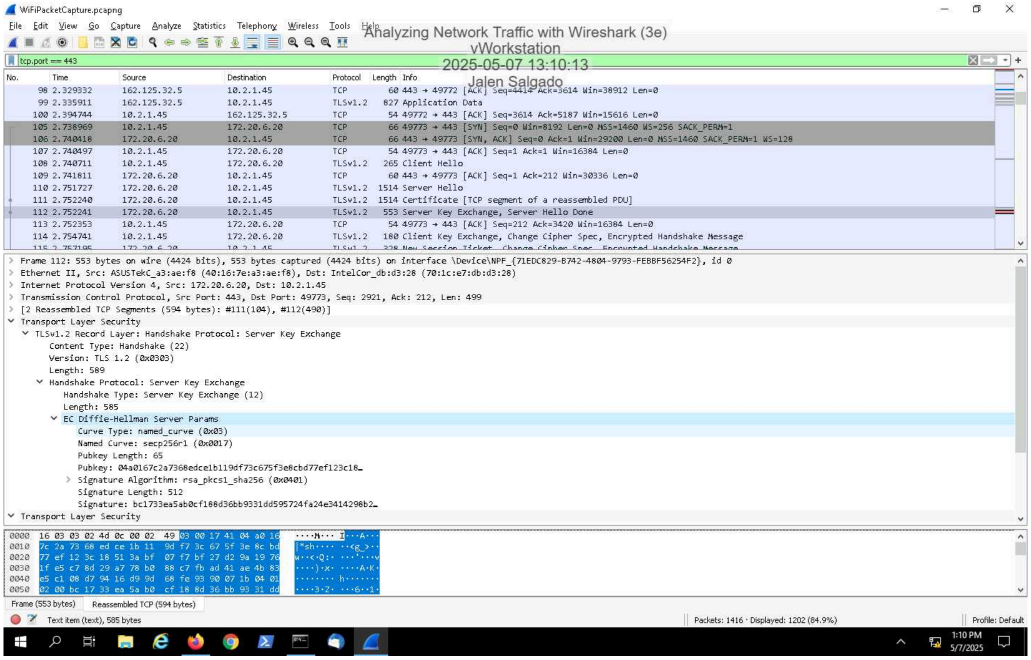
```
0000  70 1c e7 db d3 28 40 16  7e a3 ae f8 08 00 45 00   p····(@· ~·····E·
0010  05 dc ef d9 40 00 3e 06  89 eb ac 14 06 14 0a 02   ····@·>· ········
0020  01 2d 01 bb c2 6d b9 bb  a6 a6 27 fc 62 c9 50 10   ·-···m·· ··'·b·P·
0030  00 ed 19 95 00 00 d1 8d  39 d8 2e 0d d4 e1 7b 23   ········ 9·.···{#
0040  36 a1 b3 b9 c7 bf ff 47  70 ae 63 33 e7 64 04 12   6······G p·c3·d··
0050  d0 63 2a 55 95 c5 a8 37  b7 2b c4 ea 9d 33 2c c6   ·c*U···7 ·+···3,·
```

Frame (1514 bytes) | Reassembled TCP (2750 bytes)

WiFiPacketCapture.pcapng | Packets: 1416 · Displayed: 1202 (84.9%) | Profile: Default

1:05 PM
5/7/2025

27. **Make a screen capture** showing the **public key and signature hash for the certificate**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:10:13
Jalen Salgado

WiFiPacketCapture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

```
No.   Time        Source          Destination     Protocol  Length Info
   98 2.329332    162.125.32.5    10.2.1.45       TCP         60 443 → 49772 [ACK] Seq=4414 Ack=3614 Win=38912 Len=0
   99 2.335911    162.125.32.5    10.2.1.45       TLSv1.2    827 Application Data
  100 2.394744    10.2.1.45       162.125.32.5    TCP         54 49772 → 443 [ACK] Seq=3614 Ack=5187 Win=15616 Len=0
  105 2.738969    10.2.1.45       172.20.6.20     TCP         66 49773 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  106 2.740418    172.20.6.20     10.2.1.45       TCP         66 443 → 49773 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  107 2.740497    10.2.1.45       172.20.6.20     TCP         54 49773 → 443 [ACK] Seq=1 Ack=1 Win=16384 Len=0
  108 2.740711    10.2.1.45       172.20.6.20     TLSv1.2    265 Client Hello
  109 2.741811    172.20.6.20     10.2.1.45       TCP         60 443 → 49773 [ACK] Seq=1 Ack=212 Win=30336 Len=0
  110 2.751727    172.20.6.20     10.2.1.45       TLSv1.2   1514 Server Hello
  111 2.752240    172.20.6.20     10.2.1.45       TLSv1.2   1514 Certificate [TCP segment of a reassembled PDU]
  112 2.752241    172.20.6.20     10.2.1.45       TLSv1.2    553 Server Key Exchange, Server Hello Done
  113 2.752353    10.2.1.45       172.20.6.20     TCP         54 49773 → 443 [ACK] Seq=212 Ack=3420 Win=16384 Len=0
  114 2.754741    10.2.1.45       172.20.6.20     TLSv1.2    180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  115 2.757195    172.20.6.20     10.2.1.45       TLSv1.2    328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
```

```
> Frame 112: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface \Device\NPF_{71EDC829-B742-4804-9793-FEBBF56254F2}, id 0
> Ethernet II, Src: ASUSTekC_a3:ae:f8 (40:16:7e:a3:ae:f8), Dst: IntelCor_db:d3:28 (70:1c:e7:db:d3:28)
> Internet Protocol Version 4, Src: 172.20.6.20, Dst: 10.2.1.45
> Transmission Control Protocol, Src Port: 443, Dst Port: 49773, Seq: 2921, Ack: 212, Len: 499
> [2 Reassembled TCP Segments (594 bytes): #111(104), #112(490)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 589
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 585
      v EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: secp256r1 (0x0017)
          Pubkey Length: 65
          Pubkey: 04a0167c2a7368edce1b119df73c675f3e8cbd77ef123c18…
        > Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
          Signature Length: 512
          Signature: bc1733ea5ab0cf188d36bb9331dd595724fa24e3414298b2…
v Transport Layer Security
```

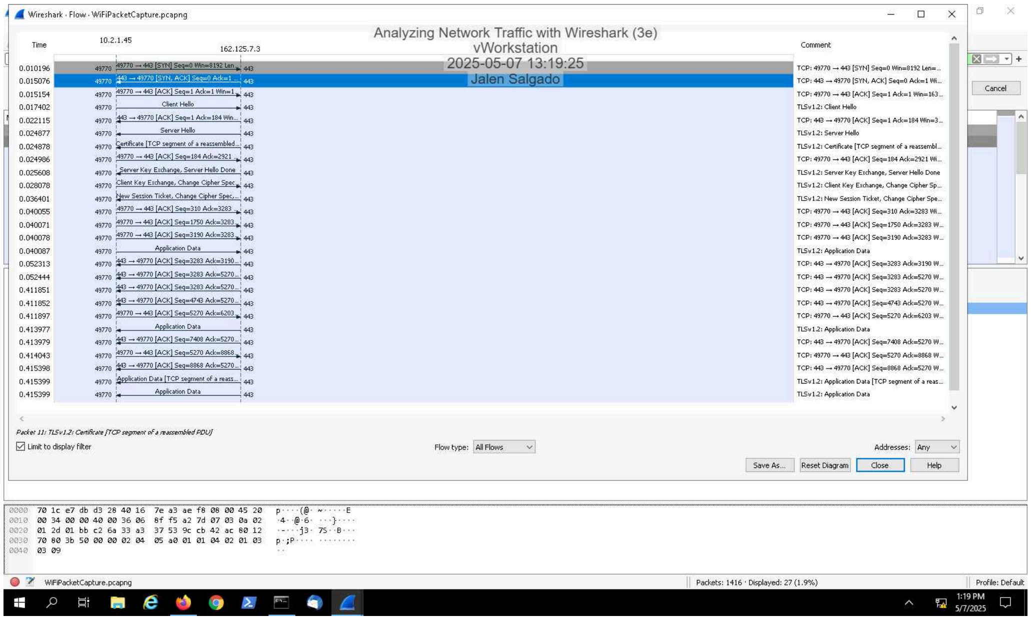
```
0000  16 03 03 02 4d 0c 00 02  49 03 00 17 41 04 a0 16   ····M··· I···A···
0010  7c 2a 73 68 ed ce 1b 11  9d f7 3c 67 5f 3e 8c bd   |*sh···· ··<g_>··
0020  77 ef 12 3c 18 51 3a bf  07 f7 bf 27 d2 9a 19 76   w··<·Q:· ···'···v
0030  1f e5 c7 8d 29 a7 78 b0  88 c7 fb ad 41 ae 4b 83   ····)·x· ····A·K·
0040  e5 c1 08 d7 94 16 d9 9d  68 fe 93 90 07 1b 04 01   ········ h·······
0050  02 00 bc 17 33 ea 5a b0  cf 18 8d 36 bb 93 31 dd   ····3·Z· ···6··1·
```

Frame (553 bytes) | Reassembled TCP (594 bytes)

Text item (text), 585 bytes | Packets: 1416 · Displayed: 1202 (84.9%) | Profile: Default

1:10 PM
5/7/2025

35. **Make a screen capture** showing the **first three-way TCP handshake in the Flow Graph**.



Wireshark · Flow · WiFiPacketCapture.pcapng

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:19:25
Jalen Salgado

```
Time       10.2.1.45            162.125.7.3    Comment
0.010196   49770  49770 → 443 [SYN] Seq=0 Win=8192 Len…              443   TCP: 49770 → 443 [SYN] Seq=0 Win=8192 Len=…
0.015076   49770  443 → 49770 [SYN, ACK] Seq=0 Ack=1 …               443   TCP: 443 → 49770 [SYN, ACK] Seq=0 Ack=1 Wi…
0.015154   49770  49770 → 443 [ACK] Seq=1 Ack=1 Win=1…               443   TCP: 49770 → 443 [ACK] Seq=1 Ack=1 Win=163…
0.017402   49770  Client Hello                                       443   TLSv1.2: Client Hello
0.022115   49770  443 → 49770 [ACK] Seq=1 Ack=184 Win…               443   TCP: 443 → 49770 [ACK] Seq=1 Ack=184 Win=3…
0.024877   49770  Server Hello                                       443   TLSv1.2: Server Hello
0.024878   49770  Certificate [TCP segment of a reassembled…         443   TLSv1.2: Certificate [TCP segment of a reassembl…
0.024986   49770  49770 → 443 [ACK] Seq=184 Ack=2921 …               443   TCP: 49770 → 443 [ACK] Seq=184 Ack=2921 Wi…
0.025608   49770  Server Key Exchange, Server Hello Done             443   TLSv1.2: Server Key Exchange, Server Hello Done
0.028078   49770  Client Key Exchange, Change Cipher Spec…           443   TLSv1.2: Client Key Exchange, Change Cipher Sp…
0.036401   49770  New Session Ticket, Change Cipher Spec,…           443   TLSv1.2: New Session Ticket, Change Cipher Spe…
0.040055   49770  49770 → 443 [ACK] Seq=310 Ack=3283 …               443   TCP: 49770 → 443 [ACK] Seq=310 Ack=3283 Wi…
0.040071   49770  49770 → 443 [ACK] Seq=1750 Ack=3283…               443   TCP: 49770 → 443 [ACK] Seq=1750 Ack=3283 W…
0.040078   49770  49770 → 443 [ACK] Seq=3190 Ack=3283…               443   TCP: 49770 → 443 [ACK] Seq=3190 Ack=3283 W…
0.040087   49770  Application Data                                   443   TLSv1.2: Application Data
0.052313   49770  443 → 49770 [ACK] Seq=3283 Ack=3190…               443   TCP: 443 → 49770 [ACK] Seq=3283 Ack=3190 W…
0.052444   49770  443 → 49770 [ACK] Seq=3283 Ack=5270…               443   TCP: 443 → 49770 [ACK] Seq=3283 Ack=5270 W…
0.411851   49770  443 → 49770 [ACK] Seq=3283 Ack=5270…               443   TCP: 443 → 49770 [ACK] Seq=3283 Ack=5270 W…
0.411852   49770  443 → 49770 [ACK] Seq=4743 Ack=5270…               443   TCP: 443 → 49770 [ACK] Seq=4743 Ack=5270 W…
0.411897   49770  49770 → 443 [ACK] Seq=5270 Ack=6203…               443   TCP: 49770 → 443 [ACK] Seq=5270 Ack=6203 W…
0.413977   49770  Application Data                                   443   TLSv1.2: Application Data
0.413979   49770  443 → 49770 [ACK] Seq=7408 Ack=5270…               443   TCP: 443 → 49770 [ACK] Seq=7408 Ack=5270 W…
0.414043   49770  49770 → 443 [ACK] Seq=5270 Ack=8868…               443   TCP: 49770 → 443 [ACK] Seq=5270 Ack=8868 W…
0.415398   49770  443 → 49770 [ACK] Seq=8868 Ack=5270…               443   TCP: 443 → 49770 [ACK] Seq=8868 Ack=5270 W…
0.415399   49770  Application Data [TCP segment of a reass…          443   TLSv1.2: Application Data [TCP segment of a reas…
0.415399   49770  Application Data                                   443   TLSv1.2: Application Data
```

Packet 11: TLSv1.2: Certificate [TCP segment of a reassembled PDU]

☑ Limit to display filter

Flow type: All Flows

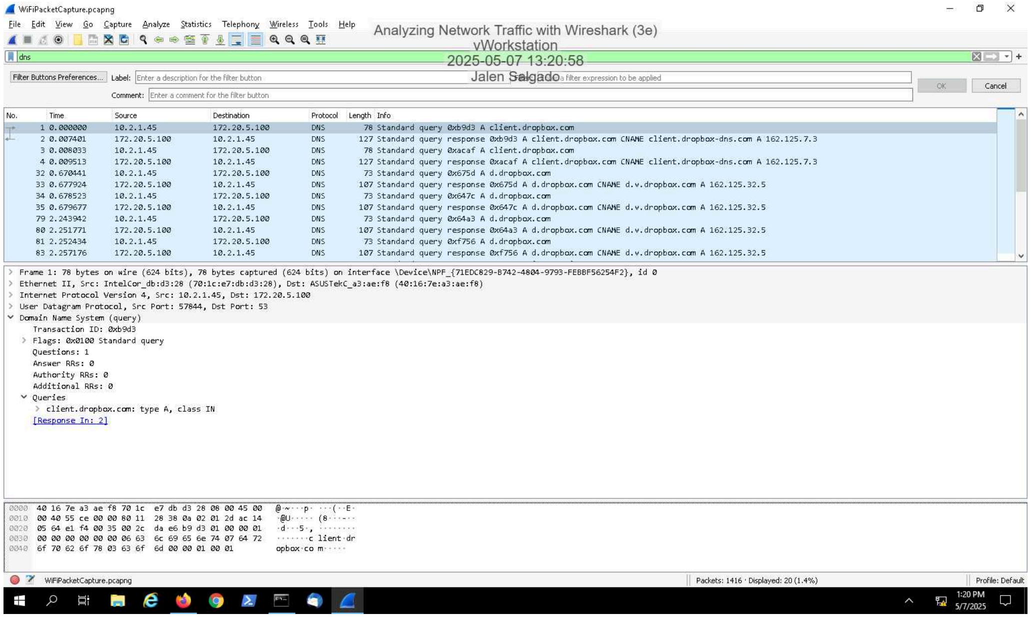
Addresses: Any

```
0000  70 1c e7 db d3 28 40 16  7e a3 ae f8 08 00 45 20   p····(@· ~·····E
0010  00 34 00 00 40 00 36 06  8f f5 a2 7d 07 03 0a 02   ·4··@·6· ···}····
0020  01 2d 01 bb c2 6a 33 a3  37 53 9c cb 42 ac 80 12   ·-···j3· 7S··B···
0030  70 80 3b 50 00 00 02 04  05 a0 01 01 04 02 01 03   p·;P···· ········
0040  03 09                                              ··
```

WiFiPacketCapture.pcapng | Packets: 1416 · Displayed: 27 (1.9%) | Profile: Default

1:19 PM
5/7/2025

40. **Make a screen capture** showing the **query posed in this packet**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:20:58
Jalen Salgado

Filter: dns

```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  10.2.1.45      172.20.5.100   DNS        78 Standard query 0xb9d3 A client.dropbox.com
   2 0.007401  172.20.5.100   10.2.1.45      DNS       127 Standard query response 0xb9d3 A client.dropbox.com CNAME client.dropbox-dns.com A 162.125.7.3
   3 0.008033  10.2.1.45      172.20.5.100   DNS        78 Standard query 0xacaf A client.dropbox.com
   4 0.009513  172.20.5.100   10.2.1.45      DNS       127 Standard query response 0xacaf A client.dropbox.com CNAME client.dropbox-dns.com A 162.125.7.3
  32 0.670441  10.2.1.45      172.20.5.100   DNS        73 Standard query 0x675d A d.dropbox.com
  33 0.677924  172.20.5.100   10.2.1.45      DNS       107 Standard query response 0x675d A d.dropbox.com CNAME d.v.dropbox.com A 162.125.32.5
  34 0.678523  10.2.1.45      172.20.5.100   DNS        73 Standard query 0x647c A d.dropbox.com
  35 0.679677  172.20.5.100   10.2.1.45      DNS       107 Standard query response 0x647c A d.dropbox.com CNAME d.v.dropbox.com A 162.125.32.5
  79 2.243942  10.2.1.45      172.20.5.100   DNS        73 Standard query 0x64a3 A d.dropbox.com
  80 2.251771  172.20.5.100   10.2.1.45      DNS       107 Standard query response 0x64a3 A d.dropbox.com CNAME d.v.dropbox.com A 162.125.32.5
  81 2.252434  10.2.1.45      172.20.5.100   DNS        73 Standard query 0xf756 A d.dropbox.com
  83 2.257176  172.20.5.100   10.2.1.45      DNS       107 Standard query response 0xf756 A d.dropbox.com CNAME d.v.dropbox.com A 162.125.32.5
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{71EDC829-B742-4804-9793-FEBBF56254F2}, id 0
> Ethernet II, Src: IntelCor_db:d3:28 (70:1c:e7:db:d3:28), Dst: ASUSTekC_a3:ae:f8 (40:16:7e:a3:ae:f8)
> Internet Protocol Version 4, Src: 10.2.1.45, Dst: 172.20.5.100
> User Datagram Protocol, Src Port: 57844, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xb9d3
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > client.dropbox.com: type A, class IN
    [Response In: 2]
```

```
0000  40 16 7e a3 ae f8 70 1c  e7 db d3 28 08 00 45 00   @·~···p· ···(··E·
0010  00 40 55 ce 00 00 80 11  28 38 0a 02 01 2d ac 14   ·@U····· (8···-··
0020  05 64 e1 f4 00 35 00 2c  da e6 b9 d3 01 00 00 01   ·d···5·, ········
0030  00 00 00 00 00 00 06 63  6c 69 65 6e 74 07 64 72   ·······c lient·dr
0040  6f 70 62 6f 78 03 63 6f  6d 00 00 01 00 01         opbox·co m·····
```

Packets: 1416 · Displayed: 20 (1.4%)

Section 3: Challenge and Analysis

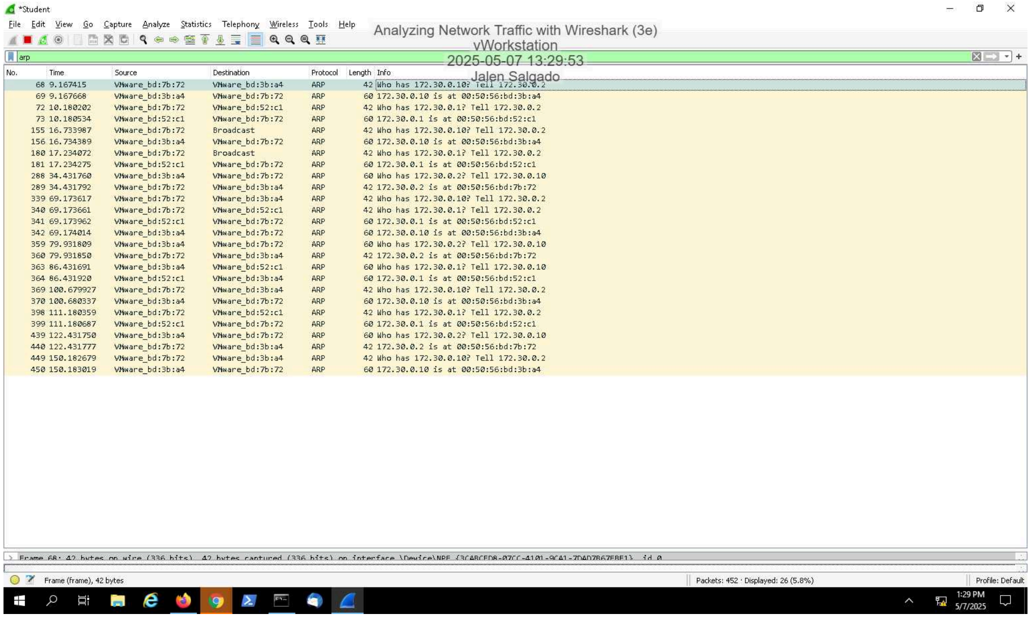
Part 1: Research Common Network Traffic

Identify at least five common protocols and their associated TCP/UDP port numbers, then **explain** their purpose and relevant features (for example, known security vulnerabilities, etc.).

HTTP: It delivers unecrypyted web content and is used for browsing websites the dont use encryption its also vulneraabler to eavesdroppiong and MITM attacks. HTTPS on port 443 is the main one. It secures the connection using TLS so no one can snoop on what you're doing. It’s solid, but if the site’s using an outdated version of TLS, it can still get hit by things like downgrade attacks. DNS on port 53 is what turns the website name into an IP address so your browser knows where to go. It usually runs over UDP, and the problem is it’s not encrypted by default, which makes it easy to spoof unless it’s using DNS over HTTPS. Then there’s just TCP, which handles the reliable delivery of all this traffic. It keeps things in order, but it can be abused with attacks like SYN floods. TLS is also a big piece here. It handles the actual encryption behind HTTPS. It's strong now, but older versions had some serious holes like Heartbleed. These protocols basically work together every time you load up a website.

Part 2: Capture and Filter Traffic Using Wireshark

Make a screen capture showing the **MAC address resolved by ARP for the DNS server**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:29:53
Jalen Salgado

arp

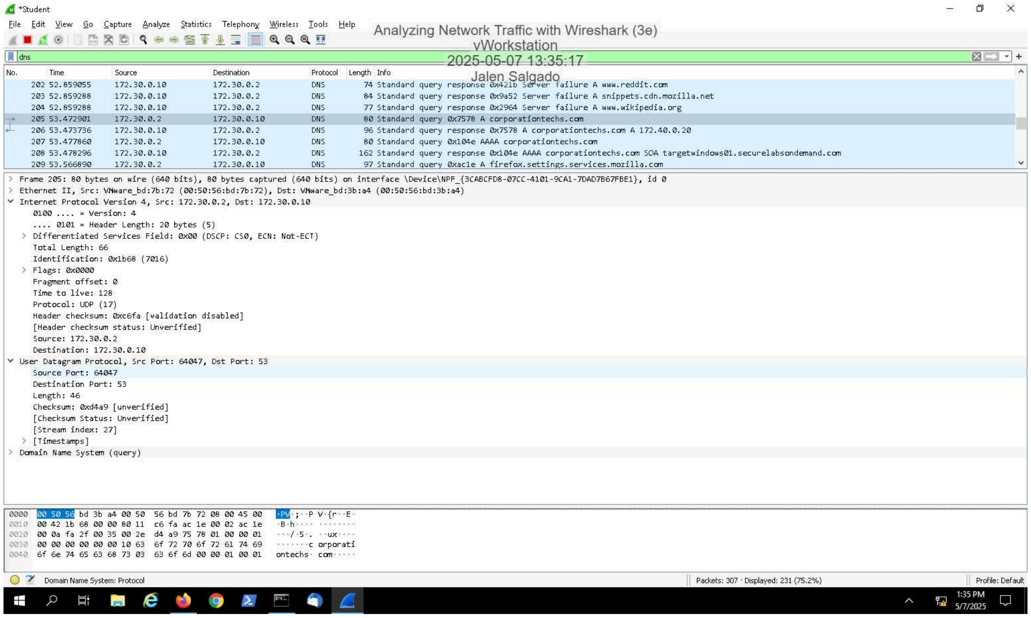
No.	Time	Source	Destination	Protocol	Length	Info
68	9.167415	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
69	9.167668	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	172.30.0.10 is at 00:50:56:bd:3b:a4
72	10.180202	VMware_bd:7b:72	VMware_bd:52:c1	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
73	10.180534	VMware_bd:52:c1	VMware_bd:7b:72	ARP	60	172.30.0.1 is at 00:50:56:bd:52:c1
155	16.733987	VMware_bd:7b:72	Broadcast	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
156	16.734389	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	172.30.0.10 is at 00:50:56:bd:3b:a4
180	17.234072	VMware_bd:7b:72	Broadcast	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
181	17.234275	VMware_bd:52:c1	VMware_bd:7b:72	ARP	60	172.30.0.1 is at 00:50:56:bd:52:c1
288	34.431760	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	Who has 172.30.0.2? Tell 172.30.0.10
289	34.431792	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	172.30.0.2 is at 00:50:56:bd:7b:72
339	69.173617	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
340	69.173661	VMware_bd:7b:72	VMware_bd:52:c1	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
341	69.173962	VMware_bd:52:c1	VMware_bd:7b:72	ARP	60	172.30.0.1 is at 00:50:56:bd:52:c1
342	69.174014	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	172.30.0.10 is at 00:50:56:bd:3b:a4
359	79.931809	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	Who has 172.30.0.2? Tell 172.30.0.10
360	79.931850	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	172.30.0.2 is at 00:50:56:bd:7b:72
363	86.431691	VMware_bd:3b:a4	VMware_bd:52:c1	ARP	60	Who has 172.30.0.1? Tell 172.30.0.10
364	86.431920	VMware_bd:52:c1	VMware_bd:3b:a4	ARP	60	172.30.0.1 is at 00:50:56:bd:52:c1
369	100.679927	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
370	100.680337	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	172.30.0.10 is at 00:50:56:bd:3b:a4
398	111.180359	VMware_bd:7b:72	VMware_bd:52:c1	ARP	42	Who has 172.30.0.1? Tell 172.30.0.2
399	111.180687	VMware_bd:52:c1	VMware_bd:7b:72	ARP	60	172.30.0.1 is at 00:50:56:bd:52:c1
439	122.431750	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	Who has 172.30.0.2? Tell 172.30.0.10
440	122.431777	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	172.30.0.2 is at 00:50:56:bd:7b:72
449	150.182679	VMware_bd:7b:72	VMware_bd:3b:a4	ARP	42	Who has 172.30.0.10? Tell 172.30.0.2
450	150.183019	VMware_bd:3b:a4	VMware_bd:7b:72	ARP	60	172.30.0.10 is at 00:50:56:bd:3b:a4

```
> Frame 68: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{3CABCED8-07CC-4101-9CA1-7DAD7B67EBE1}, id 0
```

Frame (frame), 42 bytes | Packets: 452 · Displayed: 26 (5.8%) | Profile: Default

1:29 PM
5/7/2025

Make a screen capture showing the **destination IP address and port number of the DNS server**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:35:17
Jalen Salgado

*Student — Filter: dns

```
No.  Time       Source       Destination  Protocol Length Info
202 52.859055   172.30.0.10  172.30.0.2   DNS      74 Standard query response 0x421b Server failure A www.reddit.com
203 52.859288   172.30.0.10  172.30.0.2   DNS      84 Standard query response 0x9a52 Server failure A snippets.cdn.mozilla.net
204 52.859288   172.30.0.10  172.30.0.2   DNS      77 Standard query response 0x2964 Server failure A www.wikipedia.org
205 53.472901   172.30.0.2   172.30.0.10  DNS      80 Standard query 0x7578 A corporationtechs.com
206 53.473736   172.30.0.10  172.30.0.2   DNS      96 Standard query response 0x7578 A corporationtechs.com A 172.40.0.20
207 53.477860   172.30.0.2   172.30.0.10  DNS      80 Standard query 0x104e AAAA corporationtechs.com
208 53.478296   172.30.0.10  172.30.0.2   DNS     162 Standard query response 0x104e AAAA corporationtechs.com SOA targetwindows01.securelabsondemand.com
209 53.566890   172.30.0.2   172.30.0.10  DNS      97 Standard query 0xac1e A firefox.settings.services.mozilla.com
```

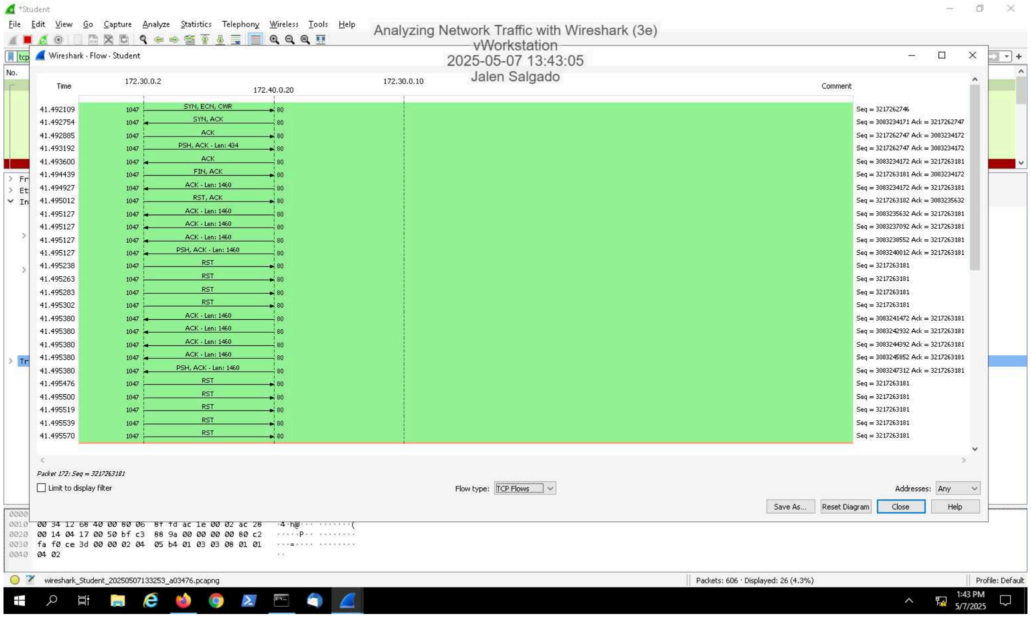
```
> Frame 205: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{3CABCFD8-07CC-4101-9CA1-7DAD7B67FBE1}, id 0
> Ethernet II, Src: VMware_bd:7b:72 (00:50:56:bd:7b:72), Dst: VMware_bd:3b:a4 (00:50:56:bd:3b:a4)
v Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x1b68 (7016)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xc6fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.0.2
    Destination: 172.30.0.10
v User Datagram Protocol, Src Port: 64047, Dst Port: 53
    Source Port: 64047
    Destination Port: 53
    Length: 46
    Checksum: 0xd4a9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 27]
  > [Timestamps]
> Domain Name System (query)
```

```
0000  00 50 56 bd 3b a4 00 50  56 bd 7b 72 08 00 45 00   ·PV·;··P V·{r··E·
0010  00 42 1b 68 00 00 80 11  c6 fa ac 1e 00 02 ac 1e   ·B·h···· ········
0020  00 0a fa 2f 00 35 00 2e  d4 a9 75 78 01 00 00 01   ···/·5·. ··ux····
0030  00 00 00 00 00 00 10 63  6f 72 70 6f 72 61 74 69   ·······c orporati
0040  6f 6e 74 65 63 68 73 03  63 6f 6d 00 00 01 00 01   ontechs· com·····
```

Domain Name System: Protocol | Packets: 307 · Displayed: 231 (75.2%) | Profile: Default

1:35 PM 5/7/2025

Make a screen capture of the **three-way handshake that took place between the client PC and the web server**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:43:05
Jalen Salgado

Wireshark · Flow · Student

```
Time        172.30.0.2   172.40.0.20   172.30.0.10   Comment
41.492109   1047 --SYN, ECN, CWR-->          80   Seq = 3217262746
41.492754   1047 <--SYN, ACK--               80   Seq = 3083234171 Ack = 3217262747
41.492885   1047 --ACK-->                    80   Seq = 3217262747 Ack = 3083234172
41.493192   1047 --PSH, ACK - Len: 434-->    80   Seq = 3217262747 Ack = 3083234172
41.493600   1047 <--ACK--                    80   Seq = 3083234172 Ack = 3217263181
41.494439   1047 --FIN, ACK-->               80   Seq = 3217263181 Ack = 3083234172
41.494927   1047 <--ACK - Len: 1460--        80   Seq = 3083234172 Ack = 3217263181
41.495012   1047 --RST, ACK-->               80   Seq = 3217263182 Ack = 3083235632
41.495127   1047 <--ACK - Len: 1460--        80   Seq = 3083235632 Ack = 3217263181
41.495127   1047 <--ACK - Len: 1460--        80   Seq = 3083237092 Ack = 3217263181
41.495127   1047 <--ACK - Len: 1460--        80   Seq = 3083238552 Ack = 3217263181
41.495127   1047 <--PSH, ACK - Len: 1460--   80   Seq = 3083240012 Ack = 3217263181
41.495238   1047 --RST-->                    80   Seq = 3217263181
41.495263   1047 --RST-->                    80   Seq = 3217263181
41.495283   1047 --RST-->                    80   Seq = 3217263181
41.495302   1047 --RST-->                    80   Seq = 3217263181
41.495380   1047 <--ACK - Len: 1460--        80   Seq = 3083241472 Ack = 3217263181
41.495380   1047 <--ACK - Len: 1460--        80   Seq = 3083242932 Ack = 3217263181
41.495380   1047 <--ACK - Len: 1460--        80   Seq = 3083244392 Ack = 3217263181
41.495380   1047 <--ACK - Len: 1460--        80   Seq = 3083245852 Ack = 3217263181
41.495380   1047 <--PSH, ACK - Len: 1460--   80   Seq = 3083247312 Ack = 3217263181
41.495476   1047 --RST-->                    80   Seq = 3217263181
41.495500   1047 --RST-->                    80   Seq = 3217263181
41.495519   1047 --RST-->                    80   Seq = 3217263181
41.495539   1047 --RST-->                    80   Seq = 3217263181
41.495570   1047 --RST-->                    80   Seq = 3217263181
```

Packet 172: Seq = 3217263181

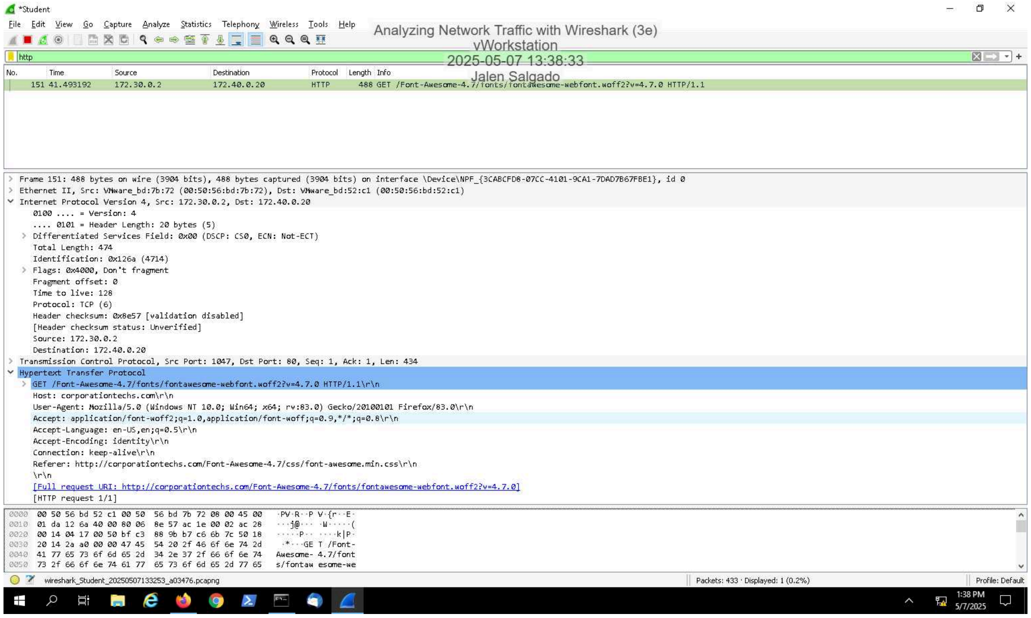
☐ Limit to display filter   Flow type: TCP Flows   Addresses: Any

```
0010  00 34 12 68 40 00 80 06  8f fd ac 1e 00 02 ac 28   ·4·h@··· ·······(
0020  00 14 04 17 00 50 bf c3  88 9a 00 00 00 00 80 c2   ·····P·· ········
0030  fa f0 ce 3d 00 00 02 04  05 b4 01 03 03 08 01 01   ···=···· ········
0040  04 02                                              ··
```

wireshark_Student_20250507133253_a03476.pcapng | Packets: 606 · Displayed: 26 (4.3%) | Profile: Default

1:43 PM 5/7/2025

Make a screen capture of the **actual HTTP traffic that was delivered from the corporationtechs.com web server**.

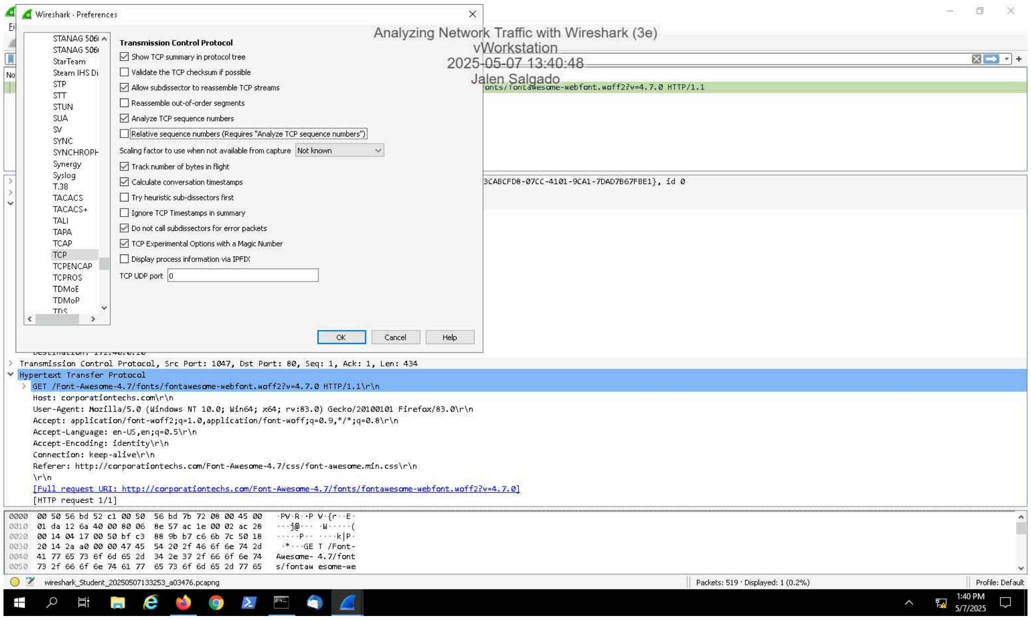

*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:38:33
Jalen Salgado

```
http

No.   Time       Source      Destination  Protocol  Length  Info
  151 41.493192  172.30.0.2  172.40.0.20  HTTP      488     GET /Font-Awesome-4.7/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1

> Frame 151: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF_{3CABCFD8-07CC-4101-9CA1-7DAD7B67FBE1}, id 0
> Ethernet II, Src: VMware_bd:7b:72 (00:50:56:bd:7b:72), Dst: VMware_bd:52:c1 (00:50:56:bd:52:c1)
v Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 474
    Identification: 0x126a (4714)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x8e57 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.30.0.2
    Destination: 172.40.0.20
> Transmission Control Protocol, Src Port: 1047, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
v Hypertext Transfer Protocol
  > GET /Font-Awesome-4.7/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1\r\n
    Host: corporationtechs.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0\r\n
    Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: identity\r\n
    Connection: keep-alive\r\n
    Referer: http://corporationtechs.com/Font-Awesome-4.7/css/font-awesome.min.css\r\n
    \r\n
    [Full request URI: http://corporationtechs.com/Font-Awesome-4.7/fonts/fontawesome-webfont.woff2?v=4.7.0]
    [HTTP request 1/1]

0000  00 50 56 bd 52 c1 00 50  56 bd 7b 72 08 00 45 00   ·PV·R··P V·{r··E·
0010  01 da 12 6a 40 00 80 06  8e 57 ac 1e 00 02 ac 28   ···j@··· ·W·····(
0020  00 14 04 17 00 50 bf c3  88 9b b7 c6 6b 7c 50 18   ·····P·· ····k|P·
0030  20 14 2a a0 00 00 47 45  54 20 2f 46 6f 6e 74 2d    ·*···GE T /Font-
0040  41 77 65 73 6f 6d 65 2d  34 2e 37 2f 66 6f 6e 74   Awesome- 4.7/font
0050  73 2f 66 6f 6e 74 61 77  65 73 6f 6d 65 2d 77 65   s/fontaw esome-we

wireshark_Student_20250507133253_a03476.pcapng    Packets: 433 · Displayed: 1 (0.2%)    Profile: Default
```

Part 3: Analyze Capture Files

Make a screen capture showing the **updated Wireshark TCP preferences for relative sequence numbers**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:40:48
Jalen Salgado

Transmission Control Protocol

- ☑ Show TCP summary in protocol tree
- ☐ Validate the TCP checksum if possible
- ☑ Allow subdissector to reassemble TCP streams
- ☐ Reassemble out-of-order segments
- ☑ Analyze TCP sequence numbers
- ☐ Relative sequence numbers (Requires "Analyze TCP sequence numbers")

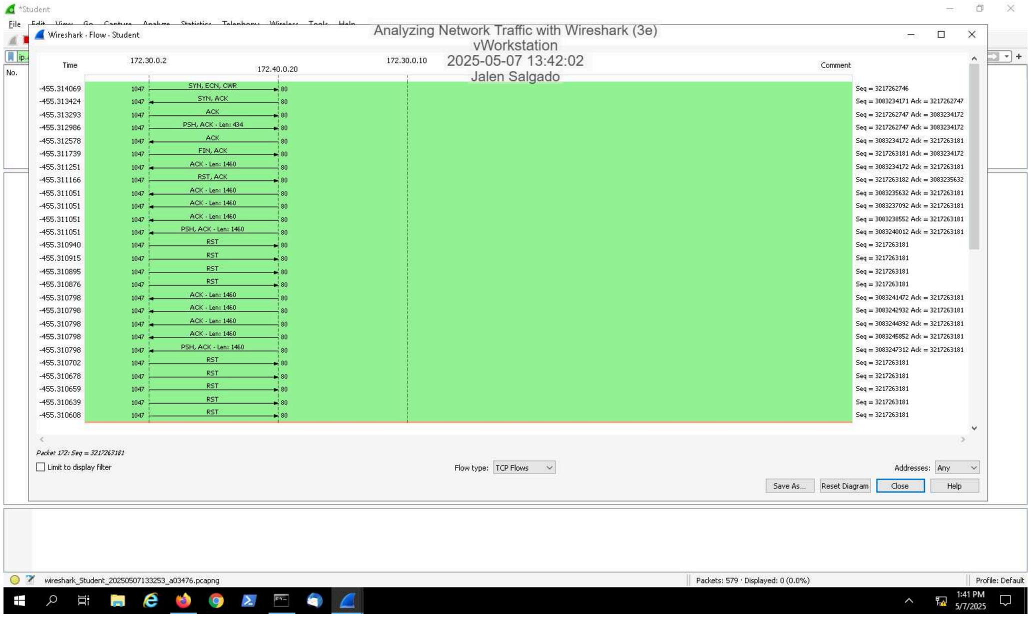
Scaling factor to use when not available from capture: Not known

- ☑ Track number of bytes in flight
- ☑ Calculate conversation timestamps
- ☐ Try heuristic sub-dissectors first
- ☐ Ignore TCP Timestamps in summary
- ☑ Do not call subdissectors for error packets
- ☑ TCP Experimental Options with a Magic Number
- ☐ Display process information via IPFIX

TCP UDP port: 0

```
> Transmission Control Protocol, Src Port: 1047, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
v Hypertext Transfer Protocol
  > GET /Font-Awesome-4.7/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1\r\n
    Host: corporationtechs.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0\r\n
    Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: identity\r\n
    Connection: keep-alive\r\n
    Referer: http://corporationtechs.com/Font-Awesome-4.7/css/font-awesome.min.css\r\n
    \r\n
    [Full request URI: http://corporationtechs.com/Font-Awesome-4.7/fonts/fontawesome-webfont.woff2?v=4.7.0]
    [HTTP request 1/1]

0000  00 50 56 bd 52 c1 00 50  56 bd 7b 72 08 00 45 00   ·PV·R··P V·{r··E·
0010  01 da 12 6a 40 00 80 06  8e 57 ac 1e 00 02 ac 28   ···j@··· ·W·····(
0020  00 14 04 17 00 50 bf c3  88 9b b7 c6 6b 7c 50 18   ·····P·· ····k|P·
0030  20 14 2a a0 00 00 47 45  54 20 2f 46 6f 6e 74 2d    ·*···GE T /Font-
0040  41 77 65 73 6f 6d 65 2d  34 2e 37 2f 66 6f 6e 74   Awesome- 4.7/font
0050  73 2f 66 6f 6e 74 61 77  65 73 6f 6d 65 2d 77 65   s/fontaw esome-we

wireshark_Student_20250507133253_a03476.pcapng    Packets: 519 · Displayed: 1 (0.2%)    Profile: Default
```

Make a screen capture showing the **flow graph displaying the sequence and acknowledgement values recorded during the three-way handshake**.



Analyzing Network Traffic with Wireshark (3e)
vWorkstation
2025-05-07 13:42:02
Jalen Salgado

```
Time           172.30.0.2        172.40.0.20        172.30.0.10      Comment

-455.314069    1047  SYN, ECN, CWR ------------> 80   Seq = 3217262746
-455.313424    1047  <------------ SYN, ACK      80   Seq = 3083234171 Ack = 3217262747
-455.313293    1047  ACK ----------------------> 80   Seq = 3217262747 Ack = 3083234172
-455.312986    1047  PSH, ACK - Len: 434 ------> 80   Seq = 3217262747 Ack = 3083234172
-455.312578    1047  <---------------------- ACK 80   Seq = 3083234172 Ack = 3217263181
-455.311739    1047  FIN, ACK -----------------> 80   Seq = 3217263181 Ack = 3083234172
-455.311251    1047  <-------- ACK - Len: 1460   80   Seq = 3083234172 Ack = 3217263181
-455.311166    1047  RST, ACK -----------------> 80   Seq = 3217263182 Ack = 3083235632
-455.311051    1047  <-------- ACK - Len: 1460   80   Seq = 3083235632 Ack = 3217263181
-455.311051    1047  <-------- ACK - Len: 1460   80   Seq = 3083237092 Ack = 3217263181
-455.311051    1047  <-------- ACK - Len: 1460   80   Seq = 3083238552 Ack = 3217263181
-455.311051    1047  <--- PSH, ACK - Len: 1460   80   Seq = 3083240012 Ack = 3217263181
-455.310940    1047  RST ----------------------> 80   Seq = 3217263181
-455.310915    1047  RST ----------------------> 80   Seq = 3217263181
-455.310895    1047  RST ----------------------> 80   Seq = 3217263181
-455.310876    1047  RST ----------------------> 80   Seq = 3217263181
-455.310798    1047  <-------- ACK - Len: 1460   80   Seq = 3083241472 Ack = 3217263181
-455.310798    1047  <-------- ACK - Len: 1460   80   Seq = 3083242932 Ack = 3217263181
-455.310798    1047  <-------- ACK - Len: 1460   80   Seq = 3083244392 Ack = 3217263181
-455.310798    1047  <-------- ACK - Len: 1460   80   Seq = 3083245852 Ack = 3217263181
-455.310798    1047  <--- PSH, ACK - Len: 1460   80   Seq = 3083247312 Ack = 3217263181
-455.310702    1047  RST ----------------------> 80   Seq = 3217263181
-455.310678    1047  RST ----------------------> 80   Seq = 3217263181
-455.310659    1047  RST ----------------------> 80   Seq = 3217263181
-455.310639    1047  RST ----------------------> 80   Seq = 3217263181
-455.310608    1047  RST ----------------------> 80   Seq = 3217263181
```

Packet 172: Seq = 3217263181

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

wireshark_Student_20250507133253_a03476.pcapng | Packets: 579 · Displayed: 0 (0.0%) | Profile: Default

1:41 PM
5/7/2025