

Analyzing Network Traffic with Wireshark (3e)

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

Student:

Mani Sai Voore

Email:

mvoore@cbu.edu

Time on Task:

22 hours, 34 minutes

Progress:

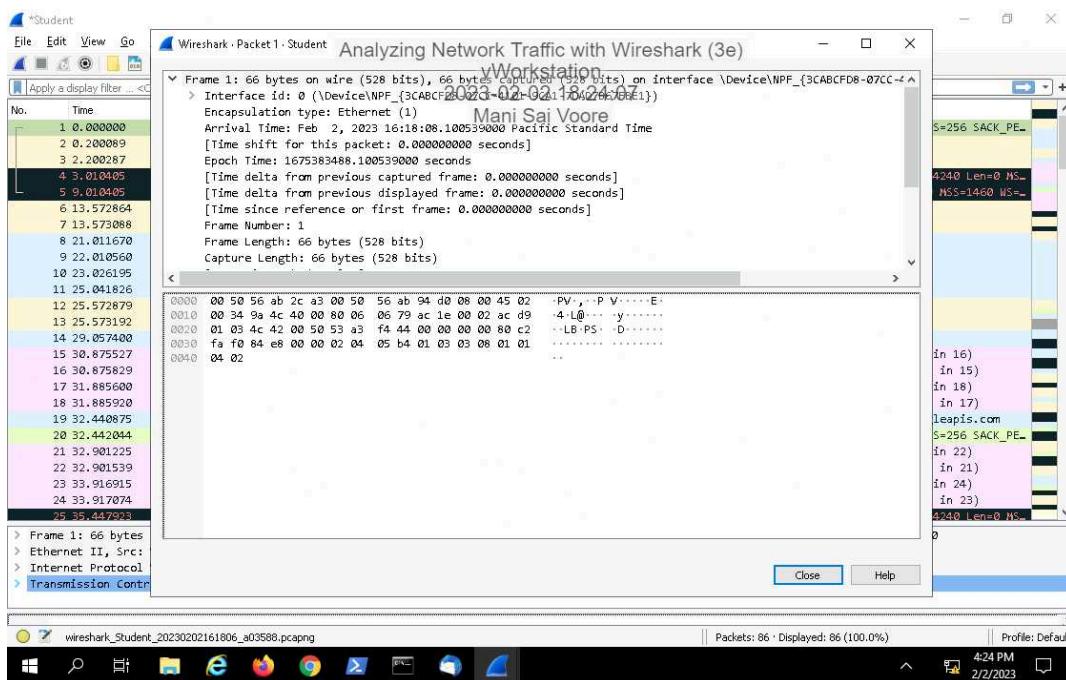
100%

Report Generated: Sunday, February 5, 2023 at 4:56 AM

Section 1: Hands-On Demonstration

Part 1: Explore Wireshark

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

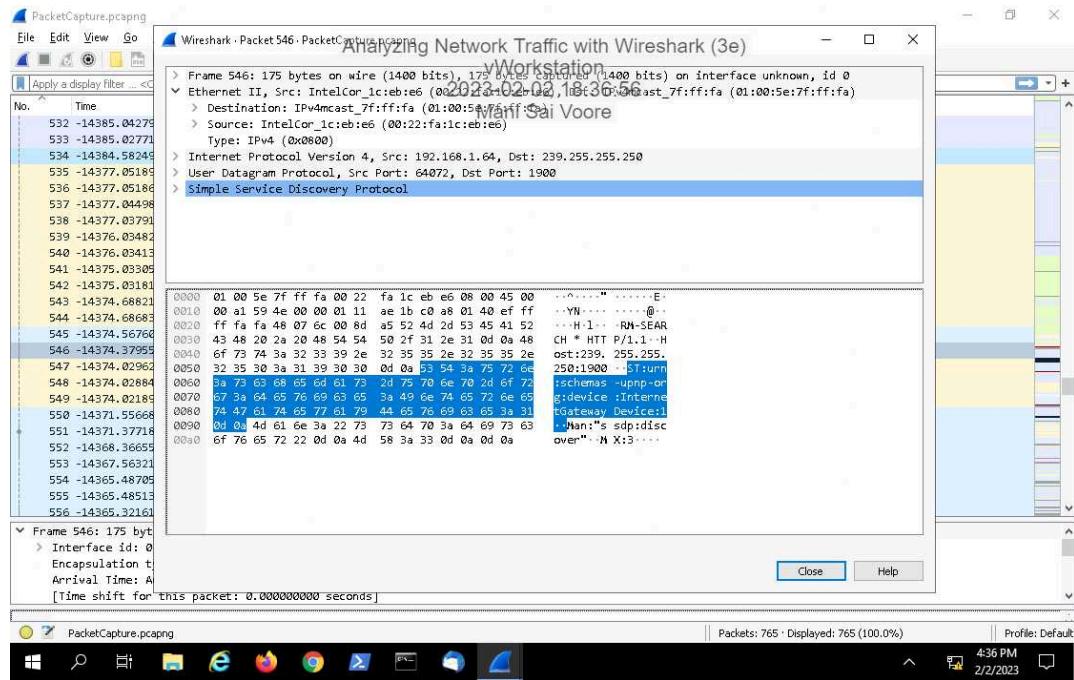


Part 2: Analyze Wireshark Capture Information

Analyzing Network Traffic with Wireshark (3e)

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

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



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

The screenshot shows a browser window with a lab guide on the left and the Wireshark interface on the right. The lab guide includes the following steps:

8. Record the code assigned by the IEEE to Intel for use in identifying Intel Core network interfaces in Packet 546.
9. Record the MAC address used for IPv4 multicast in Packet 546.
10. In the packet details pane, click the arrow at the beginning of the Ethernet II line to collapse the Data Link Layer detail.
11. In the packet details pane, click the arrow at the beginning of the Internet Protocol Version 4 line to collapse the IP detail.

The Wireshark interface shows the same details as the previous screenshot, focusing on the selected packet (Frame 546) and its MAC addresses.

Analyzing Network Traffic with Wireshark (3e)

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

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

LAB GUIDE
Section 1: Hands-On Demonstration
Part 1: Explore Wireshark
Part 2: Analyze Wireshark Capture Information
Section 2: Applied Learning
Section 3: Challenge and Analysis

Part 2: Analyze Wireshark Capture Information (2/14 completed)
Control (MAC) addresses in Packet 546.

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

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

10. In the packet details pane, click the arrow at the beginning of the Ethernet II line to collapse the Data Link Layer detail.

11. In the packet details pane, click the arrow at the beginning of the Internet Protocol line to expand the Network Layer detail.

Frame 546: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface unknown, id 0
Ethernet II, Src: IntelCor_1:ce:be:06 (00:22:fa:1c:be:06), Dst: IPv4mcast_7:ffff:fa (01:00:5e:7:f:ff:fa)
...
Source: IntelCor_1:ce:be:06 (00:22:fa:1c:be:06)
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-
0001 00 01 59 4e 00 00 01 11 fa 1b c0 a8 01 40 ff ff ..-W1...-RN-SEAR
0002 ff fa 48 07 6c 00 8d a5 52 4d 2d 53 45 41 52 CH + HTT P/1.1-H
0003 43 48 20 24 08 48 54 54 50 2f 31 2e 31 0d 08 48 ost:239.255.255.
0004 6f 73 74 34 32 33 39 2e 32 35 35 2e 32 35 35 2e 250.1900 .51urn
0005 32 35 30 3a 31 39 30 30 0d 05 54 3a 75 72 64 :schemas -upnp-org
0006 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72 gidevice :Intern
0007 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72 6e 65 etGateway Device:
0008 74 47 61 74 65 77 61 79 44 65 76 69 63 65 3a 31 .:User's sdipdisc
0009 0d 04 4d 61 6a 22 73 73 64 78 3a 64 69 73 63 over". M X:3...
000a 6f 76 65 72 22 0d 0a 4d 58 3a 33 0d 0a 0d 0a

Packets: 765 · Displayed: 765 (100.0%) 4:41 PM 2/2/2023 Profile: Default

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

LAB GUIDE
Section 1: Hands-On Demonstration
Part 1: Explore Wireshark
Part 2: Analyze Wireshark Capture Information
Section 2: Applied Learning
Section 3: Challenge and Analysis

Part 2: Analyze Wireshark Capture Information (3/14 completed)

11. In the packet details pane, click the arrow at the beginning of the Internet Protocol line to expand the Network Layer detail.

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

Note: A variety of packets can exist on any given network. The IP version will determine how the rest of the packet is interpreted. Almost all

Frame 546: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface unknown, id 0
Internet Protocol Version 4, Src: 192.168.1.64, Dst: 239.255.255.250
Version: 4
Header length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
Total Length: 161
Identification: 0x59e (22862)
Flags: 0x0000
Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0xaeab [validation disabled]

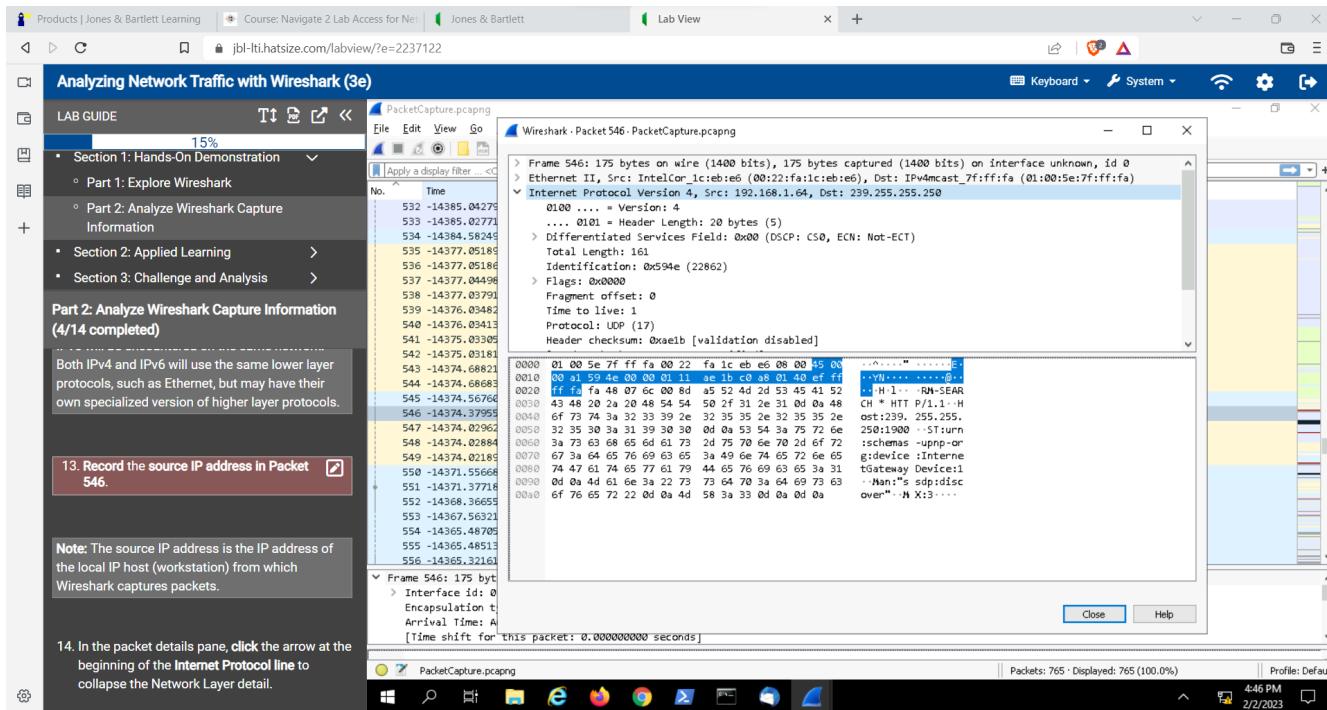
0000 01 00 5e 7f ff fa 00 22 fa 1c eb e6 08 00 45 00 ...-.-.-.-E-
0001 00 01 59 4e 00 00 01 11 fa 1b c0 a8 01 40 ff ff ..-W1...-RN-SEAR
0002 ff fa 48 07 6c 00 8d a5 52 4d 2d 53 45 41 52 CH + HTT P/1.1-H
0003 43 48 20 24 08 48 54 54 50 2f 31 2e 31 0d 08 48 ost:239.255.255.
0004 6f 73 74 34 32 33 39 2e 32 35 35 2e 32 35 35 2e 250.1900 .51urn
0005 32 35 30 3a 31 39 30 30 0d 05 54 3a 75 72 64 :schemas -upnp-org
0006 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72 gidevice :Intern
0007 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72 6e 65 etGateway Device:
0008 74 47 61 74 65 77 61 79 44 65 76 69 63 65 3a 31 .:User's sdipdisc
0009 0d 04 4d 61 6a 22 73 73 64 78 3a 64 69 73 63 over". M X:3...
000a 6f 76 65 72 22 0d 0a 4d 58 3a 33 0d 0a 0d 0a

Packets: 765 · Displayed: 765 (100.0%) 4:43 PM 2/2/2023 Profile: Default

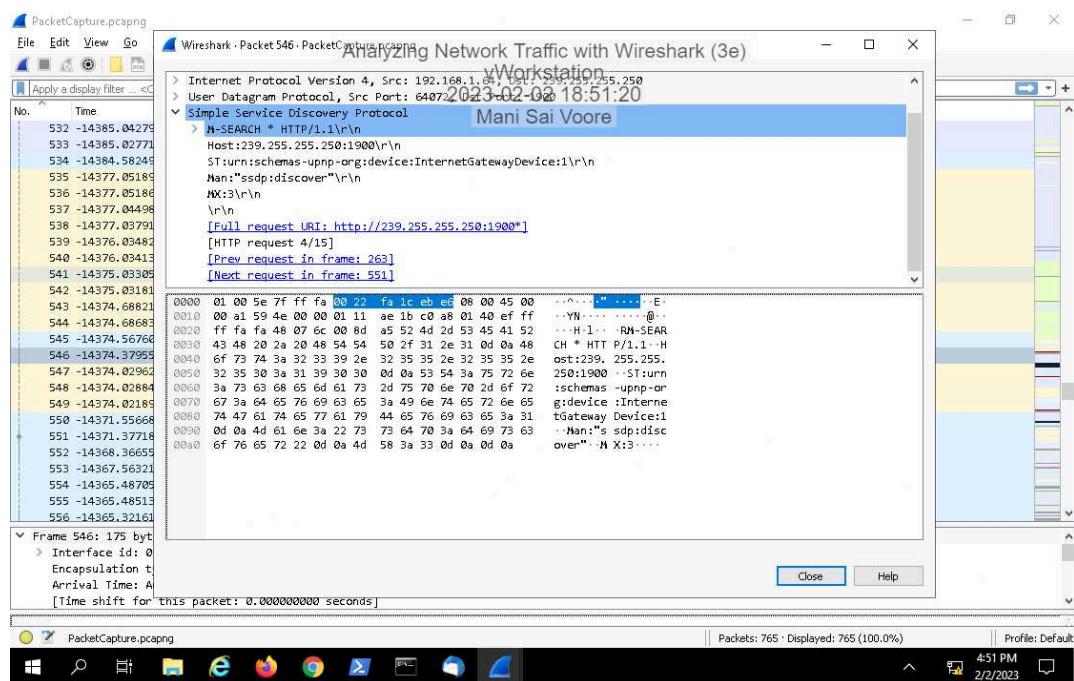
Analyzing Network Traffic with Wireshark (3e)

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

13. Record the source IP address in Packet 546.



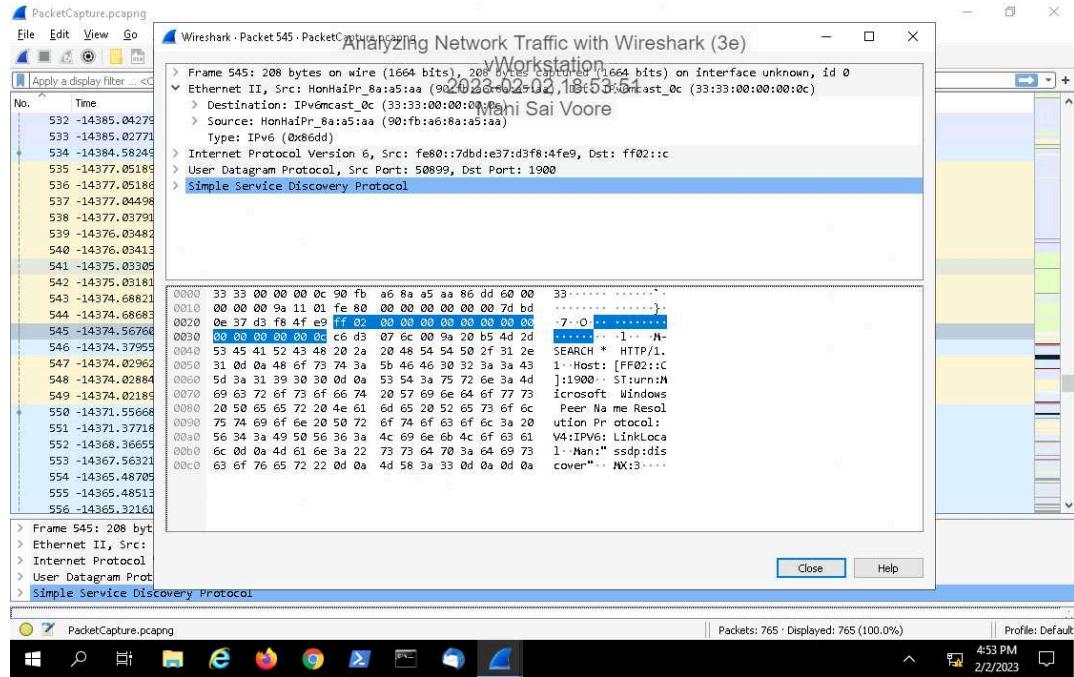
19. Make a screen capture showing the related frame numbers for Packet 546.



Analyzing Network Traffic with Wireshark (3e)

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

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



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

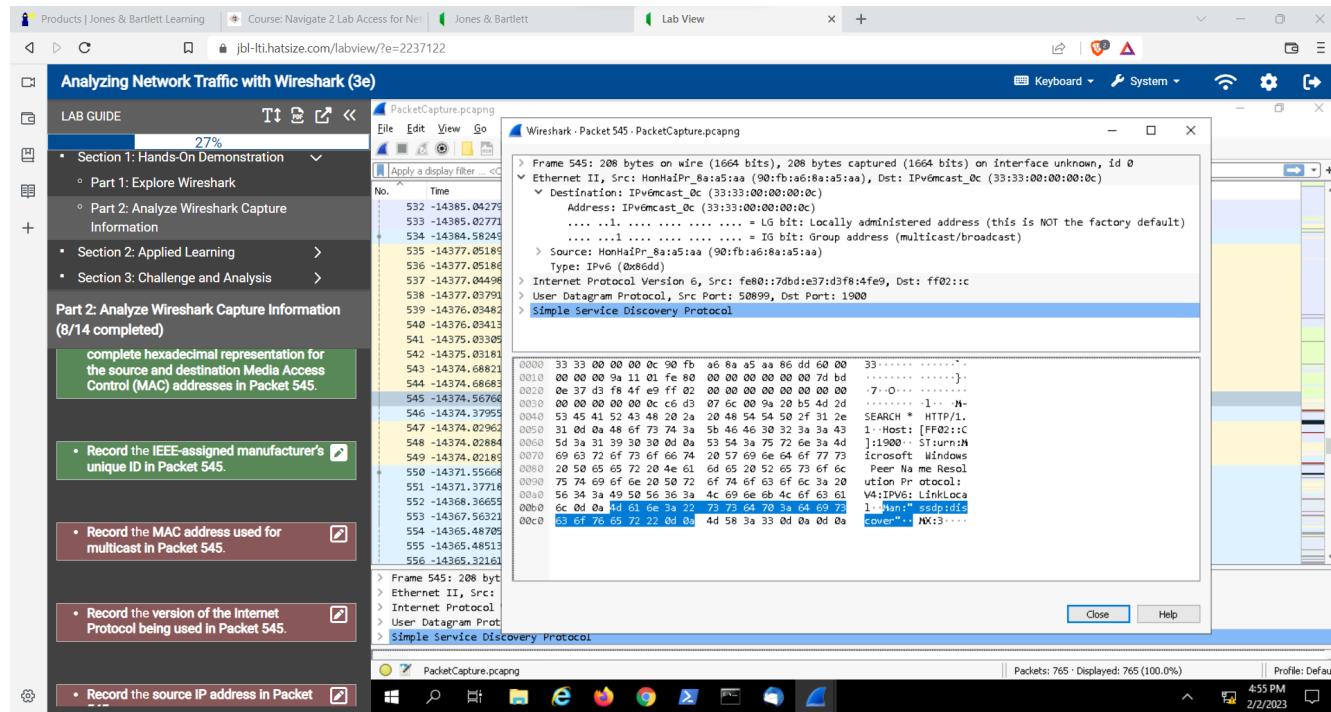
The screenshot shows the Lab View application window with the following components:

- Left Sidebar:** LAB GUIDE (24%)
 - Section 1: Hands-On Demonstration
 - Part 1: Explore Wireshark
 - Part 2: Analyze Wireshark Capture Information
 - Section 2: Applied Learning
 - Section 3: Challenge and Analysis
- Middle Area:** Analyzing Network Traffic with Wireshark (3e)
 - Packet 545 details pane (same as above)
 - Packet details pane showing the raw hex and ASCII data for the selected packet.
- Bottom Task List:**
 - Make a screen capture showing the complete hexadecimal representation for the source and destination Media Access Control (MAC) addresses in Packet 545.
 - Record the IEEE-assigned manufacturer's unique ID in Packet 545.
 - Record the MAC address used for multicast in Packet 545.
 - Record the version of the Internet Protocol being used in Packet 545.

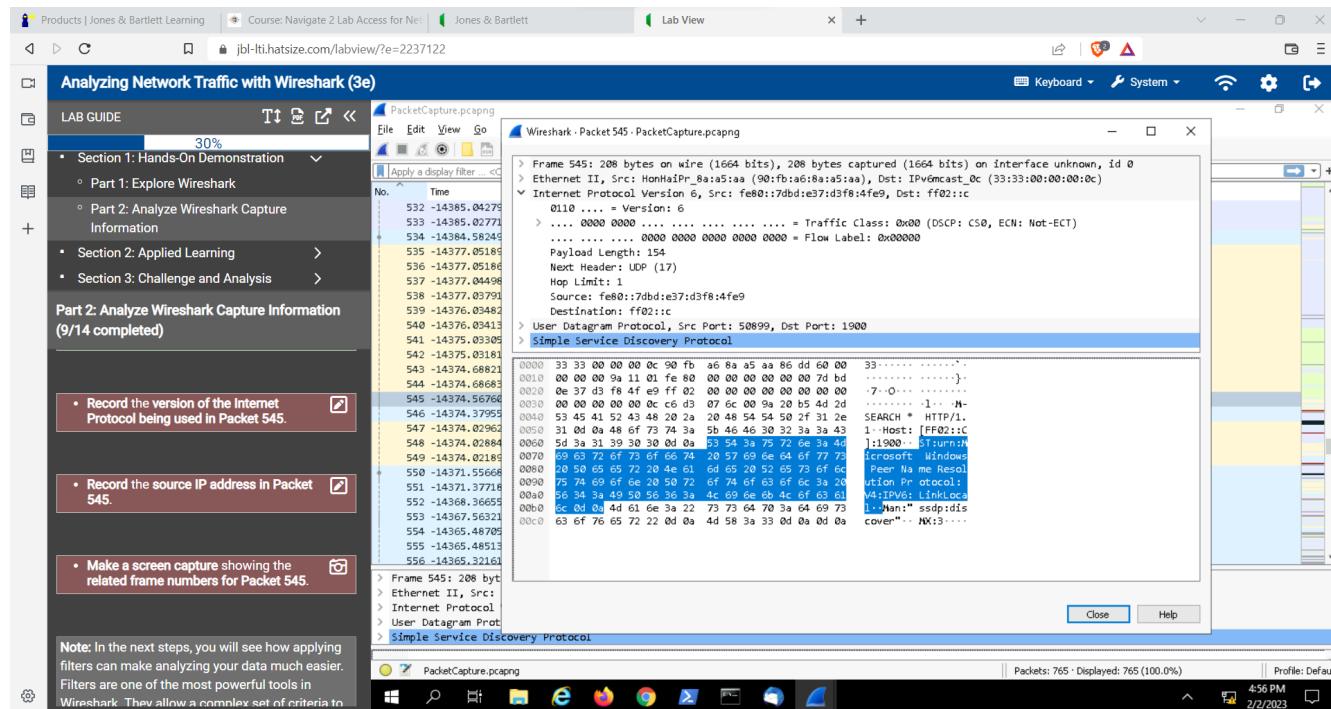
Analyzing Network Traffic with Wireshark (3e)

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

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



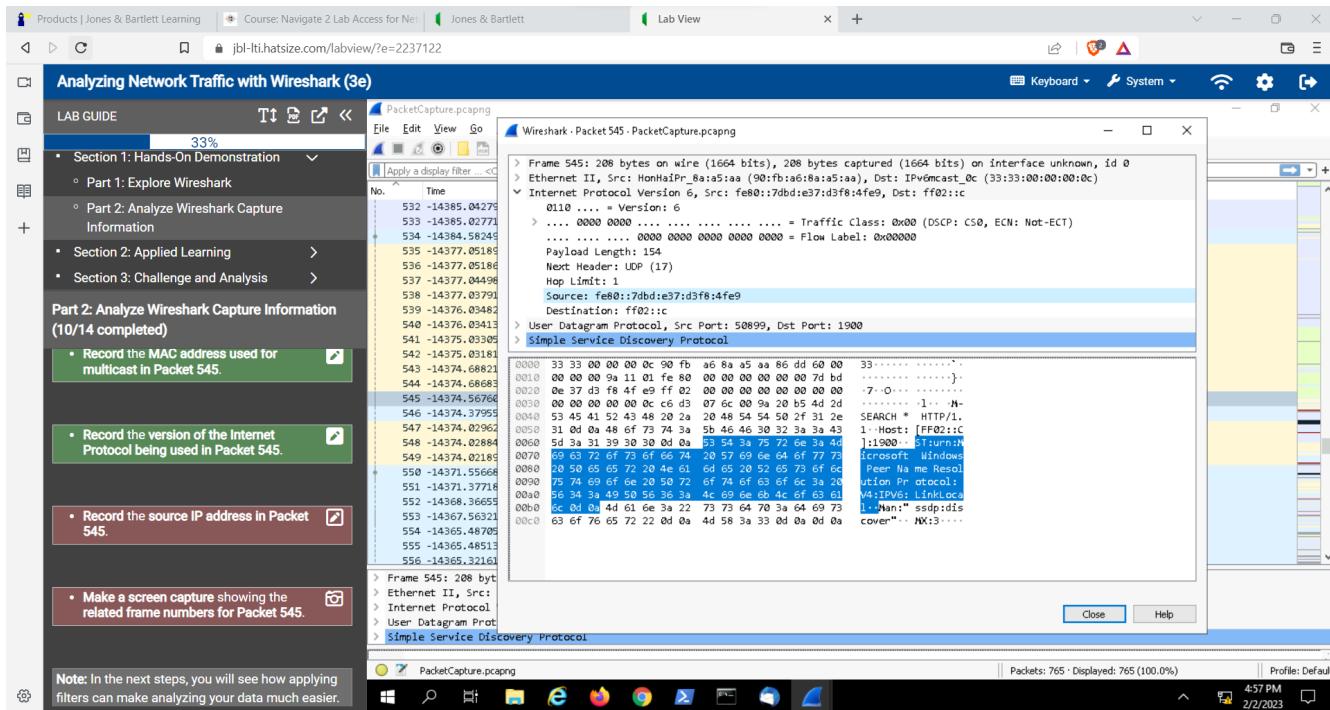
- Record the version of the Internet Protocol being used in Packet 545.



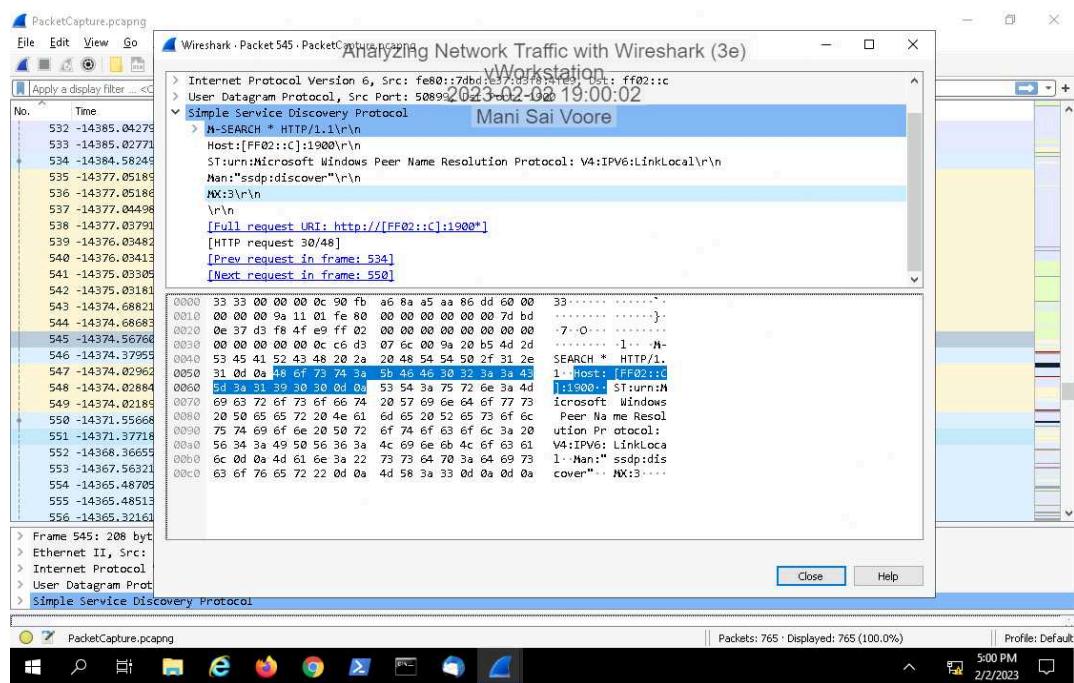
Analyzing Network Traffic with Wireshark (3e)

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

- Record the source IP address in Packet 545.



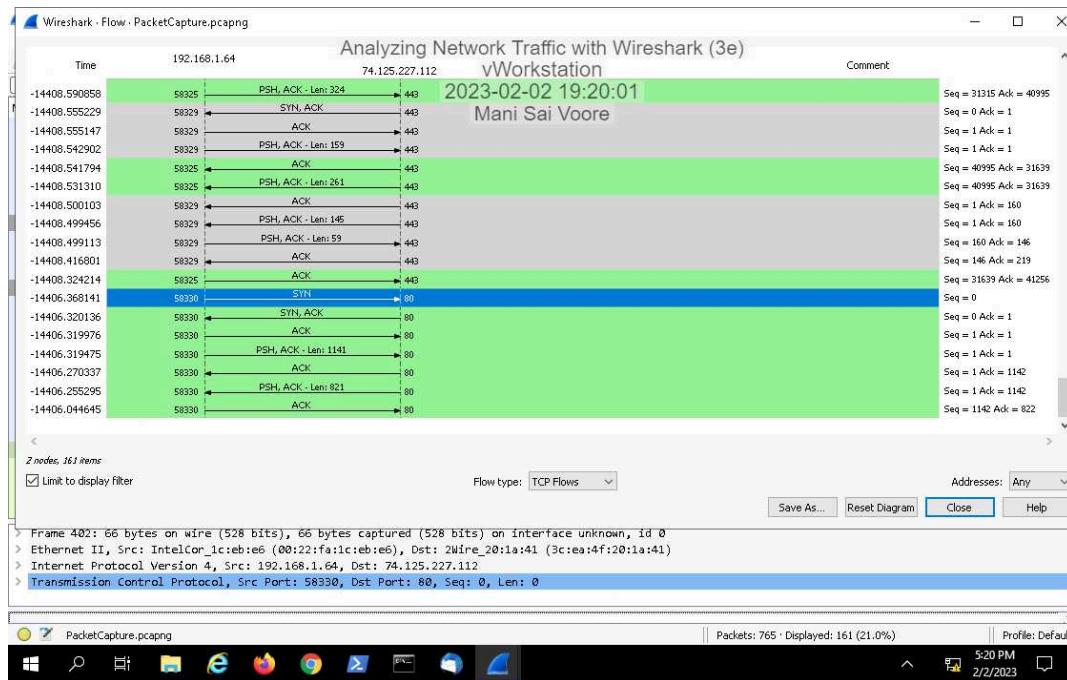
- Make a screen capture showing the related frame numbers for Packet 545.



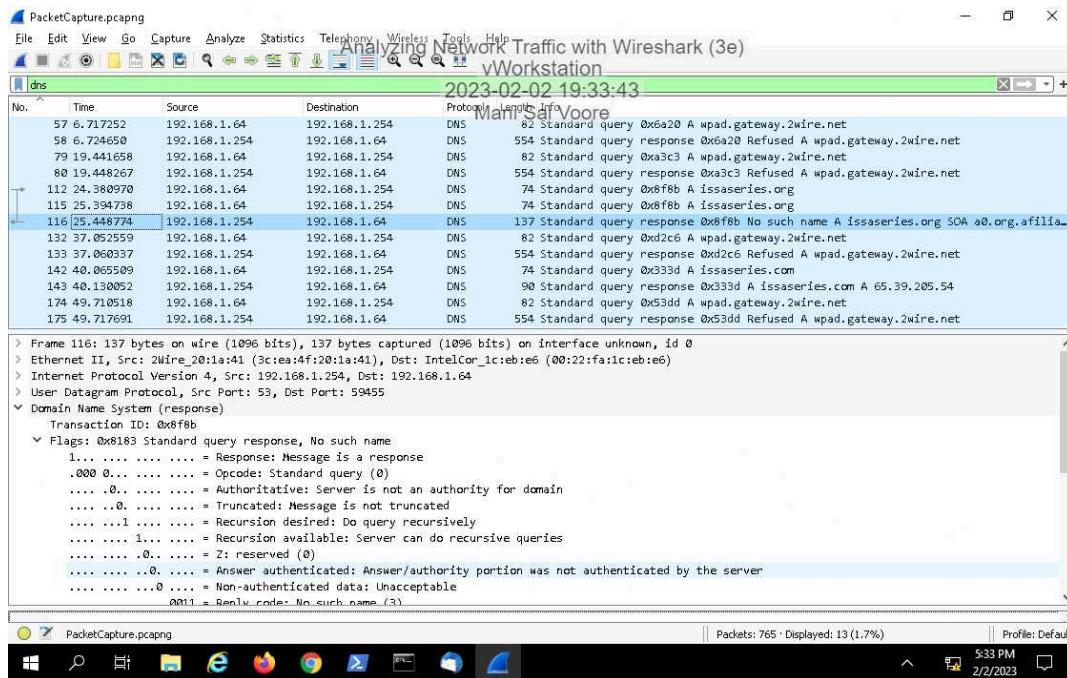
Analyzing Network Traffic with Wireshark (3e)

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

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



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



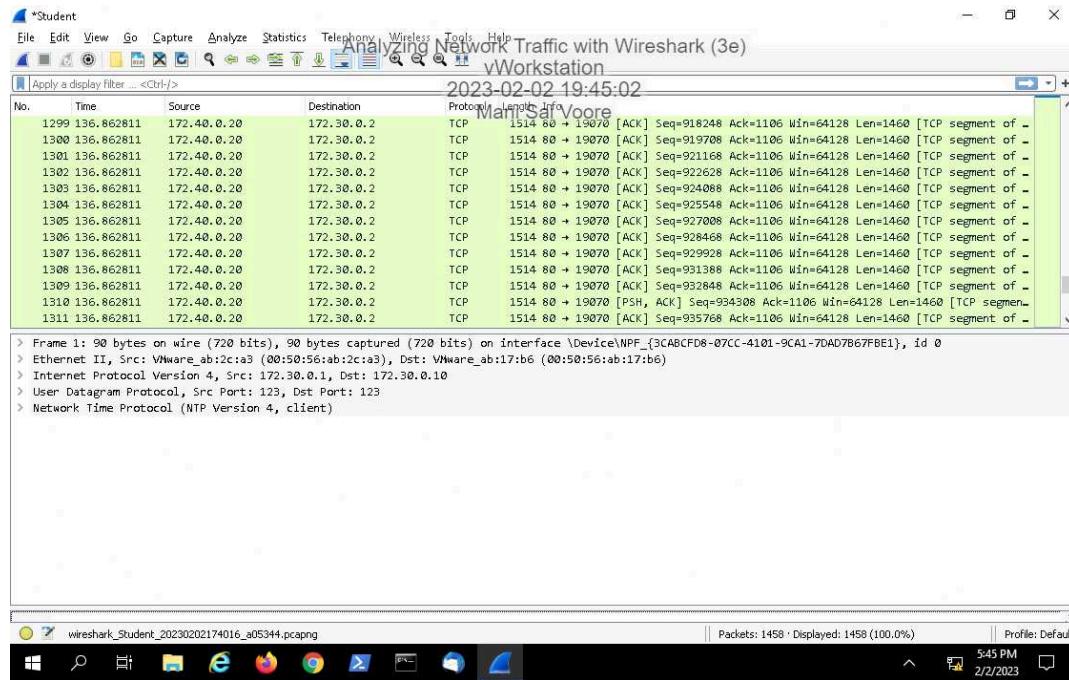
Analyzing Network Traffic with Wireshark (3e)

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

Section 2: Applied Learning

Part 1: Explore Wireshark

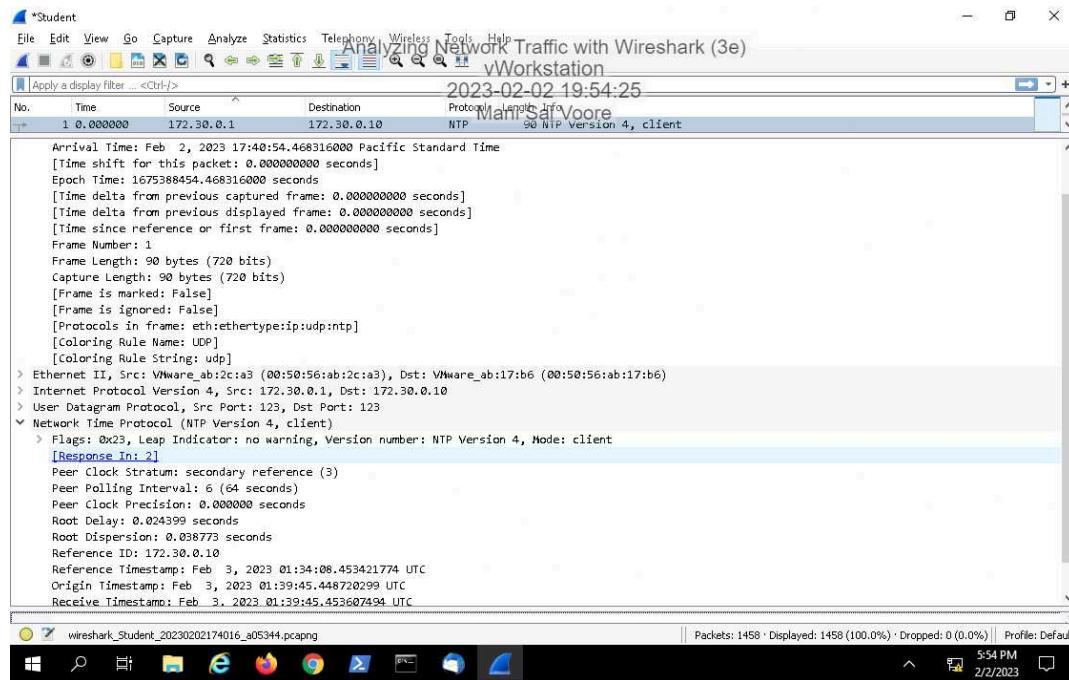
12. Make a screen capture showing the http traffic.



Analyzing Network Traffic with Wireshark (3e)

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

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



Part 2: Analyze Wireshark Capture Information

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

The screenshot shows a Microsoft Edge browser window displaying a lab guide for "Analyzing Network Traffic with Wireshark (3e)". The guide includes the following steps:

- In the packet list pane, select packet 8.
- In the packet details pane, select the frame header to display the number of bytes captured and the bytes on the wire.
- Record the number of bytes captured and the bytes on the wire.
- In the packet details pane, expand the Ethernet II line to display the Data Link Layer detail.

The browser address bar shows the URL: jbl-lti.hatsize.com/labview/?e=2237122. The status bar at the bottom indicates 1416 packets displayed.

Analyzing Network Traffic with Wireshark (3e)

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

7. Record the manufacturer of the destination device.

LAB GUIDE 54%

Section 2: Applied Learning

- Part 1: Explore Wireshark
- Part 2: Analyze Wireshark Capture Information

Part 2: Analyze Wireshark Capture Information (1/9 completed)

- The source is Intel Core hardware.
- The destination is AsustekC.
- The type of traffic carried in the next layer is Internet Protocol (IP).

Note: The MAC address for the source device is 70:1:c:e7:db:d3:28. To the left of the full MAC address, Wireshark shows IntelCor_db:d3:28. It means that Wireshark has interpreted 70:1:c:e7 as the IEEE-assigned manufacturer's unique ID.

7. Record the manufacturer of the destination device.

8. In the packet details pane, collapse the Ethernet II line to hide the Data Link Layer detail.

Wireshark 602 PM 2/2/2023

10. Record the source IP address.

LAB GUIDE 57%

Section 2: Applied Learning

- Part 1: Explore Wireshark
- Part 2: Analyze Wireshark Capture Information

Part 2: Analyze Wireshark Capture Information (2/9 completed)

destination device.

8. In the packet details pane, collapse the Ethernet II line to hide the Data Link Layer detail.

9. In the packet details pane, expand the Internet Protocol line to display the Internet Protocol detail.

10. Record the source IP address.

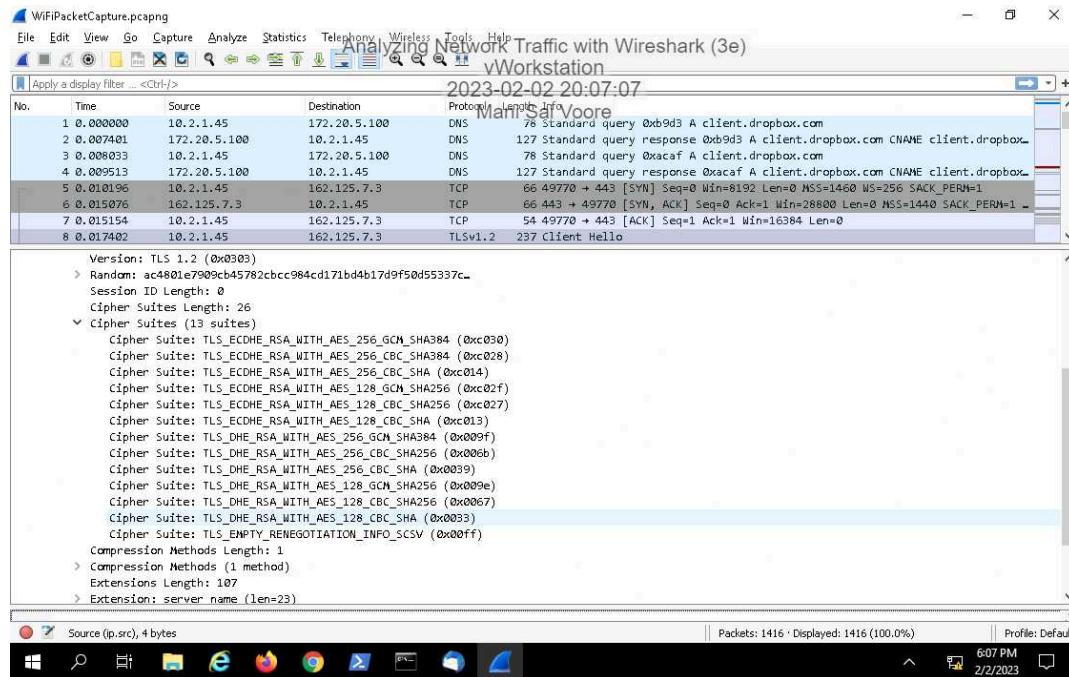
11. In the packet details pane, collapse the Internet Protocol line to hide the Network Layer detail.

Wireshark 604 PM 2/2/2023

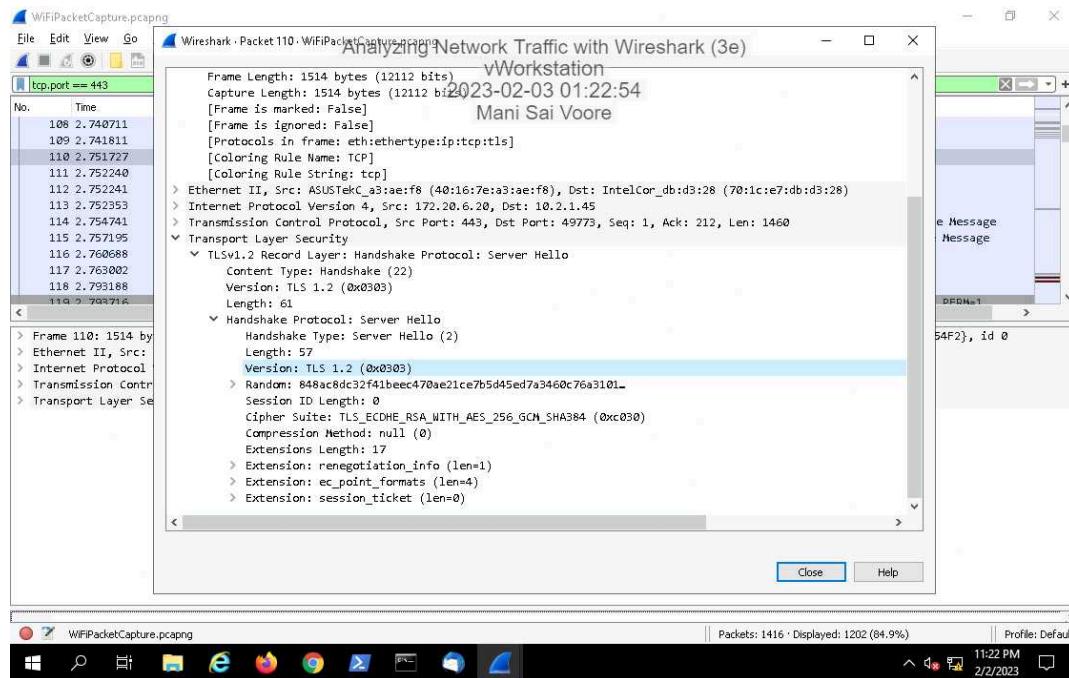
Analyzing Network Traffic with Wireshark (3e)

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

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



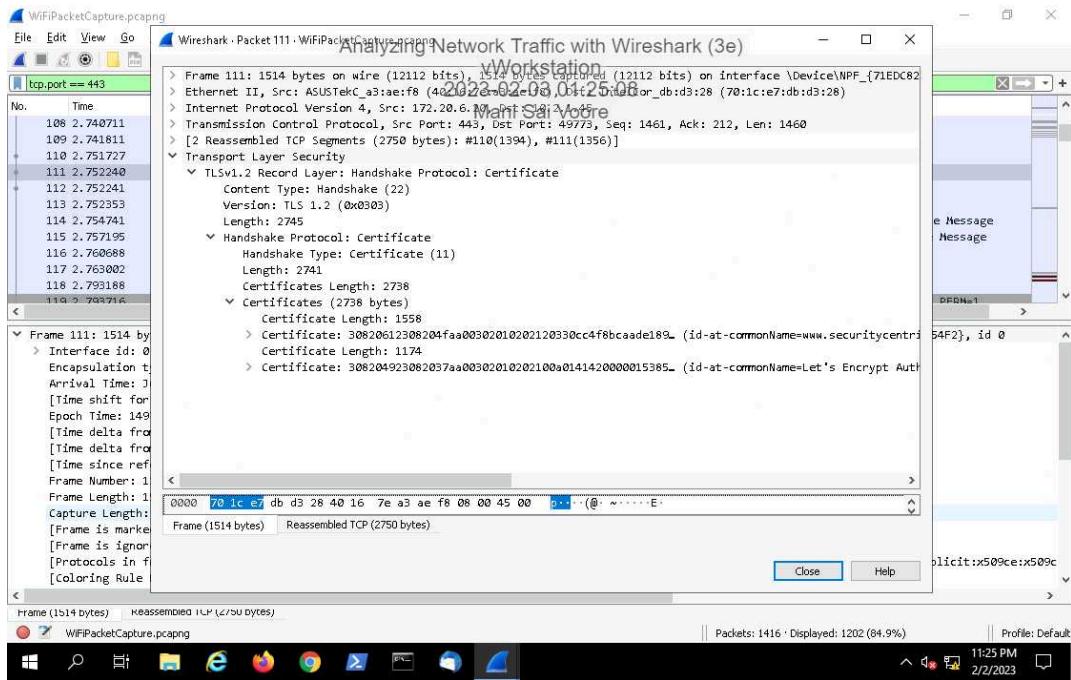
21. Make a screen capture showing the issuer of the certificate.



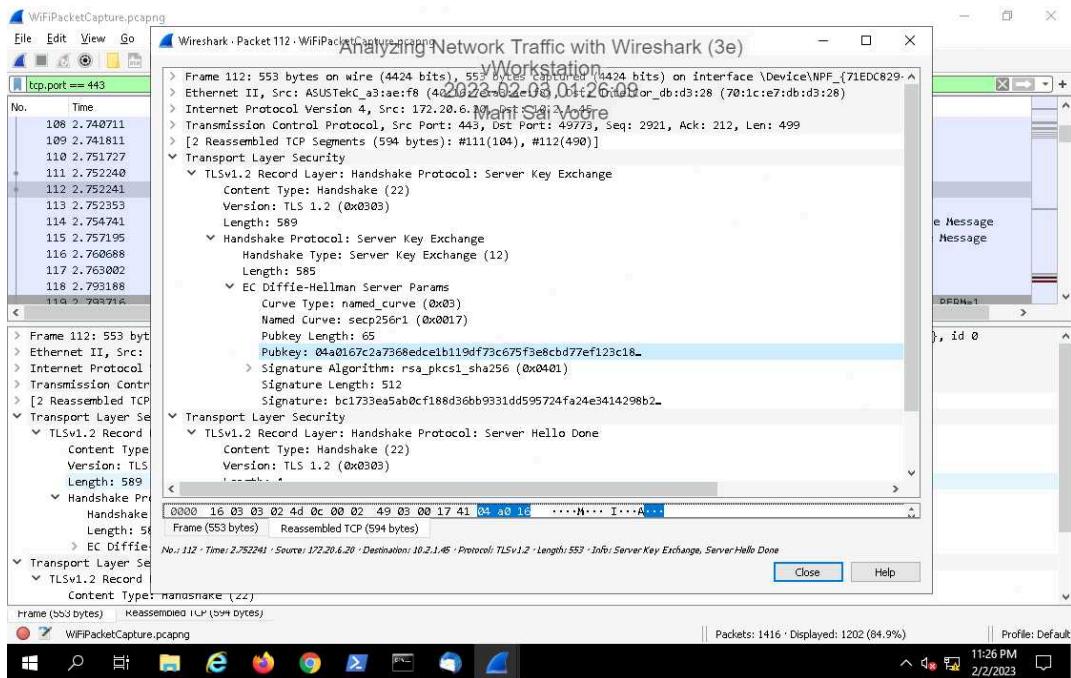
Analyzing Network Traffic with Wireshark (3e)

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

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



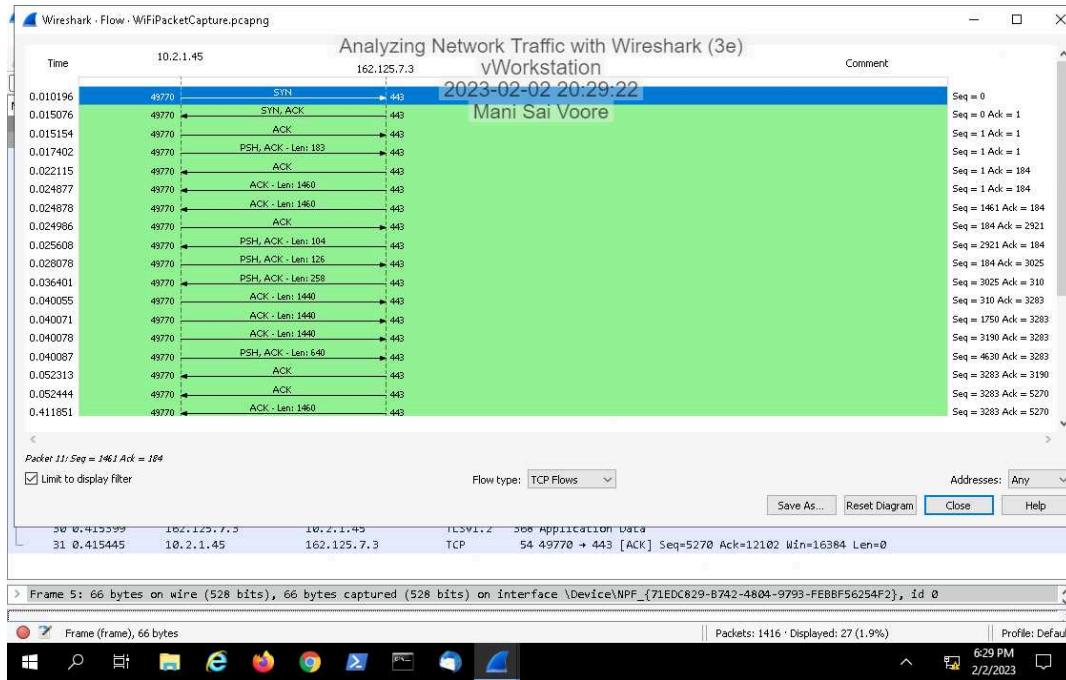
27. Make a screen capture showing the public key and signature hash for the certificate.



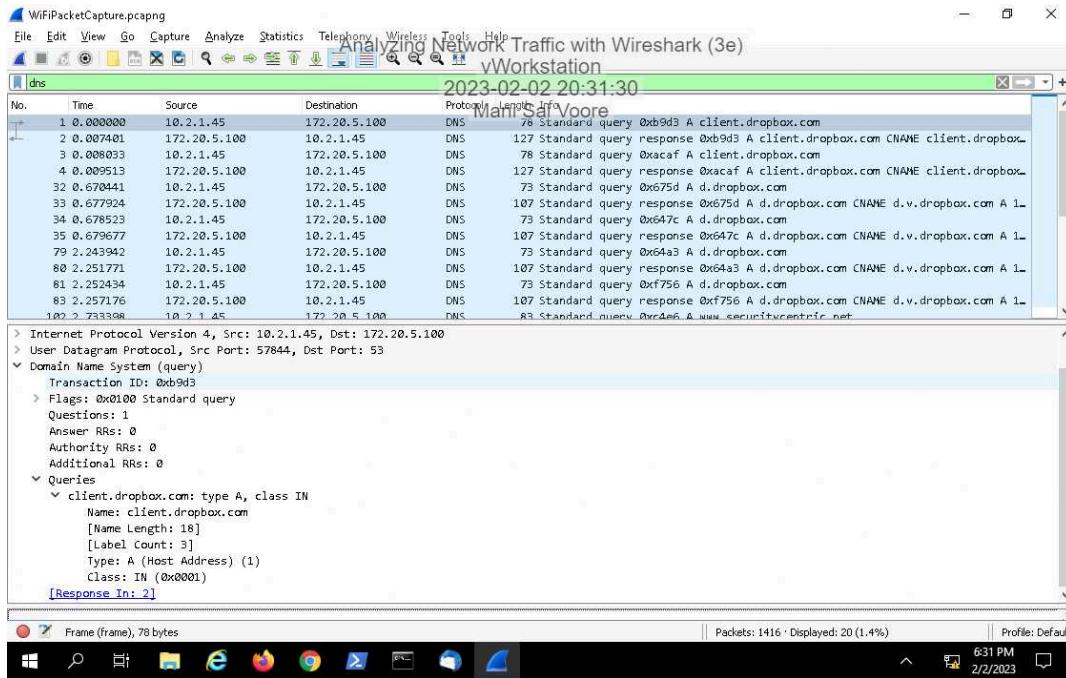
Analyzing Network Traffic with Wireshark (3e)

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

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



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



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.).

1. HTTP: It is called as Hyper Text Transfer Protocol. the port number is 80-TCP.

Purpose: Is to transfer the data for web pages and other resources on the WWW over the internet.

Features: It follows client-server model, support methods like GET and POST.

2. HTTPS: It is called as Hyper Text Transfer Protocol Secure. the port number is 443-TCP.

Purpose: which secure the data transmission layer using SSL/TLS encryption.

Features: It ensure the integrity, authenticity of data also protect from tampering.

3. DNS: It is called as Domain Name Server. the port number is 53-UDP.

Purpose: convert domain name to IP address.

Features: support multiple file transfer of both active and passive modes.

4. DHCP: it is called as Dynamic Host Configuration Protocol. the port number is 67-UDP.

Purpose: dynamically assign IP address to network devices.

Features: supports multiple OS, Automatic Configurations.

5. SMTP and FTP: It is called as Simple Mail or File Transfer Protocol. The port number is 25,20,21-TCP. 25 port number is for SMTP and remaining 2 are FTP.

Purpose: SMTP- send and receive a email message over internet.

FTP- transfer the file among computers.

Features: supports message queueing and multiple recipients(SMTP).

supports multiple transfer of both active and passive modes(FTP).

6.SNMP: It is called as Simple Network Management Protocol. The port number is 161.

Purpose: Manages the routers, switches, servers.

Features: uses and support multiple version and layering like tree.

Analyzing Network Traffic with Wireshark (3e)

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

Part 2: Capture and Filter Traffic Using Wireshark

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

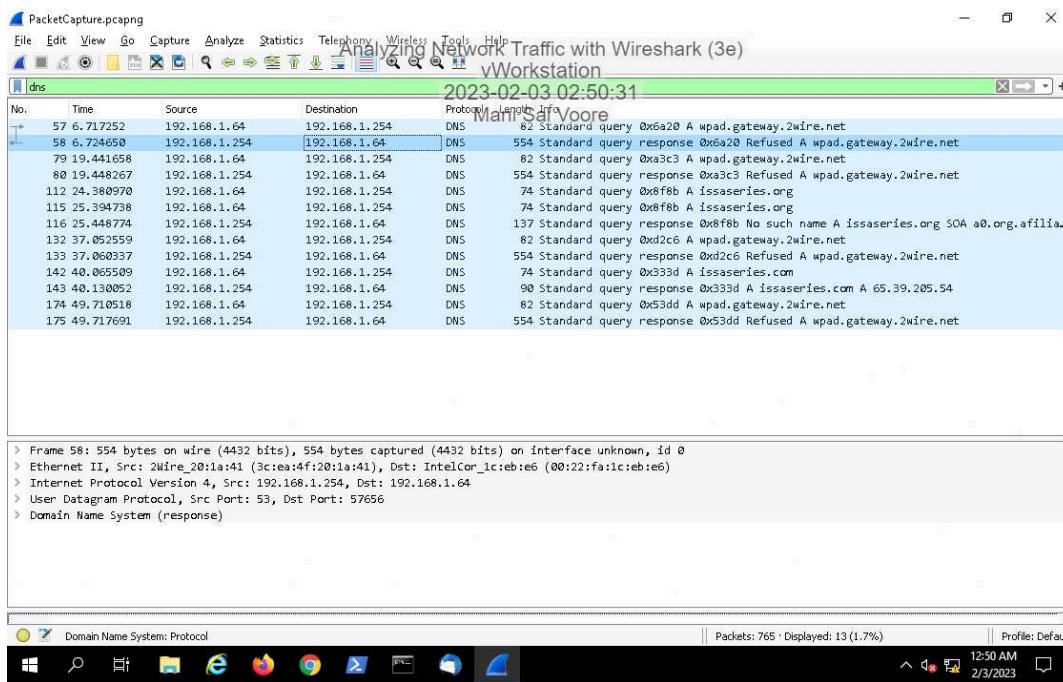
```
C:\Users\Administrator>ping 172.30.0.2
Pinging 172.30.0.2 with 32 bytes of data:
Reply from 172.30.0.2: bytes=32 time<ms TTL=128
Reply from 172.30.0.2: bytes=32 time<ms TTL=128
Reply from 172.30.0.2: bytes=32 time<ms TTL=128
N...Reply from 172.30.0.2: bytes=32 time<ms TTL=128

Ping statistics for 172.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>arp -a
Interface: 172.30.0.2 --- 0x6
  Internet Address      Physical Address      Type
  172.30.0.1          00-50-56-ab-2a-20  dynamic
  172.30.0.10         00-50-56-ab-71-9e  dynamic
  172.30.0.255        ff-ff-ff-ff-ff-ff  static
  24.0.0.22           01-00-5e-00-00-16  static
  24.0.0.251          01-00-5e-00-00-fb  static
  24.0.0.252          01-00-5e-00-00-fc  static
  255.255.255.255   ff-ff-ff-ff-ff-ff  static

Interface: 192.168.0.3 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1          00-50-56-ab-ad-43  dynamic
  192.168.0.254        00-50-56-ab-8b-4b  dynamic
  24.0.0.22           01-00-5e-00-00-16  static
  24.0.0.251          01-00-5e-00-00-fb  static
  24.0.0.252          01-00-5e-00-00-fc  static
  Winsch              Spunk Enterprise
```

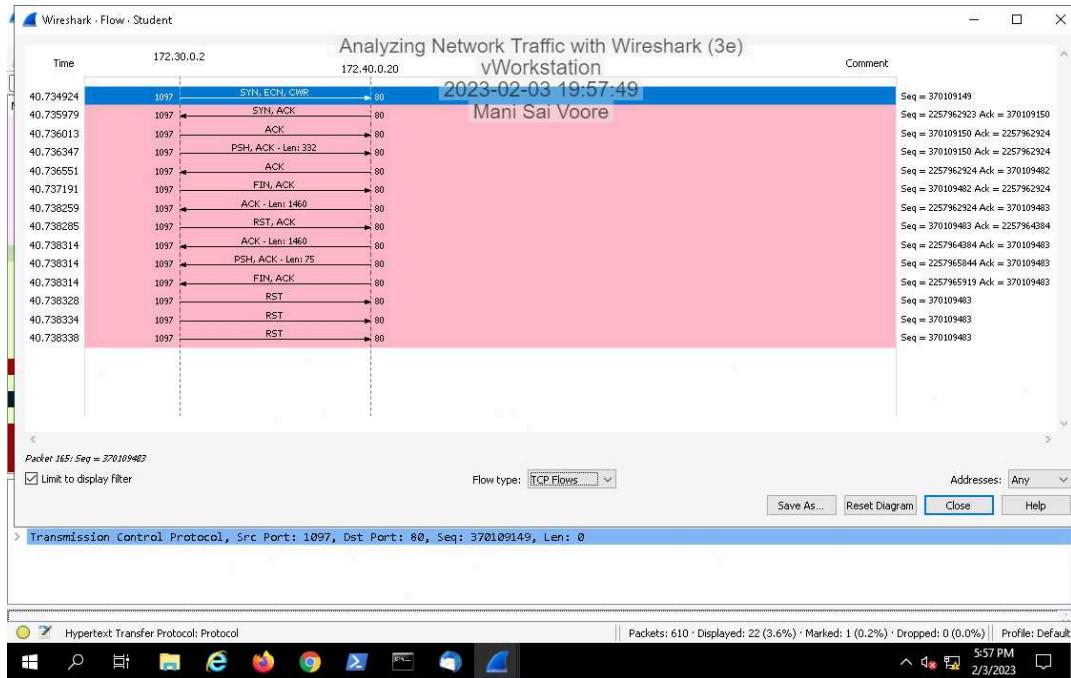
Make a screen capture showing the destination IP address and port number of the DNS server.



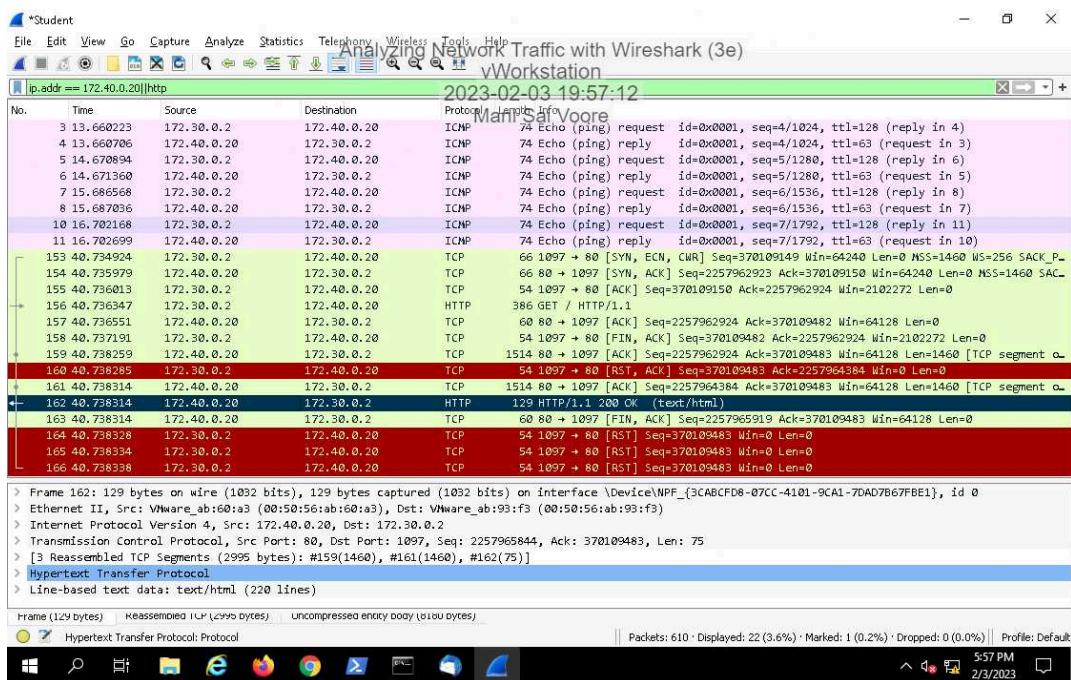
Analyzing Network Traffic with Wireshark (3e)

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

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



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

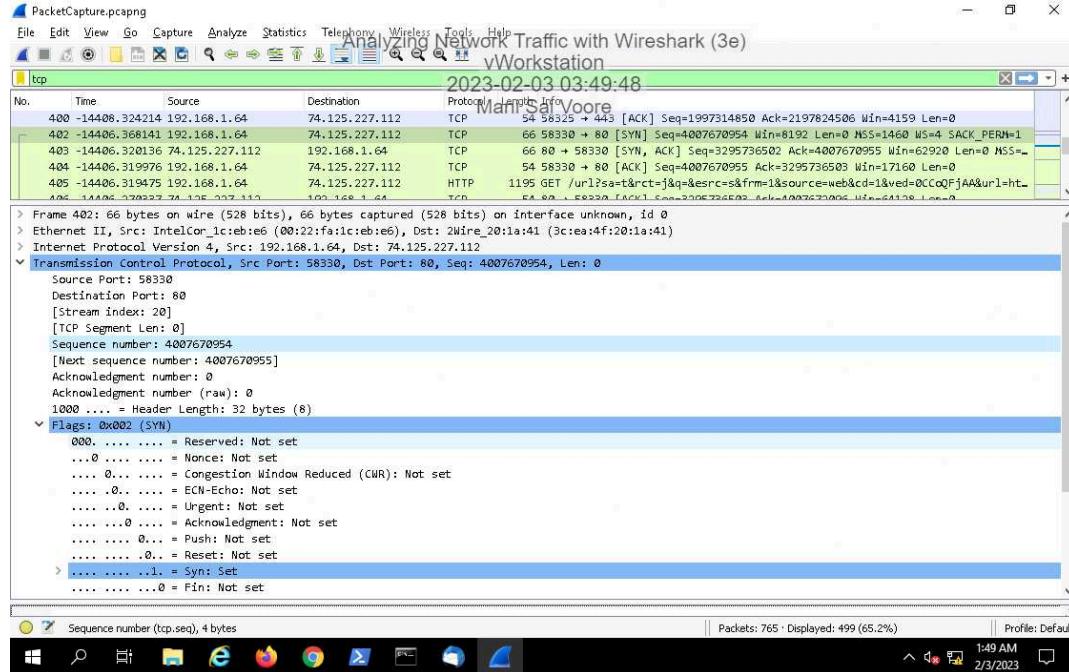


Analyzing Network Traffic with Wireshark (3e)

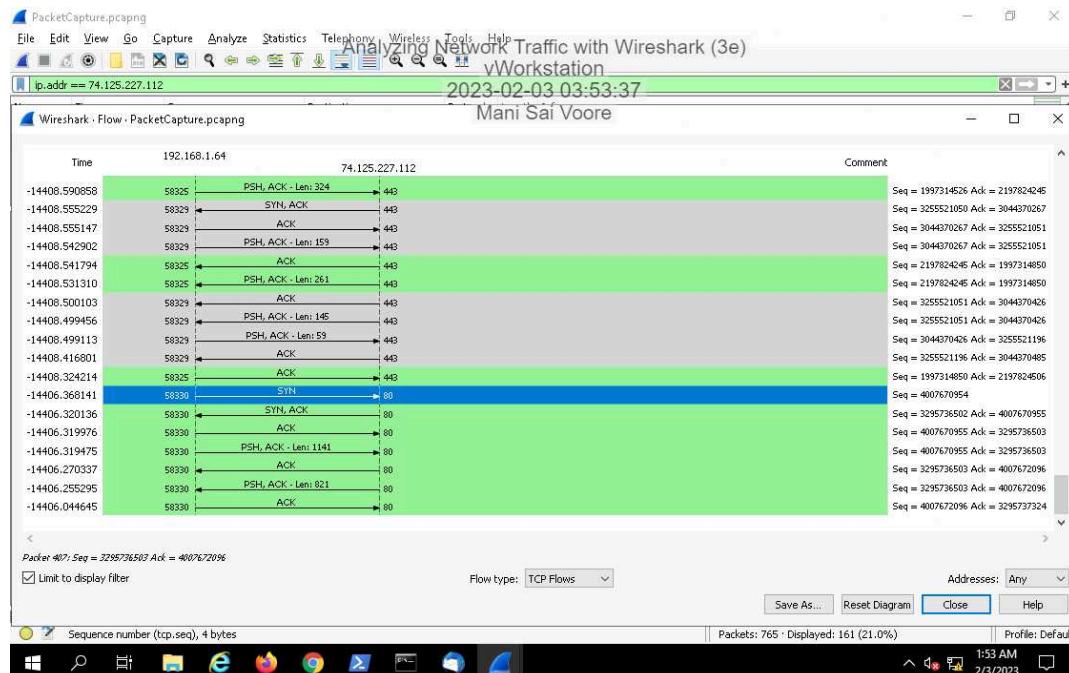
Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 01

Part 3: Analyze Capture Files

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



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)

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