Student:	Email:
Mani Sai Voore	mvoore@cbu.edu

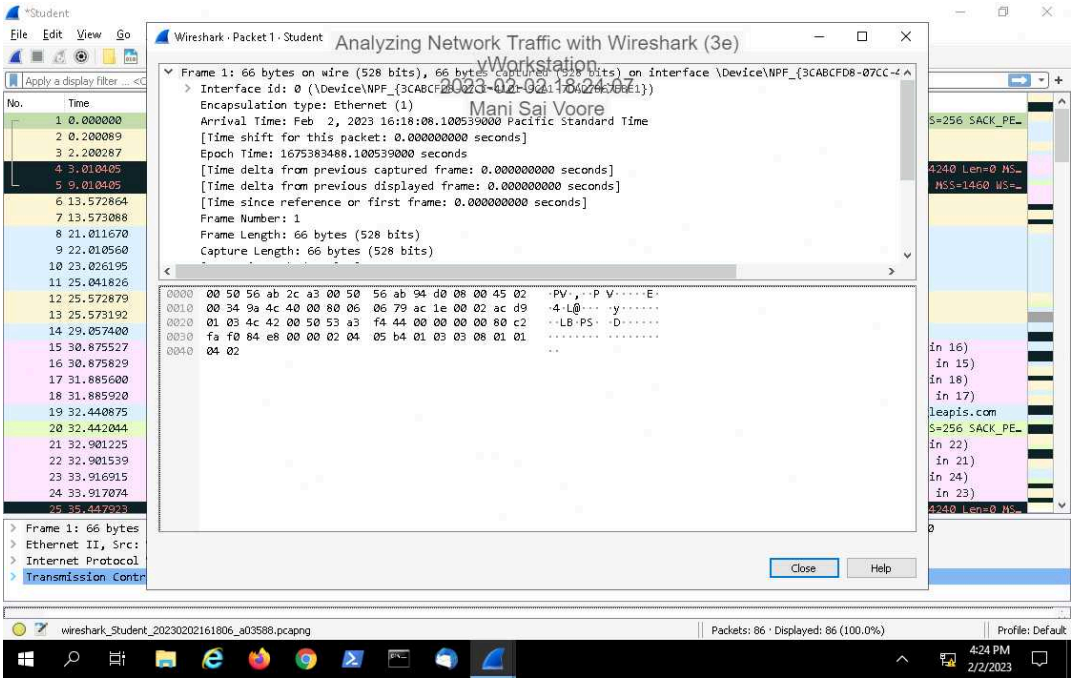
Time on Task:	Progress:
22 hours, 34 minutes	100%

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

Section 1: Hands-On Demonstration

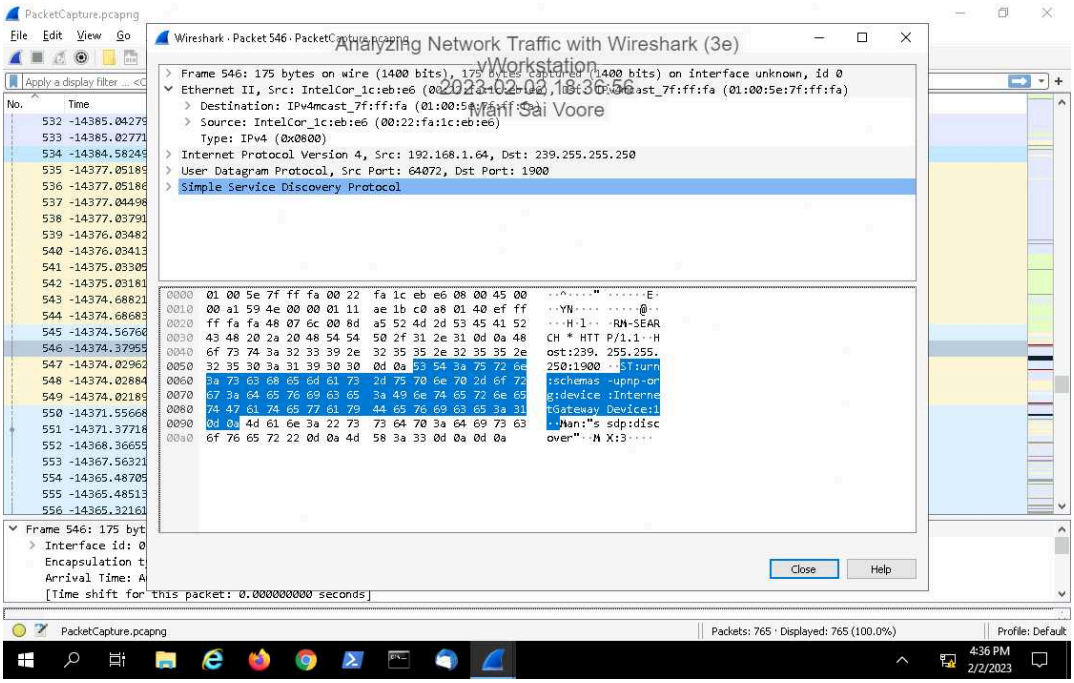
Part 1: Explore Wireshark

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

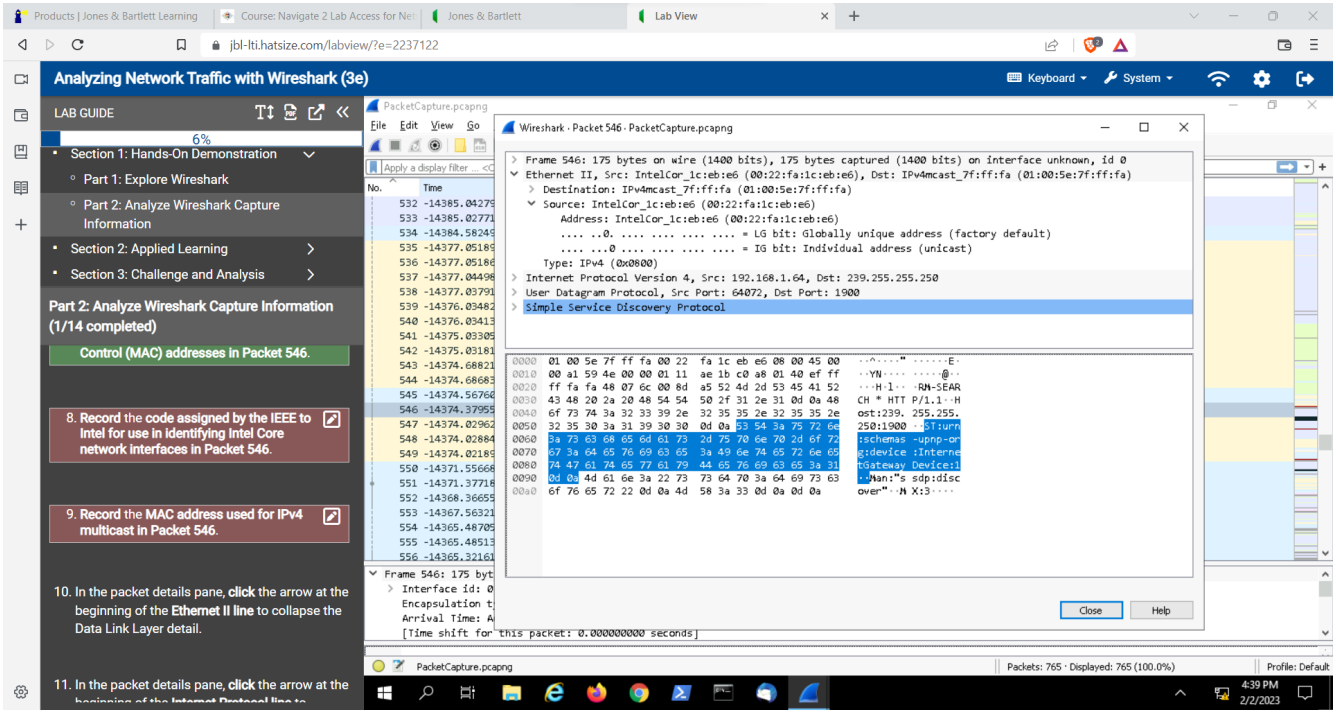


Part 2: Analyze Wireshark Capture Information

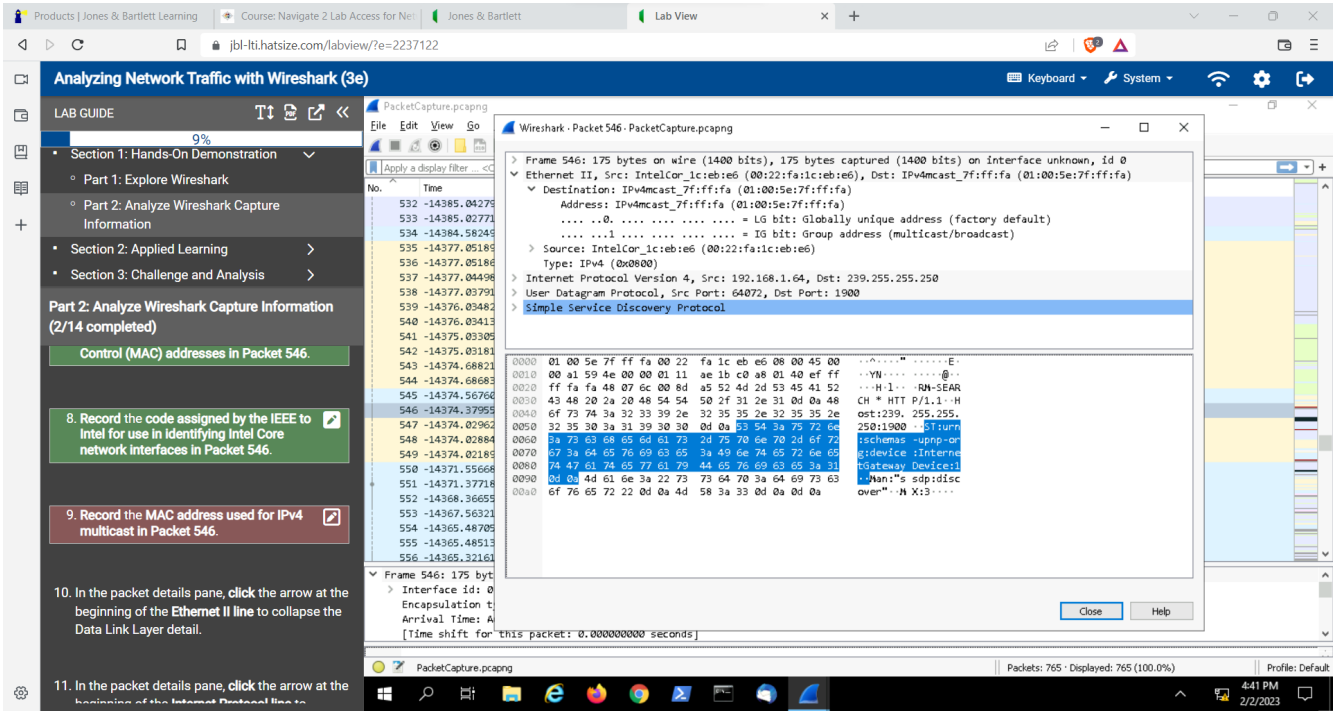
7. **Make a screen capture** showing the **complete hexadecimal representation for the source and destination Media Access Control (MAC) addresses in Packet 546**.



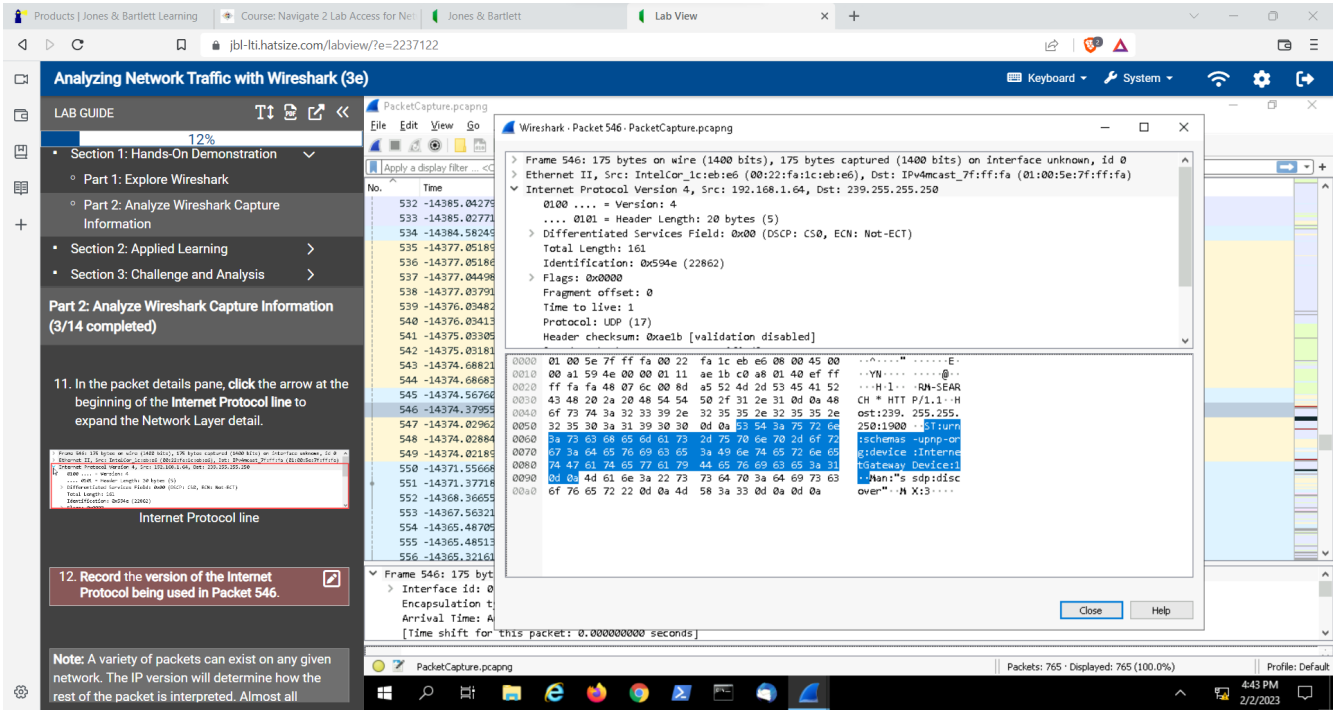
8. **Record** the **code assigned by the IEEE to Intel for use in identifying Intel Core network interfaces in Packet 546**.



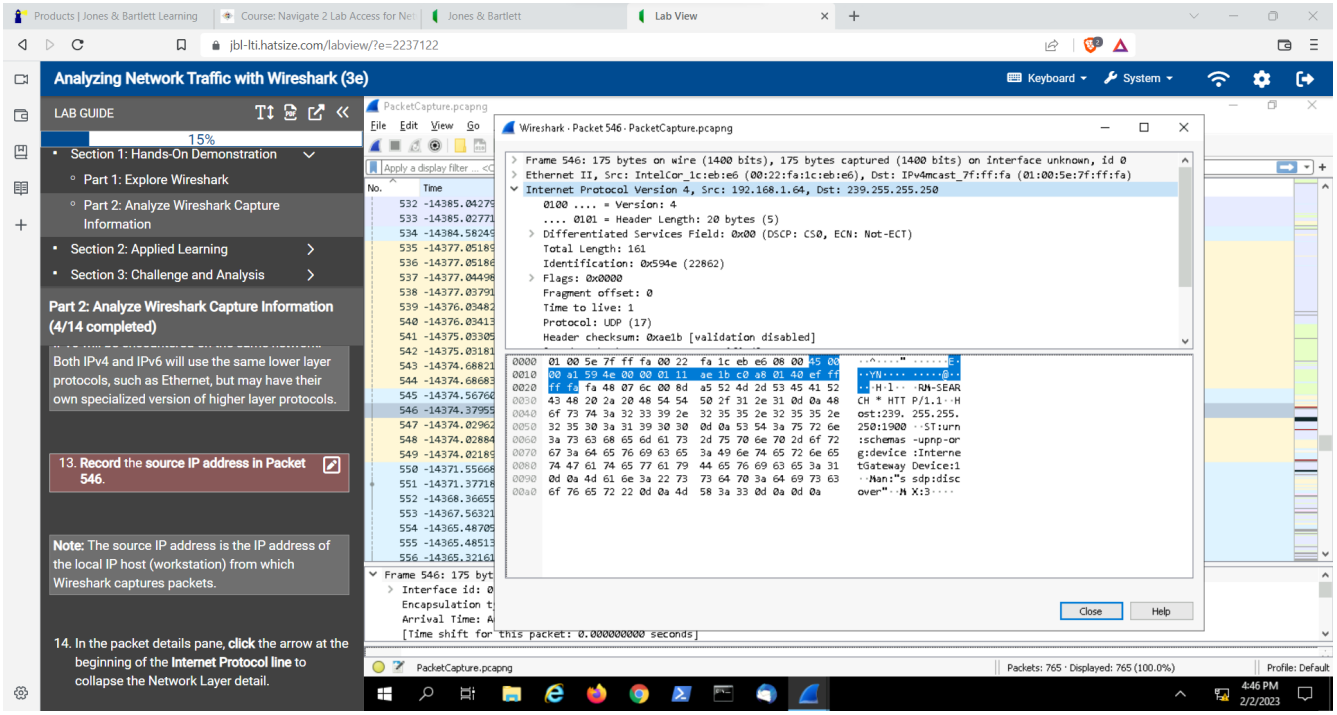
9. **Record** the **MAC address used for IPv4 multicast in Packet 546**.



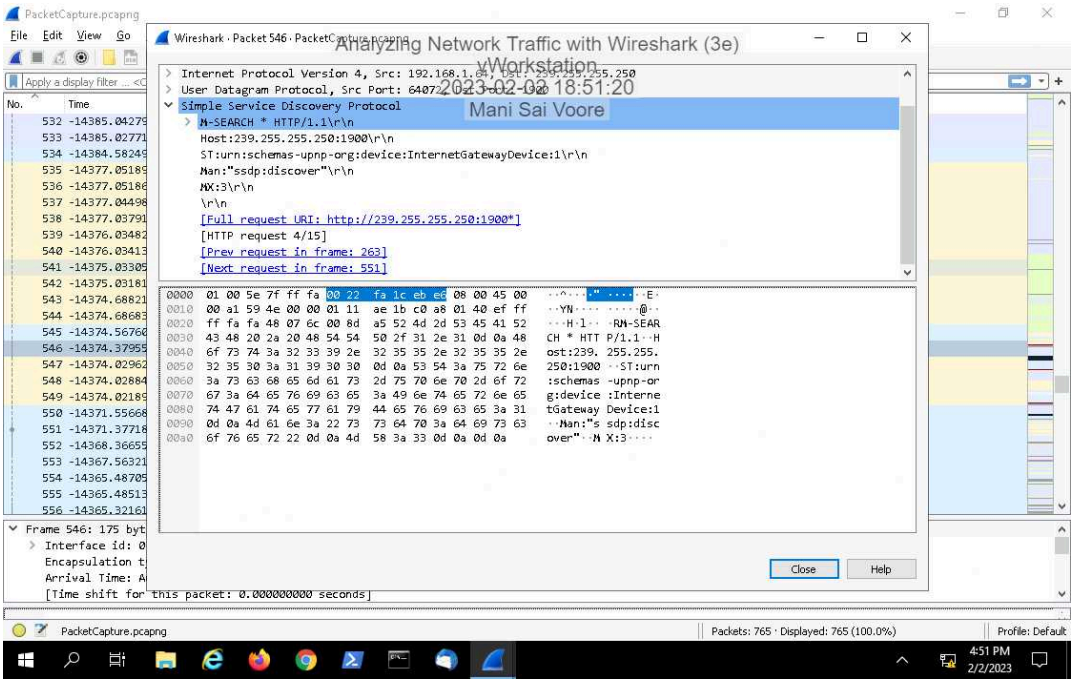
12. **Record** the **version of the Internet Protocol being used in Packet 546**.



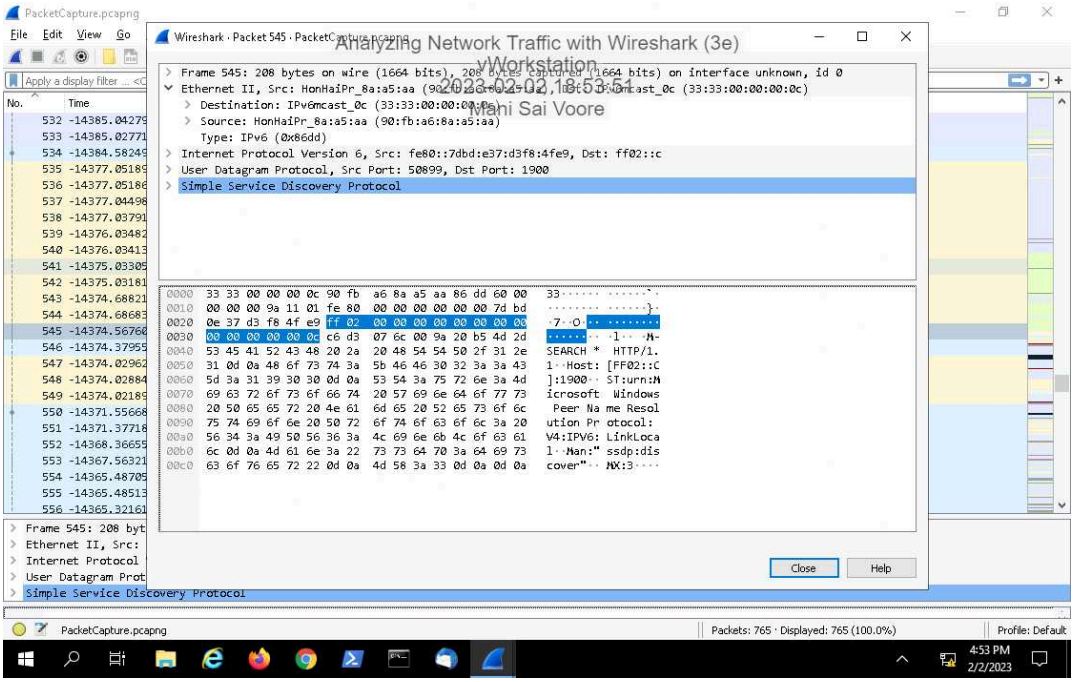
13. **Record** the **source IP address in Packet 546**.



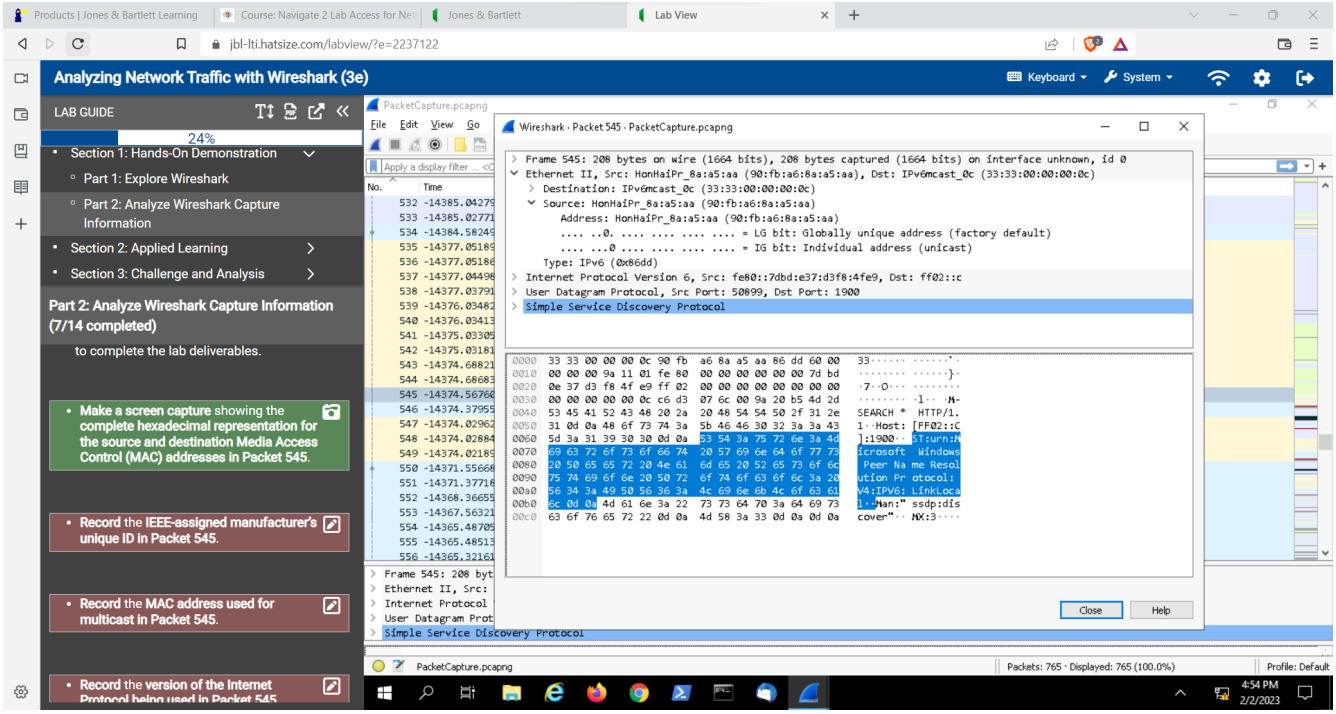
19. **Make a screen capture** showing the **related frame numbers for Packet 546**.



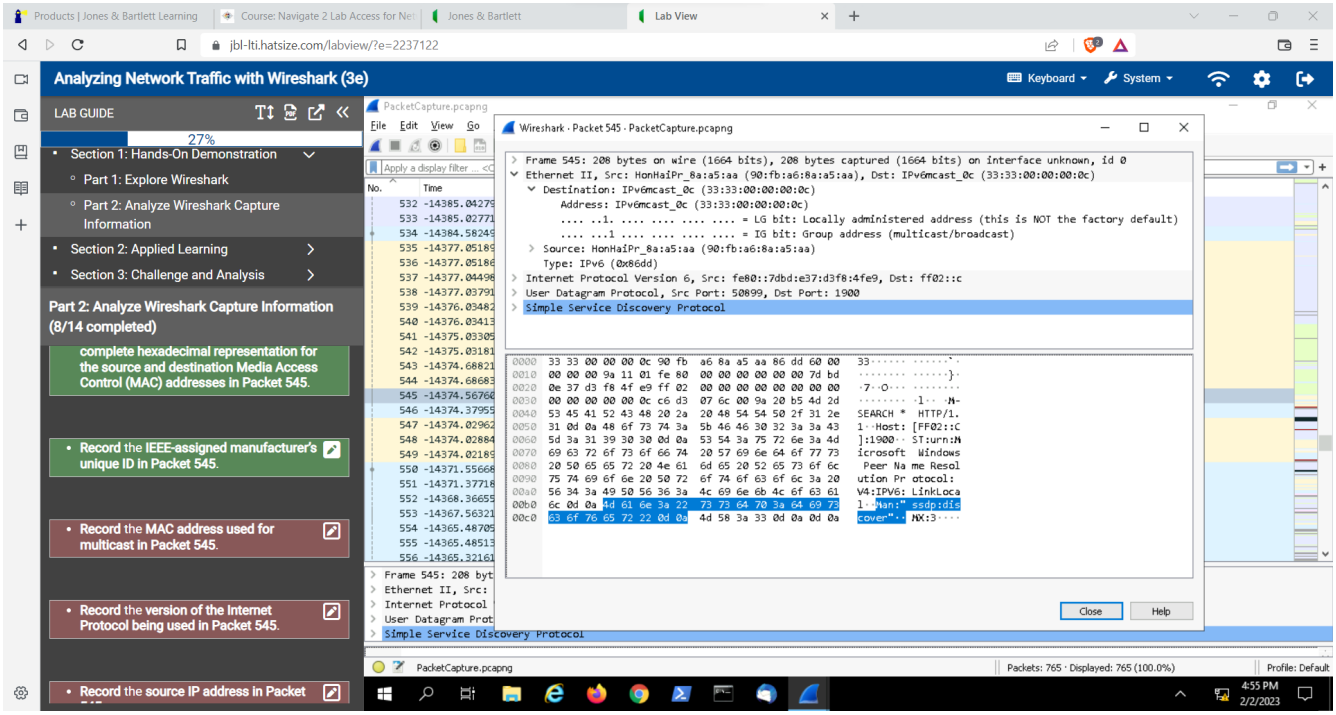
- **Make a screen capture** showing the **complete hexadecimal representation for the source and destination Media Access Control (MAC) addresses in Packet 545**.



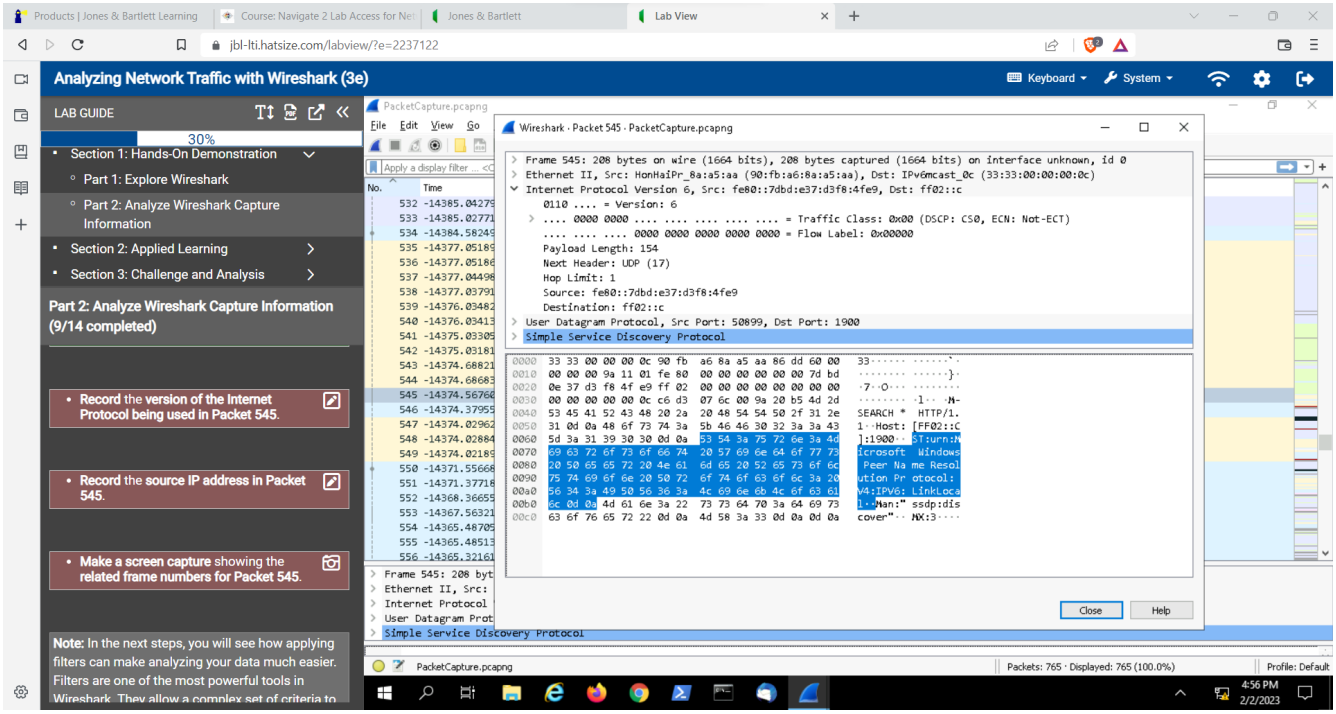
- **Record** the **IEEE-assigned manufacturer's unique ID in Packet 545**.



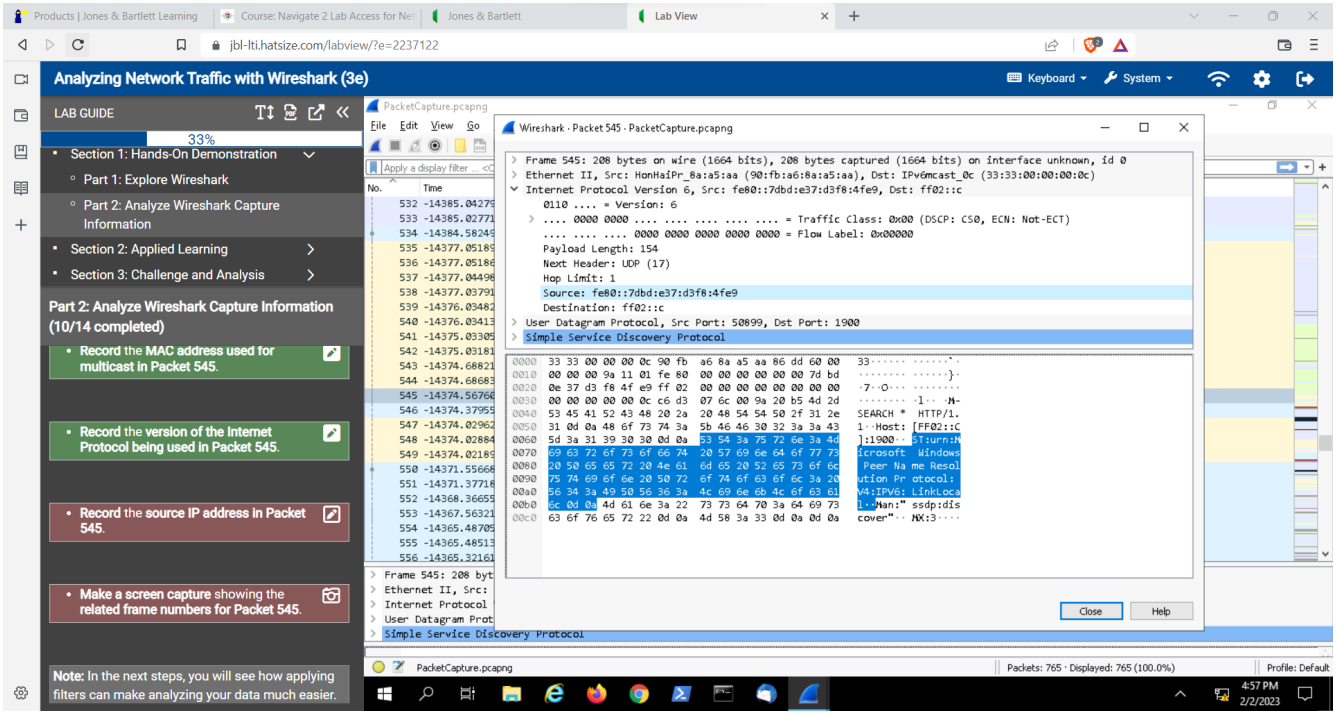
- **Record** the **MAC address used for multicast in Packet 545**.



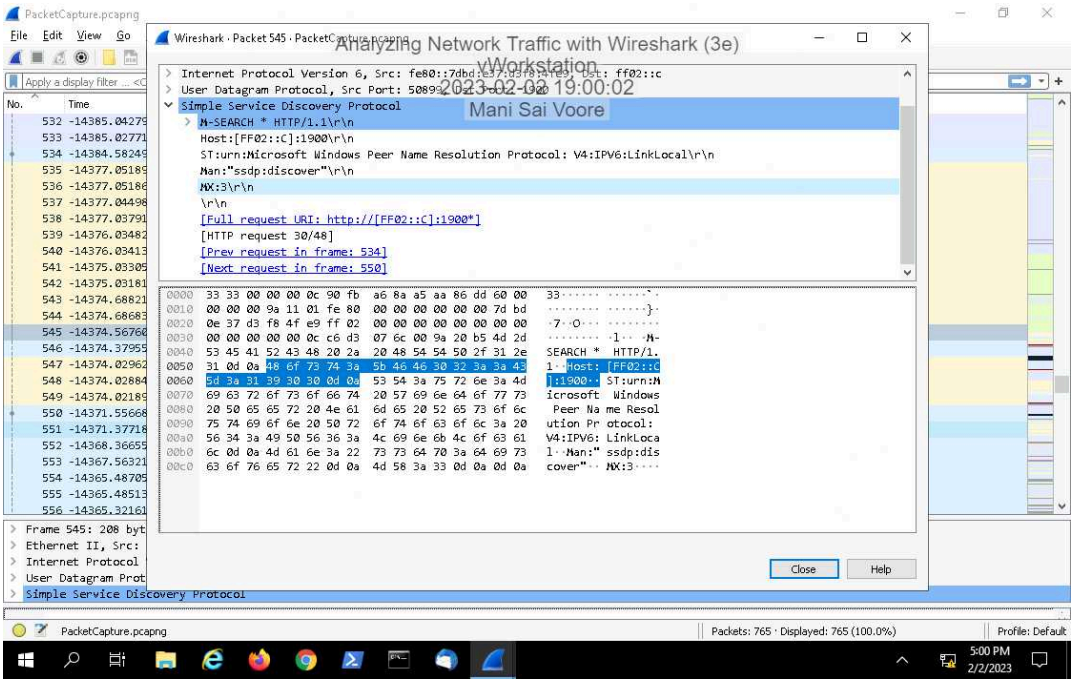
- **Record** the **version of the Internet Protocol being used in Packet 545**.



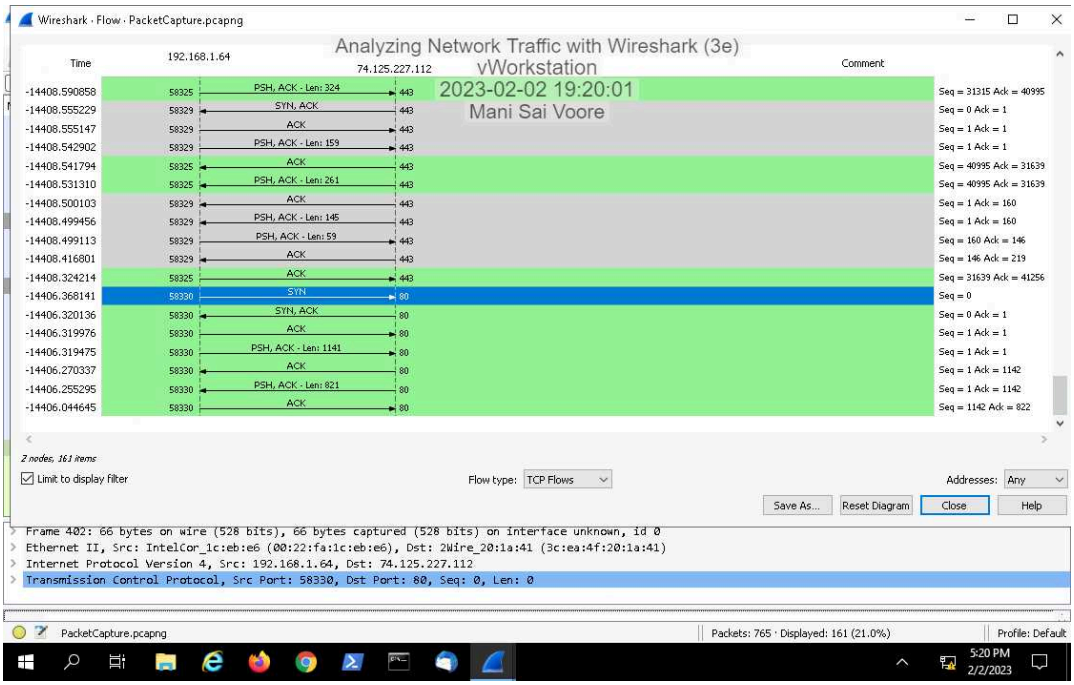
- **Record** the **source IP address in Packet 545**.



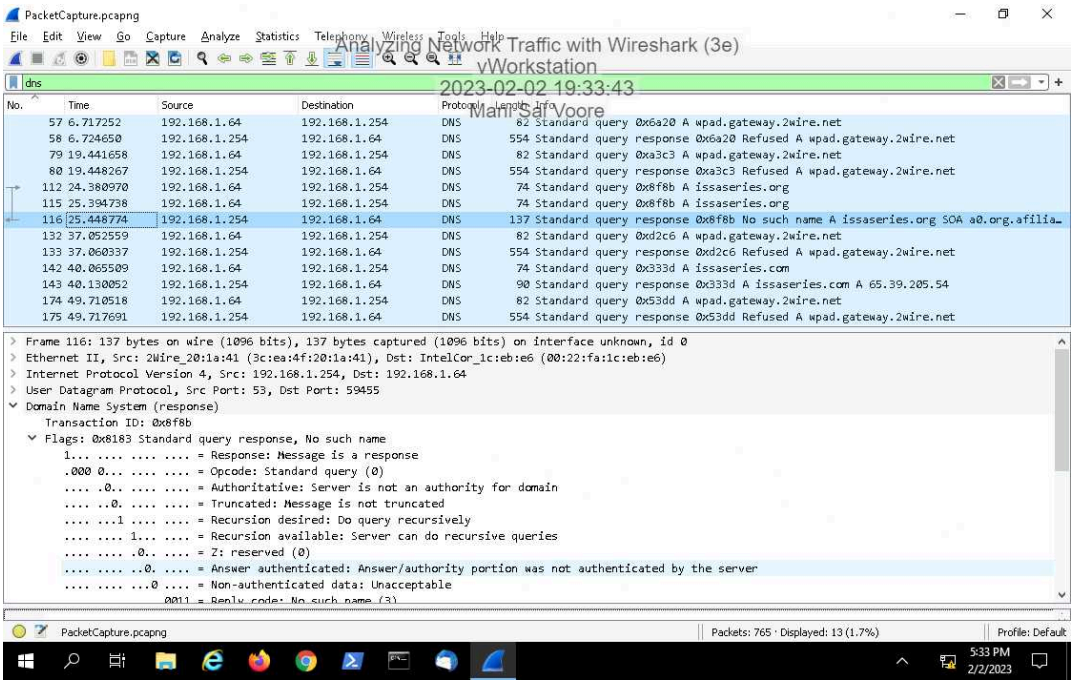
- **Make a screen capture** showing the **related frame numbers for Packet 545**.



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



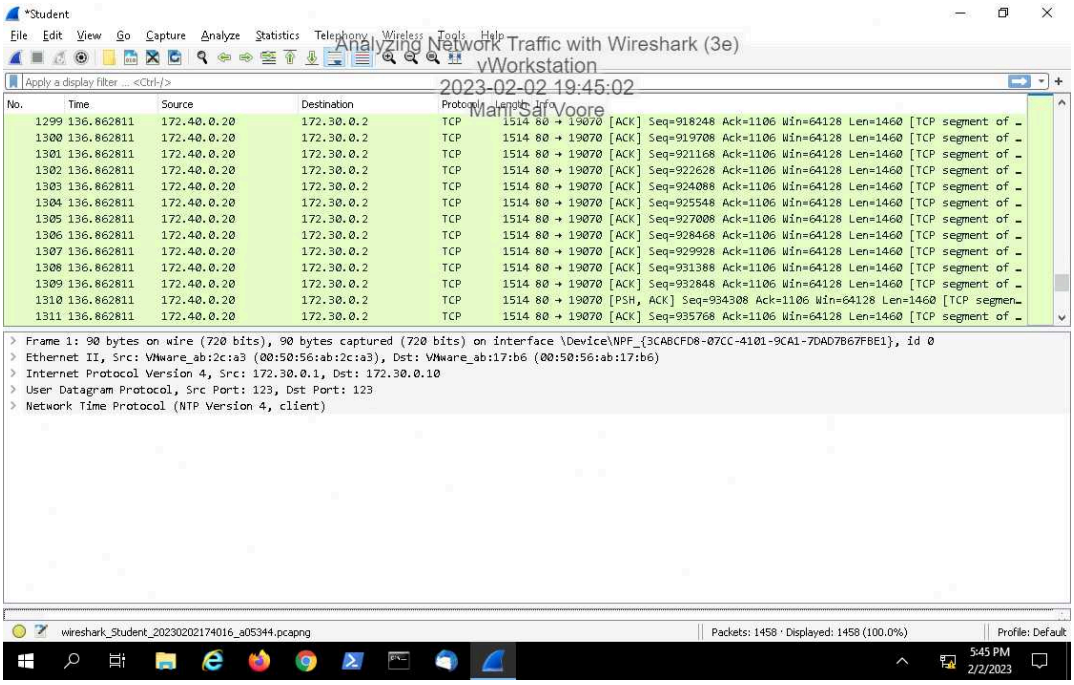
45. **Make a screen capture** showing the **response to the issaseries.org query**.



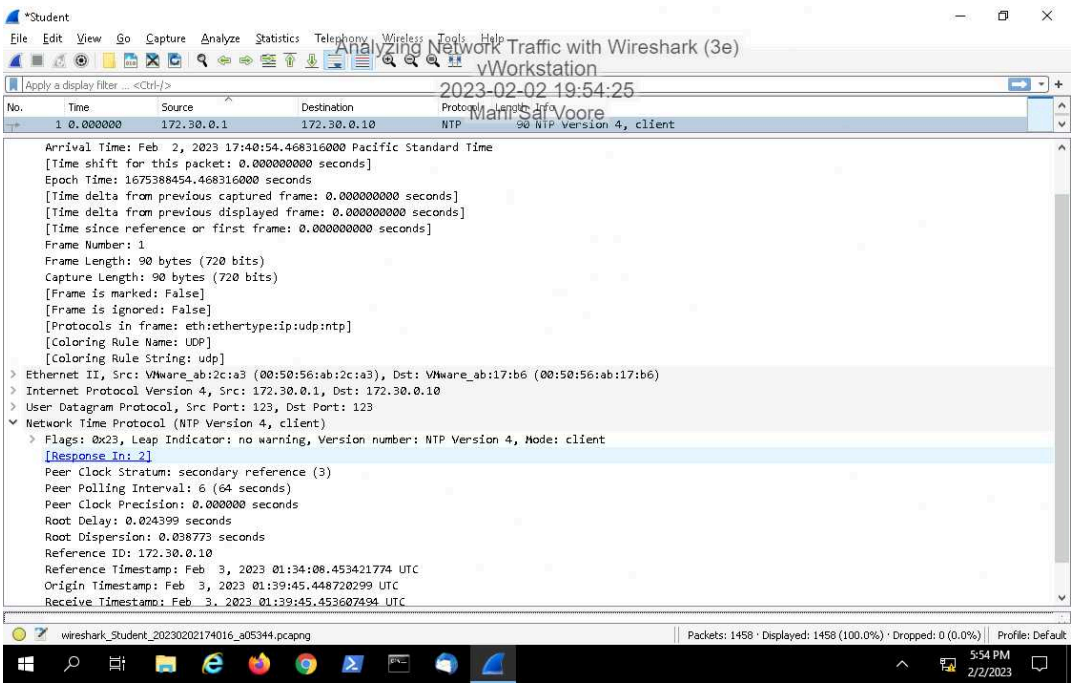
Section 2: Applied Learning

Part 1: Explore Wireshark

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

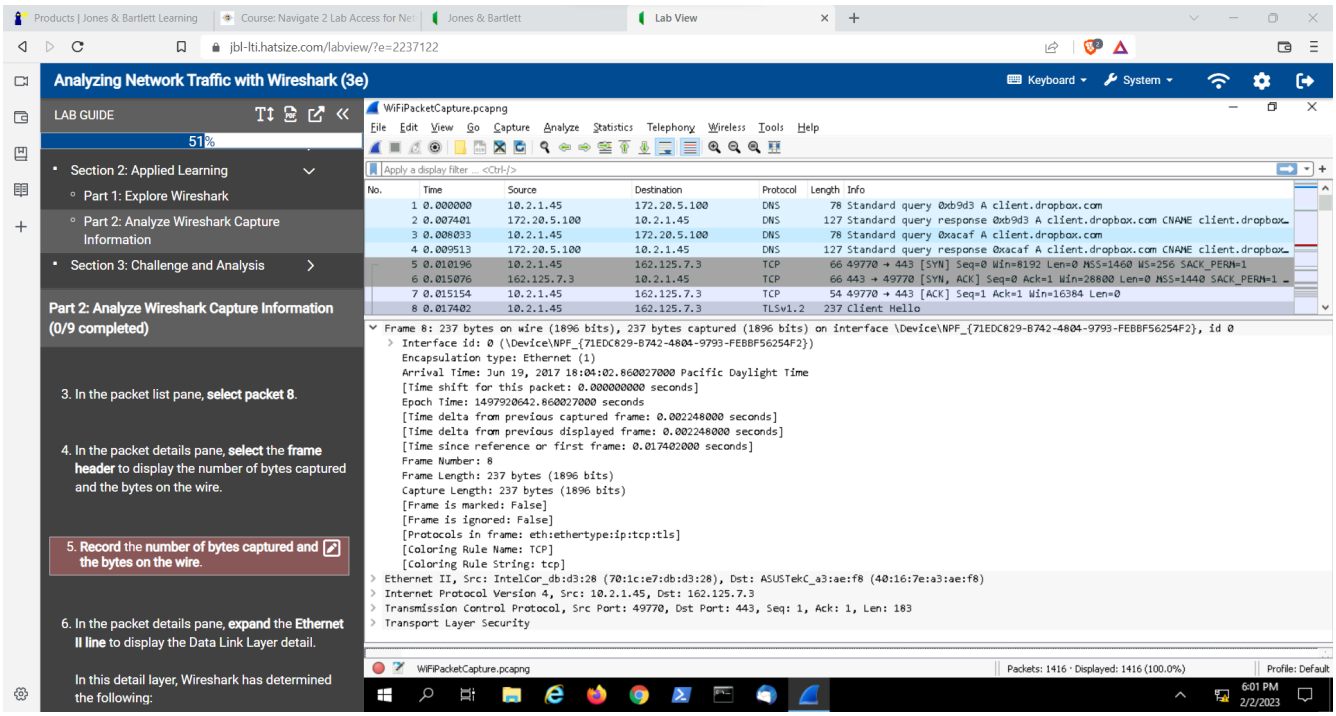


15. **Make a screen capture** showing the **fields related to time**.

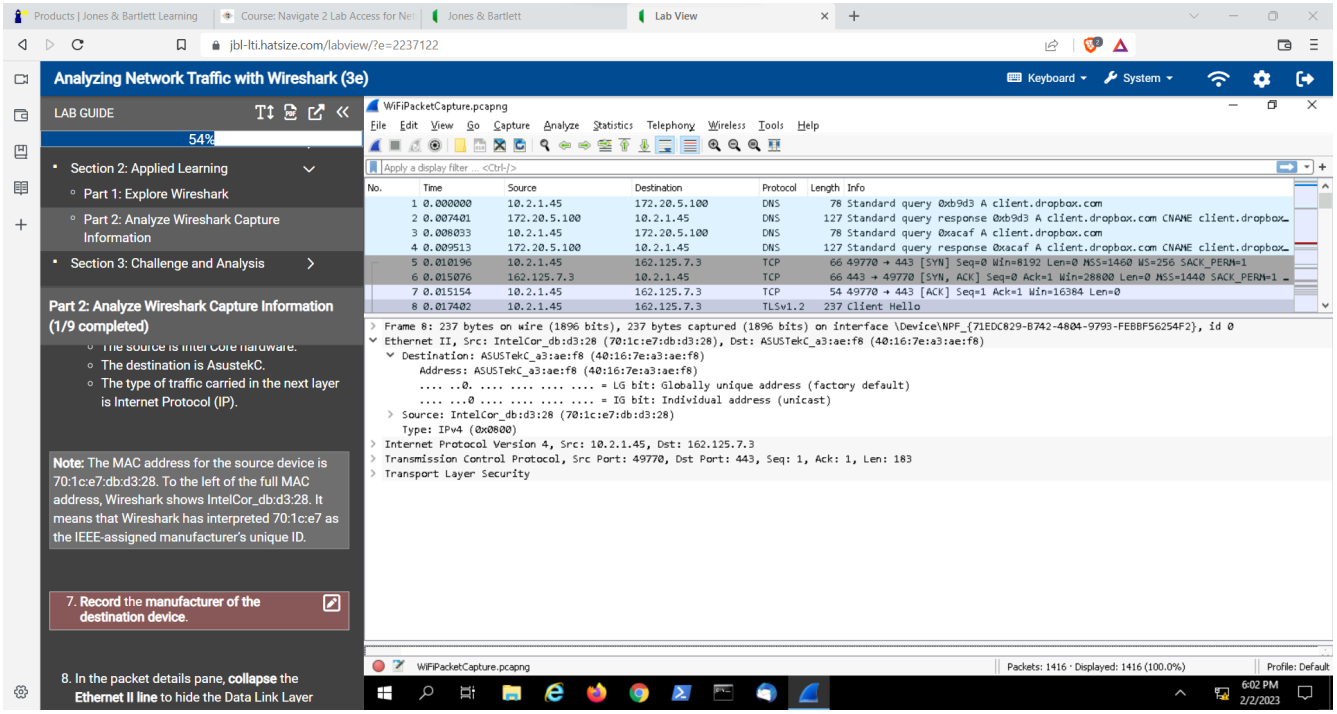


Part 2: Analyze Wireshark Capture Information

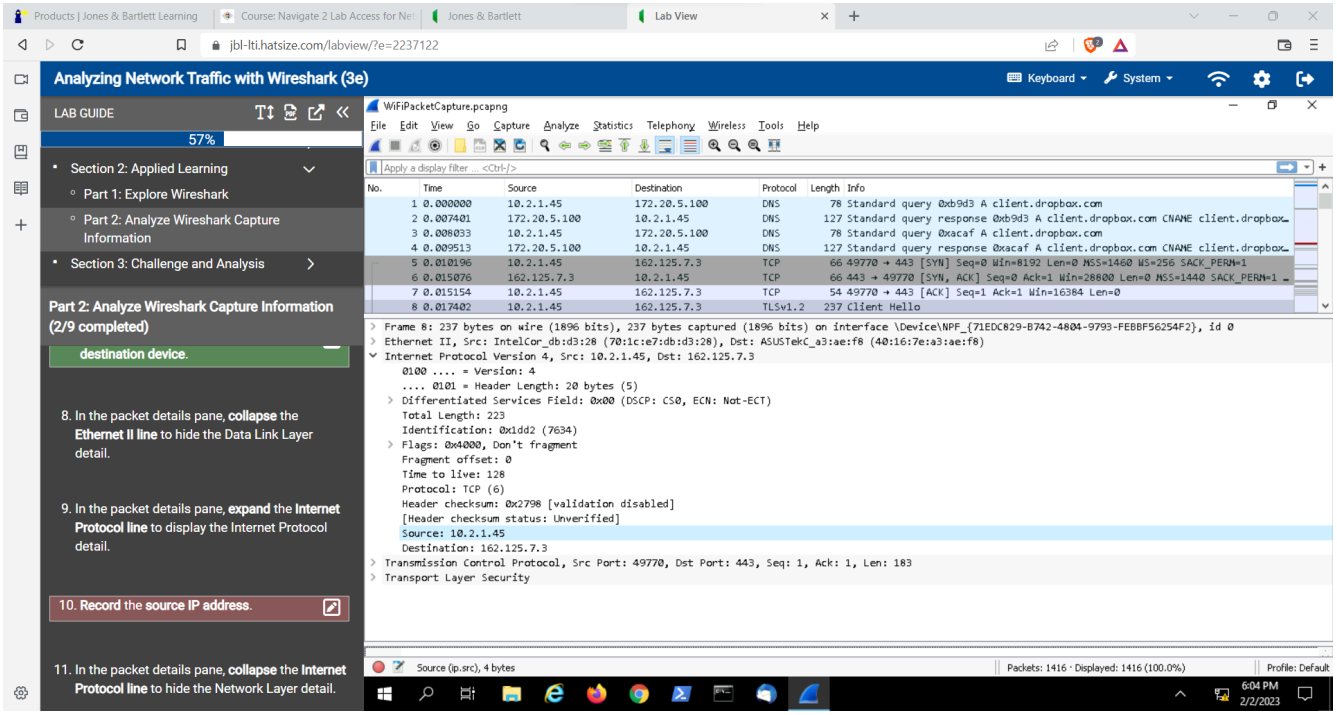
5. **Record** the **number of bytes captured and the bytes on the wire**.



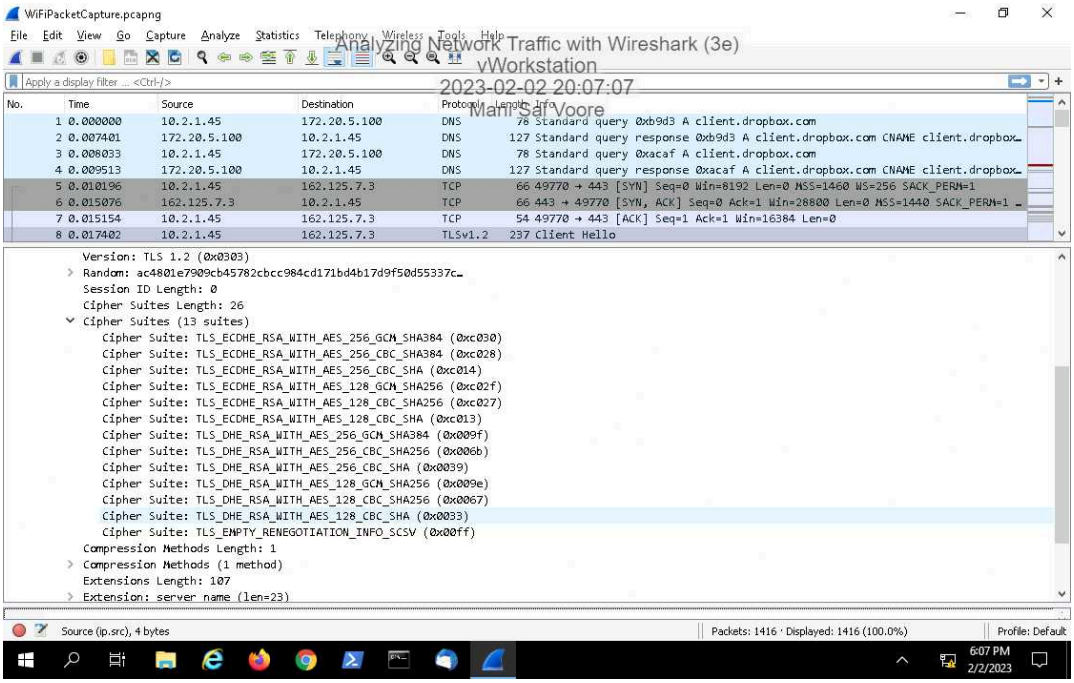
7. **Record** the **manufacturer of the destination device**.



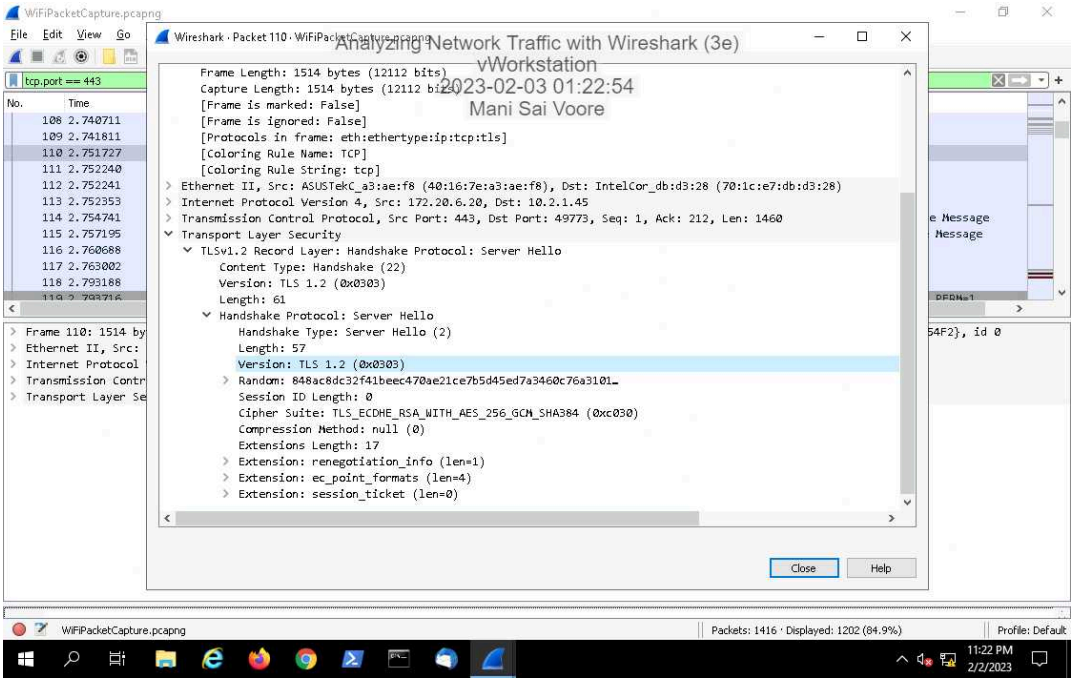
10. **Record** the **source IP address**.



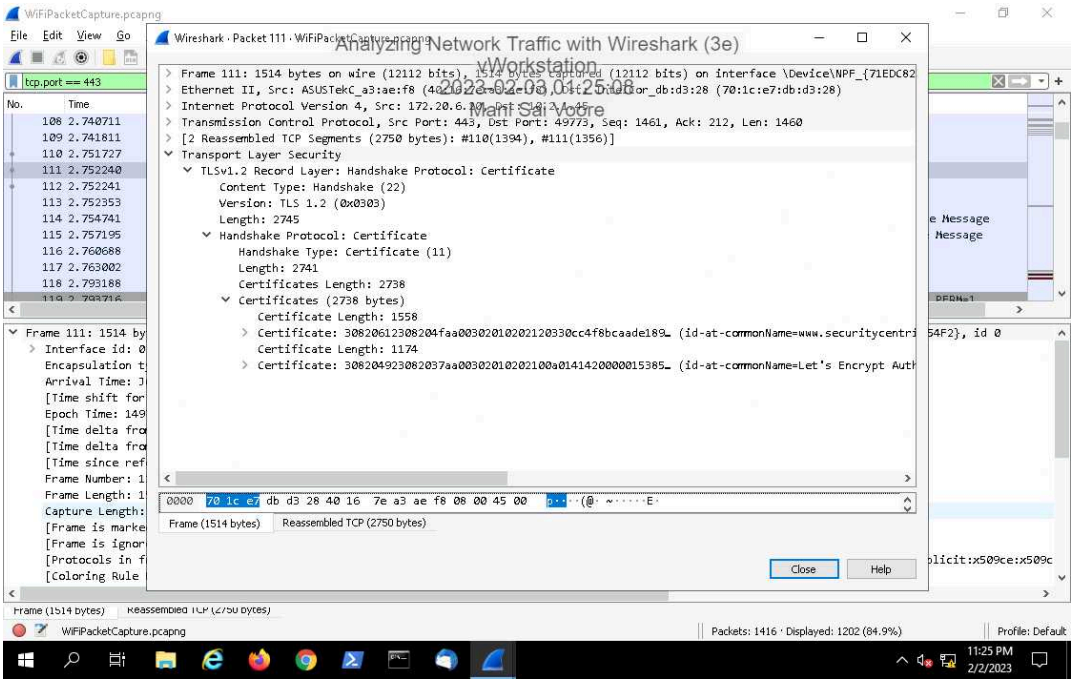
16. **Make a screen capture** showing the **entire list of cipher suites**.



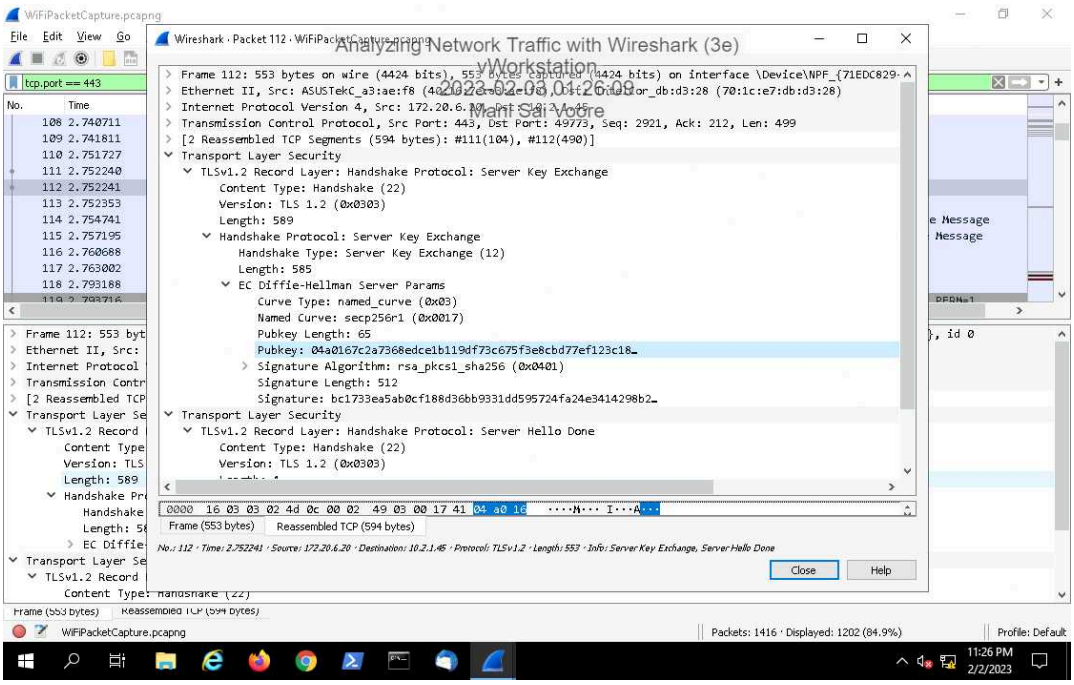
21. **Make a screen capture** showing the **issuer of the certificate**.



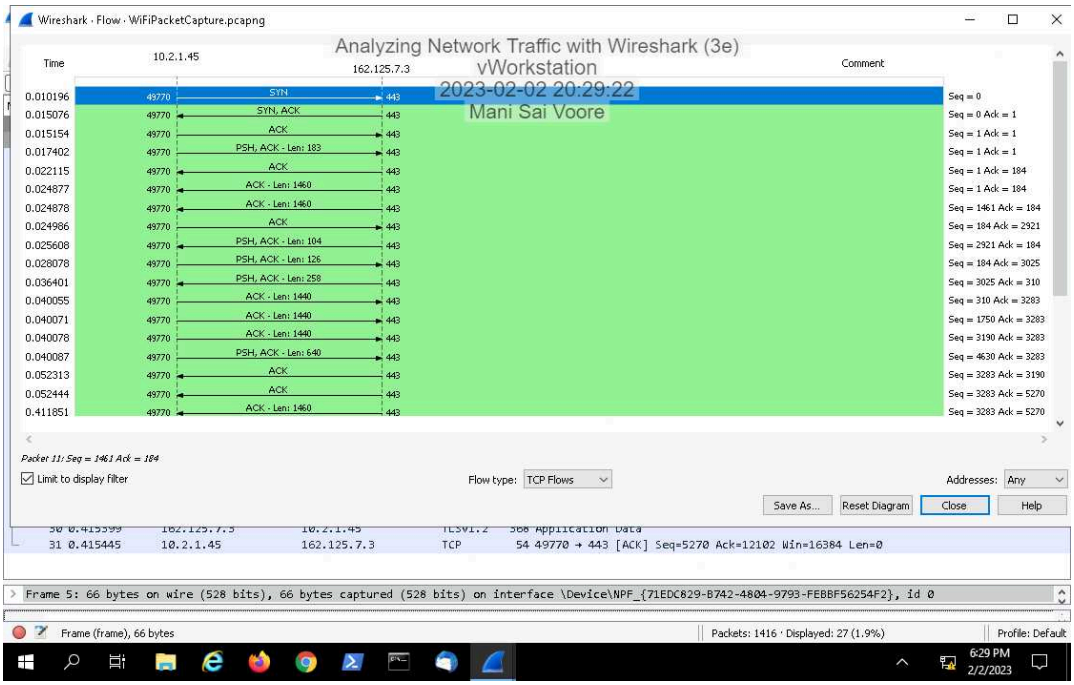
24. **Make a screen capture** showing the **details of the certificate**.



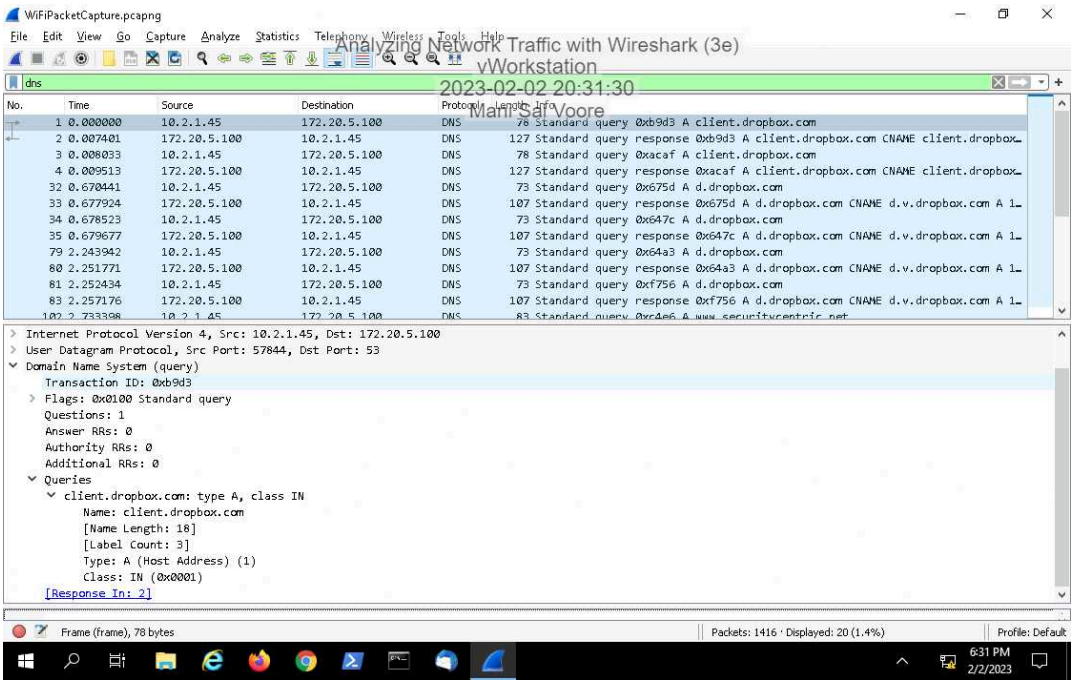
27. **Make a screen capture** showing the **public key and signature hash for the certificate**.



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).

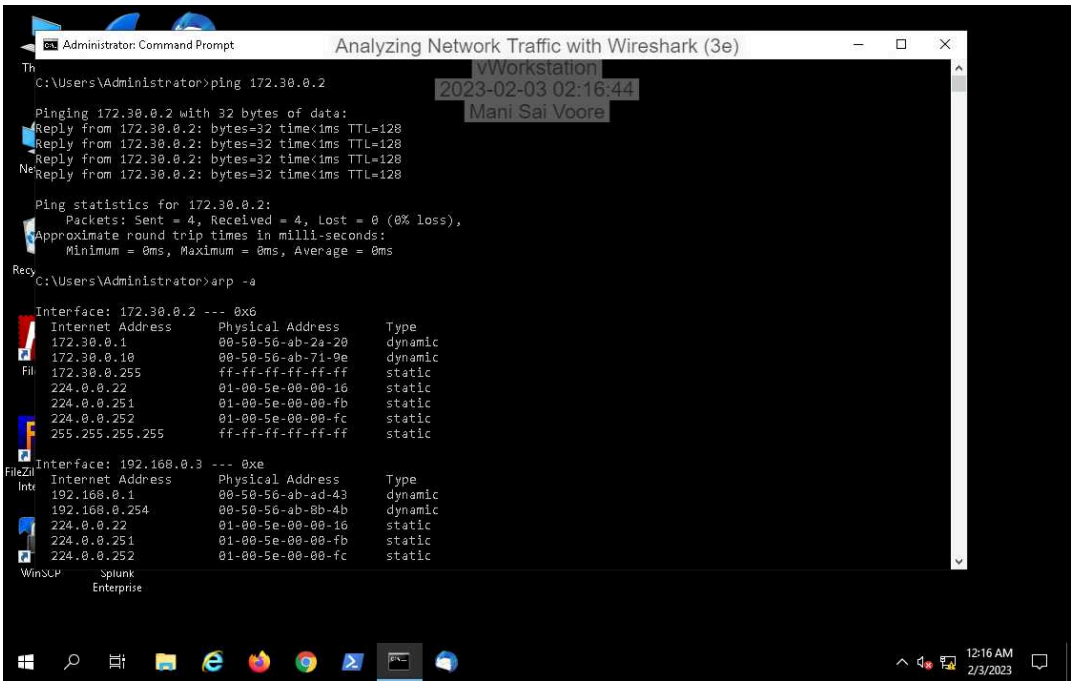
6.SNMP: It is called as Simple Network Management Protocol. The port number is 161.

   Purpose: Manages the routers, switches, servers.

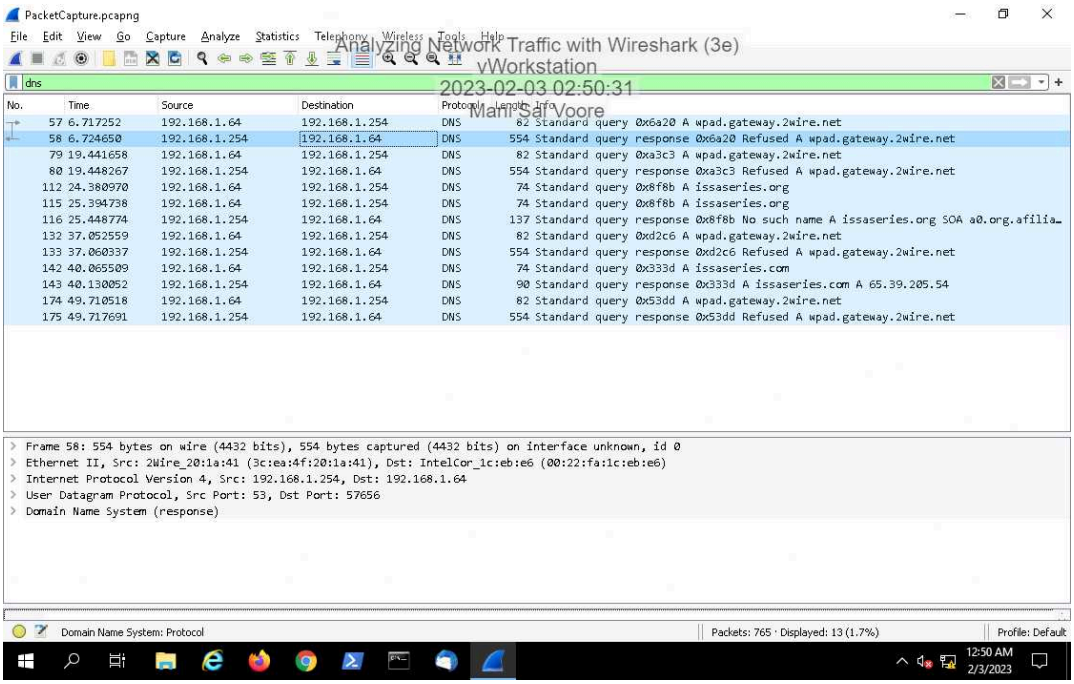
   Features: uses and support multiple version and layering like tree.

Part 2: Capture and Filter Traffic Using Wireshark

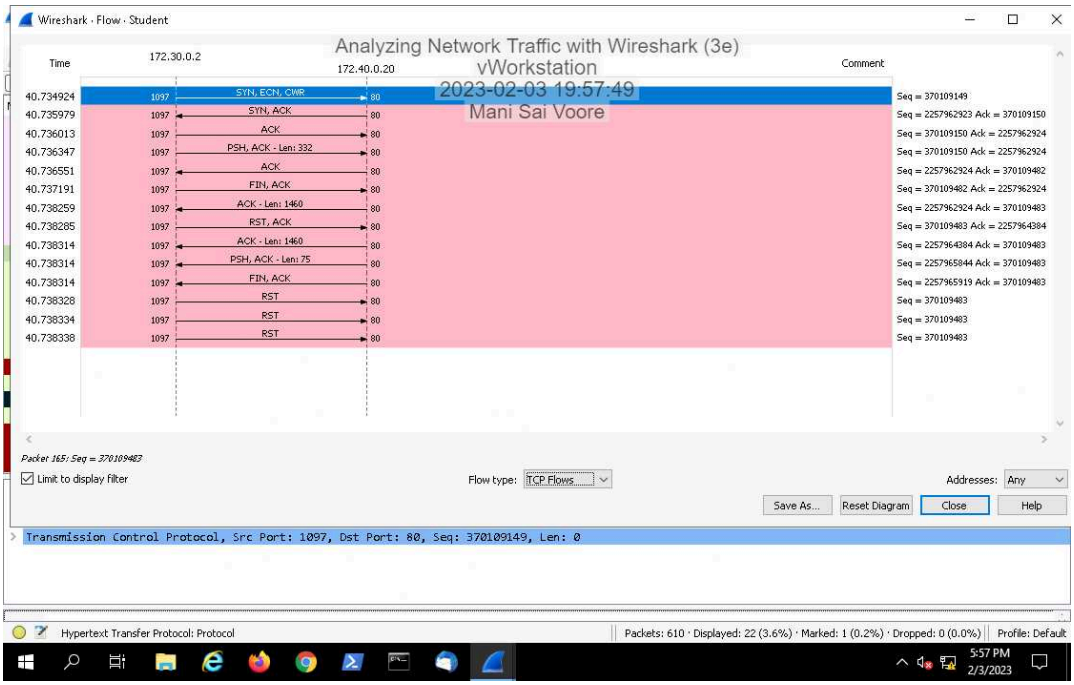
Make a screen capture showing the **MAC address resolved by ARP for the DNS server**.



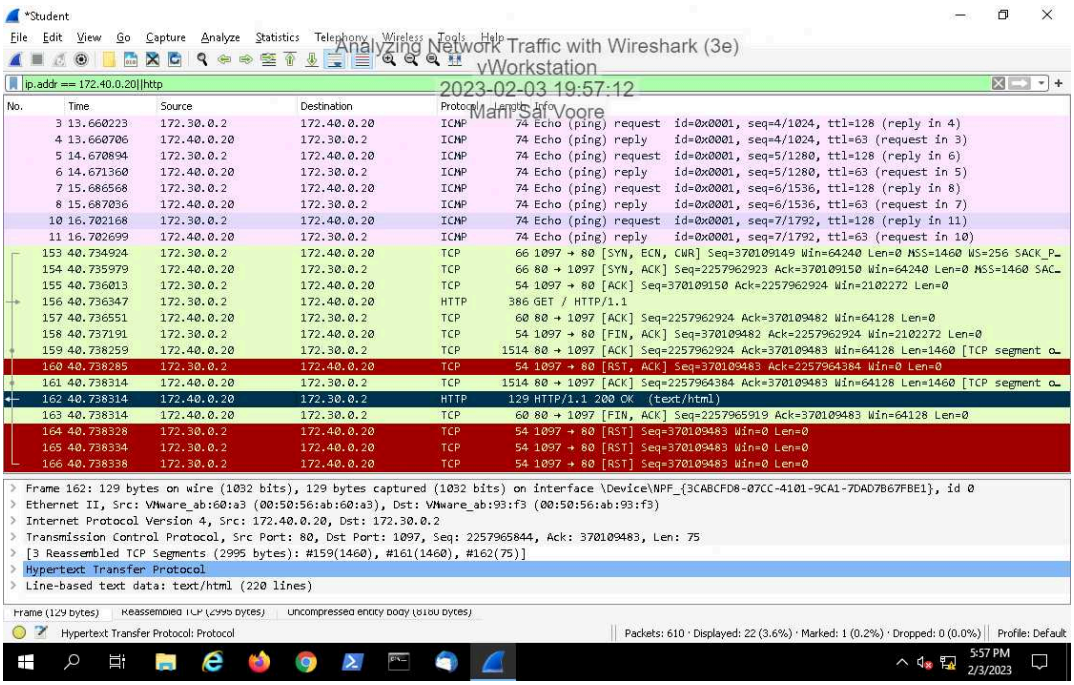
Make a screen capture showing the **destination IP address and port number of the DNS server**.



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

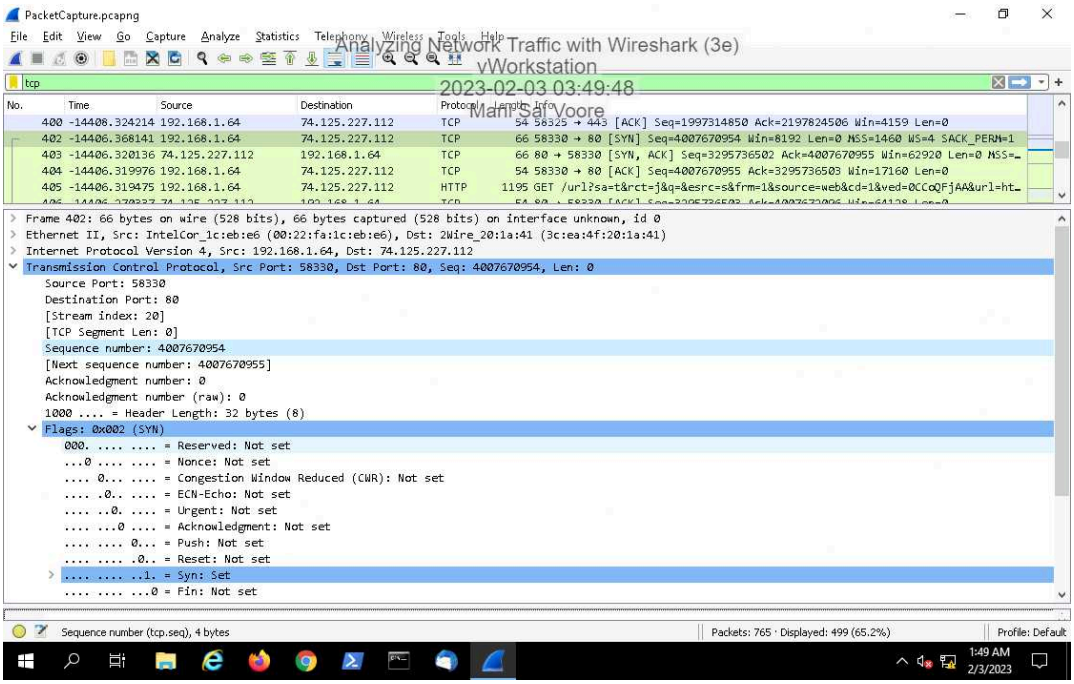


Make a screen capture of the **actual HTTP traffic that was delivered from the corporationtechs.com web server**.



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**.