

Student:

Javier Mejia

Email:

enriquem2260@gmail.com

Time on Task:

2 hours, 48 minutes

Progress:

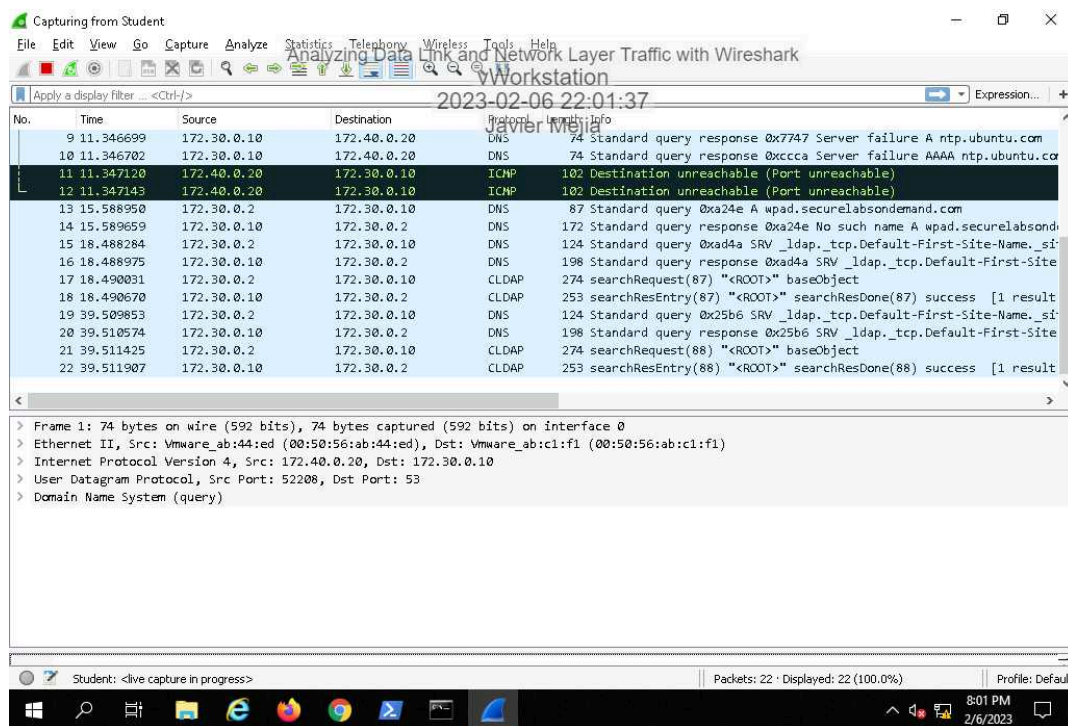
100%

Report Generated: Monday, February 6, 2023 at 11:46 PM

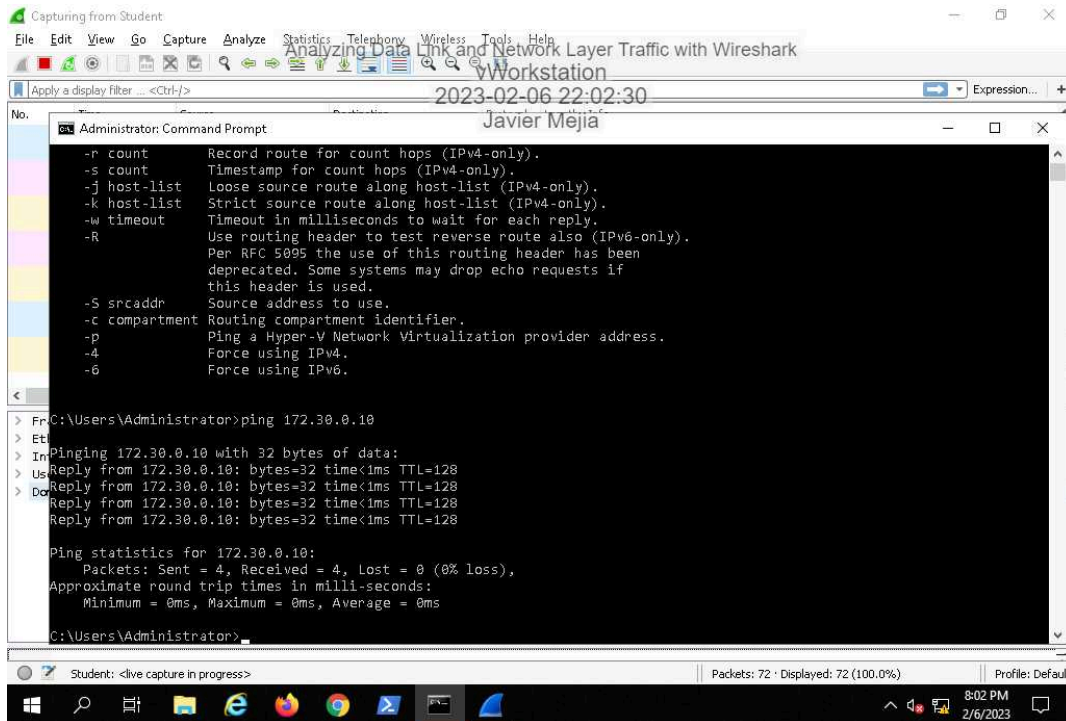
Section 1: Hands-On Demonstration

Part 1: Explore the Wireshark Application and Capture Network Traffic

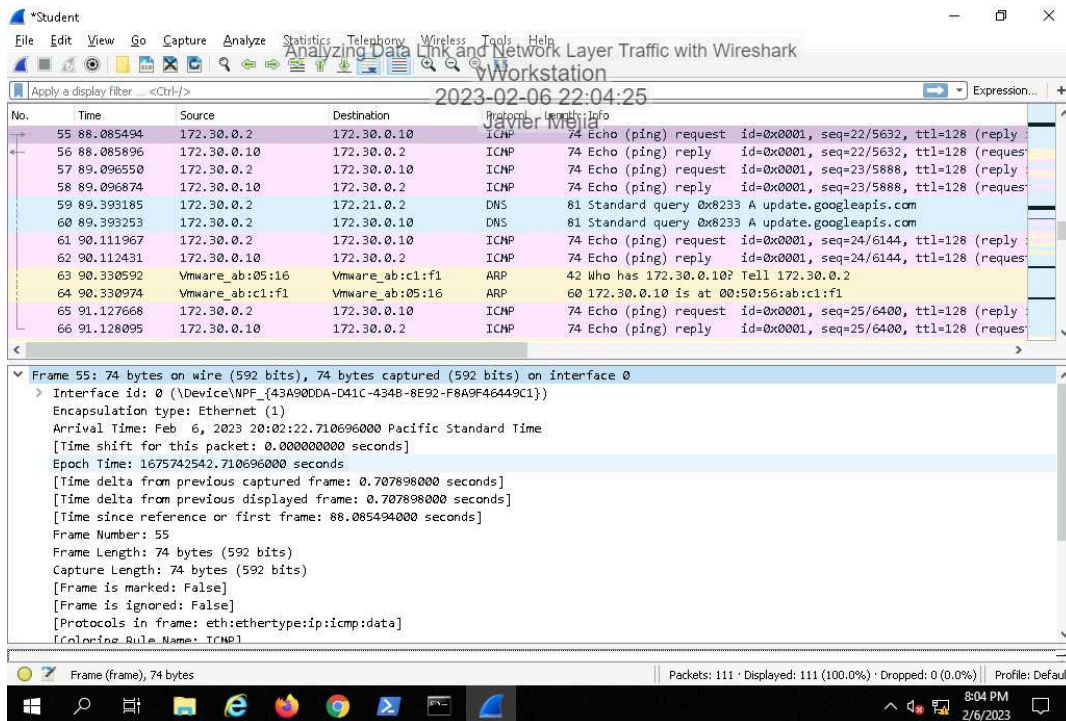
6. Make a screen capture showing the captured packets in Wireshark.



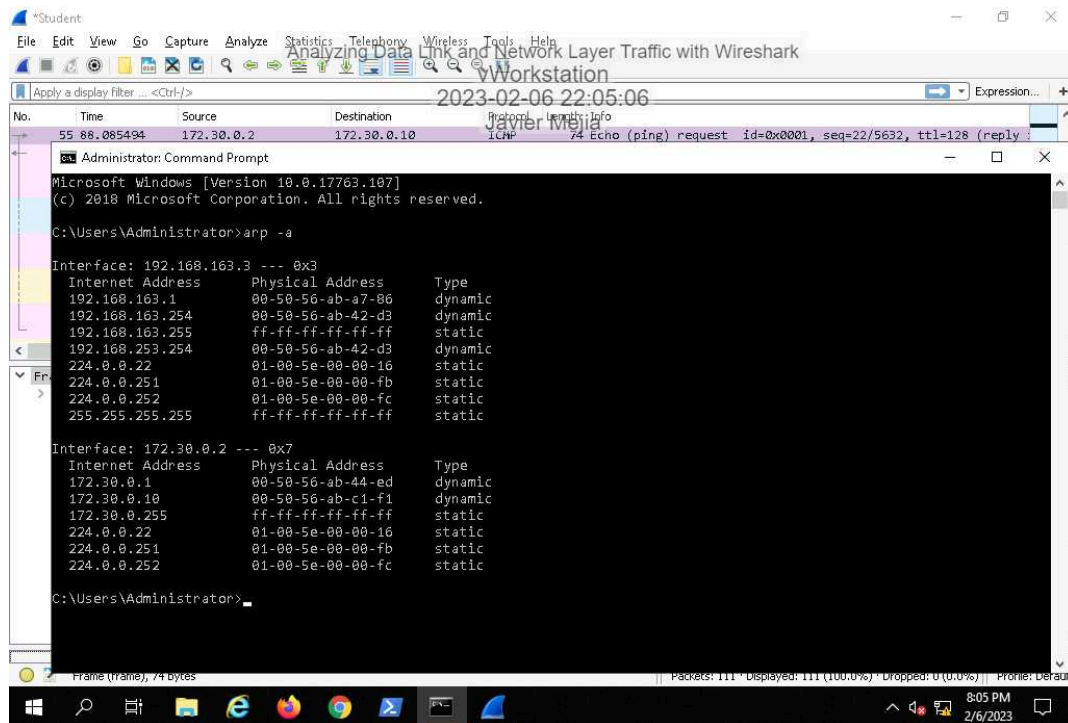
9. Make a screen capture showing the Ping results for 170.30.0.10.



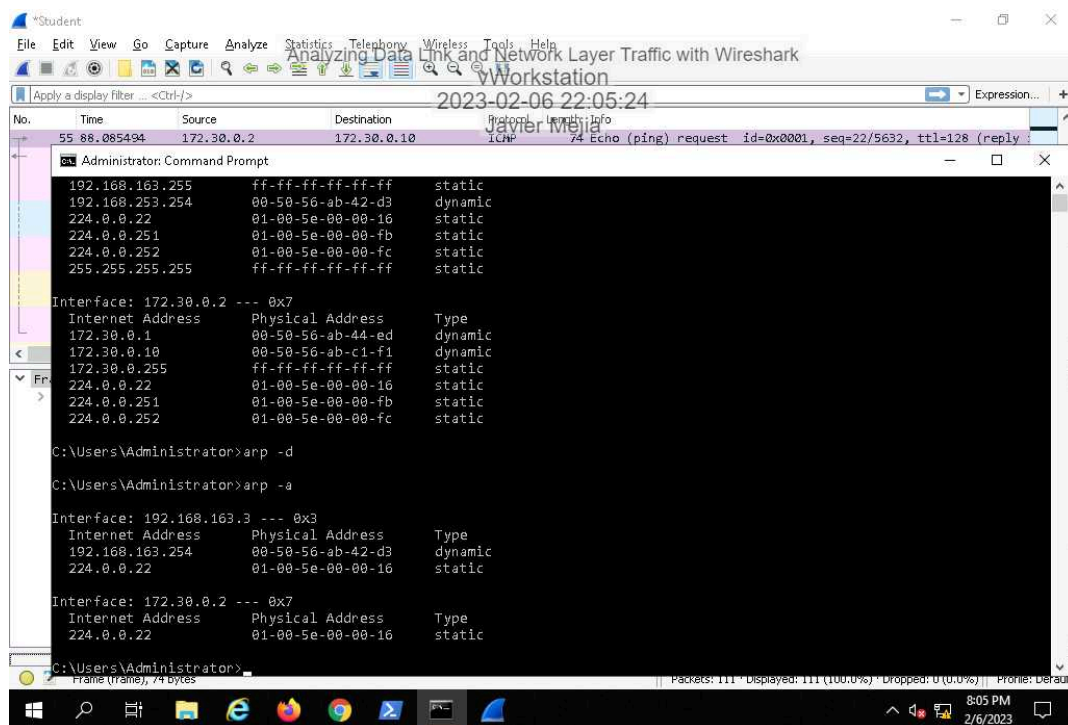
14. Make a screen capture showing the Packet details related to time.



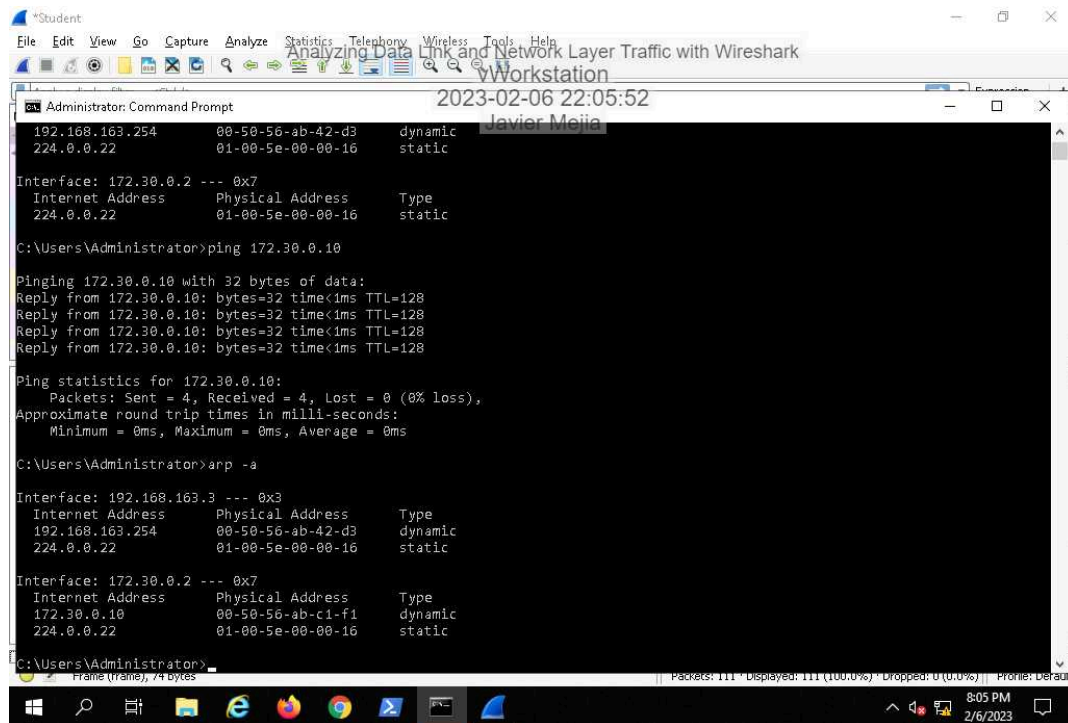
17. Make a screen capture showing the ARP table for the vWorkstation.



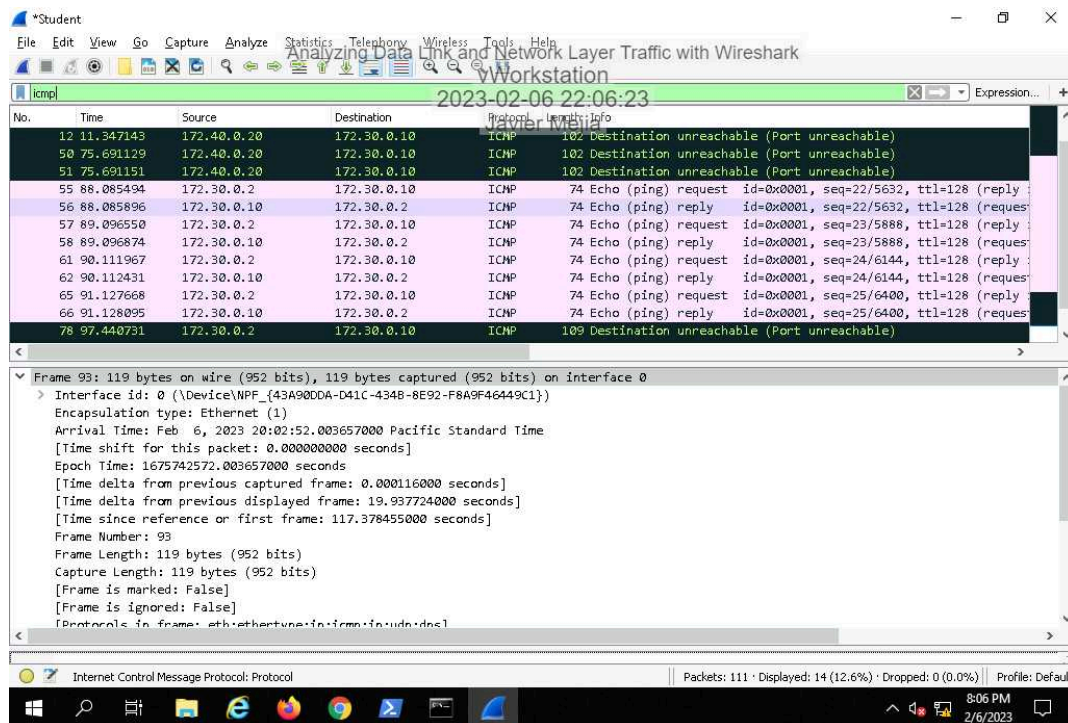
20. Make a screen capture showing the cleared ARP table on the vWorkstation.



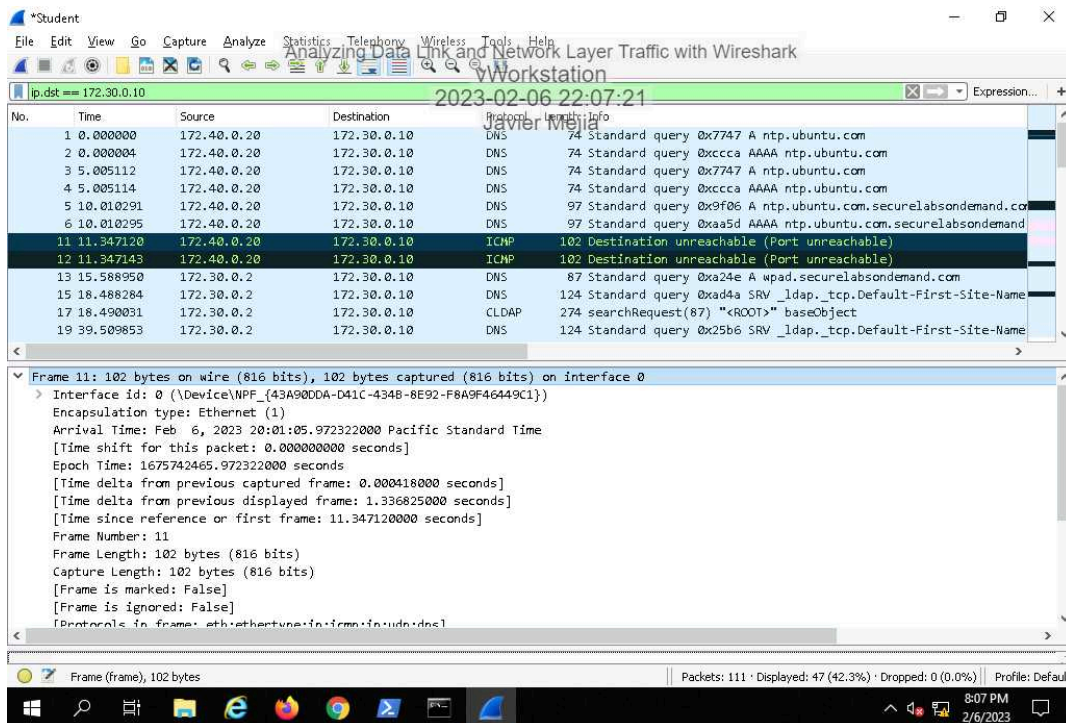
21. Make a screen capture showing the updated ARP table with the new 172.30.0.10 entry.



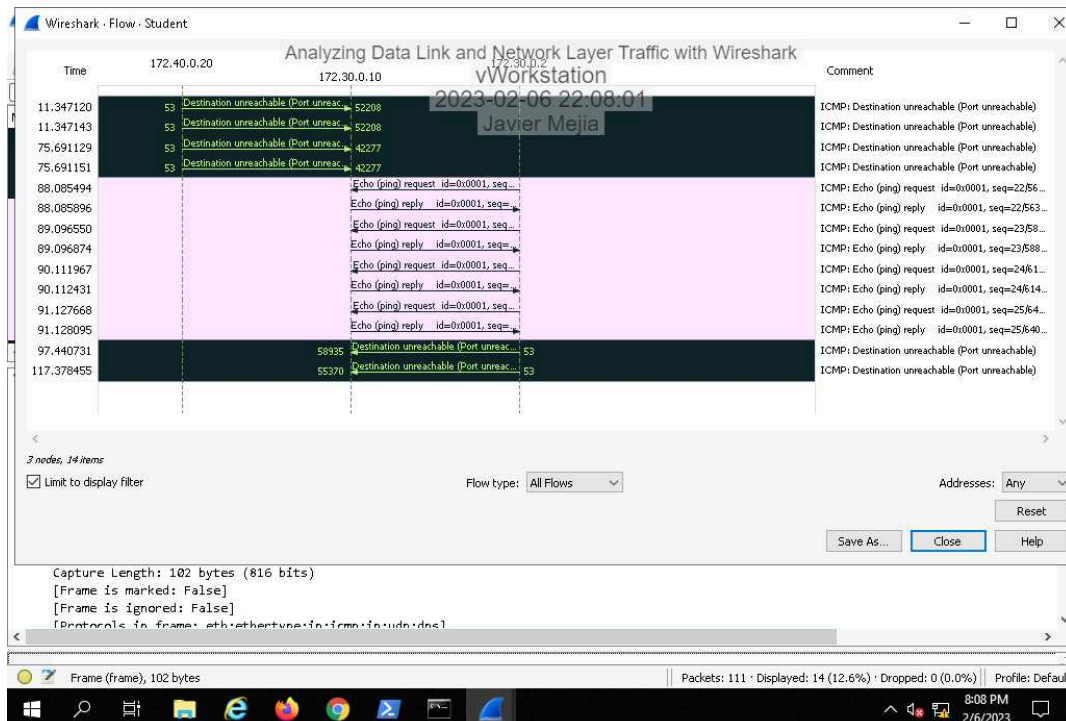
26. Make a screen capture showing the filtered list of ICMP packets.



30. Make a screen capture showing the **ICMP Packets** with the **src of 172.30.0.2** and **dst of 172.30.0.10**.

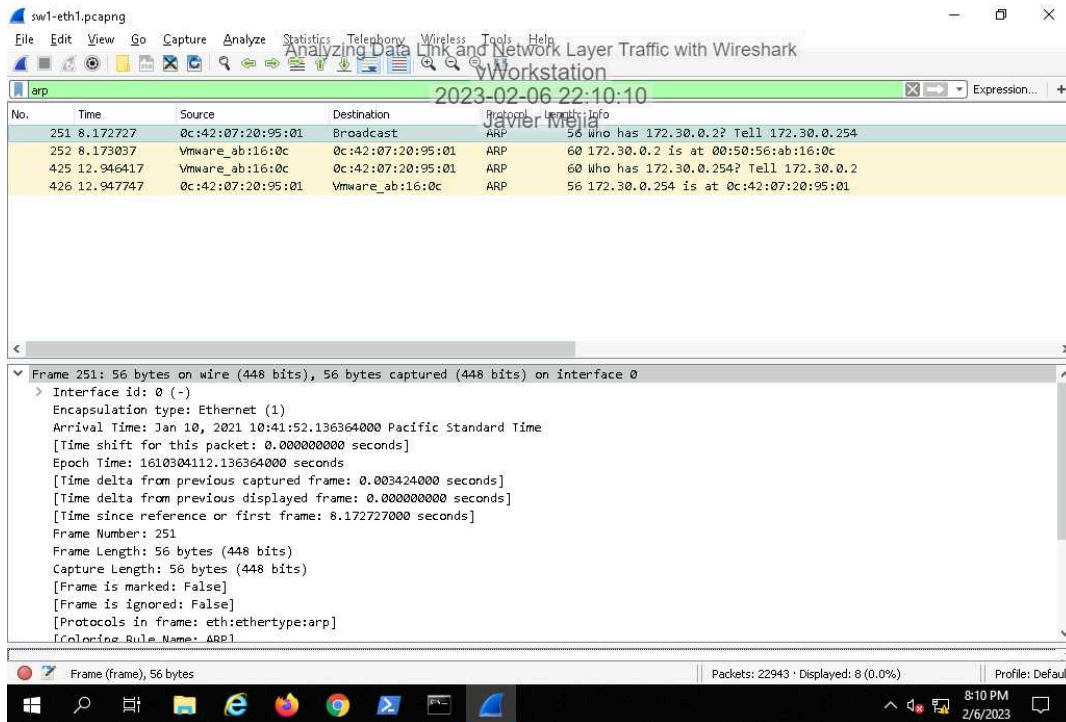


35. Make a screen capture showing the **Flow Graph** limited to display filter (ICMP packets).

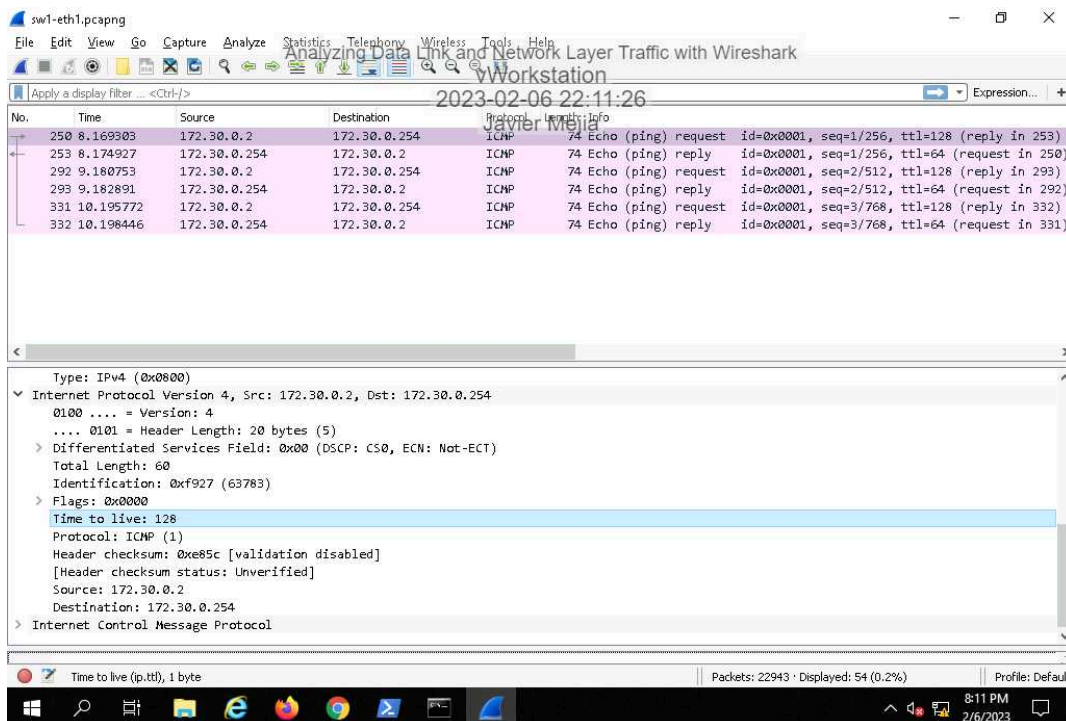


Part 2: Explore a Wireshark Capture File

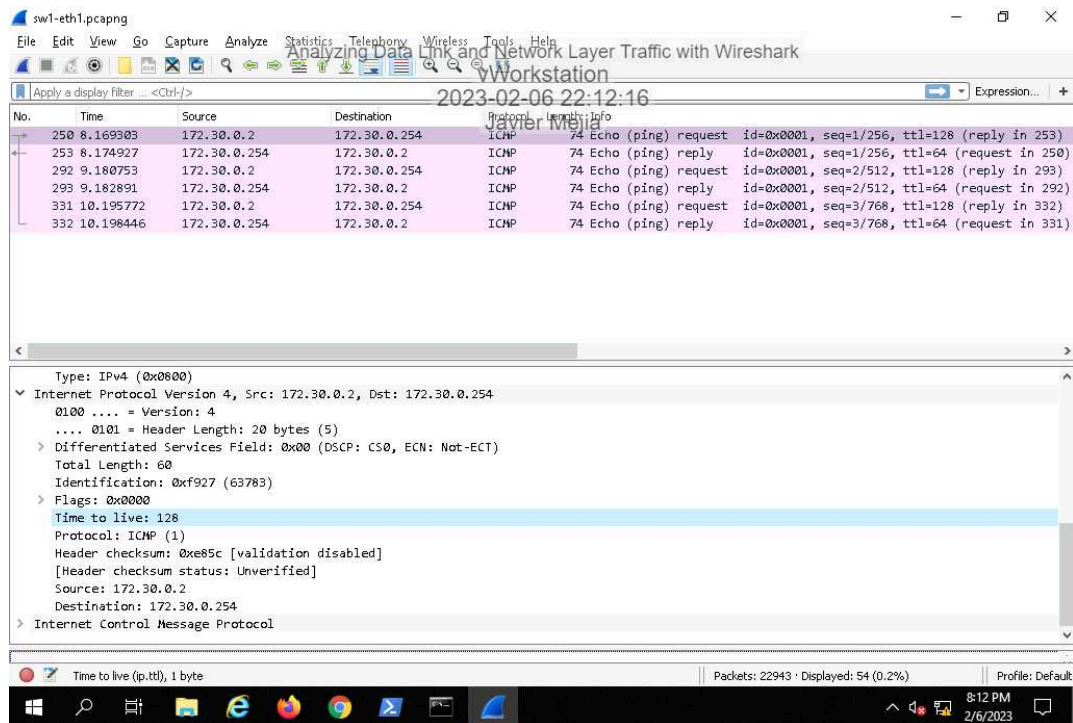
- Make a screen capture showing the ARP Packet List from your pcap file.



- Make a screen capture showing the Time to live field value for packet 21314.



15. Make a screen capture showing the Time to live field for packet 22202.



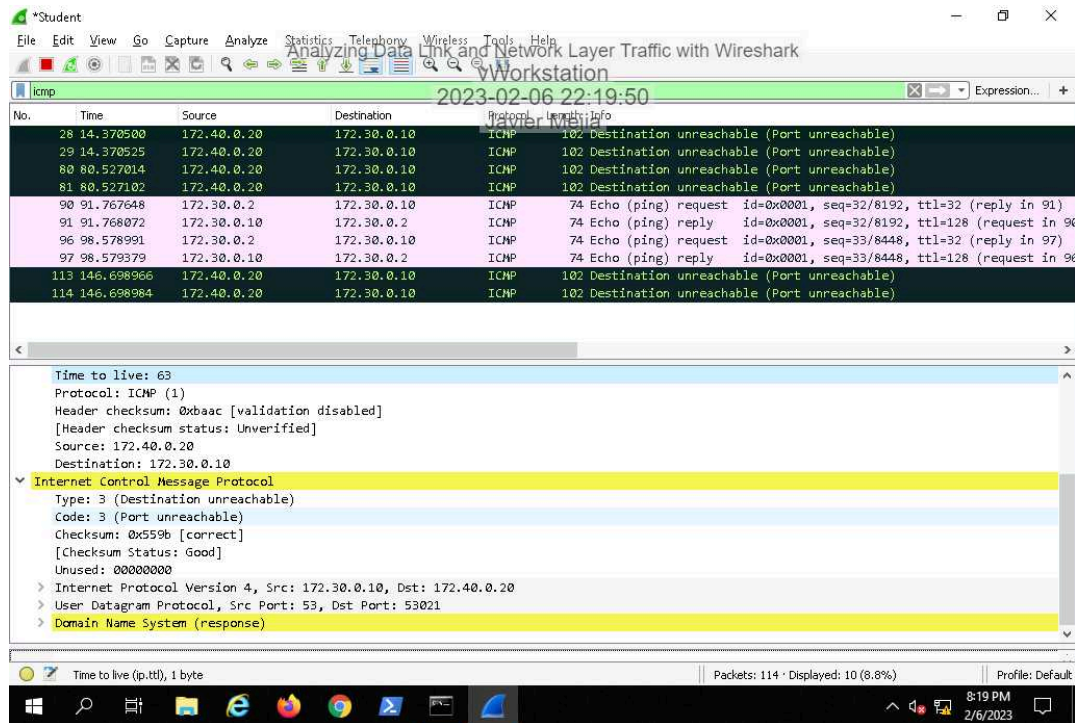
24. Record the VLAN ID of the 172.30.0.0/24 network.

I was not able to locate it.

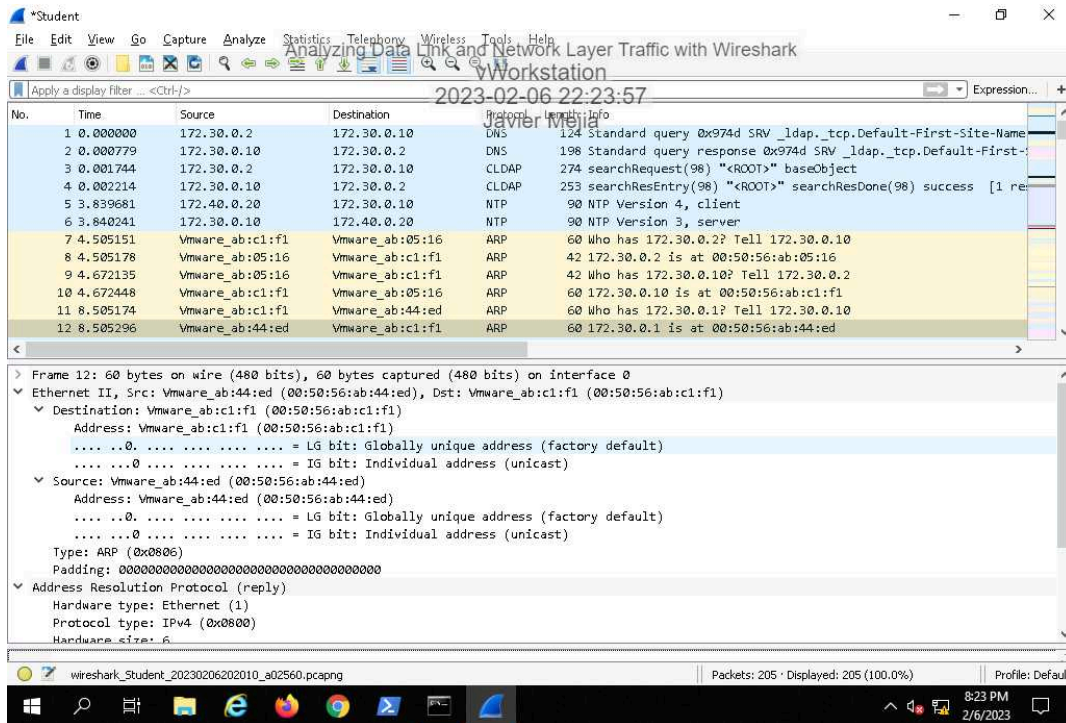
Section 2: Applied Learning

Part 1: Explore the Wireshark Application and Capture Network Traffic

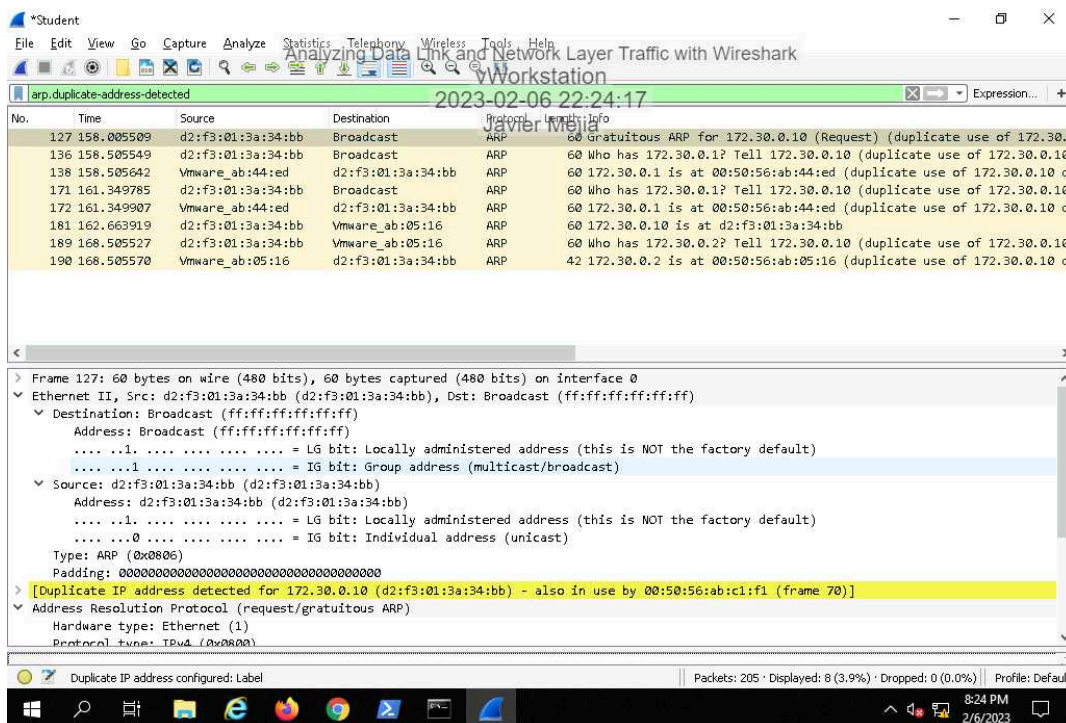
9. Make a screen capture showing the Echo request Type in the Packet Details view.



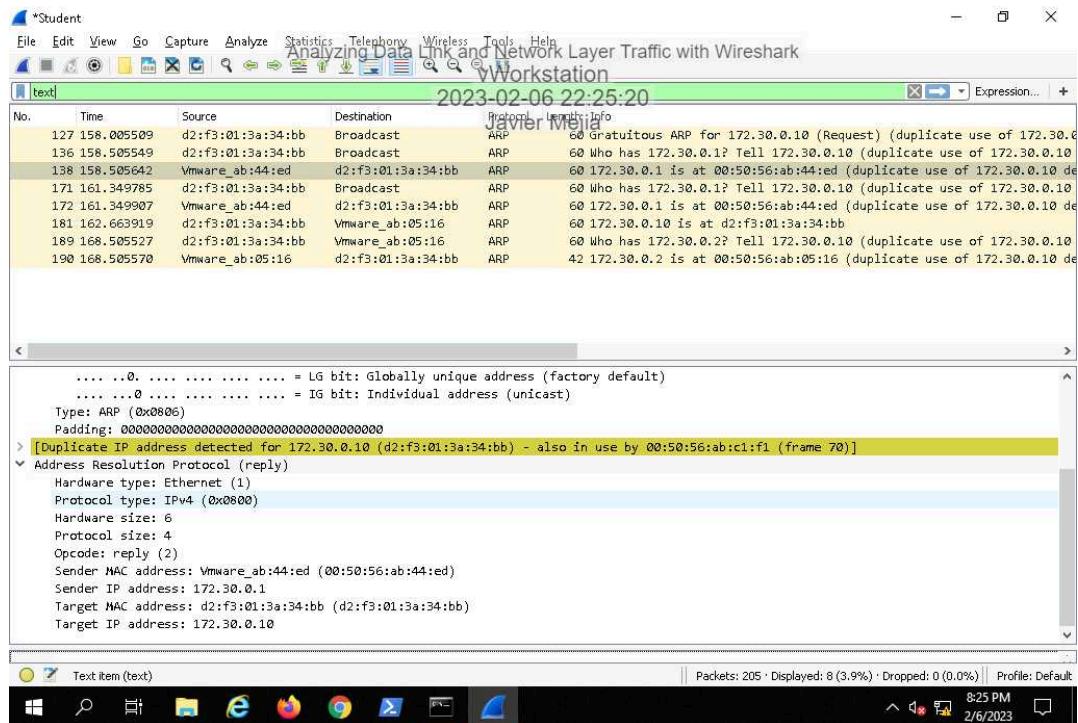
26. Make a screen capture showing the “Duplicate IP address detected” details and the Frame the original MAC address was identified in.



29. Make a screen capture showing all duplicate IP address detections in the Packet List pane.

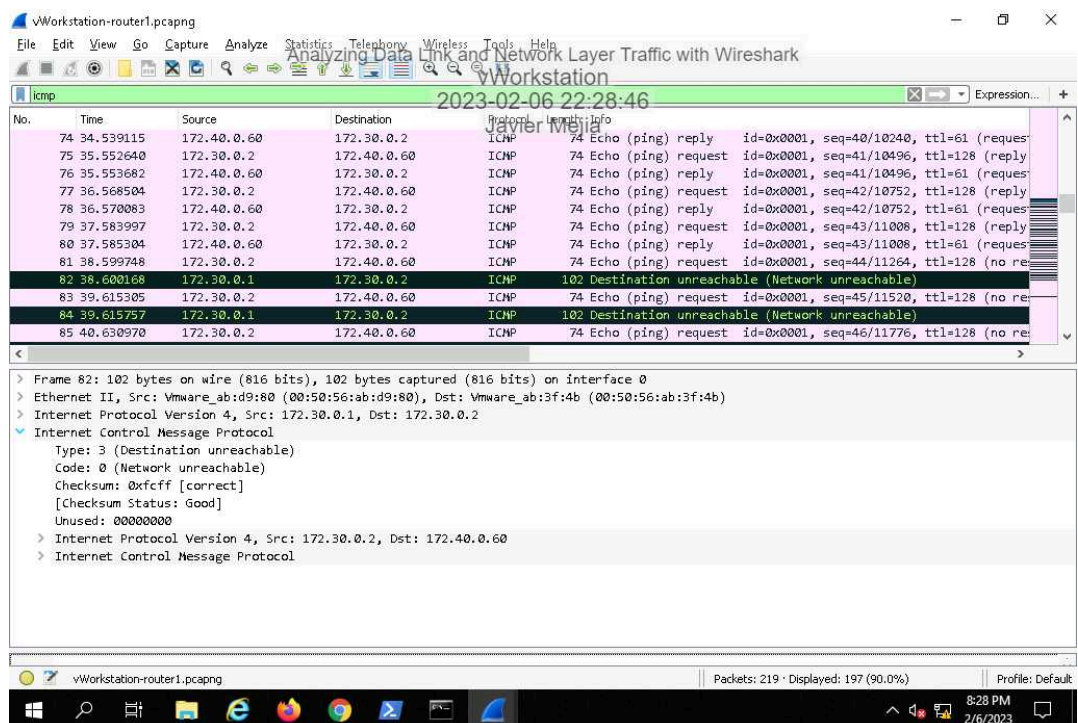


34. **Make a screen capture** showing the **filtered ARP packets** in the **Packet List View**.

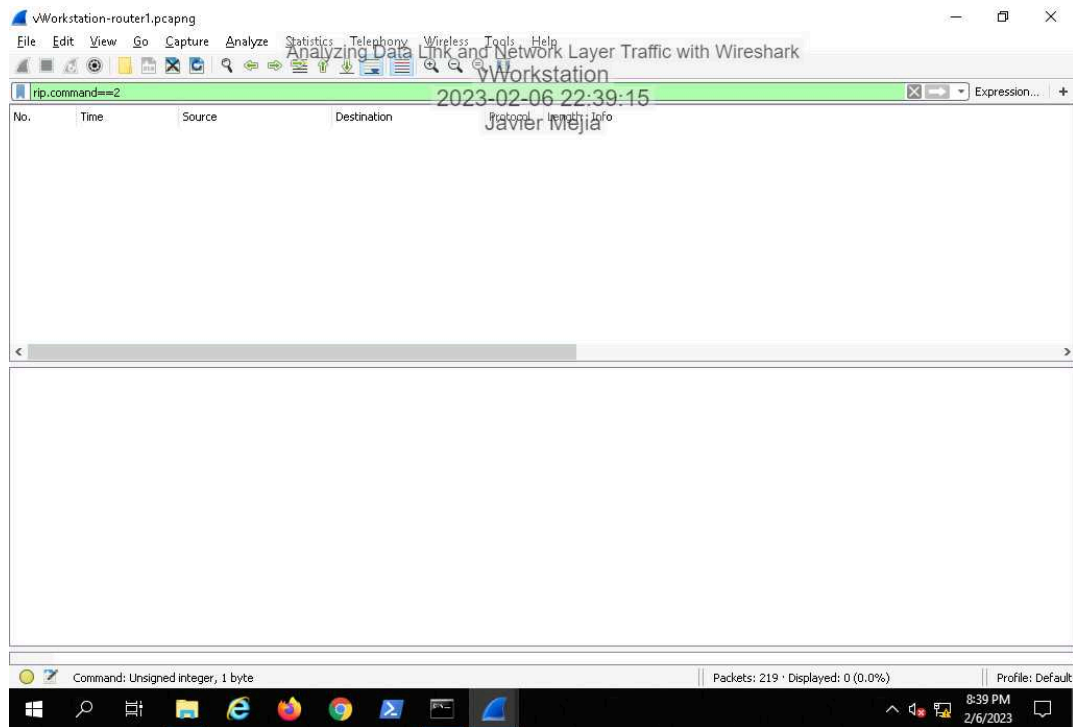


Part 2: Explore a Wireshark Capture File

5. **Make a screen capture** showing the **ICMP Type** for this packet (**Destination unreachable**).



18. **Make a screen capture** showing the **simple password** for packet 280.



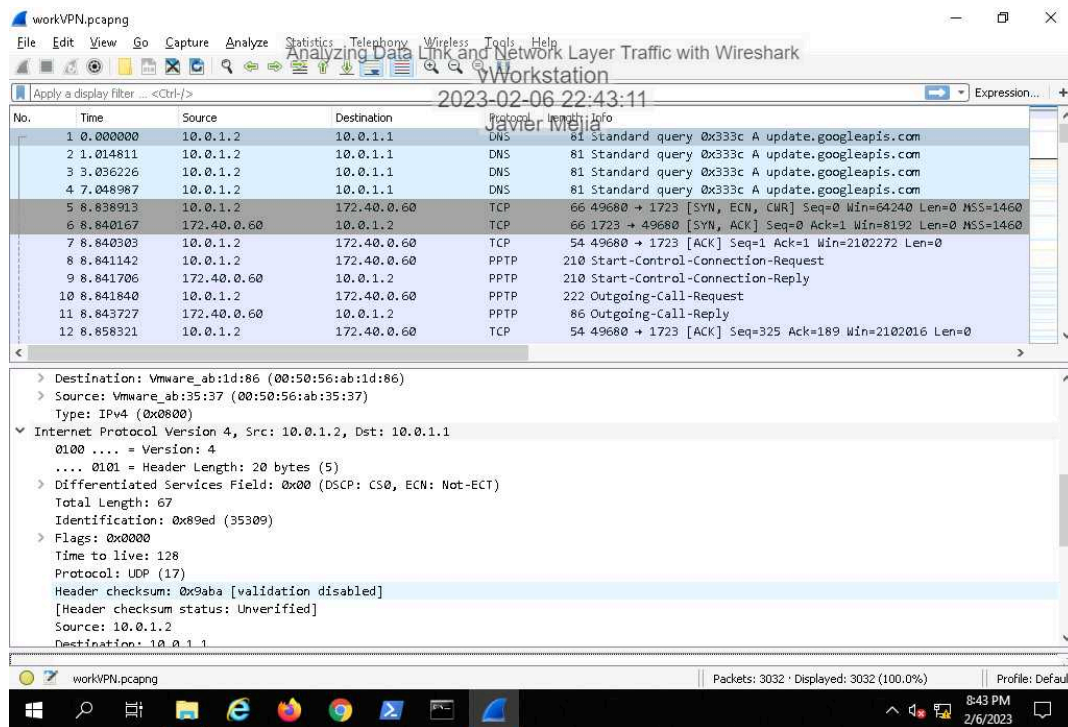
25. **Record** the number of the packet that contains the first corrected RIPv2 simple password.

Was not able to.

Section 3: Challenge and Analysis

Part 1: Identify a Rogue Host in a Packet Capture File

Make a screen capture showing the **Packet List View** with your applied conversation filter.

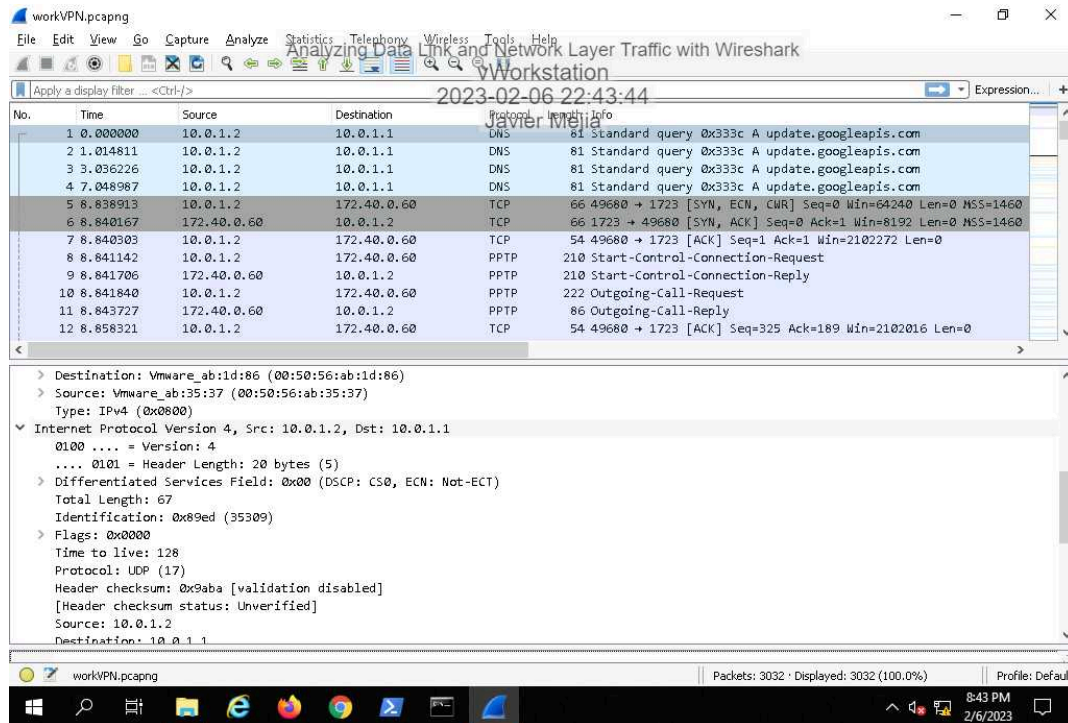


Part 2: Detect an ARP Poisoning Event in a Packet Capture File

Analyzing Data Link and Network Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 02

Make a screen capture showing the “Duplicate IP address detected for...” details in the Packet Details View.



Part 3: Determine if VPN Login Information was Compromised

Analyzing Data Link and Network Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 02

Make a screen capture showing the **ARP responses** that came before the login packet.

