

Conducting Forensic Investigations on Network Infrastructure (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

Student:

Vishal Singh Bhardvaj

Email:

Time on Task:

2 hours, 12 minutes

Progress:

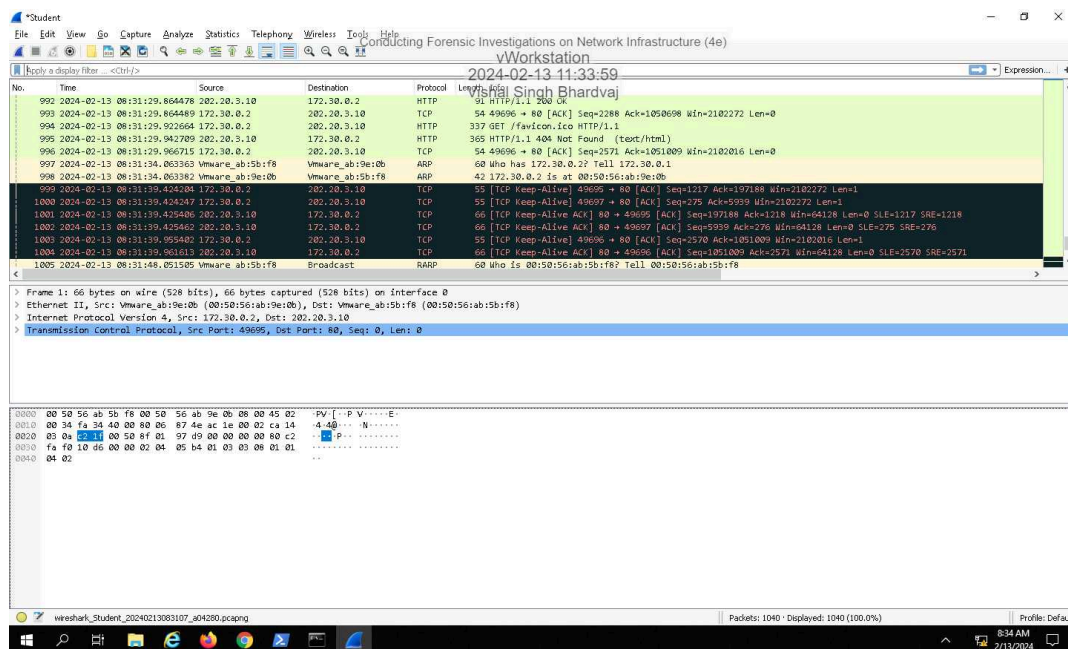
100%

Report Generated: Tuesday, February 13, 2024 at 4:05 PM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

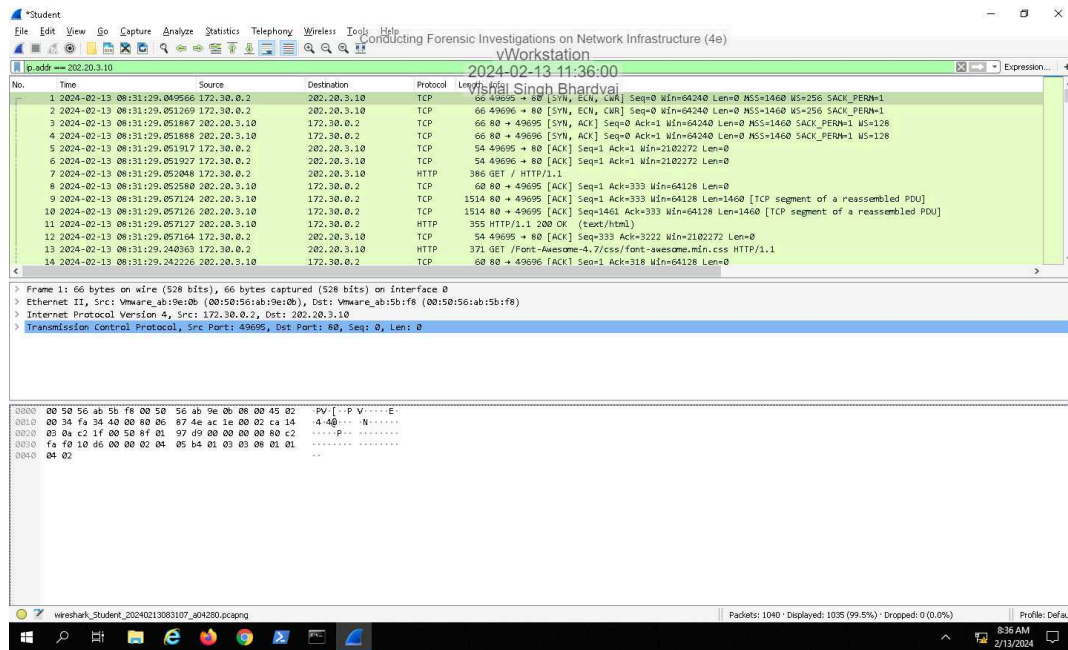
11. Make a screen capture showing the timestamp-sorted traffic.



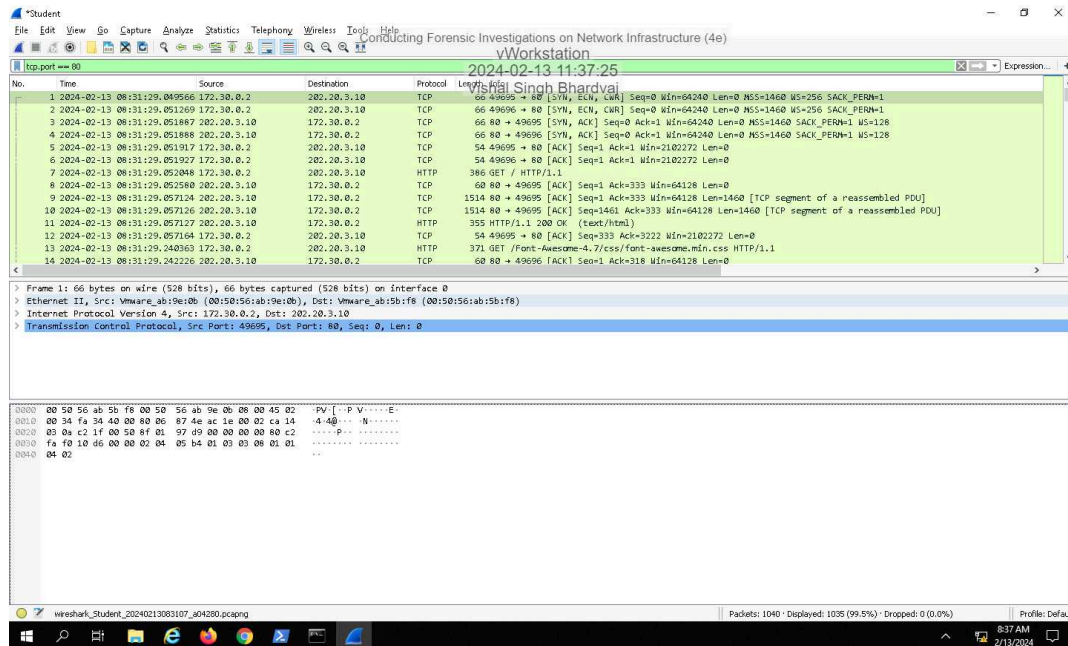
Conducting Forensic Investigations on Network Infrastructure (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

13. Make a screen capture showing the IP-filtered traffic.



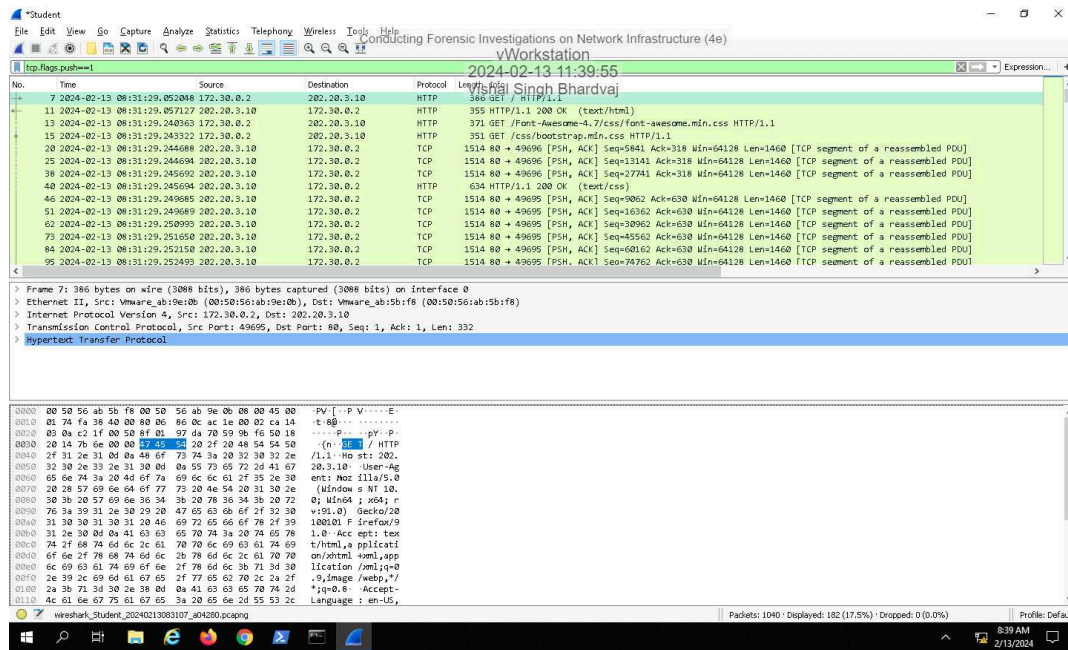
15. Make a screen capture showing the port-filtered traffic.



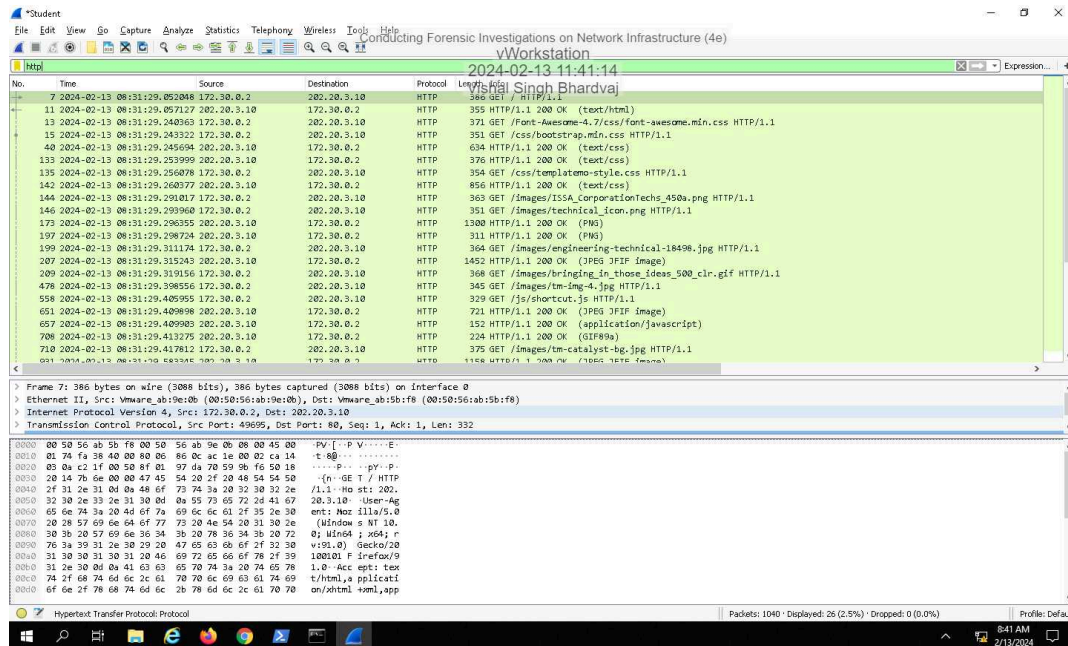
Conducting Forensic Investigations on Network Infrastructure (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

17. Make a screen capture showing the TCP push flag-filtered traffic.



19. Make a screen capture showing the http-filtered traffic.

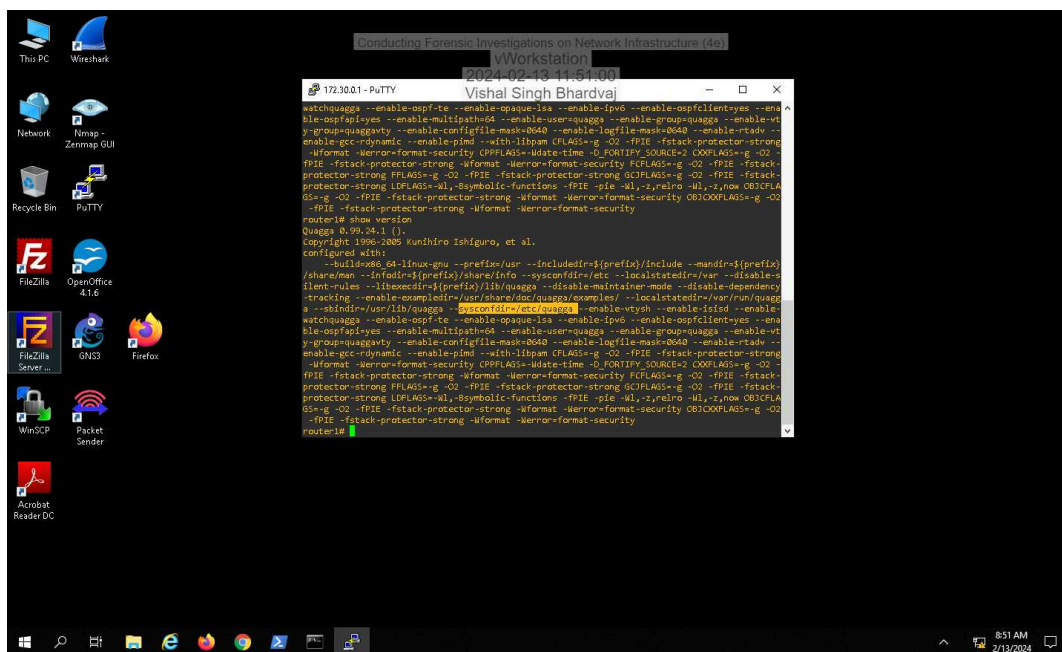


Part 2: Analyze a Router for Forensic Evidence

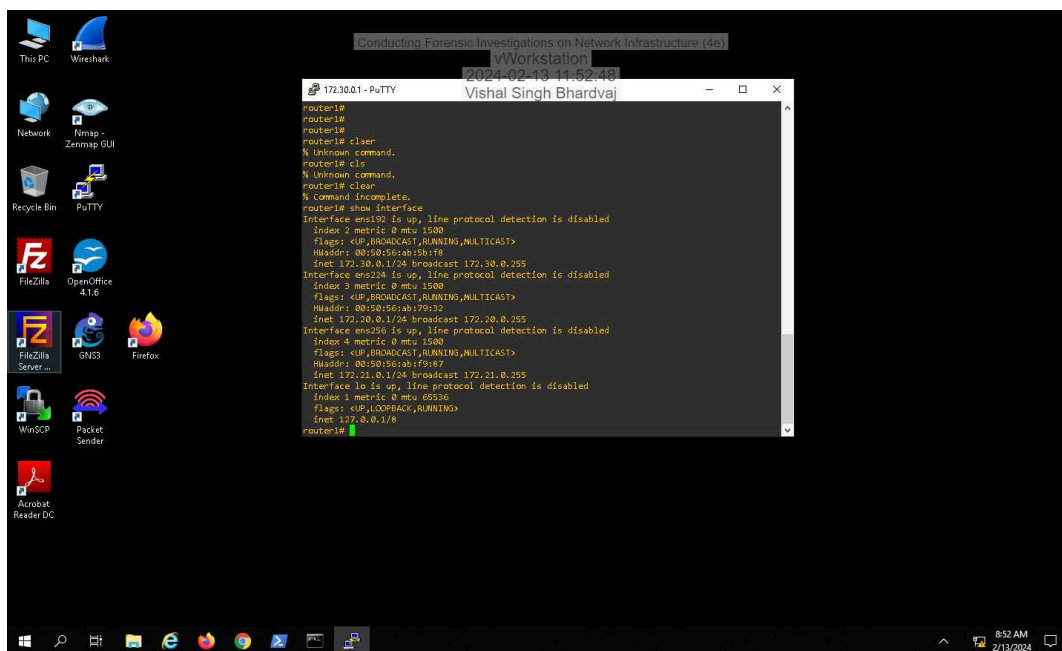
Conducting Forensic Investigations on Network Infrastructure (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

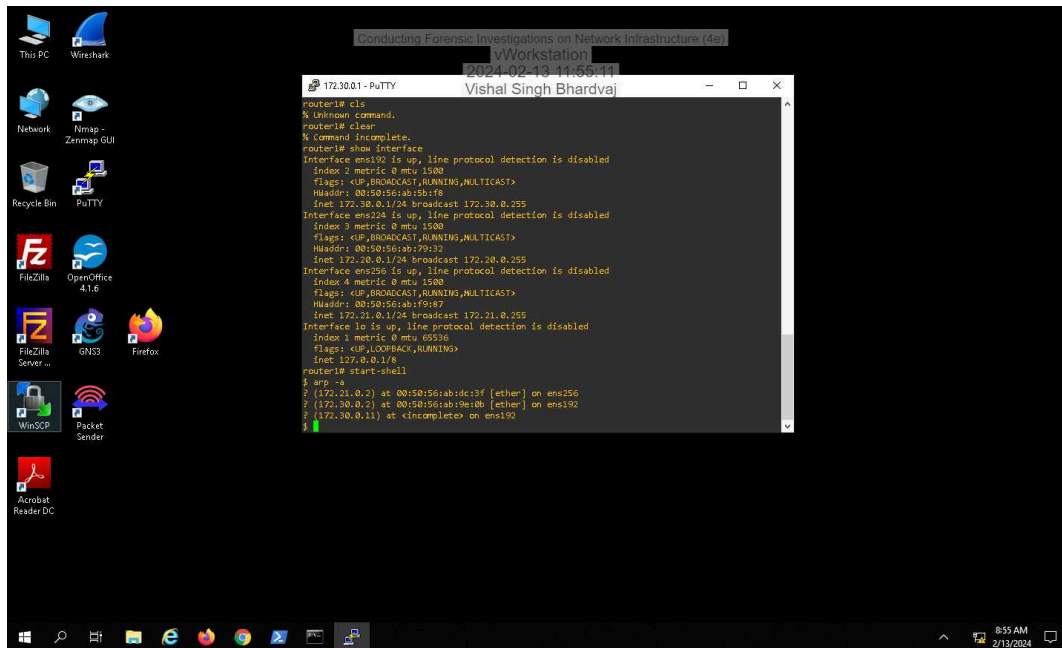
5. Make a screen capture showing the router's version output.



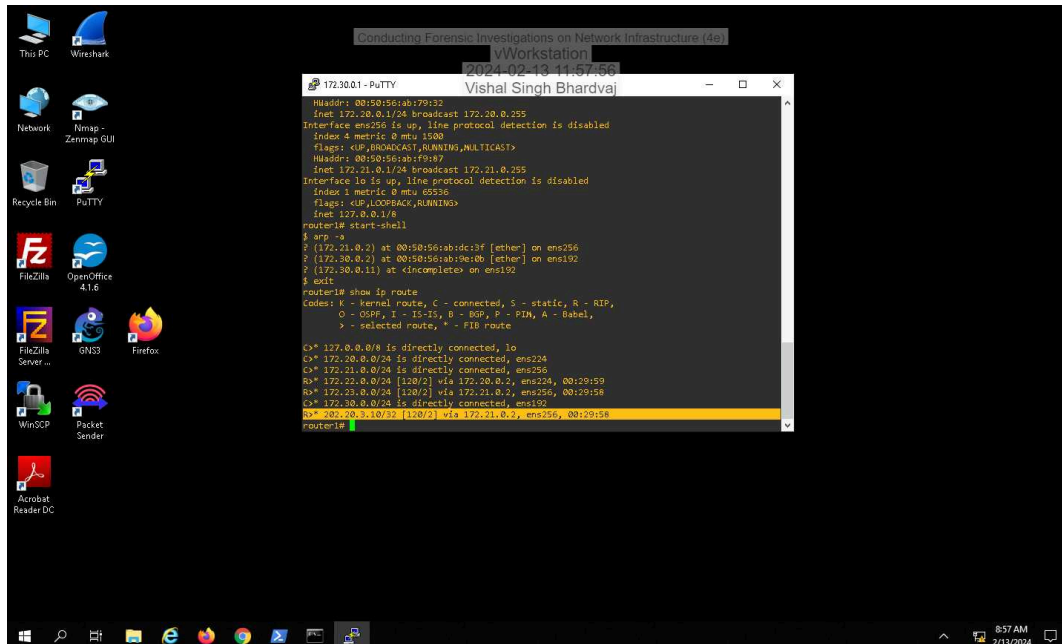
7. Make a screen capture showing the router's interface details.



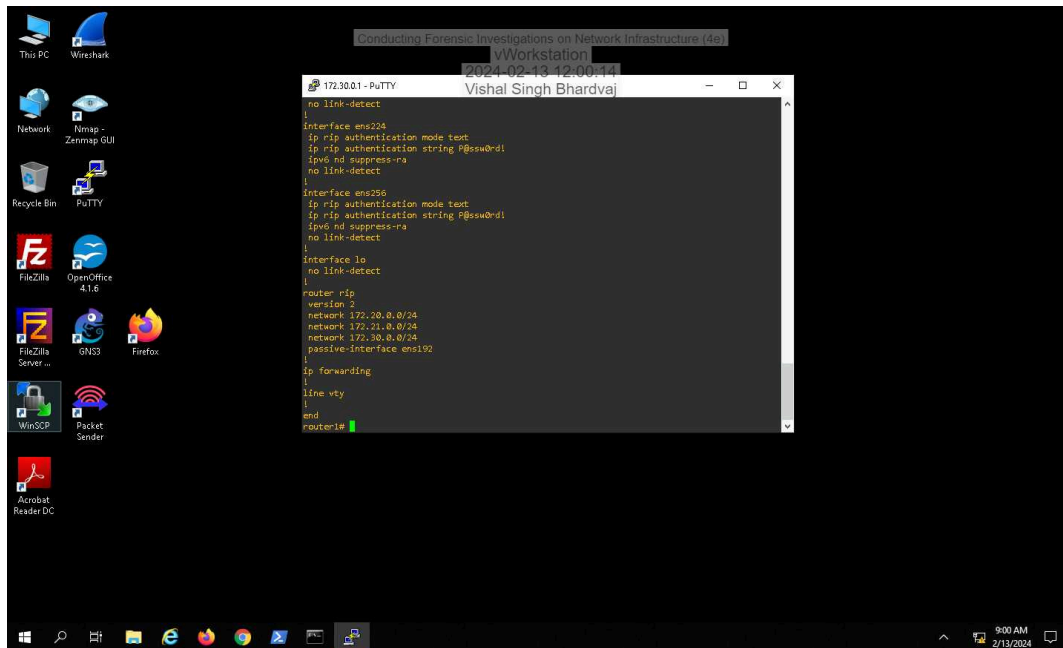
10. Make a screen capture showing the router1 ARP table.



13. Make a screen capture showing the IP routing table.



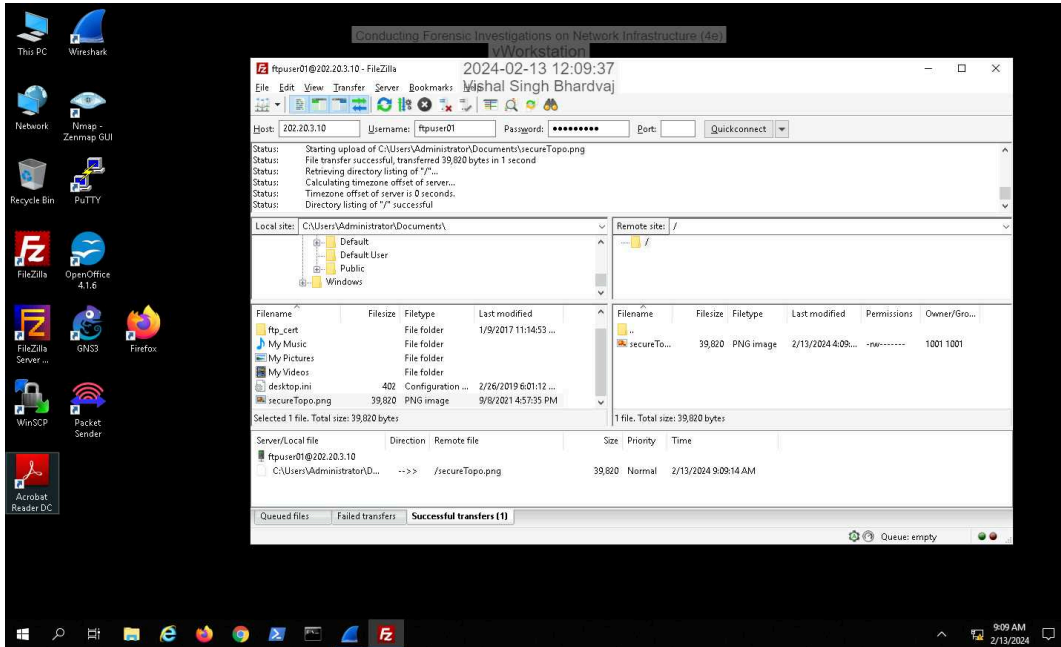
15. Make a screen capture showing the currently running configuration.



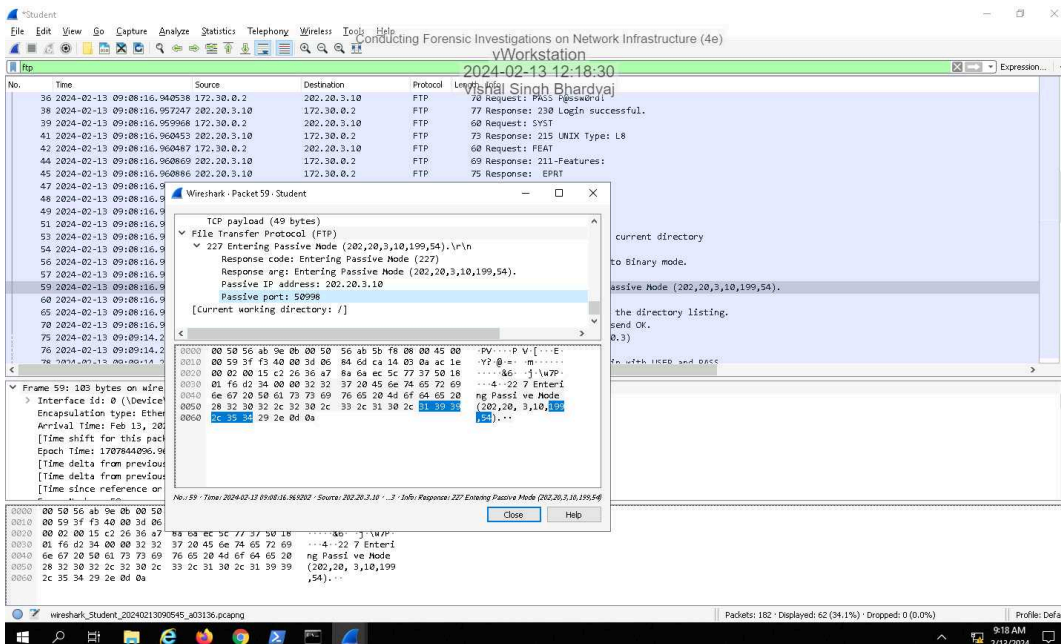
Section 2: Applied Learning

Part 1: Perform Advanced Packet Capture and Analysis

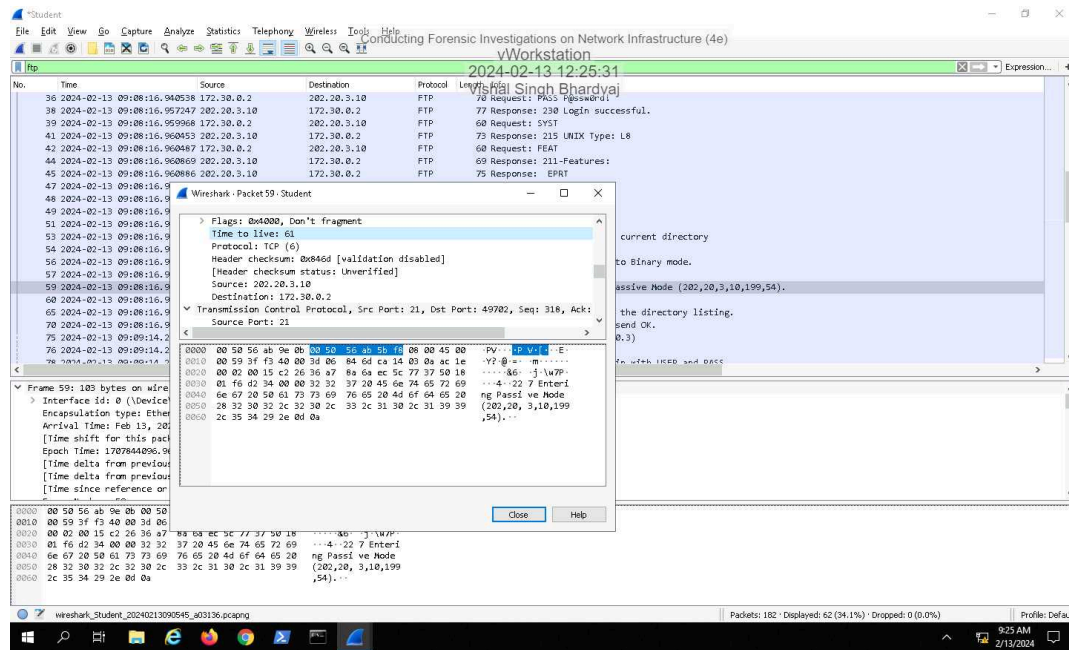
7. Make a screen capture showing the successful transfer of the secureTopo.png file.



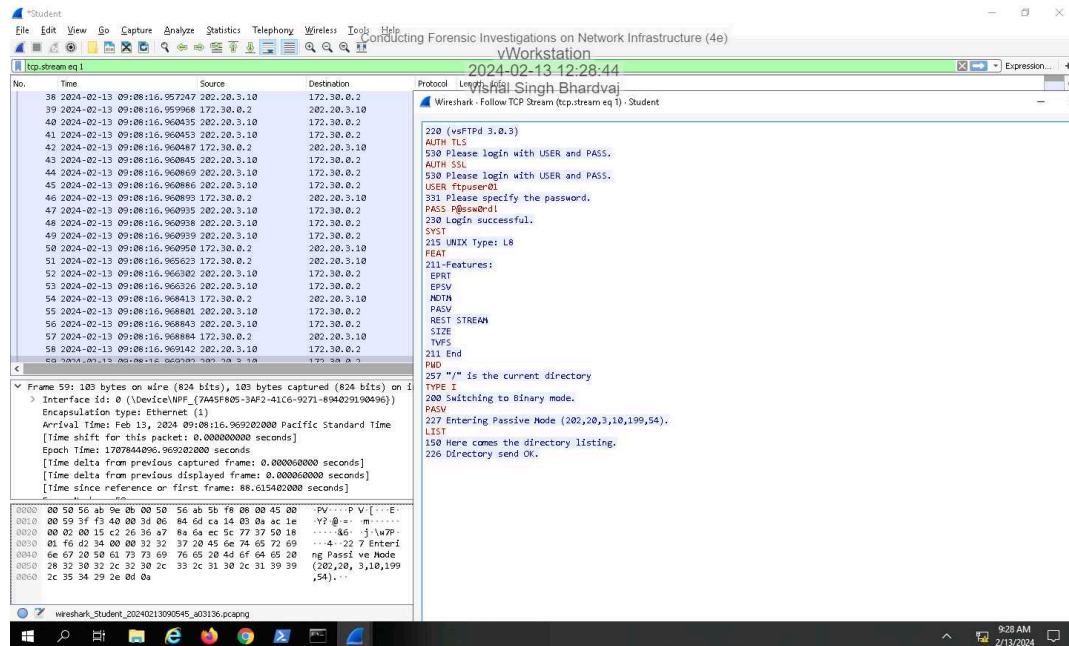
15. Make a screen capture showing the passive port specified by the FTP server in the Packet Details pane.



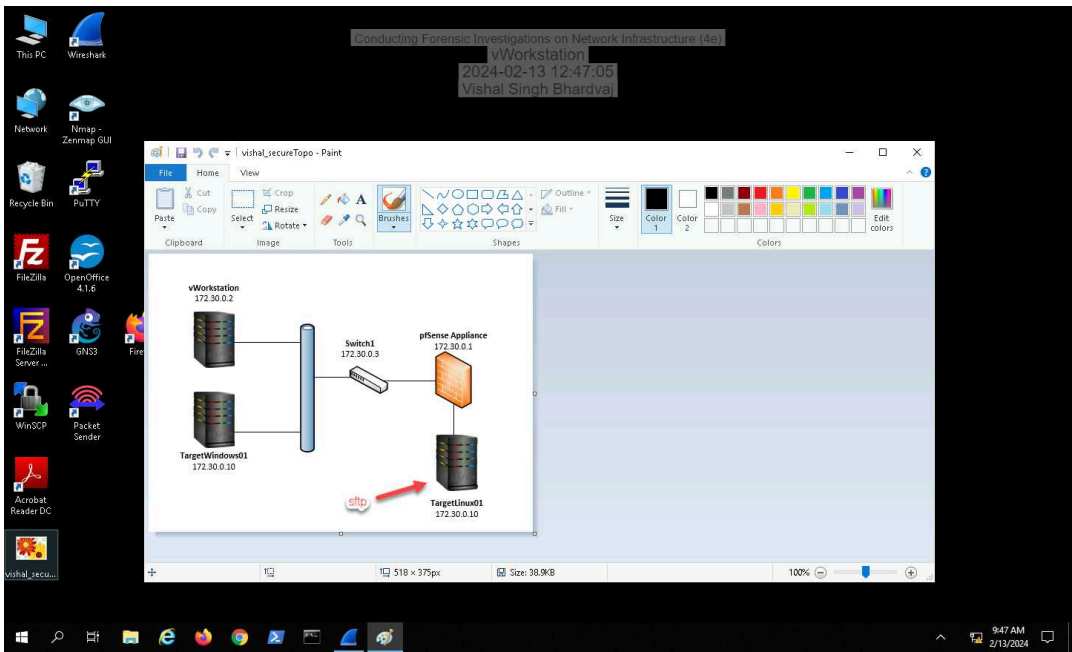
18. Make a screen capture showing the Time to live field in the Packet Details pane.



20. Make a screen capture showing the Follow TCP stream window.

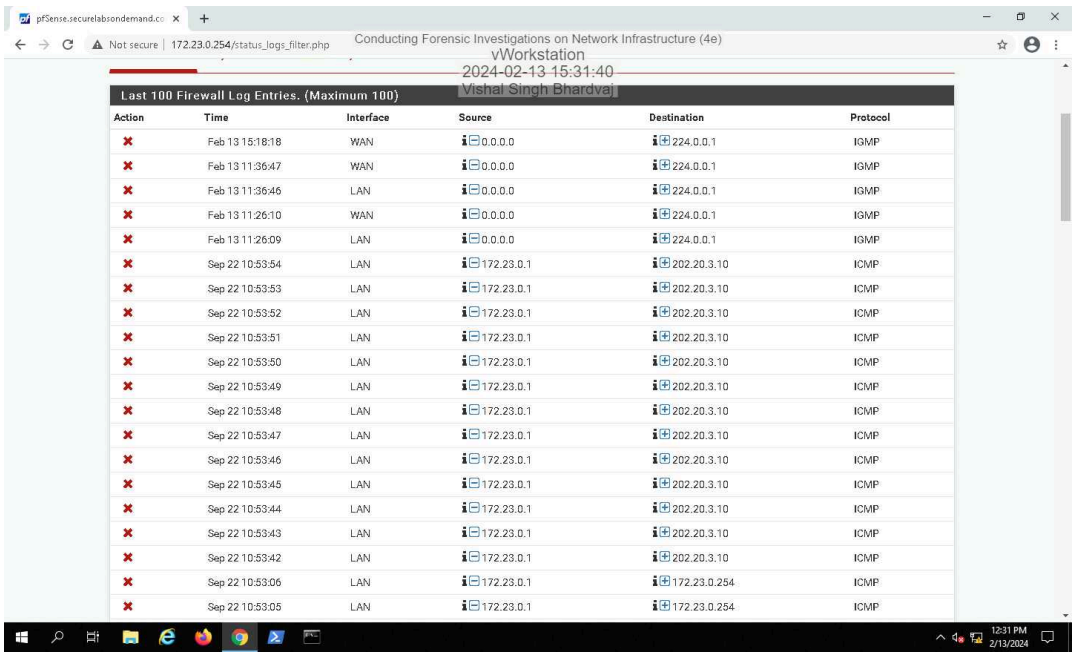


32. Make a screen capture showing the reconstituted PNG file.



Part 2: Analyze a Firewall for Forensic Evidence

9. Make a screen capture showing the entries in the firewall log.



Conducting Forensic Investigations on Network Infrastructure (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

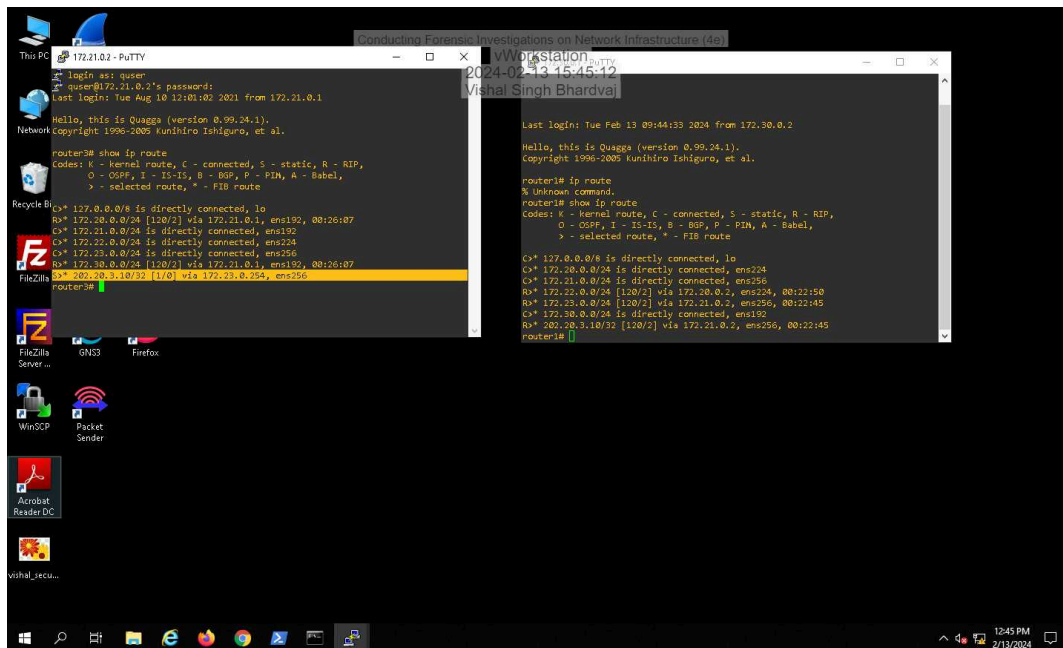
11. Make a screen capture showing the resolved entries in the firewall log.



Section 3: Challenge and Analysis

Part 1: Identify the Source of a Suspicious Route

Make a screen capture showing the non-RIP route that you discovered on the target router.



Part 2: Identify Suspicious Outgoing Connections

Record the destination IP address and Port number of the outgoing connection attempt.

Destination IP address :- 202.20.3.10

Destination Port number :- 1337

Port 1337 is usually used in gaming or proxy servers.