

# Conducting Forensic Investigations on Network Infrastructure (4e)

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

Student:

Jake Simpson

Email:

jaksimps@iu.edu

Time on Task:

0 hours, 39 minutes

Progress:

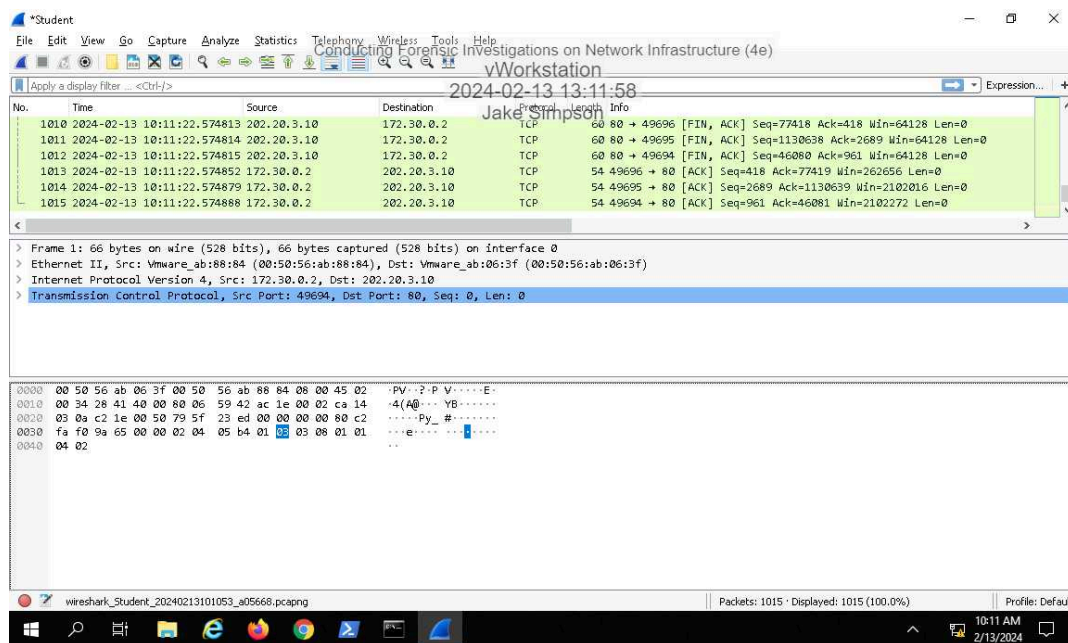
100%

Report Generated: Tuesday, February 13, 2024 at 1:48 PM

## Section 1: Hands-On Demonstration

### Part 1: Perform Packet Capture and Analysis

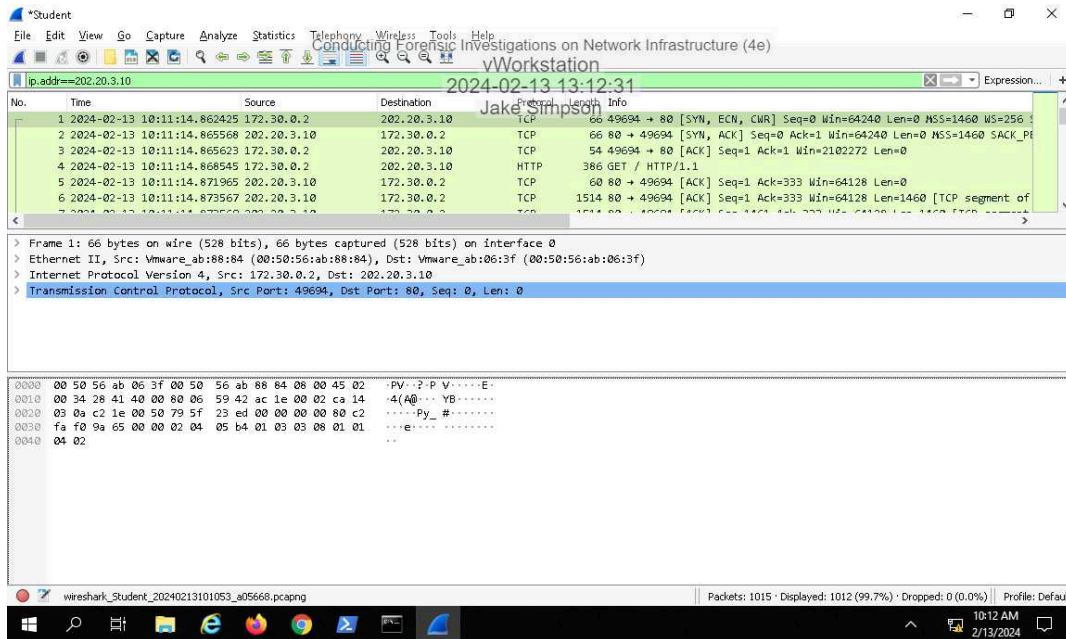
11. Make a screen capture showing the timestamp-sorted traffic.



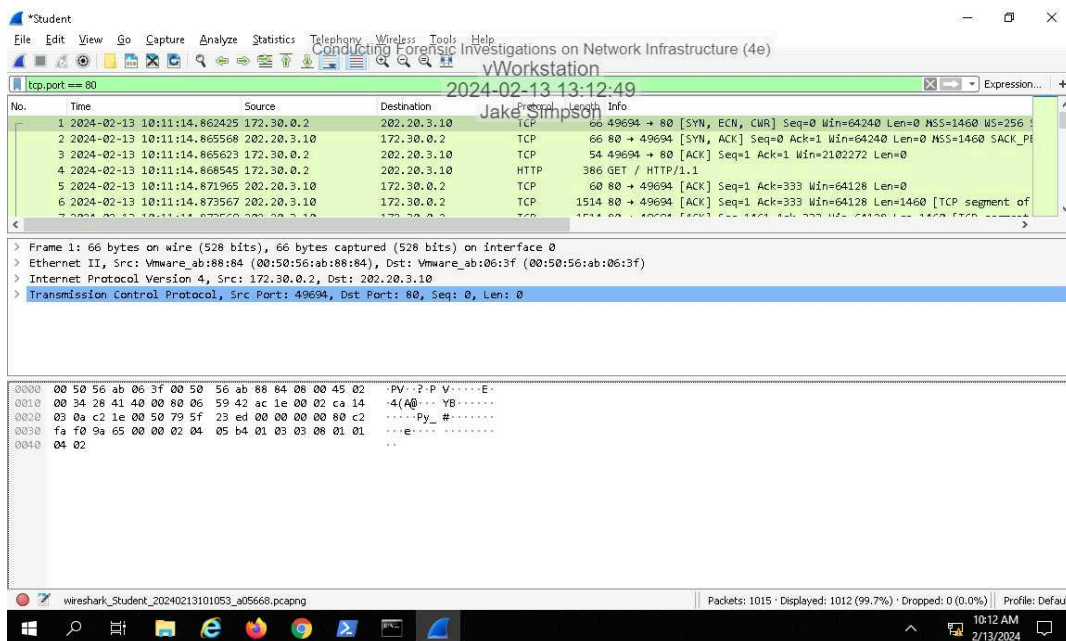
# Conducting Forensic Investigations on Network Infrastructure (4e)

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

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



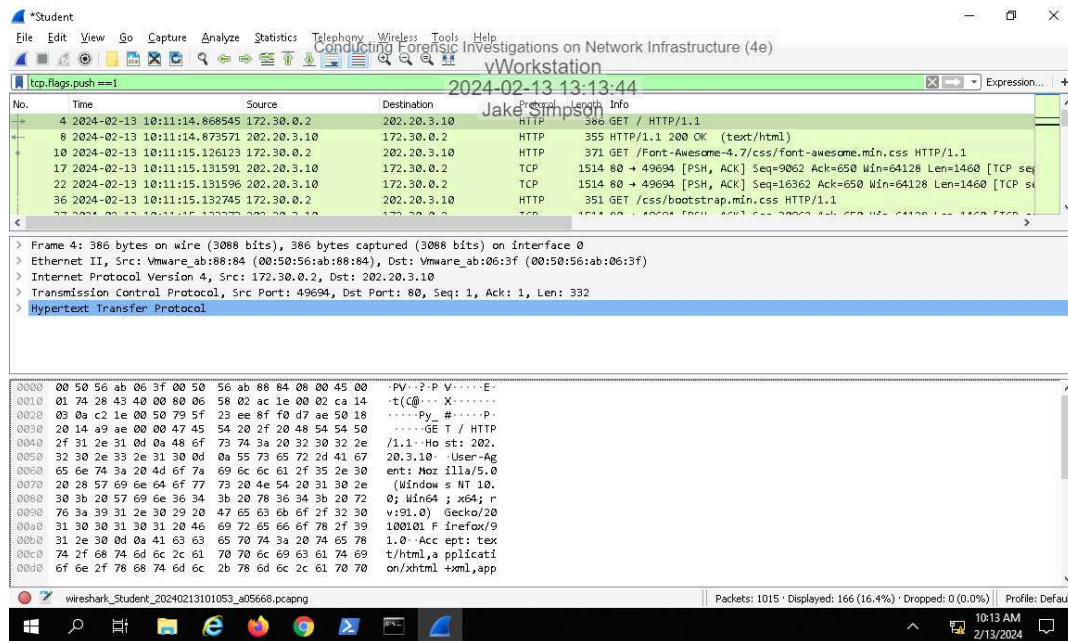
### 15. Make a screen capture showing the port-filtered traffic.



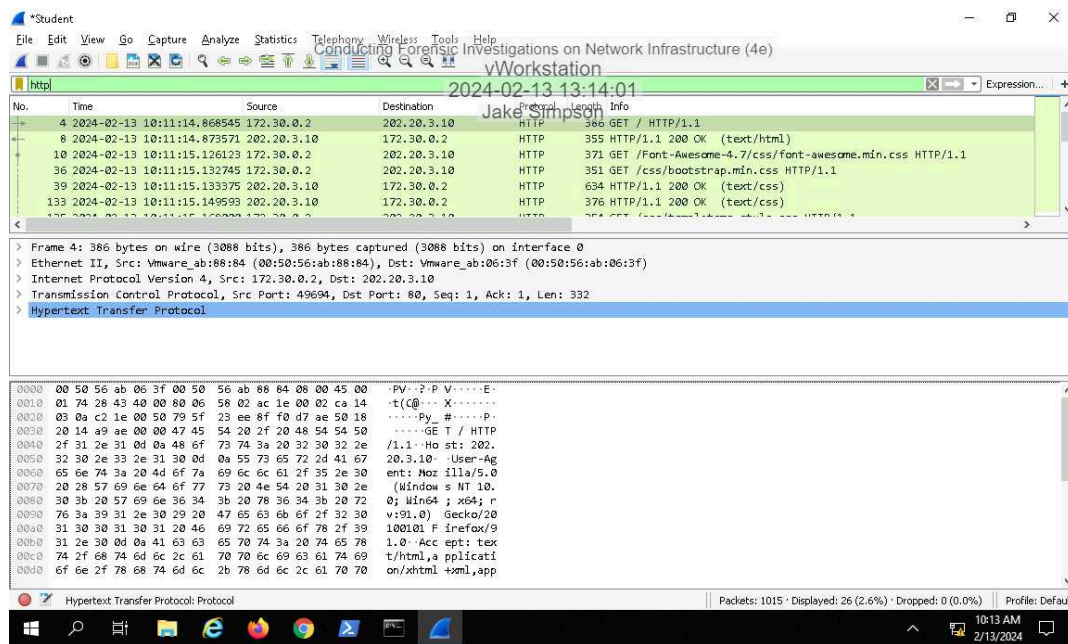
# Conducting Forensic Investigations on Network Infrastructure (4e)

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

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

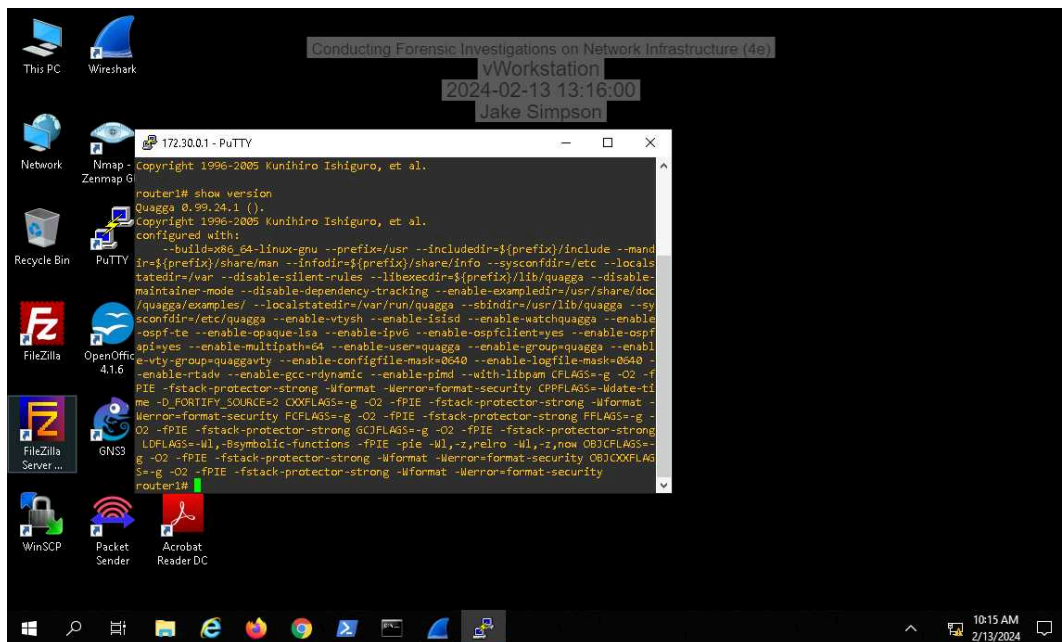


### 19. Make a screen capture showing the http-filtered traffic.

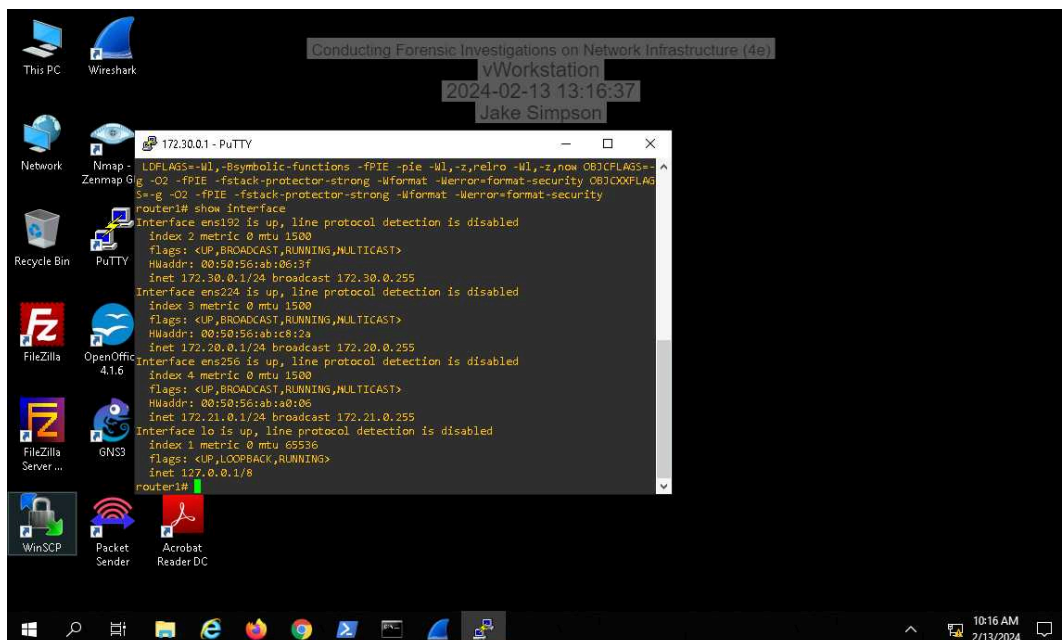


## Part 2: Analyze a Router for Forensic Evidence

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

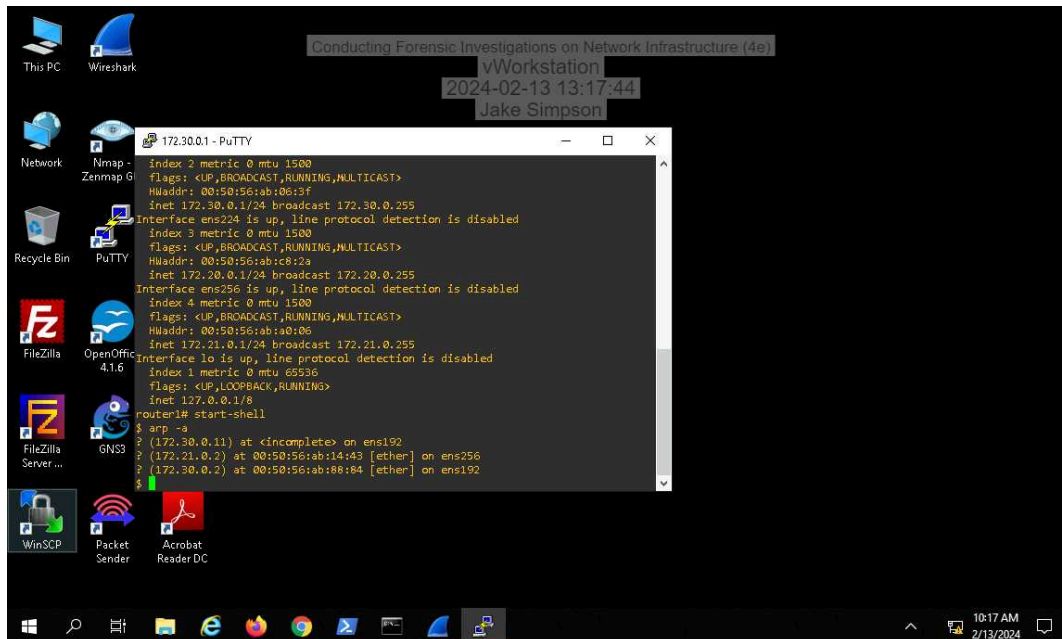


### 7. Make a screen capture showing the router's interface details.

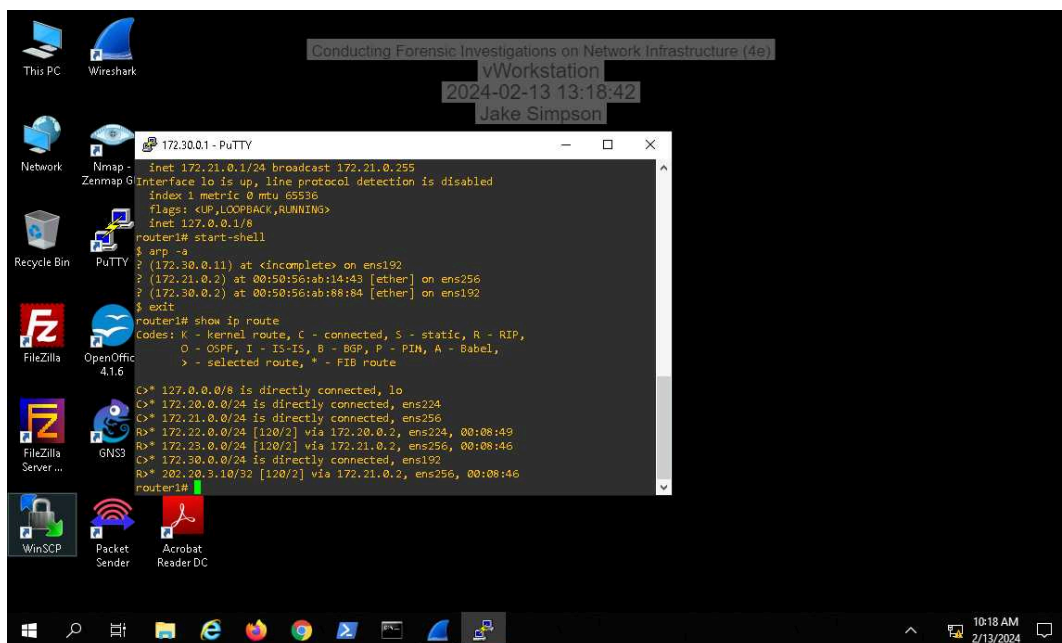




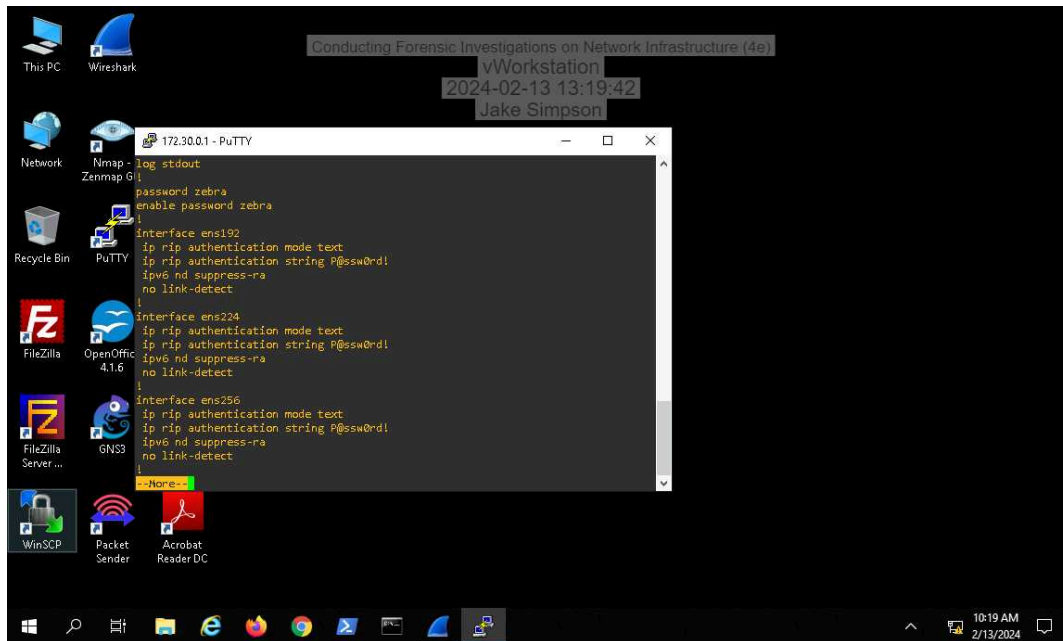
### 10. Make a screen capture showing the router1 ARP table.



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



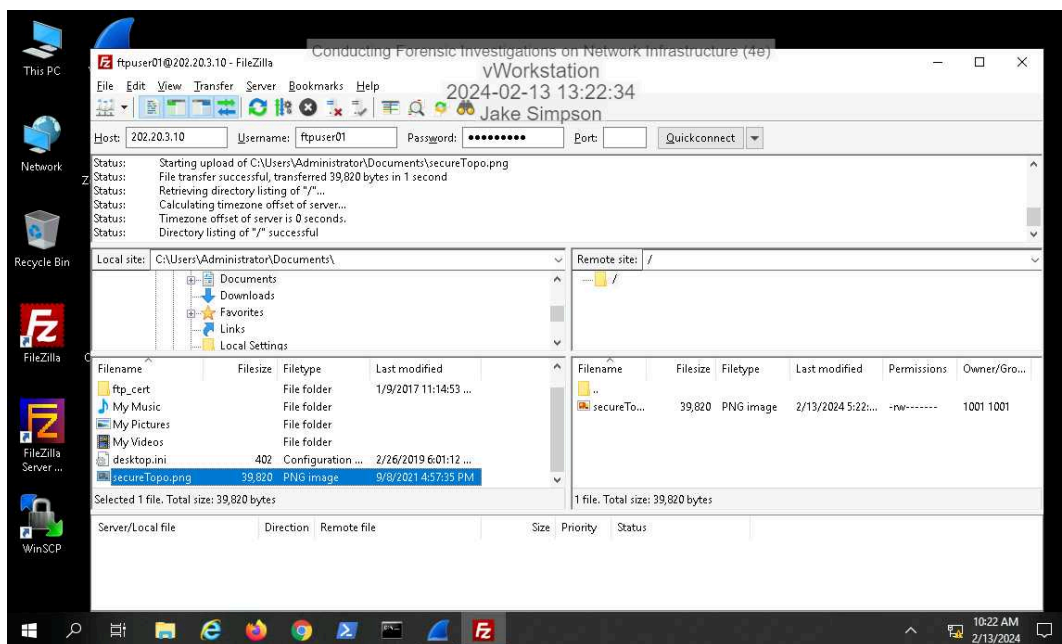
15. Make a screen capture showing the **currently running configuration**.



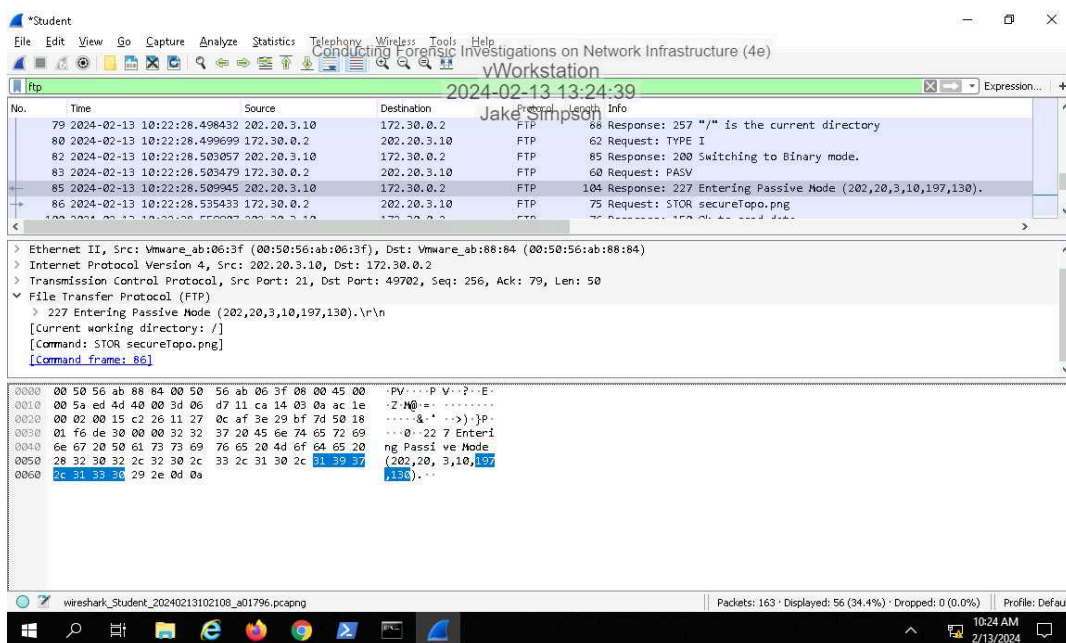
### Section 2: Applied Learning

#### Part 1: Perform Advanced Packet Capture and Analysis

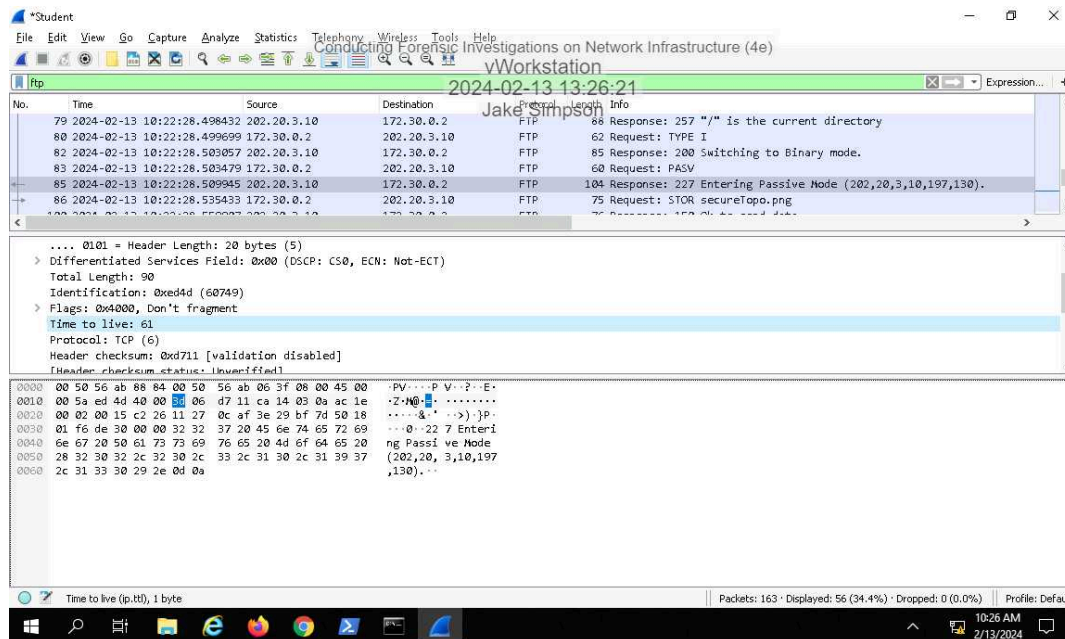
7. Make a screen capture showing the successful transfer of the secureTopo.png file.



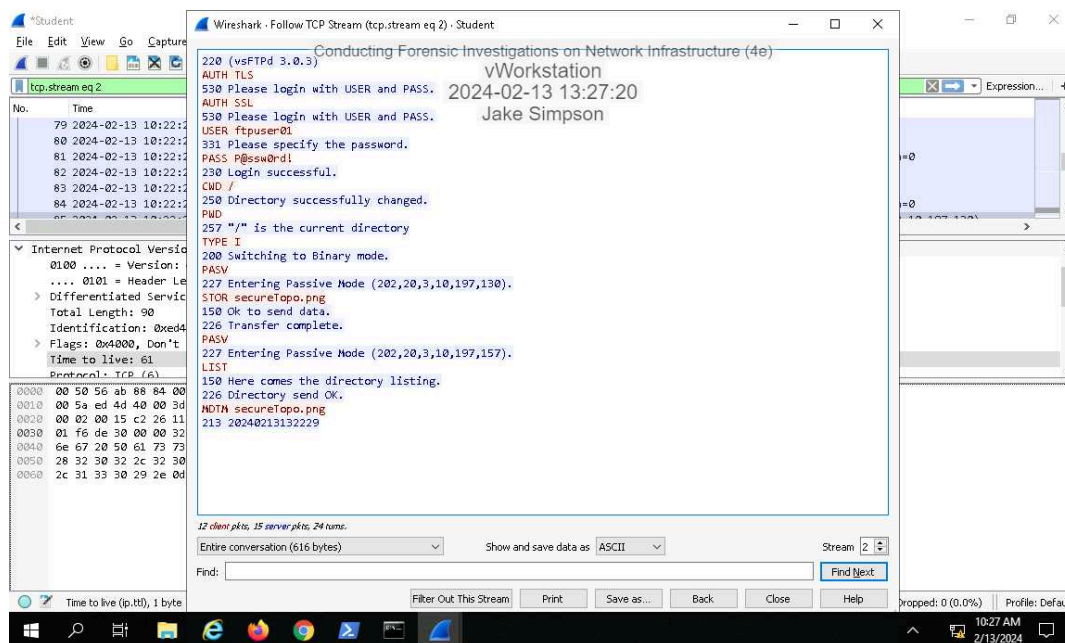
15. Make a screen capture showing the passive port specified by the FTP server in the Packet Details pane.



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

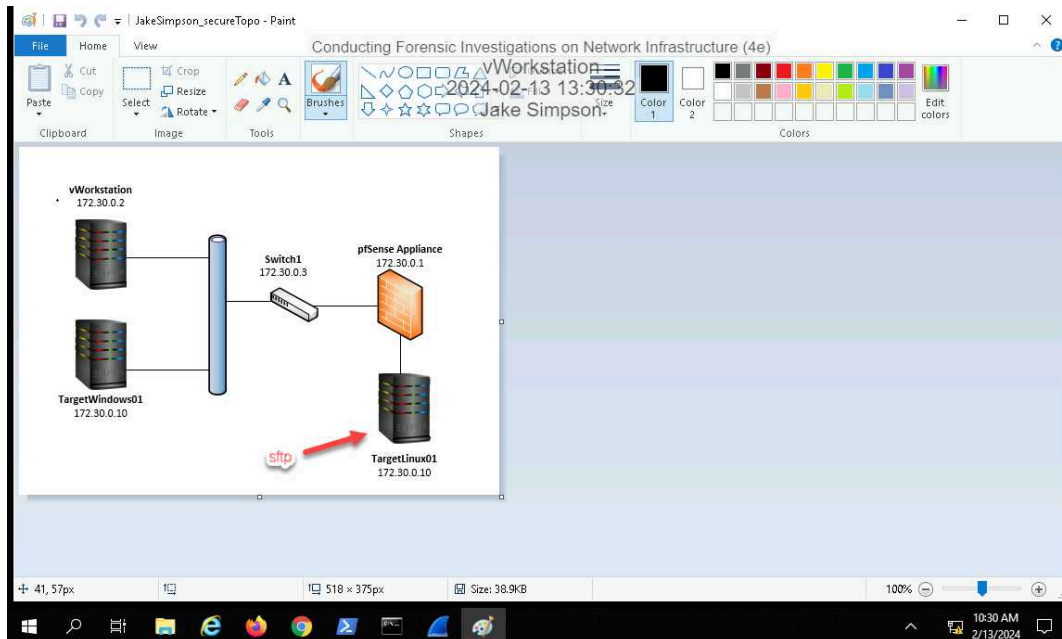


### 20. Make a screen capture showing the Follow TCP stream window.





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



## Part 2: Analyze a Firewall for Forensic Evidence

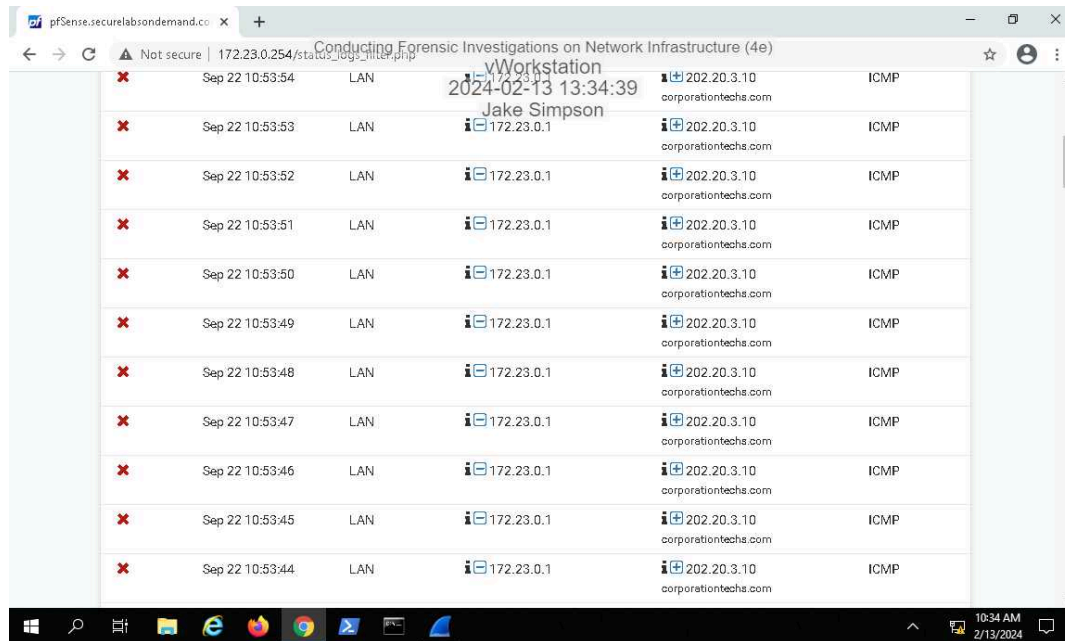
### 9. Make a screen capture showing the entries in the firewall log.

| Status | Time            | Source IP    | Source Port | Destination IP | Destination Port | Protocol |
|--------|-----------------|--------------|-------------|----------------|------------------|----------|
| ✗      | Sep 22 10:53:54 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:53 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:52 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:51 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:50 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:49 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:48 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:47 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:46 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:45 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:44 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:43 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:42 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:06 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:05 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:04 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:02 | 172.23.0.254 |             | LAN            |                  | ICMP     |
| ✗      | Sep 22 10:53:01 | 172.23.0.254 |             | LAN            |                  | ICMP     |

# Conducting Forensic Investigations on Network Infrastructure (4e)

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

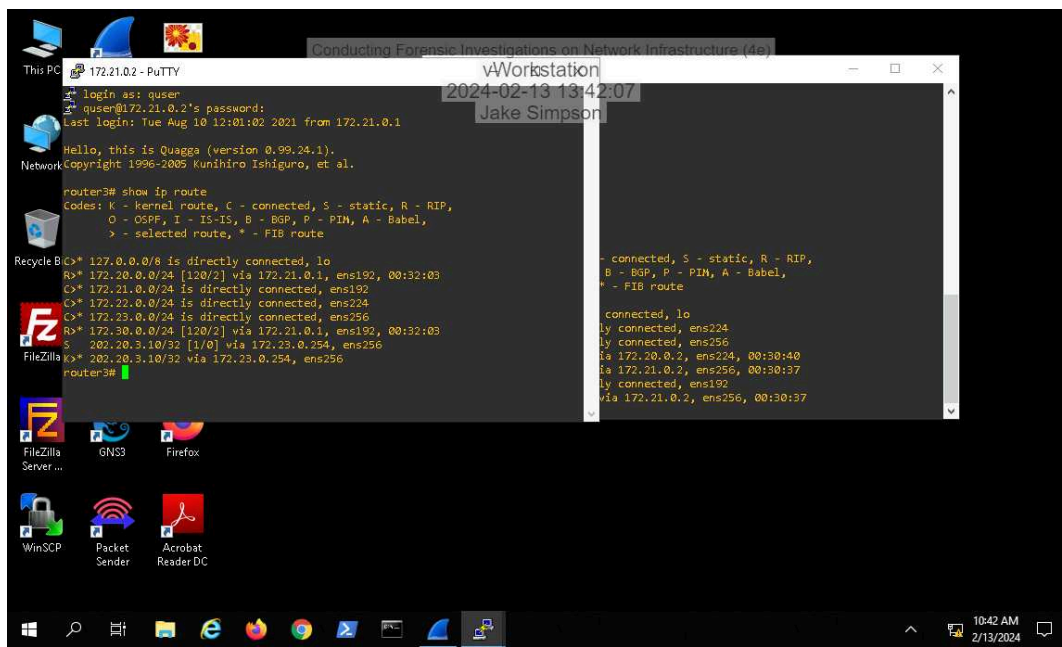
## 11. Make a screen capture showing the resolved entries in the firewall log.



### 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.

202.20.3.10:1337