

Student:	Email:
Samman Chouhan	schouhan1@hawk.iit.edu

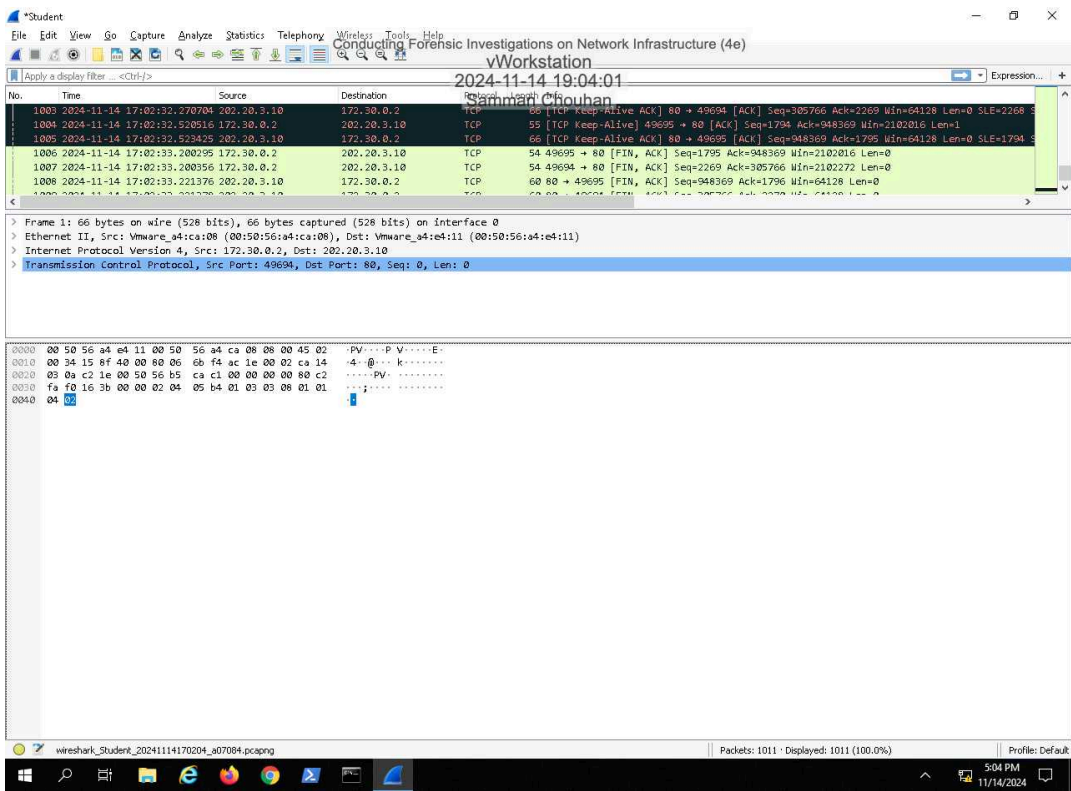
Time on Task:	Progress:
1 hour, 1 minute	100%

Report Generated: Thursday, November 14, 2024 at 10:49 PM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

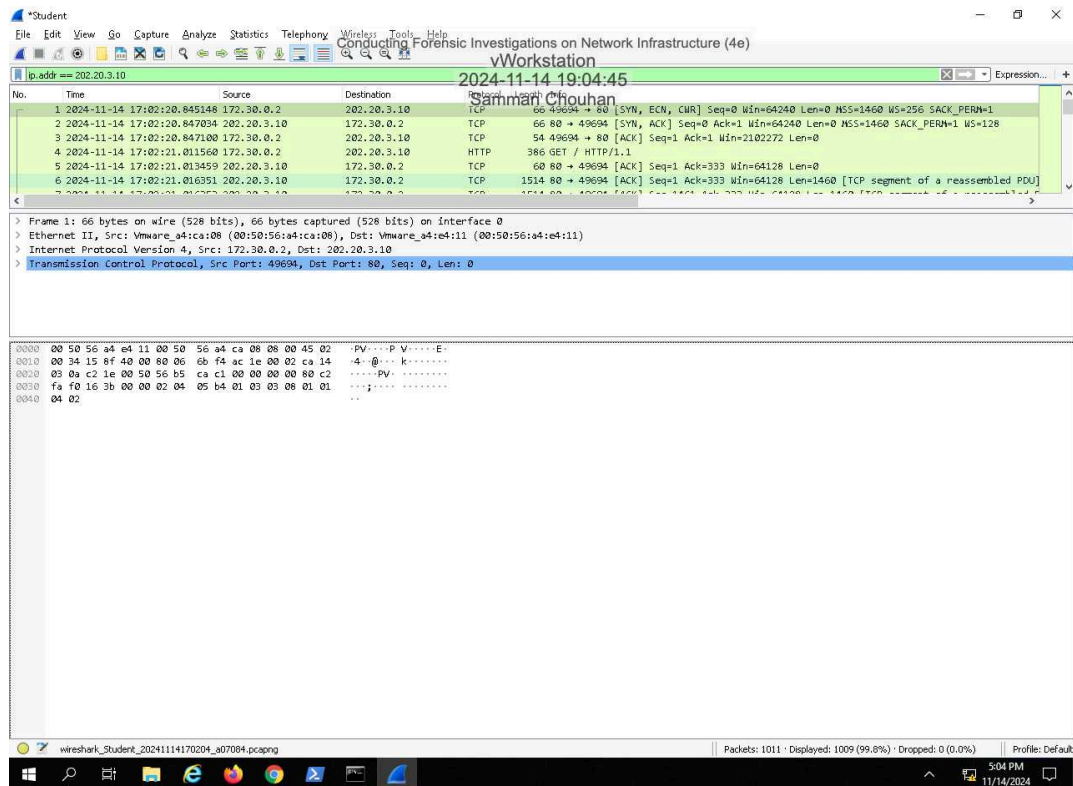
11. Make a screen capture showing the timestamp-sorted traffic.



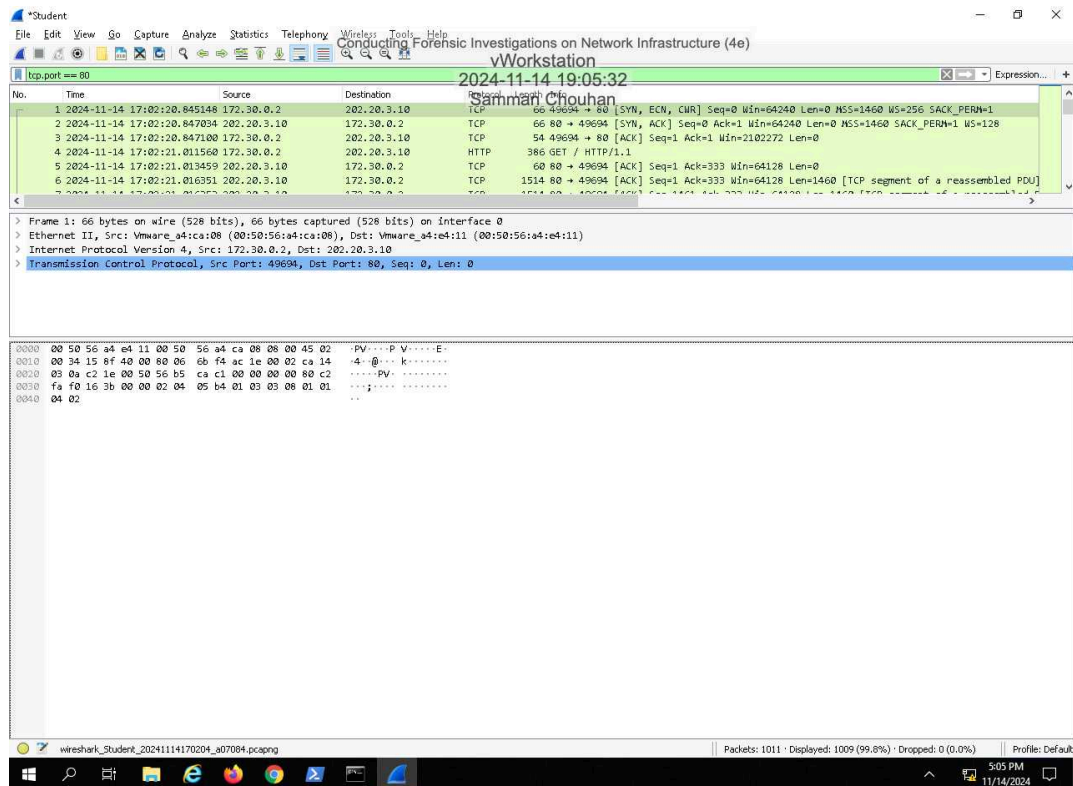
Conducting Forensic Investigations on Network Infrastructure (4e)

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

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



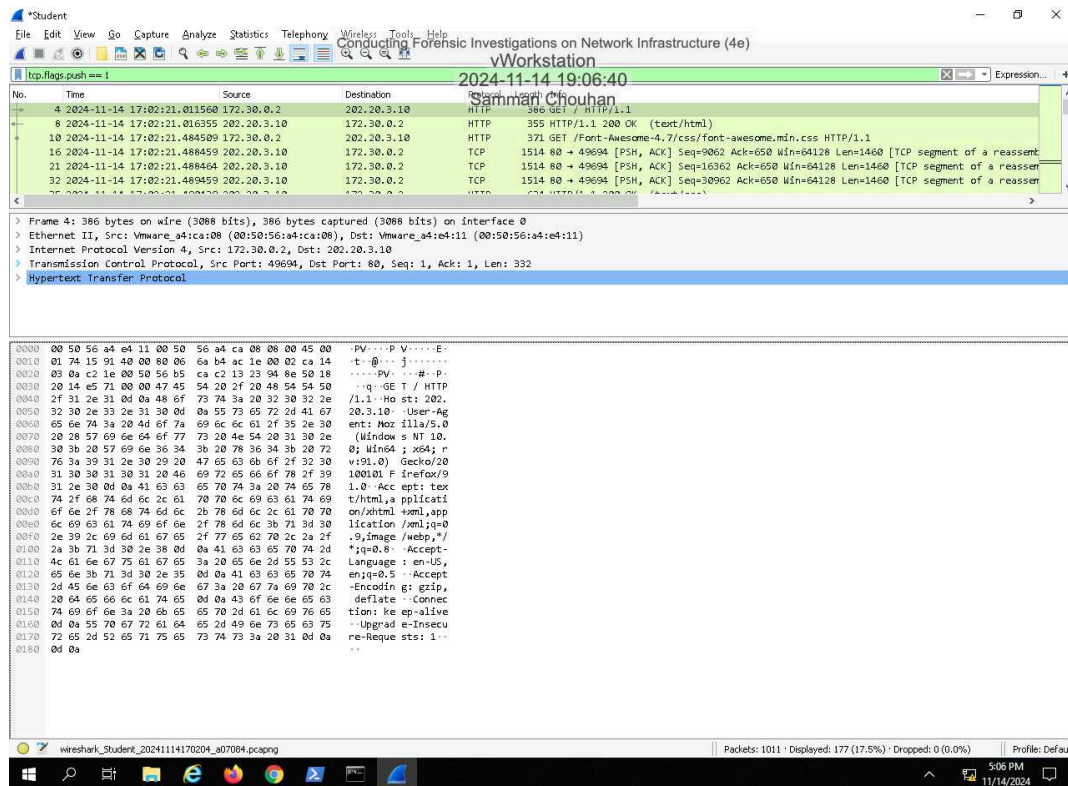
15. Make a screen capture showing the port-filtered traffic.



Conducting Forensic Investigations on Network Infrastructure (4e)

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

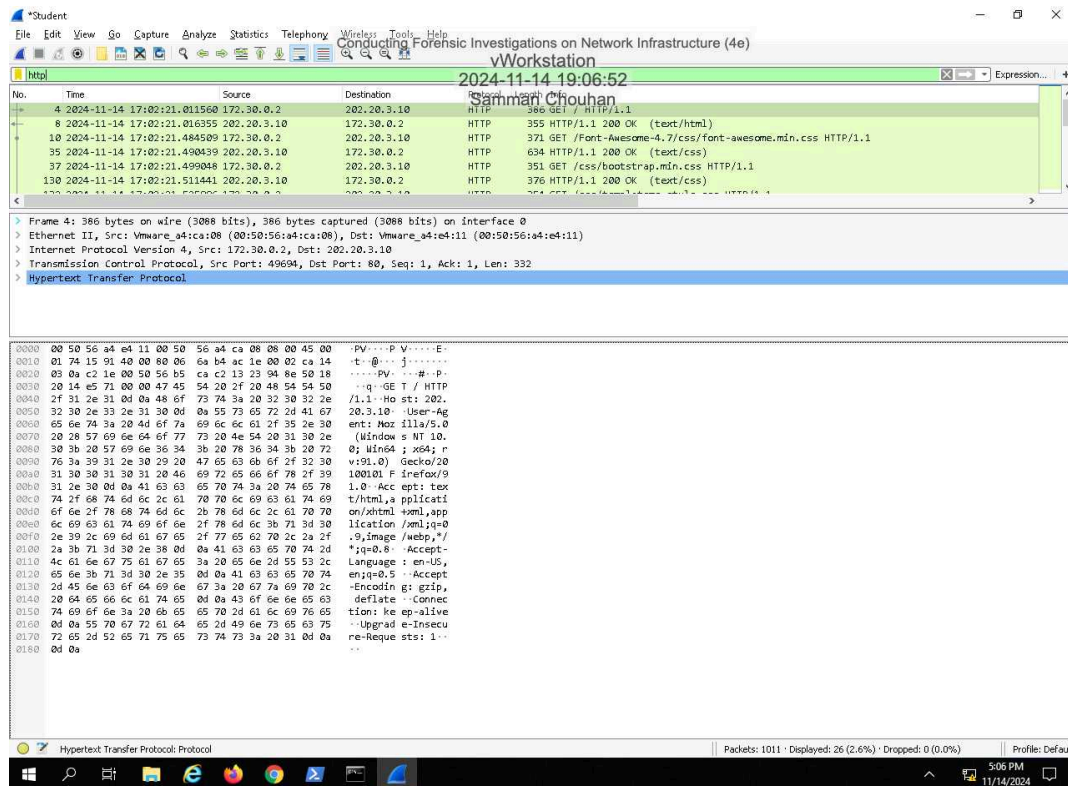
17. Make a screen capture showing the TCP push flag-filtered traffic.



Conducting Forensic Investigations on Network Infrastructure (4e)

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

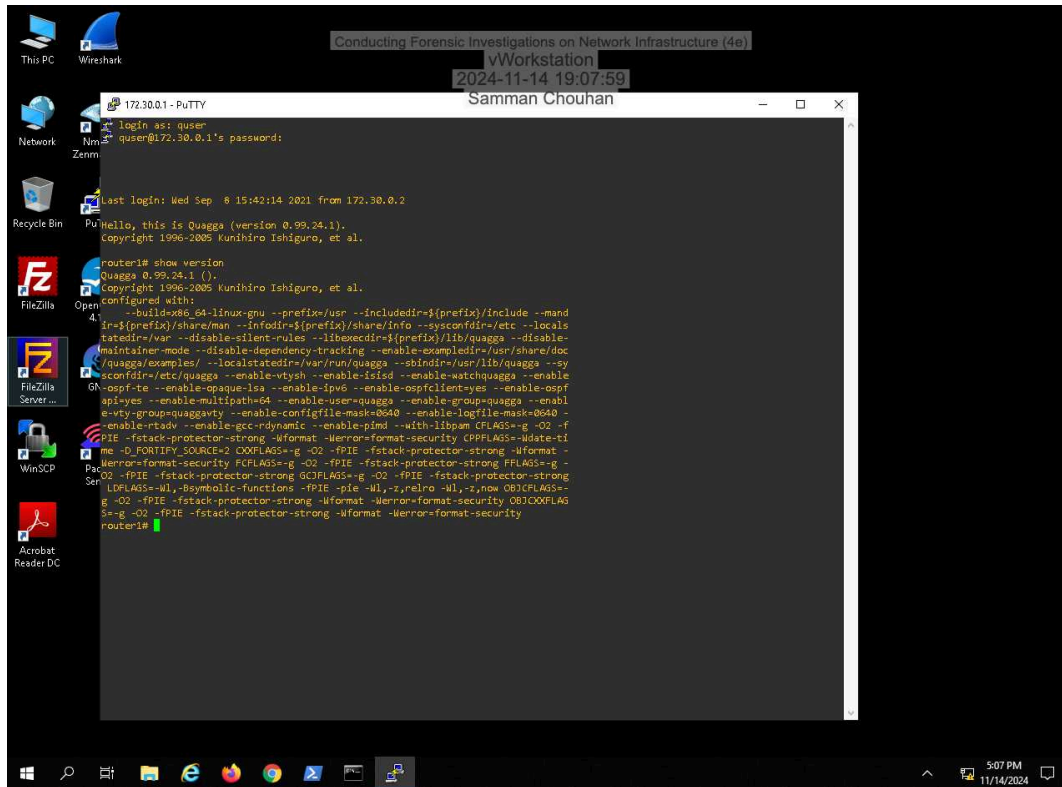
19. Make a screen capture showing the http-filtered traffic.



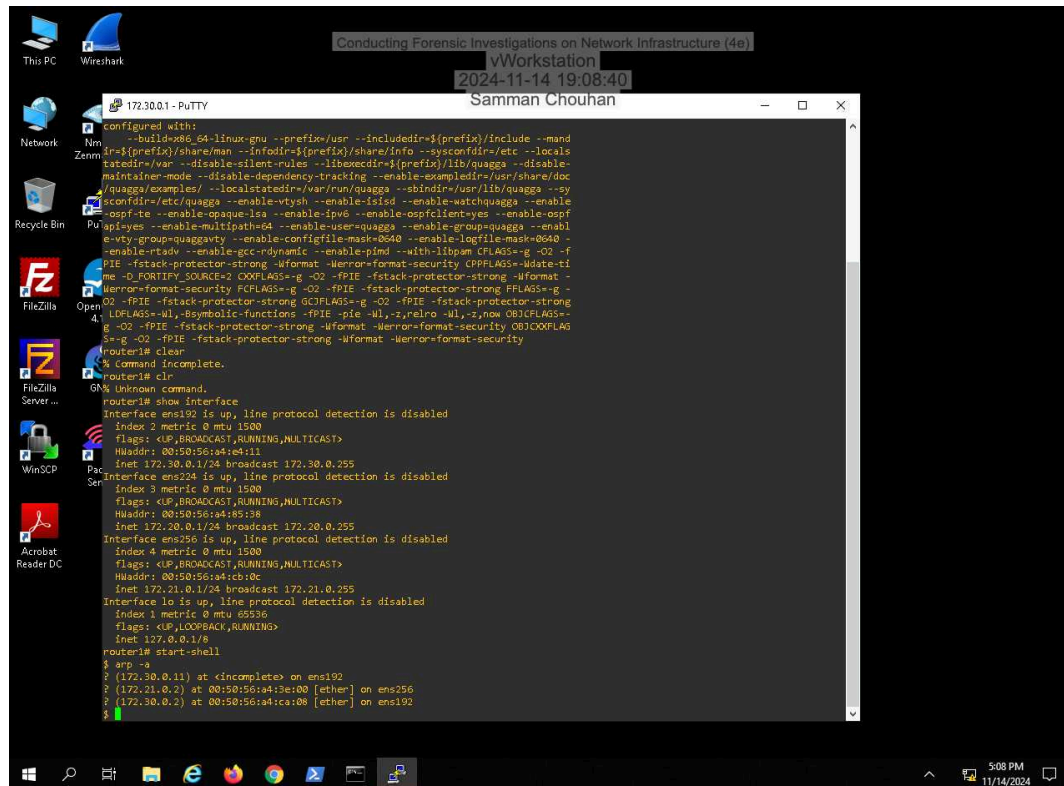
Part 2: Analyze a Router for Forensic Evidence

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

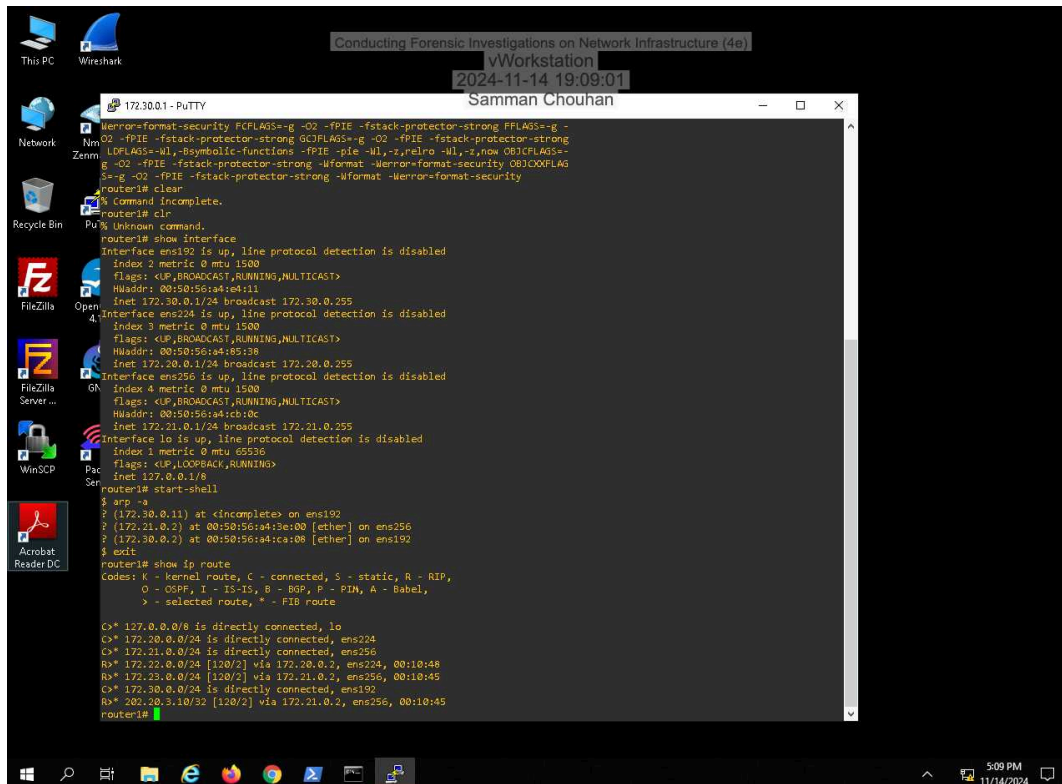
5. **Make a screen capture** showing the **router's version output**.



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



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



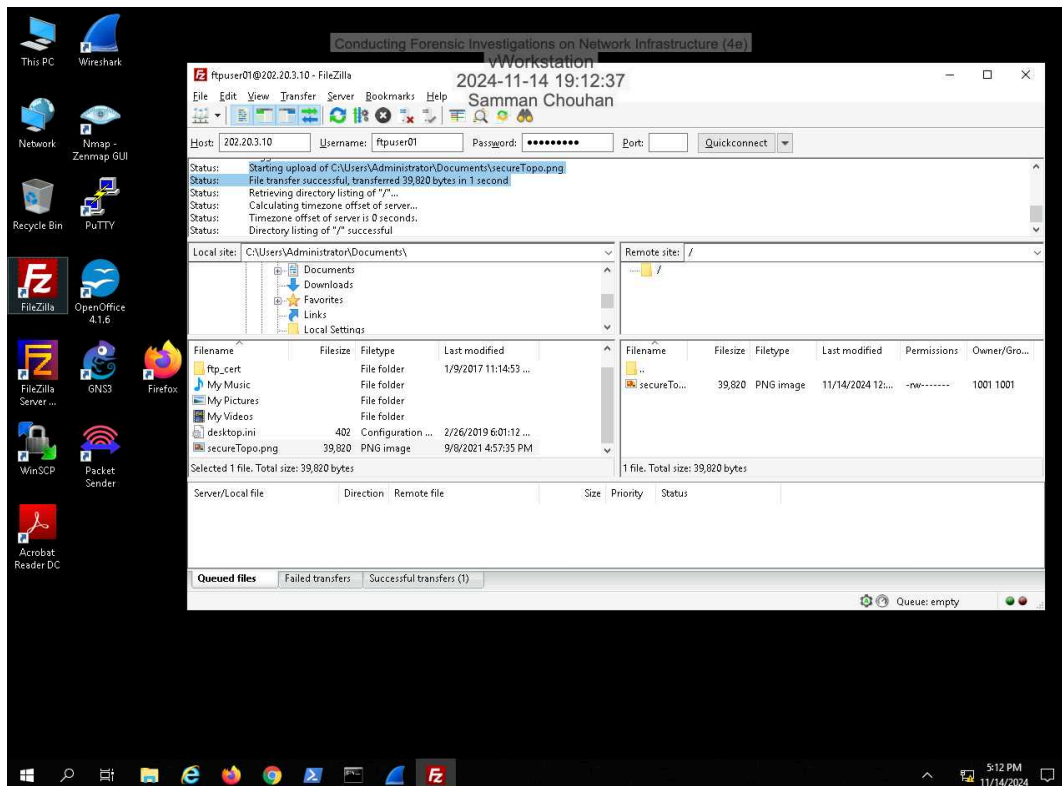
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 09

The screenshot shows a Windows 10 desktop environment. In the background, there's a vWorkstation window titled "vWorkstation" which contains a PuTTY terminal session connected to a device named "172.30.0.1". The terminal output shows the execution of several commands: "start-shell", "nmap -o", "show ip route", and "show running-config". The Nmap scan results indicate three open ports: 80 (HTTP), 22 (SSH), and 443 (HTTPS). The router configuration shows interfaces ens192, ens224, and ens256, each configured with IP addresses from the 172.30.0.x range and specific routing parameters. The desktop itself has various icons like "This PC", "Recycle Bin", "FileZilla", "WinSCP", and "Acrobat Reader DC". The taskbar at the bottom shows the Start button, search icon, and several application icons including File Explorer, Edge, Firefox, Chrome, and the vWorkstation application. The system clock indicates it's 5:09 PM on 11/14/2024.

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**.



Conducting Forensic Investigations on Network Infrastructure (4e)

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

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

The screenshot shows a Wireshark capture of an FTP session. The packet list at the top shows a sequence of packets. Packet 39 is selected, and its details are shown in the packet details pane. The details pane shows the 'File Transfer Protocol (FTP)' section expanded, displaying the '227 Entering Passive Mode (202,20,3,10,198,1)' response. The passive port is highlighted as 50689. The packet bytes pane shows the raw data of the response.

Passive FTP server port (ftp.passive.port), 5 bytes

Packets: 152 · Displayed: 150 (98.7%) · Dropped: 0 (0.0%)

Profile: Default

5:18 PM 11/14/2024

Conducting Forensic Investigations on Network Infrastructure (4e)

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

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The title bar indicates the window is titled "vWorkstation" and "Conducting Forensic Investigations on Network Infrastructure (4e)". The packet list pane shows a list of captured packets, with the selected packet (No. 41) having a Time to live field of 61. The packet details pane shows the expanded details of the selected packet, including the Time to live field (61) and the Transmission Control Protocol (TCP) details. The packet bytes pane shows the raw data of the packet, including the Time to live field (61) and the Transmission Control Protocol (TCP) details.

No.	Time	Source	Destination	Protocol	Length	Info
28	2024-11-14 17:12:03.545362	202.20.3.10	172.30.0.2	FTP	68	Response: REST STREAM
29	2024-11-14 17:12:03.545363	202.20.3.10	172.30.0.2	FTP	61	Response: SIZE
30	2024-11-14 17:12:03.545383	172.30.0.2	202.20.3.10	TCP	54	49699 → 21 [ACK] Seq=65 Ack=237 Win=2102016 Len=0
31	2024-11-14 17:12:03.545425	202.20.3.10	172.30.0.2	FTP	61	Response: TVFS
32	2024-11-14 17:12:03.545426	202.20.3.10	172.30.0.2	FTP	63	Response: 211 End
33	2024-11-14 17:12:03.545441	172.30.0.2	202.20.3.10	TCP	54	49699 → 21 [ACK] Seq=65 Ack=253 Win=2102016 Len=0
34	2024-11-14 17:12:03.550972	172.30.0.2	202.20.3.10	FTP	59	Request: PWD
35	2024-11-14 17:12:03.551712	202.20.3.10	172.30.0.2	FTP	88	Response: 257 "/" is the current directory
36	2024-11-14 17:12:03.555697	172.30.0.2	202.20.3.10	FTP	62	Request: TYPE I
37	2024-11-14 17:12:03.556730	202.20.3.10	172.30.0.2	FTP	85	Response: 200 Switching to Binary mode.
38	2024-11-14 17:12:03.556872	172.30.0.2	202.20.3.10	FTP	60	Request: PASV
39	2024-11-14 17:12:03.558162	202.20.3.10	172.30.0.2	FTP	102	Response: 227 Entering Passive Mode (202,20,3,10,198,1).
40	2024-11-14 17:12:03.566078	172.30.0.2	202.20.3.10	FTP	60	Request: LIST
41	2024-11-14 17:12:03.566693	172.30.0.2	202.20.3.10	TCP	66	49700 → 50689 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1

0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 88
Identification: 0x3c6f (15471)
> Flags: 0x4000, Don't fragment
Time to live: 61
Protocol: TCP (6)
Header checksum: 0x87f2 [validation disabled]
[Header checksum status: Unverified]
Source: 202.20.3.10
Destination: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49699, Seq: 318, Ack: 84, Len: 48
> File Transfer Protocol (FTP)

0000 00 50 50 a4 c9 00 50 50 a4 e4 11 00 00 45 00 PV....P V....E-
0010 00 58 3c 6f 40 00 06 87 f2 ca 14 03 0a ac 1e >Xco@.....
0020 00 02 00 15 c2 23 53 b9 c5 be 89 77 96 80 50 18#S....W..P.
0030 01 f6 f3 71 00 00 32 32 37 20 45 6a 74 65 72 69 ...q..22 7 Enter
0040 6e 67 20 50 61 73 73 69 76 65 20 4d 6f 64 65 20 ng Passi ve Mode
0050 28 32 30 32 2c 32 30 2c 33 2c 31 30 2c 31 39 38 (202,20,3,10,198
0060 2c 31 29 2e 0d 0a ,1)..

Time to live (p.ttl), 1 byte

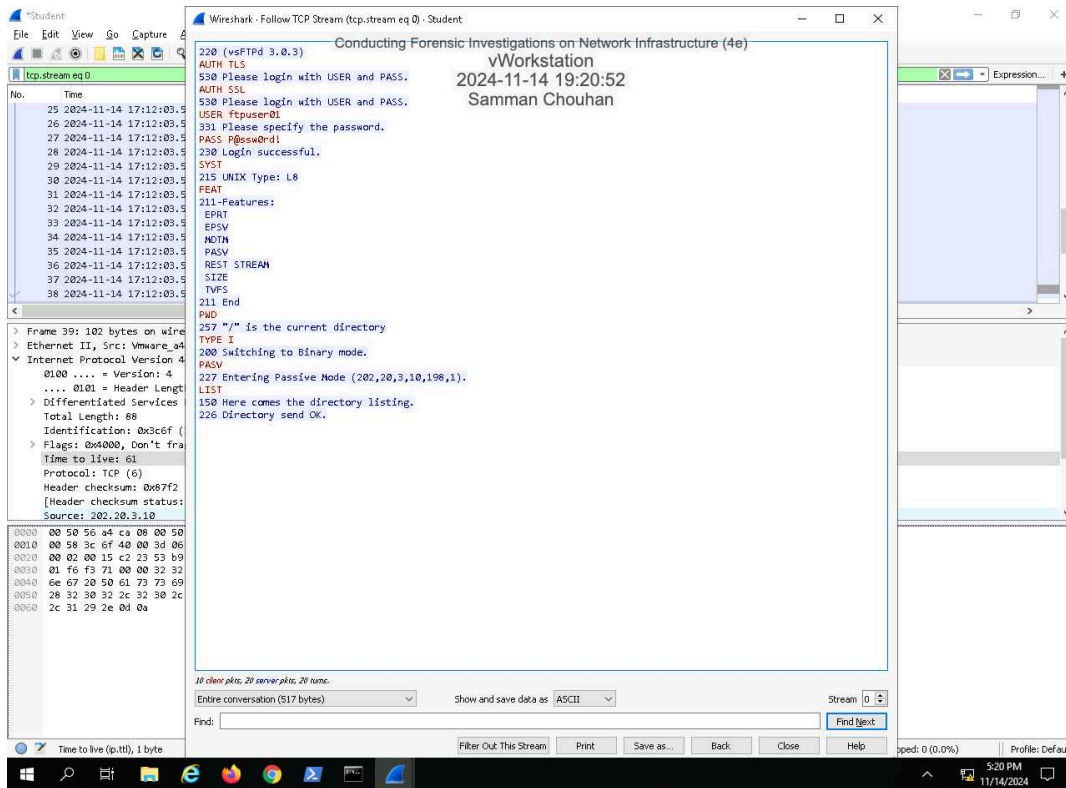
Packets: 152 · Displayed: 150 (98.7%) · Dropped: 0 (0.0%) · Profile: Default

5:18 PM
11/14/2024

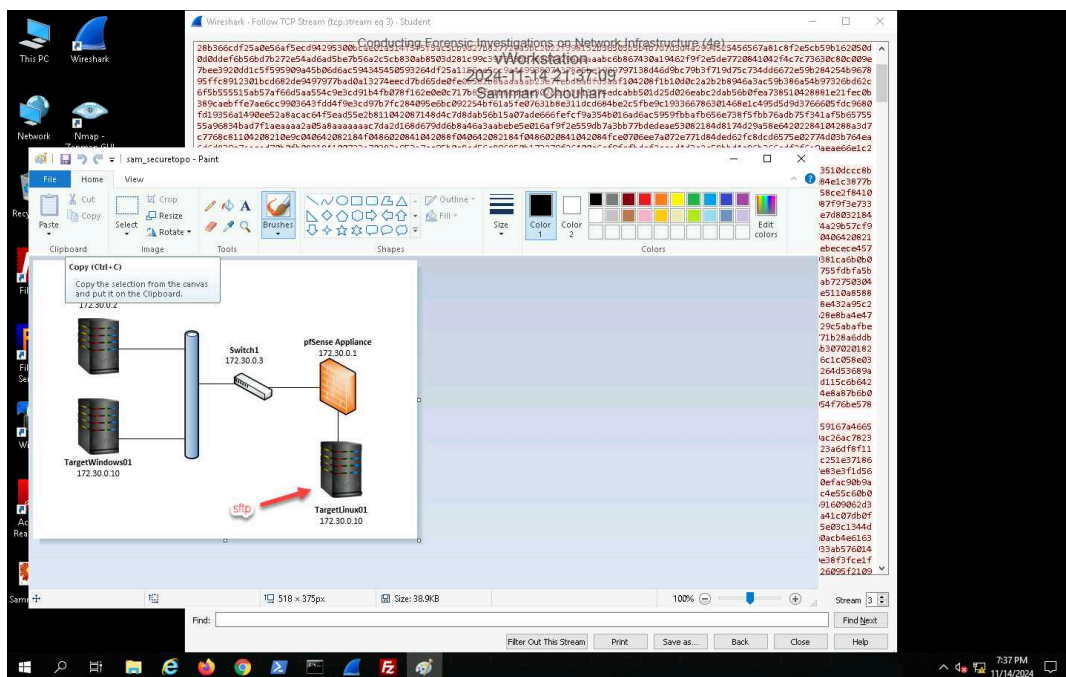
Conducting Forensic Investigations on Network Infrastructure (4e)

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

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

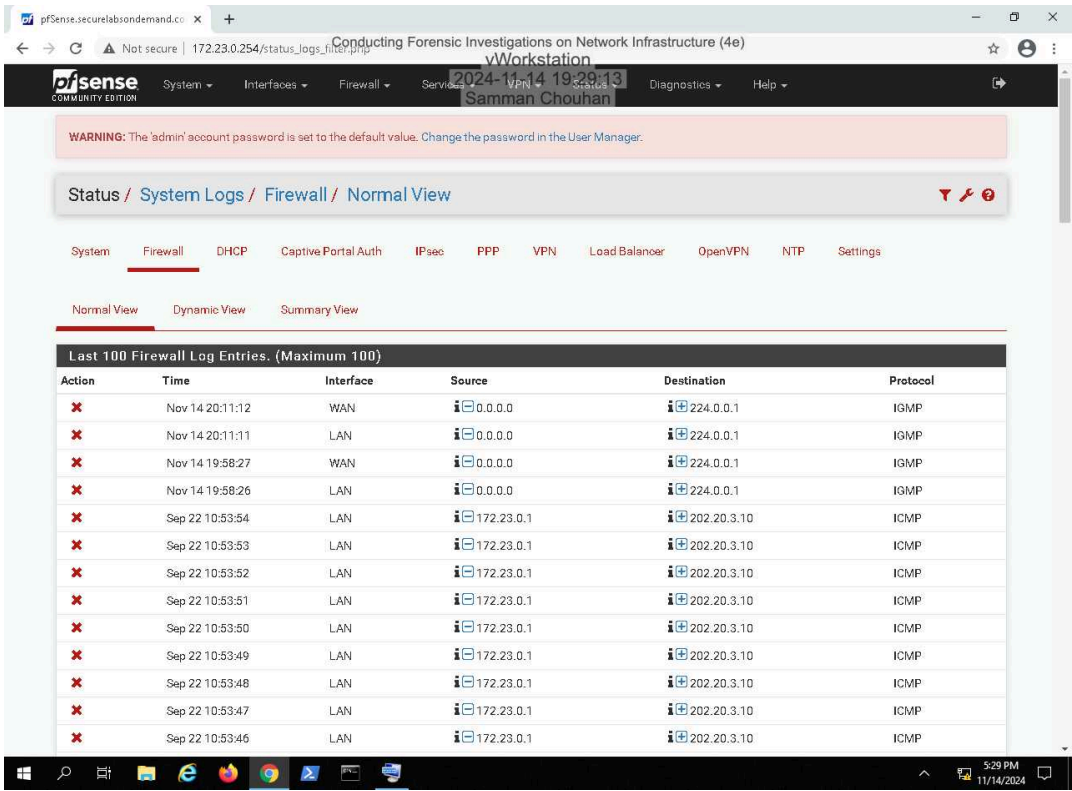


32. Make a screen capture showing the reconstituted PNG file.



Part 2: Analyze a Firewall for Forensic Evidence

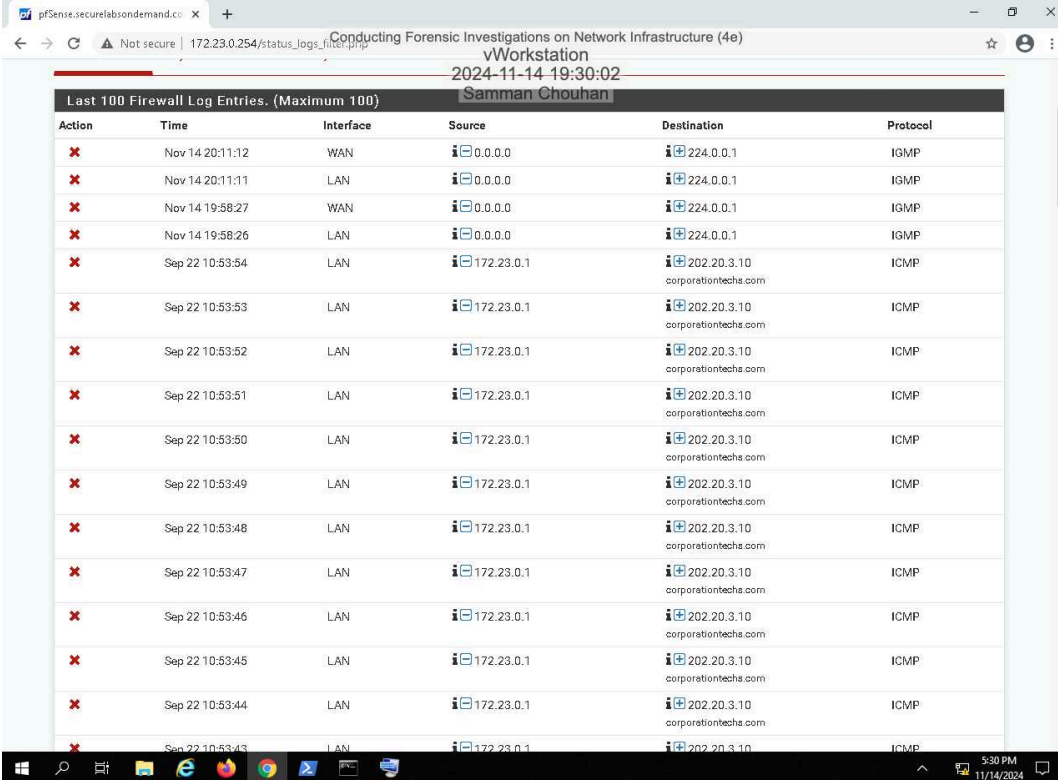
9. Make a screen capture showing the entries in the firewall log.



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.



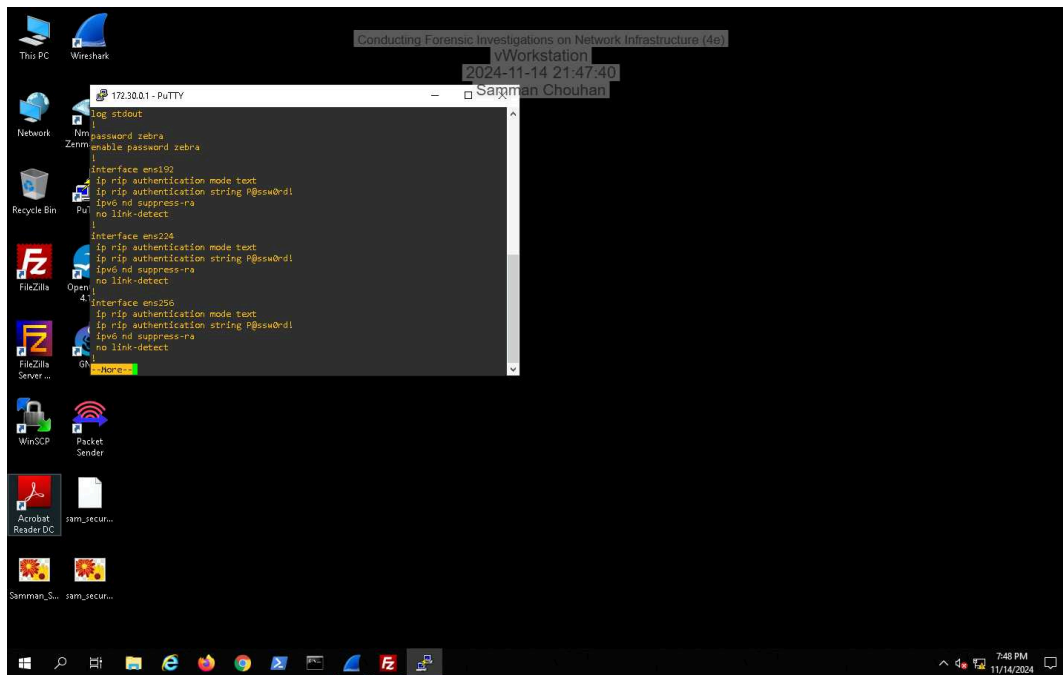
The screenshot shows a web browser window displaying the pfSense Firewall Log. The browser's address bar shows the URL `172.23.0.254/status_logs.php`. The page title is "Conducting Forensic Investigations on Network Infrastructure (4e)". The log is titled "Last 100 Firewall Log Entries. (Maximum 100)". The log entries are displayed in a table with columns: Action, Time, Interface, Source, Destination, and Protocol. The entries show a series of blocked ICMP requests from source IP 172.23.0.1 to destination IP 202.20.3.10 (corporationtechs.com) on the LAN interface. The actions are marked with a red 'X' icon, indicating they were blocked. The times range from Nov 14 20:11:12 to Sep 22 10:53:43. The protocols are all ICMP.

Action	Time	Interface	Source	Destination	Protocol
✗	Nov 14 20:11:12	WAN	0.0.0.0	224.0.0.1	IGMP
✗	Nov 14 20:11:11	LAN	0.0.0.0	224.0.0.1	IGMP
✗	Nov 14 19:58:27	WAN	0.0.0.0	224.0.0.1	IGMP
✗	Nov 14 19:58:26	LAN	0.0.0.0	224.0.0.1	IGMP
✗	Sep 22 10:53:54	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:53	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:52	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:51	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:50	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:49	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:48	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:47	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:46	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:45	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:44	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP
✗	Sep 22 10:53:43	LAN	172.23.0.1	202.20.3.10 corporationtechs.com	ICMP

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.

The destination Ip Address : 202.20.3.10The port number of the outgoing connection attempt : 21