Conducting Forensic Investigations on Network Infrastructure (4e)

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

Student:	Email:
Alexis Cherpes	cherpea@ferris.edu

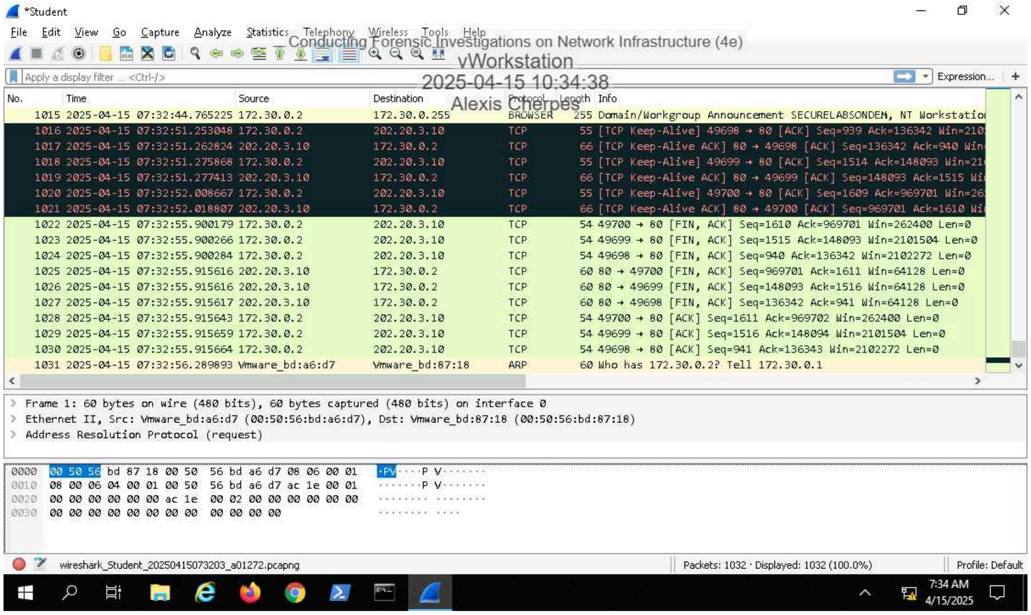
Time on Task:	Progress:
1 hour, 15 minutes	100%

Report Generated: Thursday, May 22, 2025 at 4:51 PM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

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



*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 10:34:38
Alexis Cherpes

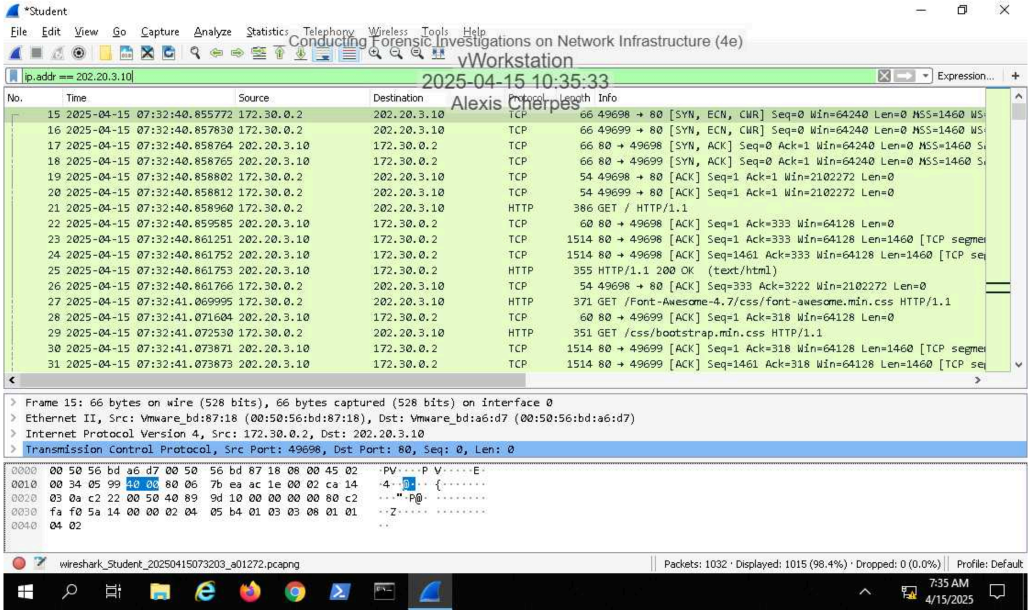
```
No.   Time                       Source            Destination      Protocol Length Info
 1015 2025-04-15 07:32:44.765225 172.30.0.2        172.30.0.255     BROWSER   255 Domain/Workgroup Announcement SECURELABSONDEM, NT Workstatio
 1016 2025-04-15 07:32:51.253048 172.30.0.2        202.20.3.10      TCP        55 [TCP Keep-Alive] 49698 → 80 [ACK] Seq=939 Ack=136342 Win=210
 1017 2025-04-15 07:32:51.262824 202.20.3.10       172.30.0.2       TCP        66 [TCP Keep-Alive ACK] 80 → 49698 [ACK] Seq=136342 Ack=940 Win
 1018 2025-04-15 07:32:51.275868 172.30.0.2        202.20.3.10      TCP        55 [TCP Keep-Alive] 49699 → 80 [ACK] Seq=1514 Ack=148093 Win=21
 1019 2025-04-15 07:32:51.277413 202.20.3.10       172.30.0.2       TCP        66 [TCP Keep-Alive ACK] 80 → 49699 [ACK] Seq=148093 Ack=1515 Wi
 1020 2025-04-15 07:32:52.008667 172.30.0.2        202.20.3.10      TCP        55 [TCP Keep-Alive] 49700 → 80 [ACK] Seq=1609 Ack=969701 Win=26
 1021 2025-04-15 07:32:52.018807 202.20.3.10       172.30.0.2       TCP        66 [TCP Keep-Alive ACK] 80 → 49700 [ACK] Seq=969701 Ack=1610 Wi
 1022 2025-04-15 07:32:55.900179 172.30.0.2        202.20.3.10      TCP        54 49700 → 80 [FIN, ACK] Seq=1610 Ack=969701 Win=262400 Len=0
 1023 2025-04-15 07:32:55.900266 172.30.0.2        202.20.3.10      TCP        54 49699 → 80 [FIN, ACK] Seq=1515 Ack=148093 Win=2101504 Len=0
 1024 2025-04-15 07:32:55.900284 172.30.0.2        202.20.3.10      TCP        54 49698 → 80 [FIN, ACK] Seq=940 Ack=136342 Win=2102272 Len=0
 1025 2025-04-15 07:32:55.915616 202.20.3.10       172.30.0.2       TCP        60 80 → 49700 [FIN, ACK] Seq=969701 Ack=1611 Win=64128 Len=0
 1026 2025-04-15 07:32:55.915616 202.20.3.10       172.30.0.2       TCP        60 80 → 49699 [FIN, ACK] Seq=148093 Ack=1516 Win=64128 Len=0
 1027 2025-04-15 07:32:55.915617 202.20.3.10       172.30.0.2       TCP        60 80 → 49698 [FIN, ACK] Seq=136342 Ack=941 Win=64128 Len=0
 1028 2025-04-15 07:32:55.915643 172.30.0.2        202.20.3.10      TCP        54 49700 → 80 [ACK] Seq=1611 Ack=969702 Win=262400 Len=0
 1029 2025-04-15 07:32:55.915659 172.30.0.2        202.20.3.10      TCP        54 49699 → 80 [ACK] Seq=1516 Ack=148094 Win=2101504 Len=0
 1030 2025-04-15 07:32:55.915664 172.30.0.2        202.20.3.10      TCP        54 49698 → 80 [ACK] Seq=941 Ack=136343 Win=2102272 Len=0
 1031 2025-04-15 07:32:56.289893 Vmware_bd:a6:d7   Vmware_bd:87:18  ARP        60 Who has 172.30.0.2? Tell 172.30.0.1
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_bd:a6:d7 (00:50:56:bd:a6:d7), Dst: Vmware_bd:87:18 (00:50:56:bd:87:18)
> Address Resolution Protocol (request)
```

```
0000  00 50 56 bd 87 18 00 50  56 bd a6 d7 08 06 00 01   ·PV····P V·······
0010  08 00 06 04 00 01 00 50  56 bd a6 d7 ac 1e 00 01   ·······P V·······
0020  00 00 00 00 00 00 ac 1e  00 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

wireshark_Student_20250415073203_a01272.pcapng | Packets: 1032 · Displayed: 1032 (100.0%) | Profile: Default

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 10:35:33
Alexis Cherpes
Expression...
7:35 AM
4/15/2025

```
ip.addr == 202.20.3.10
```

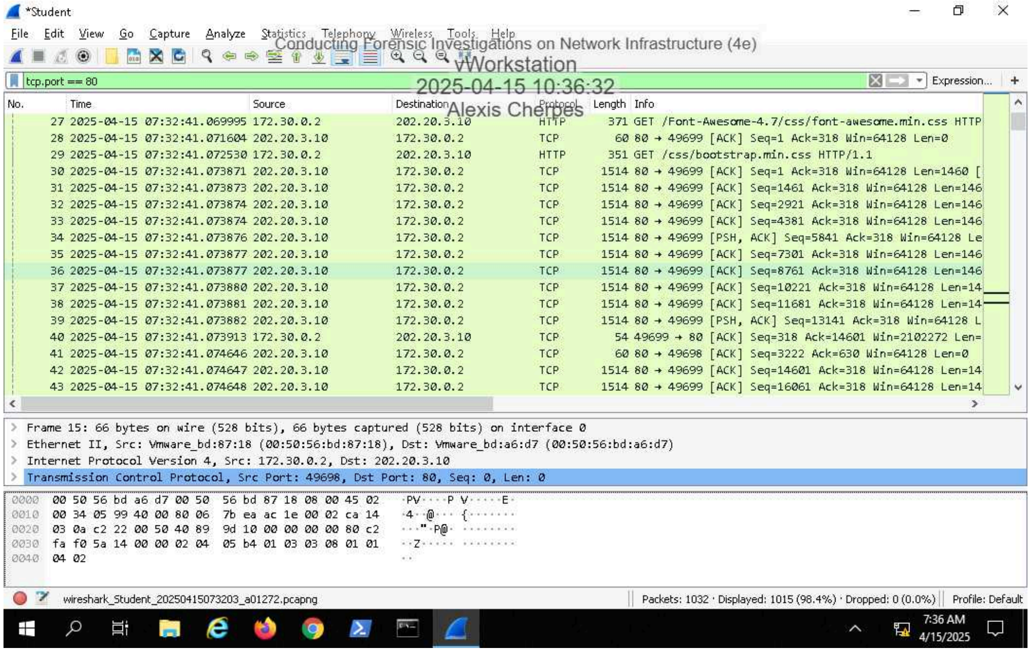
```
No.  Time                        Source        Destination   Protocol Length Info
  15 2025-04-15 07:32:40.855772 172.30.0.2    202.20.3.10   TCP        66 49698 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
  16 2025-04-15 07:32:40.857830 172.30.0.2    202.20.3.10   TCP        66 49699 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
  17 2025-04-15 07:32:40.858764 202.20.3.10   172.30.0.2    TCP        66 80 → 49698 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 S
  18 2025-04-15 07:32:40.858765 202.20.3.10   172.30.0.2    TCP        66 80 → 49699 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 S
  19 2025-04-15 07:32:40.858802 172.30.0.2    202.20.3.10   TCP        54 49698 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
  20 2025-04-15 07:32:40.858812 172.30.0.2    202.20.3.10   TCP        54 49699 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
  21 2025-04-15 07:32:40.858960 172.30.0.2    202.20.3.10   HTTP      386 GET / HTTP/1.1
  22 2025-04-15 07:32:40.859585 202.20.3.10   172.30.0.2    TCP        60 80 → 49698 [ACK] Seq=1 Ack=333 Win=64128 Len=0
  23 2025-04-15 07:32:40.861251 202.20.3.10   172.30.0.2    TCP      1514 80 → 49698 [ACK] Seq=1 Ack=333 Win=64128 Len=1460 [TCP segmen
  24 2025-04-15 07:32:40.861752 202.20.3.10   172.30.0.2    TCP      1514 80 → 49698 [ACK] Seq=1461 Ack=333 Win=64128 Len=1460 [TCP se
  25 2025-04-15 07:32:40.861753 202.20.3.10   172.30.0.2    HTTP      355 HTTP/1.1 200 OK  (text/html)
  26 2025-04-15 07:32:40.861766 172.30.0.2    202.20.3.10   TCP        54 49698 → 80 [ACK] Seq=333 Ack=3222 Win=2102272 Len=0
  27 2025-04-15 07:32:41.069995 172.30.0.2    202.20.3.10   HTTP      371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP/1.1
  28 2025-04-15 07:32:41.071604 202.20.3.10   172.30.0.2    TCP        60 80 → 49699 [ACK] Seq=1 Ack=318 Win=64128 Len=0
  29 2025-04-15 07:32:41.072530 172.30.0.2    202.20.3.10   HTTP      351 GET /css/bootstrap.min.css HTTP/1.1
  30 2025-04-15 07:32:41.073871 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=1 Ack=318 Win=64128 Len=1460 [TCP segmen
  31 2025-04-15 07:32:41.073873 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=1461 Ack=318 Win=64128 Len=1460 [TCP se
```

```
> Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_bd:87:18 (00:50:56:bd:87:18), Dst: Vmware_bd:a6:d7 (00:50:56:bd:a6:d7)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49698, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 bd a6 d7 00 50  56 bd 87 18 08 00 45 02   ·PV····P V·····E·
0010  00 34 05 99 40 00 80 06  7b ea ac 1e 00 02 ca 14   ·4··@··· {·······
0020  03 0a c2 22 00 50 40 89  9d 10 00 00 00 00 80 c2   ···"·P@· ········
0030  fa f0 5a 14 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

```
wireshark_Student_20250415073203_a01272.pcapng    Packets: 1032 · Displayed: 1015 (98.4%) · Dropped: 0 (0.0%)    Profile: Default
```

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 10:36:32
Alexis Cherpes
Expression...
7:36 AM
4/15/2025

```
tcp.port == 80
```

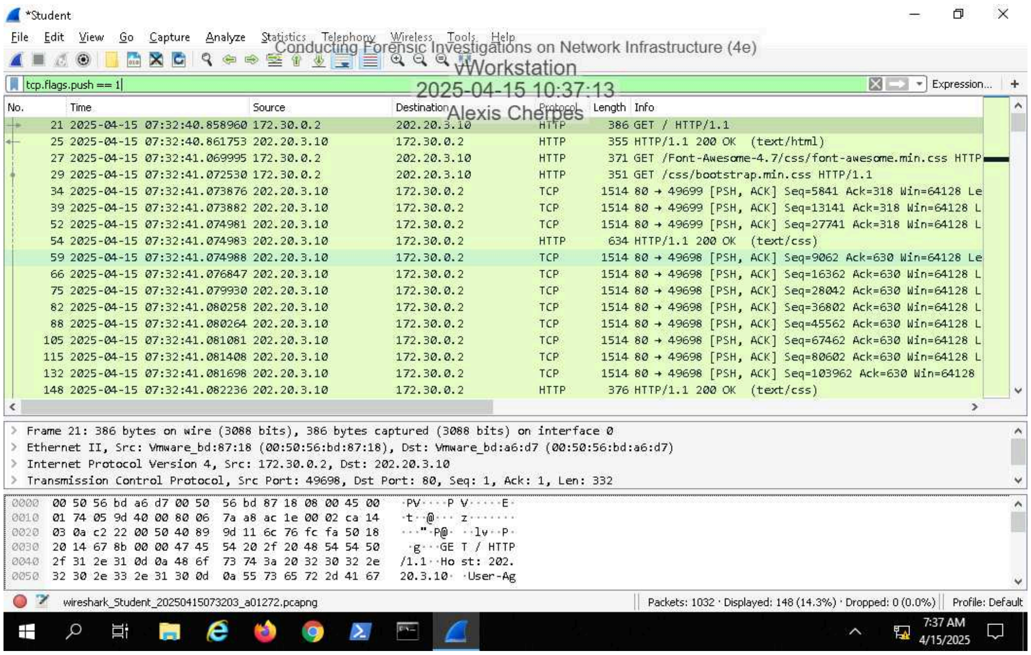
```
No.  Time                        Source        Destination   Protocol Length Info
  27 2025-04-15 07:32:41.069995 172.30.0.2    202.20.3.10   HTTP      371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP
  28 2025-04-15 07:32:41.071604 202.20.3.10   172.30.0.2    TCP        60 80 → 49699 [ACK] Seq=1 Ack=318 Win=64128 Len=0
  29 2025-04-15 07:32:41.072530 172.30.0.2    202.20.3.10   HTTP      351 GET /css/bootstrap.min.css HTTP/1.1
  30 2025-04-15 07:32:41.073871 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=1 Ack=318 Win=64128 Len=1460 [
  31 2025-04-15 07:32:41.073873 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=1461 Ack=318 Win=64128 Len=146
  32 2025-04-15 07:32:41.073874 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=2921 Ack=318 Win=64128 Len=146
  33 2025-04-15 07:32:41.073874 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=4381 Ack=318 Win=64128 Len=146
  34 2025-04-15 07:32:41.073876 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [PSH, ACK] Seq=5841 Ack=318 Win=64128 Le
  35 2025-04-15 07:32:41.073877 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=7301 Ack=318 Win=64128 Len=146
  36 2025-04-15 07:32:41.073877 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=8761 Ack=318 Win=64128 Len=146
  37 2025-04-15 07:32:41.073880 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=10221 Ack=318 Win=64128 Len=14
  38 2025-04-15 07:32:41.073881 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=11681 Ack=318 Win=64128 Len=14
  39 2025-04-15 07:32:41.073882 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [PSH, ACK] Seq=13141 Ack=318 Win=64128 L
  40 2025-04-15 07:32:41.073913 172.30.0.2    202.20.3.10   TCP        54 49699 → 80 [ACK] Seq=318 Ack=14601 Win=2102272 Len=
  41 2025-04-15 07:32:41.074646 202.20.3.10   172.30.0.2    TCP        60 80 → 49698 [ACK] Seq=3222 Ack=630 Win=64128 Len=0
  42 2025-04-15 07:32:41.074647 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=14601 Ack=318 Win=64128 Len=14
  43 2025-04-15 07:32:41.074648 202.20.3.10   172.30.0.2    TCP      1514 80 → 49699 [ACK] Seq=16061 Ack=318 Win=64128 Len=14
```

```
> Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_bd:87:18 (00:50:56:bd:87:18), Dst: Vmware_bd:a6:d7 (00:50:56:bd:a6:d7)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49698, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 bd a6 d7 00 50  56 bd 87 18 08 00 45 02   ·PV····P V·····E·
0010  00 34 05 99 40 00 80 06  7b ea ac 1e 00 02 ca 14   ·4··@··· {·······
0020  03 0a c2 22 00 50 40 89  9d 10 00 00 00 00 80 c2   ···"·P@· ········
0030  fa f0 5a 14 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

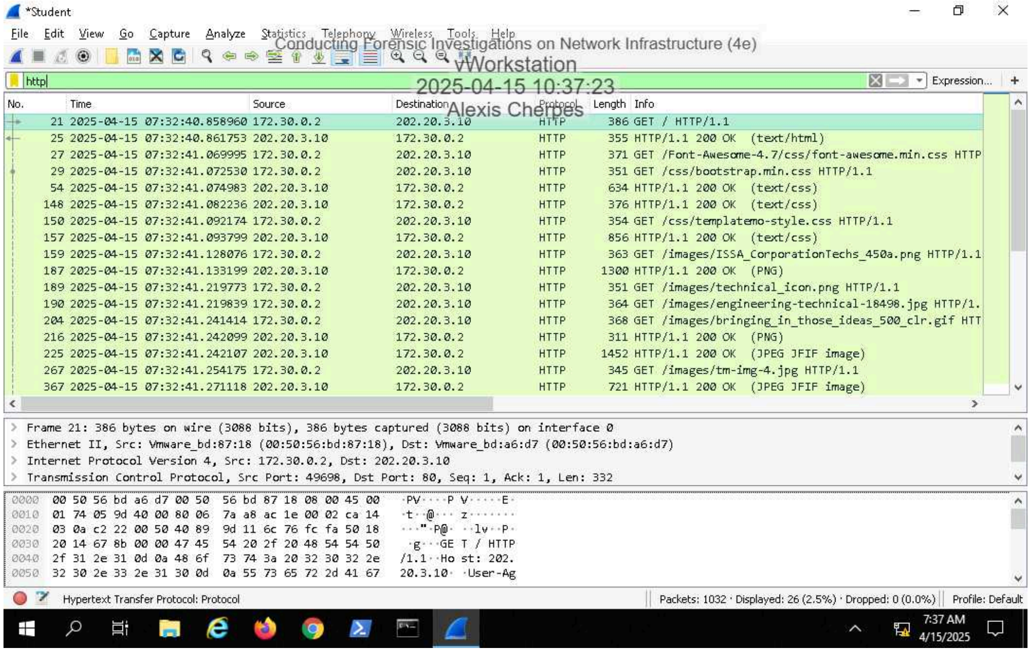
```
wireshark_Student_20250415073203_a01272.pcapng    Packets: 1032 · Displayed: 1015 (98.4%) · Dropped: 0 (0.0%)    Profile: Default
```

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



```
tcp.flags.push == 1

No.  Time                        Source        Destination   Protocol  Length Info
  21 2025-04-15 07:32:40.858960 172.30.0.2    202.20.3.10   HTTP       386 GET / HTTP/1.1
  25 2025-04-15 07:32:40.861753 202.20.3.10   172.30.0.2    HTTP       355 HTTP/1.1 200 OK  (text/html)
  27 2025-04-15 07:32:41.069995 172.30.0.2    202.20.3.10   HTTP       371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP
  29 2025-04-15 07:32:41.072530 172.30.0.2    202.20.3.10   HTTP       351 GET /css/bootstrap.min.css HTTP/1.1
  34 2025-04-15 07:32:41.073876 202.20.3.10   172.30.0.2    TCP       1514 80 → 49699 [PSH, ACK] Seq=5841 Ack=318 Win=64128 Le
  39 2025-04-15 07:32:41.073882 202.20.3.10   172.30.0.2    TCP       1514 80 → 49699 [PSH, ACK] Seq=13141 Ack=318 Win=64128 L
  52 2025-04-15 07:32:41.074981 202.20.3.10   172.30.0.2    TCP       1514 80 → 49699 [PSH, ACK] Seq=27741 Ack=318 Win=64128 L
  54 2025-04-15 07:32:41.074983 202.20.3.10   172.30.0.2    HTTP       634 HTTP/1.1 200 OK  (text/css)
  59 2025-04-15 07:32:41.074988 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=9062 Ack=630 Win=64128 Le
  66 2025-04-15 07:32:41.076847 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=16362 Ack=630 Win=64128 L
  75 2025-04-15 07:32:41.079930 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=28042 Ack=630 Win=64128 L
  82 2025-04-15 07:32:41.080258 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=36802 Ack=630 Win=64128 L
  88 2025-04-15 07:32:41.080264 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=45562 Ack=630 Win=64128 L
 105 2025-04-15 07:32:41.081081 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=67462 Ack=630 Win=64128 L
 115 2025-04-15 07:32:41.081408 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=80602 Ack=630 Win=64128 L
 132 2025-04-15 07:32:41.081698 202.20.3.10   172.30.0.2    TCP       1514 80 → 49698 [PSH, ACK] Seq=103962 Ack=630 Win=64128
 148 2025-04-15 07:32:41.082236 202.20.3.10   172.30.0.2    HTTP       376 HTTP/1.1 200 OK  (text/css)

> Frame 21: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_bd:87:18 (00:50:56:bd:87:18), Dst: Vmware_bd:a6:d7 (00:50:56:bd:a6:d7)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49698, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

0000  00 50 56 bd a6 d7 00 50  56 bd 87 18 08 00 45 00   ·PV····P V·····E·
0010  01 74 05 9d 40 00 80 06  7a a8 ac 1e 00 02 ca 14   ·t··@··· z·······
0020  03 0a c2 22 00 50 40 89  9d 11 6c 76 fc fa 50 18   ···"·P@· ··lv··P·
0030  20 14 67 8b 00 00 47 45  54 20 2f 20 48 54 54 50    ·g···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 32 30 32 2e   /1.1··Ho st: 202.
0050  32 30 2e 33 2e 31 30 0d  0a 55 73 65 72 2d 41 67   20.3.10· ·User-Ag

wireshark_Student_20250415073203_a01272.pcapng    Packets: 1032 · Displayed: 148 (14.3%) · Dropped: 0 (0.0%)    Profile: Default
```

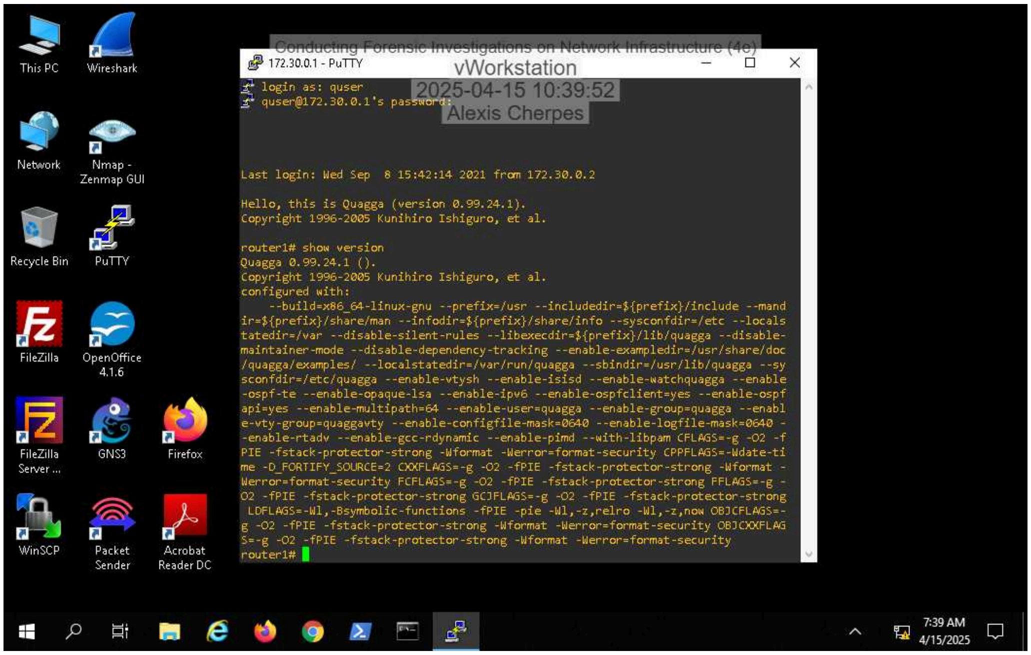
19. **Make a screen capture** showing the **http-filtered traffic**.



```
http

No.  Time                        Source        Destination   Protocol  Length Info
  21 2025-04-15 07:32:40.858960 172.30.0.2    202.20.3.10   HTTP       386 GET / HTTP/1.1
  25 2025-04-15 07:32:40.861753 202.20.3.10   172.30.0.2    HTTP       355 HTTP/1.1 200 OK  (text/html)
  27 2025-04-15 07:32:41.069995 172.30.0.2    202.20.3.10   HTTP       371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP
  29 2025-04-15 07:32:41.072530 172.30.0.2    202.20.3.10   HTTP       351 GET /css/bootstrap.min.css HTTP/1.1
  54 2025-04-15 07:32:41.074983 202.20.3.10   172.30.0.2    HTTP       634 HTTP/1.1 200 OK  (text/css)
 148 2025-04-15 07:32:41.082236 202.20.3.10   172.30.0.2    HTTP       376 HTTP/1.1 200 OK  (text/css)
 150 2025-04-15 07:32:41.092174 172.30.0.2    202.20.3.10   HTTP       354 GET /css/templatemo-style.css HTTP/1.1
 157 2025-04-15 07:32:41.093799 202.20.3.10   172.30.0.2    HTTP       856 HTTP/1.1 200 OK  (text/css)
 159 2025-04-15 07:32:41.128076 172.30.0.2    202.20.3.10   HTTP       363 GET /images/ISSA_CorporationTechs_450a.png HTTP/1.1
 187 2025-04-15 07:32:41.133199 202.20.3.10   172.30.0.2    HTTP      1300 HTTP/1.1 200 OK  (PNG)
 189 2025-04-15 07:32:41.219773 172.30.0.2    202.20.3.10   HTTP       351 GET /images/technical_icon.png HTTP/1.1
 190 2025-04-15 07:32:41.219839 172.30.0.2    202.20.3.10   HTTP       364 GET /images/engineering-technical-18498.jpg HTTP/1.
 204 2025-04-15 07:32:41.241414 172.30.0.2    202.20.3.10   HTTP       368 GET /images/bringing_in_those_ideas_500_clr.gif HTT
 216 2025-04-15 07:32:41.242099 202.20.3.10   172.30.0.2    HTTP       311 HTTP/1.1 200 OK  (PNG)
 225 2025-04-15 07:32:41.242107 202.20.3.10   172.30.0.2    HTTP      1452 HTTP/1.1 200 OK  (JPEG JFIF image)
 267 2025-04-15 07:32:41.254175 172.30.0.2    202.20.3.10   HTTP       345 GET /images/tm-img-4.jpg HTTP/1.1
 367 2025-04-15 07:32:41.271118 202.20.3.10   172.30.0.2    HTTP       721 HTTP/1.1 200 OK  (JPEG JFIF image)

> Frame 21: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_bd:87:18 (00:50:56:bd:87:18), Dst: Vmware_bd:a6:d7 (00:50:56:bd:a6:d7)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49698, Dst Port: 80, Seq: 1, Ack: 1, Len: 332

0000  00 50 56 bd a6 d7 00 50  56 bd 87 18 08 00 45 00   ·PV····P V·····E·
0010  01 74 05 9d 40 00 80 06  7a a8 ac 1e 00 02 ca 14   ·t··@··· z·······
0020  03 0a c2 22 00 50 40 89  9d 11 6c 76 fc fa 50 18   ···"·P@· ··lv··P·
0030  20 14 67 8b 00 00 47 45  54 20 2f 20 48 54 54 50    ·g···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 32 30 32 2e   /1.1··Ho st: 202.
0050  32 30 2e 33 2e 31 30 0d  0a 55 73 65 72 2d 41 67   20.3.10· ·User-Ag

Hypertext Transfer Protocol: Protocol    Packets: 1032 · Displayed: 26 (2.5%) · Dropped: 0 (0.0%)    Profile: Default
```

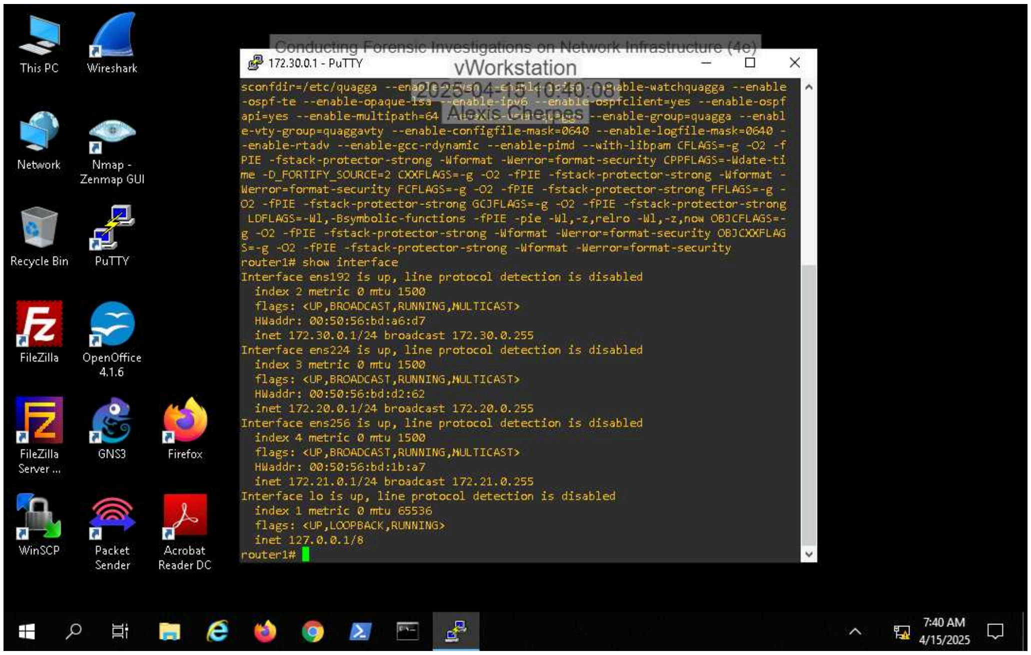
Part 2: Analyze a Router for Forensic Evidence

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



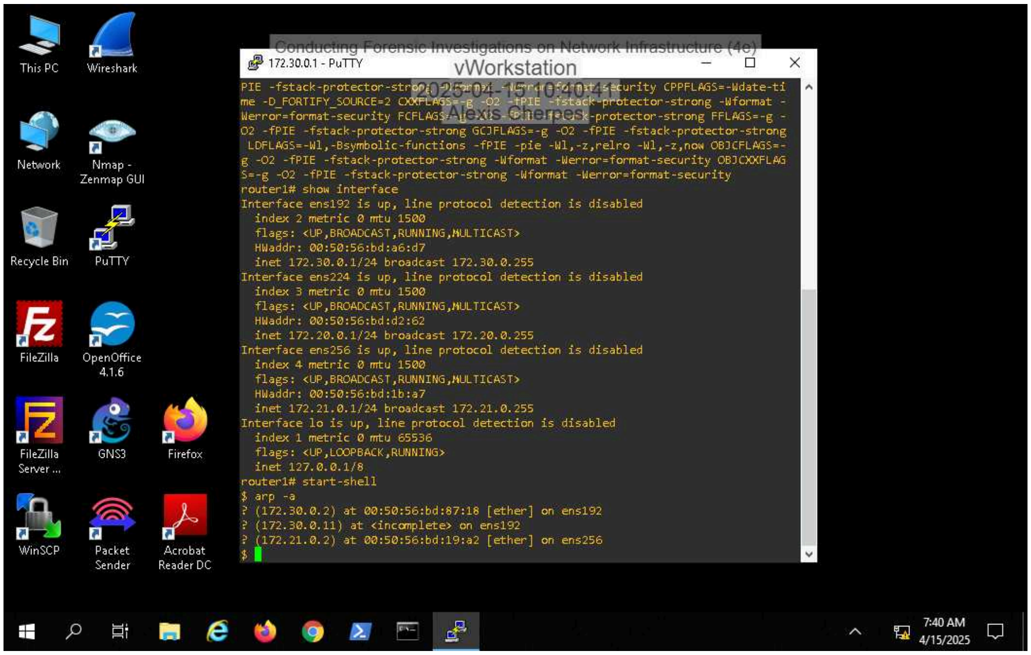
```
login as: quser
quser@172.30.0.1's password:



Last login: Wed Sep  8 15:42:14 2021 from 172.30.0.2

Hello, this is Quagga (version 0.99.24.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

router1# show version
Quagga 0.99.24.1 ().
Copyright 1996-2005 Kunihiro Ishiguro, et al.
configured with:
    --build=x86_64-linux-gnu --prefix=/usr --includedir=${prefix}/include --mand
ir=${prefix}/share/man --infodir=${prefix}/share/info --sysconfdir=/etc --locals
tatedir=/var --disable-silent-rules --libexecdir=${prefix}/lib/quagga --disable-
maintainer-mode --disable-dependency-tracking --enable-exampledir=/usr/share/doc
/quagga/examples/ --localstatedir=/var/run/quagga --sbindir=/usr/lib/quagga --sy
sconfdir=/etc/quagga --enable-vtysh --enable-isisd --enable-watchquagga --enable
-ospf-te --enable-opaque-lsa --enable-ipv6 --enable-ospfclient=yes --enable-ospf
api=yes --enable-multipath=64 --enable-user=quagga --enable-group=quagga --enabl
e-vty-group=quaggavty --enable-configfile-mask=0640 --enable-logfile-mask=0640 -
-enable-rtadv --enable-gcc-rdynamic --enable-pimd --with-libpam CFLAGS=-g -O2 -f
PIE -fstack-protector-strong -Wformat -Werror=format-security CPPFLAGS=-Wdate-ti
me -D_FORTIFY_SOURCE=2 CXXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -
Werror=format-security FCFLAGS=-g -O2 -fPIE -fstack-protector-strong FFLAGS=-g -
O2 -fPIE -fstack-protector-strong GCJFLAGS=-g -O2 -fPIE -fstack-protector-strong
 LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now OBJCFLAGS=-
g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security OBJCXXFLAG
S=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1#
```

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



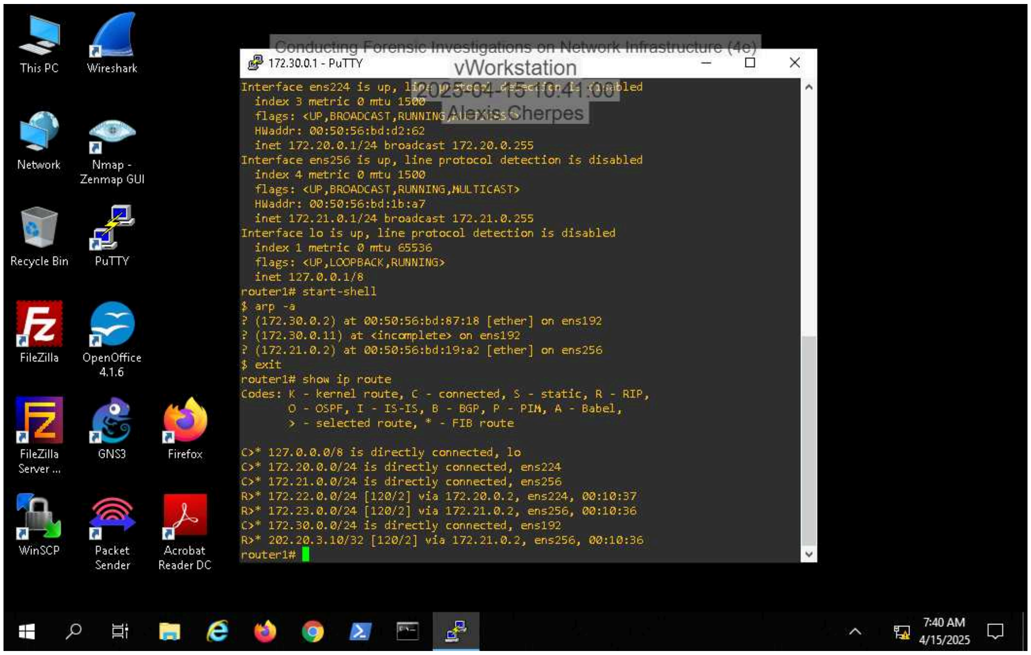
```
sconfdir=/etc/quagga --enable-vtysh --enable-isisd --enable-watchquagga --enable
-ospf-te --enable-opaque-lsa --enable-ipv6 --enable-ospfclient=yes --enable-ospf
api=yes --enable-multipath=64 --enable-user=quagga --enable-group=quagga --enabl
e-vty-group=quaggavty --enable-configfile-mask=0640 --enable-logfile-mask=0640 -
-enable-rtadv --enable-gcc-rdynamic --enable-pimd --with-libpam CFLAGS=-g -O2 -f
PIE -fstack-protector-strong -Wformat -Werror=format-security CPPFLAGS=-Wdate-ti
me -D_FORTIFY_SOURCE=2 CXXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -
Werror=format-security FCFLAGS=-g -O2 -fPIE -fstack-protector-strong FFLAGS=-g -
O2 -fPIE -fstack-protector-strong GCJFLAGS=-g -O2 -fPIE -fstack-protector-strong
 LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now OBJCFLAGS=-
g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security OBJCXXFLAG
S=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1# show interface
Interface ens192 is up, line protocol detection is disabled
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:a6:d7
  inet 172.30.0.1/24 broadcast 172.30.0.255
Interface ens224 is up, line protocol detection is disabled
  index 3 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:d2:62
  inet 172.20.0.1/24 broadcast 172.20.0.255
Interface ens256 is up, line protocol detection is disabled
  index 4 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:1b:a7
  inet 172.21.0.1/24 broadcast 172.21.0.255
Interface lo is up, line protocol detection is disabled
  index 1 metric 0 mtu 65536
  flags: <UP,LOOPBACK,RUNNING>
  inet 127.0.0.1/8
router1#
```

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



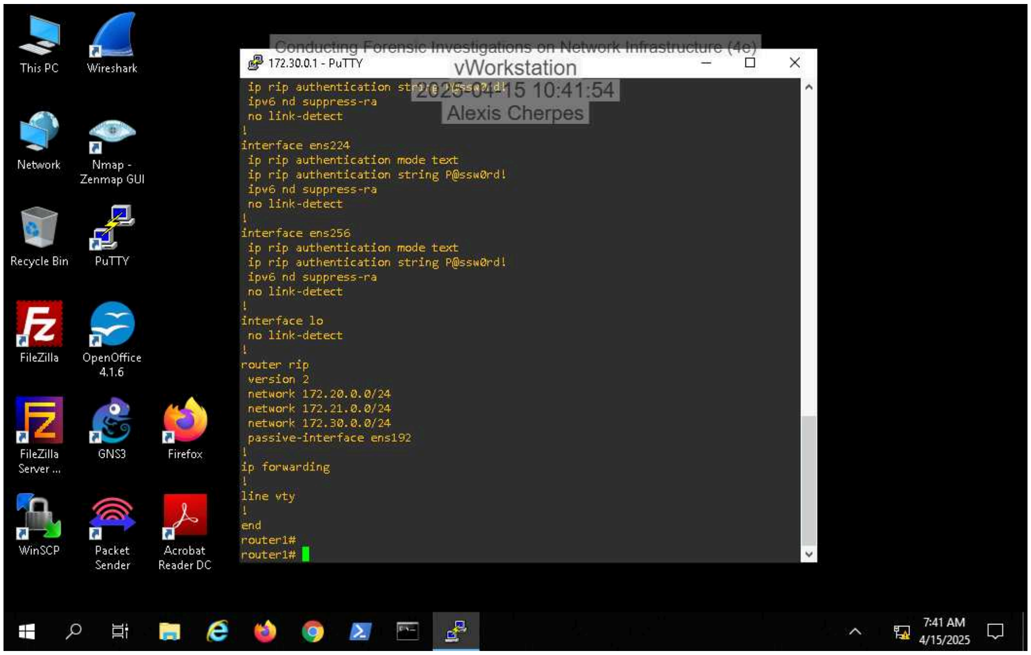
```
PIE -fstack-protector-strong -Wformat -Werror=format-security CPPFLAGS=-Wdate-ti
me -D_FORTIFY_SOURCE=2 CXXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -
Werror=format-security FCFLAGS=-g -O2 -fPIE -fstack-protector-strong FFLAGS=-g -
O2 -fPIE -fstack-protector-strong GCJFLAGS=-g -O2 -fPIE -fstack-protector-strong
 LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now OBJCFLAGS=-
g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security OBJCXXFLAG
S=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1# show interface
Interface ens192 is up, line protocol detection is disabled
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:a6:d7
  inet 172.30.0.1/24 broadcast 172.30.0.255
Interface ens224 is up, line protocol detection is disabled
  index 3 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:d2:62
  inet 172.20.0.1/24 broadcast 172.20.0.255
Interface ens256 is up, line protocol detection is disabled
  index 4 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:1b:a7
  inet 172.21.0.1/24 broadcast 172.21.0.255
Interface lo is up, line protocol detection is disabled
  index 1 metric 0 mtu 65536
  flags: <UP,LOOPBACK,RUNNING>
  inet 127.0.0.1/8
router1# start-shell
$ arp -a
? (172.30.0.2) at 00:50:56:bd:87:18 [ether] on ens192
? (172.30.0.11) at <incomplete> on ens192
? (172.21.0.2) at 00:50:56:bd:19:a2 [ether] on ens256
$
```

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



```
Interface ens224 is up, line protocol detection is disabled
  index 3 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:d2:62
  inet 172.20.0.1/24 broadcast 172.20.0.255
Interface ens256 is up, line protocol detection is disabled
  index 4 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:bd:1b:a7
  inet 172.21.0.1/24 broadcast 172.21.0.255
Interface lo is up, line protocol detection is disabled
  index 1 metric 0 mtu 65536
  flags: <UP,LOOPBACK,RUNNING>
  inet 127.0.0.1/8
router1# start-shell
$ arp -a
? (172.30.0.2) at 00:50:56:bd:87:18 [ether] on ens192
? (172.30.0.11) at <incomplete> on ens192
? (172.21.0.2) at 00:50:56:bd:19:a2 [ether] on ens256
$ exit
router1# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 172.20.0.0/24 is directly connected, ens224
C>* 172.21.0.0/24 is directly connected, ens256
R>* 172.22.0.0/24 [120/2] via 172.20.0.2, ens224, 00:10:37
R>* 172.23.0.0/24 [120/2] via 172.21.0.2, ens256, 00:10:36
C>* 172.30.0.0/24 is directly connected, ens192
R>* 202.20.3.10/32 [120/2] via 172.21.0.2, ens256, 00:10:36
router1#
```

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

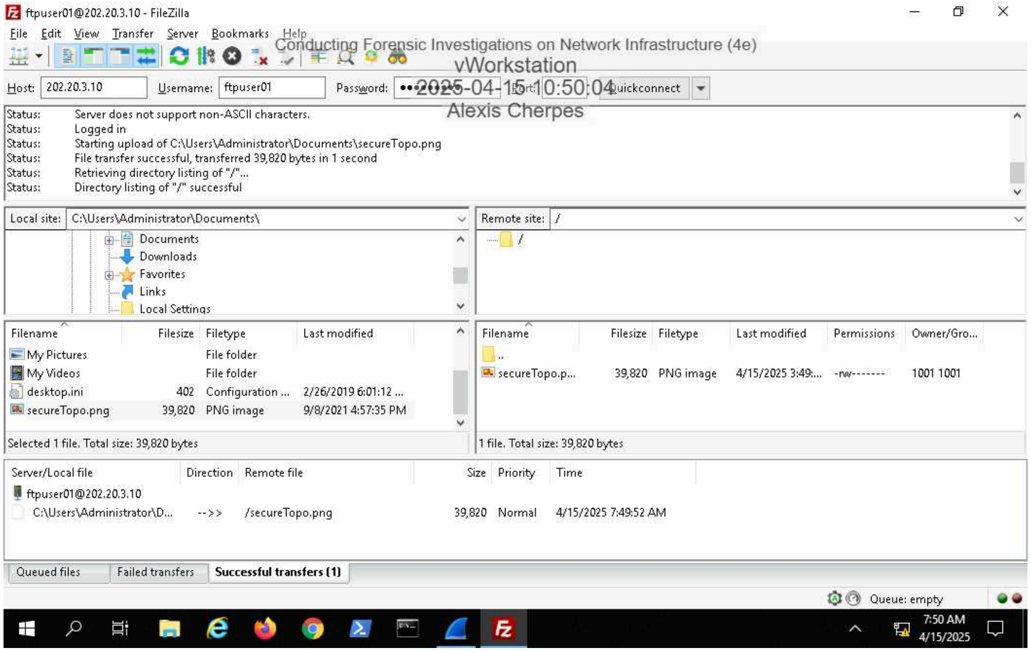


```
 ip rip authentication string P@ssw0rd!
 ipv6 nd suppress-ra
 no link-detect
!
interface ens224
 ip rip authentication mode text
 ip rip authentication string P@ssw0rd!
 ipv6 nd suppress-ra
 no link-detect
!
interface ens256
 ip rip authentication mode text
 ip rip authentication string P@ssw0rd!
 ipv6 nd suppress-ra
 no link-detect
!
interface lo
 no link-detect
!
router rip
 version 2
 network 172.20.0.0/24
 network 172.21.0.0/24
 network 172.30.0.0/24
 passive-interface ens192
!
ip forwarding
!
line vty
!
end
router1#
router1#
```

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**.



Host: 202.20.3.10 Username: ftpuser01 Password: ••

```
Status:     Server does not support non-ASCII characters.
Status:     Logged in
Status:     Starting upload of C:\Users\Administrator\Documents\secureTopo.png
Status:     File transfer successful, transferred 39,820 bytes in 1 second
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
```

Local site: C:\Users\Administrator\Documents\

- Documents
- Downloads
- Favorites
- Links
- Local Settings

Remote site: /

- /

Filename	Filesize	Filetype	Last modified
My Pictures		File folder	
My Videos		File folder	
desktop.ini	402	Configuration ...	2/26/2019 6:01:12 ...
secureTopo.png	39,820	PNG image	9/8/2021 4:57:35 PM

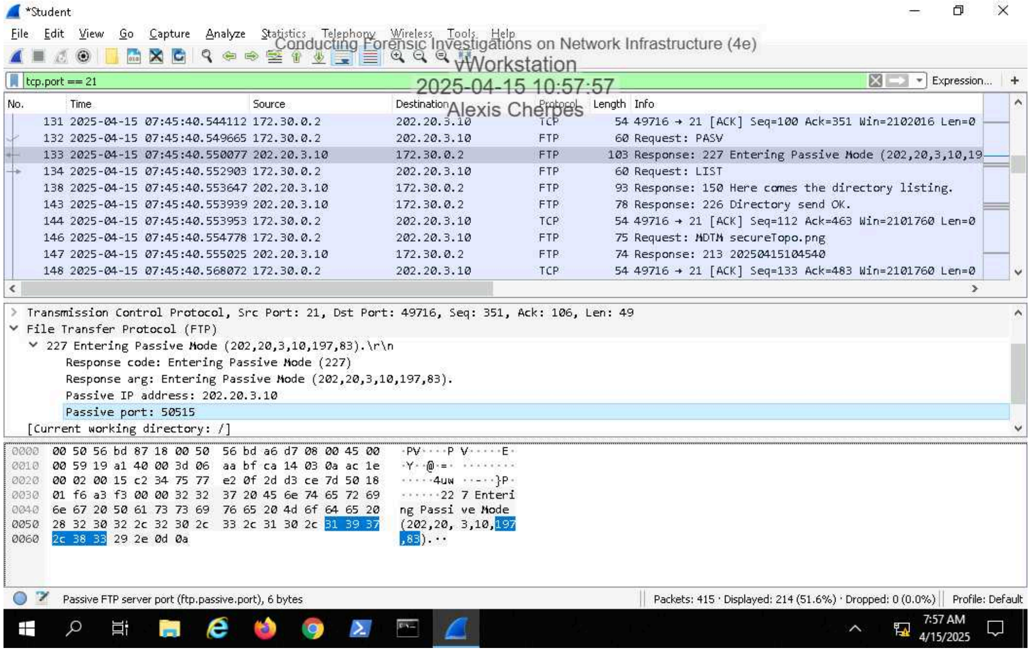
Selected 1 file. Total size: 39,820 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
secureTopo.p...	39,820	PNG image	4/15/2025 3:49:...	-rw-------	1001 1001

1 file. Total size: 39,820 bytes

Server/Local file	Direction	Remote file	Size	Priority	Time
ftpuser01@202.20.3.10					
C:\Users\Administrator\D...	-->>	/secureTopo.png	39,820	Normal	4/15/2025 7:49:52 AM

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



tcp.port == 21

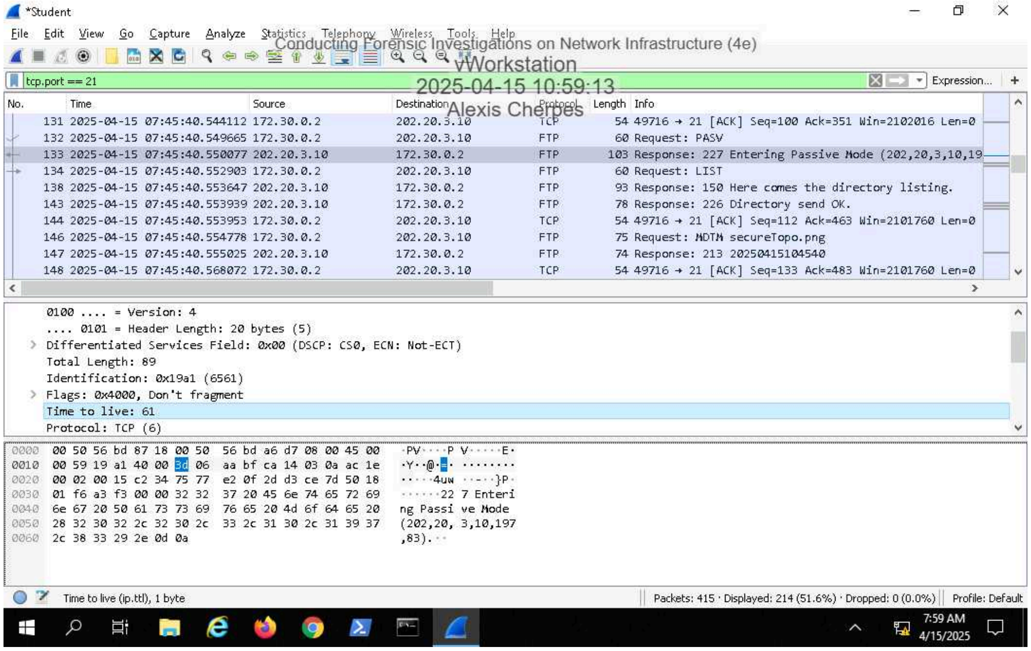
```
No.     Time                        Source       Destination  Protocol Length Info
    131 2025-04-15 07:45:40.544112 172.30.0.2   202.20.3.10  TCP       54 49716 → 21 [ACK] Seq=100 Ack=351 Win=2102016 Len=0
    132 2025-04-15 07:45:40.549665 172.30.0.2   202.20.3.10  FTP       60 Request: PASV
    133 2025-04-15 07:45:40.550077 202.20.3.10  172.30.0.2   FTP      103 Response: 227 Entering Passive Mode (202,20,3,10,19
    134 2025-04-15 07:45:40.552903 172.30.0.2   202.20.3.10  FTP       60 Request: LIST
    138 2025-04-15 07:45:40.553647 202.20.3.10  172.30.0.2   FTP       93 Response: 150 Here comes the directory listing.
    143 2025-04-15 07:45:40.553939 202.20.3.10  172.30.0.2   FTP       78 Response: 226 Directory send OK.
    144 2025-04-15 07:45:40.553953 172.30.0.2   202.20.3.10  TCP       54 49716 → 21 [ACK] Seq=112 Ack=463 Win=2101760 Len=0
    146 2025-04-15 07:45:40.554778 172.30.0.2   202.20.3.10  FTP       75 Request: MDTM secureTopo.png
    147 2025-04-15 07:45:40.555025 202.20.3.10  172.30.0.2   FTP       74 Response: 213 20250415104540
    148 2025-04-15 07:45:40.568072 172.30.0.2   202.20.3.10  TCP       54 49716 → 21 [ACK] Seq=133 Ack=483 Win=2101760 Len=0
```

```
> Transmission Control Protocol, Src Port: 21, Dst Port: 49716, Seq: 351, Ack: 106, Len: 49
v File Transfer Protocol (FTP)
  v 227 Entering Passive Mode (202,20,3,10,197,83).\r\n
        Response code: Entering Passive Mode (227)
        Response arg: Entering Passive Mode (202,20,3,10,197,83).
        Passive IP address: 202.20.3.10
        Passive port: 50515
  [Current working directory: /]
```

```
0000  00 50 56 bd 87 18 00 50  56 bd a6 d7 08 00 45 00   ·PV····P V·····E·
0010  00 59 19 a1 40 00 3d 06  aa bf ca 14 03 0a ac 1e   ·Y··@·=· ········
0020  00 02 00 15 c2 34 75 77  e2 0f 2d d3 ce 7d 50 18   ·····4uw ··-··}P·
0030  01 f6 a3 f3 00 00 32 32  37 20 45 6e 74 65 72 69   ······22 7 Enteri
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 37   (202,20, 3,10,197
0060  2c 38 33 29 2e 0d 0a                               ,83).··
```

Passive FTP server port (ftp.passive.port), 6 bytes | Packets: 415 · Displayed: 214 (51.6%) · Dropped: 0 (0.0%) | Profile: Default

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 10:59:13
Alexis Cherpes
Expression...
7:59 AM
4/15/2025

tcp.port == 21

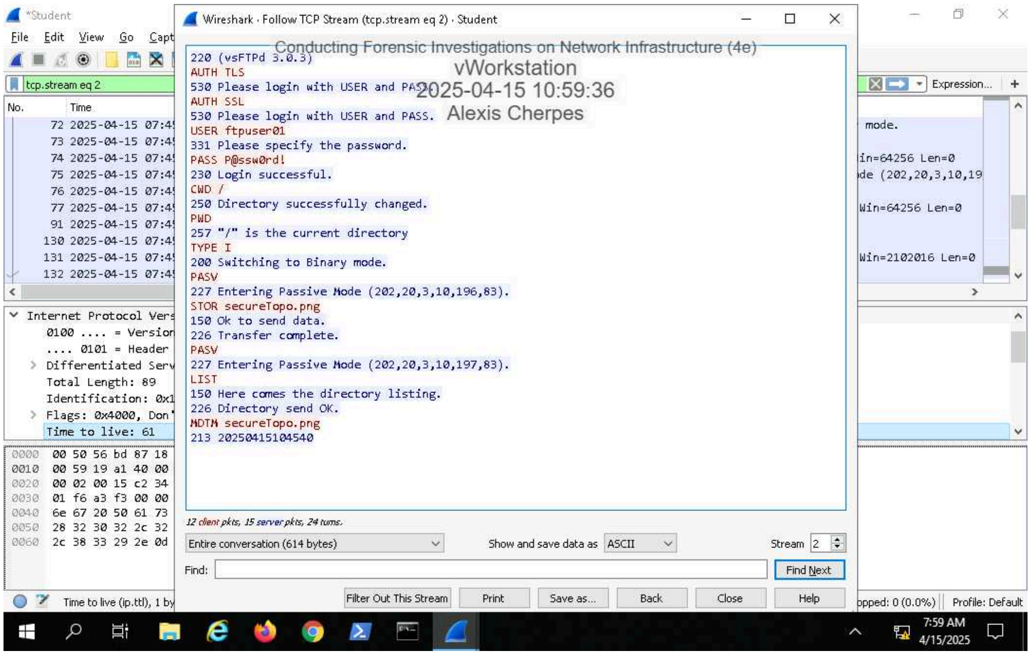
```
No.  Time                       Source       Destination  Protocol Length Info
 131 2025-04-15 07:45:40.544112 172.30.0.2   202.20.3.10  TCP      54 49716 → 21 [ACK] Seq=100 Ack=351 Win=2102016 Len=0
 132 2025-04-15 07:45:40.549665 172.30.0.2   202.20.3.10  FTP      60 Request: PASV
 133 2025-04-15 07:45:40.550077 202.20.3.10  172.30.0.2   FTP     103 Response: 227 Entering Passive Mode (202,20,3,10,19
 134 2025-04-15 07:45:40.552903 172.30.0.2   202.20.3.10  FTP      60 Request: LIST
 138 2025-04-15 07:45:40.553647 202.20.3.10  172.30.0.2   FTP      93 Response: 150 Here comes the directory listing.
 143 2025-04-15 07:45:40.553939 202.20.3.10  172.30.0.2   FTP      78 Response: 226 Directory send OK.
 144 2025-04-15 07:45:40.553953 172.30.0.2   202.20.3.10  TCP      54 49716 → 21 [ACK] Seq=112 Ack=463 Win=2101760 Len=0
 146 2025-04-15 07:45:40.554778 172.30.0.2   202.20.3.10  FTP      75 Request: MDTM secureTopo.png
 147 2025-04-15 07:45:40.555025 202.20.3.10  172.30.0.2   FTP      74 Response: 213 20250415104540
 148 2025-04-15 07:45:40.568072 172.30.0.2   202.20.3.10  TCP      54 49716 → 21 [ACK] Seq=133 Ack=483 Win=2101760 Len=0
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 89
    Identification: 0x19a1 (6561)
  > Flags: 0x4000, Don't fragment
    Time to live: 61
    Protocol: TCP (6)
```

```
0000  00 50 56 bd 87 18 00 50  56 bd a6 d7 08 00 45 00   ·PV····P V·····E·
0010  00 59 19 a1 40 00 3d 06  aa bf ca 14 03 0a ac 1e   ·Y··@·=· ········
0020  00 02 00 15 c2 34 75 77  e2 0f 2d d3 ce 7d 50 18   ·····4uw ··-··}P·
0030  01 f6 a3 f3 00 00 32 32  37 20 45 6e 74 65 72 69   ······22 7 Enteri
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 37   (202,20, 3,10,197
0060  2c 38 33 29 2e 0d 0a                               ,83).··
```

Time to live (ip.ttl), 1 byte | Packets: 415 · Displayed: 214 (51.6%) · Dropped: 0 (0.0%) | Profile: Default

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



```
220 (vsFTPd 3.0.3)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER ftpuser01
331 Please specify the password.
PASS P@ssw0rd!
230 Login successful.
CWD /
250 Directory successfully changed.
PWD
257 "/" is the current directory
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (202,20,3,10,196,83).
STOR secureTopo.png
150 Ok to send data.
226 Transfer complete.
PASV
227 Entering Passive Mode (202,20,3,10,197,83).
LIST
150 Here comes the directory listing.
226 Directory send OK.
MDTM secureTopo.png
213 20250415104540
```

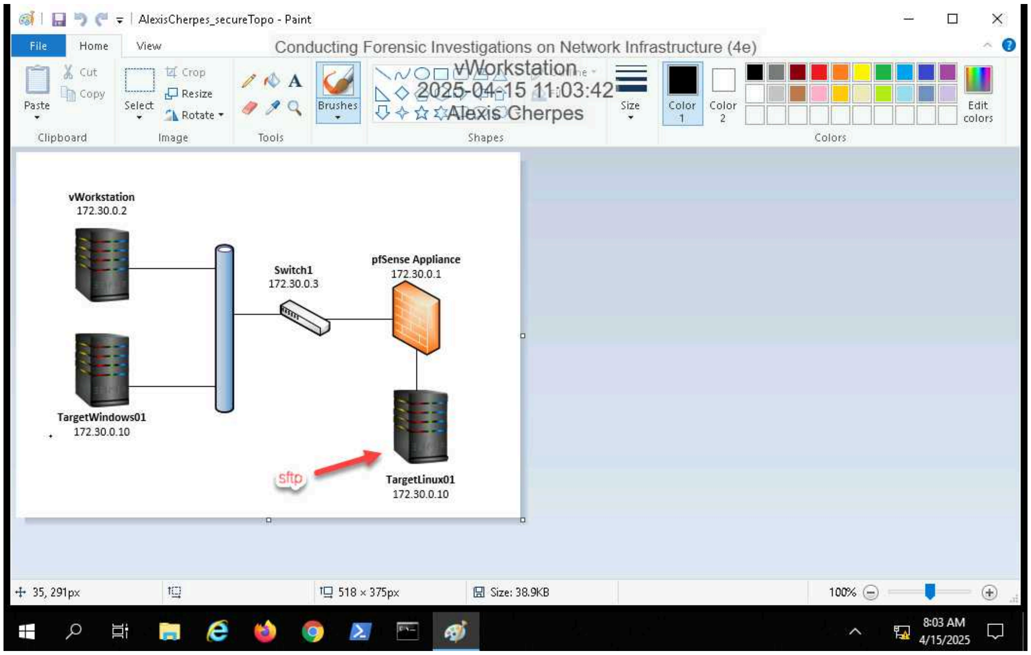
12 client pkts, 15 server pkts, 24 turns.

Entire conversation (614 bytes) | Show and save data as: ASCII | Stream: 2

Find:

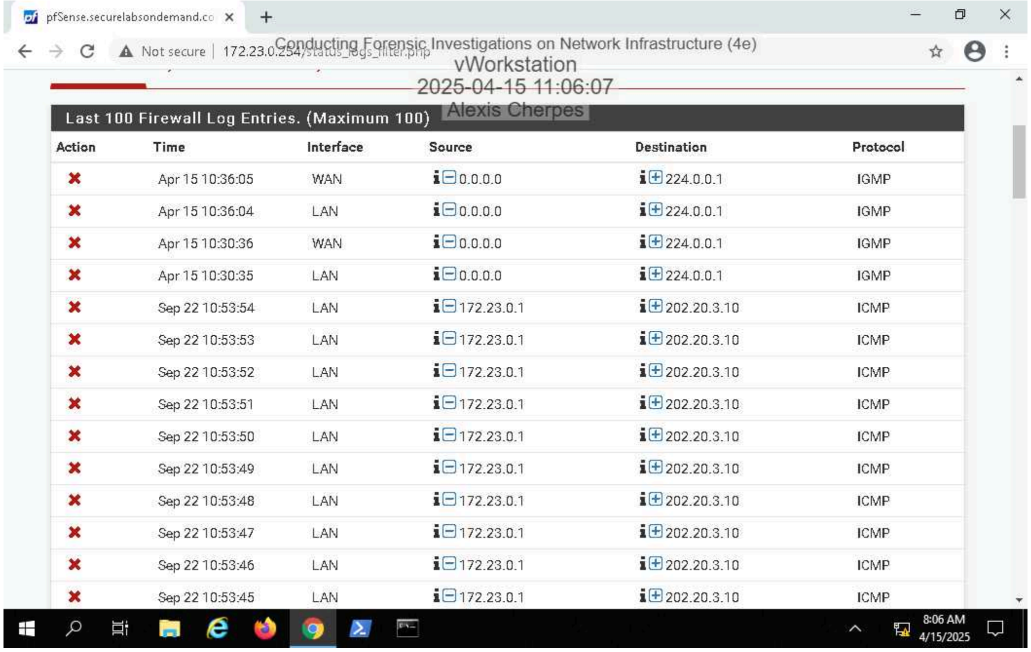
Time to live (ip.ttl), 1 by... | ...opped: 0 (0.0%) | Profile: Default

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



Part 2: Analyze a Firewall for Forensic Evidence

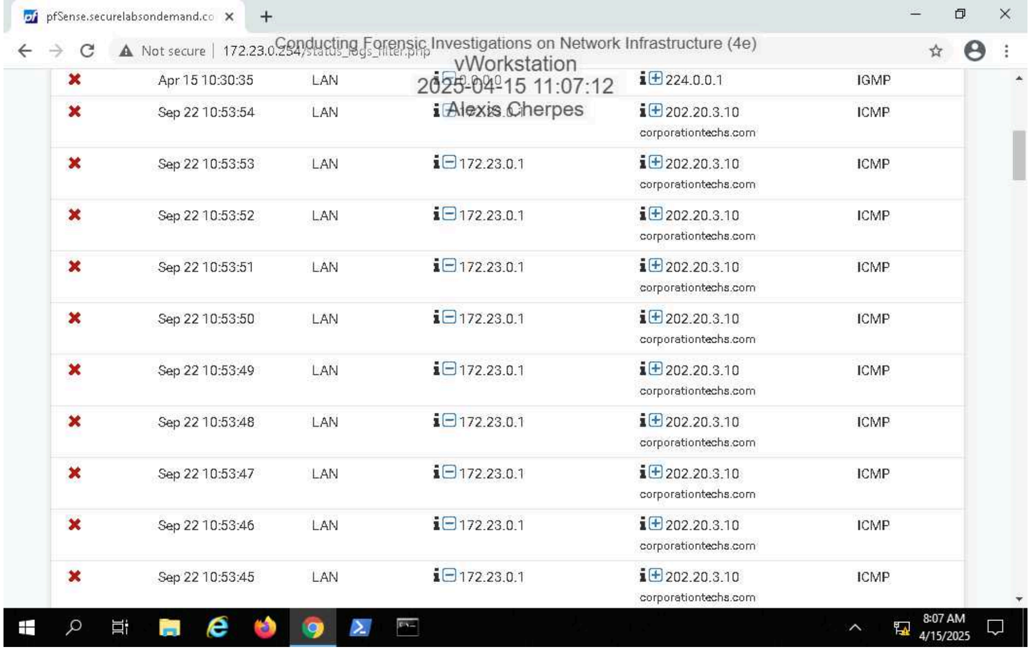
9. **Make a screen capture** showing the **entries in the firewall log**.


pfSense.securelabsondemand.co
Not secure | 172.23.0.254/status_logs_filter.php
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 11:06:07
Alexis Cherpes
8:06 AM
4/15/2025

Last 100 Firewall Log Entries. (Maximum 100)

Action	Time	Interface	Source	Destination	Protocol
✖	Apr 15 10:36:05	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 15 10:36:04	LAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 15 10:30:36	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 15 10:30:35	LAN	0.0.0.0	224.0.0.1	IGMP
✖	Sep 22 10:53:54	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:53	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:52	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:51	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:50	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:49	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:48	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:47	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:46	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:45	LAN	172.23.0.1	202.20.3.10	ICMP

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



pfSense.securelabsondemand.co
Not secure | 172.23.0.254/status_logs_filter.php

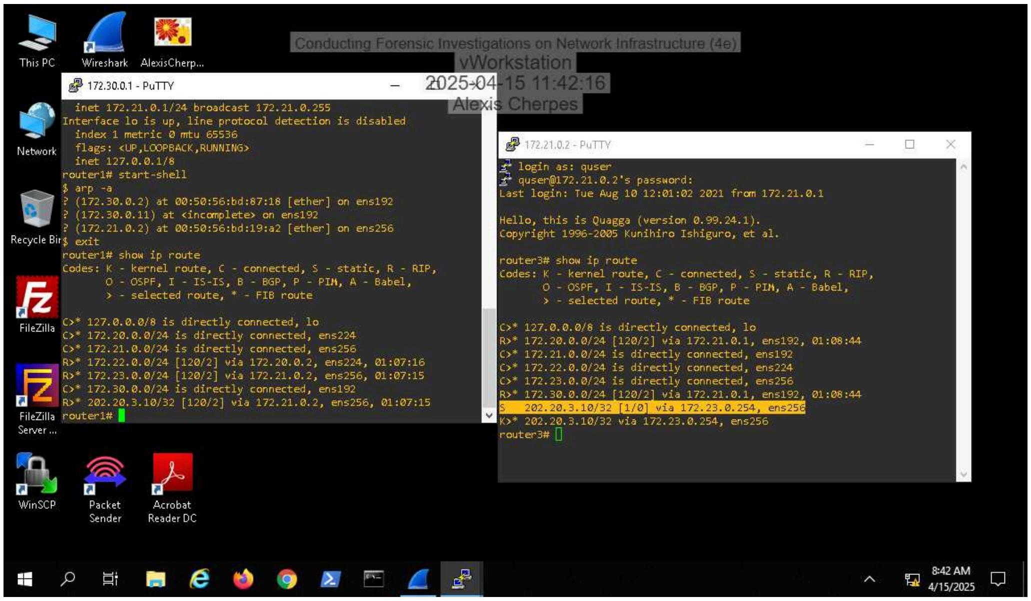
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-04-15 11:07:12
Alexis Cherpes

✖	Apr 15 10:30:35	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

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**.



```
  inet 172.21.0.1/24 broadcast 172.21.0.255
Interface lo is up, line protocol detection is disabled
  index 1 metric 0 mtu 65536
  flags: <UP,LOOPBACK,RUNNING>
  inet 127.0.0.1/8
router1# start-shell
$ arp -a
? (172.30.0.2) at 00:50:56:bd:87:18 [ether] on ens192
? (172.30.0.11) at <incomplete> on ens192
? (172.21.0.2) at 00:50:56:bd:19:a2 [ether] on ens256
$ exit
router1# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 172.20.0.0/24 is directly connected, ens224
C>* 172.21.0.0/24 is directly connected, ens256
R>* 172.22.0.0/24 [120/2] via 172.20.0.2, ens224, 01:07:16
R>* 172.23.0.0/24 [120/2] via 172.21.0.2, ens256, 01:07:15
C>* 172.30.0.0/24 is directly connected, ens192
R>* 202.20.3.10/32 [120/2] via 172.21.0.2, ens256, 01:07:15
router1#
```

```
login as: quser
quser@172.21.0.2's password:
Last login: Tue Aug 10 12:01:02 2021 from 172.21.0.1

Hello, this is Quagga (version 0.99.24.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

router3# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
R>* 172.20.0.0/24 [120/2] via 172.21.0.1, ens192, 01:08:44
C>* 172.21.0.0/24 is directly connected, ens192
C>* 172.22.0.0/24 is directly connected, ens224
C>* 172.23.0.0/24 is directly connected, ens256
R>* 172.30.0.0/24 [120/2] via 172.21.0.1, ens192, 01:08:44
S   202.20.3.10/32 [1/0] via 172.23.0.254, ens256
K>* 202.20.3.10/32 via 172.23.0.254, ens256
router3#
```

Part 2: Identify Suspicious Outgoing Connections

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

The destination IP is 202.20.3.10. The destination Port Number is 1337.