Student: Karan Atul Vora	Email: kxv230021@utdallas.edu

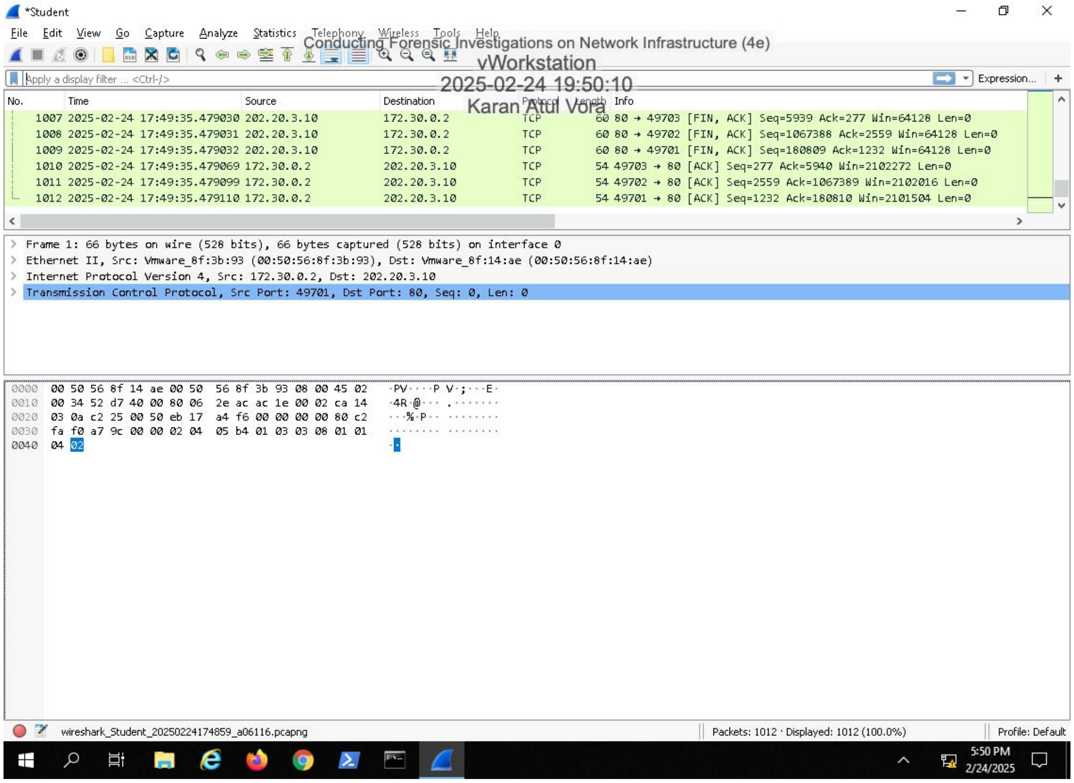
Time on Task: 1 hour, 1 minute	Progress: 100%

Report Generated: Monday, February 24, 2025 at 9:48 PM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

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



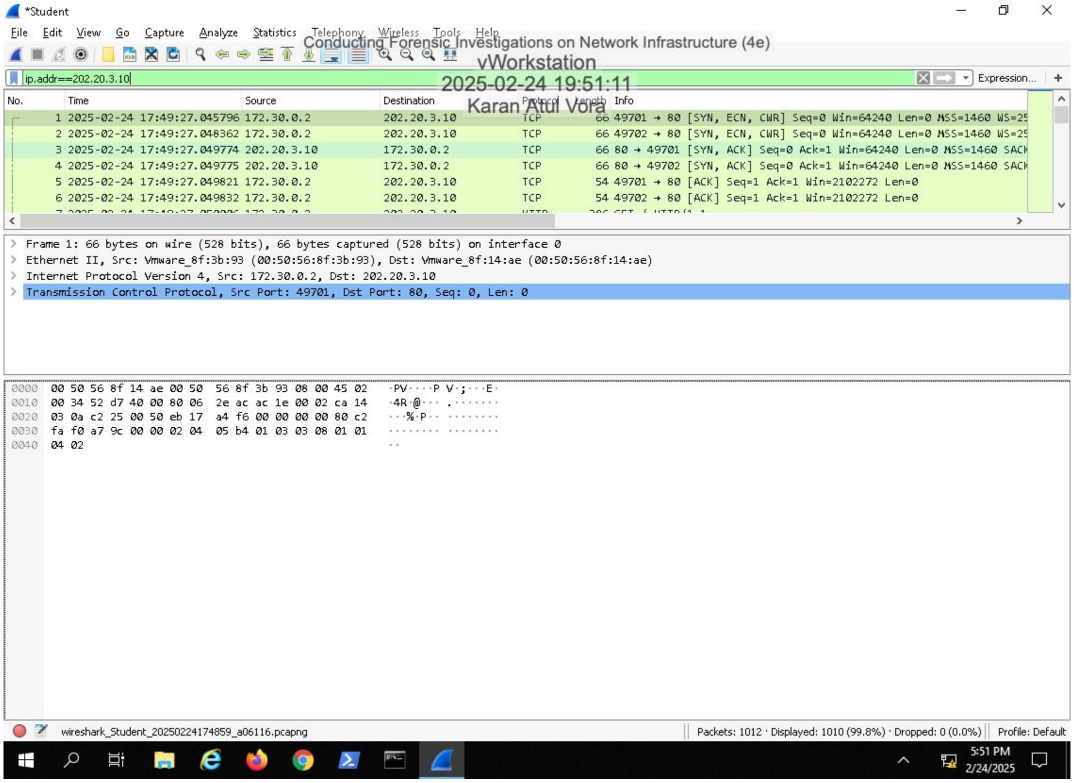
```
No.  Time                          Source        Destination   Protocol Length Info
1007 2025-02-24 17:49:35.479030 202.20.3.10   172.30.0.2    TCP      60 80 → 49703 [FIN, ACK] Seq=5939 Ack=277 Win=64128 Len=0
1008 2025-02-24 17:49:35.479031 202.20.3.10   172.30.0.2    TCP      60 80 → 49702 [FIN, ACK] Seq=1067388 Ack=2559 Win=64128 Len=0
1009 2025-02-24 17:49:35.479032 202.20.3.10   172.30.0.2    TCP      60 80 → 49701 [FIN, ACK] Seq=180809 Ack=1232 Win=64128 Len=0
1010 2025-02-24 17:49:35.479069 172.30.0.2    202.20.3.10   TCP      54 49703 → 80 [ACK] Seq=277 Ack=5940 Win=2102272 Len=0
1011 2025-02-24 17:49:35.479099 172.30.0.2    202.20.3.10   TCP      54 49702 → 80 [ACK] Seq=2559 Ack=1067389 Win=2102016 Len=0
1012 2025-02-24 17:49:35.479110 172.30.0.2    202.20.3.10   TCP      54 49701 → 80 [ACK] Seq=1232 Ack=180810 Win=2101504 Len=0
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_8f:3b:93 (00:50:56:8f:3b:93), Dst: Vmware_8f:14:ae (00:50:56:8f:14:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49701, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 8f 14 ae 00 50  56 8f 3b 93 08 00 45 02   ·PV····P V·;···E·
0010  00 34 52 d7 40 00 80 06  2e ac ac 1e 00 02 ca 14   ·4R·@··· .·······
0020  03 0a c2 25 00 50 eb 17  a4 f6 00 00 00 00 80 c2   ···%·P·· ········
0030  fa f0 a7 9c 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

wireshark_Student_20250224174859_a06116.pcapng | Packets: 1012 · Displayed: 1012 (100.0%) | Profile: Default

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



ip.addr==202.20.3.10

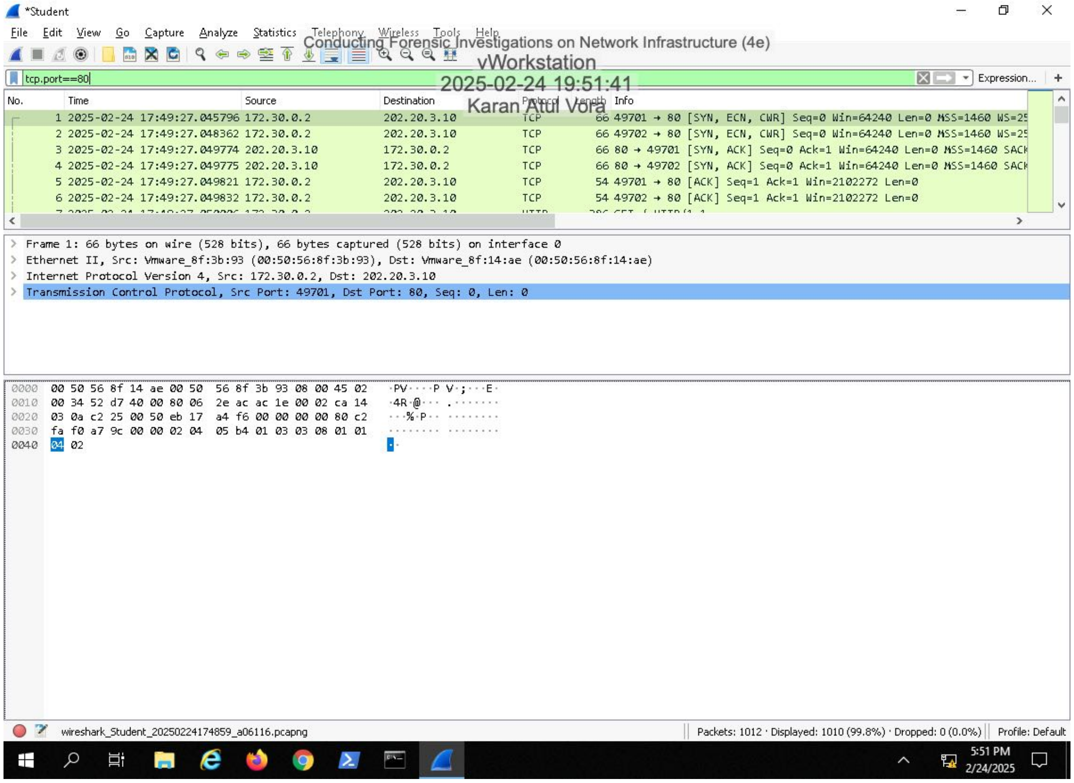
```
No.   Time                       Source        Destination   Protocol Length Info
    1 2025-02-24 17:49:27.045796 172.30.0.2    202.20.3.10   TCP      66 49701 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
    2 2025-02-24 17:49:27.048362 172.30.0.2    202.20.3.10   TCP      66 49702 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
    3 2025-02-24 17:49:27.049774 202.20.3.10   172.30.0.2    TCP      66 80 → 49701 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
    4 2025-02-24 17:49:27.049775 202.20.3.10   172.30.0.2    TCP      66 80 → 49702 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
    5 2025-02-24 17:49:27.049821 172.30.0.2    202.20.3.10   TCP      54 49701 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
    6 2025-02-24 17:49:27.049832 172.30.0.2    202.20.3.10   TCP      54 49702 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_8f:3b:93 (00:50:56:8f:3b:93), Dst: Vmware_8f:14:ae (00:50:56:8f:14:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49701, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 8f 14 ae 00 50  56 8f 3b 93 08 00 45 02   ·PV····P V·;···E·
0010  00 34 52 d7 40 00 80 06  2e ac ac 1e 00 02 ca 14   ·4R·@··· .·······
0020  03 0a c2 25 00 50 eb 17  a4 f6 00 00 00 00 80 c2   ···%·P·· ········
0030  fa f0 a7 9c 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

wireshark_Student_20250224174859_a06116.pcapng | Packets: 1012 · Displayed: 1010 (99.8%) · Dropped: 0 (0.0%) | Profile: Default

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



tcp.port==80

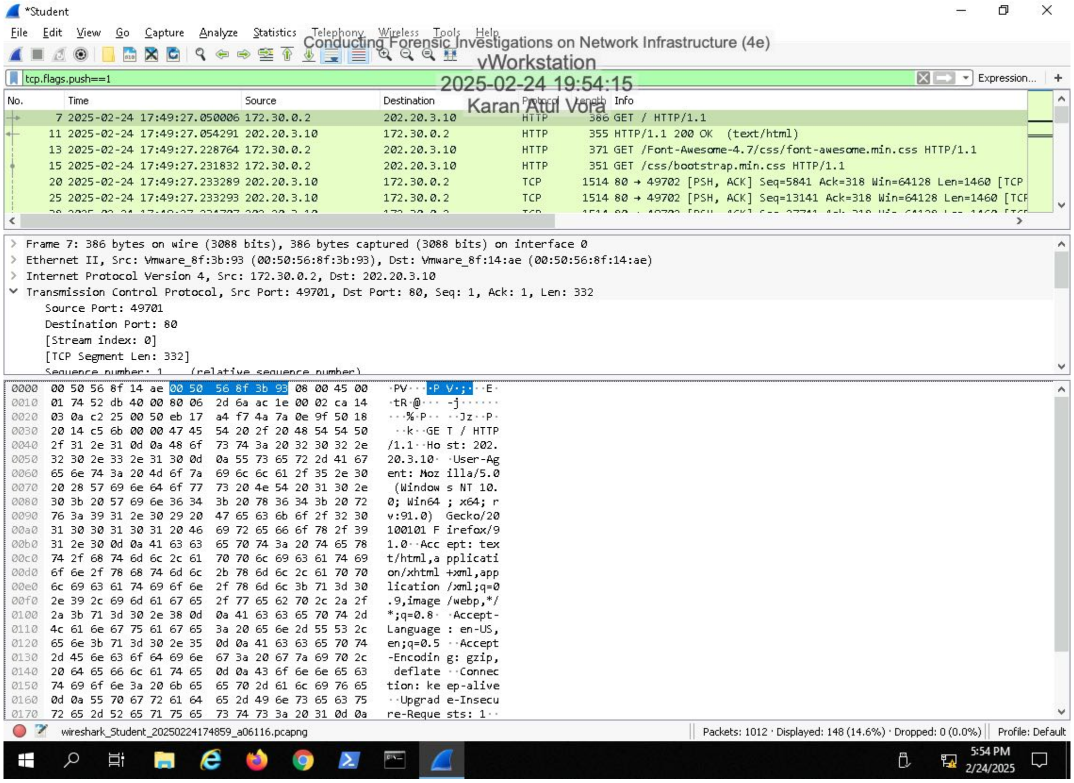
```
No.  Time                        Source       Destination  Protocol Length Info
   1 2025-02-24 17:49:27.045796 172.30.0.2   202.20.3.10  TCP      66 49701 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
   2 2025-02-24 17:49:27.048362 172.30.0.2   202.20.3.10  TCP      66 49702 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
   3 2025-02-24 17:49:27.049774 202.20.3.10  172.30.0.2   TCP      66 80 → 49701 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
   4 2025-02-24 17:49:27.049775 202.20.3.10  172.30.0.2   TCP      66 80 → 49702 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
   5 2025-02-24 17:49:27.049821 172.30.0.2   202.20.3.10  TCP      54 49701 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
   6 2025-02-24 17:49:27.049832 172.30.0.2   202.20.3.10  TCP      54 49702 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_8f:3b:93 (00:50:56:8f:3b:93), Dst: Vmware_8f:14:ae (00:50:56:8f:14:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49701, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 8f 14 ae 00 50  56 8f 3b 93 08 00 45 02   ·PV····P V·;···E·
0010  00 34 52 d7 40 00 80 06  2e ac ac 1e 00 02 ca 14   ·4R·@··· .·······
0020  03 0a c2 25 00 50 eb 17  a4 f6 00 00 00 00 80 c2   ···%·P·· ········
0030  fa f0 a7 9c 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

wireshark_Student_20250224174859_a06116.pcapng | Packets: 1012 · Displayed: 1010 (99.8%) · Dropped: 0 (0.0%) | Profile: Default

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



tcp.flags.push==1

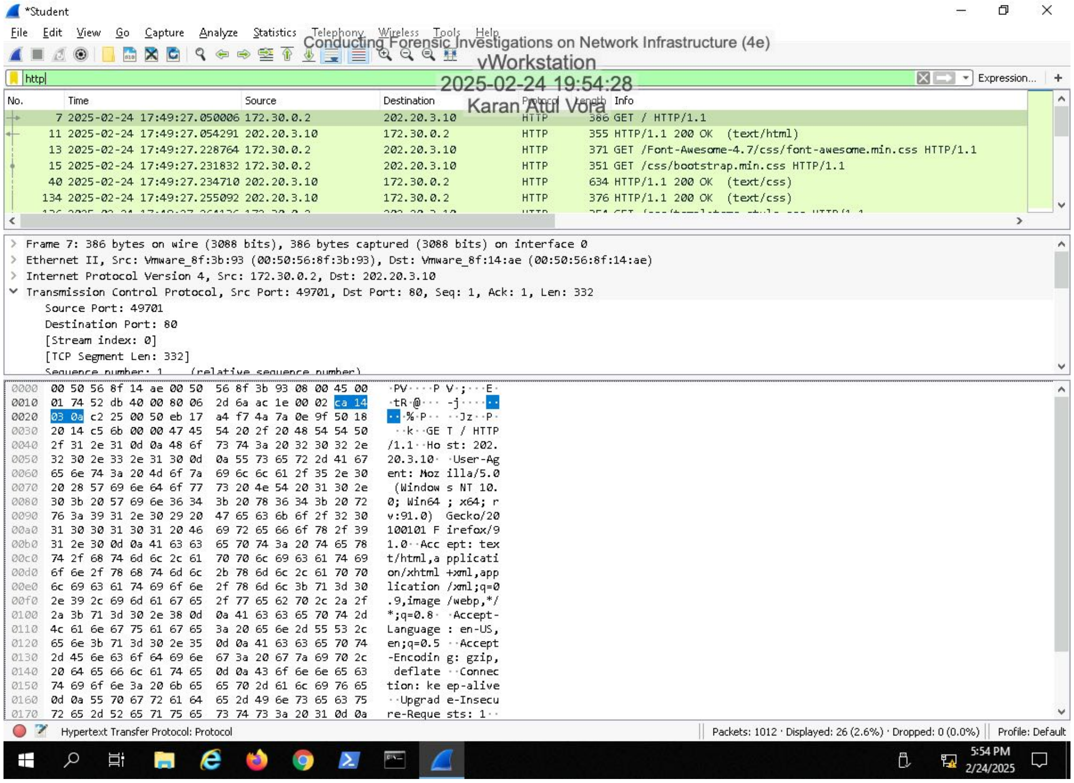
```
No.   Time                        Source        Destination   Protocol Length Info
    7 2025-02-24 17:49:27.050006 172.30.0.2    202.20.3.10   HTTP      386 GET / HTTP/1.1
   11 2025-02-24 17:49:27.054291 202.20.3.10   172.30.0.2    HTTP      355 HTTP/1.1 200 OK  (text/html)
   13 2025-02-24 17:49:27.228764 172.30.0.2    202.20.3.10   HTTP      371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP/1.1
   15 2025-02-24 17:49:27.231832 172.30.0.2    202.20.3.10   HTTP      351 GET /css/bootstrap.min.css HTTP/1.1
   20 2025-02-24 17:49:27.233289 202.20.3.10   172.30.0.2    TCP      1514 80 → 49702 [PSH, ACK] Seq=5841 Ack=318 Win=64128 Len=1460 [TCP
   25 2025-02-24 17:49:27.233293 202.20.3.10   172.30.0.2    TCP      1514 80 → 49702 [PSH, ACK] Seq=13141 Ack=318 Win=64128 Len=1460 [TCP
```

```
> Frame 7: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_8f:3b:93 (00:50:56:8f:3b:93), Dst: Vmware_8f:14:ae (00:50:56:8f:14:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
v Transmission Control Protocol, Src Port: 49701, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
    Source Port: 49701
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 332]
    Sequence number: 1    (relative sequence number)
```

```
0000  00 50 56 8f 14 ae 00 50  56 8f 3b 93 08 00 45 00   ·PV···P V·;···E·
0010  01 74 52 db 40 00 80 06  2d 6a ac 1e 00 02 ca 14   ·tR·@··· -j······
0020  03 0a c2 25 00 50 eb 17  a4 f7 4a 7a 0e 9f 50 18   ···%·P·· ··Jz··P·
0030  20 14 c5 6b 00 00 47 45  54 20 2f 20 48 54 54 50    ··k··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
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e    (Window s NT 10.
0080  30 3b 20 57 69 6e 36 34  3b 20 78 36 34 3b 20 72   0; Win64 ; x64; r
0090  76 3a 39 31 2e 30 29 20  47 65 63 6b 6f 2f 32 30   v:91.0)  Gecko/20
00a0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 39   100101 F irefox/9
00b0  31 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.0··Acc ept: tex
00c0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
00d0  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
00e0  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
00f0  2e 39 2c 69 6d 61 67 65  2f 77 65 62 70 2c 2a 2f   .9,image /webp,*/
0100  2a 3b 71 3d 30 2e 38 0d  0a 41 63 63 65 70 74 2d   *;q=0.8· ·Accept-
0110  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
0120  65 6e 3b 71 3d 30 2e 35  0d 0a 41 63 63 65 70 74   en;q=0.5 ··Accept
0130  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0140  20 64 65 66 6c 61 74 65  0d 0a 43 6f 6e 6e 65 63    deflate ··Connec
0150  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0160  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0170  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
```

wireshark_Student_20250224174859_a06116.pcapng | Packets: 1012 · Displayed: 148 (14.6%) · Dropped: 0 (0.0%) | Profile: Default

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 19:54:28
Karan Atul Vora

http

```
No.   Time                          Source        Destination   Protocol Length Info
    7 2025-02-24 17:49:27.050006 172.30.0.2     202.20.3.10   HTTP     386 GET / HTTP/1.1
   11 2025-02-24 17:49:27.054291 202.20.3.10    172.30.0.2    HTTP     355 HTTP/1.1 200 OK  (text/html)
   13 2025-02-24 17:49:27.228764 172.30.0.2     202.20.3.10   HTTP     371 GET /Font-Awesome-4.7/css/font-awesome.min.css HTTP/1.1
   15 2025-02-24 17:49:27.231832 172.30.0.2     202.20.3.10   HTTP     351 GET /css/bootstrap.min.css HTTP/1.1
   40 2025-02-24 17:49:27.234710 202.20.3.10    172.30.0.2    HTTP     634 HTTP/1.1 200 OK  (text/css)
  134 2025-02-24 17:49:27.255092 202.20.3.10    172.30.0.2    HTTP     376 HTTP/1.1 200 OK  (text/css)
```

```
> Frame 7: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_8f:3b:93 (00:50:56:8f:3b:93), Dst: Vmware_8f:14:ae (00:50:56:8f:14:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
v Transmission Control Protocol, Src Port: 49701, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
    Source Port: 49701
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 332]
    Sequence number: 1    (relative sequence number)
```

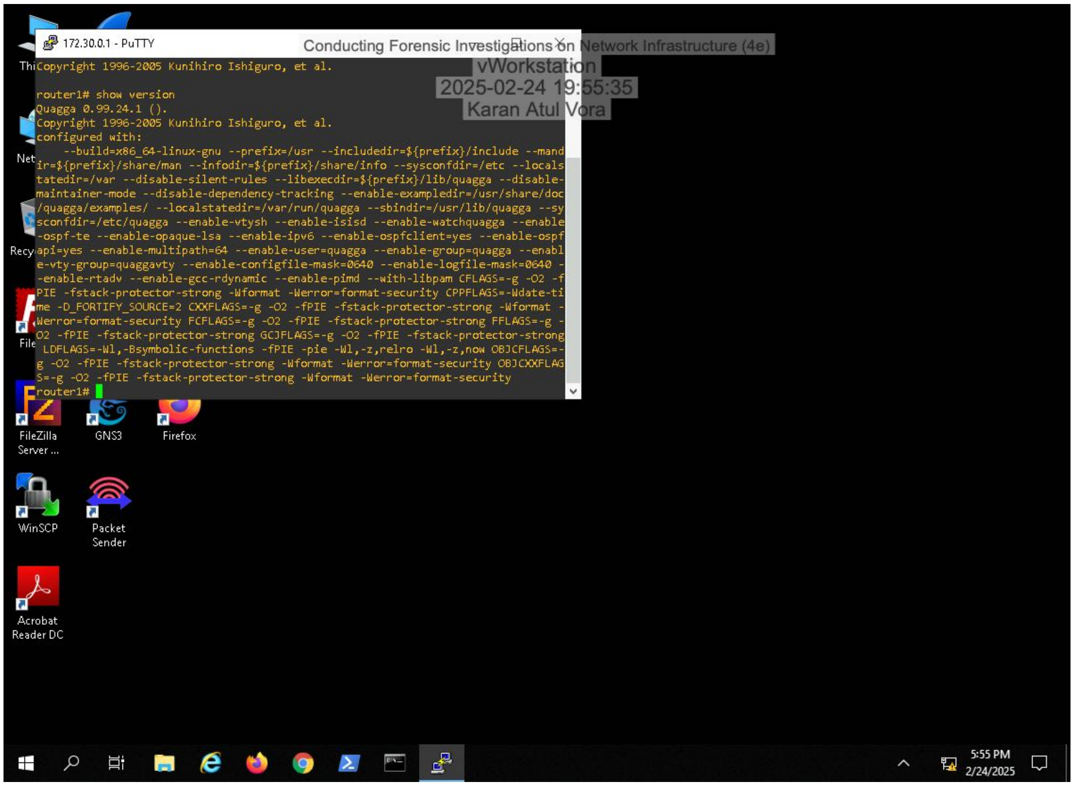
```
0000  00 50 56 8f 14 ae 00 50  56 8f 3b 93 08 00 45 00   ·PV····P V·;···E·
0010  01 74 52 db 40 00 80 06  2d 6a ac 1e 00 02 ca 14   ·tR·@··· -j······
0020  03 0a c2 25 00 50 eb 17  a4 f7 4a 7a 0e 9f 50 18   ···%·P·· ··Jz··P·
0030  20 14 c5 6b 00 00 47 45  54 20 2f 20 48 54 54 50    ··k··GE T / HTTP
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
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e    (Window s NT 10.
0080  30 3b 20 57 69 6e 36 34  3b 20 78 36 34 3b 20 72   0; Win64 ; x64; r
0090  76 3a 39 31 2e 30 29 20  47 65 63 6b 6f 2f 32 30   v:91.0)  Gecko/20
00a0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 39   100101 F irefox/9
00b0  31 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.0··Acc ept: tex
00c0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
00d0  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
00e0  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
00f0  2e 39 2c 69 6d 61 67 65  2f 77 65 62 70 2c 2a 2f   .9,image /webp,*/
0100  2a 3b 71 3d 30 2e 38 0d  0a 41 63 63 65 70 74 2d   *;q=0.8· ·Accept-
0110  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
0120  65 6e 3b 71 3d 30 2e 35  0d 0a 41 63 63 65 70 74   en;q=0.5 ··Accept
0130  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0140  20 64 65 66 6c 61 74 65  0d 0a 43 6f 6e 6e 65 63    deflate ··Connec
0150  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0160  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0170  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
```

Hypertext Transfer Protocol: Protocol | Packets: 1012 · Displayed: 26 (2.6%) · Dropped: 0 (0.0%) | Profile: Default

5:54 PM
2/24/2025

Part 2: Analyze a Router for Forensic Evidence

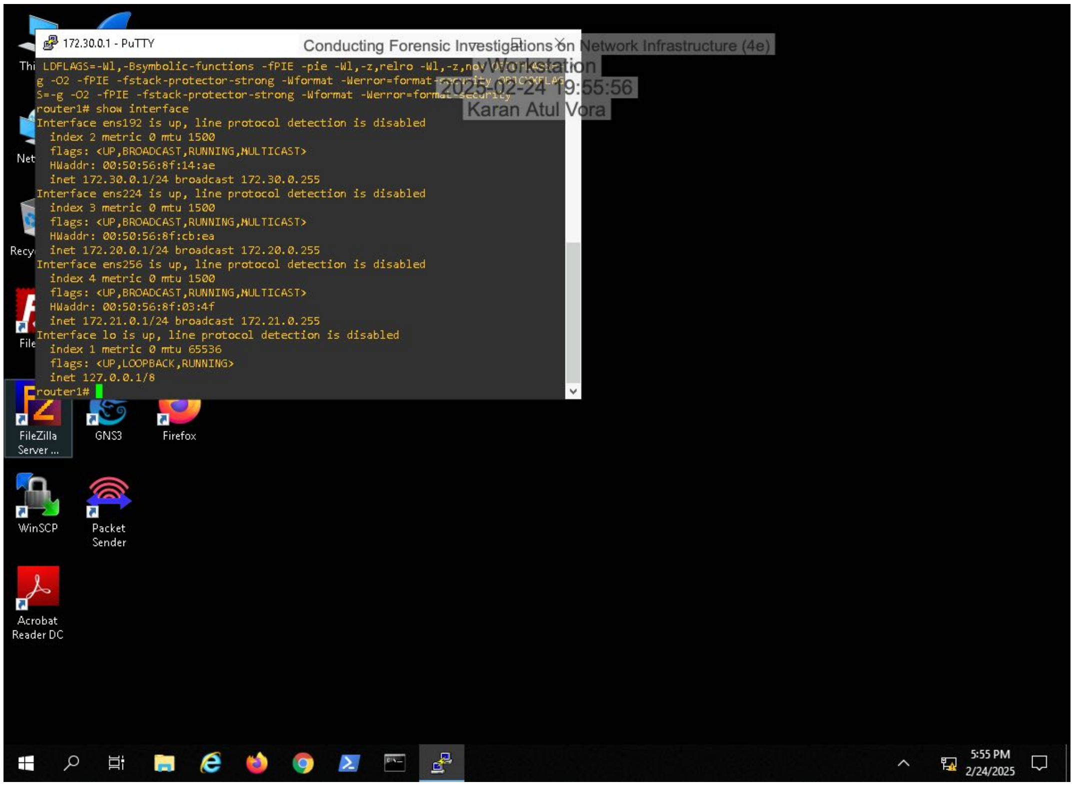
5. **Make a screen capture** showing the **router's version output**.



```
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#
```

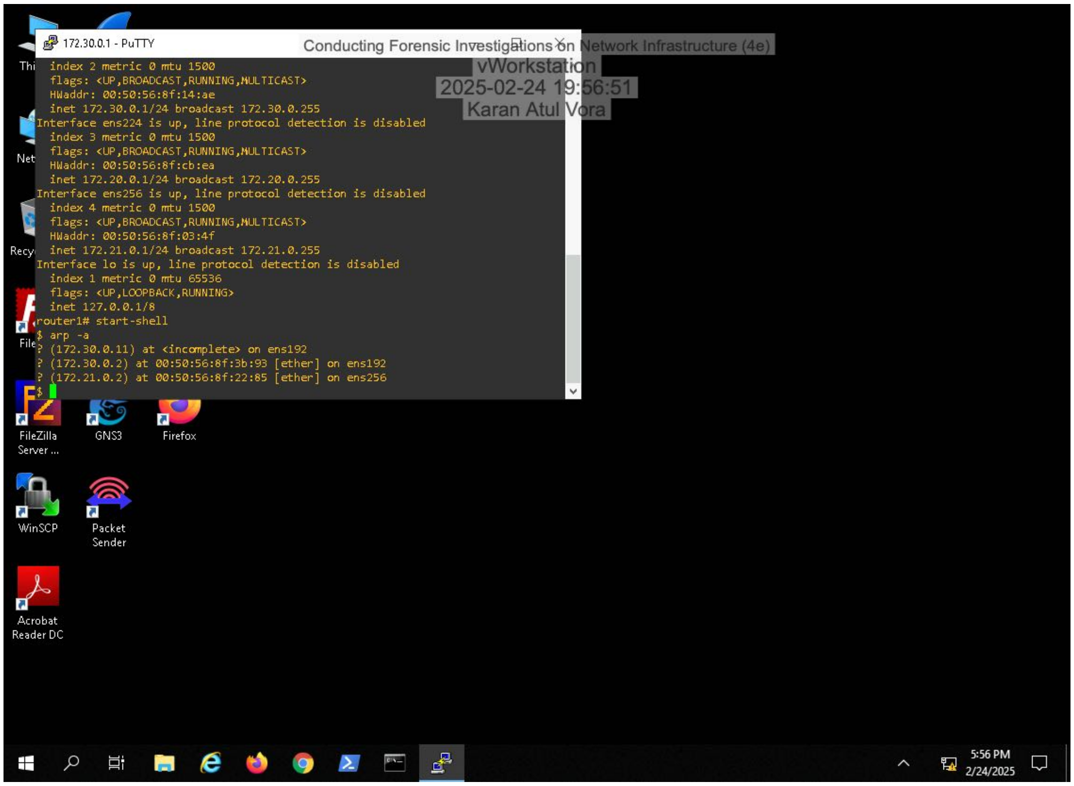
7. **Make a screen capture** showing the **router's interface details**.



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 19:55:56
Karan Atul Vora

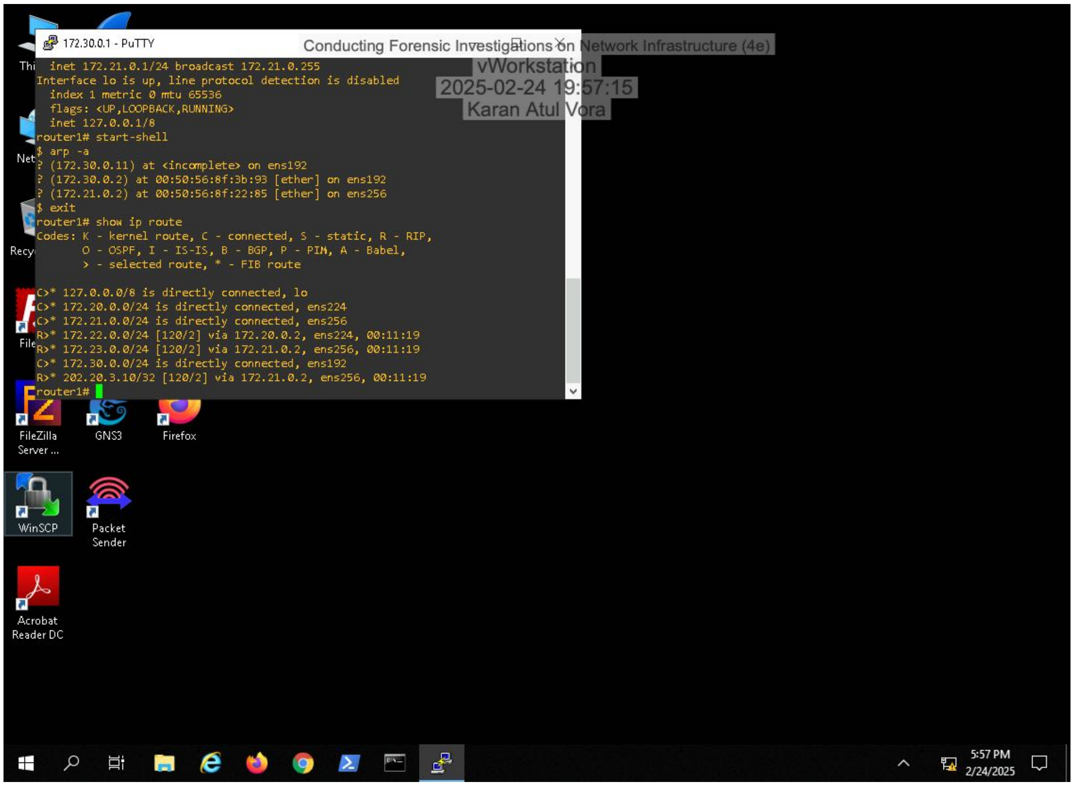
```
LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now
g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security OBJCXXFLAG
S=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1# show interface
Interface ens192 is up, line protocol detection is disabled
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8f:14:ae
  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: 00:50:56:8f:cb:ea
  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: 00:50:56:8f:03:4f
  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**.



```
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8f:14:ae
  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: 00:50:56:8f:cb:ea
  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: 00:50:56:8f:03:4f
  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
? (172.30.0.11) at <incomplete> on ens192
? (172.30.0.2) at 00:50:56:8f:3b:93 [ether] on ens192
? (172.21.0.2) at 00:50:56:8f:22:85 [ether] on ens256
$
```

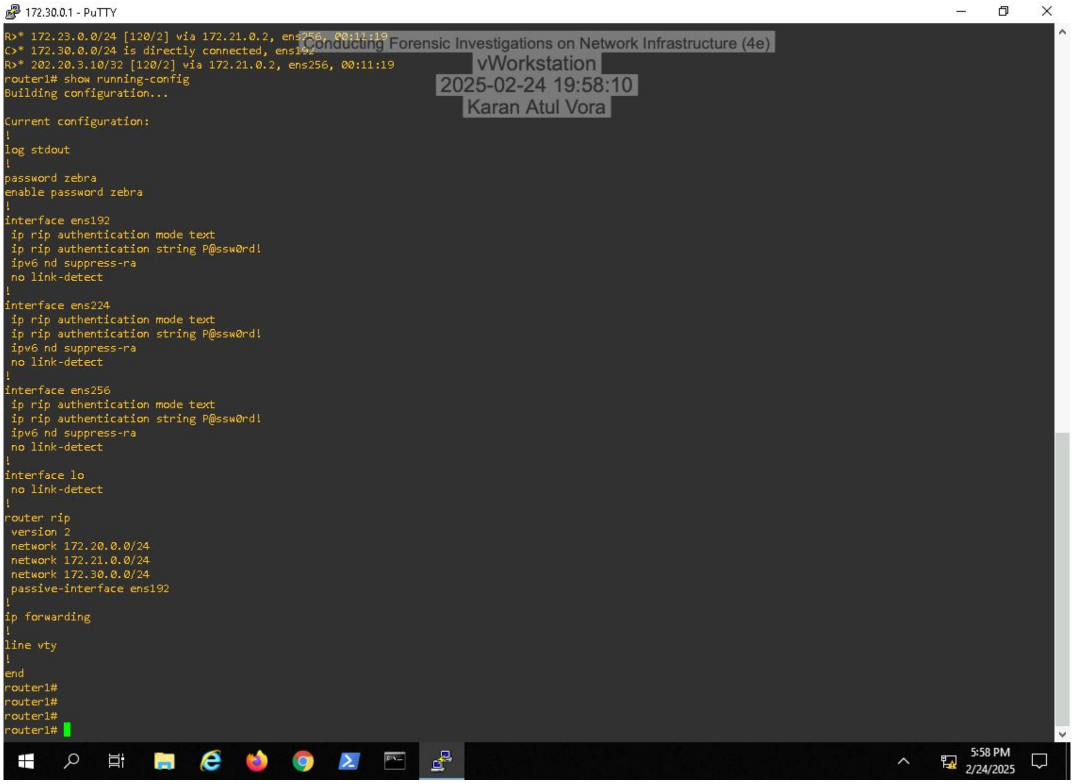
13. **Make a screen capture** showing the **IP routing table**.



```
  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
? (172.30.0.11) at <incomplete> on ens192
? (172.30.0.2) at 00:50:56:8f:3b:93 [ether] on ens192
? (172.21.0.2) at 00:50:56:8f:22:85 [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, 00:11:19
R>* 172.23.0.0/24 [120/2] via 172.21.0.2, ens256, 00:11:19
C>* 172.30.0.0/24 is directly connected, ens192
R>* 202.20.3.10/32 [120/2] via 172.21.0.2, ens256, 00:11:19
router1#
```

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



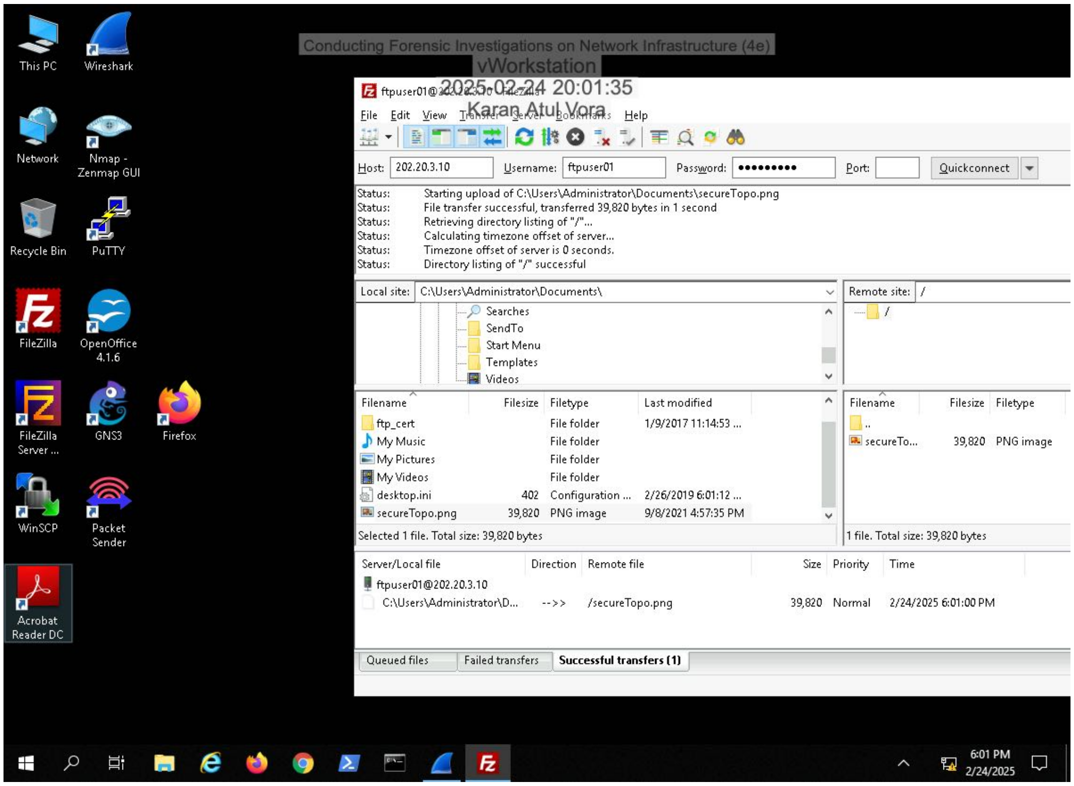
```
R>* 172.23.0.0/24 [120/2] via 172.21.0.2, ens256, 00:11:19
C>* 172.30.0.0/24 is directly connected, ens192
R>* 202.20.3.10/32 [120/2] via 172.21.0.2, ens256, 00:11:19
router1# show running-config
Building configuration...

Current configuration:
!
log stdout
!
password zebra
enable password zebra
!
interface ens192
 ip rip authentication mode text
 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#
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**.



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 20:01:35
Karan Atul Vora

Host: 202.20.3.10 Username: ftpuser01 Password: ●●●●●●●●● Port:

```
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:     Calculating timezone offset of server...
Status:     Timezone offset of server is 0 seconds.
Status:     Directory listing of "/" successful
```

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

Remote site: /

Filename	Filesize	Filetype	Last modified
ftp_cert		File folder	1/9/2017 11:14:53 ...
My Music		File folder	
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

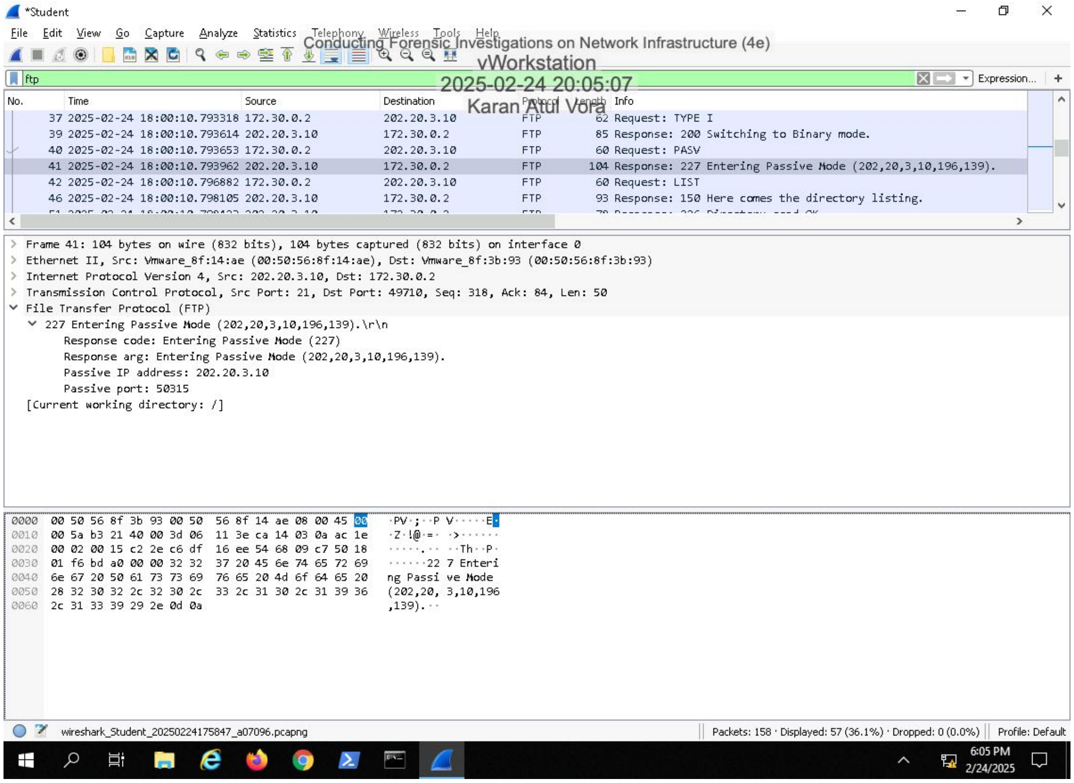
Selected 1 file. Total size: 39,820 bytes

Filename	Filesize	Filetype
..		
secureTo...	39,820	PNG image

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	2/24/2025 6:01:00 PM

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


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 20:05:07
Karan Atul Vora

Filter: ftp

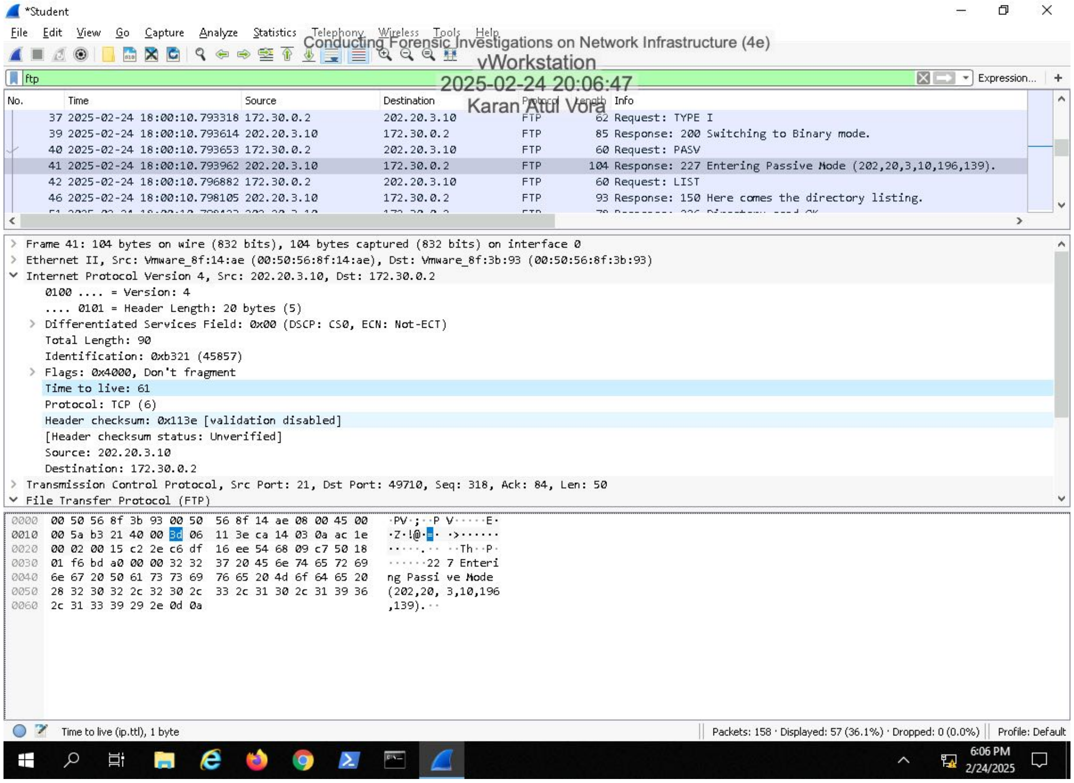
```
No.  Time                        Source       Destination  Protocol Length Info
  37 2025-02-24 18:00:10.793318 172.30.0.2   202.20.3.10  FTP       62 Request: TYPE I
  39 2025-02-24 18:00:10.793614 202.20.3.10  172.30.0.2   FTP       85 Response: 200 Switching to Binary mode.
  40 2025-02-24 18:00:10.793653 172.30.0.2   202.20.3.10  FTP       60 Request: PASV
  41 2025-02-24 18:00:10.793962 202.20.3.10  172.30.0.2   FTP      104 Response: 227 Entering Passive Mode (202,20,3,10,196,139).
  42 2025-02-24 18:00:10.796882 172.30.0.2   202.20.3.10  FTP       60 Request: LIST
  46 2025-02-24 18:00:10.798105 202.20.3.10  172.30.0.2   FTP       93 Response: 150 Here comes the directory listing.
```

```
> Frame 41: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
> Ethernet II, Src: Vmware_8f:14:ae (00:50:56:8f:14:ae), Dst: Vmware_8f:3b:93 (00:50:56:8f:3b:93)
> Internet Protocol Version 4, Src: 202.20.3.10, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49710, Seq: 318, Ack: 84, Len: 50
v File Transfer Protocol (FTP)
  v 227 Entering Passive Mode (202,20,3,10,196,139).\r\n
        Response code: Entering Passive Mode (227)
        Response arg: Entering Passive Mode (202,20,3,10,196,139).
        Passive IP address: 202.20.3.10
        Passive port: 50315
    [Current working directory: /]
```

```
0000  00 50 56 8f 3b 93 00 50  56 8f 14 ae 08 00 45 00   ·PV·;··P V·····E·
0010  00 5a b3 21 40 00 3d 06  11 3e ca 14 03 0a ac 1e   ·Z·!@·=· ·>······
0020  00 02 00 15 c2 2e c6 df  16 ee 54 68 09 c7 50 18   ······.·· ··Th··P·
0030  01 f6 bd a0 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 36   (202,20, 3,10,196
0060  2c 31 33 39 29 2e 0d 0a                            ,139).··
```

wireshark_Student_20250224175847_a07096.pcapng | Packets: 158 · Displayed: 57 (36.1%) · Dropped: 0 (0.0%) | Profile: Default

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



ftp

```
No. Time                       Source       Destination  Protocol Length Info
 37 2025-02-24 18:00:10.793318 172.30.0.2   202.20.3.10  FTP       62 Request: TYPE I
 39 2025-02-24 18:00:10.793614 202.20.3.10  172.30.0.2   FTP       85 Response: 200 Switching to Binary mode.
 40 2025-02-24 18:00:10.793653 172.30.0.2   202.20.3.10  FTP       60 Request: PASV
 41 2025-02-24 18:00:10.793962 202.20.3.10  172.30.0.2   FTP      104 Response: 227 Entering Passive Mode (202,20,3,10,196,139).
 42 2025-02-24 18:00:10.796882 172.30.0.2   202.20.3.10  FTP       60 Request: LIST
 46 2025-02-24 18:00:10.798105 202.20.3.10  172.30.0.2   FTP       93 Response: 150 Here comes the directory listing.
```

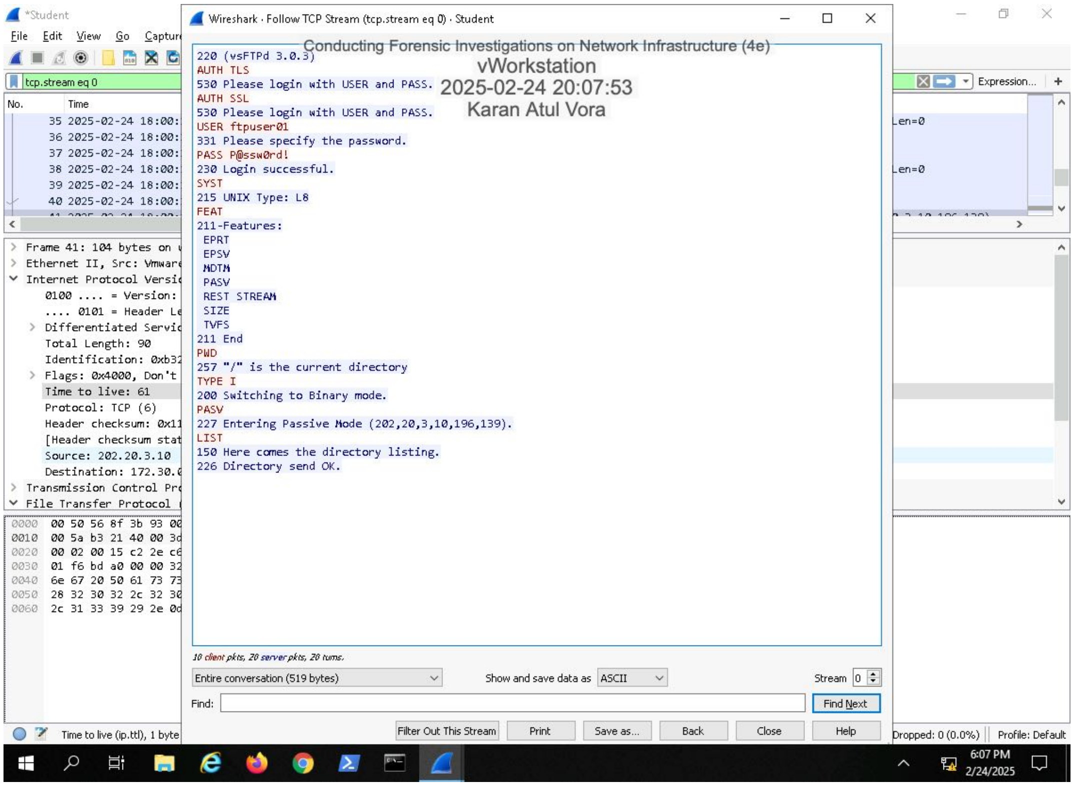
```
> Frame 41: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
> Ethernet II, Src: Vmware_8f:14:ae (00:50:56:8f:14:ae), Dst: Vmware_8f:3b:93 (00:50:56:8f:3b:93)
v Internet Protocol Version 4, Src: 202.20.3.10, Dst: 172.30.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 90
    Identification: 0xb321 (45857)
  > Flags: 0x4000, Don't fragment
    Time to live: 61
    Protocol: TCP (6)
    Header checksum: 0x113e [validation disabled]
    [Header checksum status: Unverified]
    Source: 202.20.3.10
    Destination: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49710, Seq: 318, Ack: 84, Len: 50
v File Transfer Protocol (FTP)
```

```
0000  00 50 56 8f 3b 93 00 50  56 8f 14 ae 08 00 45 00   ·PV·;··P V·····E·
0010  00 5a b3 21 40 00 3d 06  11 3e ca 14 03 0a ac 1e   ·Z·!@·=· ·>······
0020  00 02 00 15 c2 2e c6 df  16 ee 54 68 09 c7 50 18   ·····.·· ··Th··P·
0030  01 f6 bd a0 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 36   (202,20, 3,10,196
0060  2c 31 33 39 29 2e 0d 0a                            ,139).··
```

Time to live (ip.ttl), 1 byte | Packets: 158 · Displayed: 57 (36.1%) · Dropped: 0 (0.0%) | Profile: Default

6:06 PM
2/24/2025

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



Wireshark · Follow TCP Stream (tcp.stream eq 0) · Student

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 20:07:53
Karan Atul Vora

```
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.
SYST
215 UNIX Type: L8
FEAT
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
PWD
257 "/" is the current directory
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (202,20,3,10,196,139).
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

10 client pkts, 20 server pkts, 20 turns.

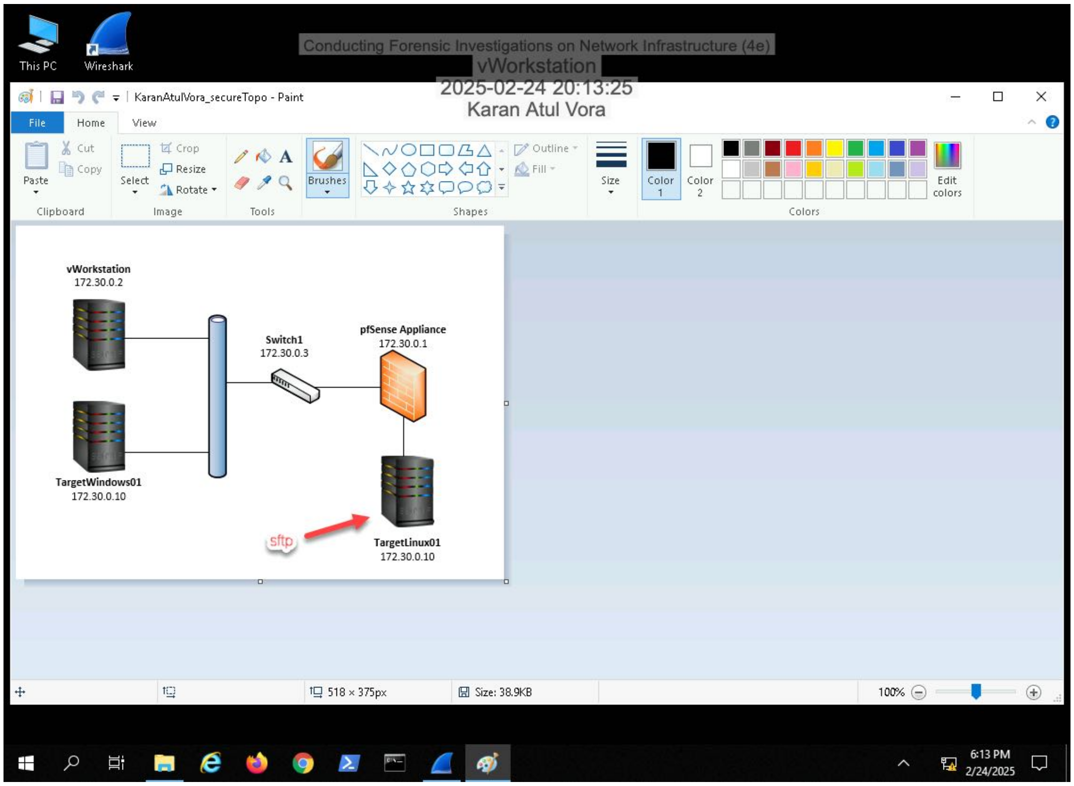
Entire conversation (519 bytes) — Show and save data as: ASCII — Stream: 0

```
35 2025-02-24 18:00:
36 2025-02-24 18:00:
37 2025-02-24 18:00:
38 2025-02-24 18:00:
39 2025-02-24 18:00:
40 2025-02-24 18:00:

> Frame 41: 104 bytes on
> Ethernet II, Src: Vmware
v Internet Protocol Versi
    0100 .... = Version:
    .... 0101 = Header Le
  > Differentiated Servic
    Total Length: 90
    Identification: 0xb32
  > Flags: 0x4000, Don't
    Time to live: 61
    Protocol: TCP (6)
    Header checksum: 0x11
    [Header checksum stat
    Source: 202.20.3.10
    Destination: 172.30.
> Transmission Control Pr
v File Transfer Protocol

0000  00 50 56 8f 3b 93 00
0010  00 5a b3 21 40 00 3d
0020  00 02 00 15 c2 2e c6
0030  01 f6 bd a0 00 00 32
0040  6e 67 20 50 61 73 73
0050  28 32 30 32 2c 32 30
0060  2c 31 33 39 29 2e 0d
```

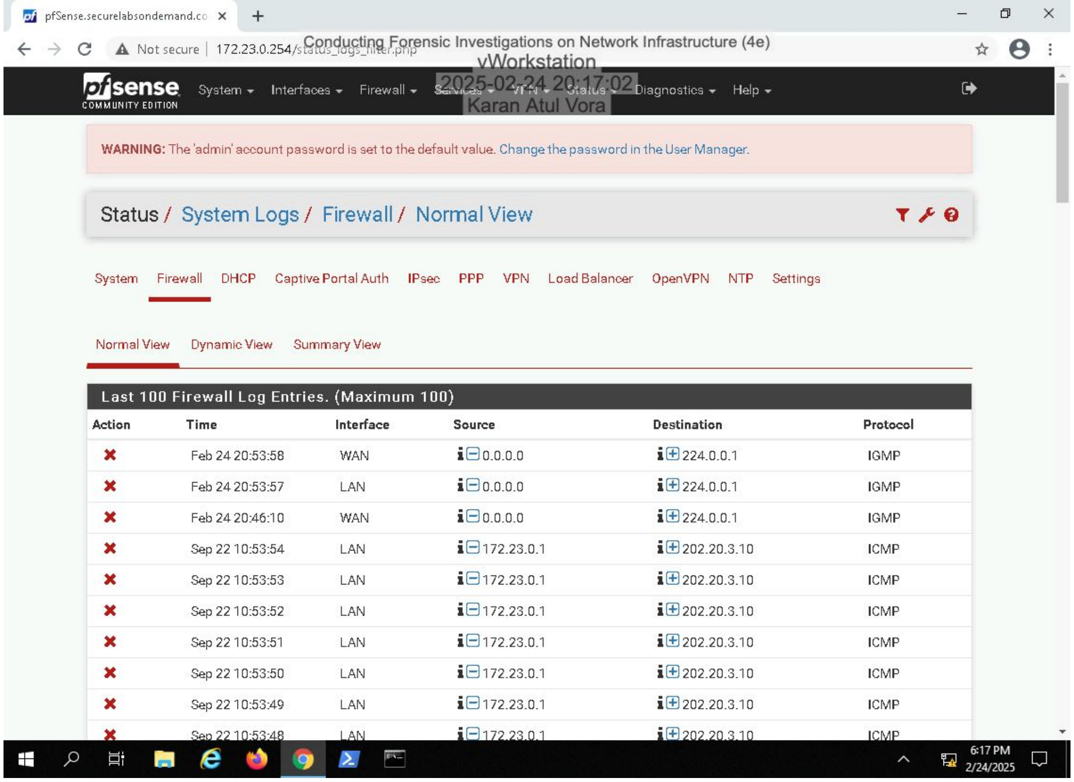
32. **Make a screen capture** showing the **reconstituted PNG file**.



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 20:13:25
Karan Atul Vora

Part 2: Analyze a Firewall for Forensic Evidence

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

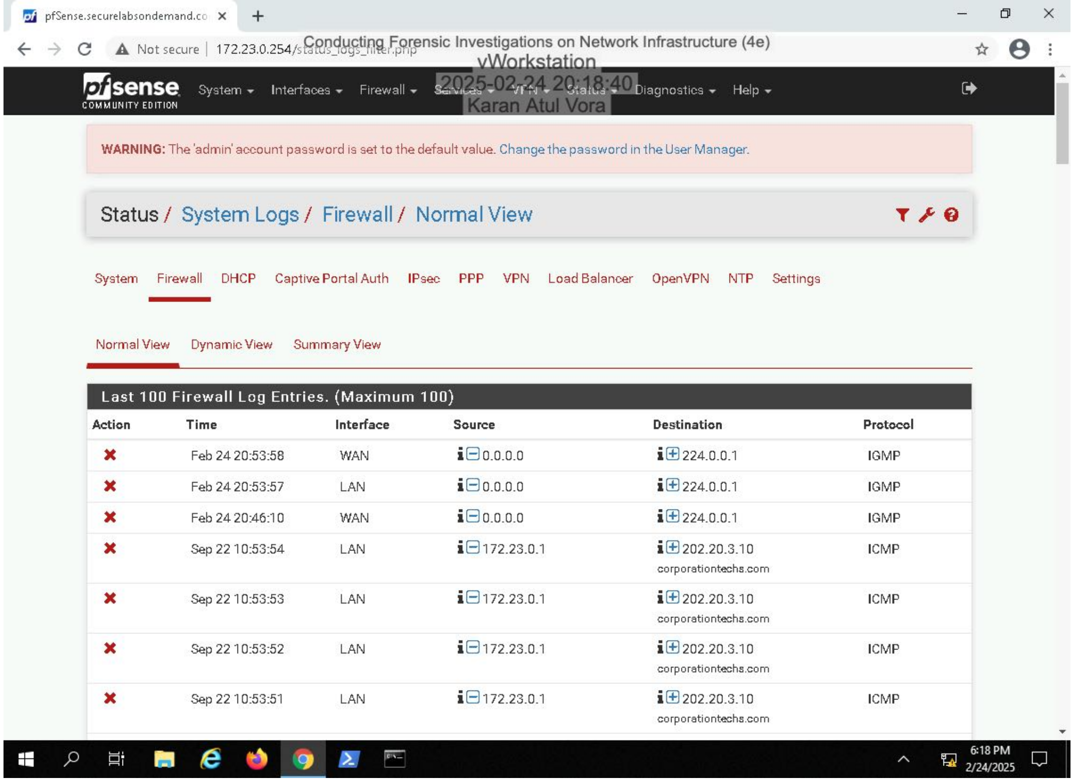


WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Last 100 Firewall Log Entries. (Maximum 100)

Action	Time	Interface	Source	Destination	Protocol
✖	Feb 24 20:53:58	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Feb 24 20:53:57	LAN	0.0.0.0	224.0.0.1	IGMP
✖	Feb 24 20:46:10	WAN	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

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
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
6:18 PM
2/24/2025

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2025-02-24 20:18:40
Karan Atul Vora

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / System Logs / Firewall / Normal View

System | Firewall | DHCP | Captive Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | NTP | Settings

Normal View | Dynamic View | Summary View

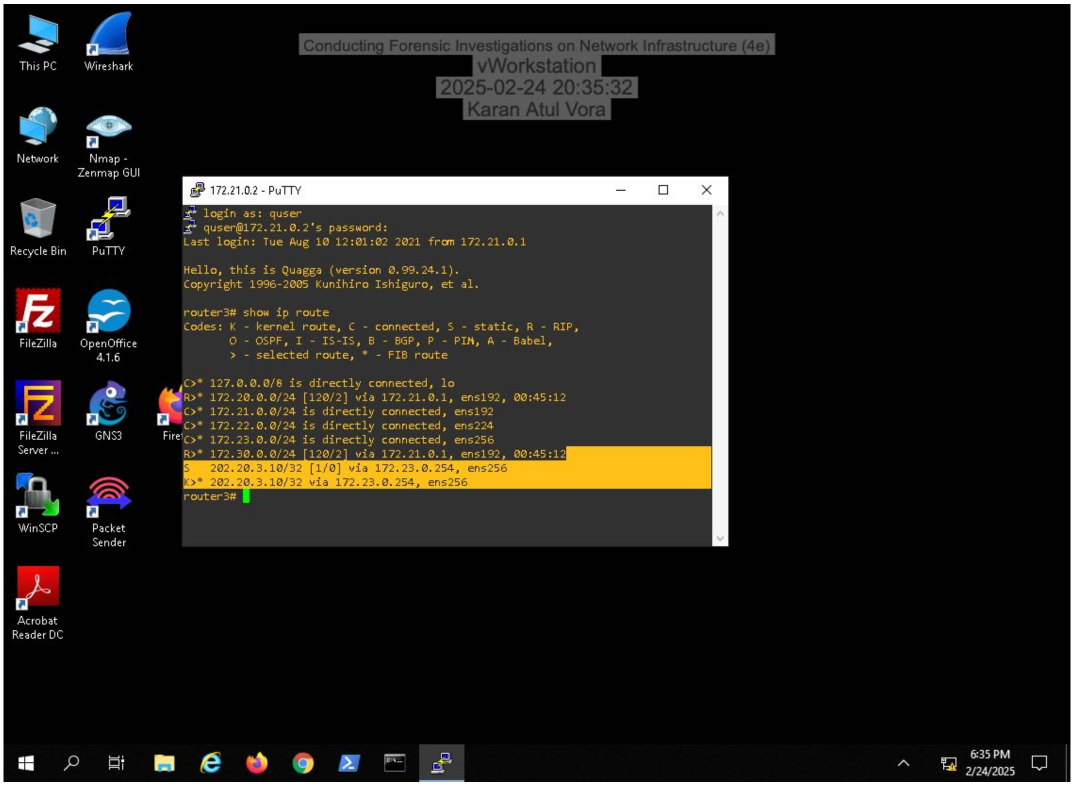
Last 100 Firewall Log Entries. (Maximum 100)

Action	Time	Interface	Source	Destination	Protocol
✖	Feb 24 20:53:58	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Feb 24 20:53:57	LAN	0.0.0.0	224.0.0.1	IGMP
✖	Feb 24 20:46:10	WAN	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

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**.



```
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, 00:45:12
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, 00:45:12
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.

202.20.3.10, 1337