Conducting Forensic Investigations on Network Infrastructure (4e)

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

Student:	Email:
muhammad zahid	zahid1mz@cmich.edu

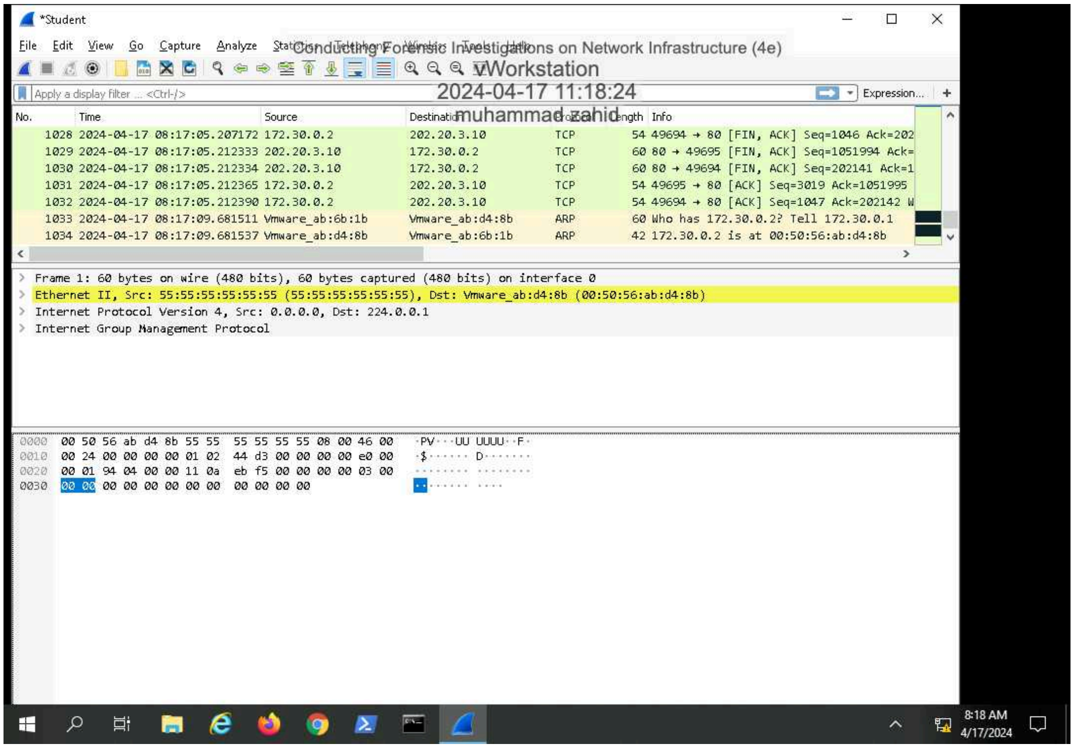
Time on Task:	Progress:
1 hour, 10 minutes	100%

Report Generated: Wednesday, April 17, 2024 at 11:44 AM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

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

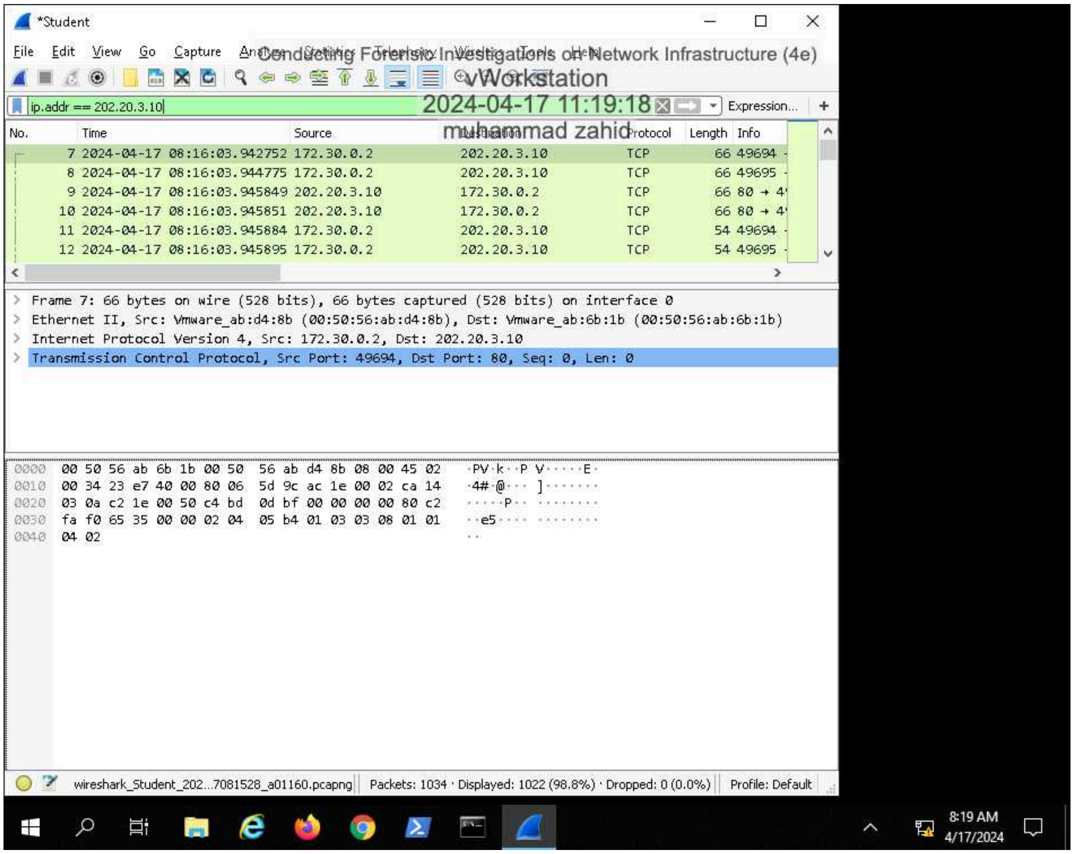


```
No.   Time                        Source             Destination        Protocol Length Info
 1028 2024-04-17 08:17:05.207172 172.30.0.2         202.20.3.10        TCP      54 49694 → 80 [FIN, ACK] Seq=1046 Ack=202
 1029 2024-04-17 08:17:05.212333 202.20.3.10        172.30.0.2         TCP      60 80 → 49695 [FIN, ACK] Seq=1051994 Ack=
 1030 2024-04-17 08:17:05.212334 202.20.3.10        172.30.0.2         TCP      60 80 → 49694 [FIN, ACK] Seq=202141 Ack=1
 1031 2024-04-17 08:17:05.212365 172.30.0.2         202.20.3.10        TCP      54 49695 → 80 [ACK] Seq=3019 Ack=1051995
 1032 2024-04-17 08:17:05.212390 172.30.0.2         202.20.3.10        TCP      54 49694 → 80 [ACK] Seq=1047 Ack=202142 W
 1033 2024-04-17 08:17:09.681511 Vmware_ab:6b:1b    Vmware_ab:d4:8b    ARP      60 Who has 172.30.0.2? Tell 172.30.0.1
 1034 2024-04-17 08:17:09.681537 Vmware_ab:d4:8b    Vmware_ab:6b:1b    ARP      42 172.30.0.2 is at 00:50:56:ab:d4:8b
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 55:55:55:55:55:55 (55:55:55:55:55:55), Dst: Vmware_ab:d4:8b (00:50:56:ab:d4:8b)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 224.0.0.1
> Internet Group Management Protocol
```

```
0000  00 50 56 ab d4 8b 55 55  55 55 55 55 08 00 46 00   ·PV···UU UUUU··F·
0010  00 24 00 00 00 00 01 02  44 d3 00 00 00 00 e0 00   ·$······ D·······
0020  00 01 94 04 00 00 11 0a  eb f5 00 00 00 00 03 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

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



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:19:18
muhammad zahid

ip.addr == 202.20.3.10

```
No.  Time                        Source        Destination   Protocol  Length  Info
   7 2024-04-17 08:16:03.942752 172.30.0.2    202.20.3.10   TCP       66 49694 -
   8 2024-04-17 08:16:03.944775 172.30.0.2    202.20.3.10   TCP       66 49695 -
   9 2024-04-17 08:16:03.945849 202.20.3.10   172.30.0.2    TCP       66 80 → 4
  10 2024-04-17 08:16:03.945851 202.20.3.10   172.30.0.2    TCP       66 80 → 4
  11 2024-04-17 08:16:03.945884 172.30.0.2    202.20.3.10   TCP       54 49694 -
  12 2024-04-17 08:16:03.945895 172.30.0.2    202.20.3.10   TCP       54 49695 -
```

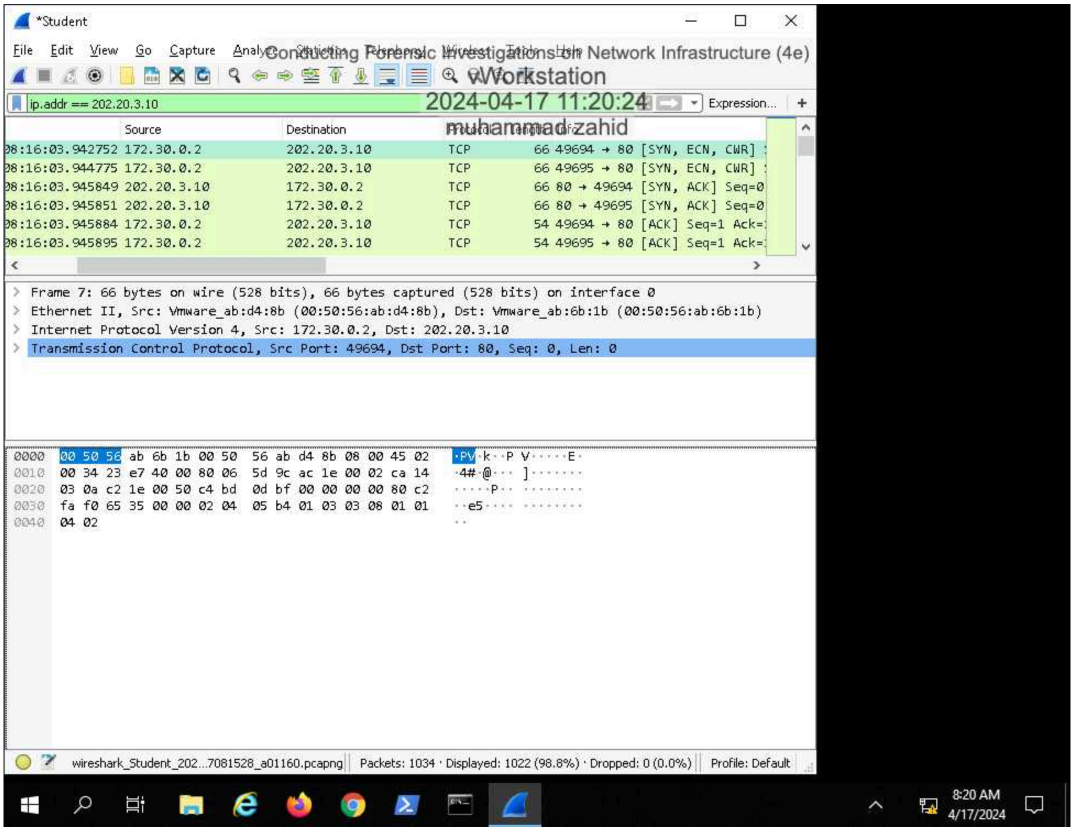
```
> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_ab:d4:8b (00:50:56:ab:d4:8b), Dst: Vmware_ab:6b:1b (00:50:56:ab:6b:1b)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49694, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 ab 6b 1b 00 50  56 ab d4 8b 08 00 45 02   ·PV·k··P V·····E·
0010  00 34 23 e7 40 00 80 06  5d 9c ac 1e 00 02 ca 14   ·4#·@··· ]·······
0020  03 0a c2 1e 00 50 c4 bd  0d bf 00 00 00 00 80 c2   ·····P·· ········
0030  fa f0 65 35 00 00 02 04  05 b4 01 03 03 08 01 01   ··e5···· ········
0040  04 02                                              ··
```

wireshark_Student_202...7081528_a01160.pcapng | Packets: 1034 · Displayed: 1022 (98.8%) · Dropped: 0 (0.0%) | Profile: Default

8:19 AM
4/17/2024

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



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:20:24
muhammad zahid

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

```
08:16:03.942752 172.30.0.2    202.20.3.10   TCP   66 49694 → 80 [SYN, ECN, CWR]
08:16:03.944775 172.30.0.2    202.20.3.10   TCP   66 49695 → 80 [SYN, ECN, CWR]
08:16:03.945849 202.20.3.10   172.30.0.2    TCP   66 80 → 49694 [SYN, ACK] Seq=0
08:16:03.945851 202.20.3.10   172.30.0.2    TCP   66 80 → 49695 [SYN, ACK] Seq=0
08:16:03.945884 172.30.0.2    202.20.3.10   TCP   54 49694 → 80 [ACK] Seq=1 Ack=
08:16:03.945895 172.30.0.2    202.20.3.10   TCP   54 49695 → 80 [ACK] Seq=1 Ack=
```

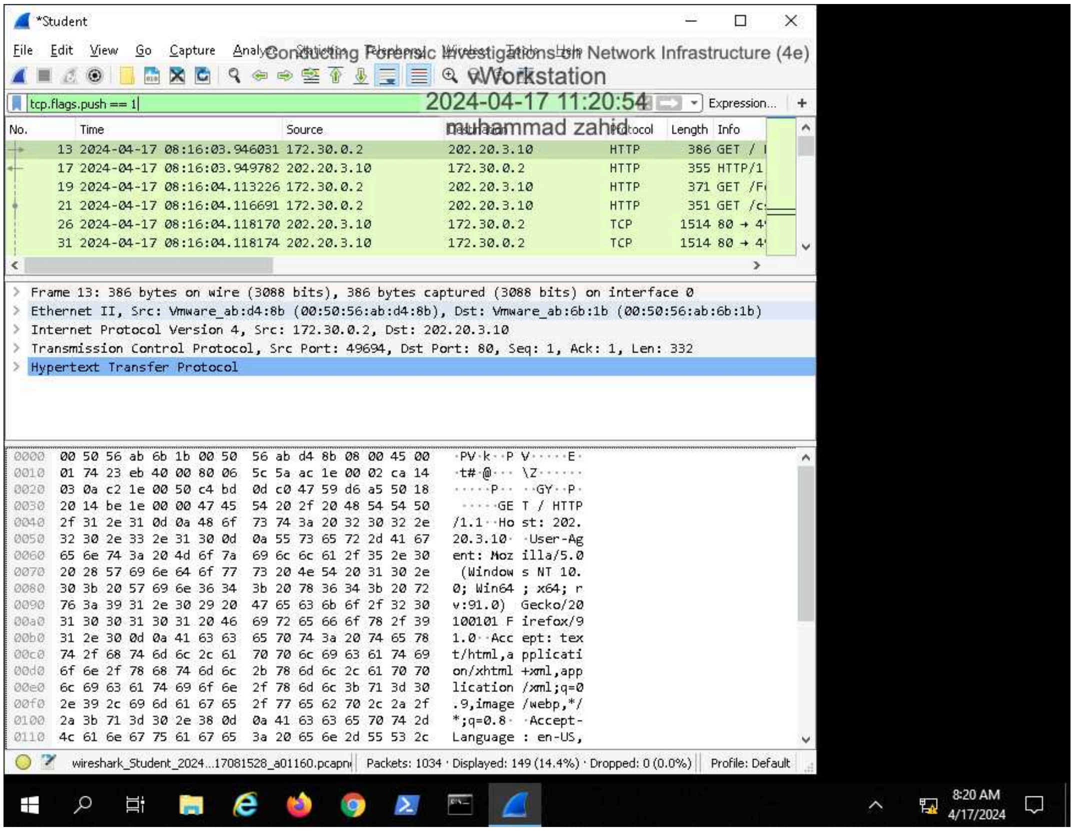
```
> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_ab:d4:8b (00:50:56:ab:d4:8b), Dst: Vmware_ab:6b:1b (00:50:56:ab:6b:1b)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49694, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 50 56 ab 6b 1b 00 50  56 ab d4 8b 08 00 45 02   ·PV·k··P V·····E·
0010  00 34 23 e7 40 00 80 06  5d 9c ac 1e 00 02 ca 14   ·4#·@··· ]·······
0020  03 0a c2 1e 00 50 c4 bd  0d bf 00 00 00 00 80 c2   ·····P·· ········
0030  fa f0 65 35 00 00 02 04  05 b4 01 03 03 08 01 01   ··e5···· ········
0040  04 02                                              ··
```

wireshark_Student_202...7081528_a01160.pcapng | Packets: 1034 · Displayed: 1022 (98.8%) · Dropped: 0 (0.0%) | Profile: Default

8:20 AM
4/17/2024

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



tcp.flags.push == 1

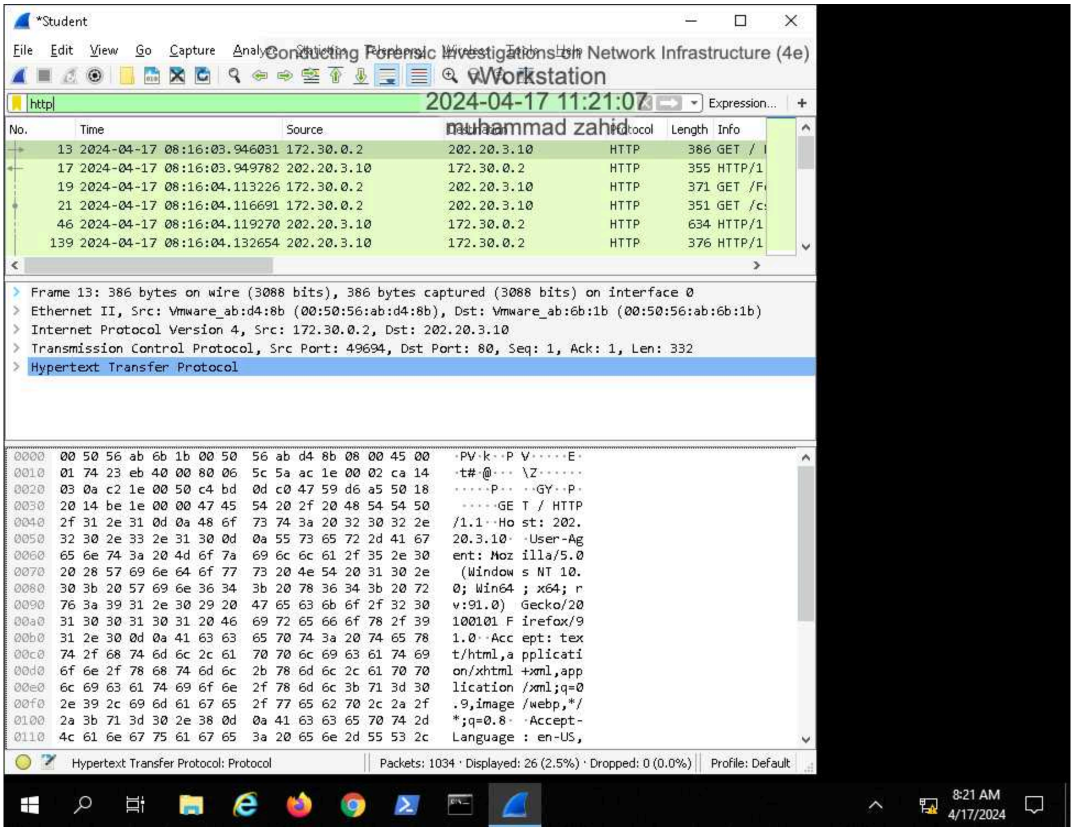
```
No.   Time                        Source        Destination   Protocol  Length  Info
   13 2024-04-17 08:16:03.946031 172.30.0.2    202.20.3.10   HTTP       386 GET / I
   17 2024-04-17 08:16:03.949782 202.20.3.10   172.30.0.2    HTTP       355 HTTP/1
   19 2024-04-17 08:16:04.113226 172.30.0.2    202.20.3.10   HTTP       371 GET /F
   21 2024-04-17 08:16:04.116691 172.30.0.2    202.20.3.10   HTTP       351 GET /c
   26 2024-04-17 08:16:04.118170 202.20.3.10   172.30.0.2    TCP       1514 80 → 4
   31 2024-04-17 08:16:04.118174 202.20.3.10   172.30.0.2    TCP       1514 80 → 4
```

```
> Frame 13: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_ab:d4:8b (00:50:56:ab:d4:8b), Dst: Vmware_ab:6b:1b (00:50:56:ab:6b:1b)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49694, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
> Hypertext Transfer Protocol
```

```
0000  00 50 56 ab 6b 1b 00 50  56 ab d4 8b 08 00 45 00   ·PV·k··P V·····E·
0010  01 74 23 eb 40 00 80 06  5c 5a ac 1e 00 02 ca 14   ·t#·@··· \Z······
0020  03 0a c2 1e 00 50 c4 bd  0d c0 47 59 d6 a5 50 18   ·····P·· ··GY··P·
0030  20 14 be 1e 00 00 47 45  54 20 2f 20 48 54 54 50    ·····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,
```

wireshark_Student_2024...17081528_a01160.pcapng | Packets: 1034 · Displayed: 149 (14.4%) · 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...
8:21 AM
4/17/2024

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:21:07
muhammad zahid

http

```
No.   Time                        Source        Destination   Protocol  Length Info
   13 2024-04-17 08:16:03.946031 172.30.0.2    202.20.3.10   HTTP         386 GET / I
   17 2024-04-17 08:16:03.949782 202.20.3.10   172.30.0.2    HTTP         355 HTTP/1
   19 2024-04-17 08:16:04.113226 172.30.0.2    202.20.3.10   HTTP         371 GET /F
   21 2024-04-17 08:16:04.116691 172.30.0.2    202.20.3.10   HTTP         351 GET /c:
   46 2024-04-17 08:16:04.119270 202.20.3.10   172.30.0.2    HTTP         634 HTTP/1
  139 2024-04-17 08:16:04.132654 202.20.3.10   172.30.0.2    HTTP         376 HTTP/1
```

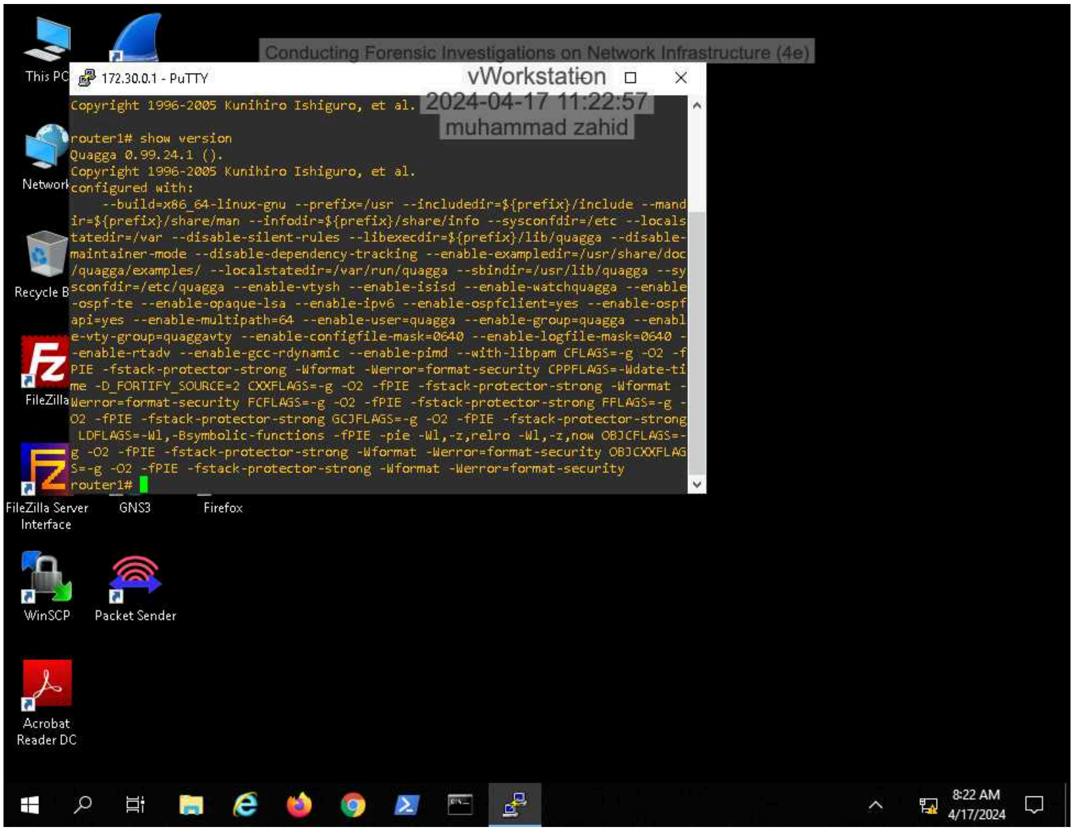
```
> Frame 13: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
> Ethernet II, Src: Vmware_ab:d4:8b (00:50:56:ab:d4:8b), Dst: Vmware_ab:6b:1b (00:50:56:ab:6b:1b)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 202.20.3.10
> Transmission Control Protocol, Src Port: 49694, Dst Port: 80, Seq: 1, Ack: 1, Len: 332
> Hypertext Transfer Protocol
```

```
0000  00 50 56 ab 6b 1b 00 50  56 ab d4 8b 08 00 45 00   ·PV·k··P V·····E·
0010  01 74 23 eb 40 00 80 06  5c 5a ac 1e 00 02 ca 14   ·t#·@··· \Z······
0020  03 0a c2 1e 00 50 c4 bd  0d c0 47 59 d6 a5 50 18   ·····P·· ··GY··P·
0030  20 14 be 1e 00 00 47 45  54 20 2f 20 48 54 54 50    ·····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,
```

Hypertext Transfer Protocol: Protocol | Packets: 1034 · Displayed: 26 (2.5%) · Dropped: 0 (0.0%) | Profile: Default

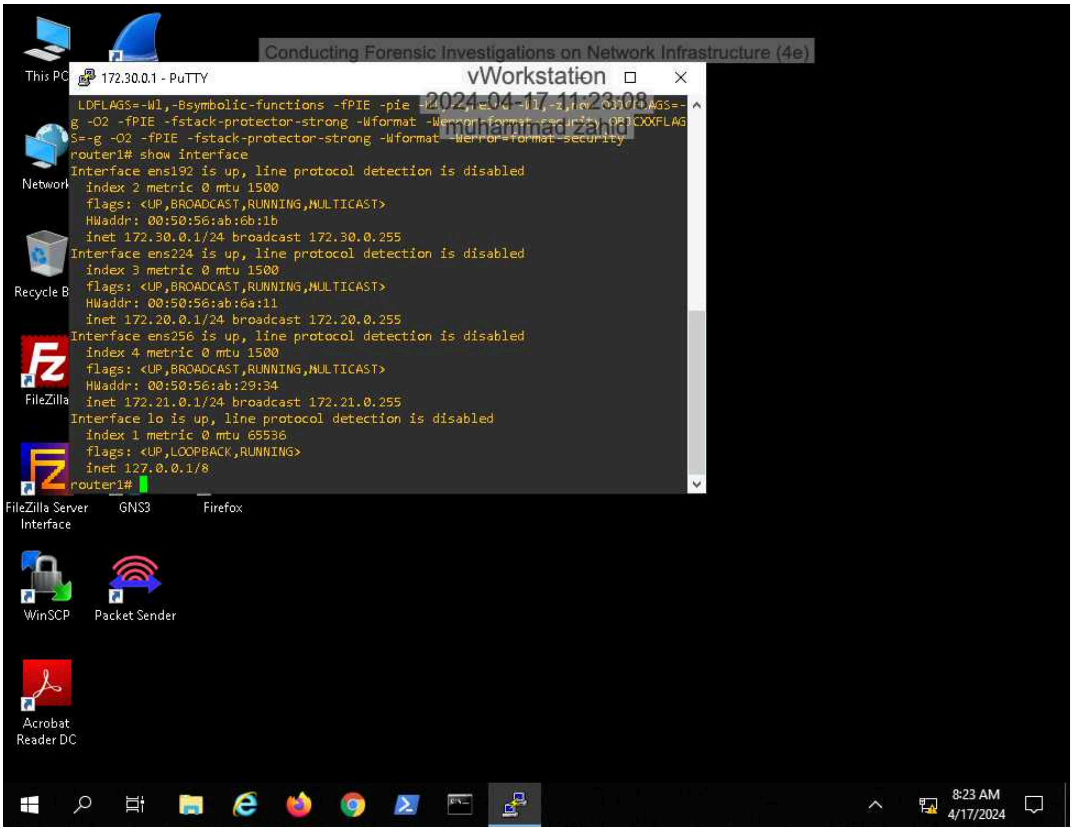
Part 2: Analyze a Router for Forensic Evidence

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



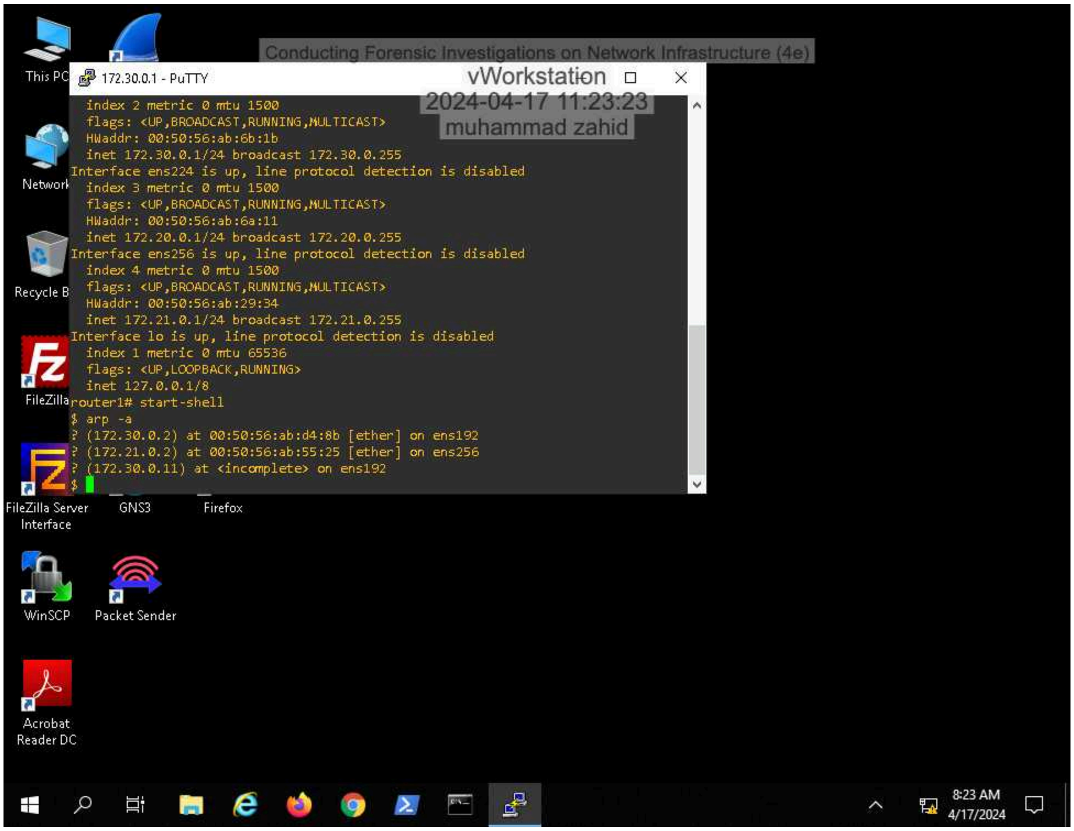
```
Copyright 1996-2005 Kunihiro Ishiguro, et al.

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**.



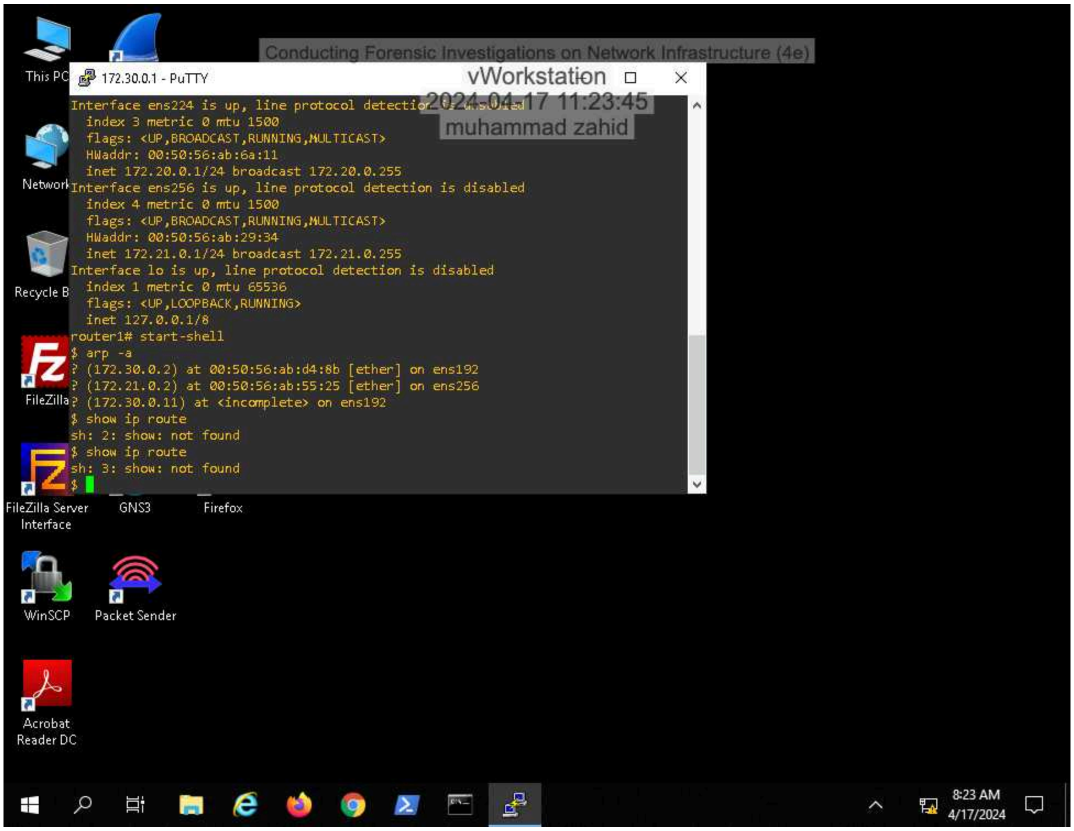
```
 LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie [illegible]AGS=-
g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security OBJCXXFLAG
S=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1# show interface
Interface ens192 is up, line protocol detection is disabled
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:ab:6b:1b
  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:ab:6a:11
  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:ab:29:34
  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**.



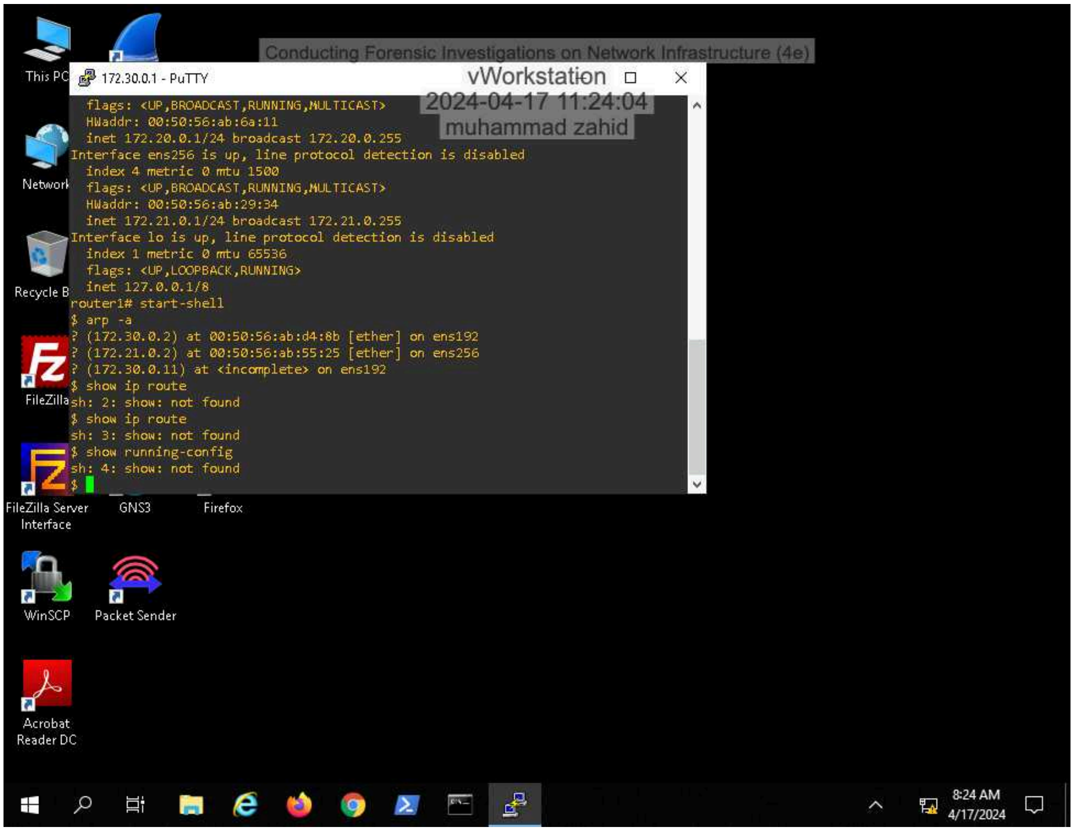
```
  index 2 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:ab:6b:1b
  inet 172.30.0.1/24 broadcast 172.30.0.255
Interface ens224 is up, line protocol detection is disabled
  index 3 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:ab:6a:11
  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:ab:29:34
  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:ab:d4:8b [ether] on ens192
? (172.21.0.2) at 00:50:56:ab:55:25 [ether] on ens256
? (172.30.0.11) at <incomplete> on ens192
$
```

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:ab:6a:11
  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:ab:29:34
  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:ab:d4:8b [ether] on ens192
? (172.21.0.2) at 00:50:56:ab:55:25 [ether] on ens256
? (172.30.0.11) at <incomplete> on ens192
$ show ip route
sh: 2: show: not found
$ show ip route
sh: 3: show: not found
$
```

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

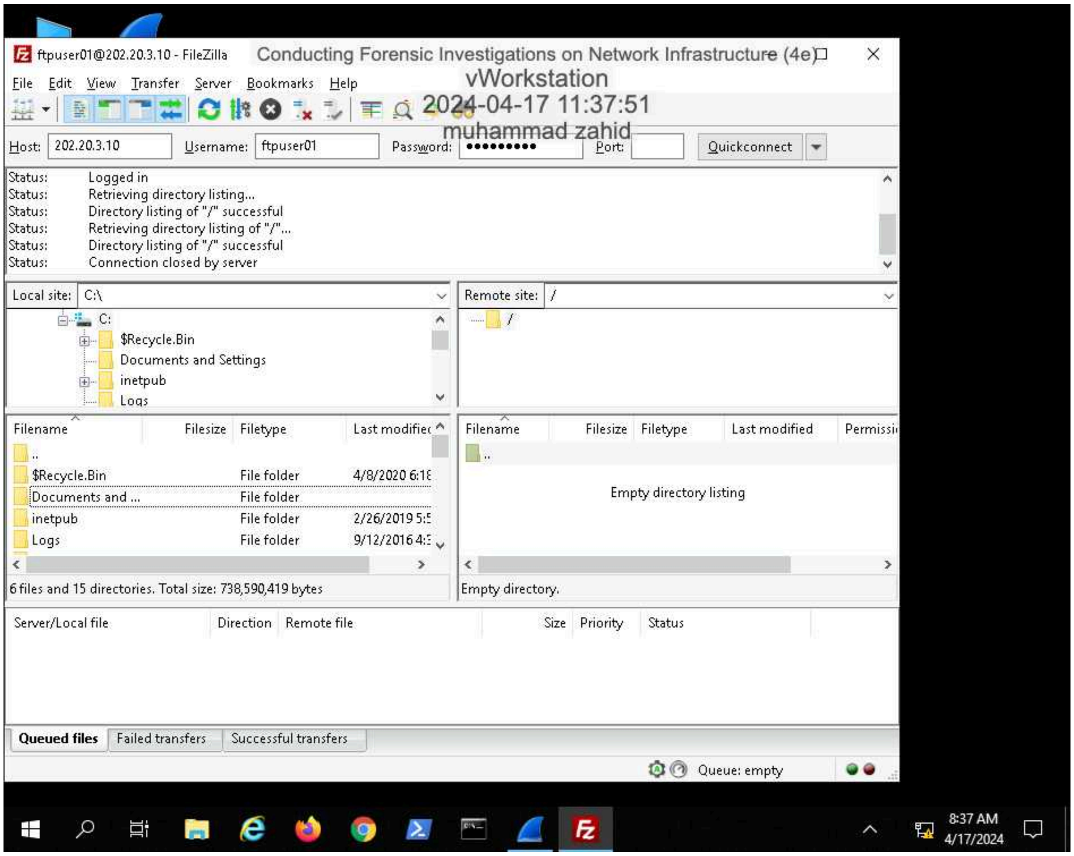


```
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:ab:6a:11
  inet 172.20.0.1/24 broadcast 172.20.0.255
Interface ens256 is up, line protocol detection is disabled
  index 4 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:ab:29:34
  inet 172.21.0.1/24 broadcast 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:ab:d4:8b [ether] on ens192
? (172.21.0.2) at 00:50:56:ab:55:25 [ether] on ens256
? (172.30.0.11) at <incomplete> on ens192
$ show ip route
sh: 2: show: not found
$ show ip route
sh: 3: show: not found
$ show running-config
sh: 4: show: not found
$
```

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: ••••••••• Port:

```
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
Status:     Connection closed by server
```

Local site: C:\

Remote site: /

Filename	Filesize	Filetype	Last modified
..			
$Recycle.Bin		File folder	4/8/2020 6:18
Documents and ...		File folder	
inetpub		File folder	2/26/2019 5:5
Logs		File folder	9/12/2016 4:3

6 files and 15 directories. Total size: 738,590,419 bytes

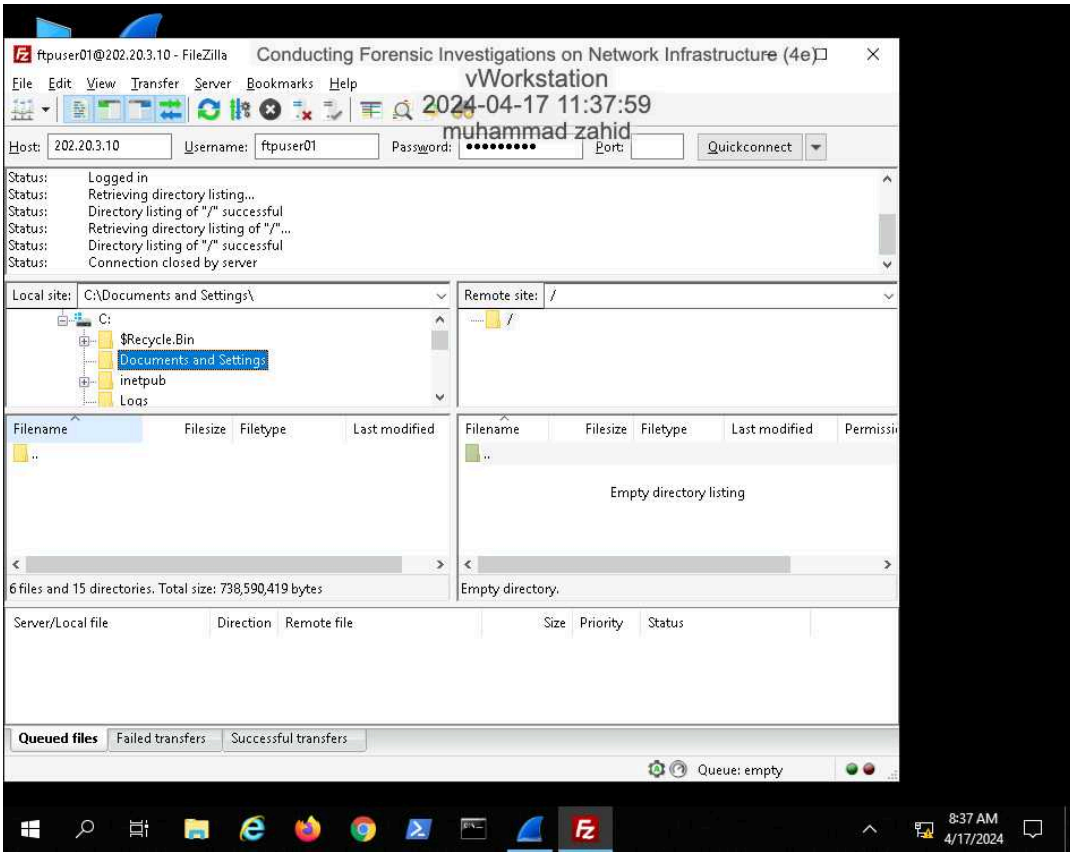
Filename	Filesize	Filetype	Last modified	Permissi
..				

Empty directory listing

Empty directory.

Server/Local file	Direction	Remote file	Size	Priority	Status

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



ftpuser01@202.20.3.10 - FileZilla

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:37:59
muhammad zahid

Host: 202.20.3.10 Username: ftpuser01 Password: ••••••••• Port:

```
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
Status:     Connection closed by server
```

Local site: C:\Documents and Settings\

Remote site: /

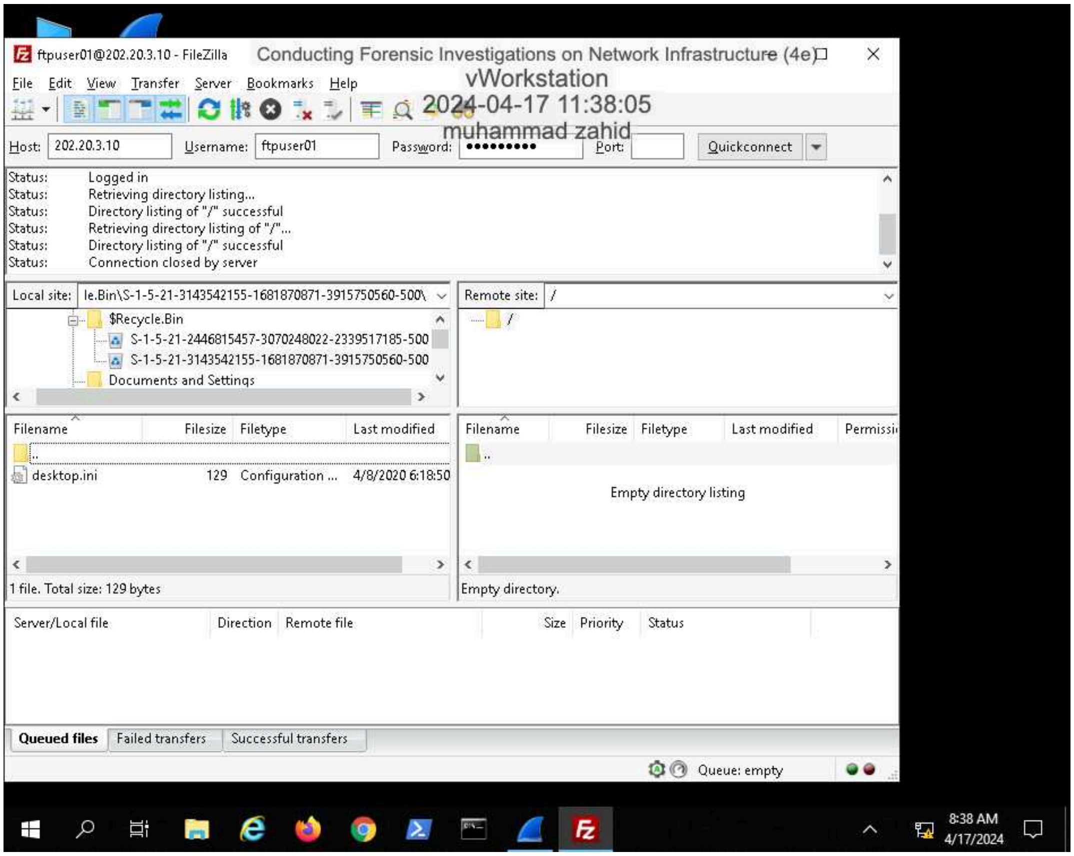
Empty directory listing

6 files and 15 directories. Total size: 738,590,419 bytes

Empty directory.

Queue: empty

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



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:38:05
muhammad zahid

Host: 202.20.3.10 Username: ftpuser01 Password: ••••••••• Port:

```
Status:     Logged in
Status:     Retrieving directory listing...
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
Status:     Connection closed by server
```

Local site: le.Bin\S-1-5-21-3143542155-1681870871-3915750560-500\

```
$Recycle.Bin
    S-1-5-21-2446815457-3070248022-2339517185-500
    S-1-5-21-3143542155-1681870871-3915750560-500
Documents and Settings
```

Remote site: /

```
/
```

Filename	Filesize	Filetype	Last modified
..			
desktop.ini	129	Configuration ...	4/8/2020 6:18:50

1 file. Total size: 129 bytes

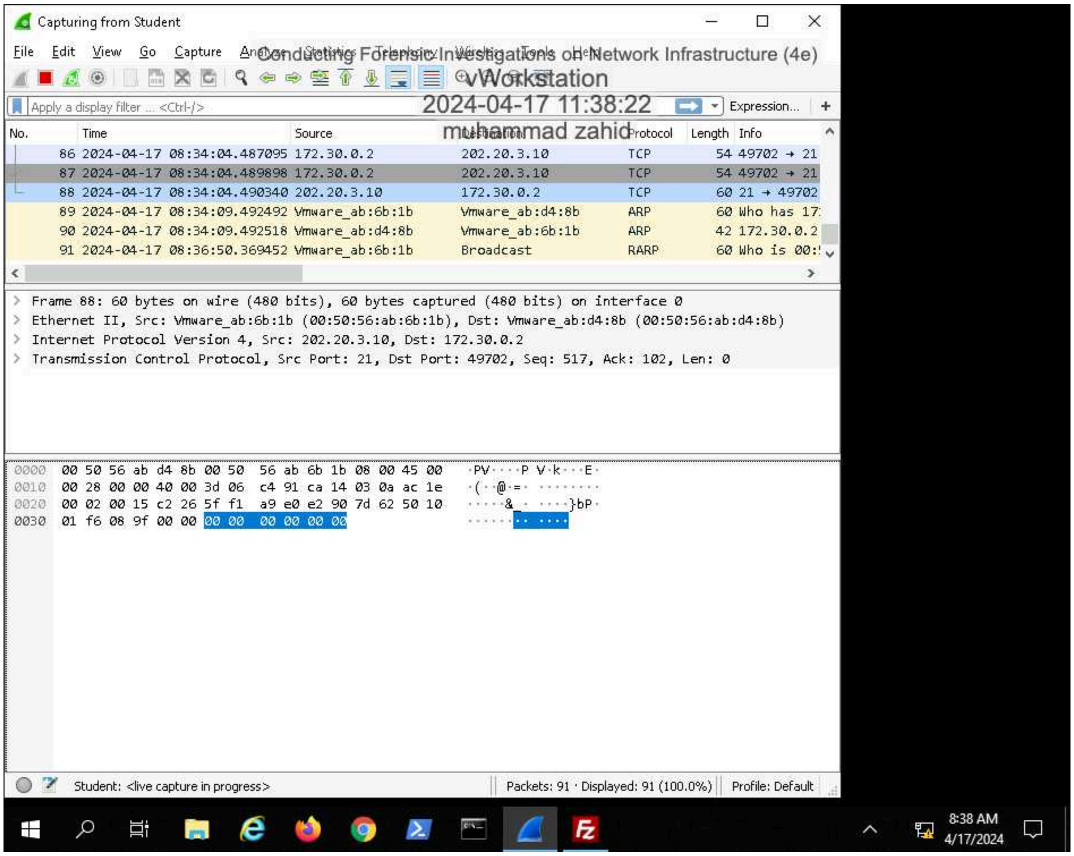
Filename	Filesize	Filetype	Last modified	Permissi
..				

Empty directory listing

Empty directory.

Server/Local file	Direction	Remote file	Size	Priority	Status

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



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:38:22
muhammad zahid

```
No.   Time                          Source             Destination        Protocol  Length Info
   86 2024-04-17 08:34:04.487095 172.30.0.2         202.20.3.10        TCP         54 49702 → 21
   87 2024-04-17 08:34:04.489898 172.30.0.2         202.20.3.10        TCP         54 49702 → 21
   88 2024-04-17 08:34:04.490340 202.20.3.10        172.30.0.2         TCP         60 21 → 49702
   89 2024-04-17 08:34:09.492492 Vmware_ab:6b:1b    Vmware_ab:d4:8b    ARP         60 Who has 17:
   90 2024-04-17 08:34:09.492518 Vmware_ab:d4:8b    Vmware_ab:6b:1b    ARP         42 172.30.0.2
   91 2024-04-17 08:36:50.369452 Vmware_ab:6b:1b    Broadcast          RARP        60 Who is 00:!
```

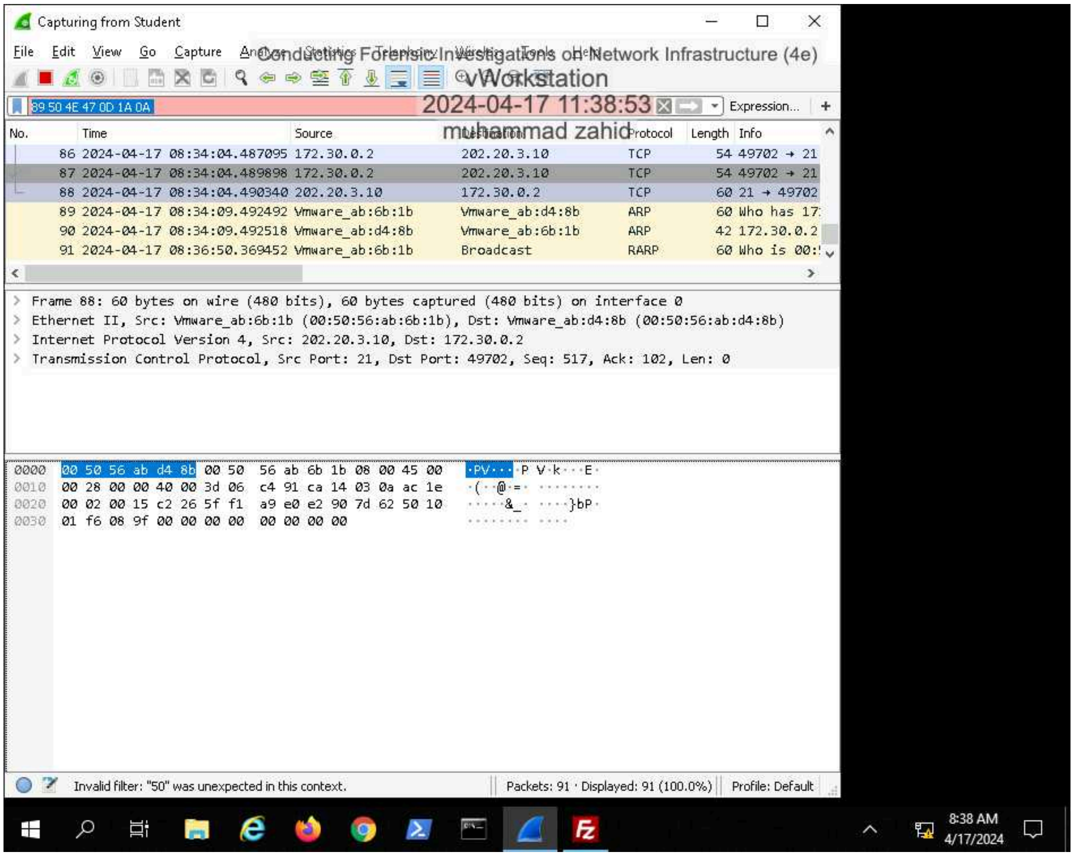
```
> Frame 88: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_ab:6b:1b (00:50:56:ab:6b:1b), Dst: Vmware_ab:d4:8b (00:50:56:ab:d4:8b)
> Internet Protocol Version 4, Src: 202.20.3.10, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49702, Seq: 517, Ack: 102, Len: 0
```

```
0000  00 50 56 ab d4 8b 00 50  56 ab 6b 1b 08 00 45 00   ·PV····P V·k···E·
0010  00 28 00 00 40 00 3d 06  c4 91 ca 14 03 0a ac 1e   ·(··@·=· ········
0020  00 02 00 15 c2 26 5f f1  a9 e0 e2 90 7d 62 50 10   ·····&_· ····}bP·
0030  01 f6 08 9f 00 00 00 00  00 00 00 00               ········ ····
```

Student: <live capture in progress> | Packets: 91 · Displayed: 91 (100.0%) | Profile: Default

8:38 AM
4/17/2024

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



Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:38:53
muhammad zahid

89 50 4E 47 0D 1A 0A

```
No.  Time                        Source             Destination        Protocol  Length  Info
  86 2024-04-17 08:34:04.487095 172.30.0.2         202.20.3.10        TCP       54 49702 → 21
  87 2024-04-17 08:34:04.489898 172.30.0.2         202.20.3.10        TCP       54 49702 → 21
  88 2024-04-17 08:34:04.490340 202.20.3.10        172.30.0.2         TCP       60 21 → 49702
  89 2024-04-17 08:34:09.492492 Vmware_ab:6b:1b    Vmware_ab:d4:8b    ARP       60 Who has 17:
  90 2024-04-17 08:34:09.492518 Vmware_ab:d4:8b    Vmware_ab:6b:1b    ARP       42 172.30.0.2
  91 2024-04-17 08:36:50.369452 Vmware_ab:6b:1b    Broadcast          RARP      60 Who is 00:!
```

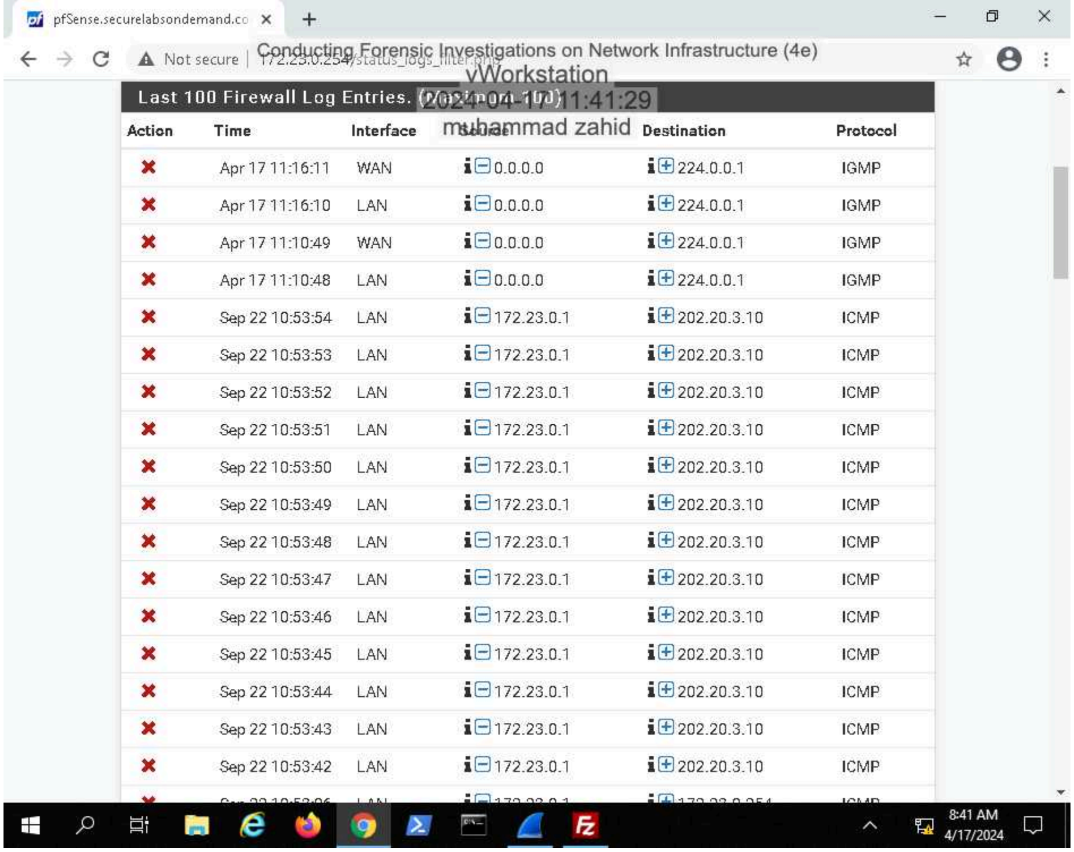
```
> Frame 88: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_ab:6b:1b (00:50:56:ab:6b:1b), Dst: Vmware_ab:d4:8b (00:50:56:ab:d4:8b)
> Internet Protocol Version 4, Src: 202.20.3.10, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49702, Seq: 517, Ack: 102, Len: 0
```

```
0000  00 50 56 ab d4 8b 00 50  56 ab 6b 1b 08 00 45 00   ·PV··· P V·k···E·
0010  00 28 00 00 40 00 3d 06  c4 91 ca 14 03 0a ac 1e   ·(··@·=· ········
0020  00 02 00 15 c2 26 5f f1  a9 e0 e2 90 7d 62 50 10   ·····&_· ····}bP·
0030  01 f6 08 9f 00 00 00 00  00 00 00 00               ········ ····
```

Invalid filter: "50" was unexpected in this context. | Packets: 91 · Displayed: 91 (100.0%) | Profile: Default

Part 2: Analyze a Firewall for Forensic Evidence

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

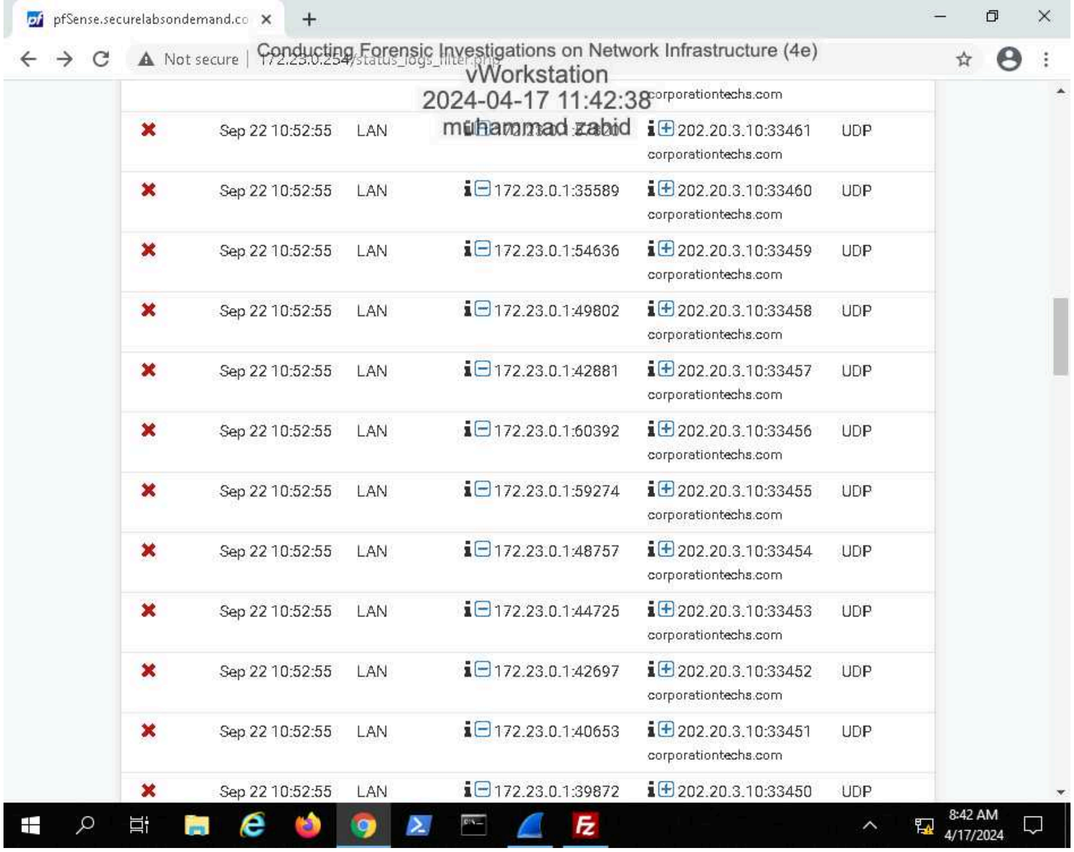

pfSense.securelabsondemand.co
Not secure | 172.23.0.254/status_logs_filter.php
8:41 AM
4/17/2024

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:41:29
muhammad zahid

Last 100 Firewall Log Entries. (Maximum 100)

Action	Time	Interface	Source	Destination	Protocol
✖	Apr 17 11:16:11	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 17 11:16:10	LAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 17 11:10:49	WAN	0.0.0.0	224.0.0.1	IGMP
✖	Apr 17 11:10:48	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
✖	Sep 22 10:53:44	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:43	LAN	172.23.0.1	202.20.3.10	ICMP
✖	Sep 22 10:53:42	LAN	172.23.0.1	202.20.3.10	ICMP

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

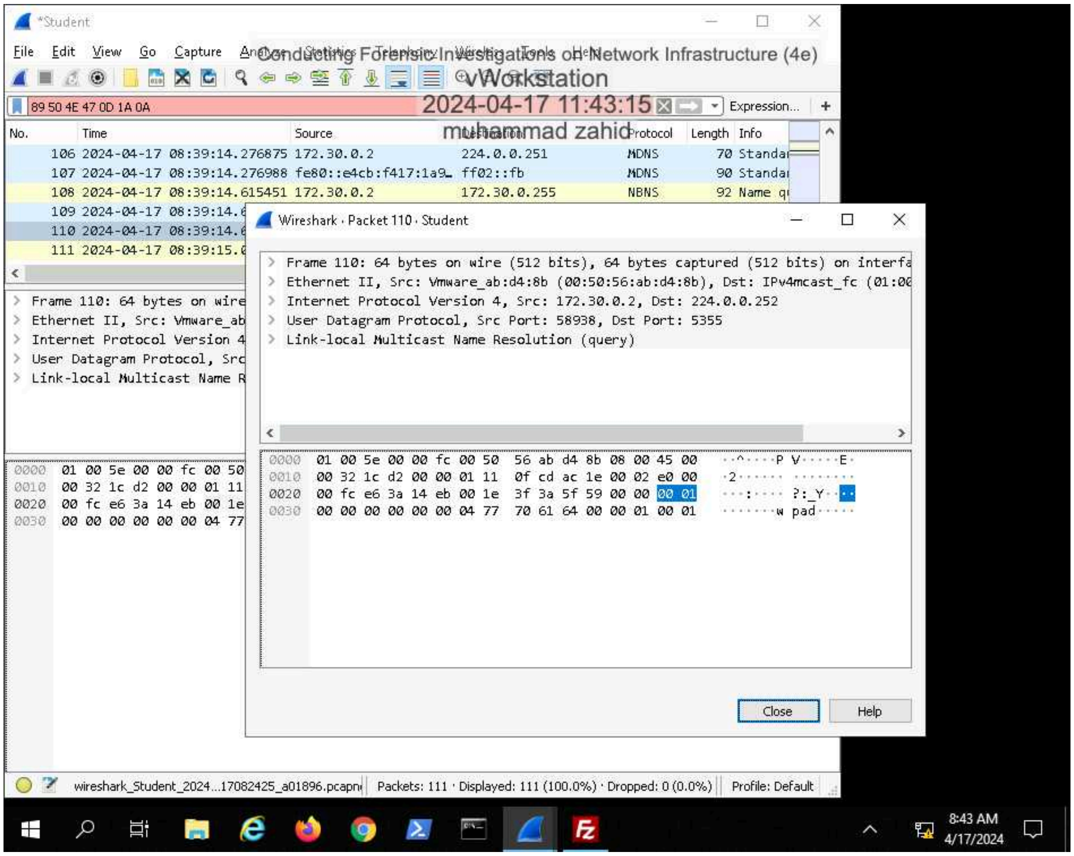

pfSense.securelabsondemand.co
Not secure
172.23.0.254/status_logs_filter.php
Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:42:38
muhammad zahid
8:42 AM
4/17/2024

				corporationtechs.com	
✖	Sep 22 10:52:55	LAN	[illegible]	202.20.3.10:33461 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:35589	202.20.3.10:33460 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:54636	202.20.3.10:33459 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:49802	202.20.3.10:33458 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:42881	202.20.3.10:33457 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:60392	202.20.3.10:33456 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:59274	202.20.3.10:33455 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:48757	202.20.3.10:33454 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:44725	202.20.3.10:33453 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:42697	202.20.3.10:33452 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:40653	202.20.3.10:33451 corporationtechs.com	UDP
✖	Sep 22 10:52:55	LAN	172.23.0.1:39872	202.20.3.10:33450	UDP

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**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Wireshark · Packet 110 · Student
Close
Help
8:43 AM
4/17/2024

Conducting Forensic Investigations on Network Infrastructure (4e)
vWorkstation
2024-04-17 11:43:15
muhammad zahid

89 50 4E 47 0D 1A 0A

```
No.  Time                       Source                   Destination    Protocol  Length  Info
106  2024-04-17 08:39:14.276875 172.30.0.2               224.0.0.251    MDNS      70      Standar
107  2024-04-17 08:39:14.276988 fe80::e4cb:f417:1a9…     ff02::fb       MDNS      90      Standar
108  2024-04-17 08:39:14.615451 172.30.0.2               172.30.0.255   NBNS      92      Name qu
109  2024-04-17 08:39:14.6
110  2024-04-17 08:39:14.6
111  2024-04-17 08:39:15.0
```

```
> Frame 110: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interfa
> Ethernet II, Src: Vmware_ab:d4:8b (00:50:56:ab:d4:8b), Dst: IPv4mcast_fc (01:00
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 224.0.0.252
> User Datagram Protocol, Src Port: 58938, Dst Port: 5355
> Link-local Multicast Name Resolution (query)
```

```
0000  01 00 5e 00 00 fc 00 50  56 ab d4 8b 08 00 45 00   ··^····P V·····E·
0010  00 32 1c d2 00 00 01 11  0f cd ac 1e 00 02 e0 00   ·2······ ········
0020  00 fc e6 3a 14 eb 00 1e  3f 3a 5f 59 00 00 00 01   ···:···· ?:_Y····
0030  00 00 00 00 00 00 04 77  70 61 64 00 00 01 00 01   ·······w pad·····
```

wireshark_Student_2024...17082425_a01896.pcapng | Packets: 111 · Displayed: 111 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Part 2: Identify Suspicious Outgoing Connections

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

192.168.0.2 Port 22