

Student:  
Jordan Calvert

Email:  
jordanryancalvert@gmail.com

Time on Task:  
6 hours, 5 minutes

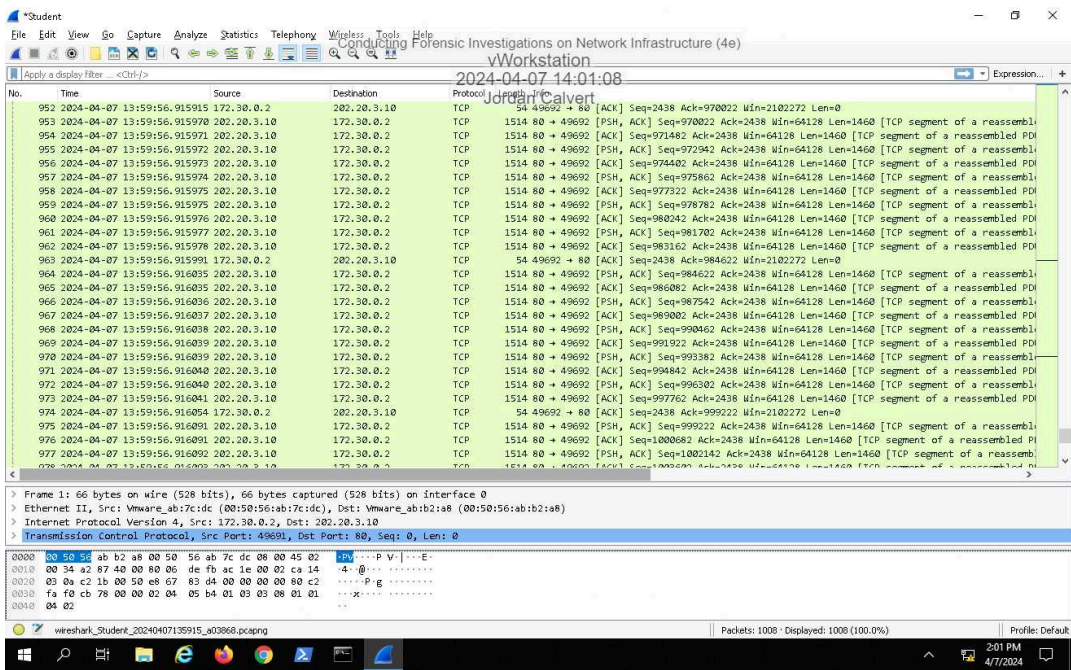
Progress:  
100%

Report Generated: Wednesday, May 15, 2024 at 10:49 AM

Section 1: Hands-On Demonstration

Part 1: Perform Packet Capture and Analysis

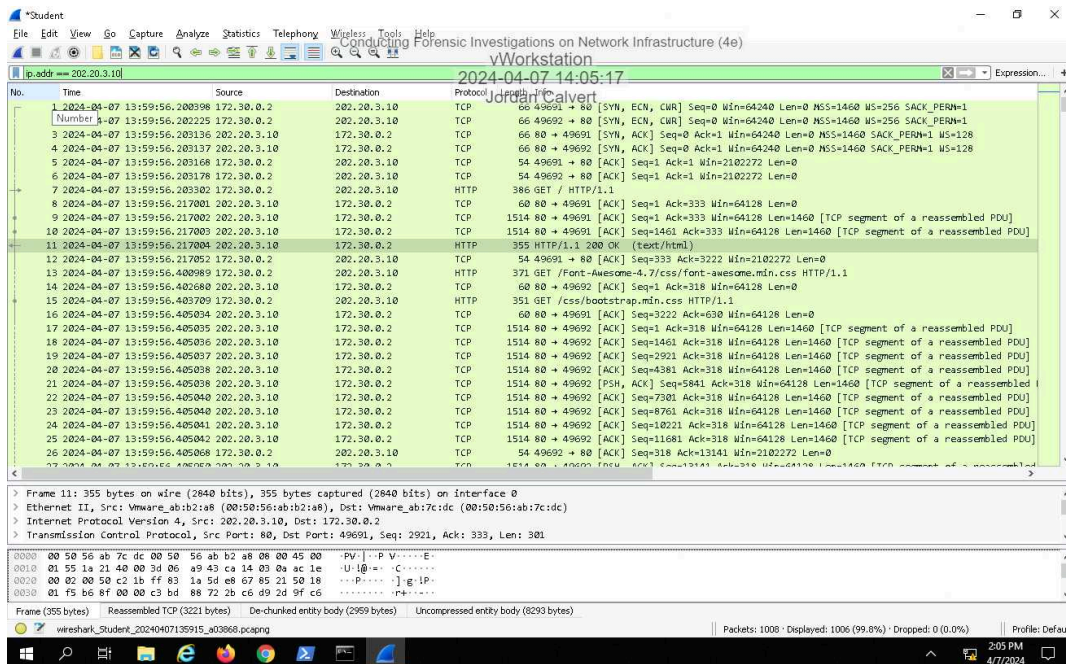
11. Make a screen capture showing the timestamp-sorted traffic.



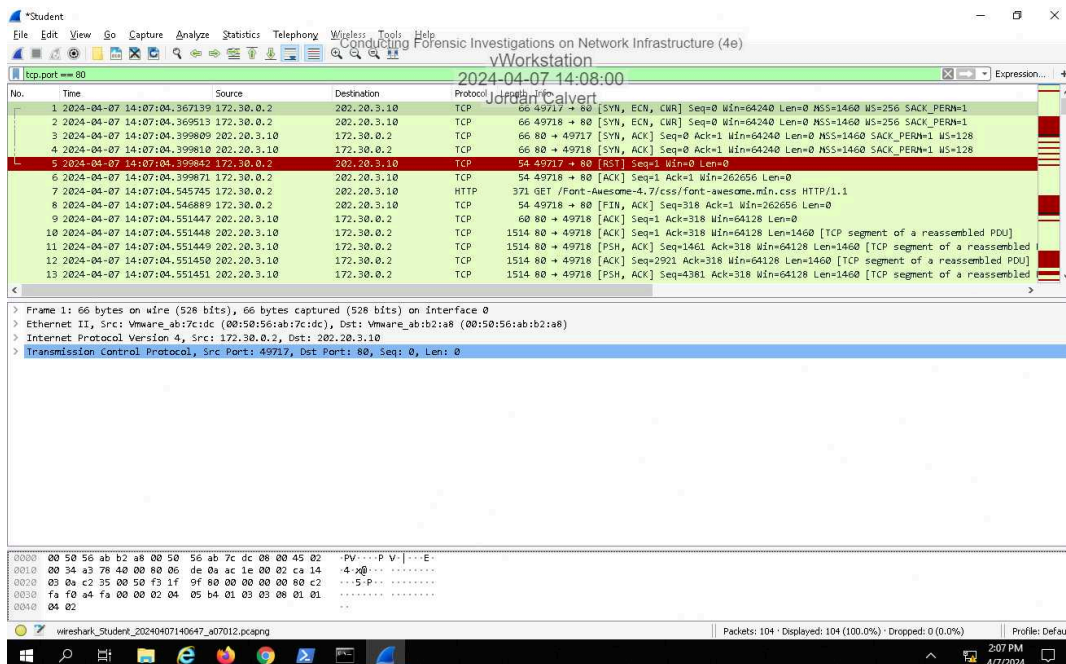
# Conducting Forensic Investigations on Network Infrastructure (4e)

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

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



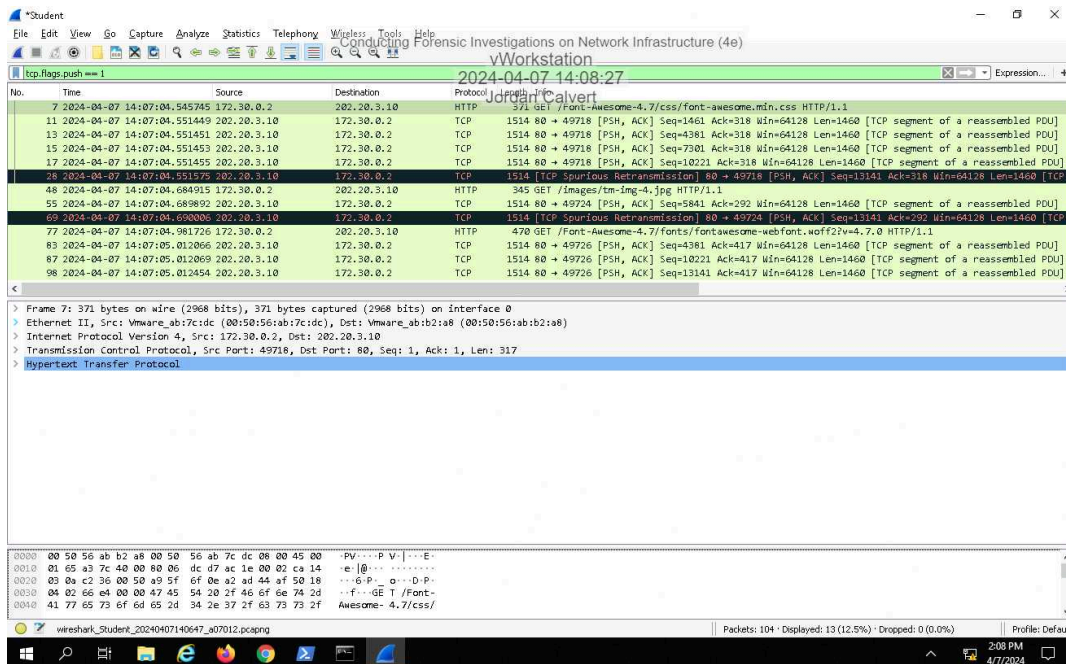
### 15. Make a screen capture showing the port-filtered traffic.



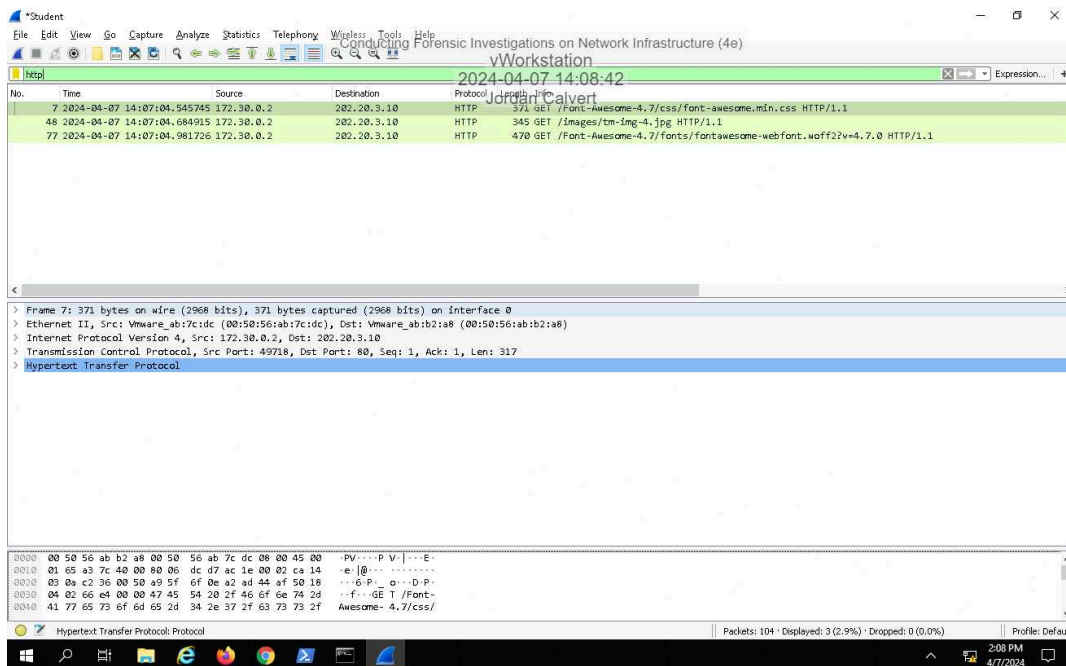
# Conducting Forensic Investigations on Network Infrastructure (4e)

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

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



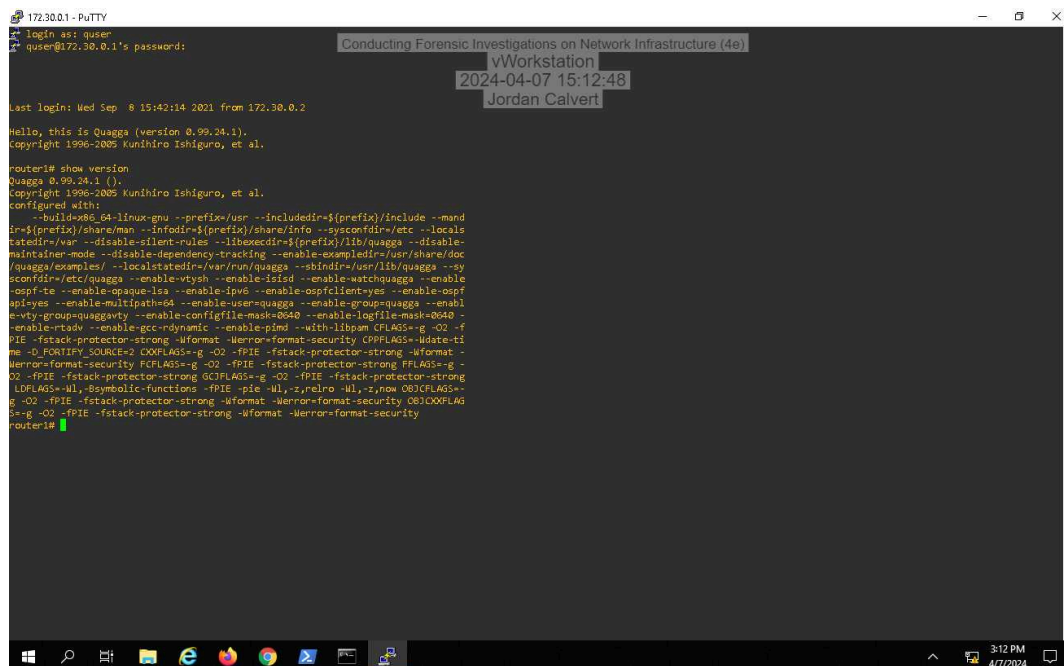
### 19. Make a screen capture showing the http-filtered traffic.



## Part 2: Analyze a Router for Forensic Evidence



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



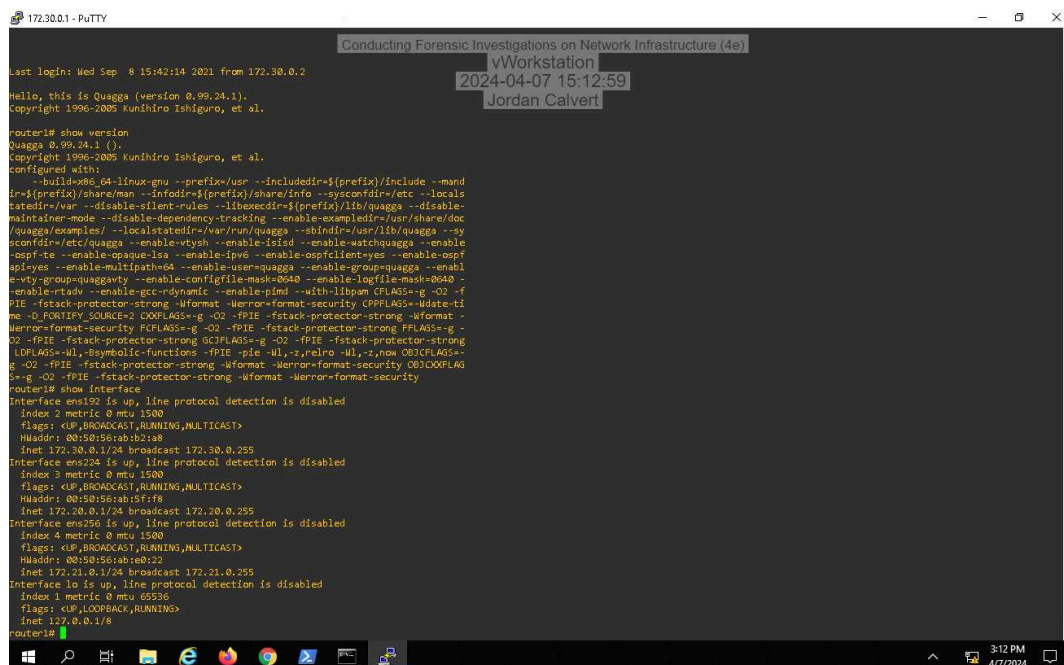
```
172.30.0.1 - PuTTY
login api quagga
quagga@172.30.0.1's password:

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 Kunihiko Ishiguro, et al.

router1# show version
Quagga 0.99.24.1 ().
Copyright 1996-2005 Kunihiko Ishiguro, et al.
configured with:
  --build=x86_64-linux-gnu --prefix=/usr --includedir=$(prefix)/include --mandir=$(prefix)/share/man --infodir=$(prefix)/share/info --sysconfdir=/etc --localstatedir=/var --disable-silent-rules --libexecdir=$(prefix)/lib/quagga --disable-maintainer-mode --disable-dependency-tracking --enable-exempdir=/usr/share/doc/quagga/examples/ --localstatedir=/var/run/quagga --sbindir=/usr/lib/quagga --sysconfdir=/etc/quagga --enable-vtysh --enable-isisd --enable-watchquagga --enable-ospf-te --enable-ospf-lsa --enable-ipv6 --enable-ospfclient=yes --enable-ospfapi=yes --enable-multipath=64 --enable-user=quagga --enable-group=quagga --enable-vty-group=quaggavty --enable-configfile-mask=0040 --enable-logfile-mask=0040 --enable-rtadv --enable-gcc-dynamic --enable-pimd --with-libpam CFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security CPPFLAGS=-D_FORTIFY_SOURCE=2 COXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security FCFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security GCOFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now O0CFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security O0COXFLAG=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security
router1#
```

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



```
172.30.0.1 - PuTTY
login api quagga
quagga@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 Kunihiko Ishiguro, et al.

router1# show version
Quagga 0.99.24.1 ().
Copyright 1996-2005 Kunihiko Ishiguro, et al.
configured with:
  --build=x86_64-linux-gnu --prefix=/usr --includedir=$(prefix)/include --mandir=$(prefix)/share/man --infodir=$(prefix)/share/info --sysconfdir=/etc --localstatedir=/var --disable-silent-rules --libexecdir=$(prefix)/lib/quagga --disable-maintainer-mode --disable-dependency-tracking --enable-exempdir=/usr/share/doc/quagga/examples/ --localstatedir=/var/run/quagga --sbindir=/usr/lib/quagga --sysconfdir=/etc/quagga --enable-vtysh --enable-isisd --enable-watchquagga --enable-ospf-te --enable-ospf-lsa --enable-ipv6 --enable-ospfclient=yes --enable-ospfapi=yes --enable-multipath=64 --enable-user=quagga --enable-group=quagga --enable-vty-group=quaggavty --enable-configfile-mask=0040 --enable-logfile-mask=0040 --enable-rtadv --enable-gcc-dynamic --enable-pimd --with-libpam CFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security CPPFLAGS=-D_FORTIFY_SOURCE=2 COXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security FCFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security GCOFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now O0CFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security O0COXFLAG=-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>
  Hardware address 00:50:56:ab:02:18
  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>
  Hardware address 00:50:56:ab:0f:18
  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>
  Hardware address 00:50:56:ab:e0:22
  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#
```

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

The screenshot shows a Windows desktop with a taskbar at the bottom containing icons for File Explorer, Edge, Firefox, Chrome, and other applications. The system clock in the bottom right corner displays '3:47 PM 4/2/2024'.

In the background, a terminal window displays the output of the 'show version' command on a Quagga router. The output includes the login time 'Wed Sep 8 15:42:14 2021', the version '0.99.24.1', and the copyright notice 'Copyright 1996-2005 Kunihiro Ishiguro, et al.'. It also shows the router's configuration, including the hostname 'sharaman', the user 'maintainer', and various interface configurations for 'en0' and 'en1'.

In the foreground, an 'Administrator Command Prompt' window is open. It shows the command 'arp -a' being entered, which results in a table of network addresses. The table has four columns: 'Interface', 'Internet Address', 'Physical Address', and 'Type'. The data rows show addresses for interfaces 172.30.0.2 and 192.168.52.2.

Interface	Internet Address	Physical Address	Type
172.30.0.2	172.30.0.1	00-50-56-ab-b2-ab	dynamic
172.30.0.2	172.30.0.255	ff-ff-ff-ff-ff-ff	static
172.30.0.2	224.0.0.22	01-00-5e-00-00-16	static
172.30.0.2	224.0.0.251	01-00-5e-00-00-fb	static
172.30.0.2	224.0.0.252	01-00-5e-00-00-fc	static
192.168.52.2	192.168.52.254	00-50-56-ab-b2-ab	dynamic
192.168.52.2	192.168.255.254	00-50-56-ab-b2-ab	dynamic
192.168.52.2	224.0.0.22	01-00-5e-00-00-16	static
192.168.52.2	224.0.0.251	01-00-5e-00-00-fb	static
192.168.52.2	224.0.0.252	01-00-5e-00-00-fc	static
192.168.52.2	255.255.255.255	ff-ff-ff-ff-ff-ff	static

[illegible]

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

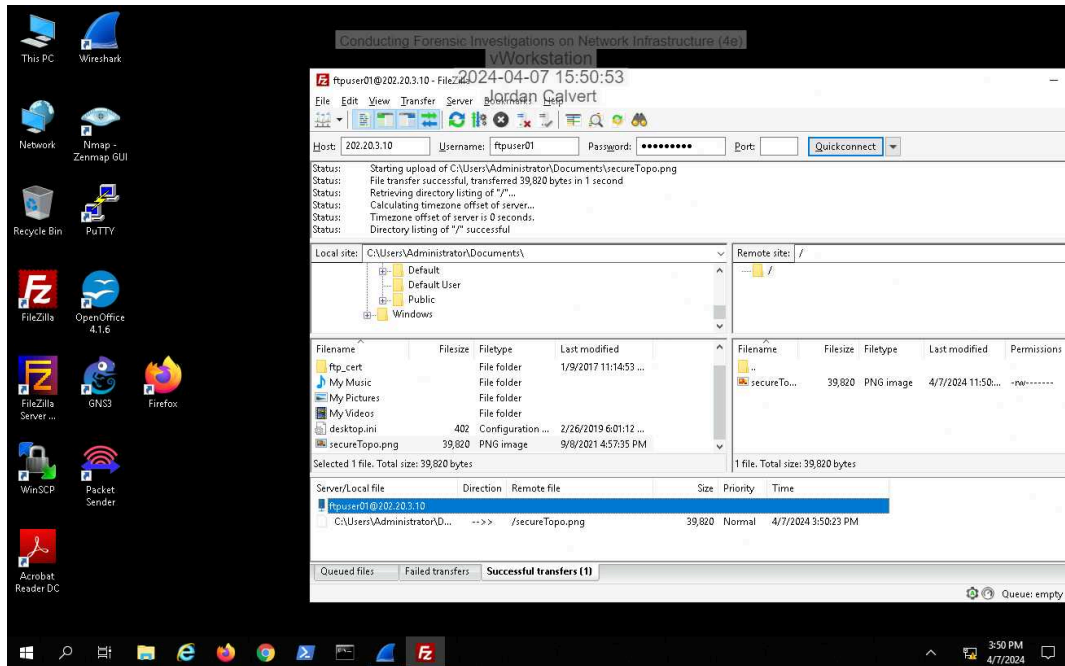
```
172.30.0.1 - PuTTY
C>* 172.20.0.0/24 is directly connected, ens224
C>* 172.21.0.0/24 is directly connected, ens256
C>* 172.22.0.0/24 [120/2] via 172.20.0.2, ens224, 01:53:36
C>* 172.23.0.0/24 [120/2] via 172.21.0.2, ens256, 01:53:38
C>* 172.30.0.0/24 is directly connected, ens192
C>* 202.20.3.10/32 [120/2] via 172.21.0.2, ens256, 01:53:33
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@ssw0rd1
 ipv6 nd suppress-ra
 no link-detect
!
interface ens224
 ip rip authentication mode text
 ip rip authentication string P@ssw0rd1
 ipv6 nd suppress-ra
 no link-detect
!
interface ens256
 ip rip authentication mode text
 ip rip authentication string P@ssw0rd1
 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#
```

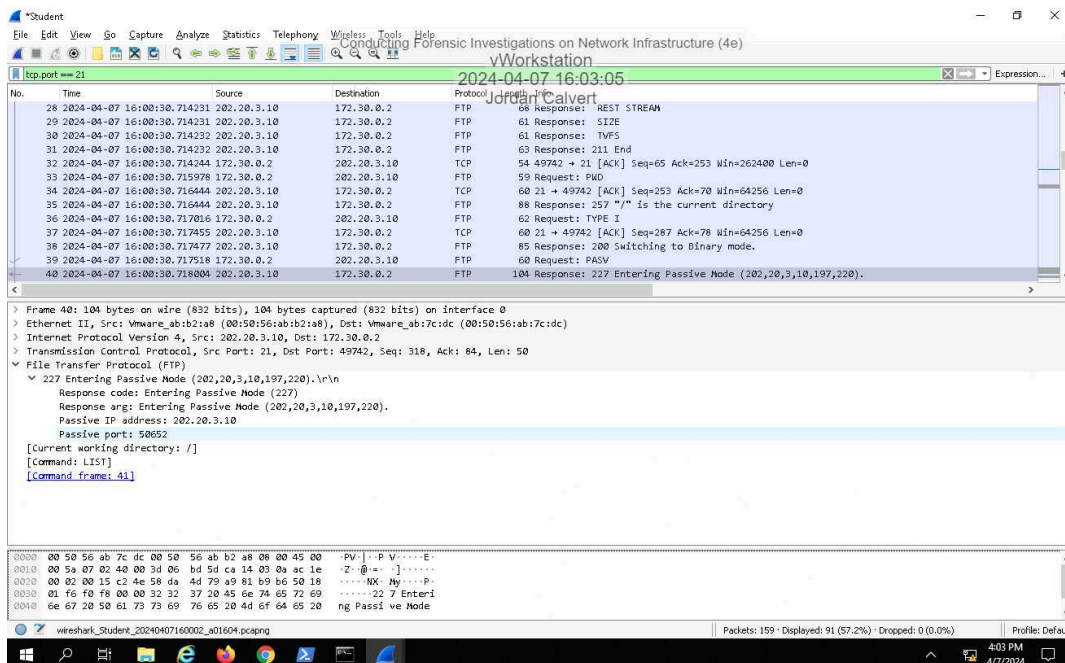
### Section 2: Applied Learning

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

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

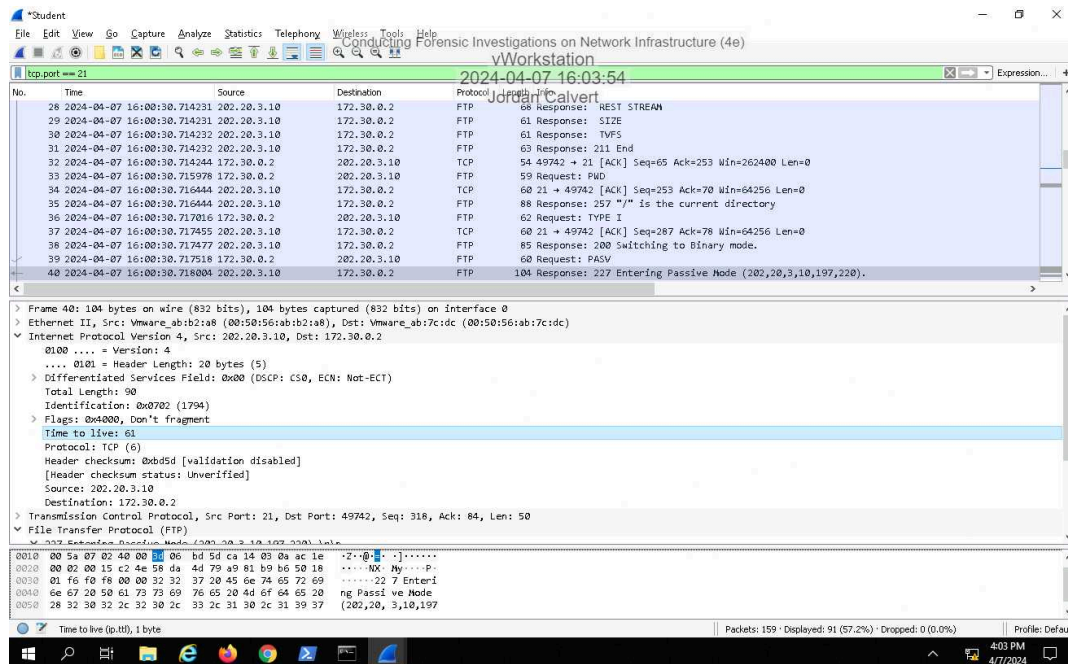


15. Make a screen capture showing the **passive port specified by the FTP server in the Packet Details pane**.

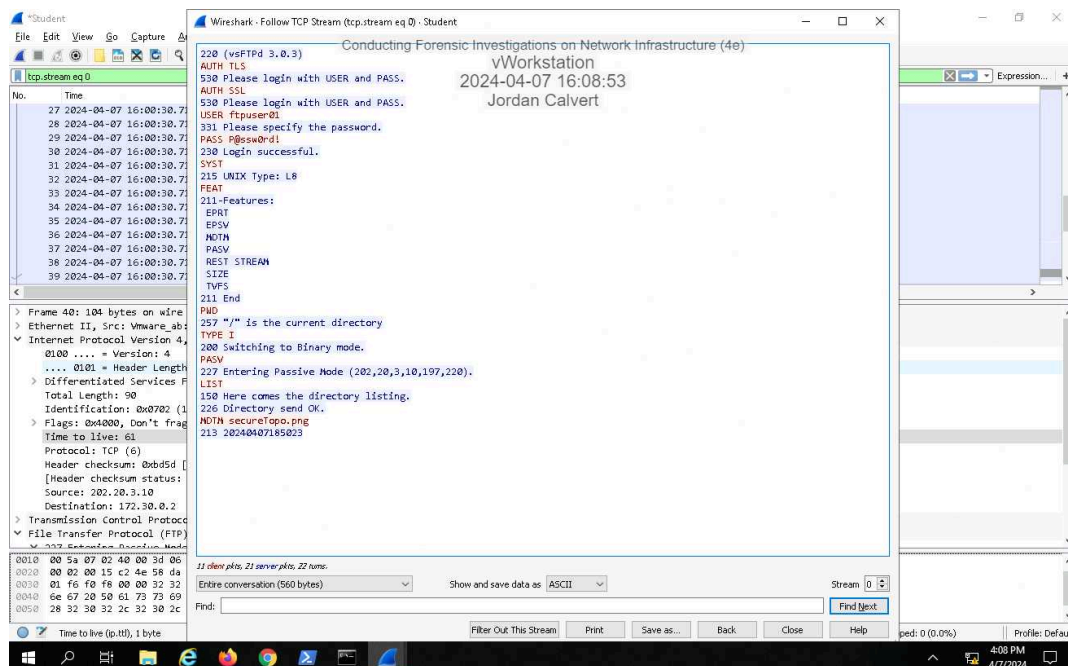




### 18. Make a screen capture showing the Time to live field in the Packet Details pane.

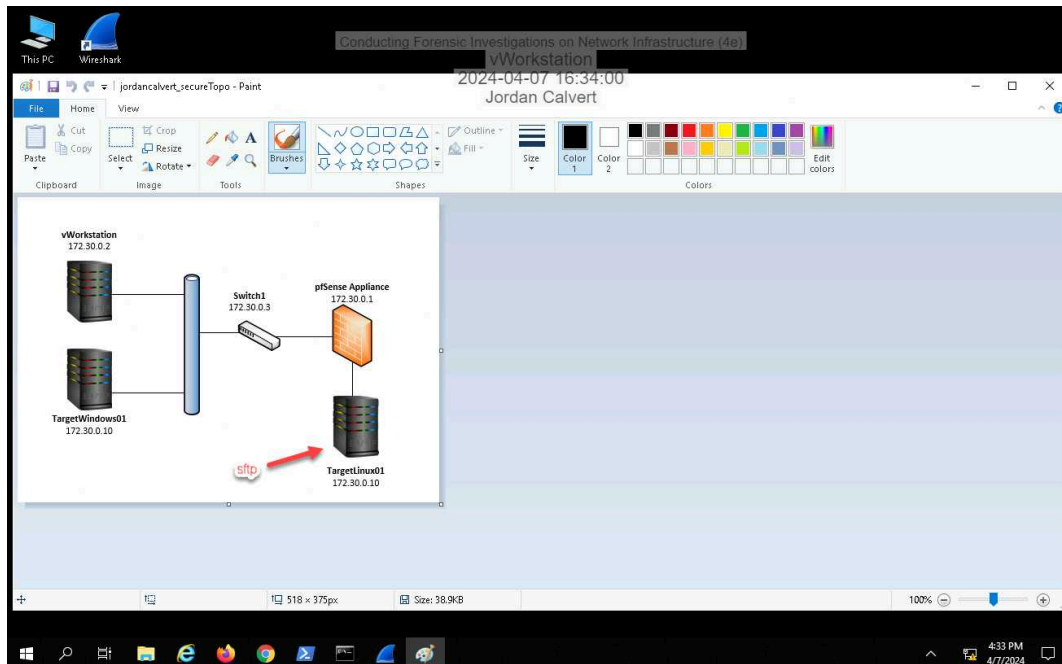


### 20. Make a screen capture showing the Follow TCP stream window.



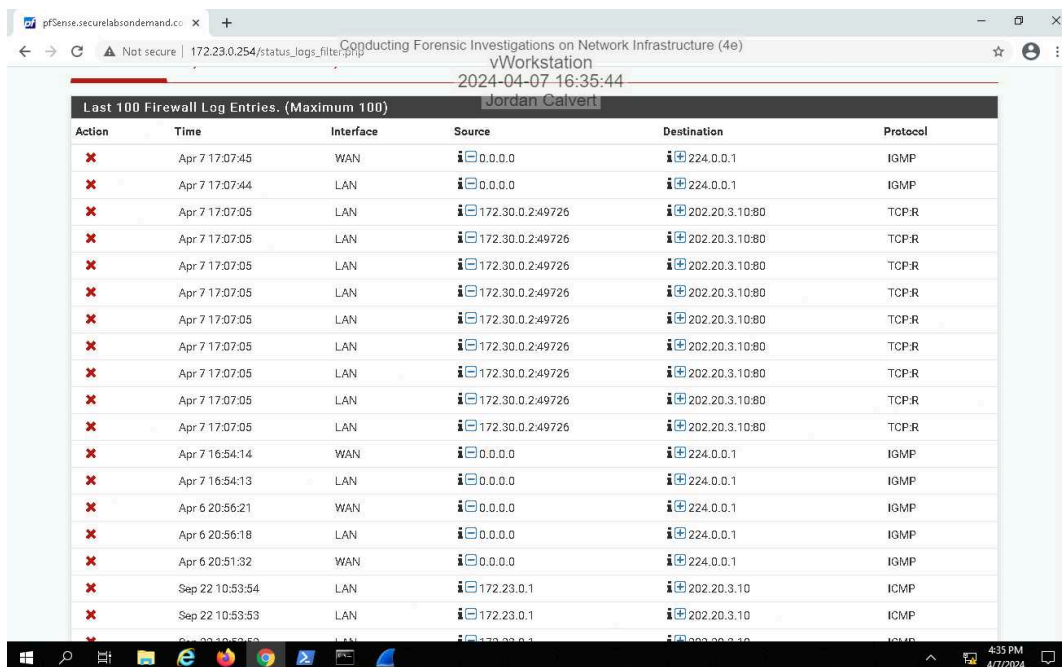


### 32. Make a screen capture showing the reconstituted PNG file.

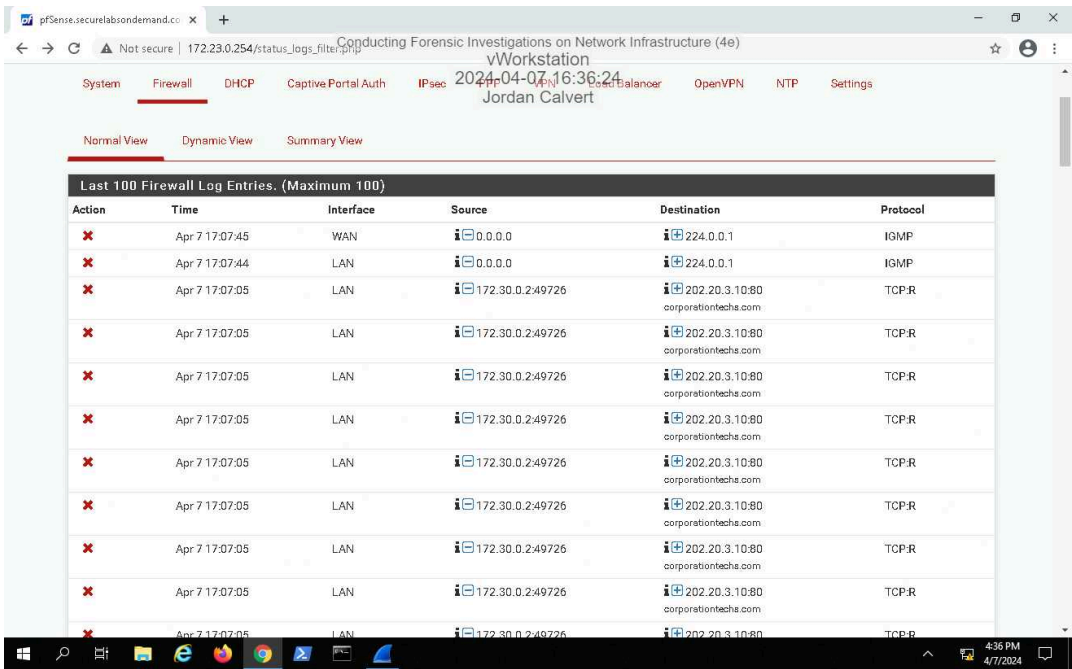


## Part 2: Analyze a Firewall for Forensic Evidence

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



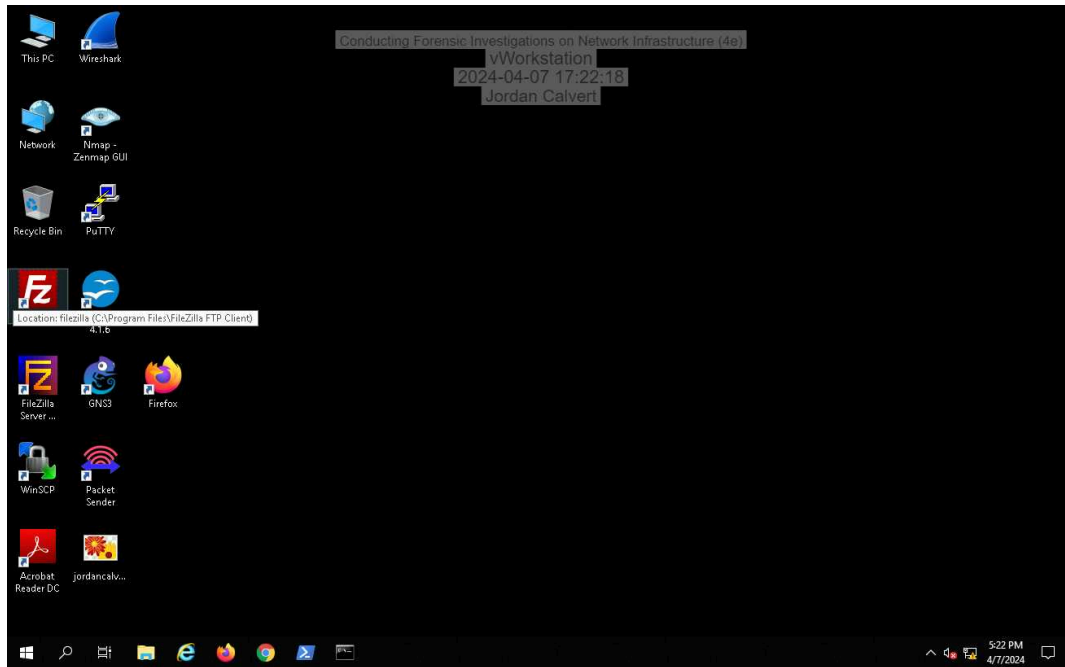
11. Make a screen capture showing the resolved entries in the firewall log.



## Section 3: Challenge and Analysis

### Part 1: Identify the Source of a Suspicious Route

**Make a screen capture** showing the non-RIP route that you discovered on the target router.



### Part 2: Identify Suspicious Outgoing Connections

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

port 443