Computer Networks

Lab # 09:
Wireshark – Packet Capture & Analysis

Introduction:

Wireshark is in fact one of the best tools for packet capturing and analysis. It is used for observing the messages exchanged between computers and supports a variety of protocols.

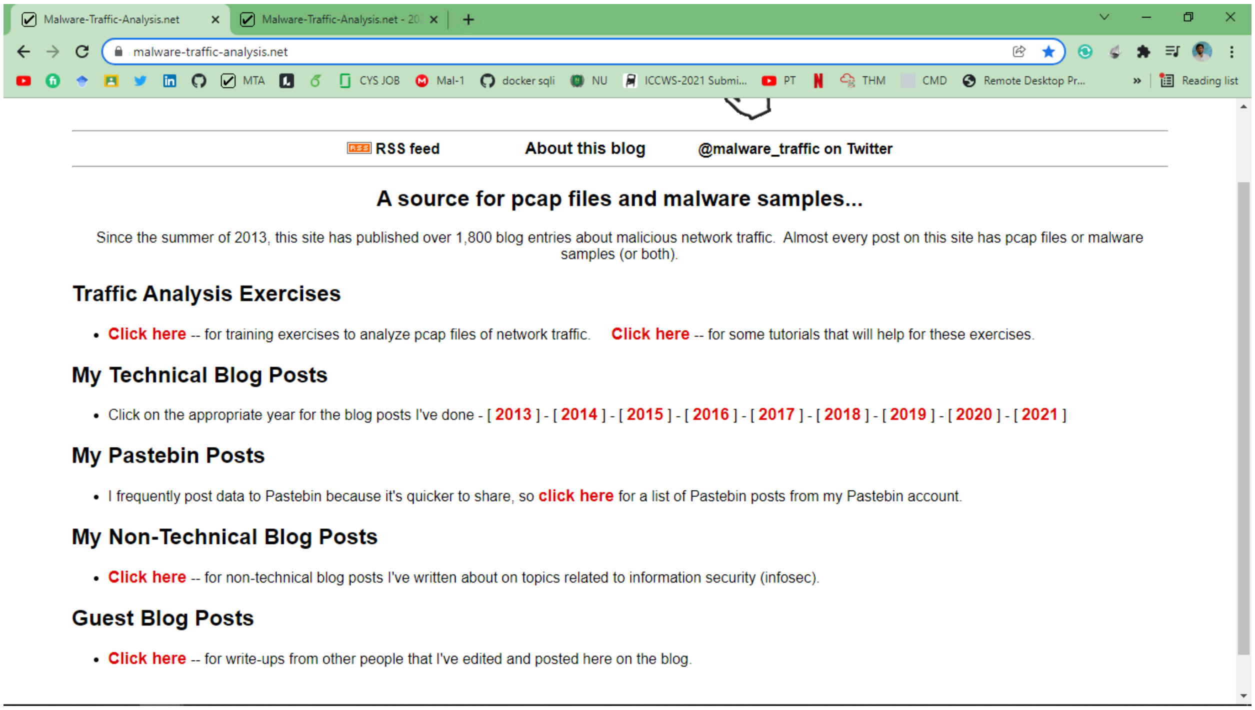
Wireshark consists of 2 parts:

1. The packet capture library receives a copy of every link layer frame that is sent from or received by your computer.
2. The packet analyzer which displays the contents of all fields within a protocol message.

Packet Capture:

You may perform the packet capturing with the following steps:

1. Start up your web browser. Search any website, this will generate some traffic (HTTP, HTTPS and TCP etc.). In my case (https://malware-traffic-analysis.net/)


Malware-Traffic-Analysis.net
Malware-Traffic-Analysis.net - 20
malware-traffic-analysis.net
MTA
CYS JOB
Mal-1
docker sqli
NU
ICCWS-2021 Submi...
PT
THM
CMD
Remote Desktop Pr...
Reading list

RSS feed   About this blog   @malware_traffic on Twitter

A source for pcap files and malware samples...

Since the summer of 2013, this site has published over 1,800 blog entries about malicious network traffic. Almost every post on this site has pcap files or malware samples (or both).

Traffic Analysis Exercises

- **Click here** -- for training exercises to analyze pcap files of network traffic. **Click here** -- for some tutorials that will help for these exercises.

My Technical Blog Posts

- Click on the appropriate year for the blog posts I've done - [**2013**] - [**2014**] - [**2015**] - [**2016**] - [**2017**] - [**2018**] - [**2019**] - [**2020**] - [**2021**]

My Pastebin Posts

- I frequently post data to Pastebin because it's quicker to share, so **click here** for a list of Pastebin posts from my Pastebin account.

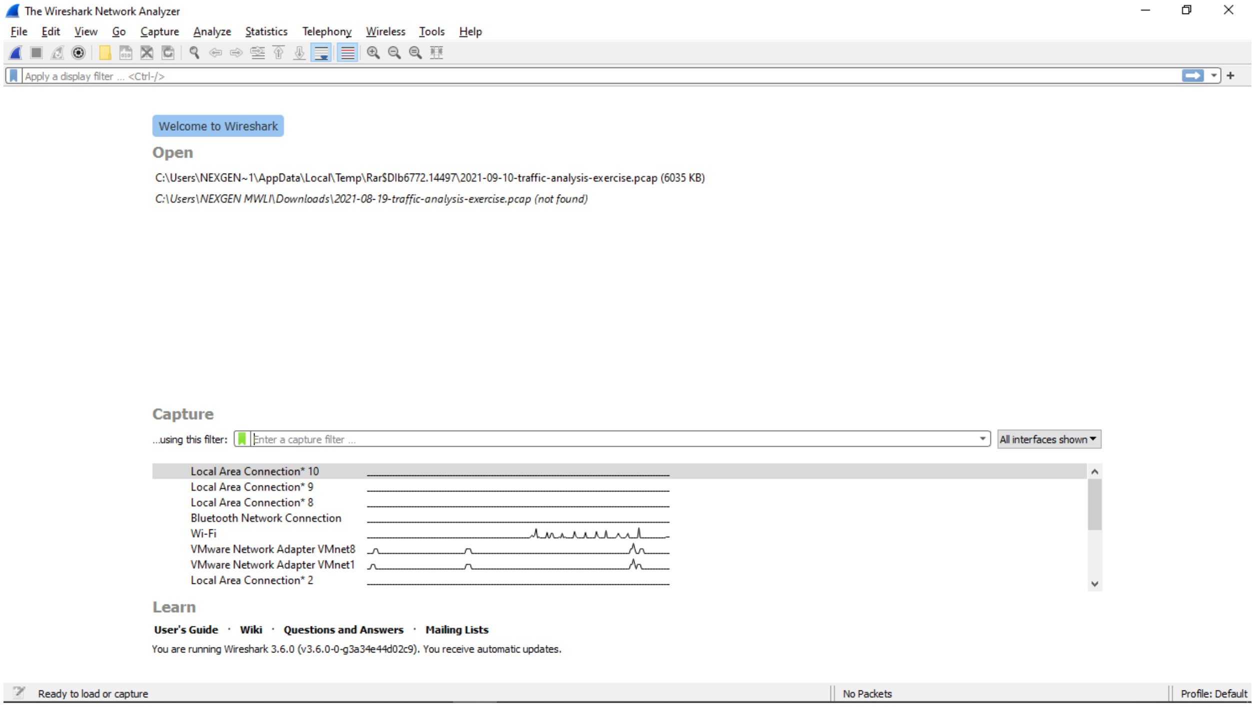
My Non-Technical Blog Posts

- **Click here** -- for non-technical blog posts I've written about on topics related to information security (infosec).

Guest Blog Posts

- **Click here** -- for write-ups from other people that I've edited and posted here on the blog.

2. Start up the Wireshark software. You will initially see the default window. Wireshark has not started the packet capturing.



Open

C:\Users\NEXGEN~1\AppData\Local\Temp\Rar$DIb6772.14497\2021-09-10-traffic-analysis-exercise.pcap (6035 KB)

C:\Users\NEXGEN MWLI\Downloads\2021-08-19-traffic-analysis-exercise.pcap (not found)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2

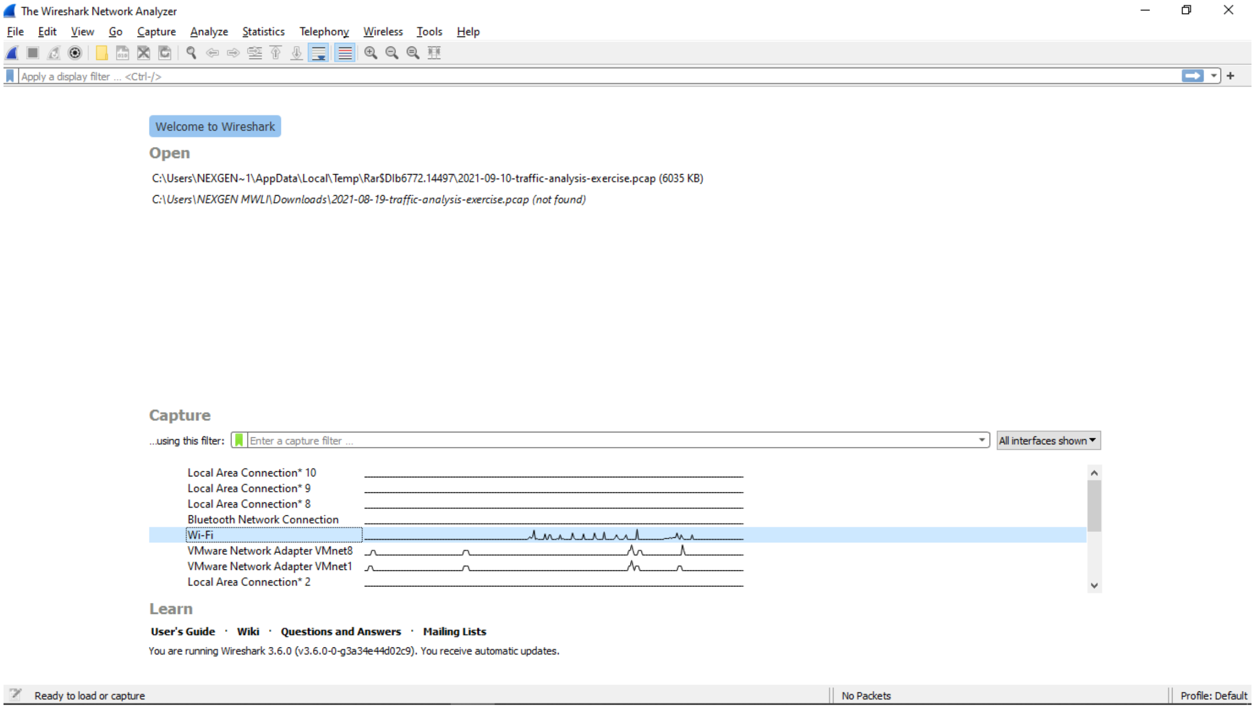
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

3. Select an interface to start the packet capture. Interfaces can be Ethernet, eth0, Wi-Fi, VMware and Local Area Connections etc.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open

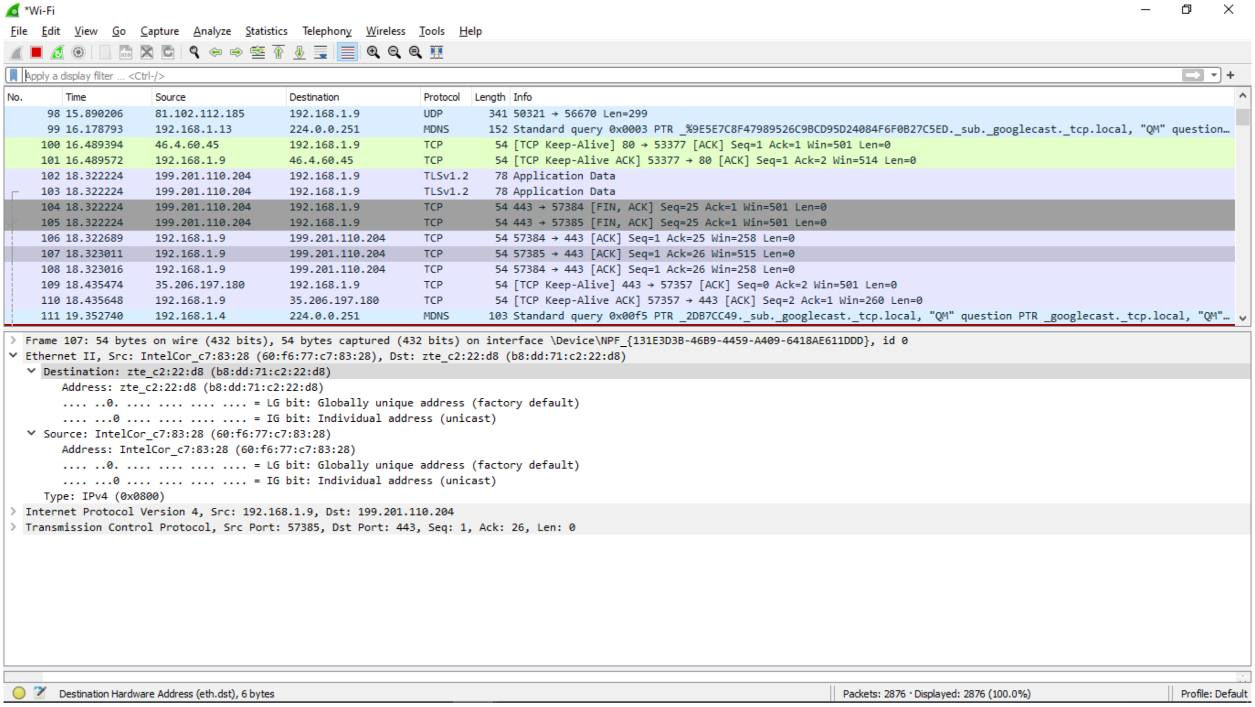
C:\Users\NEXGEN~1\AppData\Local\Temp\Rar$DIb6772.14497\2021-09-10-traffic-analysis-exercise.pcap (6035 KB)
C:\Users\NEXGEN MWLI\Downloads\2021-08-19-traffic-analysis-exercise.pcap (not found)

Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

4. Start the packet capturing by clicking on the selected “interface” (Wi-Fi in my case). You can also start (after selecting the interface) by clicking the **Blue button** on the Top Left.



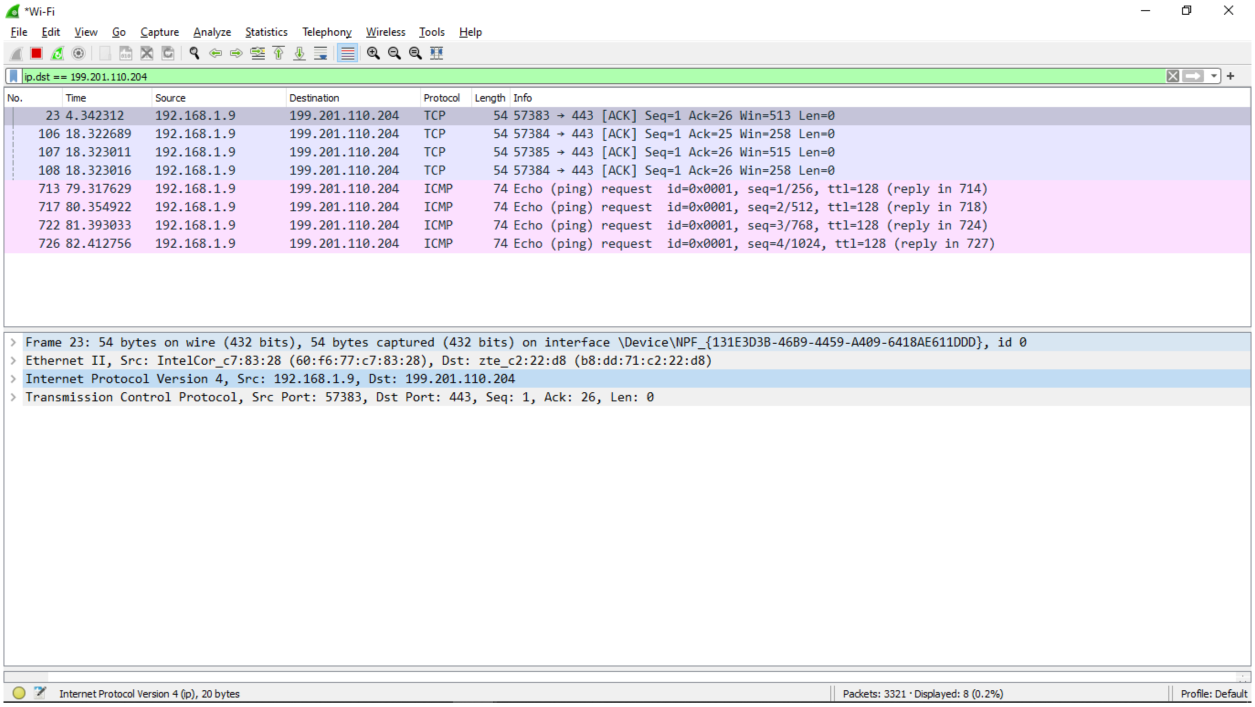
```
No.  Time        Source           Destination      Protocol Length Info
  98 15.890206   81.102.112.185   192.168.1.9      UDP       341 50321 → 56670 Len=299
  99 16.178793   192.168.1.13     224.0.0.251      MDNS      152 Standard query 0x0003 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question…
 100 16.489394   46.4.60.45       192.168.1.9      TCP        54 [TCP Keep-Alive] 80 → 53377 [ACK] Seq=1 Ack=1 Win=501 Len=0
 101 16.489572   192.168.1.9      46.4.60.45       TCP        54 [TCP Keep-Alive ACK] 53377 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
 102 18.322224   199.201.110.204  192.168.1.9      TLSv1.2    78 Application Data
 103 18.322224   199.201.110.204  192.168.1.9      TLSv1.2    78 Application Data
 104 18.322224   199.201.110.204  192.168.1.9      TCP        54 443 → 57384 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
 105 18.322224   199.201.110.204  192.168.1.9      TCP        54 443 → 57385 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
 106 18.322689   192.168.1.9      199.201.110.204  TCP        54 57384 → 443 [ACK] Seq=1 Ack=25 Win=258 Len=0
 107 18.323011   192.168.1.9      199.201.110.204  TCP        54 57385 → 443 [ACK] Seq=1 Ack=26 Win=515 Len=0
 108 18.323016   192.168.1.9      199.201.110.204  TCP        54 57384 → 443 [ACK] Seq=1 Ack=26 Win=258 Len=0
 109 18.435474   35.206.197.180   192.168.1.9      TCP        54 [TCP Keep-Alive] 443 → 57357 [ACK] Seq=0 Ack=2 Win=501 Len=0
 110 18.435648   192.168.1.9      35.206.197.180   TCP        54 [TCP Keep-Alive ACK] 57357 → 443 [ACK] Seq=2 Ack=1 Win=260 Len=0
 111 19.352740   192.168.1.4      224.0.0.251      MDNS      103 Standard query 0x00f5 PTR _2DB7CC49._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM"…
```

```
> Frame 107: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{131E3D3B-46B9-4459-A409-6418AE611DDD}, id 0
v Ethernet II, Src: IntelCor_c7:83:28 (60:f6:77:c7:83:28), Dst: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
  v Destination: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
      Address: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_c7:83:28 (60:f6:77:c7:83:28)
      Address: IntelCor_c7:83:28 (60:f6:77:c7:83:28)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 199.201.110.204
> Transmission Control Protocol, Src Port: 57385, Dst Port: 443, Seq: 1, Ack: 26, Len: 0
```

```
Destination Hardware Address (eth.dst), 6 bytes    Packets: 2876 · Displayed: 2876 (100.0%)    Profile: Default
```

Wireshark Filters:

1. IP Address filters with respect to:
   a. Destination IP Address: ip.dst == 199.201.110.204
   b. Source IP Address: ip.src == 192.168.1.9


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

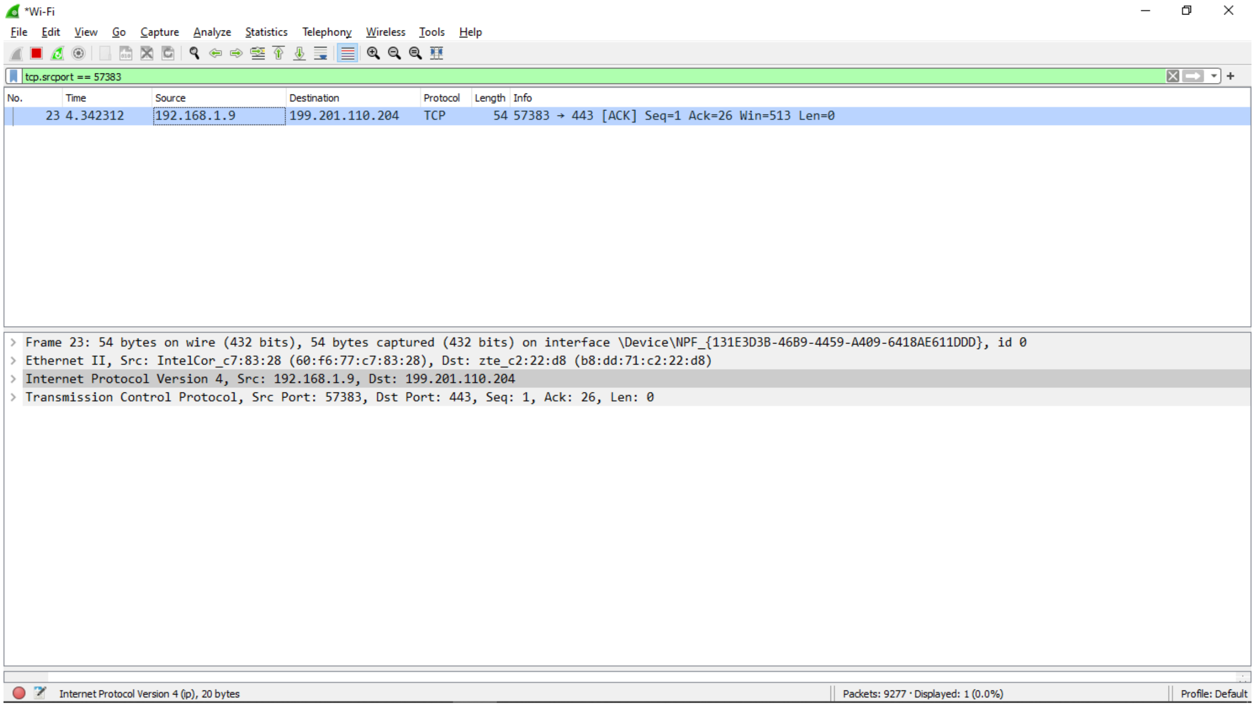
ip.dst == 199.201.110.204

No.	Time	Source	Destination	Protocol	Length	Info
23	4.342312	192.168.1.9	199.201.110.204	TCP	54	57383 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
106	18.322689	192.168.1.9	199.201.110.204	TCP	54	57384 → 443 [ACK] Seq=1 Ack=25 Win=258 Len=0
107	18.323011	192.168.1.9	199.201.110.204	TCP	54	57385 → 443 [ACK] Seq=1 Ack=26 Win=515 Len=0
108	18.323016	192.168.1.9	199.201.110.204	TCP	54	57384 → 443 [ACK] Seq=1 Ack=26 Win=258 Len=0
713	79.317629	192.168.1.9	199.201.110.204	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 714)
717	80.354922	192.168.1.9	199.201.110.204	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 718)
722	81.393033	192.168.1.9	199.201.110.204	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 724)
726	82.412756	192.168.1.9	199.201.110.204	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 727)

```
> Frame 23: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{131E3D3B-46B9-4459-A409-6418AE611DDD}, id 0
> Ethernet II, Src: IntelCor_c7:83:28 (60:f6:77:c7:83:28), Dst: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 199.201.110.204
> Transmission Control Protocol, Src Port: 57383, Dst Port: 443, Seq: 1, Ack: 26, Len: 0
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 3321 · Displayed: 8 (0.2%) | Profile: Default

2. Port filtering w.r.t protocol i.e. TCP, UDP etc. For example:
    a. tcp.srcport == 57383
    b. tcp.dstport == 443


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

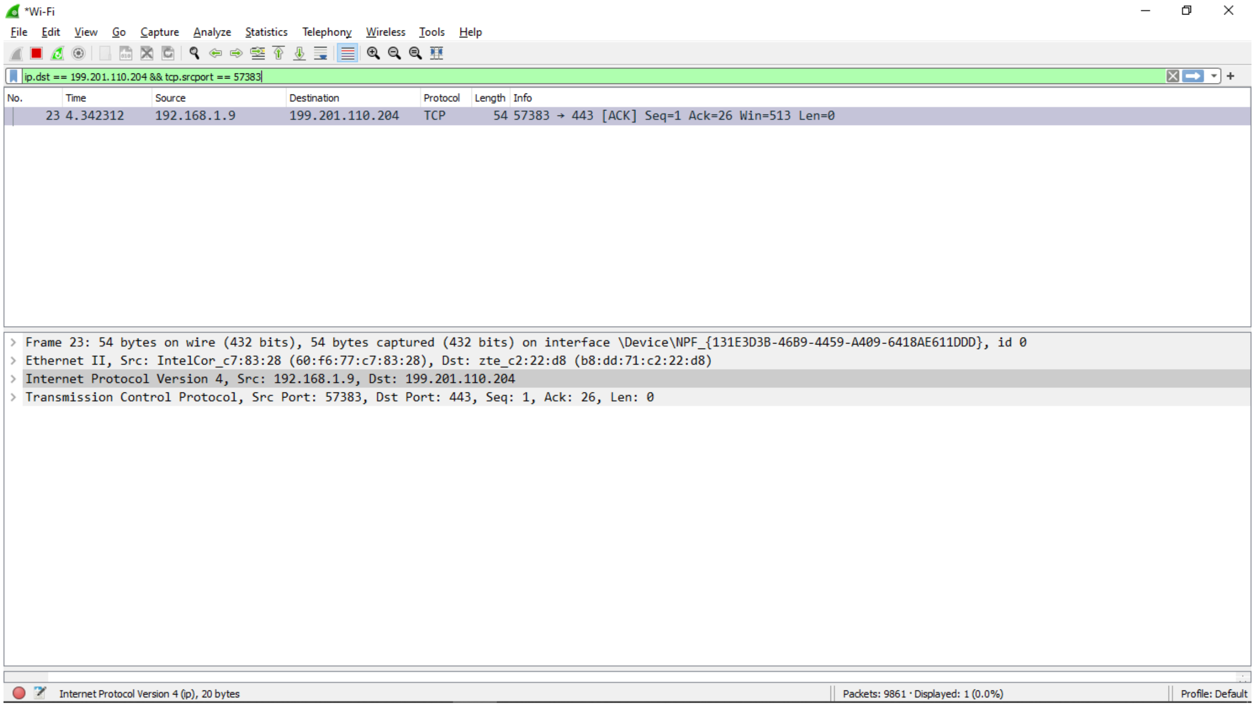
tcp.srcport == 57383

No.	Time	Source	Destination	Protocol	Length	Info
23	4.342312	192.168.1.9	199.201.110.204	TCP	54	57383 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0

```
> Frame 23: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{131E3D3B-46B9-4459-A409-6418AE611DDD}, id 0
> Ethernet II, Src: IntelCor_c7:83:28 (60:f6:77:c7:83:28), Dst: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 199.201.110.204
> Transmission Control Protocol, Src Port: 57383, Dst Port: 443, Seq: 1, Ack: 26, Len: 0
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 9277 · Displayed: 1 (0.0%) | Profile: Default

3. Combined IP and Port filtering, for example:
   a. ip.dst == 199.201.110.204 && tcp.srcport == 57383
   b. ip.dst == 199.201.110.204 && tcp.dstport == 443
   c. *ip.src == 192.168.1.9* && tcp.srcport == 57383
   d. *ip.src == 192.168.1.9* && tcp.dstport == 443


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

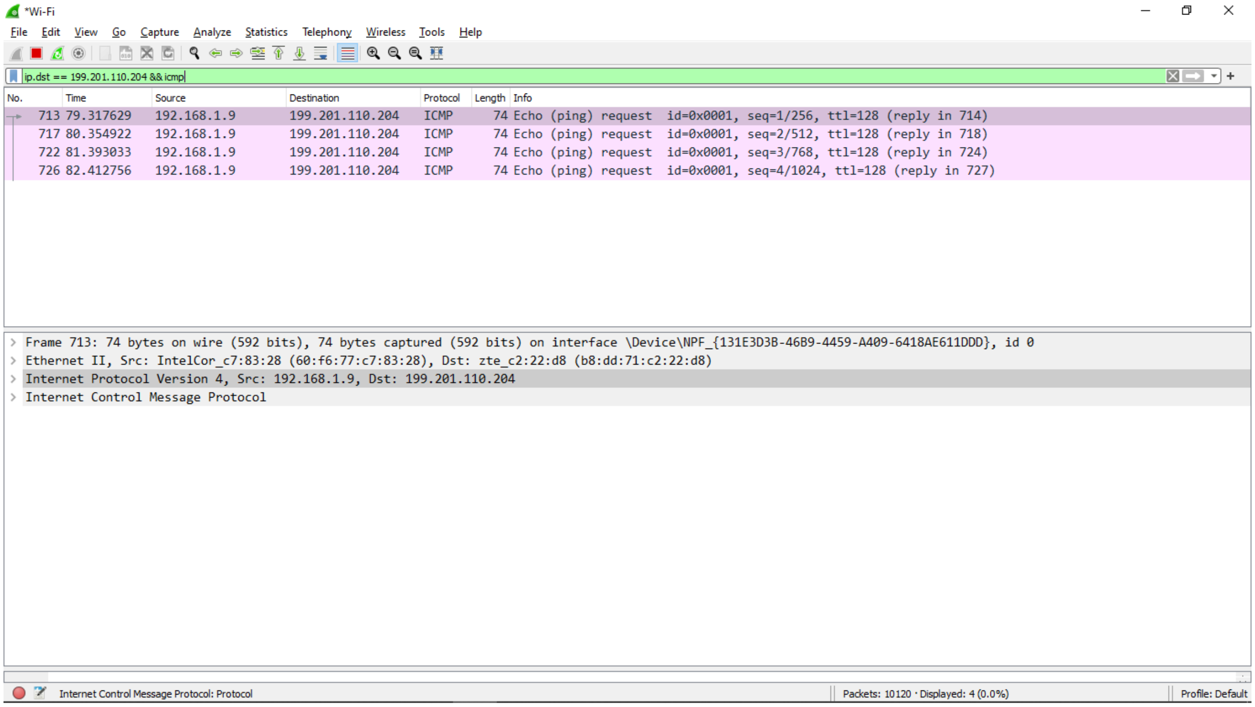
```
ip.dst == 199.201.110.204 && tcp.srcport == 57383

No.   Time         Source          Destination       Protocol  Length  Info
   23 4.342312     192.168.1.9     199.201.110.204   TCP           54  57383 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0

> Frame 23: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{131E3D3B-46B9-4459-A409-6418AE611DDD}, id 0
> Ethernet II, Src: IntelCor_c7:83:28 (60:f6:77:c7:83:28), Dst: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 199.201.110.204
> Transmission Control Protocol, Src Port: 57383, Dst Port: 443, Seq: 1, Ack: 26, Len: 0

Internet Protocol Version 4 (ip), 20 bytes          Packets: 9861 · Displayed: 1 (0.0%)          Profile: Default
```

4. Combined IP and Protocol filtering, for example:
    a. ip.dst == 199.201.110.204 && tcp
    b. ip.dst == 199.201.110.204 && icmp
    c. ip.src == 192.168.1.9 && tcp
    d. ip.src == 192.168.1.9 && icmp


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 199.201.110.204 && icmp

```
No.  Time         Source        Destination      Protocol Length Info
 713 79.317629    192.168.1.9   199.201.110.204  ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 714)
 717 80.354922    192.168.1.9   199.201.110.204  ICMP       74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 718)
 722 81.393033    192.168.1.9   199.201.110.204  ICMP       74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 724)
 726 82.412756    192.168.1.9   199.201.110.204  ICMP       74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 727)
```

```
> Frame 713: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{131E3D3B-46B9-4459-A409-6418AE611DDD}, id 0
> Ethernet II, Src: IntelCor_c7:83:28 (60:f6:77:c7:83:28), Dst: zte_c2:22:d8 (b8:dd:71:c2:22:d8)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 199.201.110.204
> Internet Control Message Protocol
```

Internet Control Message Protocol: Protocol | Packets: 10120 · Displayed: 4 (0.0%) | Profile: Default