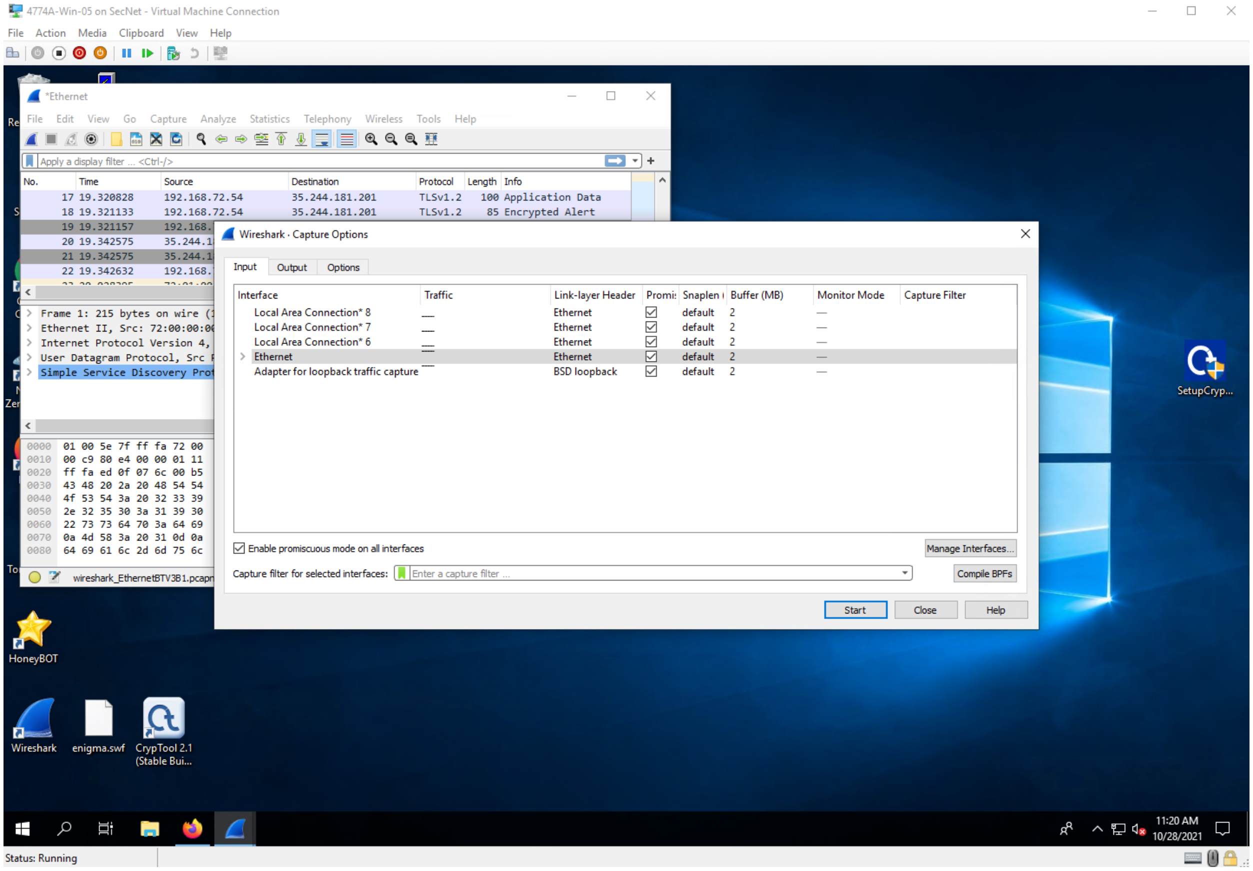
Jamel Douglas
JED18C
Lab 8 - Wireshark
10/19/2021

1 Wireshark I

Screenshots

Step 17



4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
HoneyBOT
Wireshark
enigma.swf
CrypTool 2.1 (Stable Bui...
SetupCryp...
11:20 AM
10/28/2021
Status: Running

```
No.   Time        Source          Destination     Protocol  Length Info
   17 19.320828   192.168.72.54   35.244.181.201  TLSv1.2      100 Application Data
   18 19.321133   192.168.72.54   35.244.181.201  TLSv1.2       85 Encrypted Alert
   19 19.321157   192.168.
   20 19.342575   35.244.1
   21 19.342575   35.244.1
   22 19.342632   192.168.
```

```
> Frame 1: 215 bytes on wire (
> Ethernet II, Src: 72:00:00:0
> Internet Protocol Version 4,
> User Datagram Protocol, Src
> Simple Service Discovery Prot
```

```
0000  01 00 5e 7f ff fa 72 00
0010  00 c9 80 e4 00 00 01 11
0020  ff fa ed 0f 07 6c 00 b5
0030  43 48 20 2a 20 48 54 54
0040  4f 53 54 3a 20 32 33 39
0050  2e 32 35 30 3a 31 39 30
0060  22 73 73 64 70 3a 64 69
0070  0a 4d 58 3a 20 31 0d 0a
0080  64 69 61 6c 2d 6d 75 6c
```

wireshark_EthernetBTV3B1.pcapn

Wireshark · Capture Options

Input | Output | Options

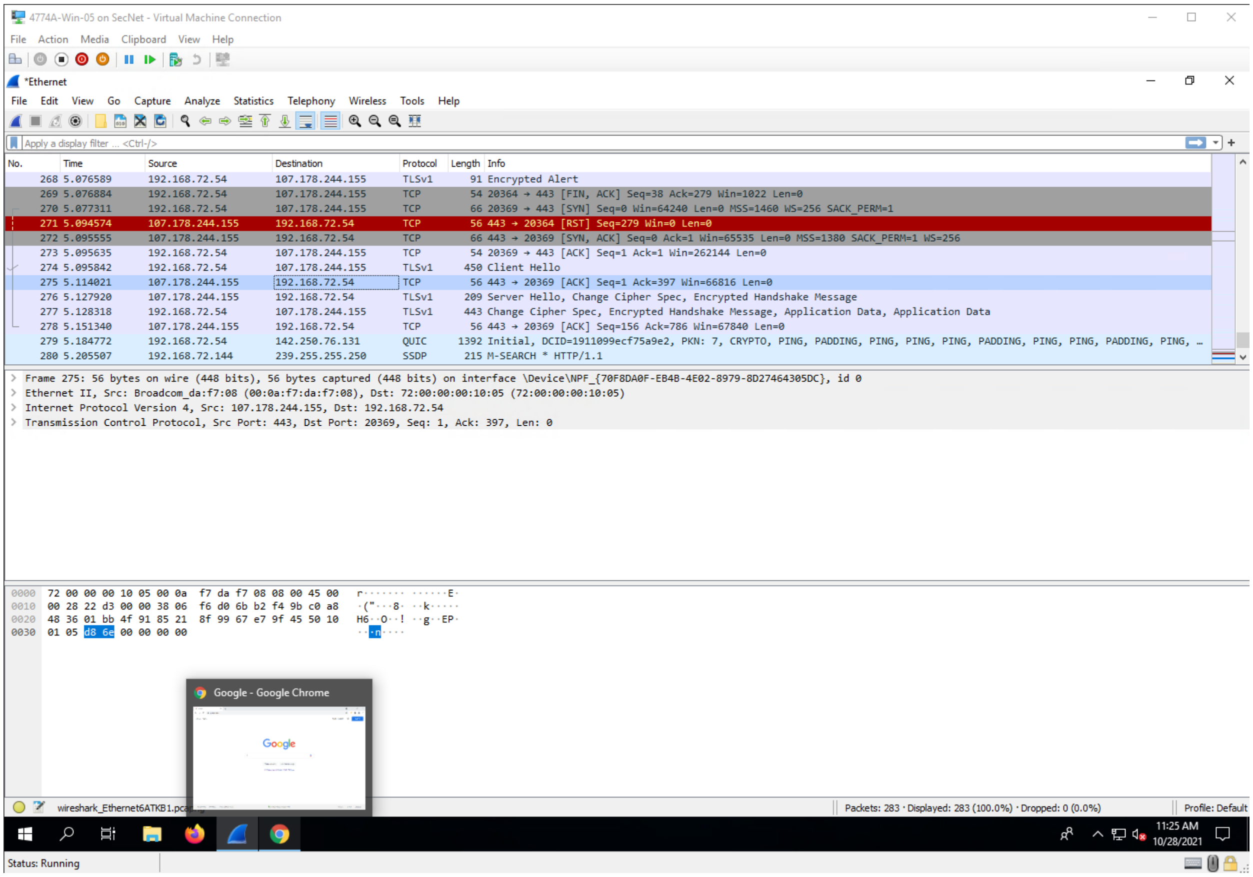
Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (MB)	Monitor Mode	Capture Filter
Local Area Connection* 8	___	Ethernet	☑	default	2	—	
Local Area Connection* 7	___	Ethernet	☑	default	2	—	
Local Area Connection* 6	___	Ethernet	☑	default	2	—	
> Ethernet	___	Ethernet	☑	default	2	—	
Adapter for loopback traffic capture	___	BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Manage Interfaces... | Compile BPFs | Start | Close | Help

Step 25



4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Google - Google Chrome
Google
11:25 AM
10/28/2021

```
No.   Time      Source           Destination      Protocol Length Info
  268 5.076589  192.168.72.54    107.178.244.155  TLSv1     91 Encrypted Alert
  269 5.076884  192.168.72.54    107.178.244.155  TCP       54 20364 → 443 [FIN, ACK] Seq=38 Ack=279 Win=1022 Len=0
  270 5.077311  192.168.72.54    107.178.244.155  TCP       66 20369 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  271 5.094574  107.178.244.155  192.168.72.54    TCP       56 443 → 20364 [RST] Seq=279 Win=0 Len=0
  272 5.095555  107.178.244.155  192.168.72.54    TCP       66 443 → 20369 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM=1 WS=256
  273 5.095635  192.168.72.54    107.178.244.155  TCP       54 20369 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  274 5.095842  192.168.72.54    107.178.244.155  TLSv1    450 Client Hello
  275 5.114021  107.178.244.155  192.168.72.54    TCP       56 443 → 20369 [ACK] Seq=1 Ack=397 Win=66816 Len=0
  276 5.127920  107.178.244.155  192.168.72.54    TLSv1    209 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  277 5.128318  192.168.72.54    107.178.244.155  TLSv1    443 Change Cipher Spec, Encrypted Handshake Message, Application Data, Application Data
  278 5.151340  107.178.244.155  192.168.72.54    TCP       56 443 → 20369 [ACK] Seq=156 Ack=786 Win=67840 Len=0
  279 5.184772  192.168.72.54    142.250.76.131   QUIC    1392 Initial, DCID=1911099ecf75a9e2, PKN: 7, CRYPTO, PING, PADDING, PING, PING, PING, PADDING, PING, PING, PADDING, PING, …
  280 5.205507  192.168.72.144   239.255.255.250  SSDP     215 M-SEARCH * HTTP/1.1
```

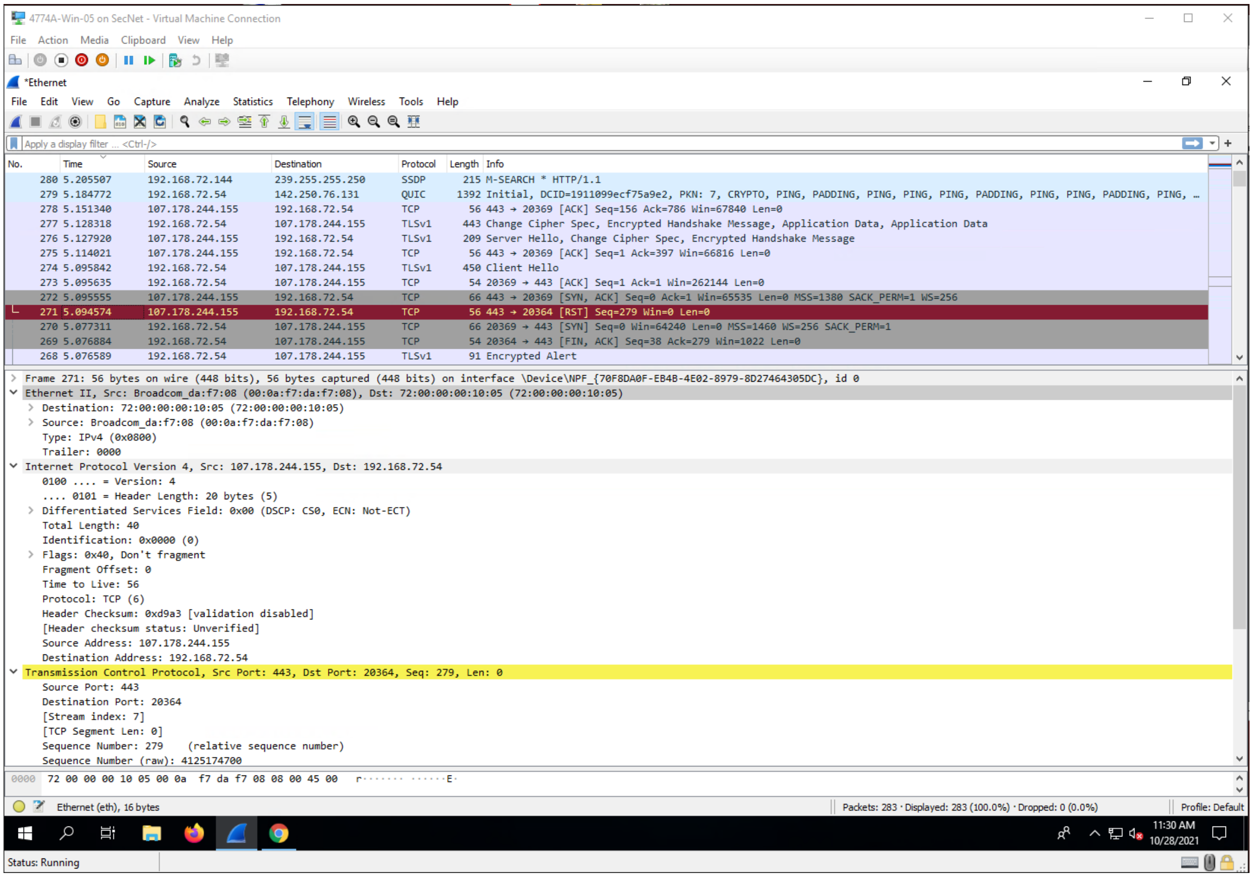
```
> Frame 275: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{70F8DA0F-EB4B-4E02-8979-8D27464305DC}, id 0
> Ethernet II, Src: Broadcom_da:f7:08 (00:0a:f7:da:f7:08), Dst: 72:00:00:00:10:05 (72:00:00:00:10:05)
> Internet Protocol Version 4, Src: 107.178.244.155, Dst: 192.168.72.54
> Transmission Control Protocol, Src Port: 443, Dst Port: 20369, Seq: 1, Ack: 397, Len: 0
```

```
0000  72 00 00 00 10 05 00 0a  f7 da f7 08 08 00 45 00   r······· ······E·
0010  00 28 22 d3 00 00 38 06  f6 d0 6b b2 f4 9b c0 a8   ·("···8· ··k·····
0020  48 36 01 bb 4f 91 85 21  8f 99 67 e7 9f 45 50 10   H6··O··! ··g··EP·
0030  01 05 d8 6e 00 00 00 00                            ···n····
```

wireshark_Ethernet6ATKB1.pca… | Packets: 283 · Displayed: 283 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Status: Running

Step 30


4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
280	5.205507	192.168.72.144	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
279	5.184772	192.168.72.54	142.250.76.131	QUIC	1392	Initial, DCID=1911099ecf75a9e2, PKN: 7, CRYPTO, PING, PADDING, PING, PING, PING, PADDING, PING, PING, PADDING, PING, …
278	5.151340	107.178.244.155	192.168.72.54	TCP	56	443 → 20369 [ACK] Seq=156 Ack=786 Win=67840 Len=0
277	5.128318	192.168.72.54	107.178.244.155	TLSv1	443	Change Cipher Spec, Encrypted Handshake Message, Application Data, Application Data
276	5.127920	107.178.244.155	192.168.72.54	TLSv1	209	Server Hello, Change Cipher Spec, Encrypted Handshake Message
275	5.114021	107.178.244.155	192.168.72.54	TCP	56	443 → 20369 [ACK] Seq=1 Ack=397 Win=66816 Len=0
274	5.095842	192.168.72.54	107.178.244.155	TLSv1	450	Client Hello
273	5.095635	192.168.72.54	107.178.244.155	TCP	54	20369 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
272	5.095555	107.178.244.155	192.168.72.54	TCP	66	443 → 20369 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 SACK_PERM=1 WS=256
271	5.094574	107.178.244.155	192.168.72.54	TCP	56	443 → 20364 [RST] Seq=279 Win=0 Len=0
270	5.077311	192.168.72.54	107.178.244.155	TCP	66	20369 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
269	5.076884	192.168.72.54	107.178.244.155	TCP	54	20364 → 443 [FIN, ACK] Seq=38 Ack=279 Win=1022 Len=0
268	5.076589	192.168.72.54	107.178.244.155	TLSv1	91	Encrypted Alert

```
> Frame 271: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{70F8DA0F-EB4B-4E02-8979-8D27464305DC}, id 0
v Ethernet II, Src: Broadcom_da:f7:08 (00:0a:f7:da:f7:08), Dst: 72:00:00:00:10:05 (72:00:00:00:10:05)
  > Destination: 72:00:00:00:10:05 (72:00:00:00:10:05)
  > Source: Broadcom_da:f7:08 (00:0a:f7:da:f7:08)
    Type: IPv4 (0x0800)
    Trailer: 0000
v Internet Protocol Version 4, Src: 107.178.244.155, Dst: 192.168.72.54
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x0000 (0)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 56
    Protocol: TCP (6)
    Header Checksum: 0xd9a3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 107.178.244.155
    Destination Address: 192.168.72.54
v Transmission Control Protocol, Src Port: 443, Dst Port: 20364, Seq: 279, Len: 0
    Source Port: 443
    Destination Port: 20364
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence Number: 279    (relative sequence number)
    Sequence Number (raw): 4125174700
```

```
0000  72 00 00 00 10 05 00 0a  f7 da f7 08 08 00 45 00   r······· ······E·
```

Ethernet (eth), 16 bytes | Packets: 283 · Displayed: 283 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

11:30 AM
10/28/2021

Status: Running

Project Questions

1. My IP address is 192.168.72.54
2. One of the remote IP addresses my computer was communicating with was 107.178.244.155
3. I captured 280 packets
4. The blue entities are of the Simple Service Discovery Protocol (SSDP) and QUIC protocol types.

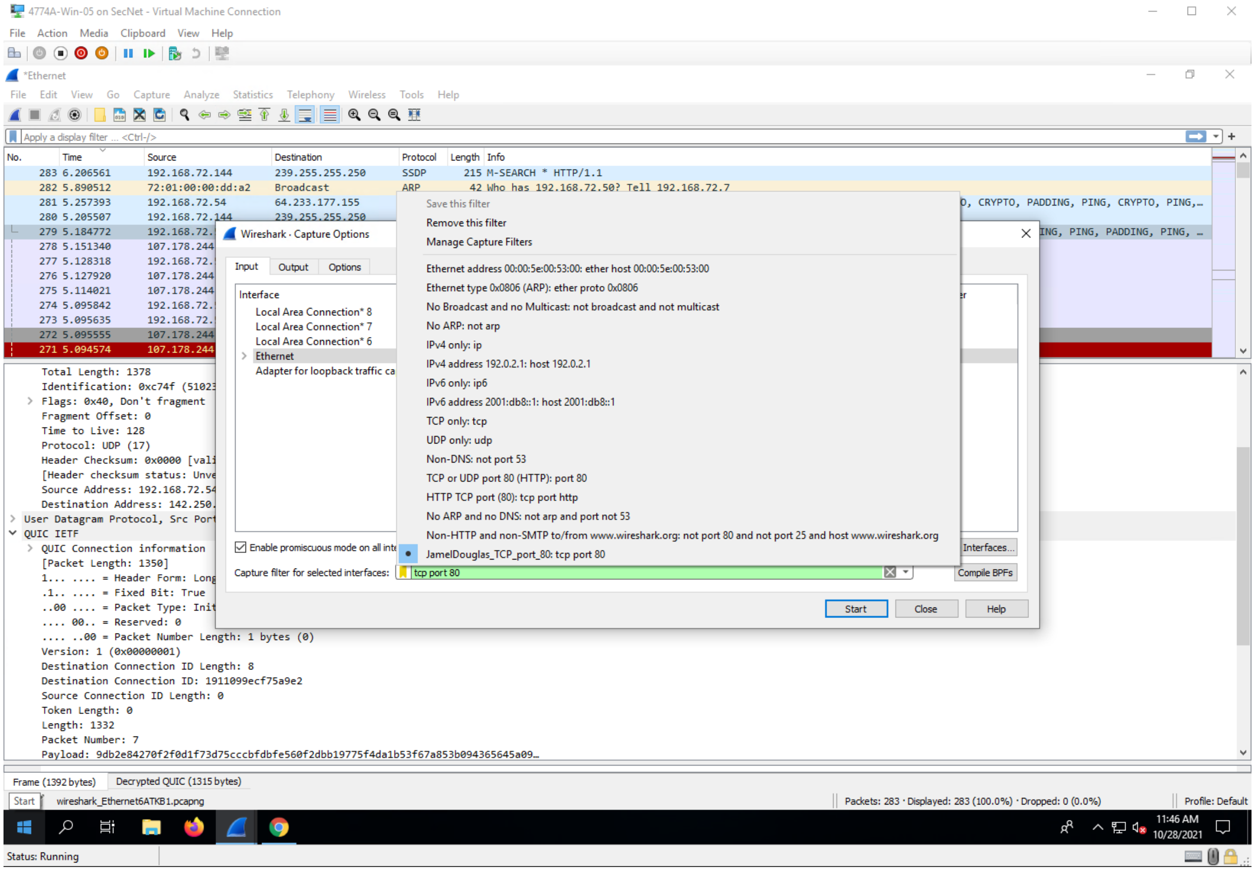
Thought Questions

1. The different colors represent different types of packets.
2. My computer sometimes got packets addressed for a machine with a different MAC address. These packets are broadcast packets and get sent to every machine on the network, the machine that it is meant for will then reply once it gets the packet.
3. The number of packets sent/received on a single mouse click depends on the content that is being displayed.
4. Yes, you can filter out specific packets so that only those ones a logged.

2 Wireshark II

Screenshots

Step 7


4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Capture Options
Input
Output
Options
Interfaces…
Compile BPFs
Start
Close
Help

```
No.  Time      Source             Destination       Protocol  Length Info
 283 6.206561  192.168.72.144     239.255.255.250   SSDP      215 M-SEARCH * HTTP/1.1
 282 5.890512  72:01:00:00:dd:a2  Broadcast         ARP        42 Who has 192.168.72.50? Tell 192.168.72.7
 281 5.257393  192.168.72.54      64.233.177.155                   O, CRYPTO, PADDING, PING, CRYPTO, PING,…
 280 5.205507  192.168.72.144     239.255.255.250
 279 5.184772  192.168.72.                                         ING, PING, PADDING, PING, …
 278 5.151340  107.178.244
 277 5.128318  192.168.72.
 276 5.127920  107.178.244
 275 5.114021  107.178.244
 274 5.095842  192.168.72.
 273 5.095635  192.168.72.
 272 5.095555  107.178.244
 271 5.094574  107.178.244
```

```
    Total Length: 1378
    Identification: 0xc74f (51023
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [vali
    [Header checksum status: Unve
    Source Address: 192.168.72.54
    Destination Address: 142.250.
> User Datagram Protocol, Src Port
v QUIC IETF
  > QUIC Connection information
    [Packet Length: 1350]
    1... .... = Header Form: Long
    .1.. .... = Fixed Bit: True
    ..00 .... = Packet Type: Init
    .... 00.. = Reserved: 0
    .... ..00 = Packet Number Length: 1 bytes (0)
    Version: 1 (0x00000001)
    Destination Connection ID Length: 8
    Destination Connection ID: 1911099ecf75a9e2
    Source Connection ID Length: 0
    Token Length: 0
    Length: 1332
    Packet Number: 7
    Payload: 9db2e84270f2f0d1f73d75cccbfdbfe560f2dbb19775f4da1b53f67a853b094365645a09…
```

Interface
- Local Area Connection* 8
- Local Area Connection* 7
- Local Area Connection* 6
- Ethernet
- Adapter for loopback traffic ca

☑ Enable promiscuous mode on all inte

Capture filter for selected interfaces: tcp port 80

Save this filter
Remove this filter
Manage Capture Filters

Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): ether proto 0x0806
No Broadcast and no Multicast: not broadcast and not multicast
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: host 192.0.2.1
IPv6 only: ip6
IPv6 address 2001:db8::1: host 2001:db8::1
TCP only: tcp
UDP only: udp
Non-DNS: not port 53
TCP or UDP port 80 (HTTP): port 80
HTTP TCP port (80): tcp port http
No ARP and no DNS: not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www.wireshark.org
● JamelDouglas_TCP_port_80: tcp port 80

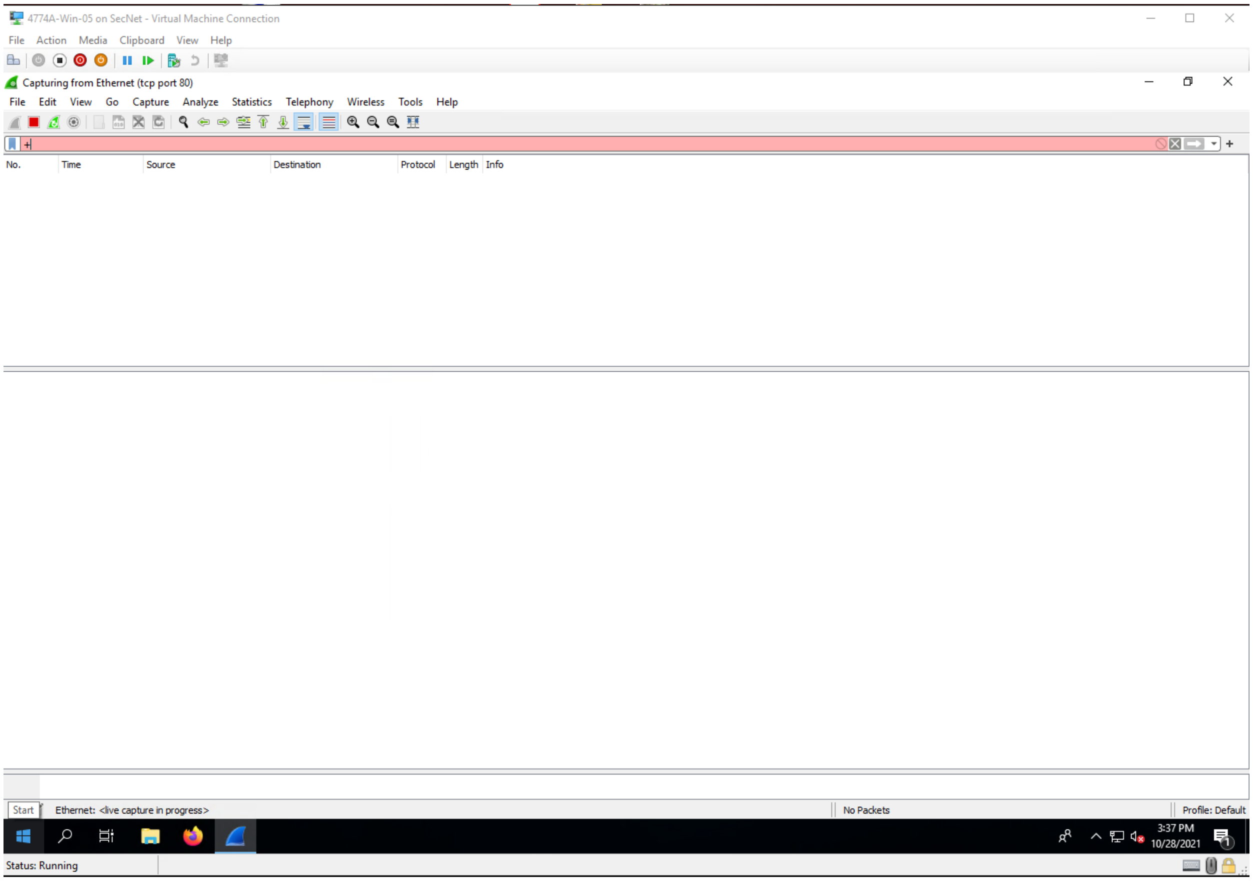
Frame (1392 bytes) Decrypted QUIC (1315 bytes)

Start wireshark_Ethernet6ATKB1.pcapng Packets: 283 · Displayed: 283 (100.0%) · Dropped: 0 (0.0%) Profile: Default

11:46 AM 10/28/2021

Status: Running

Step 20


4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Start
3:37 PM
10/28/2021

Capturing from Ethernet (tcp port 80)

Ethernet: <live capture in progress>

No Packets

Profile: Default

Status: Running

Project Questions

1. I did not capture any packets. Sites now use encrypted protocols (HTTPS) to communicate, port 80 is pretty much obsolete.
2. I did not capture any packets; I was unable to determine the row number.
3. I did not capture any packets; I was not able to see the source port on a GET request.
4. My IP address is 192.168.72.54.

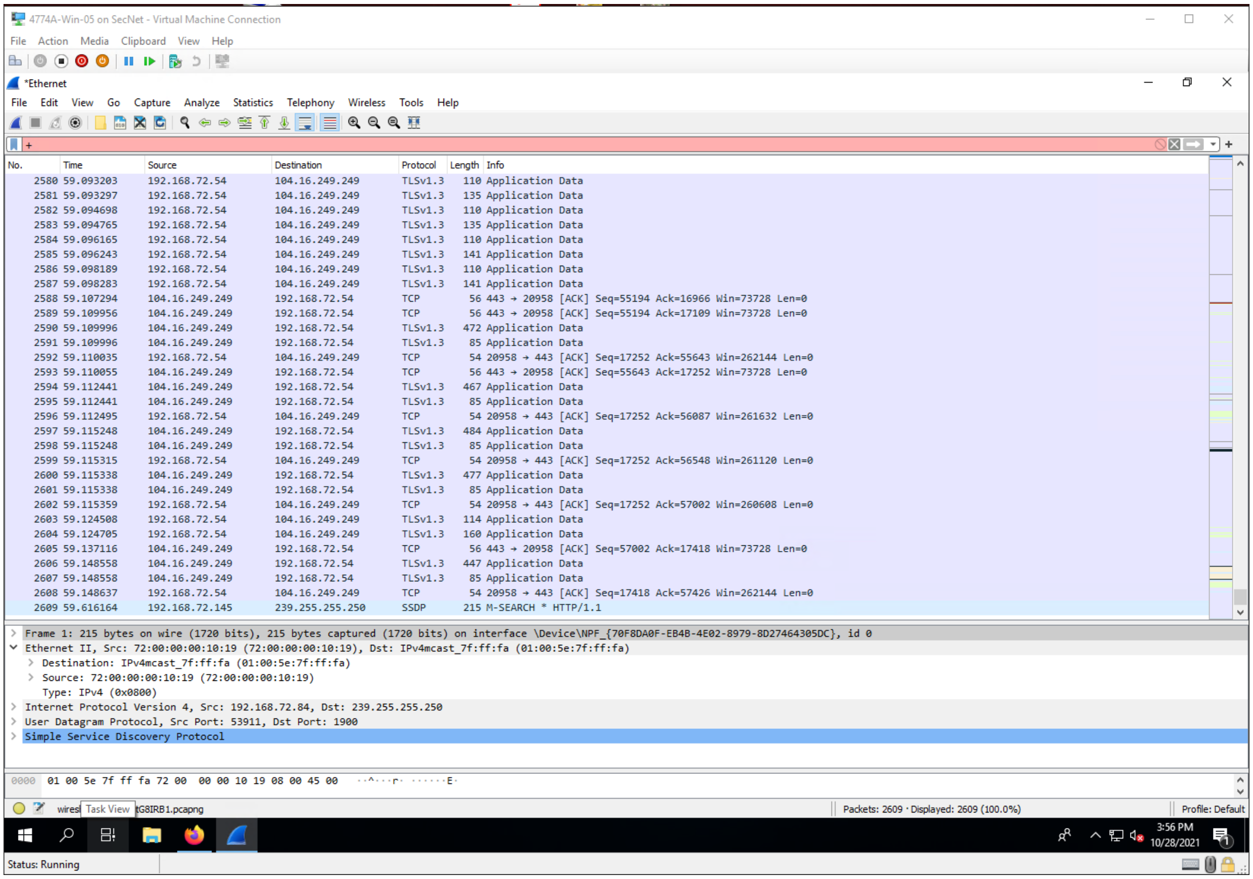
Thought Questions

1. Computers break up information into packets to send them because that is the most efficient way to transfer data. Sending data as one big packet could eat up all the available bandwidth.
2. SYN is used to initiate a connection. ACK is used to confirm that other side has received SYN. FIN is used to terminate connections. GET is an HTTP method that requests the specified resource.
3. Sequence numbers allow packets to be reconstructed in order if they were received out of order
4. My computer sends a packet to the webserver to establish a connection with it. It would also send a packet to request a certain resource, which in this case could be a home page.

4 Wireshark IV

Screenshots

Step 10

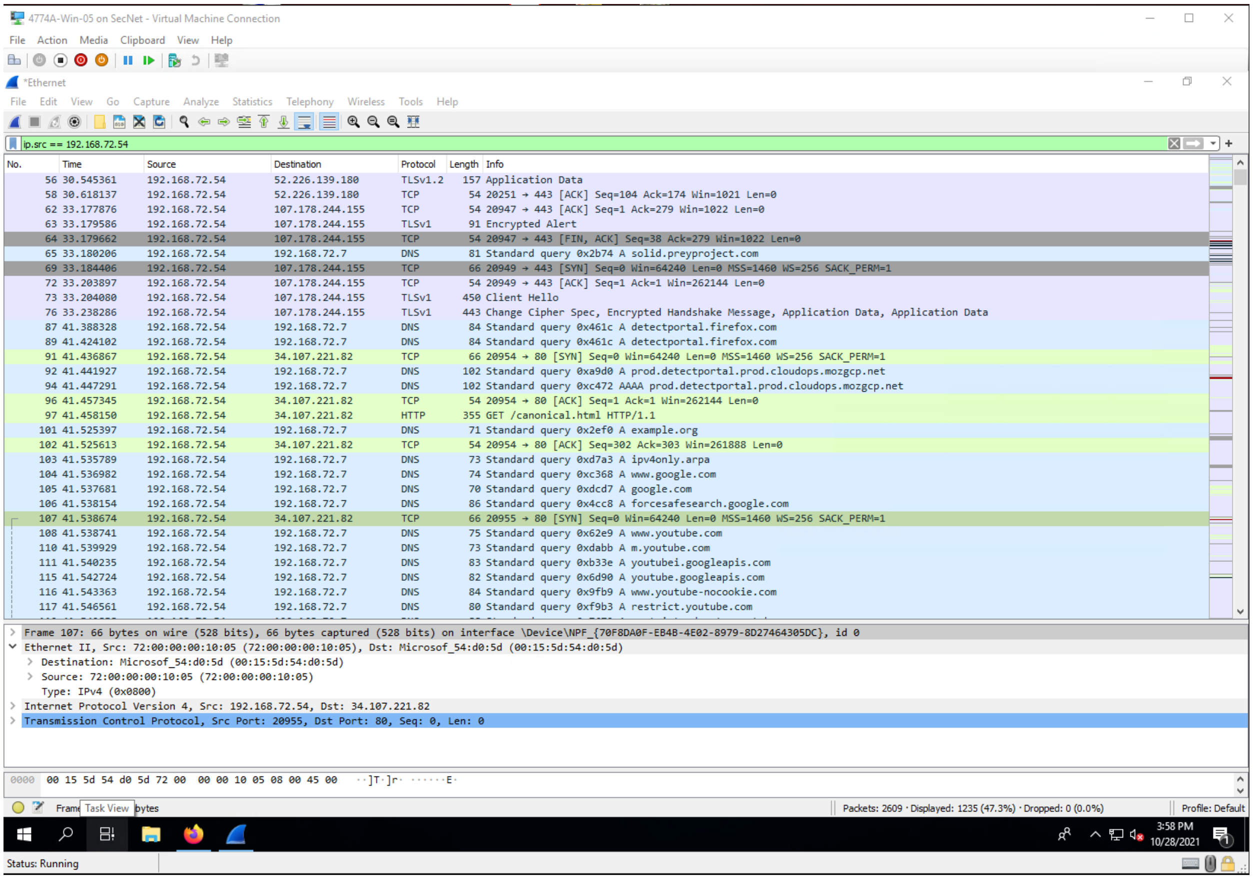

4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wiresl Task View tG8IRB1.pcapng
Packets: 2609 · Displayed: 2609 (100.0%)
Profile: Default
3:56 PM
10/28/2021
Status: Running

```
No.     Time        Source           Destination      Protocol Length Info
   2580 59.093203   192.168.72.54    104.16.249.249   TLSv1.3   110 Application Data
   2581 59.093297   192.168.72.54    104.16.249.249   TLSv1.3   135 Application Data
   2582 59.094698   192.168.72.54    104.16.249.249   TLSv1.3   110 Application Data
   2583 59.094765   192.168.72.54    104.16.249.249   TLSv1.3   135 Application Data
   2584 59.096165   192.168.72.54    104.16.249.249   TLSv1.3   110 Application Data
   2585 59.096243   192.168.72.54    104.16.249.249   TLSv1.3   141 Application Data
   2586 59.098189   192.168.72.54    104.16.249.249   TLSv1.3   110 Application Data
   2587 59.098283   192.168.72.54    104.16.249.249   TLSv1.3   141 Application Data
   2588 59.107294   104.16.249.249   192.168.72.54    TCP        56 443 → 20958 [ACK] Seq=55194 Ack=16966 Win=73728 Len=0
   2589 59.109956   104.16.249.249   192.168.72.54    TCP        56 443 → 20958 [ACK] Seq=55194 Ack=17109 Win=73728 Len=0
   2590 59.109996   104.16.249.249   192.168.72.54    TLSv1.3   472 Application Data
   2591 59.109996   104.16.249.249   192.168.72.54    TLSv1.3    85 Application Data
   2592 59.110035   192.168.72.54    104.16.249.249   TCP        54 20958 → 443 [ACK] Seq=17252 Ack=55643 Win=262144 Len=0
   2593 59.110055   104.16.249.249   192.168.72.54    TCP        56 443 → 20958 [ACK] Seq=55643 Ack=17252 Win=73728 Len=0
   2594 59.112441   104.16.249.249   192.168.72.54    TLSv1.3   467 Application Data
   2595 59.112441   104.16.249.249   192.168.72.54    TLSv1.3    85 Application Data
   2596 59.112495   192.168.72.54    104.16.249.249   TCP        54 20958 → 443 [ACK] Seq=17252 Ack=56087 Win=261632 Len=0
   2597 59.115248   104.16.249.249   192.168.72.54    TLSv1.3   484 Application Data
   2598 59.115248   104.16.249.249   192.168.72.54    TLSv1.3    85 Application Data
   2599 59.115315   192.168.72.54    104.16.249.249   TCP        54 20958 → 443 [ACK] Seq=17252 Ack=56548 Win=261120 Len=0
   2600 59.115338   104.16.249.249   192.168.72.54    TLSv1.3   477 Application Data
   2601 59.115338   104.16.249.249   192.168.72.54    TLSv1.3    85 Application Data
   2602 59.115359   192.168.72.54    104.16.249.249   TCP        54 20958 → 443 [ACK] Seq=17252 Ack=57002 Win=260608 Len=0
   2603 59.124508   192.168.72.54    104.16.249.249   TLSv1.3   114 Application Data
   2604 59.124705   192.168.72.54    104.16.249.249   TLSv1.3   160 Application Data
   2605 59.137116   104.16.249.249   192.168.72.54    TCP        56 443 → 20958 [ACK] Seq=57002 Ack=17418 Win=73728 Len=0
   2606 59.148558   104.16.249.249   192.168.72.54    TLSv1.3   447 Application Data
   2607 59.148558   104.16.249.249   192.168.72.54    TLSv1.3    85 Application Data
   2608 59.148637   192.168.72.54    104.16.249.249   TCP        54 20958 → 443 [ACK] Seq=17418 Ack=57426 Win=262144 Len=0
   2609 59.616164   192.168.72.145   239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1

> Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{70F8DA0F-EB4B-4E02-8979-8D27464305DC}, id 0
v Ethernet II, Src: 72:00:00:00:10:19 (72:00:00:00:10:19), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Source: 72:00:00:00:10:19 (72:00:00:00:10:19)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.72.84, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53911, Dst Port: 1900
> Simple Service Discovery Protocol

0000  01 00 5e 7f ff fa 72 00  00 00 10 19 08 00 45 00   ··^···r· ······E·
```

Step 14



4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.72.54

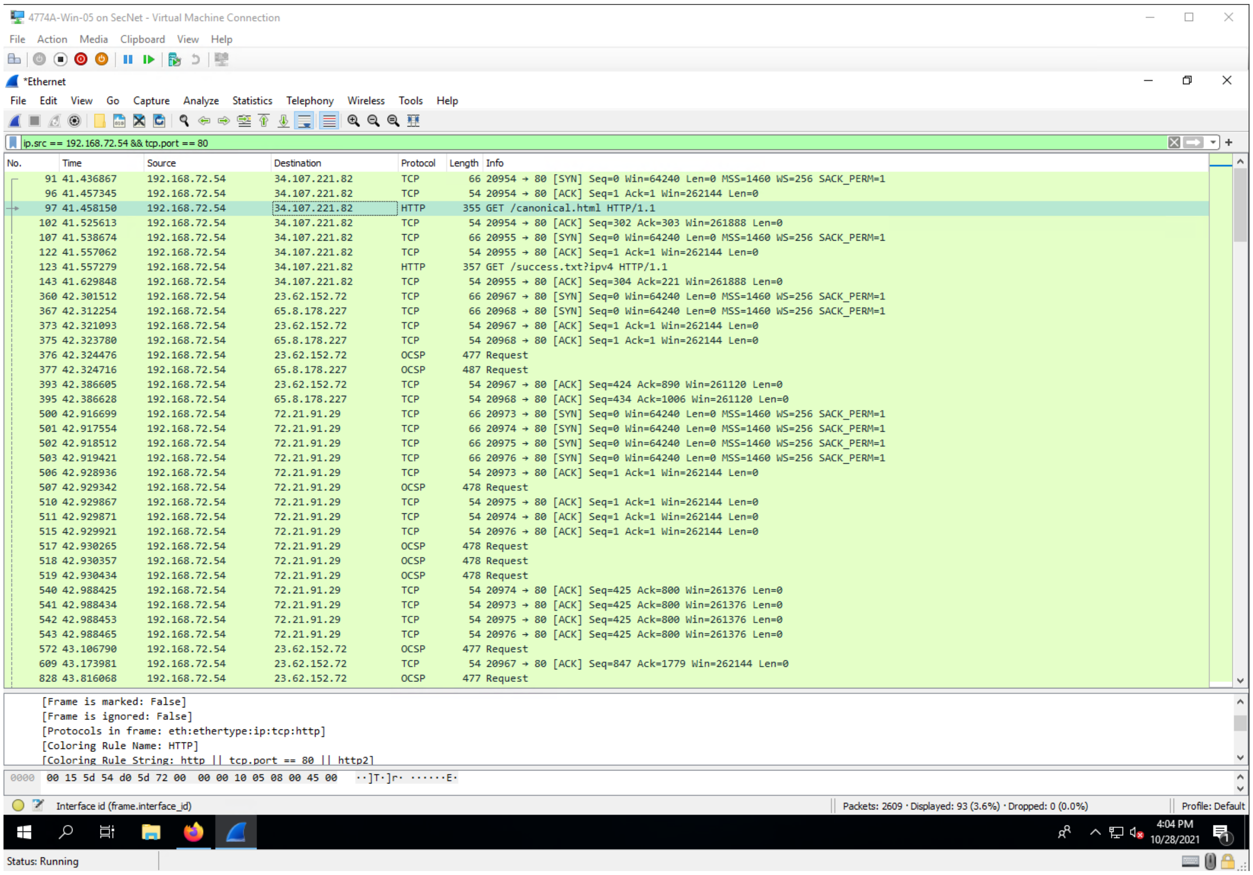
```
No.    Time        Source          Destination      Protocol  Length Info
    56 30.545361   192.168.72.54   52.226.139.180   TLSv1.2    157 Application Data
    58 30.618137   192.168.72.54   52.226.139.180   TCP         54 20251 → 443 [ACK] Seq=104 Ack=174 Win=1021 Len=0
    62 33.177876   192.168.72.54   107.178.244.155  TCP         54 20947 → 443 [ACK] Seq=1 Ack=279 Win=1022 Len=0
    63 33.179586   192.168.72.54   107.178.244.155  TLSv1       91 Encrypted Alert
    64 33.179662   192.168.72.54   107.178.244.155  TCP         54 20947 → 443 [FIN, ACK] Seq=38 Ack=279 Win=1022 Len=0
    65 33.180206   192.168.72.54   192.168.72.7     DNS         81 Standard query 0x2b74 A solid.preyproject.com
    69 33.184406   192.168.72.54   107.178.244.155  TCP         66 20949 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    72 33.203897   192.168.72.54   107.178.244.155  TCP         54 20949 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    73 33.204080   192.168.72.54   107.178.244.155  TLSv1      450 Client Hello
    76 33.238286   192.168.72.54   107.178.244.155  TLSv1      443 Change Cipher Spec, Encrypted Handshake Message, Application Data, Application Data
    87 41.388328   192.168.72.54   192.168.72.7     DNS         84 Standard query 0x461c A detectportal.firefox.com
    89 41.424102   192.168.72.54   192.168.72.7     DNS         84 Standard query 0x461c A detectportal.firefox.com
    91 41.436867   192.168.72.54   34.107.221.82    TCP         66 20954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    92 41.441927   192.168.72.54   192.168.72.7     DNS        102 Standard query 0xa9d0 A prod.detectportal.prod.cloudops.mozgcp.net
    94 41.447291   192.168.72.54   192.168.72.7     DNS        102 Standard query 0xc472 AAAA prod.detectportal.prod.cloudops.mozgcp.net
    96 41.457345   192.168.72.54   34.107.221.82    TCP         54 20954 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    97 41.458150   192.168.72.54   34.107.221.82    HTTP       355 GET /canonical.html HTTP/1.1
   101 41.525397   192.168.72.54   192.168.72.7     DNS         71 Standard query 0x2ef0 A example.org
   102 41.525613   192.168.72.54   34.107.221.82    TCP         54 20954 → 80 [ACK] Seq=302 Ack=303 Win=261888 Len=0
   103 41.535789   192.168.72.54   192.168.72.7     DNS         73 Standard query 0xd7a3 A ipv4only.arpa
   104 41.536982   192.168.72.54   192.168.72.7     DNS         74 Standard query 0xc368 A www.google.com
   105 41.537681   192.168.72.54   192.168.72.7     DNS         70 Standard query 0xdcd7 A google.com
   106 41.538154   192.168.72.54   192.168.72.7     DNS         86 Standard query 0x4cc8 A forcesafesearch.google.com
   107 41.538674   192.168.72.54   34.107.221.82    TCP         66 20955 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   108 41.538741   192.168.72.54   192.168.72.7     DNS         75 Standard query 0x62e9 A www.youtube.com
   110 41.539929   192.168.72.54   192.168.72.7     DNS         73 Standard query 0xdabb A m.youtube.com
   111 41.540235   192.168.72.54   192.168.72.7     DNS         83 Standard query 0xb33e A youtubei.googleapis.com
   115 41.542724   192.168.72.54   192.168.72.7     DNS         82 Standard query 0x6d90 A youtube.googleapis.com
   116 41.543363   192.168.72.54   192.168.72.7     DNS         84 Standard query 0x9fb9 A www.youtube-nocookie.com
   117 41.546561   192.168.72.54   192.168.72.7     DNS         80 Standard query 0xf9b3 A restrict.youtube.com
```

```
> Frame 107: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{70F8DA0F-EB4B-4E02-8979-8D27464305DC}, id 0
v Ethernet II, Src: 72:00:00:00:10:05 (72:00:00:00:10:05), Dst: Microsof_54:d0:5d (00:15:5d:54:d0:5d)
  > Destination: Microsof_54:d0:5d (00:15:5d:54:d0:5d)
  > Source: 72:00:00:00:10:05 (72:00:00:00:10:05)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.72.54, Dst: 34.107.221.82
> Transmission Control Protocol, Src Port: 20955, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 15 5d 54 d0 5d 72 00  00 00 10 05 08 00 45 00   ··]T·]r· ······E·
```

Packets: 2609 · Displayed: 1235 (47.3%) · Dropped: 0 (0.0%)

Step 24


4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.72.54 && tcp.port == 80

```
No.    Time       Source          Destination     Protocol  Length Info
    91 41.436867  192.168.72.54   34.107.221.82   TCP       66 20954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    96 41.457345  192.168.72.54   34.107.221.82   TCP       54 20954 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    97 41.458150  192.168.72.54   34.107.221.82   HTTP     355 GET /canonical.html HTTP/1.1
   102 41.525613  192.168.72.54   34.107.221.82   TCP       54 20954 → 80 [ACK] Seq=302 Ack=303 Win=261888 Len=0
   107 41.538674  192.168.72.54   34.107.221.82   TCP       66 20955 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   122 41.557062  192.168.72.54   34.107.221.82   TCP       54 20955 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   123 41.557279  192.168.72.54   34.107.221.82   HTTP     357 GET /success.txt?ipv4 HTTP/1.1
   143 41.629848  192.168.72.54   34.107.221.82   TCP       54 20955 → 80 [ACK] Seq=304 Ack=221 Win=261888 Len=0
   360 42.301512  192.168.72.54   23.62.152.72    TCP       66 20967 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   367 42.312254  192.168.72.54   65.8.178.227    TCP       66 20968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   373 42.321093  192.168.72.54   23.62.152.72    TCP       54 20967 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   375 42.323780  192.168.72.54   65.8.178.227    TCP       54 20968 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   376 42.324476  192.168.72.54   23.62.152.72    OCSP     477 Request
   377 42.324716  192.168.72.54   65.8.178.227    OCSP     487 Request
   393 42.386605  192.168.72.54   23.62.152.72    TCP       54 20967 → 80 [ACK] Seq=424 Ack=890 Win=261120 Len=0
   395 42.386628  192.168.72.54   65.8.178.227    TCP       54 20968 → 80 [ACK] Seq=434 Ack=1006 Win=261120 Len=0
   500 42.916699  192.168.72.54   72.21.91.29     TCP       66 20973 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   501 42.917554  192.168.72.54   72.21.91.29     TCP       66 20974 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   502 42.918512  192.168.72.54   72.21.91.29     TCP       66 20975 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   503 42.919421  192.168.72.54   72.21.91.29     TCP       66 20976 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   506 42.928936  192.168.72.54   72.21.91.29     TCP       54 20973 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   507 42.929342  192.168.72.54   72.21.91.29     OCSP     478 Request
   510 42.929867  192.168.72.54   72.21.91.29     TCP       54 20975 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   511 42.929871  192.168.72.54   72.21.91.29     TCP       54 20974 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   515 42.929921  192.168.72.54   72.21.91.29     TCP       54 20976 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   517 42.930265  192.168.72.54   72.21.91.29     OCSP     478 Request
   518 42.930357  192.168.72.54   72.21.91.29     OCSP     478 Request
   519 42.930434  192.168.72.54   72.21.91.29     OCSP     478 Request
   540 42.988425  192.168.72.54   72.21.91.29     TCP       54 20974 → 80 [ACK] Seq=425 Ack=800 Win=261376 Len=0
   541 42.988434  192.168.72.54   72.21.91.29     TCP       54 20973 → 80 [ACK] Seq=425 Ack=800 Win=261376 Len=0
   542 42.988453  192.168.72.54   72.21.91.29     TCP       54 20975 → 80 [ACK] Seq=425 Ack=800 Win=261376 Len=0
   543 42.988465  192.168.72.54   72.21.91.29     TCP       54 20976 → 80 [ACK] Seq=425 Ack=800 Win=261376 Len=0
   572 43.106790  192.168.72.54   23.62.152.72    OCSP     477 Request
   609 43.173981  192.168.72.54   23.62.152.72    TCP       54 20967 → 80 [ACK] Seq=847 Ack=1779 Win=262144 Len=0
   828 43.816068  192.168.72.54   23.62.152.72    OCSP     477 Request
```

```
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
0000  00 15 5d 54 d0 5d 72 00  00 00 10 05 08 00 45 00   ··]T·]r· ······E·
```

Interface id (frame.interface_id) | Packets: 2609 · Displayed: 93 (3.6%) · Dropped: 0 (0.0%) | Profile: Default

Project Questions

1. My IP address is 192.168.72.54
2. I captured 2609 packets.
3. With the filters there were only 93 packets, meaning that 2516 packets were removed.
4. The most common destination IP address was 72.21.91.29.

Thought Questions

1. Yes, you would be able to filter a person’s traffic if you know their IP address and the type of packet that you are looking for.
2. There are many fields to filter because there are many different protocols, each having their own specific metadata that could be filtered out.
3. Another protocol used to manage traffic across networks is UDP.
4. The endpoint 104.16.249.249 was sent/received 794 packets during the scan.