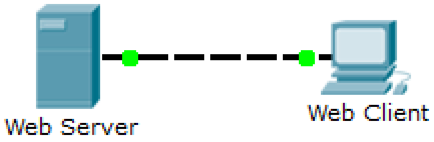
Sri Lanka Institute of Information Technology

Year 2 – Semester 1
IT2050 – Computer Networks
Lab sheet - TCP

Topology



Part 1: Examine HTTP Web Traffic

In Part 1 of this activity, you will use Packet Tracer (PT) Simulation mode to generate web traffic and examine HTTP.

➢ **Switch from Realtime to Simulation mode**

- Click the **Simulation** mode icon to switch from **Realtime** mode to **Simulation** mode.

- Select **HTTP** from the **Event List Filters**.

HTTP may already be the only visible event. Click **Edit Filters** to display the available visible events. Toggle the **Show All/None** check box and notice how the check boxes switch from unchecked to checked or checked to unchecked, depending on the current state.

Click the **Show All/None** check box until all boxes are cleared and then select **HTTP**. Click anywhere outside of the **Edit Filters** box to hide it. The Visible Events should now only display HTTP.

- **Generate web (HTTP) traffic**

- Click **Web Client** in the far-left pane.

- Click the **Desktop** tab and click the **Web Browser** icon to open it.

- In the URL field, enter **www.osi.local** and click **Go**.

  Because time in Simulation mode is event-driven, you must use the **Capture/Forward** button to display network events.

- Click **Capture/Forward** four times. There should be four events in the Event List. Look at the Web Client web browser page. Did anything change?

  ……………………………………………………………………………………………….

- **Explore the contents of the HTTP packet**

- Click the first colored square box under the **Event List** > **Info** column. It may be necessary to expand the **Simulation Panel** or use the scrollbar directly below the **Event List**.

  The **PDU Information at Device: Web Client** window displays. In this window, there are only two tabs (**OSI Model** and **Outbound PDU Details**) because this is the start of the transmission. As more events are examined, there will be three tabs displayed, adding a tab for **Inbound PDU Details**. When an event is the last event in the stream of traffic, only the **OSI Model** and **Inbound PDU Details** tabs are displayed.

- Ensure that the **OSI Model** tab is selected. Under the **Out Layers** column, ensure that the **Layer 7** box is highlighted.
  What is the text displayed next to the **Layer 7** label?

  ……………………………………………………………………………………………….
  What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes?
  ………………………………………………………………………………………………

- Click **Next Layer**. Layer 4 should be highlighted. What is the **Dst Port** value?

  ……………………………………………………………………………………………….

- Click **Next Layer**. Layer 3 should be highlighted. What is the **Dest. IP** value?

  ……………………………………………………………………………………………….

- Click **Next Layer**. What information is displayed at this layer?

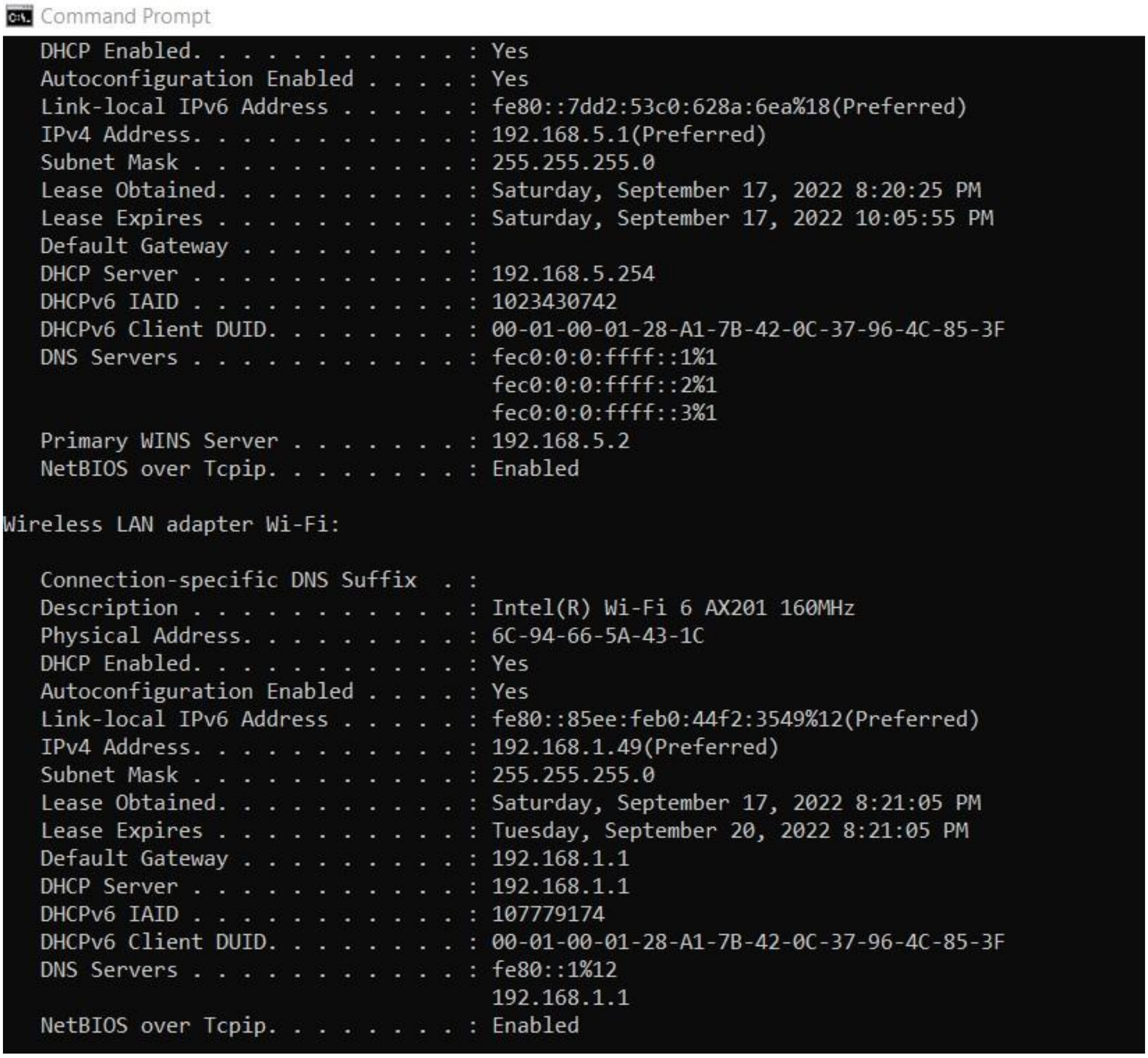
  ………………………………………………………………………………………………

Close all browser windows before beginning this lab activity.

Part 1: Prepare Wireshark to capture packets

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

1. Open a command window, type **ipconfig /all**, and then press Enter.



```
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7dd2:53c0:628a:6ea%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.5.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, September 17, 2022 8:20:25 PM
   Lease Expires . . . . . . . . . . : Saturday, September 17, 2022 10:05:55 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.5.254
   DHCPv6 IAID . . . . . . . . . . . : 1023430742
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-A1-7B-42-0C-37-96-4C-85-3F
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   Primary WINS Server . . . . . . . : 192.168.5.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 6C-94-66-5A-43-1C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::85ee:feb0:44f2:3549%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.49(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, September 17, 2022 8:21:05 PM
   Lease Expires . . . . . . . . . . : Tuesday, September 20, 2022 8:21:05 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 107779174
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-A1-7B-42-0C-37-96-4C-85-3F
   DNS Servers . . . . . . . . . . . : fe80::1%12
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2. Note your PC interface's IP address and MAC (physical)

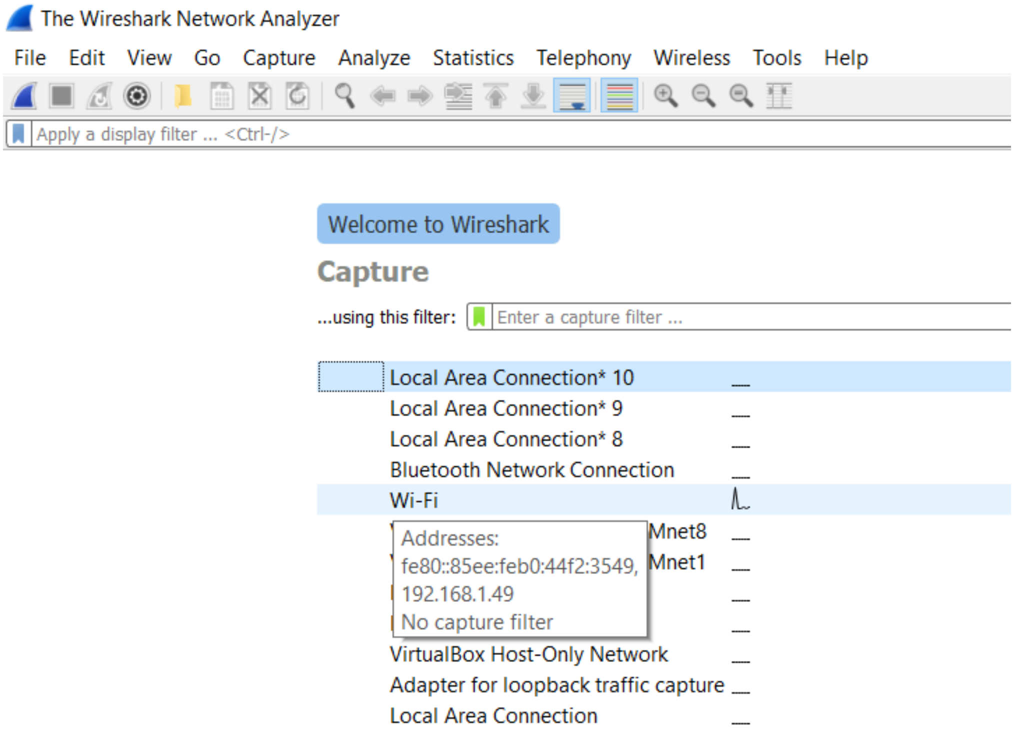
   address. IP address: ……………………………….

   Physical address: ……………………………

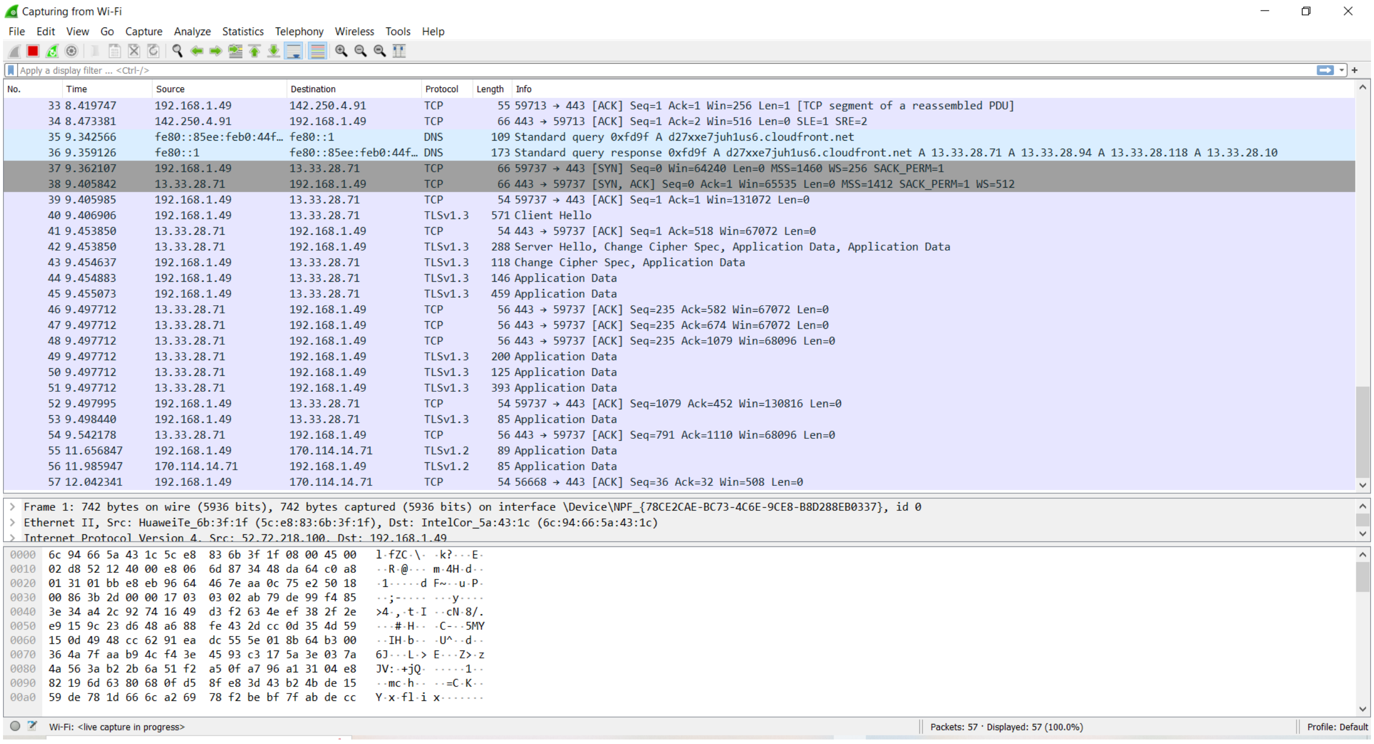
3. Start Wireshark and select the interface connected to your LAN (Your instructor will show you how to do this.).

Part 2: Capture and locate packets

1. Start the data capture.
2. Open a browser and navigate to www.google.com. Minimize the browser and return to Wireshark. Stop the data capture.
3. The capture window is now active. Locate the **Source**, **Destination**, and **Protocol** columns.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Mnet8
Mnet1
Addresses:
fe80::85ee:feb0:44f2:3549,
192.168.1.49
No capture filter
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Local Area Connection


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source                 Destination            Protocol  Length Info
   33 8.419747    192.168.1.49           142.250.4.91           TCP         55 59713 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
   34 8.473381    142.250.4.91           192.168.1.49           TCP         66 443 → 59713 [ACK] Seq=1 Ack=2 Win=516 Len=0 SLE=1 SRE=2
   35 9.342566    fe80::85ee:feb0:44f…   fe80::1                DNS        109 Standard query 0xfd9f A d27xxe7juh1us6.cloudfront.net
   36 9.359126    fe80::1                fe80::85ee:feb0:44f…   DNS        173 Standard query response 0xfd9f A d27xxe7juh1us6.cloudfront.net A 13.33.28.71 A 13.33.28.94 A 13.33.28.118 A 13.33.28.10
   37 9.362107    192.168.1.49           13.33.28.71            TCP         66 59737 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   38 9.405842    13.33.28.71            192.168.1.49           TCP         66 443 → 59737 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 WS=512
   39 9.405985    192.168.1.49           13.33.28.71            TCP         54 59737 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
   40 9.406906    192.168.1.49           13.33.28.71            TLSv1.3    571 Client Hello
   41 9.453850    13.33.28.71            192.168.1.49           TCP         54 443 → 59737 [ACK] Seq=1 Ack=518 Win=67072 Len=0
   42 9.453850    13.33.28.71            192.168.1.49           TLSv1.3    288 Server Hello, Change Cipher Spec, Application Data, Application Data
   43 9.454637    192.168.1.49           13.33.28.71            TLSv1.3    118 Change Cipher Spec, Application Data
   44 9.454883    192.168.1.49           13.33.28.71            TLSv1.3    146 Application Data
   45 9.455073    192.168.1.49           13.33.28.71            TLSv1.3    459 Application Data
   46 9.497712    13.33.28.71            192.168.1.49           TCP         56 443 → 59737 [ACK] Seq=235 Ack=582 Win=67072 Len=0
   47 9.497712    13.33.28.71            192.168.1.49           TCP         56 443 → 59737 [ACK] Seq=235 Ack=674 Win=67072 Len=0
   48 9.497712    13.33.28.71            192.168.1.49           TCP         56 443 → 59737 [ACK] Seq=235 Ack=1079 Win=68096 Len=0
   49 9.497712    13.33.28.71            192.168.1.49           TLSv1.3    200 Application Data
   50 9.497712    13.33.28.71            192.168.1.49           TLSv1.3    125 Application Data
   51 9.497712    13.33.28.71            192.168.1.49           TLSv1.3    393 Application Data
   52 9.497995    192.168.1.49           13.33.28.71            TCP         54 59737 → 443 [ACK] Seq=1079 Ack=452 Win=130816 Len=0
   53 9.498440    192.168.1.49           13.33.28.71            TLSv1.3     85 Application Data
   54 9.542178    13.33.28.71            192.168.1.49           TCP         56 443 → 59737 [ACK] Seq=791 Ack=1110 Win=68096 Len=0
   55 11.656847   192.168.1.49           170.114.14.71          TLSv1.2     89 Application Data
   56 11.985947   170.114.14.71          192.168.1.49           TLSv1.2     85 Application Data
   57 12.042341   192.168.1.49           170.114.14.71          TCP         54 56668 → 443 [ACK] Seq=36 Ack=32 Win=508 Len=0
```

```
> Frame 1: 742 bytes on wire (5936 bits), 742 bytes captured (5936 bits) on interface \Device\NPF_{78CE2CAE-BC73-4C6E-9CE8-B8D288EB0337}, id 0
> Ethernet II, Src: HuaweiTe_6b:3f:1f (5c:e8:83:6b:3f:1f), Dst: IntelCor_5a:43:1c (6c:94:66:5a:43:1c)
> Internet Protocol Version 4, Src: 52.72.218.100, Dst: 192.168.1.49
```

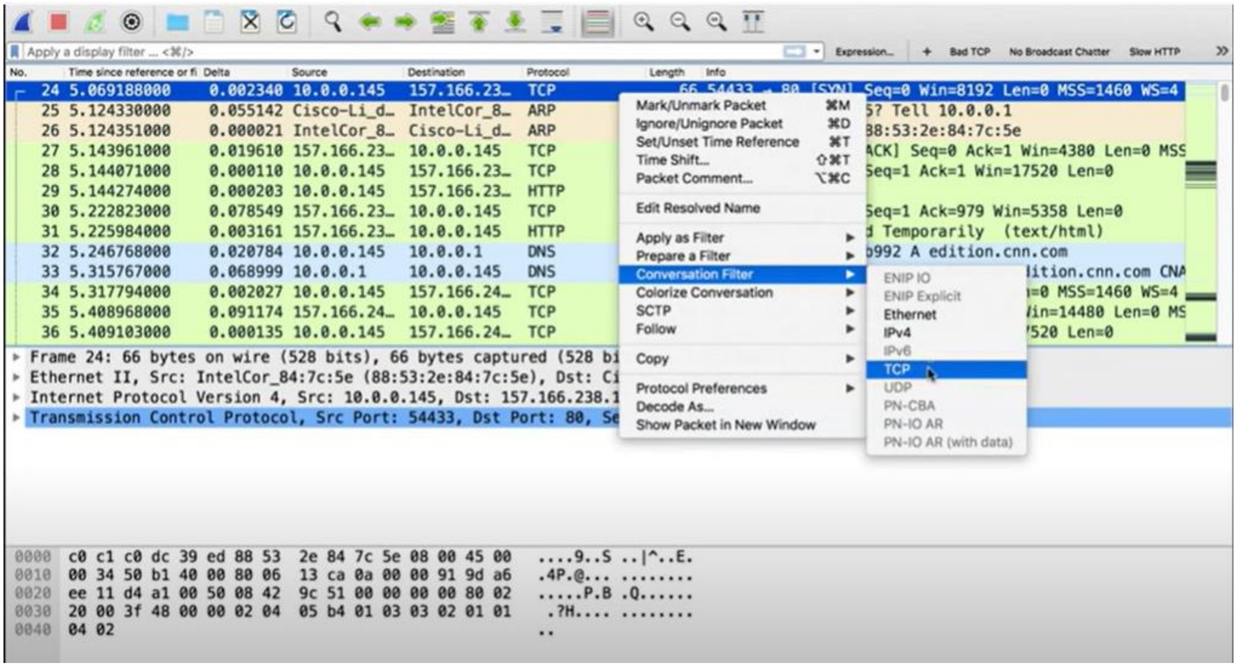
```
0000  6c 94 66 5a 43 1c 5c e8  83 6b 3f 1f 08 00 45 00   l·fZC·\· ·k?···E·
0010  02 d8 52 12 40 00 e8 06  6d 87 34 48 da 64 c0 a8   ··R·@··· m·4H·d··
0020  01 31 01 bb e8 eb 96 64  46 7e aa 0c 75 e2 50 18   ·1·····d F~··u·P·
0030  00 86 3b 2d 00 00 17 03  03 02 ab 79 de 99 f4 85   ··;-···· ···y····
0040  3e 34 a4 2c 92 74 16 49  d3 f2 63 4e ef 38 2f 2e   >4·,·t·I ··cN·8/.
0050  e9 15 9c 23 d6 48 a6 88  fe 43 2d cc 0d 35 4d 59   ···#·H·· ·C-··5MY
0060  15 0d 49 48 cc 62 91 ea  dc 55 5e 01 8b 64 b3 00   ··IH·b·· ·U^··d··
0070  36 4a 7f aa b9 4c f4 3e  45 93 c3 17 5a 3e 03 7a   6J···L·> E···Z>·z
0080  4a 56 3a b2 2b 6a 51 f2  a5 0f a7 96 a1 31 04 e8   JV:·+jQ· ·····1··
0090  82 19 6d 63 80 68 0f d5  8f e8 3d 43 b2 4b de 15   ··mc·h·· ··=C·K··
00a0  59 de 78 1d 66 6c a2 69  78 f2 be bf 7f ab de cc   Y·x·fl·i x·······
```

Wi-Fi: <live capture in progress>   Packets: 57 · Displayed: 57 (100.0%)   Profile: Default

4. Find the appropriate packet for the start of your TCP three-way handshake. In the example, frame 14 is the start of the TCP three-way handshake. What is the destination IP address of this packet?

   ………………………………………….

   If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter tool to filter TCP.

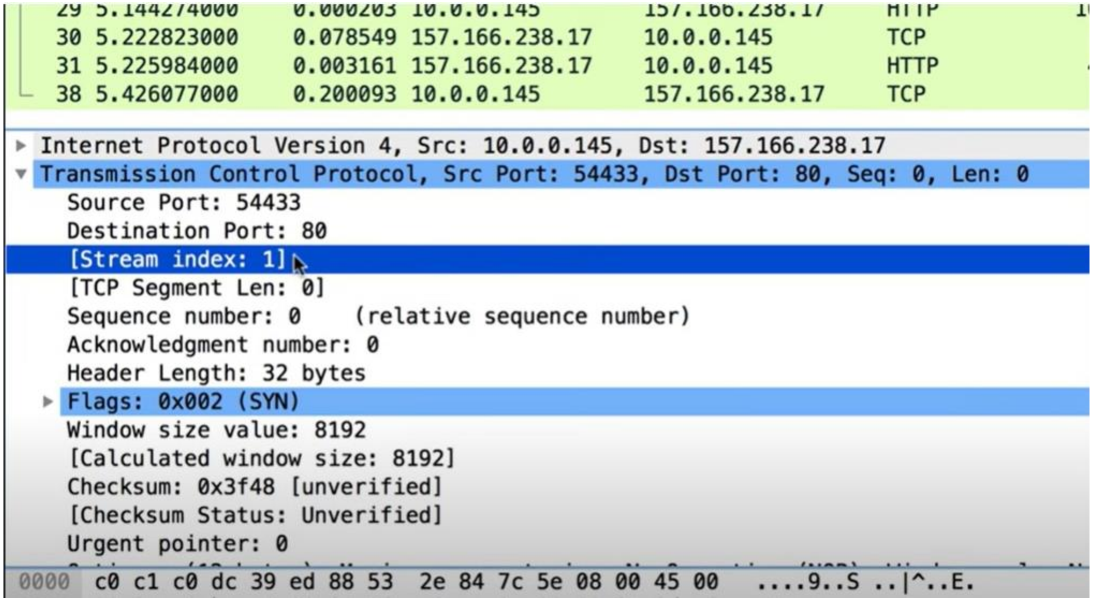


```
No.  Time since reference or fi Delta    Source        Destination   Protocol   Length  Info
 24 5.069188000    0.002340 10.0.0.145    157.166.23…   TCP          66 54433 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
 25 5.124330000    0.055142 Cisco-Li_d…   IntelCor_8…   ARP          5? Tell 10.0.0.1
 26 5.124351000    0.000021 IntelCor_8…   Cisco-Li_d…   ARP          88:53:2e:84:7c:5e
 27 5.143961000    0.019610 157.166.23…   10.0.0.145    TCP          ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS
 28 5.144071000    0.000110 10.0.0.145    157.166.23…   TCP          Seq=1 Ack=1 Win=17520 Len=0
 29 5.144274000    0.000203 10.0.0.145    157.166.23…   HTTP
 30 5.222823000    0.078549 157.166.23…   10.0.0.145    TCP          Seq=1 Ack=979 Win=5358 Len=0
 31 5.225984000    0.003161 157.166.23…   10.0.0.145    HTTP         d Temporarily  (text/html)
 32 5.246768000    0.020784 10.0.0.145    10.0.0.1      DNS          b992 A edition.cnn.com
 33 5.315767000    0.068999 10.0.0.1      10.0.0.145    DNS          dition.cnn.com CNA
 34 5.317794000    0.002027 10.0.0.145    157.166.24…   TCP          n=0 MSS=1460 WS=4
 35 5.408968000    0.091174 157.166.24…   10.0.0.145    TCP          Win=14480 Len=0 MS
 36 5.409103000    0.000135 10.0.0.145    157.166.24…   TCP          7520 Len=0
▸ Frame 24: 66 bytes on wire (528 bits), 66 bytes captured (528 bi
▸ Ethernet II, Src: IntelCor_84:7c:5e (88:53:2e:84:7c:5e), Dst: Ci
▸ Internet Protocol Version 4, Src: 10.0.0.145, Dst: 157.166.238.1
▸ Transmission Control Protocol, Src Port: 54433, Dst Port: 80, Se

0000  c0 c1 c0 dc 39 ed 88 53  2e 84 7c 5e 08 00 45 00   ....9..S ..|^..E.
0010  00 34 50 b1 40 00 80 06  13 ca 0a 00 00 91 9d a6   .4P.@... ........
0020  ee 11 d4 a1 00 50 08 42  9c 51 00 00 00 00 80 02   .....P.B .Q......
0030  20 00 3f 48 00 00 02 04  05 b4 01 03 03 02 01 01    .?H.... ........
0040  04 02                                              ..
```

Part 3: Examine packets

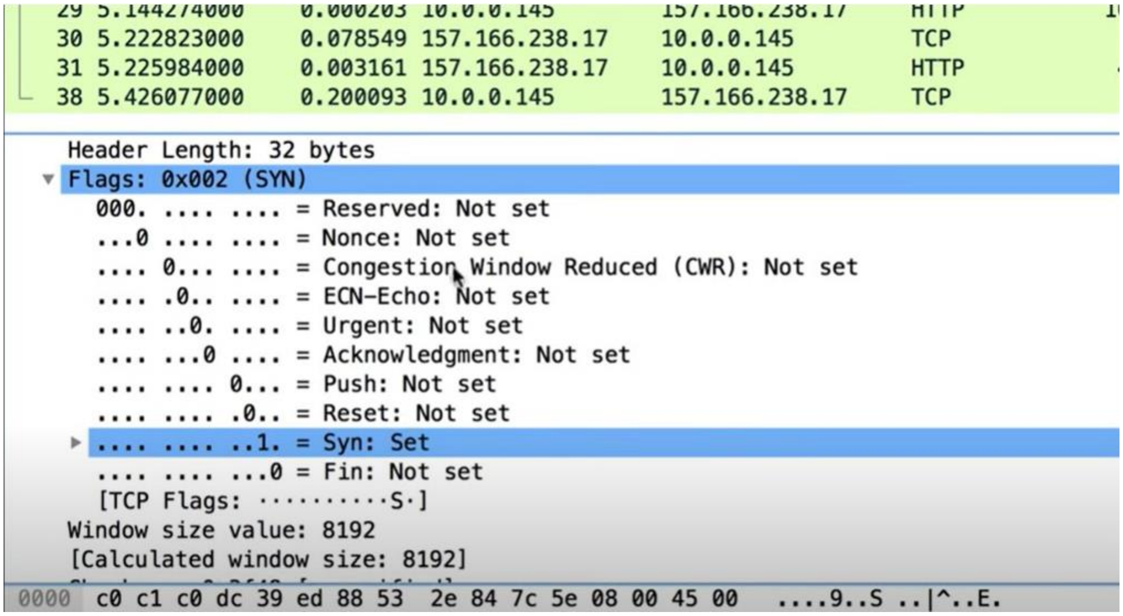
1. In the packet list pane (top section of the main window), select the first packet of TCP three-way handshake. This highlights the line and displays the decoded information from that packet in the two lower panes. Examine the TCP information in the packet details pane (middle section of the main window).
2. Expand the **Transmission Control Protocol** line in the packet details pane to expand the view of the TCP information.



```
 29 5.144274000    0.000203 10.0.0.145       157.166.238.17     HTTP
 30 5.222823000    0.078549 157.166.238.17   10.0.0.145         TCP
 31 5.225984000    0.003161 157.166.238.17   10.0.0.145         HTTP
 38 5.426077000    0.200093 10.0.0.145       157.166.238.17     TCP

▶ Internet Protocol Version 4, Src: 10.0.0.145, Dst: 157.166.238.17
▼ Transmission Control Protocol, Src Port: 54433, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 54433
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  ▶ Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x3f48 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
0000  c0 c1 c0 dc 39 ed 88 53  2e 84 7c 5e 08 00 45 00   ....9..S ..|^..E.
```

3. Expand **Flags** line. Look at the source and destination ports and the flags that are set.



```
 29 5.144274000    0.000203 10.0.0.145       157.166.238.17     HTTP
 30 5.222823000    0.078549 157.166.238.17   10.0.0.145         TCP
 31 5.225984000    0.003161 157.166.238.17   10.0.0.145         HTTP
 38 5.426077000    0.200093 10.0.0.145       157.166.238.17     TCP

    Header Length: 32 bytes
  ▼ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▶ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window size value: 8192
    [Calculated window size: 8192]
0000  c0 c1 c0 dc 39 ed 88 53  2e 84 7c 5e 08 00 45 00   ....9..S ..|^..E.
```

State the following:

TCP source port number? ………………………………………..

How would you classify the source port (dynamic/registered/well-known)?

………………………..

What is the TCP destination port number? ………………………………..

How would you classify the destination port (dynamic/registered/well-known)? …………………………..

Which flag (or flags) is set?

……………………………………………….

What is the relative sequence number set to?

………………………..

4. Locate the next packet in the three-way handshake. This is line 15 in the above figure.
5. Write down the following:

What is the value of the source on ports?

………………………………………………

Which flags are set?

…………………………………………………………..

What are the relative sequence and acknowledgement numbers set to?
....