Week One: Assignment 1: Examine TCP/IP and OSI Models in Action

CLOUD AND NETWORK SECURITY S2-2025

Cynthia W. Kamau

CS-CNS09-25020

Contents

Abstract 3

Part 1: Examine HTTP Web Traffic 4

Step 1: Switch from Real-time to Simulation mode 4

Step 2: Generate web (HTTP) traffic 5

Part 2: Display Elements of the TCP/IP Protocol Suite 14

Step 1: View Additional Events 14

Challenge Questions 19

Conclusion 20

Abstract

This simulation-based activity is designed to provide foundational knowledge of network communication by focusing on two main objectives: examining HTTP web traffic and displaying elements of the TCP/IP protocol suite. Utilizing Packet Tracer's simulation mode, the activity demonstrates how data is transmitted across a network and mapped to the layers of the TCP/IP and OSI models. As data moves through the network, it is segmented into protocol data units (PDUs), each associated with a specific layer, ensuring accurate reassembly at the destination. The simulation guides users through the process of requesting a web page via a client PC browser, allowing observation of the encapsulation and decapsulation processes at each protocol layer. This activity supports a clearer understanding of layered network architectures and the fundamental operations of internet communication protocols.

Keywords: *TCP/IP protocol suite, OSI model, HTTP traffic, Packet Tracer, protocol data unit (PDU), network simulation, web communication, network layers, encapsulation, decapsulation*

Part 1: Examine HTTP Web Traffic

Step 1: Switch from Real-time to Simulation mode

I clicked the Simulation mode icon to switch from **Realtime** mode to **Simulation** mode.

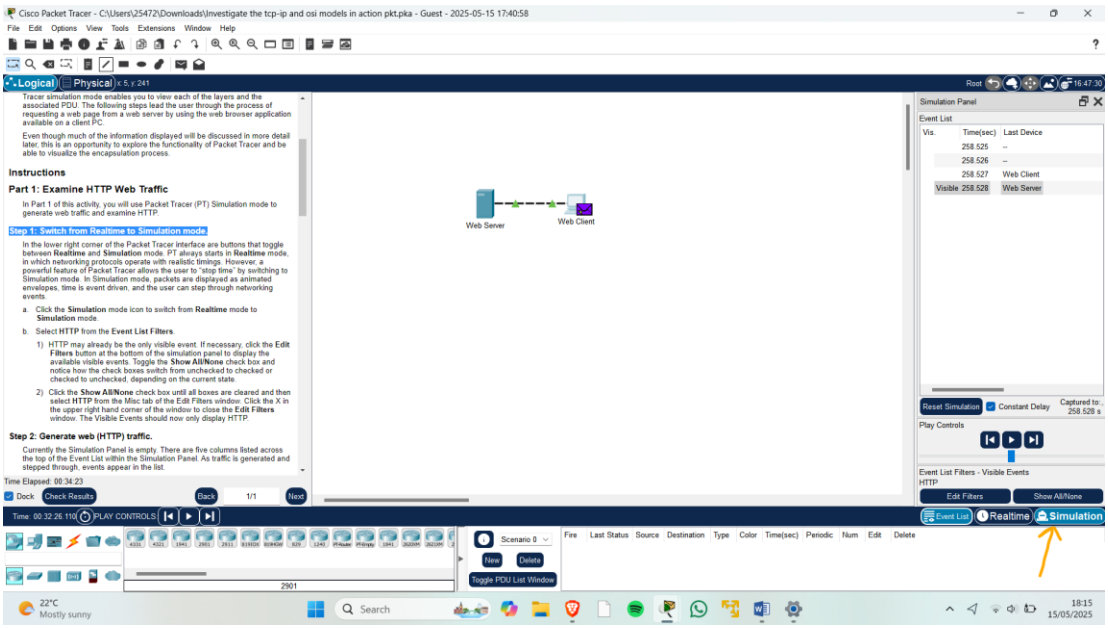

Figure 1: Evidence of clicking the simulation button

Then selected **HTTP** from the **Event List Filters.**

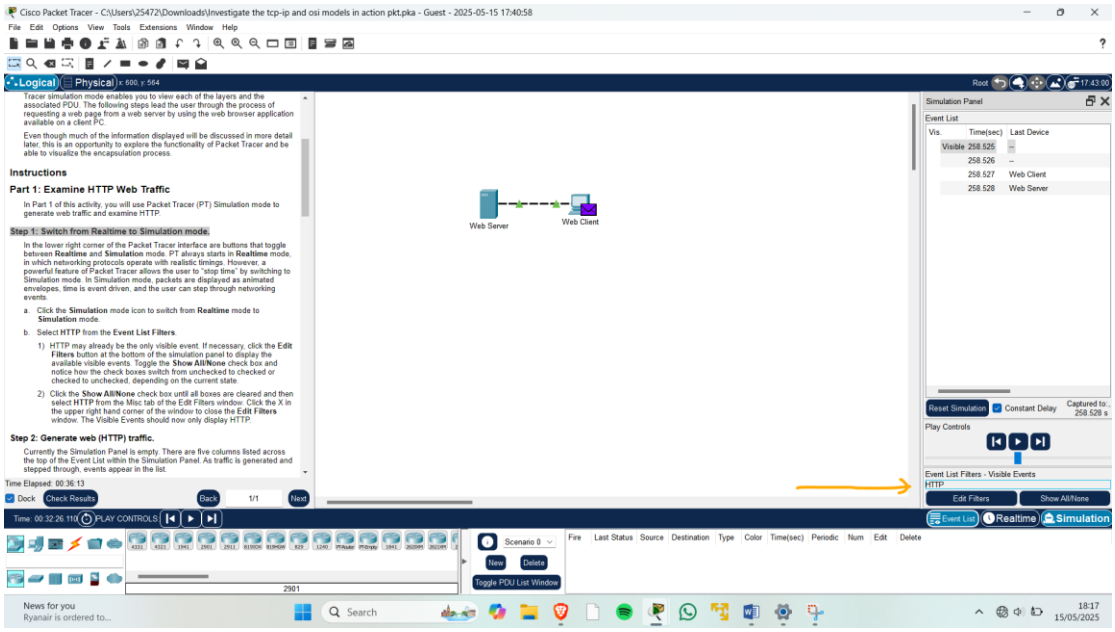

Figure 2: Evidence of clicking the HTTP from the Event List Filters

Step 2: Generate web (HTTP) traffic

I clicked the **Web Client**, then clicked the **Desktop tab** and clicked the **Web Browser** icon to open it. I then entered the URL www.osi.local on the URL field.

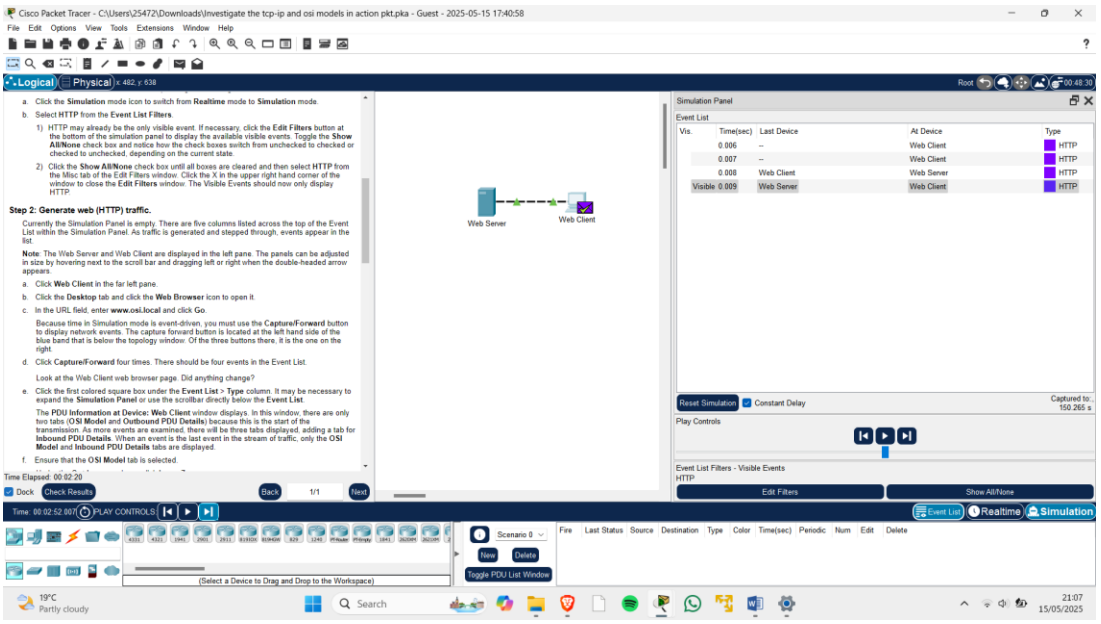

Figure 3: Evidence of Web Browser requested initiated

I clicked **Capture/Forward** four times and the Web Client browser page changed.

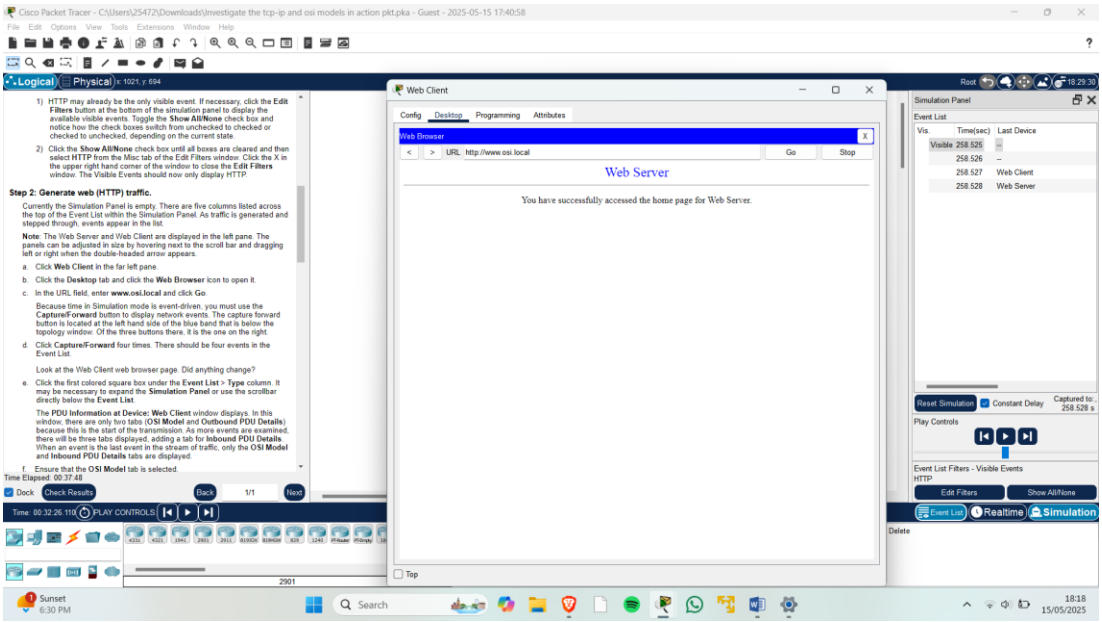

Figure 4: Evidence of changed Web Client browser page

I clicked the first colored square box under **Event List>Type column** and the **PDU Information at Device: Web Client window** popped up. *In this window only two tabs (OSI Model and Outbound PDU Details) because this is the start of the transmission.*

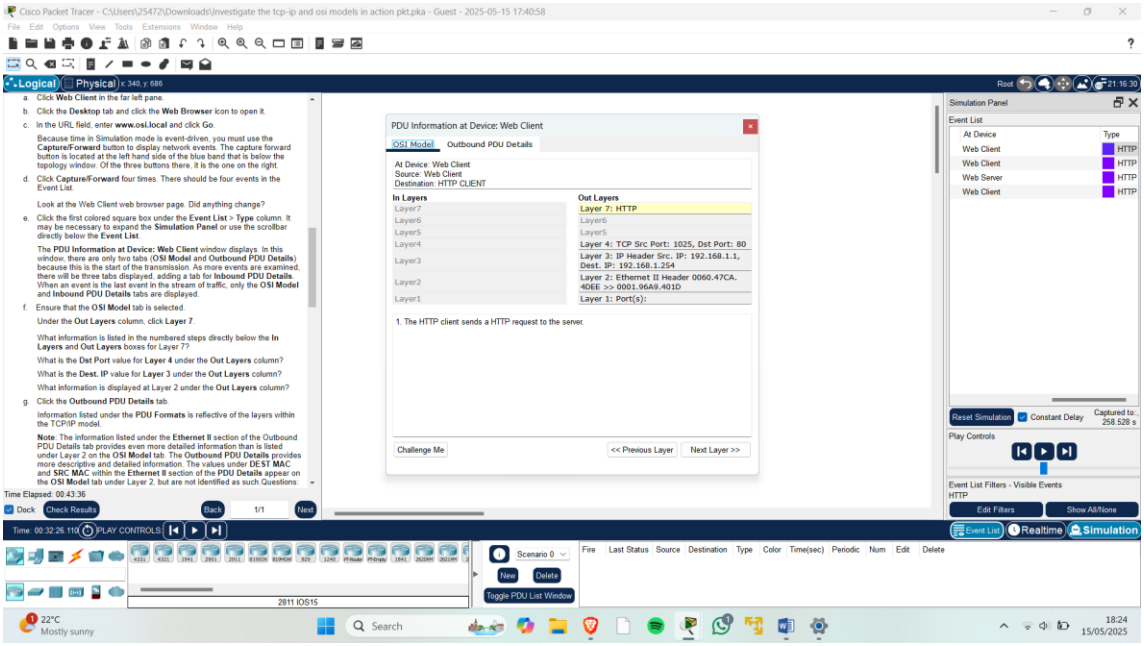

Figure 5: Evidence of the two tabs in the window

What information is listed in the numbered steps directly below the In Layers and Out Layers boxes for Layer 7?	**The HTTP client sends a HTTP request to the server**
What is the Dst Port value for Layer 4 under the Out Layers column?	**Out Layers: Layer 4: Dst Port: 80**
What is the Dest.IP value for Layer 3 under the Out Layers column?	**Out Layers: Layer 3: Dest Ip: 192.168.1.254**
What information is displayed at Layer 2 under the Out Layers column?	**Out Layers: Layer 2: Ethernet II Header 00600.47CA.4DEE>>0001.96A9.401D**

Table 1: Answers to the questions asked

I clicked the **Outbound PDU** Details tab. Information listed under the PDU Formats is reflective of the layers within TCP/IP model.

Note: The information listed under the Ethernet II section of the Outbound PDU Details tab provides even more detailed information than is listed under Layer 2 on the OSI Model tab. The Outbound PDU Details provides more descriptive and detailed information. The values under DEST MAX and SRC MAC within the Ethernet II section of the PDU Details appear on the OSI Model tab under Layer 2, but are not identified as such

Questions

1. What is the common information listed under the IP section of PDU Details, as compared to the information listed under the OSI Model tab and with which layer is it associated?

   SRC IP: 192.168.1.1 and DST IP: 192.168.1.254, these are similar to Out Layers of Layer 3:

   IP Header Src Ip: 192.168.1.1, Dest Ip: 192.168.1.254

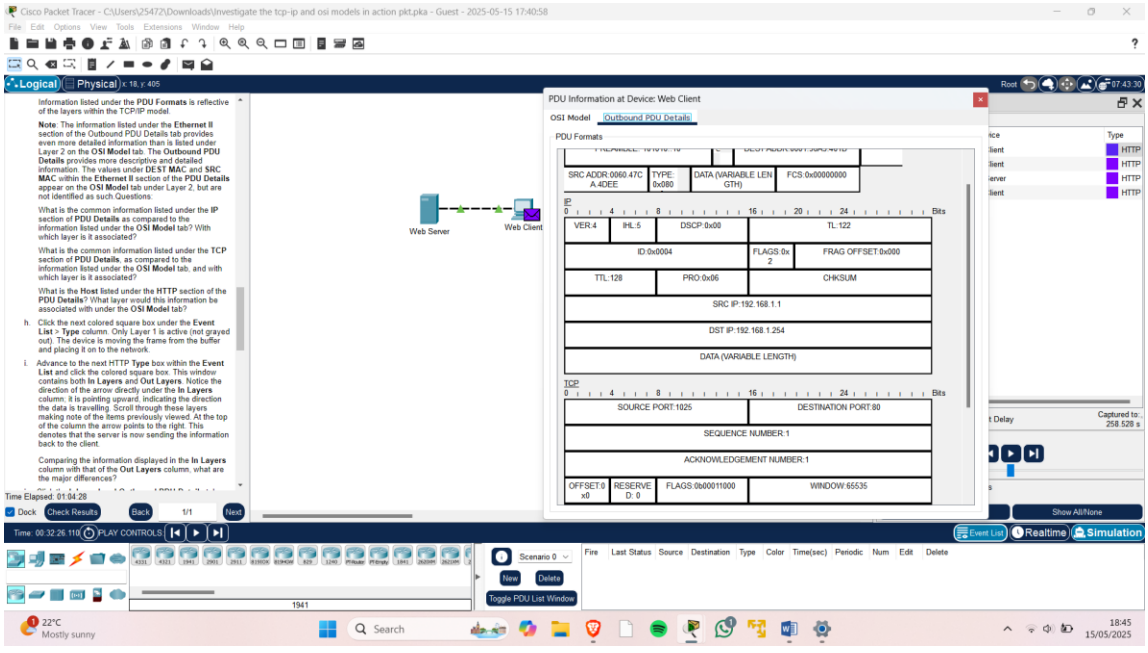

Figure 6: Evidence of the IP section of the Outbound PDU Details tab

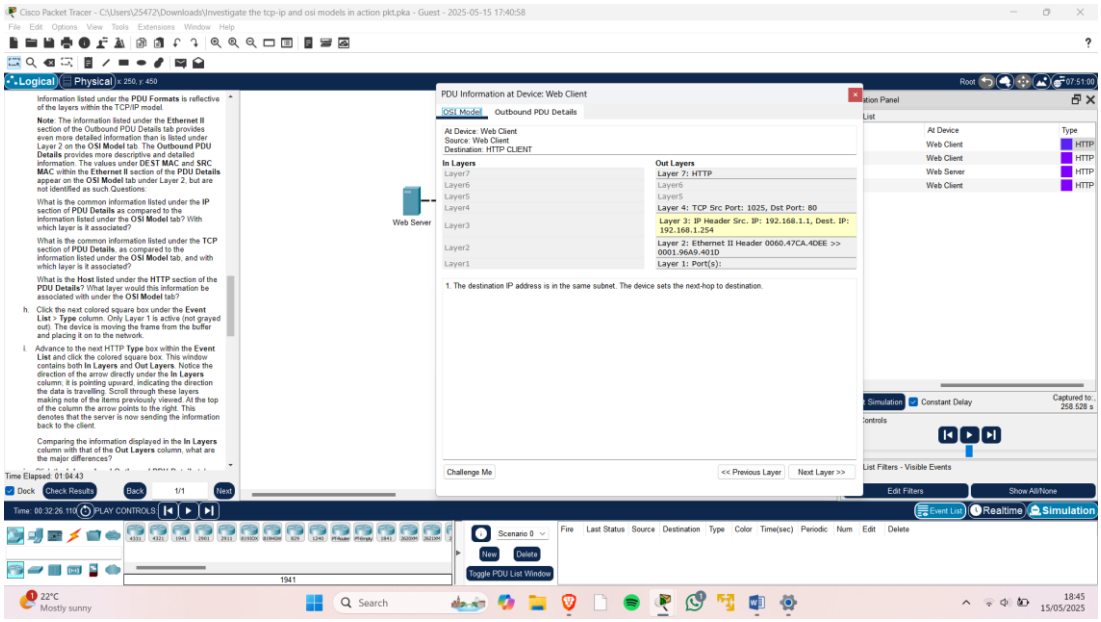

Figure 6: Evidence of the IP section of the OSI Model tab

2. What is the common information listed under the TCP section of PDU Details, as compared to the information listed under the OSI Model tab and with which layer is it associated?

SOURCE PORT: 1025 and DESTINATION PORT: 80, these are similar to Out Layers of Layer 4: TCP Src Port: 1025, Dst Port: 80

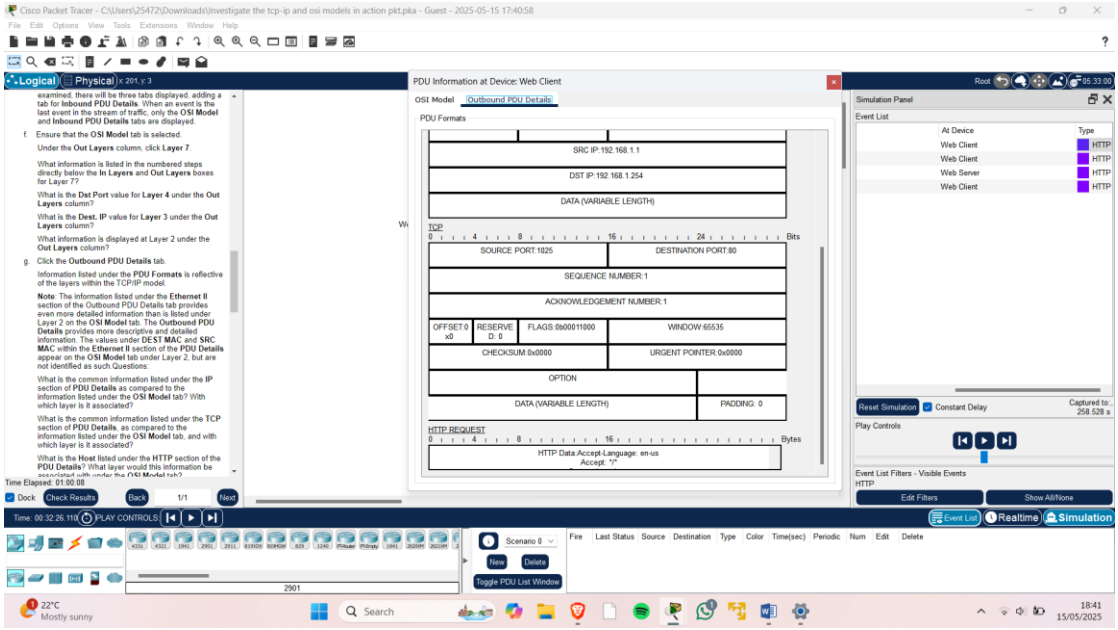

Figure 7: evidence of the TCP section of the Outbound PDU Details tab

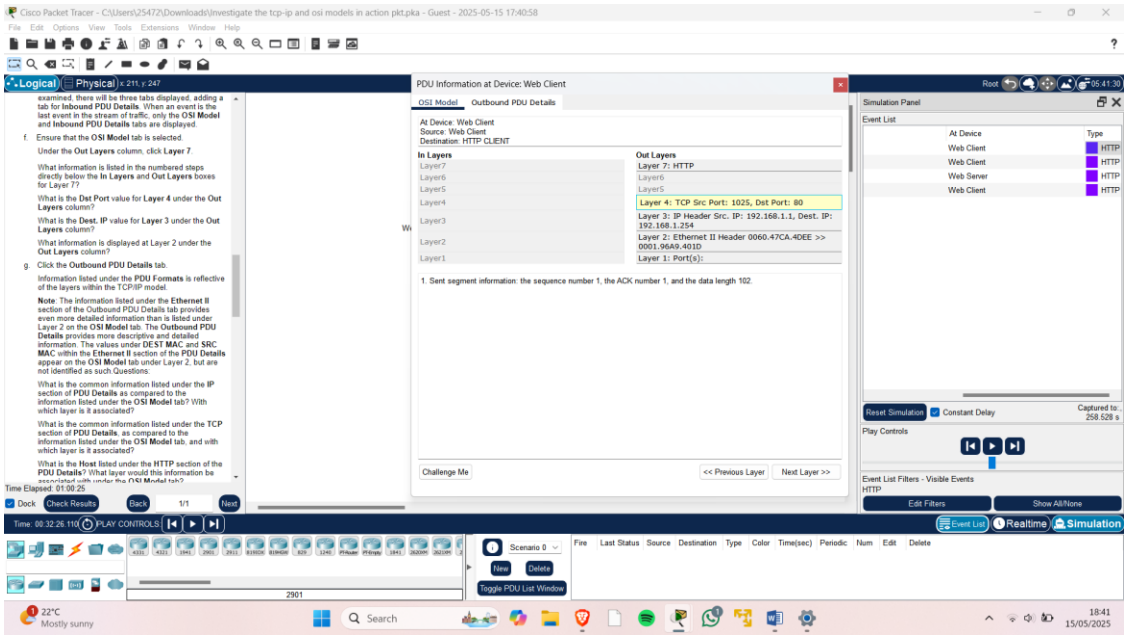

Figure 8: evidence of the TCP section of the OSI Model tab

3. What is the Host listed under the HTTP section of the PDU Details?

   The Host: www.osi.local . What layer would this information be associated with under the OSI Model tab? **Layer 7**

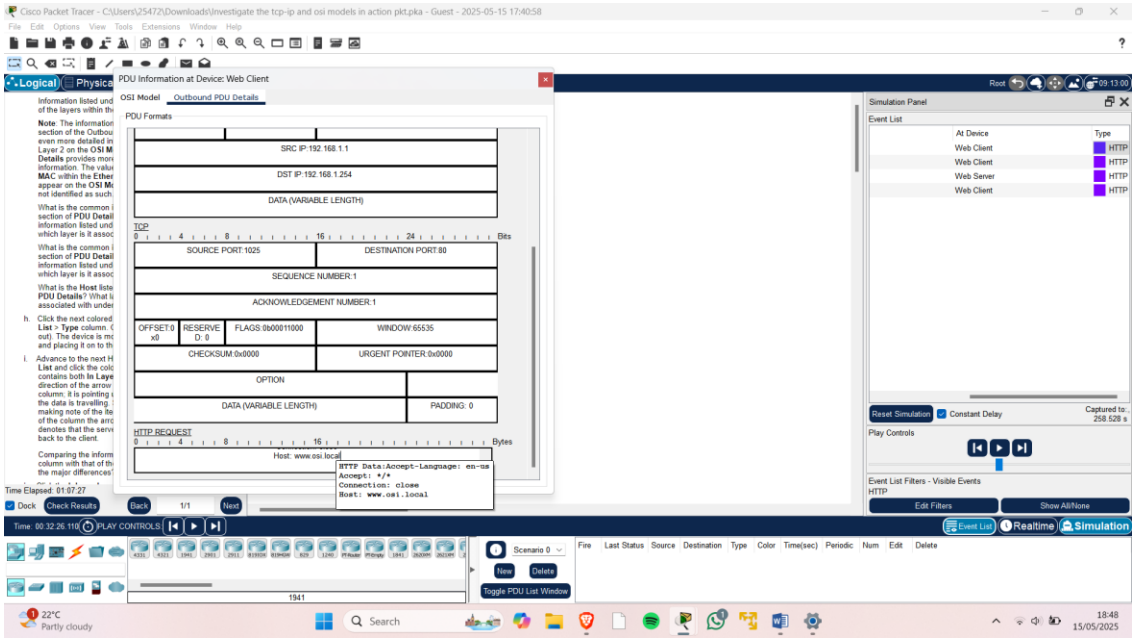

Figure 9: Evidence of host name in the Outbound PDU Details tab

I clicked the **next colored square box** under the **Event List > Type column**. I observed that Only Layer 1 is active (not grayed out). The device is moving the frame from the buffer and placing it on the network.

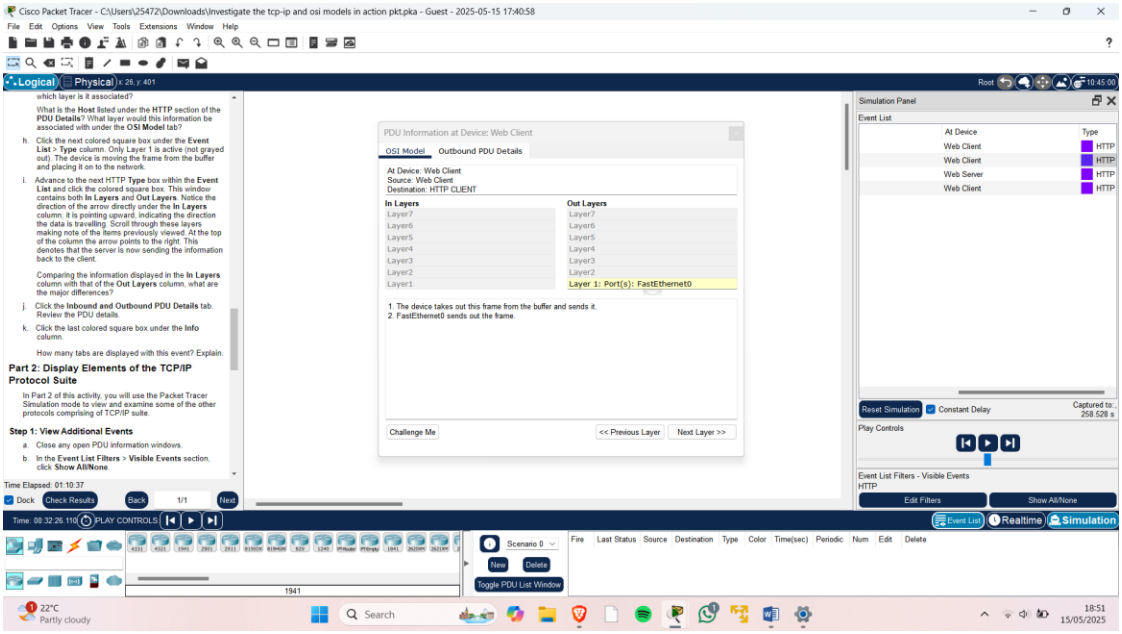

Figure 10: Evidence of the active Layer 1

Advancing to the **next HTTP Type** box within the **Event List** and clicking the colored square box. The PDU Information at Device: Web Server window contains both In Layers and Out Layers.

Note: Notice the direction of the arrow directly under the In Layers column; it is pointing upward, indicating the direction the data is travelling. Scroll through these layers making note of the items previously viewed. At the top of the column the arrow points to the right. This denotes that the server is now sending the information back to the client.

Question: Comparing the information displayed in the In Layers column with that of the Out Layers column, what are the major differences?

1. **In layer 4, The In Layers have TCP Src Port as 1025 and Dst Port as 80 whereas The Out Layers have the TCP Src Port as 80 and the Dst Port as 1025**

2. **In Layer 3, The In Layers have the IP Header Src. IP as 192.168.1.1 and the Dest. Ip as 192.168.1.254 whereas The Out Layers have the IP Header Src. IP as 192.168.1.254 and the Des. IP as 192.168.1.1**
3. **In Layer 2 the In Layers have the Ethernet II Header as 0060.47CA.4DEE>>0001.96A9.401D whereas the Out Layers have the Ethernet II Header as 0001.96A9.401D>>0060.47CA.4DEE**

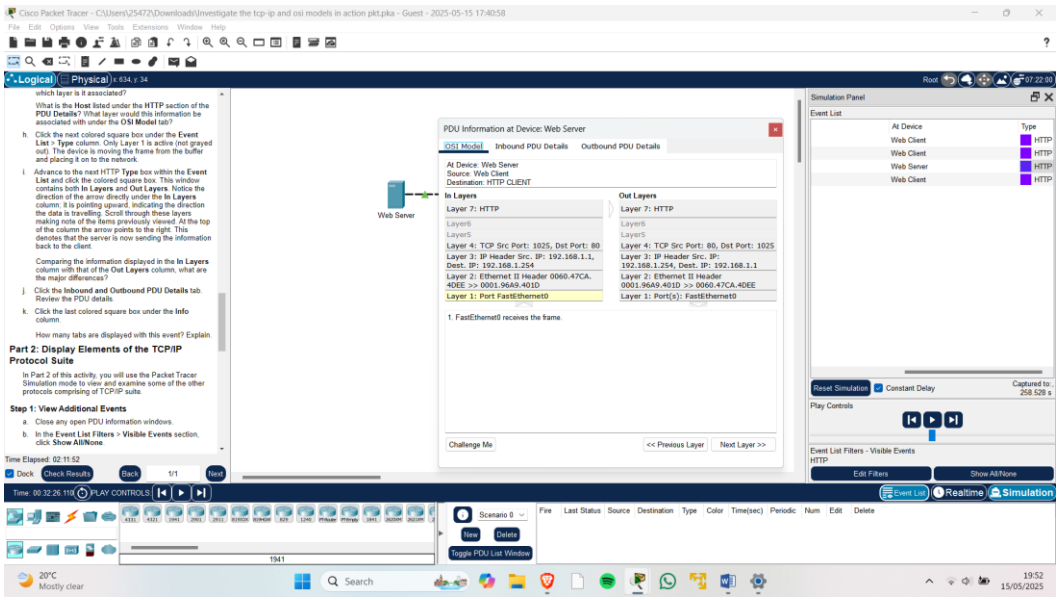

Figure 11: Evidence of the answers provided above

I reviewed the Inbound and Outbound PDU Details and observed that the HTTP Request in the Inbound details tab was indicating a closed connection with the host – www.osi.local whereas the HTTP Answer in the Outbound details tab gave more information on the Server: PT-Server/5.2 and the content type which was text/html.

Hypothesis: *The closed connection in the Inbound PDU indicates the client finished sending the request, while the Outbound PDU shows the server's HTTP response with header details.*

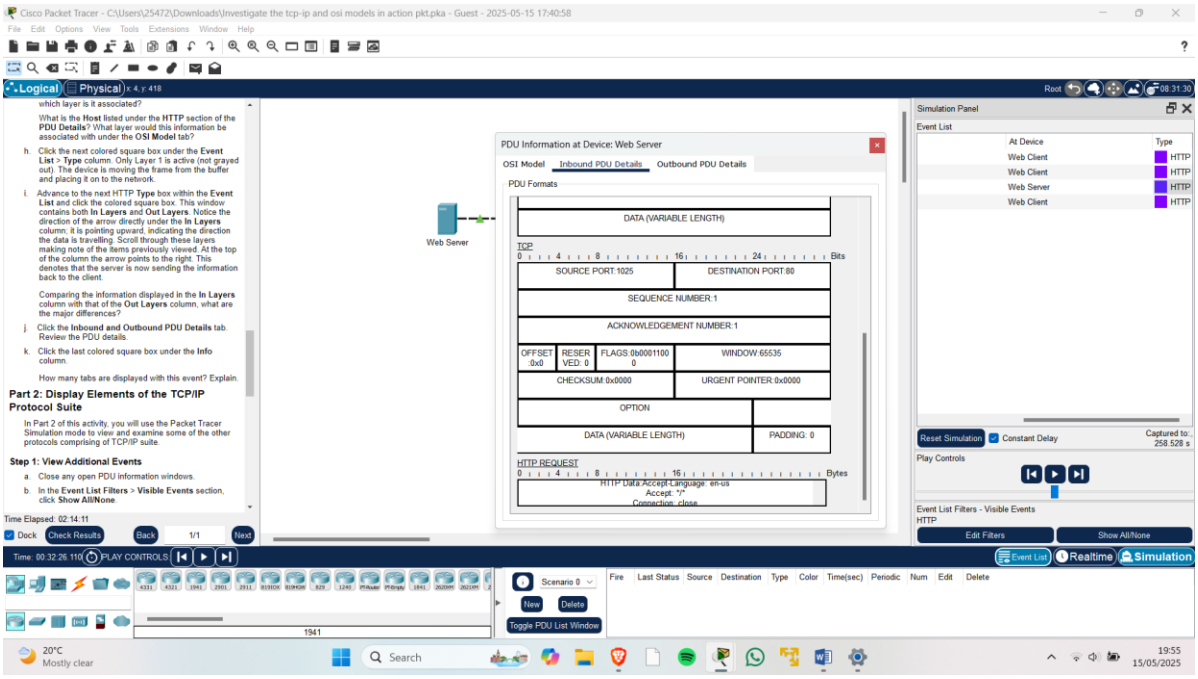

Figure 12: Evidence of inbound PDU details tab- HTTP request

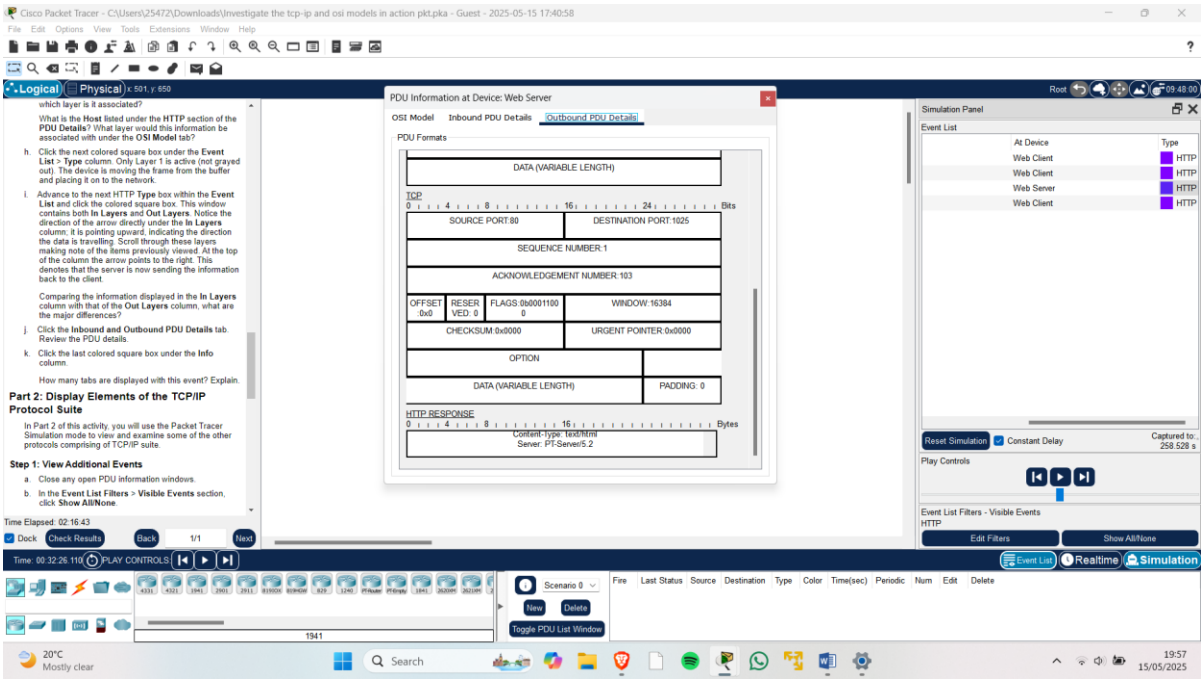

Figure 13: Evidence of outbound PDU details tab – HTTP response

I clicked the **last colored square** box under the Indo column and observed that **there was only information from the In Layers column.**

Question: How many tabs are displayed with this event? Explain. **The tabs are two namely the OSI Model and the Inbound PDU Details, because the Web Server replied the Web Client and The Web Client received the information as we have In Layers only.**

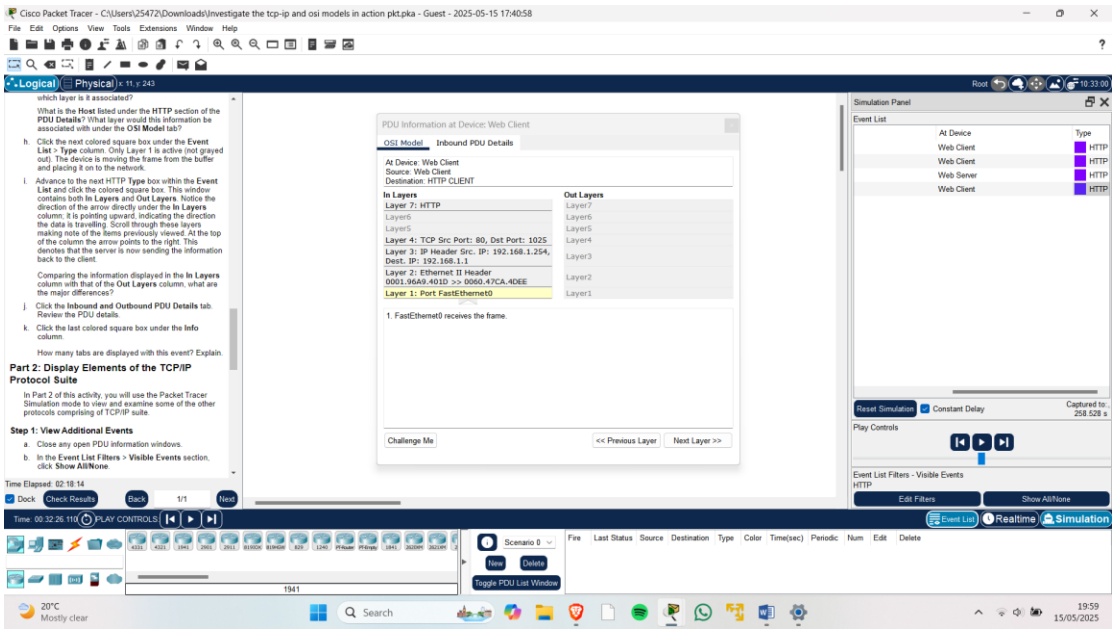

Figure 14: Evidence of the two tabs

Part 2: Display Elements of the TCP/IP Protocol Suite

Step 1: View Additional Events

I clicked the **Event List Filters>Visible Events section** and selected **Show All/None.**

Question: What additional Event Types are displayed? **DNS, ARP, TCP**

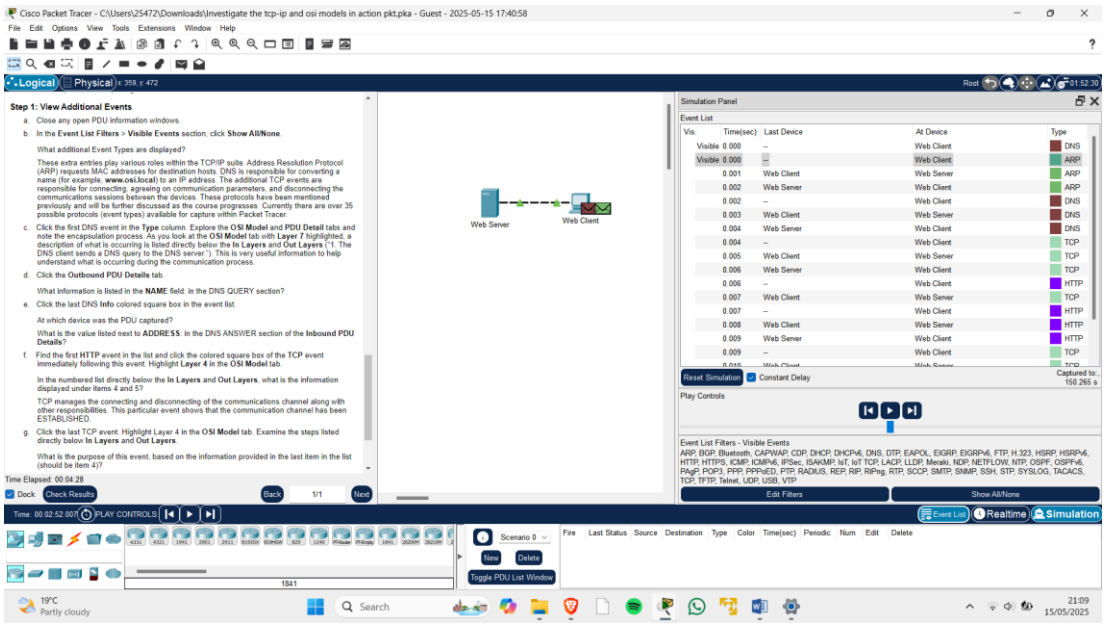

Figure 15: Evidence of the other additional Event Types

Note: These extra entries play various roles within the TCP/IP suite. Address Resolution Protocol (ARP) requests MAC addresses for destination hosts. DNS is responsible for converting a name (for example www.osi.local) to an IP address. The additional TCP events are responsible for connecting, agreeing on communication parameters, and disconnecting the communications sessions between the devices.

I clicked the **first DNS event** in the Type Column. I observed the **encapsulation note** – *The DNS client sends an A DNS query to the DNS Server.*

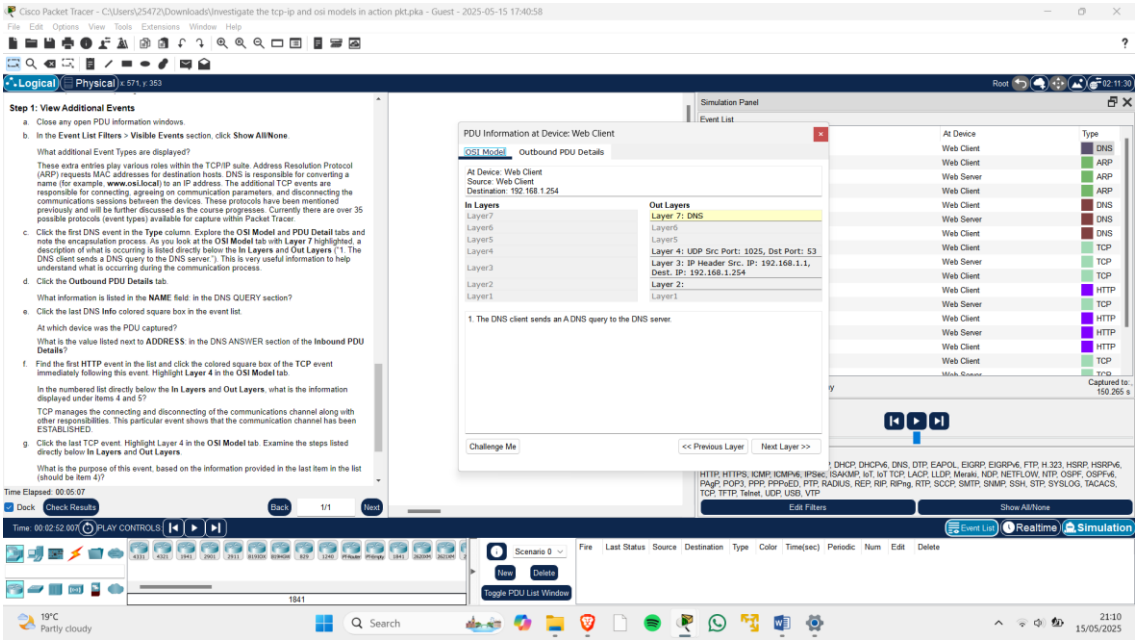

Figure 16: Evidence of the encapsulation note

I clicked the **Outbound PDU Details** tab on the PDU Information at Device:Web Client Window.

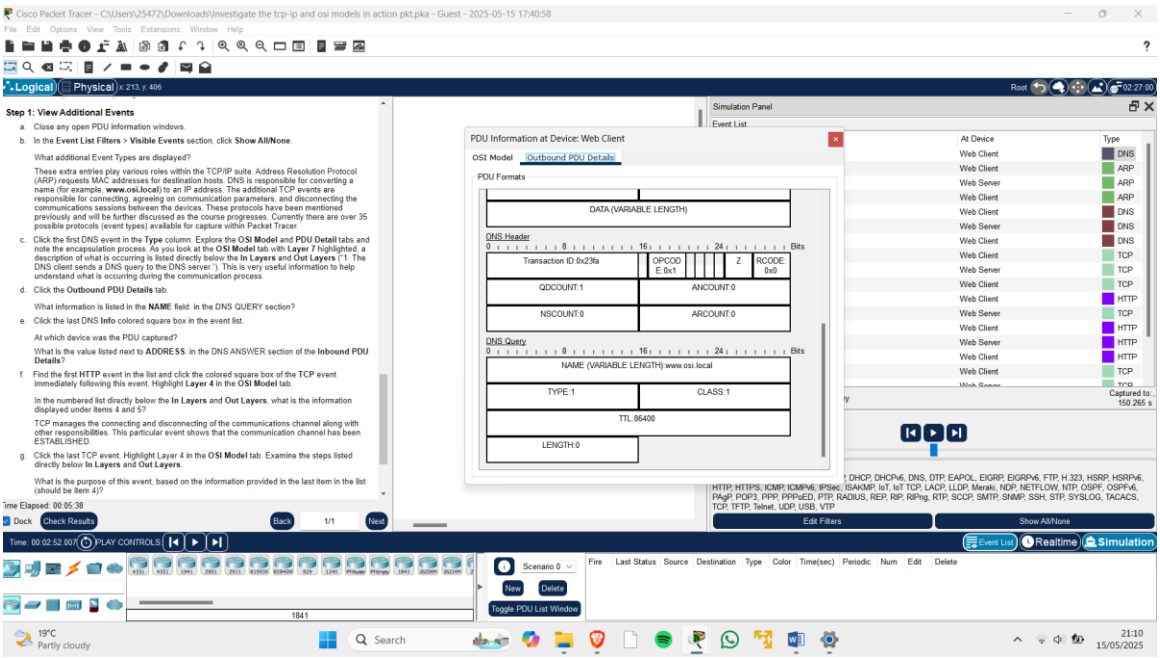

Figure 17: Evidence of the Outbound PDU Details tab

Question: What information is listed in the NAME field: in the DNS QUERY section?

www.osi.local

I clicked the last **DNS info colored square box** in the event list. **Question**: At which device was the PDU captured? **Web Client**

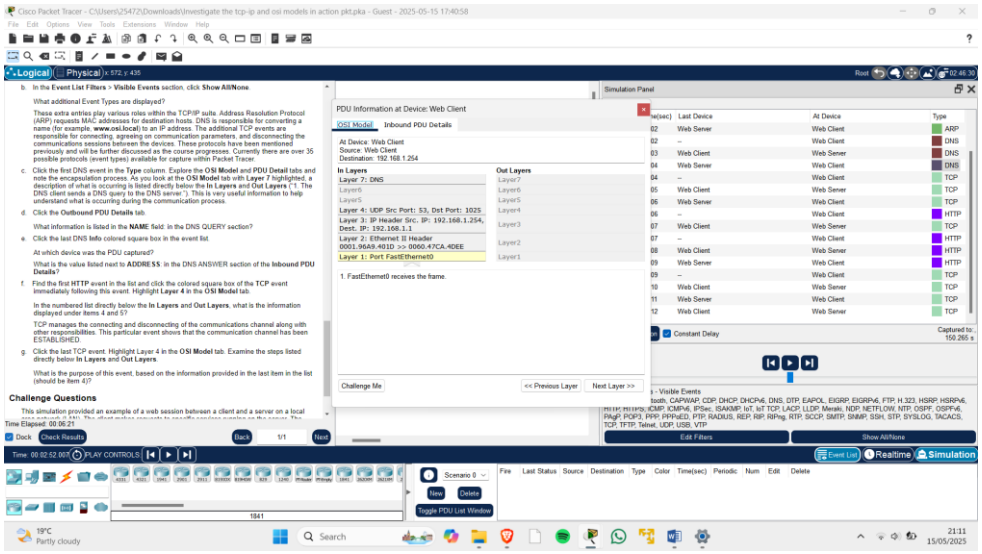

Figure 18: Evidence of the device

What is the value listed next to ADDRESS: in the DNS ANSWER section of the Inbound PDU Details? **www.osi.local**

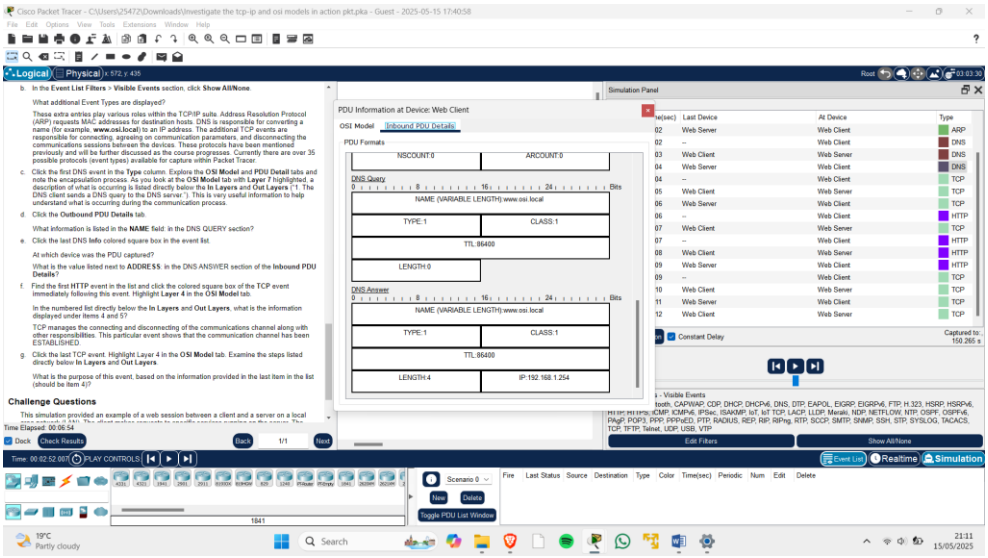

Figure 19: Evidence of the value

I found the **first HTTP event** in the list and clicked the **colored square box of the TCP event following immediately** after this event.

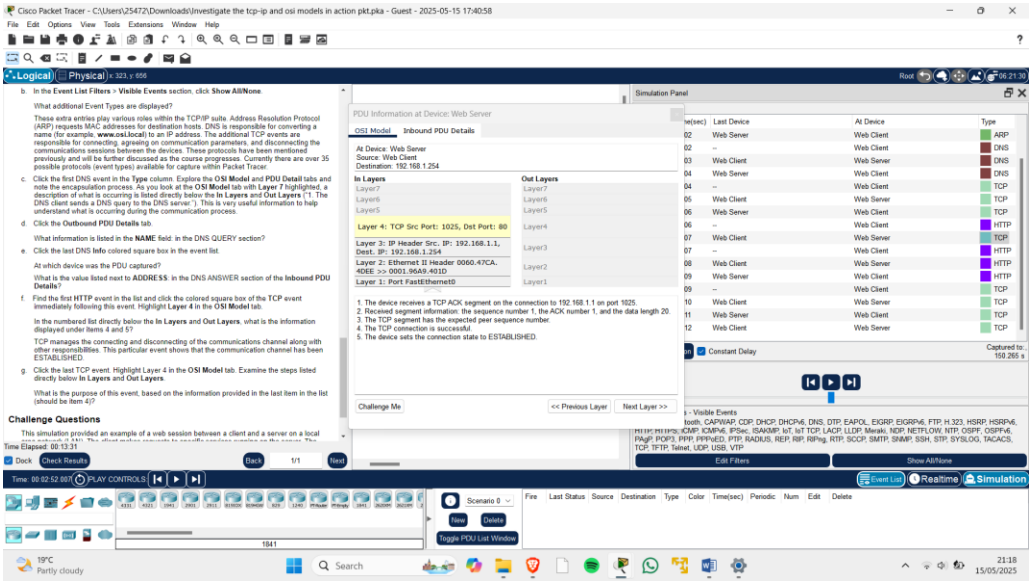

Figure 20: Evidence of the OSI Model tab of the TCP event

Question: In the numbered list directly below the In Layers and Out Layers, what is the information displayed under items 4 and 5? **The TCP connection is successful and The device sets the connection state to ESTABLISHED**

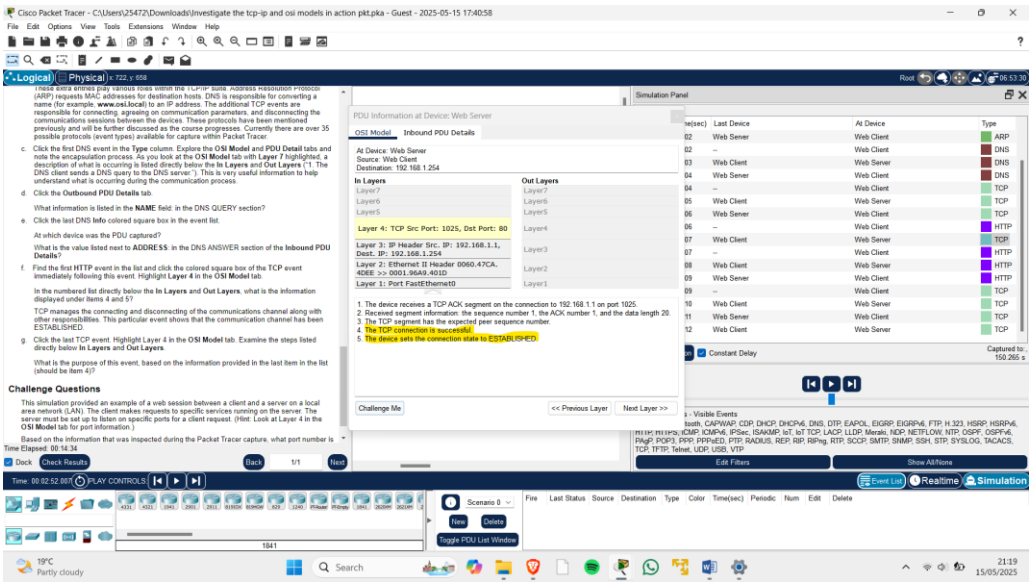

Figure 21: Evidence of the Layer 4 of the In Layers of the OSI model tab of the TCP event

Note: TCP manages the connecting and disconnecting of the communications channel along with other responsibilities. This particular event shows that the communication channel has been ESTABLISHED.

I clicked the **last TCP event** and **highlighted Layer 4** in the OSI Model tab.

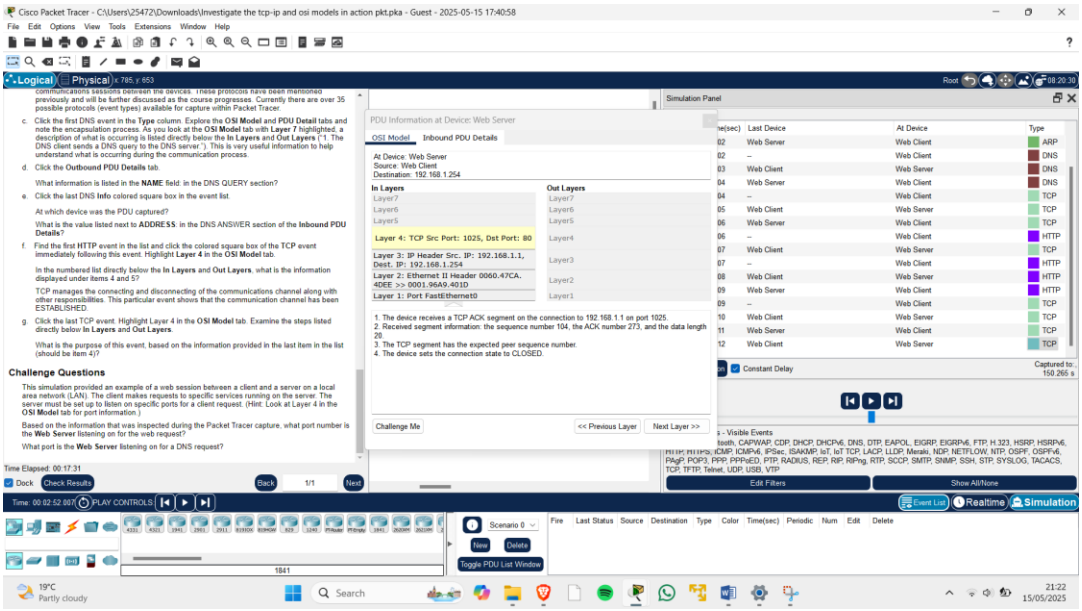

Figure 22: Evidence of Layer 4 of the TCP event

Question: Examine the steps listed directly below In Layers and Out Layers.

1. **The device receives a TCP ACK segment on the segment on the connection to 192.168.1.1 on port 1025**
2. **Received segment information: the sequence number 104, the ACK number 273, and the data length 20**
3. **The TCP segment has the expected peer sequence number**
4. **The device sets the connection state to CLOSED**

What is the purpose of this event, based on the information provided in the last item in the list (should be item 4)? **The device sets the connection state to be CLOSED i.e the Web Server closes the connection.**

Challenge Questions

The client makes requests to specific services running on the server. The server must be set up to listen on specific ports for a client request.

Question: Based on the information that was inspected during the Packet Tracer capture, what port number is the Web Server listening on for the web request? **Destination Port 80**

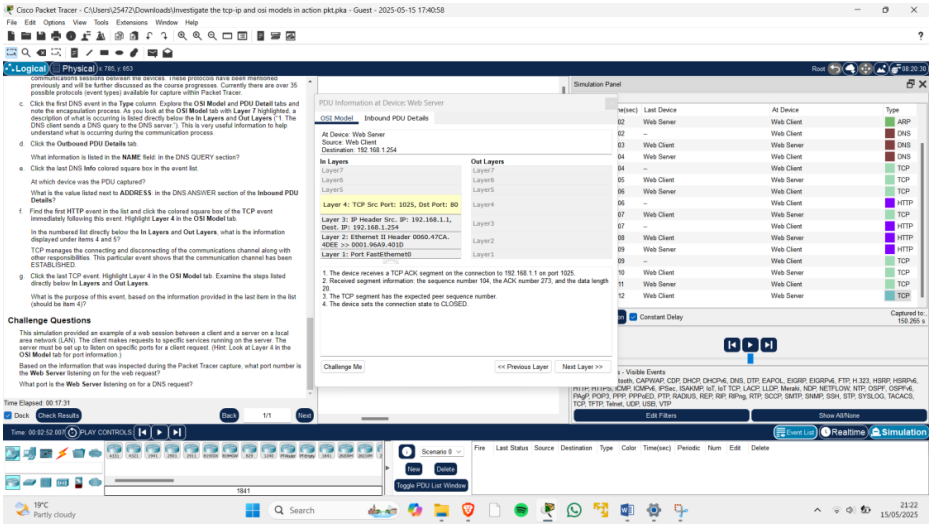

Figure 23: Evidence of destination port of the HTTP

What port is the web Server listening on for a DNS request? **Destination Port 53**

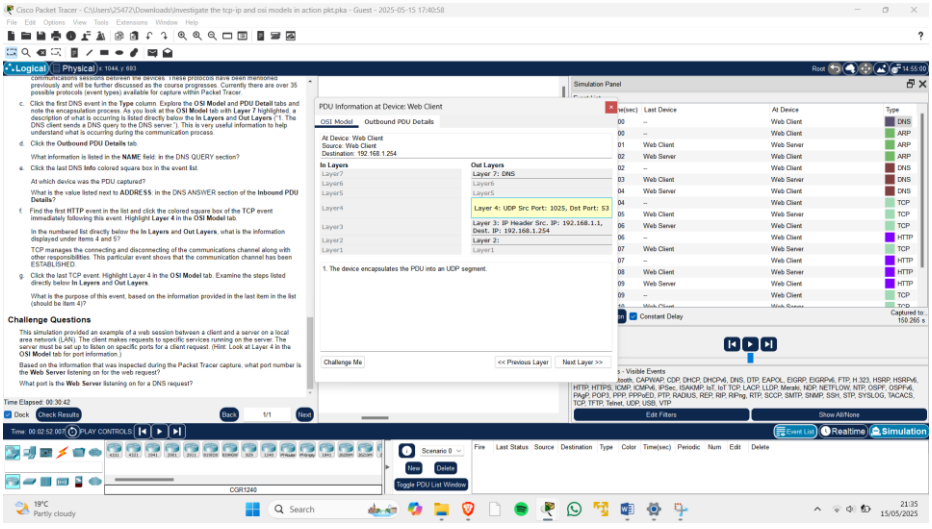

Figure 24: Evidence of destination port of the DNS

Conclusion

This Packet Tracer activity helped me better understand how the TCP/IP and OSI models work together in real network communication. By following the process of a web request and looking at the PDUs at each layer, I was able to see how data is broken down, labeled, and reassembled as it moves through the network. It clearly showed the role each layer and protocol plays, making it easier to connect the theory with how things actually happen when devices communicate.