

Course: Cloud and Network Security – C2-2025

Student Name: **Naomi Kwamboka Onyancha**

Student No: **CS-CNS09-25098**

**Thursday, May 14, 2025**

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

Introduction .....	3
Answers to the question .....	3
Section A - <b>Installing Packet Tracer</b> .....	3
Section B – Assignment 1.....	4
Objectives.....	4
Part 1: Examine HTTP Web Traffic.....	4
Step 1: Switch from Realtime to Stimulation mode.....	4
Step 2: Generate web (HTTP) Traffic .....	5
Step 3: Explore the Contents of the HTTP packet.....	10
Part 2: Display Elements of the TCP/IP Protocol Suite .....	17
Step 1: View Additional Events .....	17
Challenge Questions .....	21
Conclusion.....	22

## Introduction

This report explores the practical implementation of the TCP/IP and OSI models using Cisco Packet Tracer, a network simulation tool widely used in IT and networking education. The simulation begins with the installation and setup of Cisco Packet Tracer, followed by the creation of a simple network consisting of a Web Client (PC) and a Web Server.

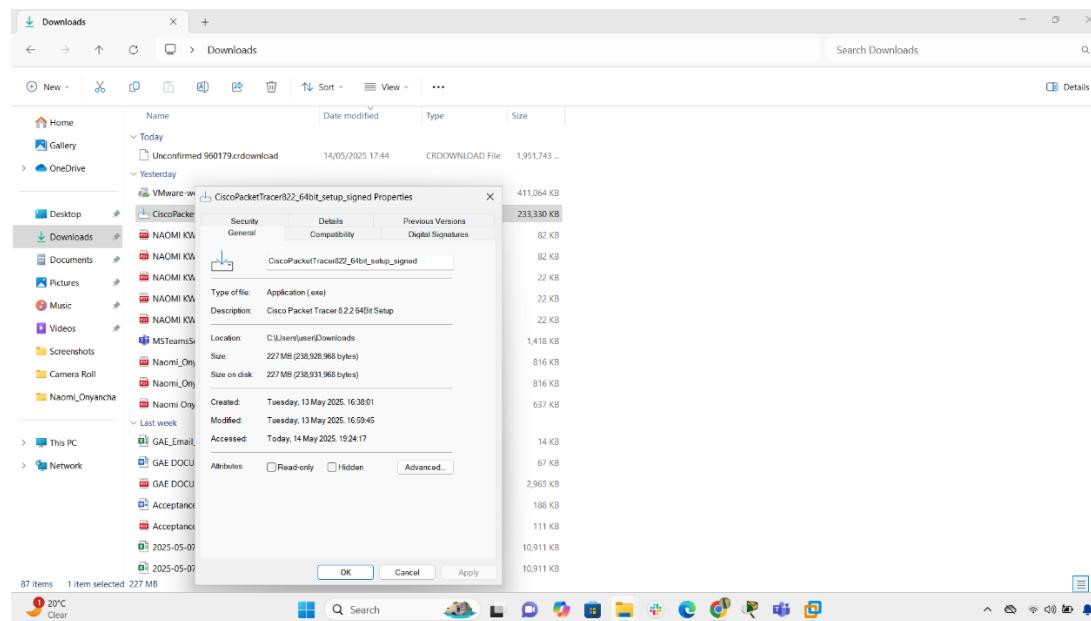
The main objective of this exercise is to observe how data travels between devices across the network using the HTTP protocol, and to understand how different layers of the OSI and TCP/IP models are involved during communication. By using Simulation Mode and tools such as the Capture/Forward button, network events can be analyzed step-by-step, making it easier to visualize how protocols function in a real-world scenario.

This report documents the process, observations, and analysis of the data exchange between the client and server, demonstrating the importance of each networking layer and the role of packet encapsulation and de-encapsulation.

## Answers to the question

### Section A- Installing Packet Tracer

In this section, Cisco Packet tracer is installed as a workspace for our assignment. It is recommended to download the latest version. That was 8.2.



## Section B – Assignment 1

### Objectives

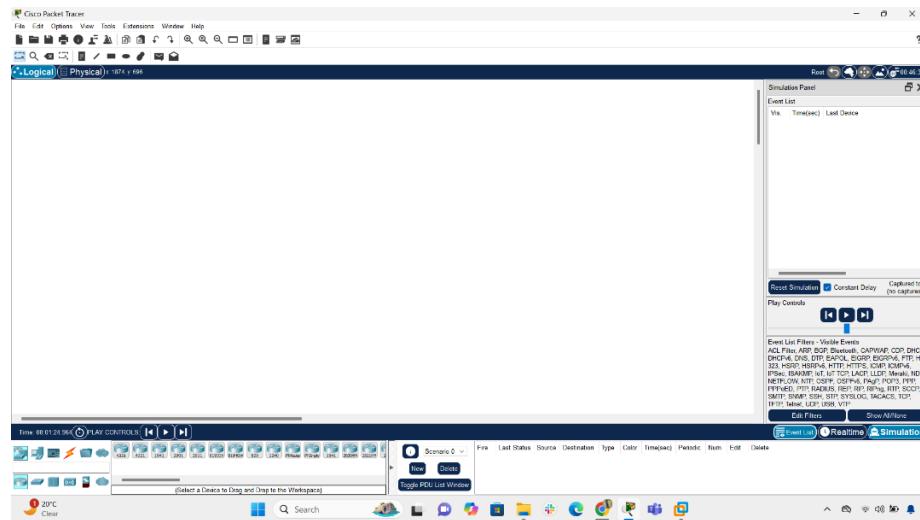
Part 1: Examine HTTP Web Traffic

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

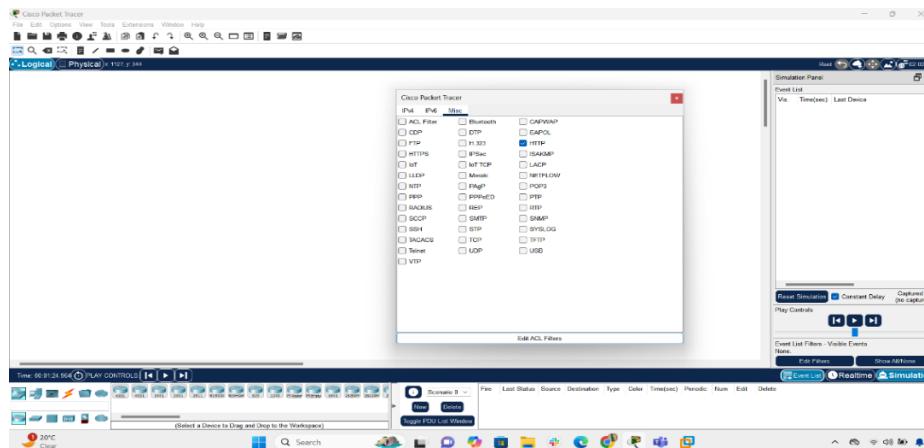
*Part 1: Examine HTTP Web Traffic*

Step 1: Switch from Realtime to Stimulation mode

A) The main goal of switching from Real time to stimulation mode it was in order to monitor traffic. We will be able to see packet moving through the network slowly. Simulation allows us to see protocols in action; HTTP. Here we are going to understand the process visually.

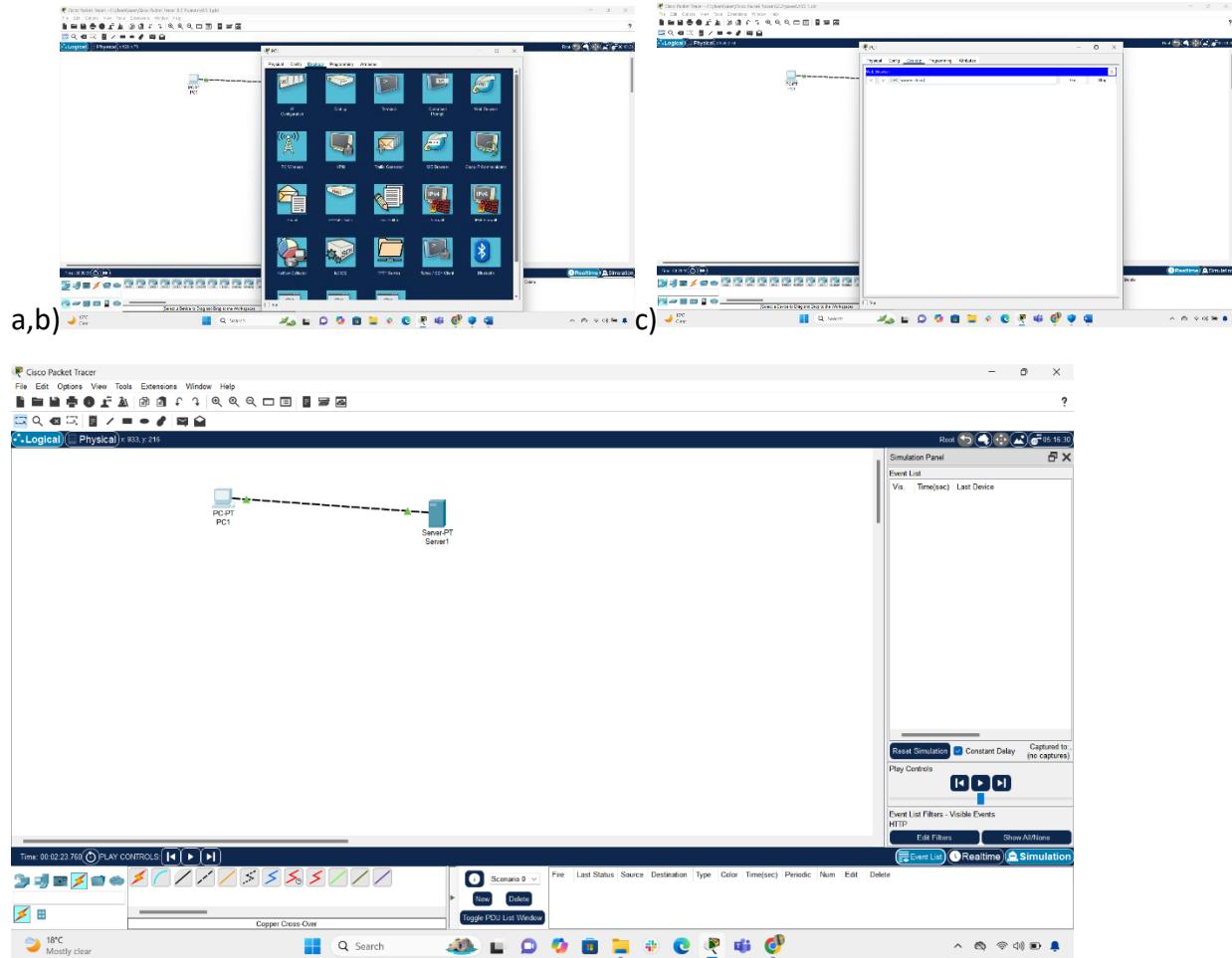


b) Select HTTP



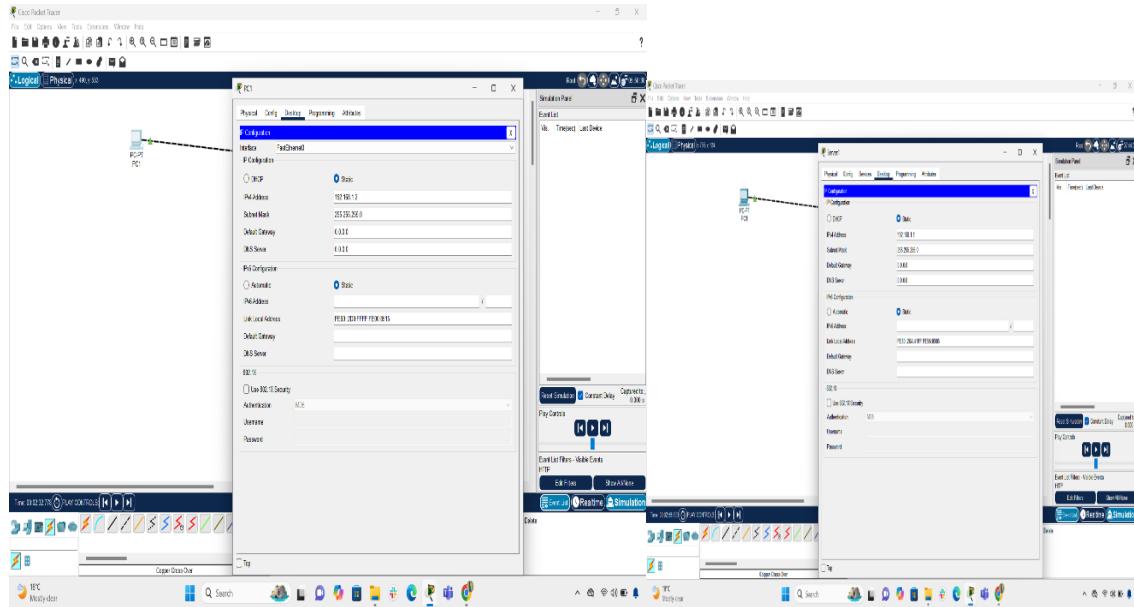
## Step 2: Generate web (HTTP) Traffic

In this step , we are going to identify our tools, Web Client(PC), Server and Copper Cross-Over Cable to connect the two.

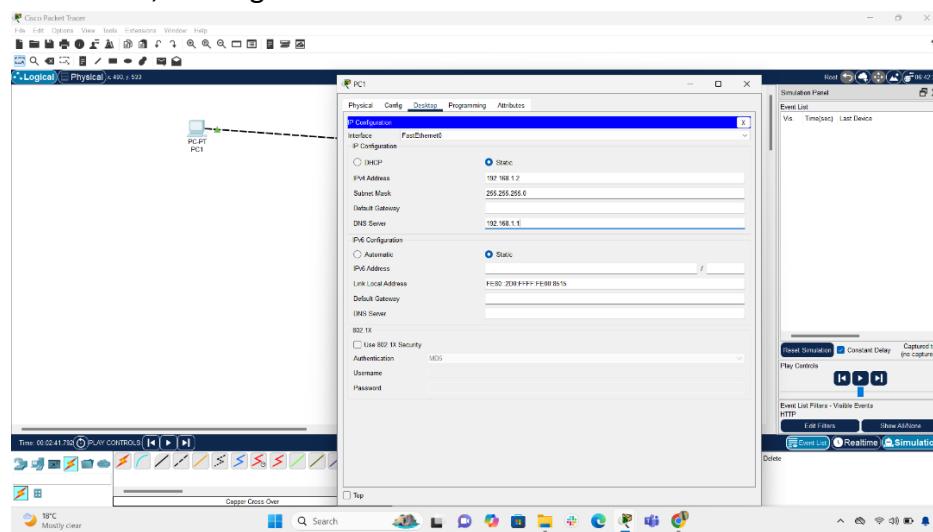


The next step, we should do IP Configuration on both :

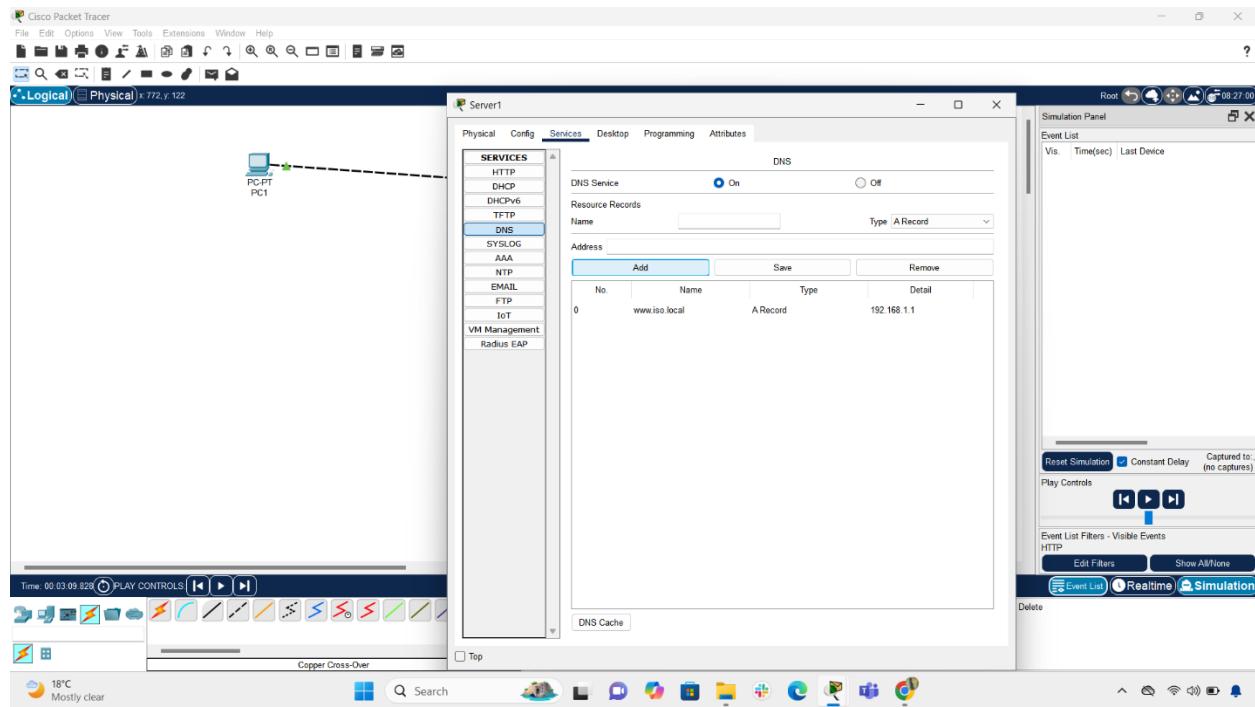
- **Web Client:** 192.168.1.2, **Subnet Mask:** 255.255.255.0
- **Server:** 192.168.1.1, **Subnet Mask:** 255.255.255.0



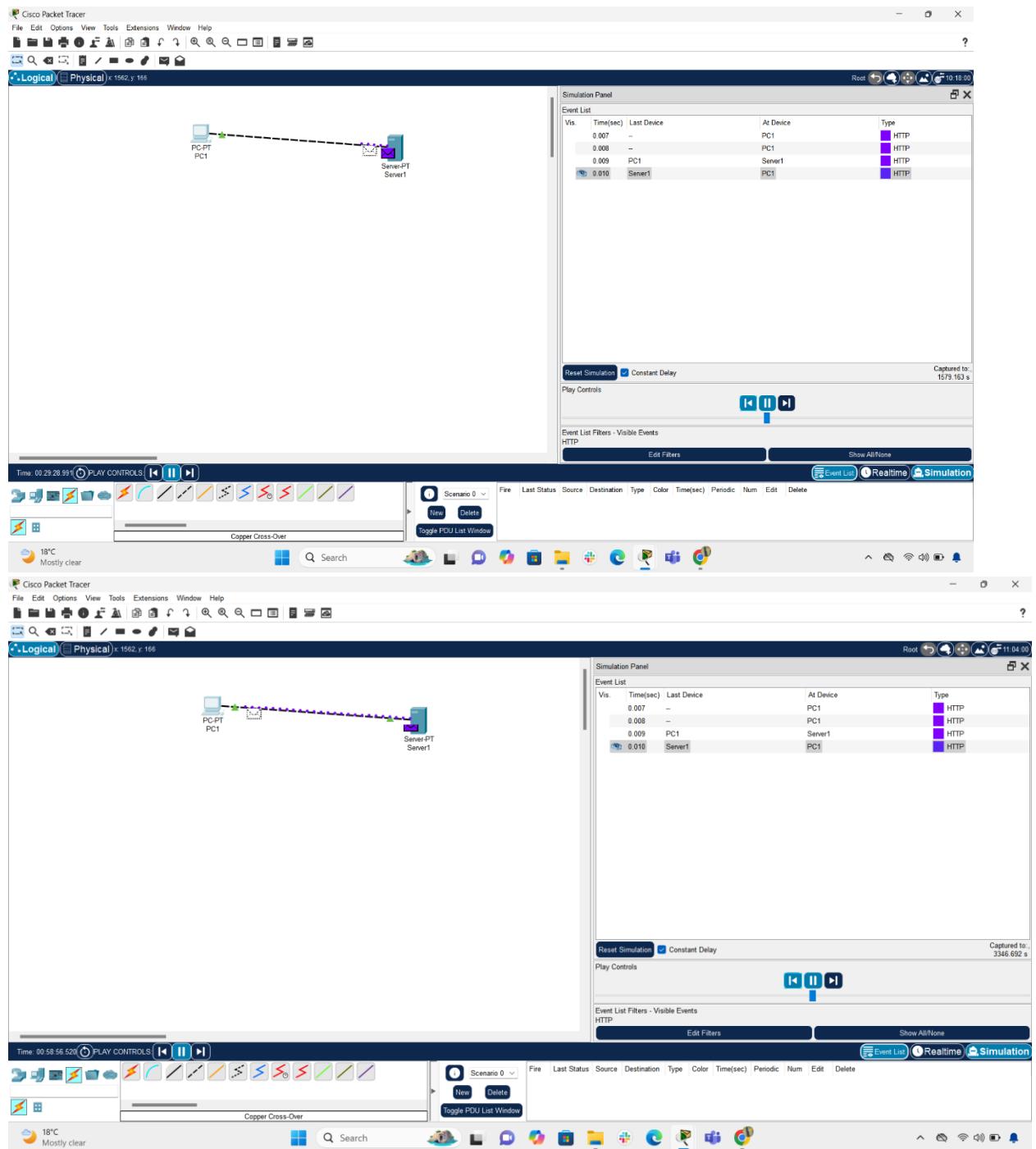
Remember, to assign the IP address of the DNS Server to the PC too.

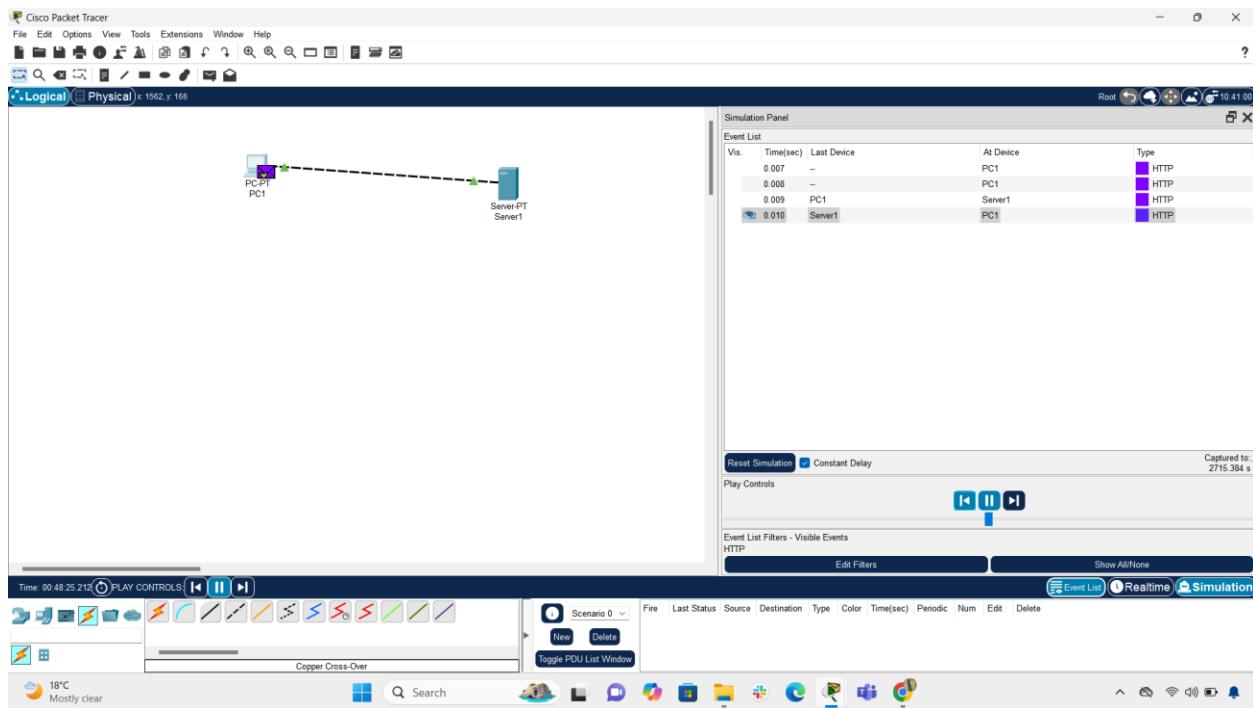


On the Server, we are going to turn on the DNS, input the URL [www.iso.local](http://www.iso.local) and finally assign the Server's IP address to it; Click Add. **NB: Make sure the HTTP is on.**

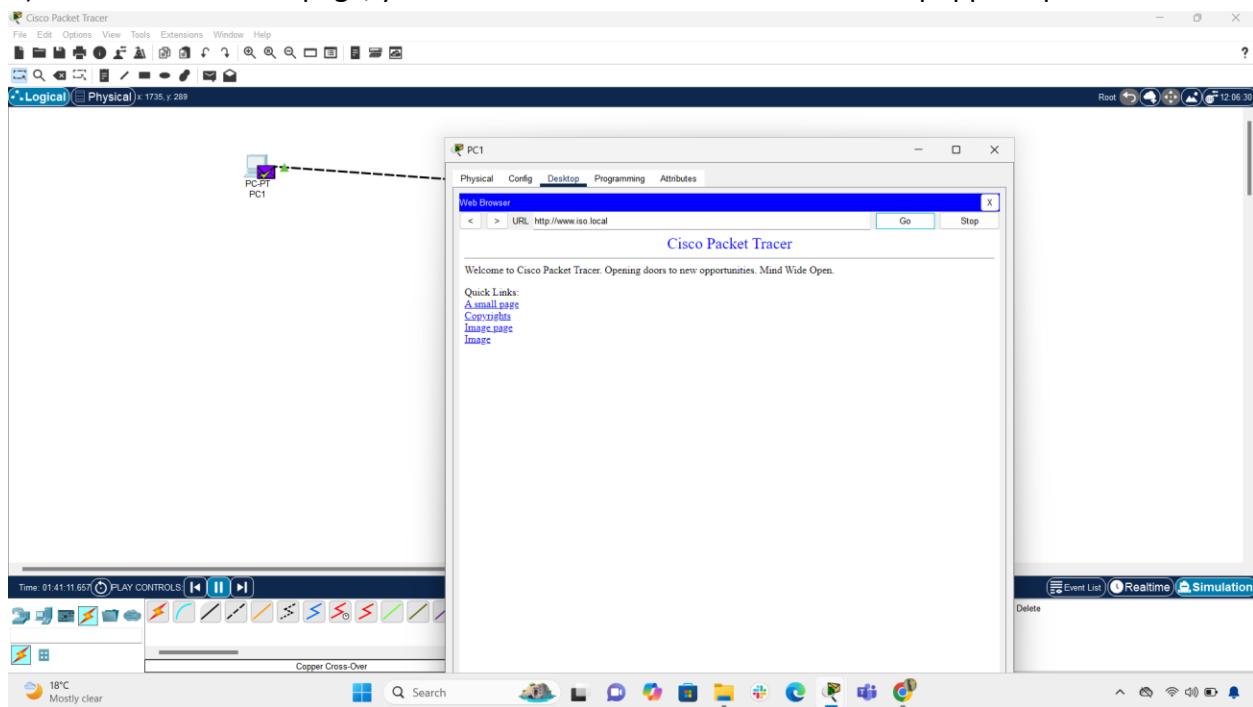


d) Next, we go to our PC on the Desktop Tab then we click Web Browser icon and in the URL Field we enter [www.osi.local](http://www.osi.local) and click go. Then we use the capture forward button and click it four times. These are some of the observations you will see





d)At the Web Browser page, you can see 'Cisco Packet Tracer' website popped up.

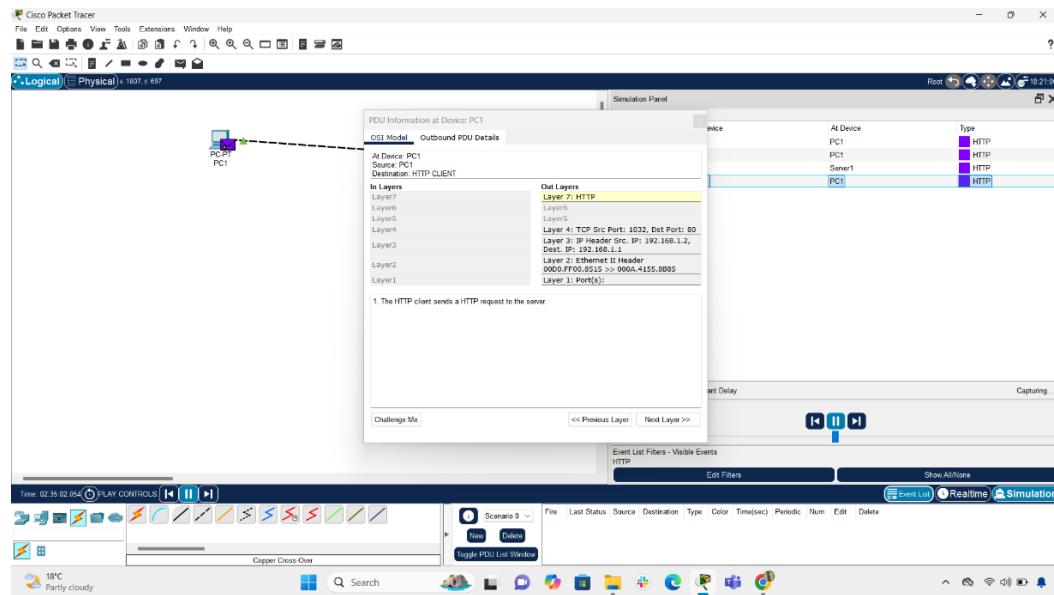


### Step 3: Explore the Contents of the HTTP packet

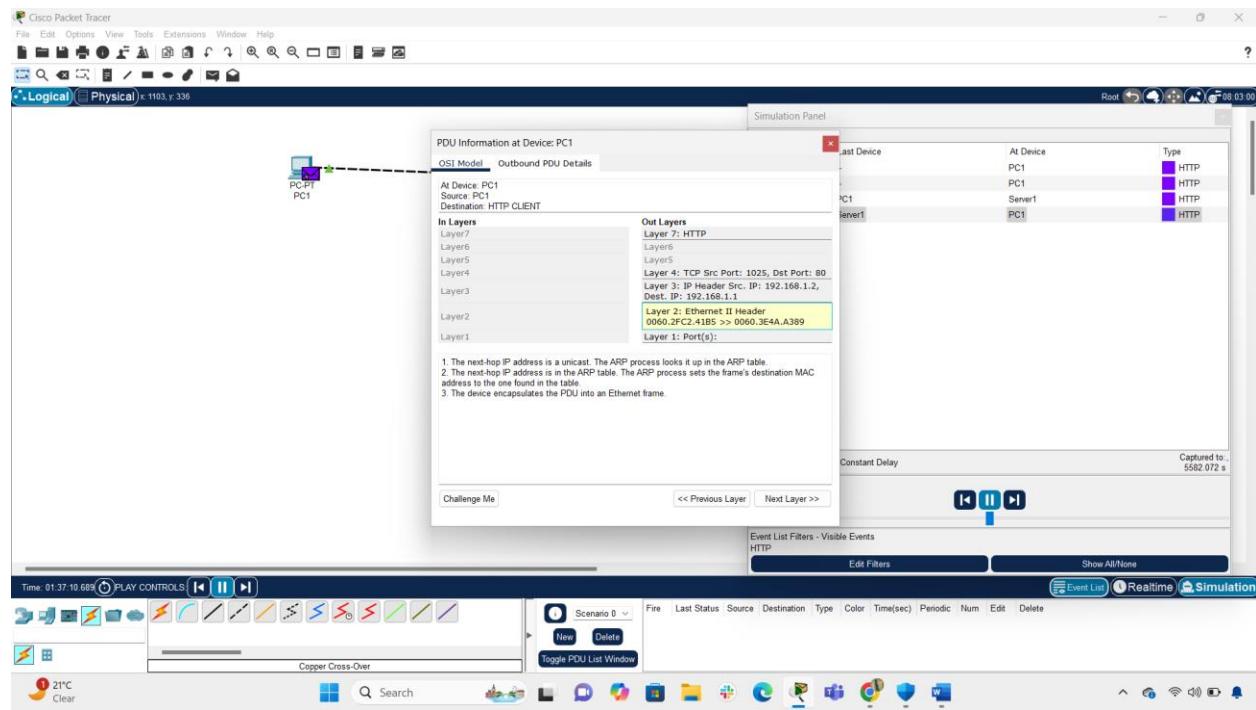
- a) When the first colored square box is selected PDU information at Device: Web Client(PC) pops up. They are only two tabs (OSI Model and Outbound PDU details).
- b) At the OSI Model tab, under Out Layers Column, when Layer 7 is selected there is a message at the bottom that says ***The HTTP Client send a HTTP request to the Server.***

**Dst Port value for layer 4 : 80**

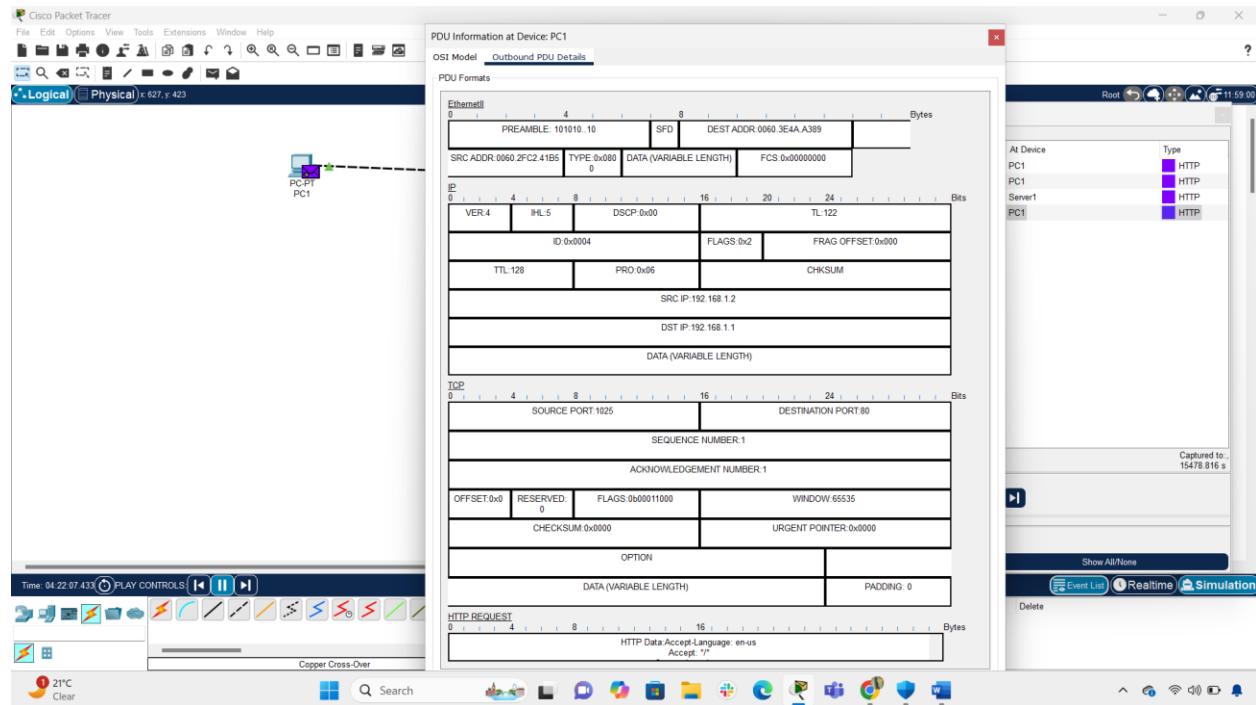
**Dest. IP value for Layer 3 : 192.168.1.1 NB: THIS IS THE SERVER'S ADDRESS**



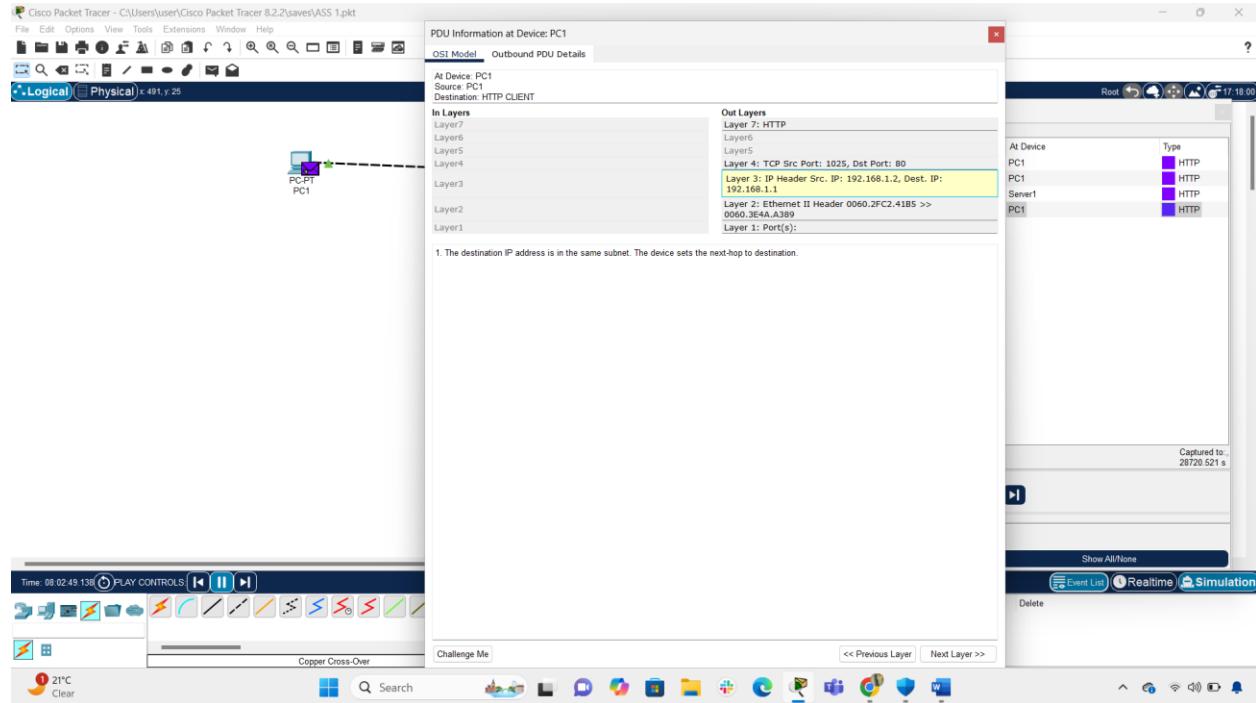
**The Information displayed at Layer 2 under the Out Layers is Ethernet II Header  
0060.2FC2.41B5 >>0060.3E4A.A389**



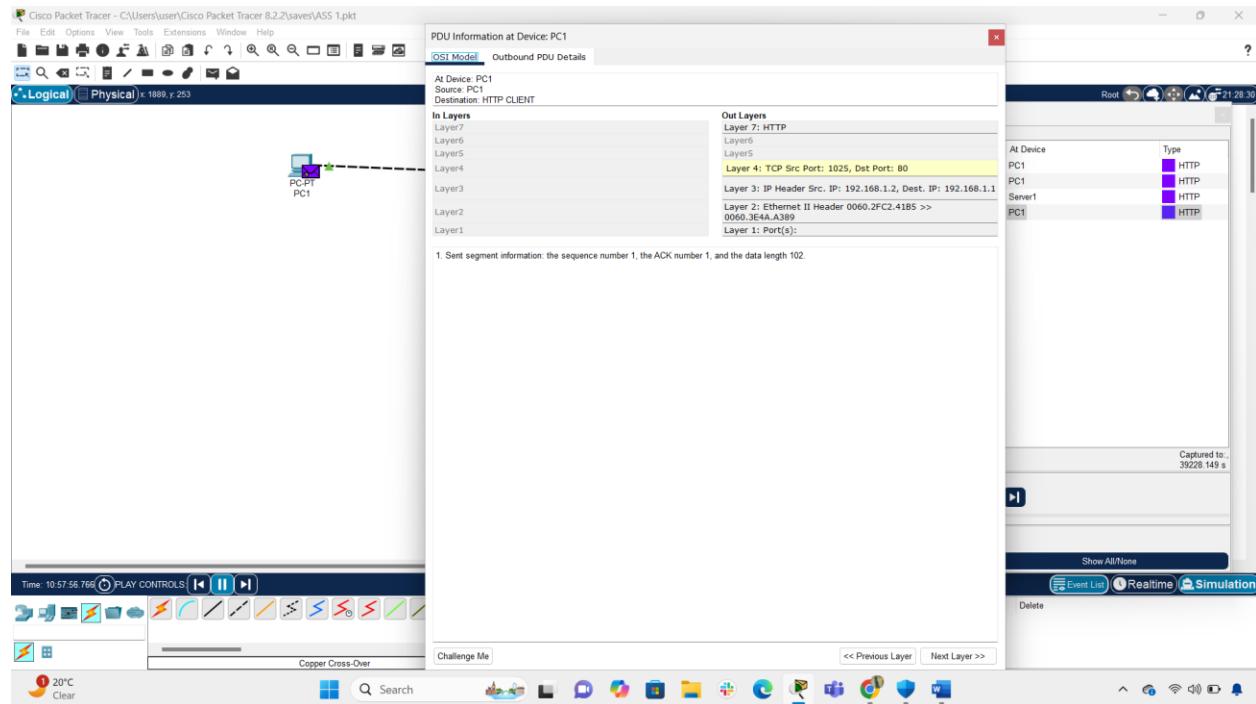
When you click the Outbound PDU Details tab you will note that the information listed under Ethernet II section is more detailed than in the OSI Model.



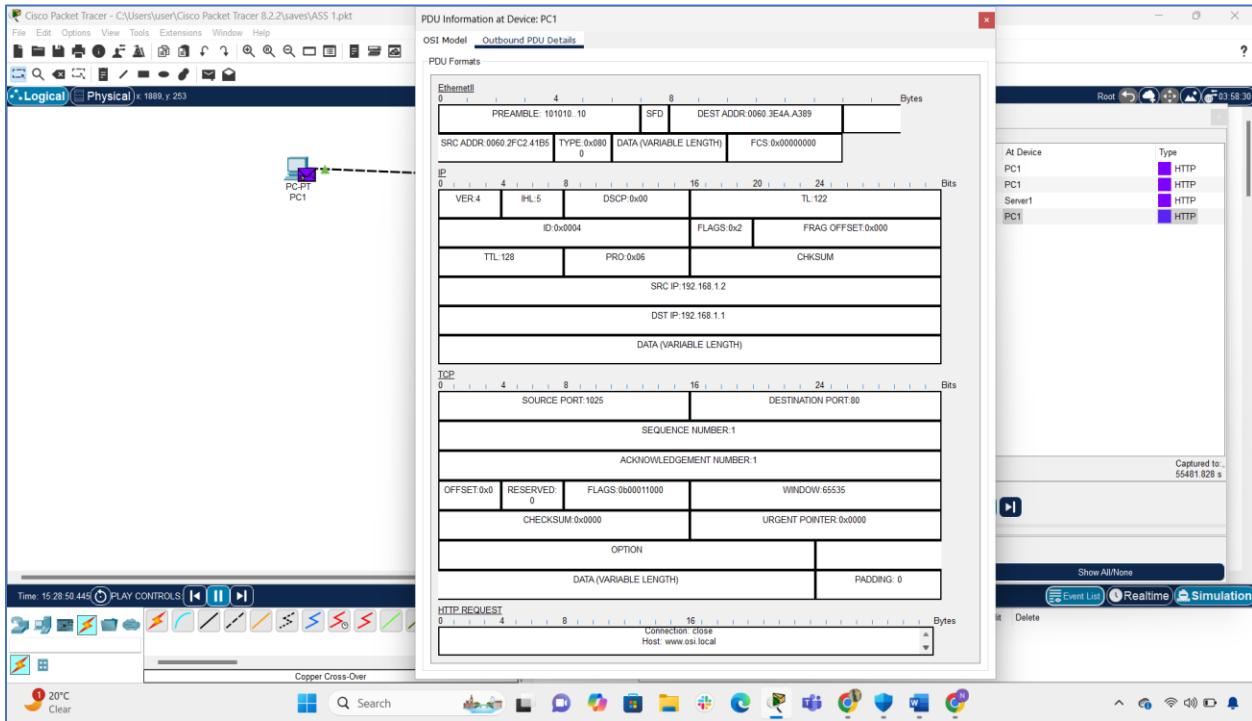
**The common information listed under the IP section under the PDU Details as compared to the information under the OSI Model Tab is the Src IP address(Web Client's) and the Dest. IP address(Server's). This is seen at Layer 3 of the OSI model.**



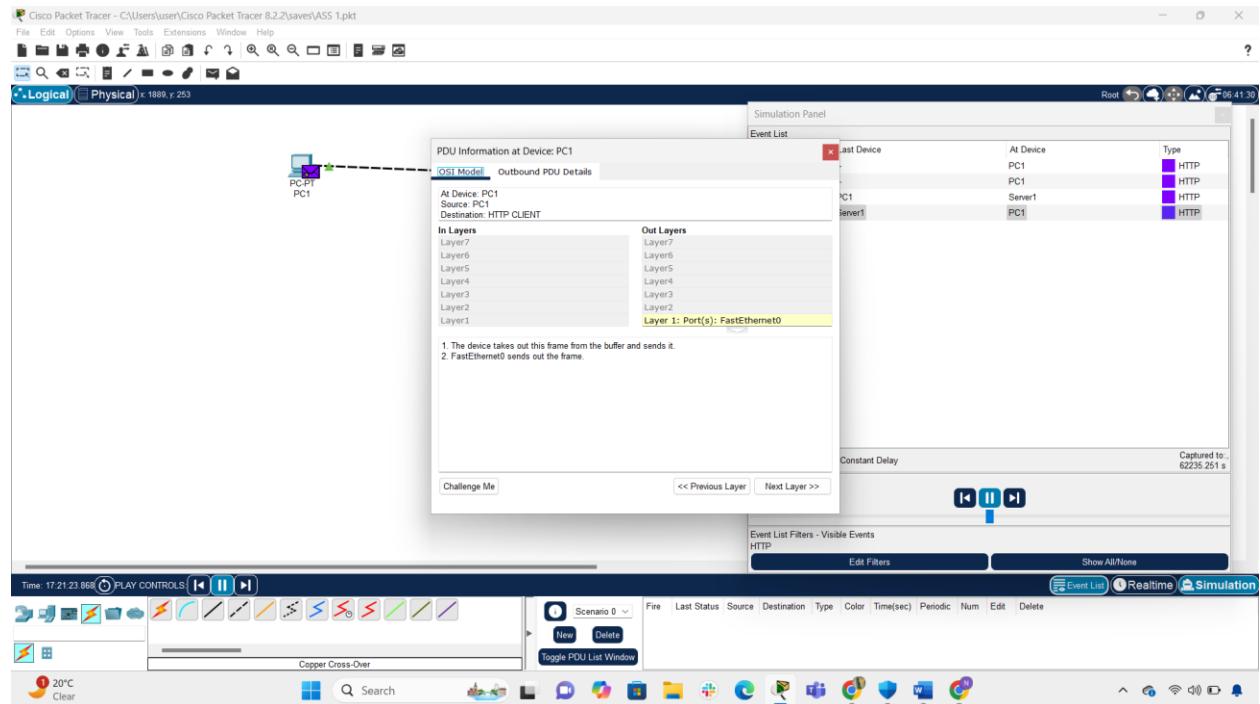
**c)The common information listed under the TCP Section of PDU sections as compared to OSI Model is the Src Port: 1025 and the Dst Port : 80 . These is located in Layer 4 of the OSI Model.**



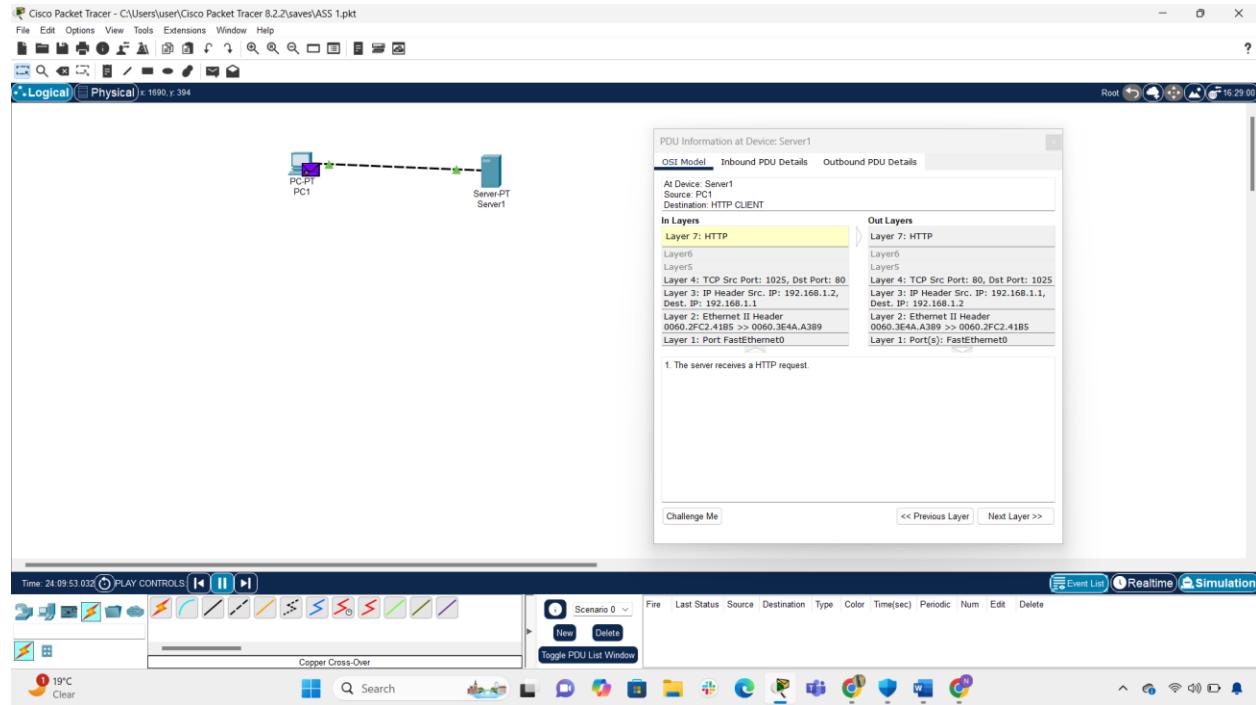
c) The Host listed under the HTTP section of the PDU Details is [www.osi.local](http://www.osi.local). This information is associated with Layer 7 under the OSI Model.



d) When you click the next colored square box, only Layer 1 is active; as shown below. The device takes out this frame from the buffer and sends it. Copper Cross-over cable (FastEthernet0) sends out the frame.



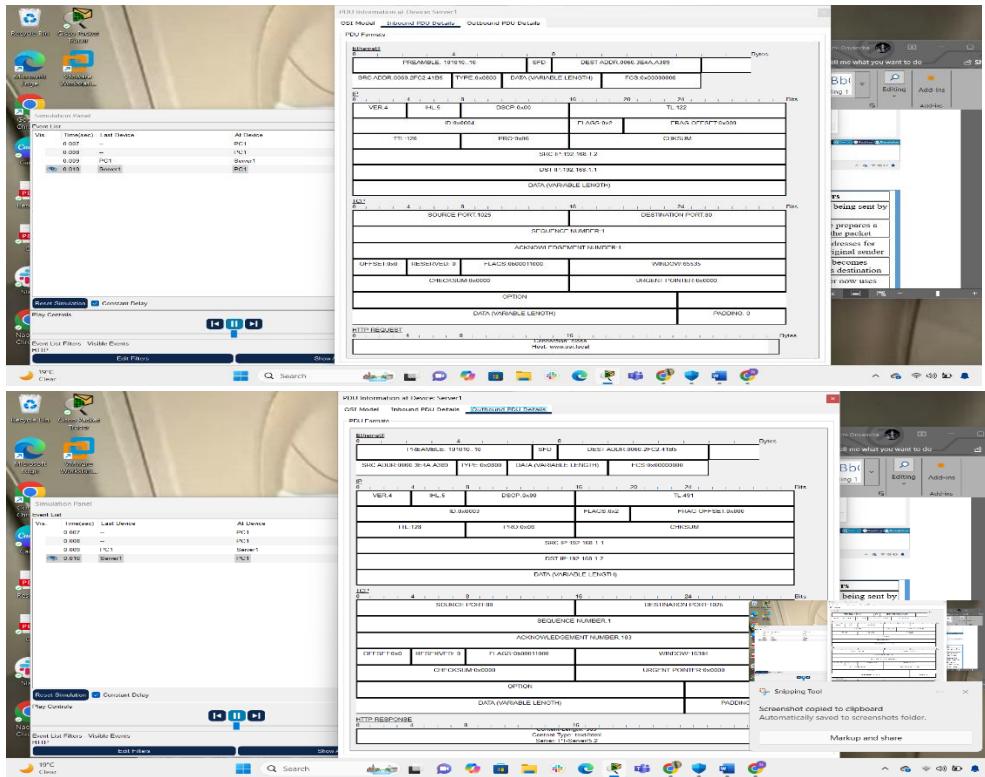
e) Click the next HTTP Type box. This window shows In layers and the Out Layers. In this case the In Layers represent the PC (Webclient) and the Out Layers (Server). The arrows shows how the data is travelling. At the top the arrow points to the right , this shows the server is now sending info to the client.



e) These are the major differences between the two;

Aspect	In Layers	Out Layers
<b>Direction</b>	Incoming traffic (data received by the device)	Outgoing traffic (data being sent by the device)
<b>Purpose</b>	Shows how the device processes the received packet layer by layer	Shows how the device prepares a response or forwards the packet
<b>Layer 2 (Ethernet)</b>	Shows the <b>source MAC</b> as the sender and <b>destination MAC</b> as this device	Reverses the MAC addresses for sending back to the original sender
<b>Layer 3 (IP)</b>	Shows the packet's <b>source IP</b> (original sender) and <b>destination IP</b>	Reverses IPs—server becomes source, client becomes destination
<b>Layer 4 (TCP)</b>	Shows incoming <b>source port</b> (client) and <b>destination port</b> (server: 80)	Reverses ports—server now uses port 80 as <b>source</b>
<b>Layer 7 (HTTP)</b>	Shows the incoming HTTP request data	Shows the outgoing HTTP response (if applicable)
<b>Usage Context</b>	Used to inspect and analyze what a device <b>receives</b>	Used to inspect what a device <b>sends out</b>

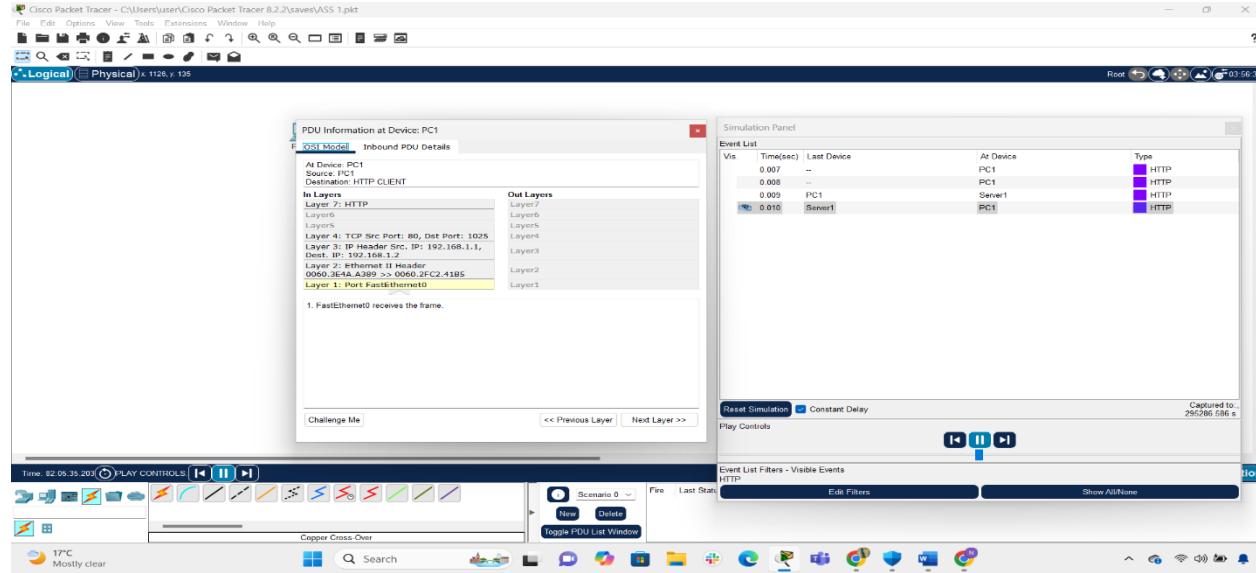
Here is a view of The Inbound and Outbound PDU Tab.



f) Here is a review between the Inbound and Outbound;

Layer	Inbound (PC1 → Server1)	Outbound (Server1 → PC1)
<b>Application (Layer 7)</b>	HTTP Request (Accept: /)	HTTP Response (Content-Type: text/html; Server: PT-Server/5.2)
<b>Transport (Layer 4)</b>	Source Port: <b>1025</b> Destination Port: <b>80</b>	Source Port: <b>80</b> Destination Port: <b>1025</b>
<b>Network (Layer 3)</b>	Source IP: <b>192.168.1.2</b> Destination IP: <b>192.168.1.1</b>	Source IP: <b>192.168.1.1</b> Destination IP: <b>192.168.1.2</b>
<b>Data Link (Layer 2)</b>	Source MAC: <b>0060.2FC2.41B5</b> Destination MAC: <b>0060.3E4A.A389</b>	Source MAC: <b>0060.3E4A.A389</b> Destination MAC: <b>0060.2FC2.41B5</b>
<b>Physical (Layer 1)</b>	Arrives at Server1 via <b>FastEthernet0</b>	Leaves Server1 via <b>FastEthernet0</b>

**g) The last HTTP Type box , we see two tabs only that is OST Model and Inbound PDU. All this is happening in the PC which is our Web Client, because the message has already left the Server now it has arrived the PC.** Here is a visual of what is happening and a simple explanation behind every layer.

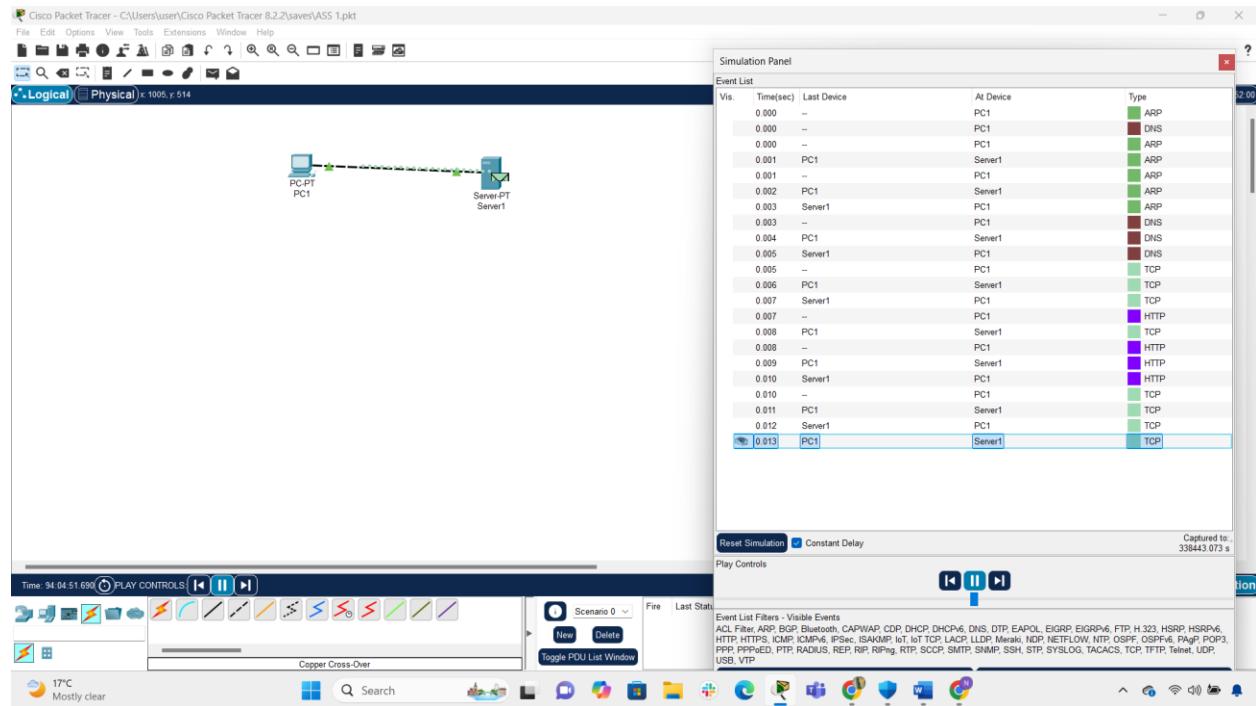


OSI Layer	Simple Description	What Happens on PC1
<b>Layer 1 – Physical</b>	<i>"The message physically arrives."</i>	The message comes in through FastEthernet0. FastEthernet0 receives the frame.
<b>Layer 2 – Data Link</b>	<i>"The PC checks the MAC address to confirm the message is for it."</i>	PC1 sees the Ethernet frame is addressed to its MAC: From: 0060.3E4A.A389 To: 0060.2FC2.4185
<b>Layer 3 – Network</b>	<i>"Now it checks IP addresses to route it correctly."</i>	Source IP: 192.168.1.1 (Server1) Destination IP: 192.168.1.2 (PC1) PC1 confirms: "Yes, this is for me."
<b>Layer 4 – Transport</b>	<i>"Check the ports to see what type of message it is."</i>	Source port: 80 (HTTP) Destination port: 1025 (used by PC1) PC1 says: "This is for my web browser."
<b>Layer 5 – Session</b>	<i>"Keep track of the ongoing conversation."</i>	PC1 maintains the session with Server1 to keep the HTTP connection alive and organized.
<b>Layer 6 – Presentation</b>	<i>"Make the message readable."</i>	Any data formatting or decoding (if needed) happens here so the message can be understood.
<b>Layer 7 – Application</b>	<i>"Show the webpage to the user."</i>	The HTTP content is passed to the web browser so the user can see the webpage.

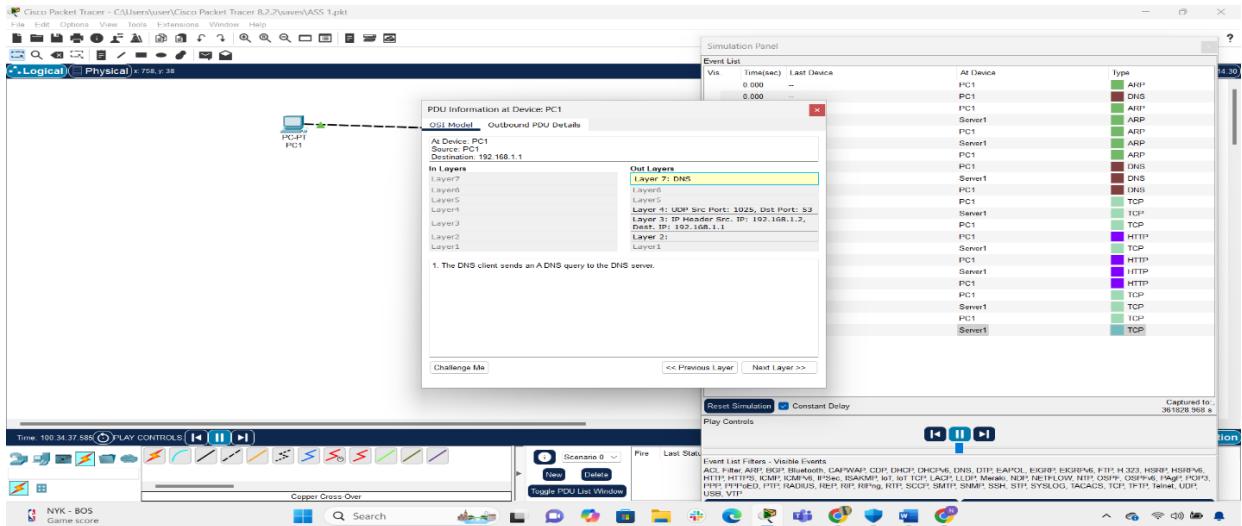
## Part 2: Display Elements of the TCP/IP Protocol Suite

### Step 1: View Additional Events

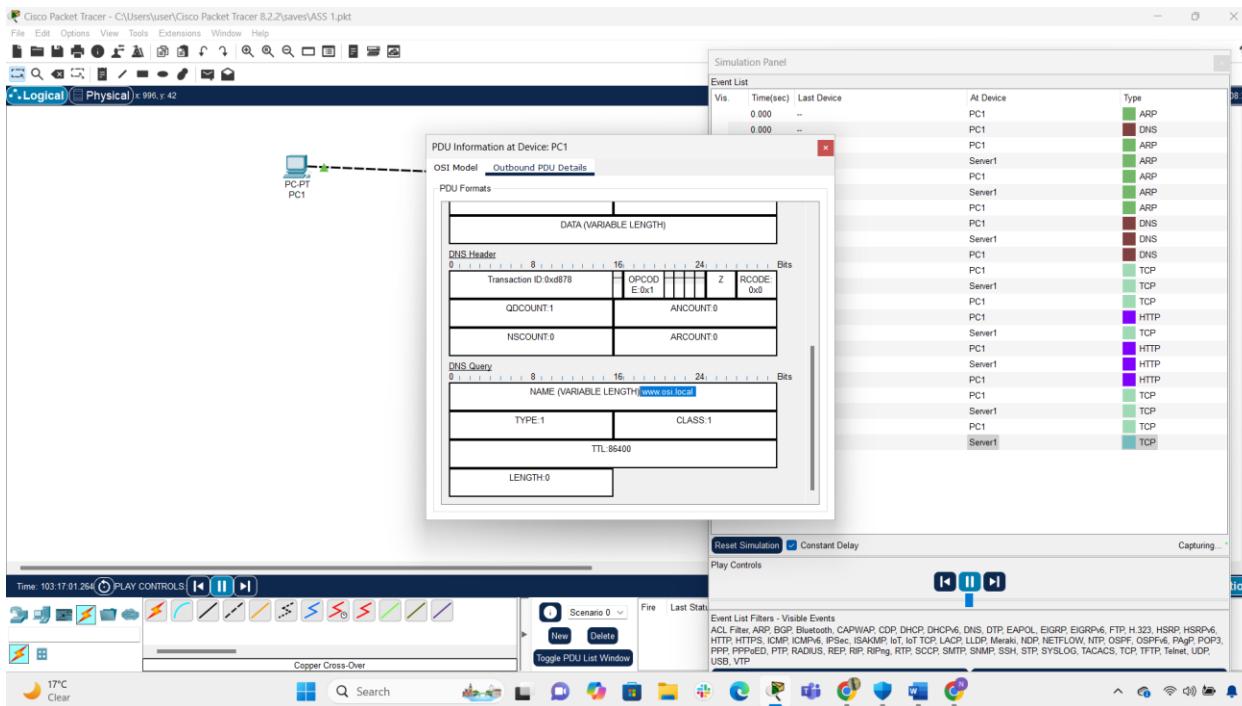
b) We are able to see **Address Resolution Protocol (ARP)** that requests MAC Addresses for destination hosts. **DNS** is responsible for converting a name, in our case([www.osi.local](http://www.osi.local)) to an IP address. The additional **TCP** events are responsible for connecting, agreeing on communication parameters and disconnecting the communications sessions between devices.



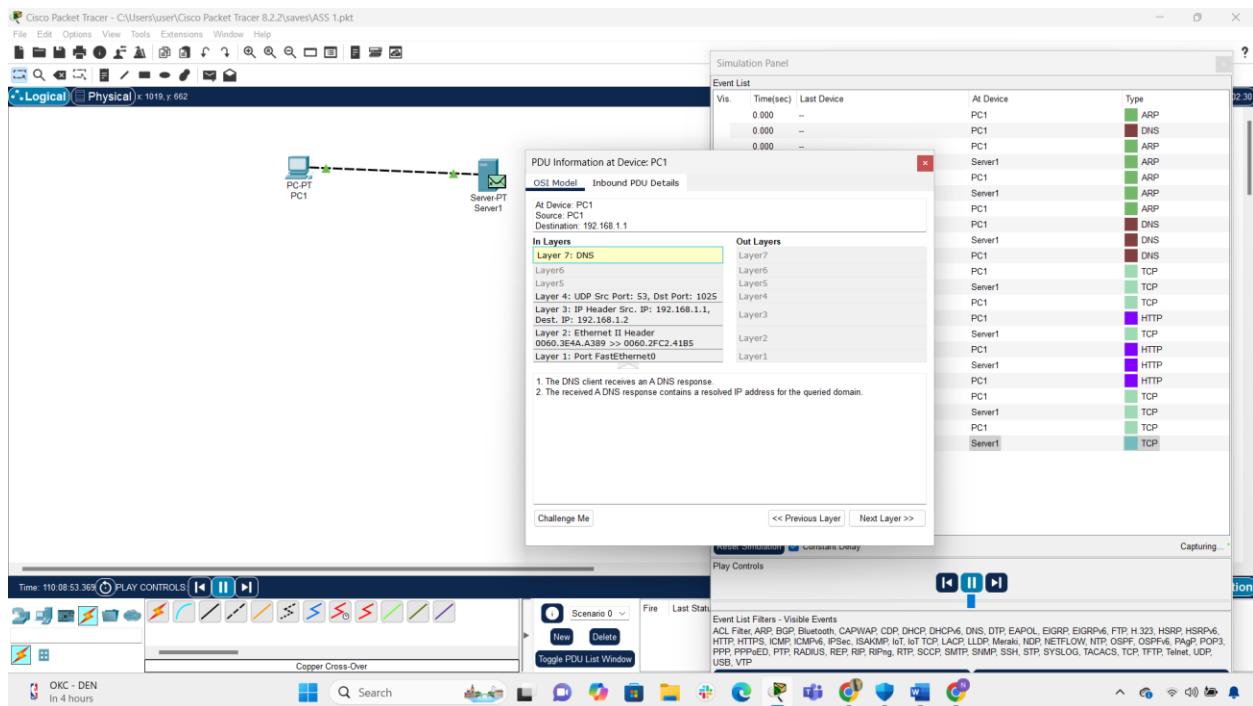
c) After Clicking the first DNS event in the type column, we can observe the OSI and the PDU Detail tabs as seen below. On Layer 7 on the OSI Model tab it states that '1. The DNS client sends an A DNS query to the DNS server.'



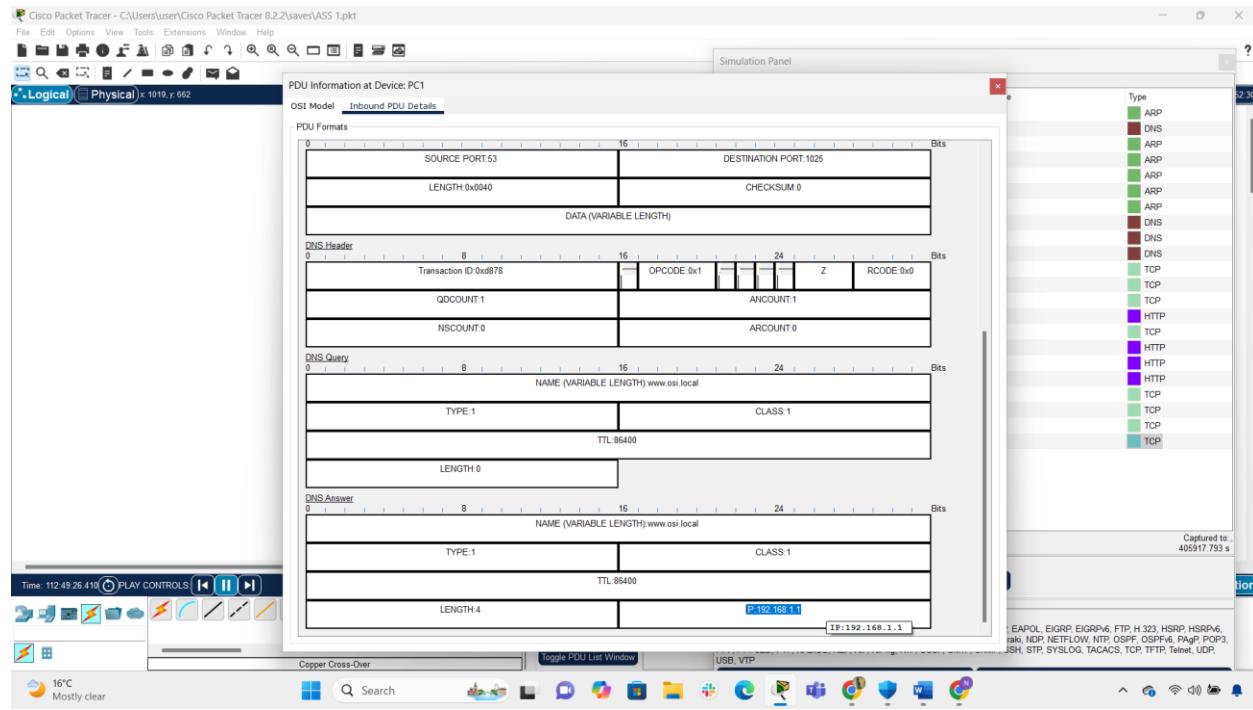
**d) Clicking the PDU Details tab, under the DNS QUERY Section in the NAME field :  
www.osi.local is listed as seen below.**



**e) Click at the last DNS. The PDU was captured in the Web Client device ; in our case that is PC1.**



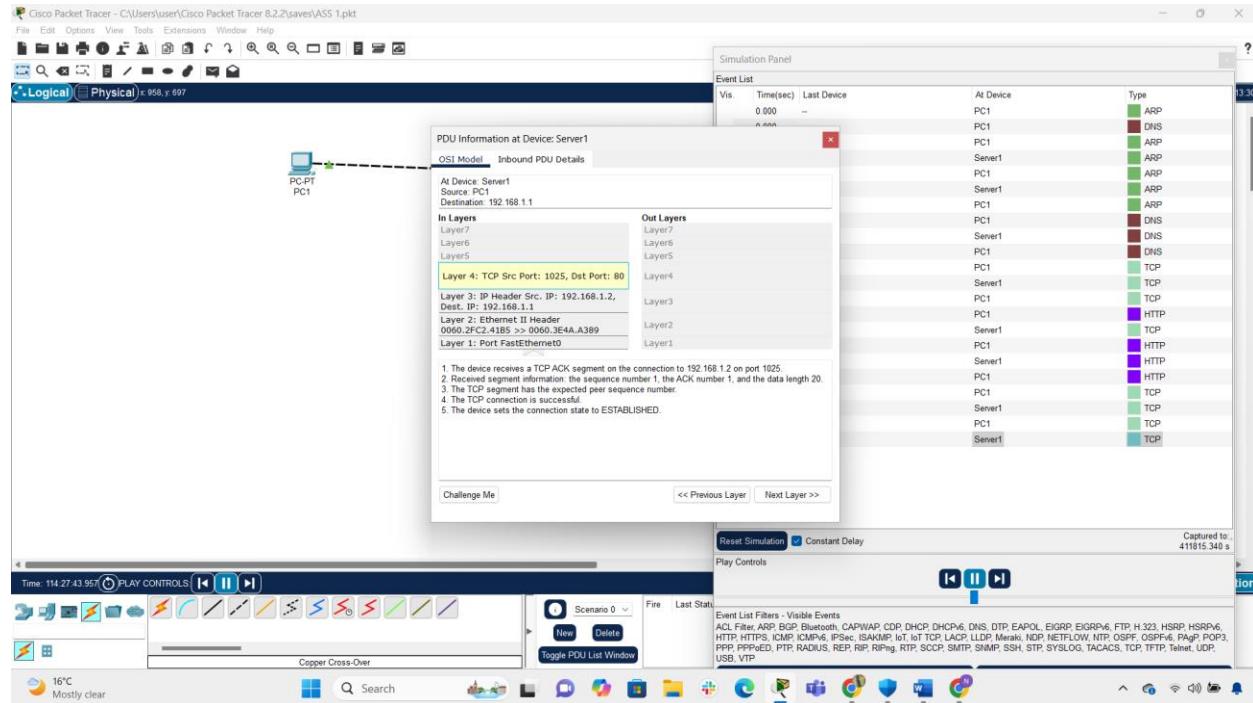
e) The value listed next to ADDRESS : in the DNS ANSWER section of the Inbound PDU Details is IP:192.168.1.1



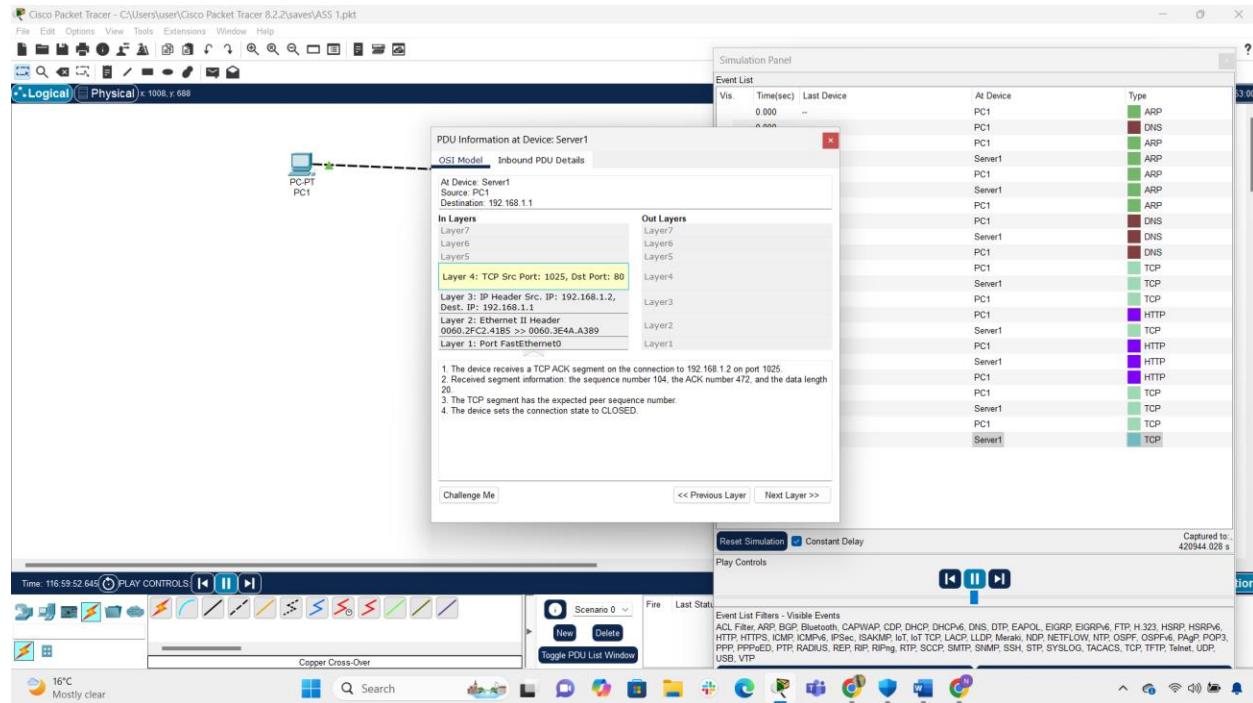
f) Click the TCP event just immediately after the first HTTP event. At the layer 4 in the OSI Model tab. The information under items 4 and 5 is;

4. The TCP connection is successful.

5. The device sets the connection state to ESTABLISHED.

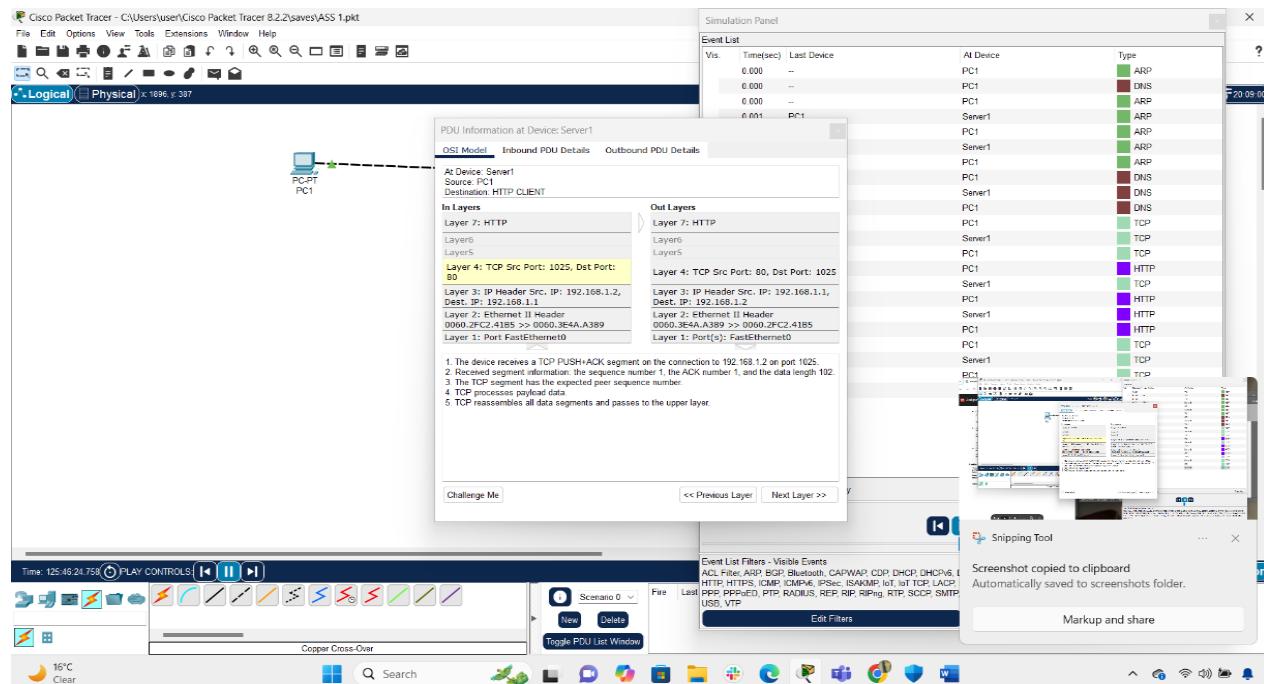


**g) Click the last TCP event. Layer 4 in the OSI Model tab. The purpose of this event as described in item 4 ‘The device sets the connection state to CLOSED.’ is the TCP connection termination process, where both devices agree to end the session cleanly.**



### Challenge Questions

**Based on the information, during Packet Tracer capture, what port number is the web server listening on for the web request? Port 80.**



## Conclusion

The Packet tracer demonstrated a full HTTP communication session between a client and a server using the OSI Model. By using simulation, I analyzed how each Layer contributes to data transmission; from addressing, port assignment and protocol use. I got to understand layered communication , TCP/IP behavior and various protocols interactions in real-world networking