-: Experiment -2 :-

Aim → Implementation of basic Ethernet using Cisco Packet Tracer to understand and make IP, TCP and UDP Header analysis.

Objective 1 → An overview on headers (i.e. Ethernet, IP, TCP & UDP), ICMP, FTP & TFTP.

Ethernet → i) Adelely used technology for wired Local Area Network.
ii) Uses frames to encapsulate data, containing MAC addresses for source & destination.
iii) Supports speed from 10 mBps to 100 GBps.

IP → i) Internet protocol is responsible for addressing and routing packet of data across networks.
ii) It is basically of two types → a) IPv4 (32-bit address)
b) IPv6 (128-bit address)

TCP → i) TCP stands for Transmission Control Protocol.
ii) TCP ensures reliable, ordered and error checked delivery of data between applications.

UDP → i) UDP stands for User Datagram Protocol.
ii) The purpose of UDP is to allow low latency, connectionless communication.
iii) Common uses of UDP is streaming media and online gaming.

ICMP → i) ICMP stands for Internet Control Message Protocol.
ii) Operates at the network layer, primarily for control messages.
iii) Used for troubleshooting and monitoring network ~~connecting~~ connectivity.

FTP → i) FTP stands for File Transfer Protocol.
ii) Supports authentication and can operate in both active and passive modes.
iii) Used for uploading and downloading files from web servers.

TFTP → i) TFTP stands for Trivial File Transfer Protocol

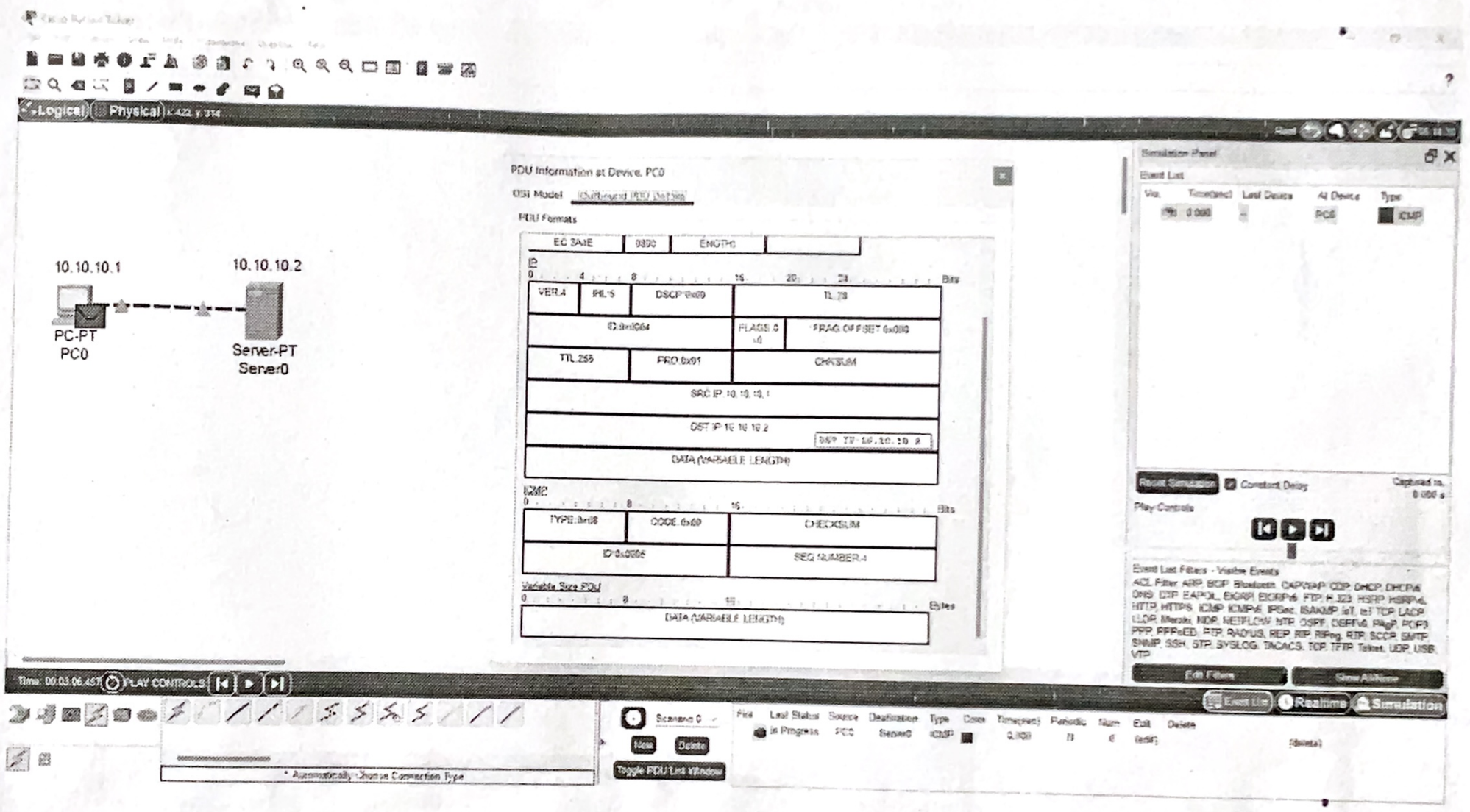
ii) Purpose is a simple version of FTP for transferring files with minimal overhead.

iii) Common uses booting devices over a network and transferring firmware or configuration files.

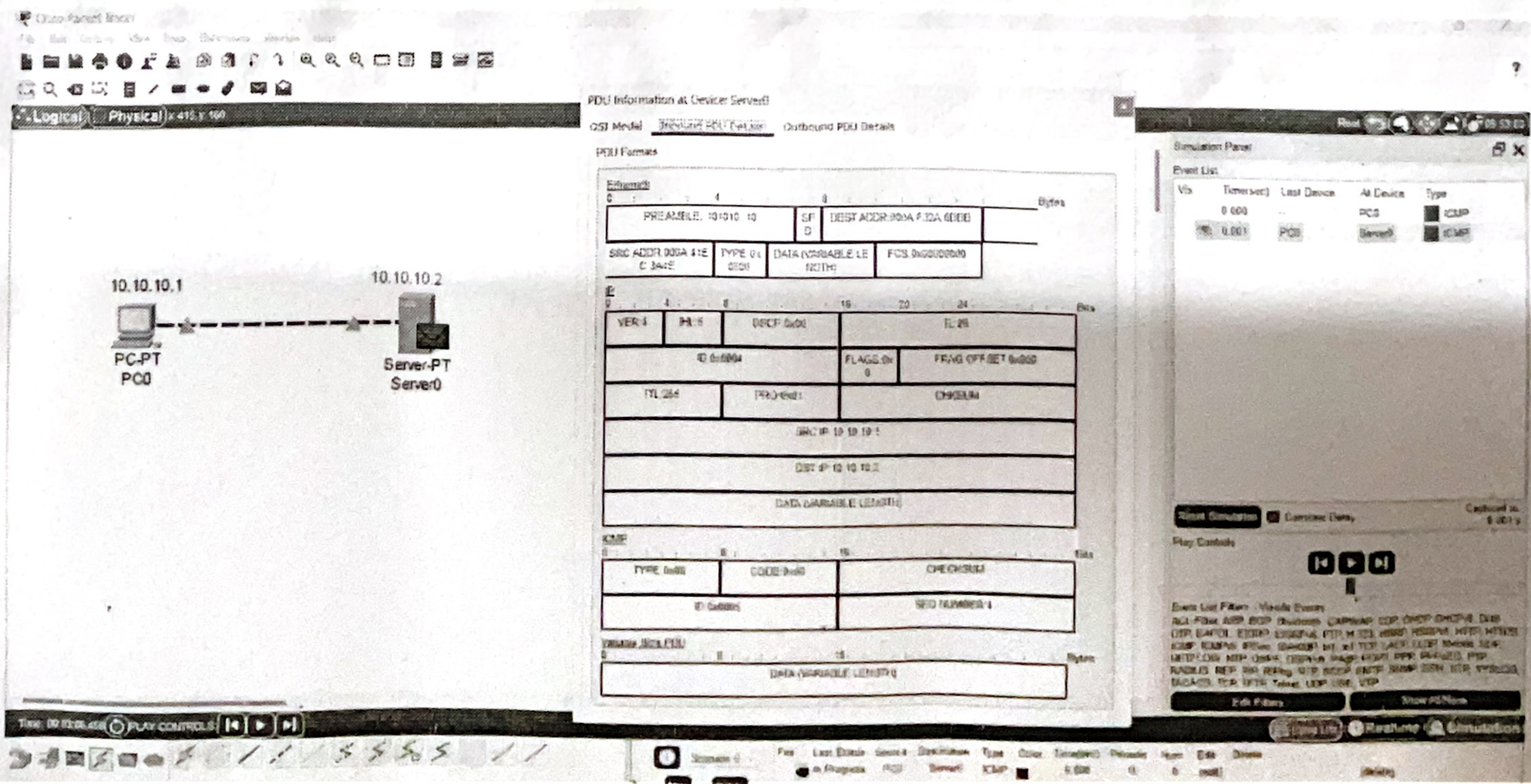
Objective 2 → Configuration of an Ethernet using the network devices in Cisco Packet Tracer.

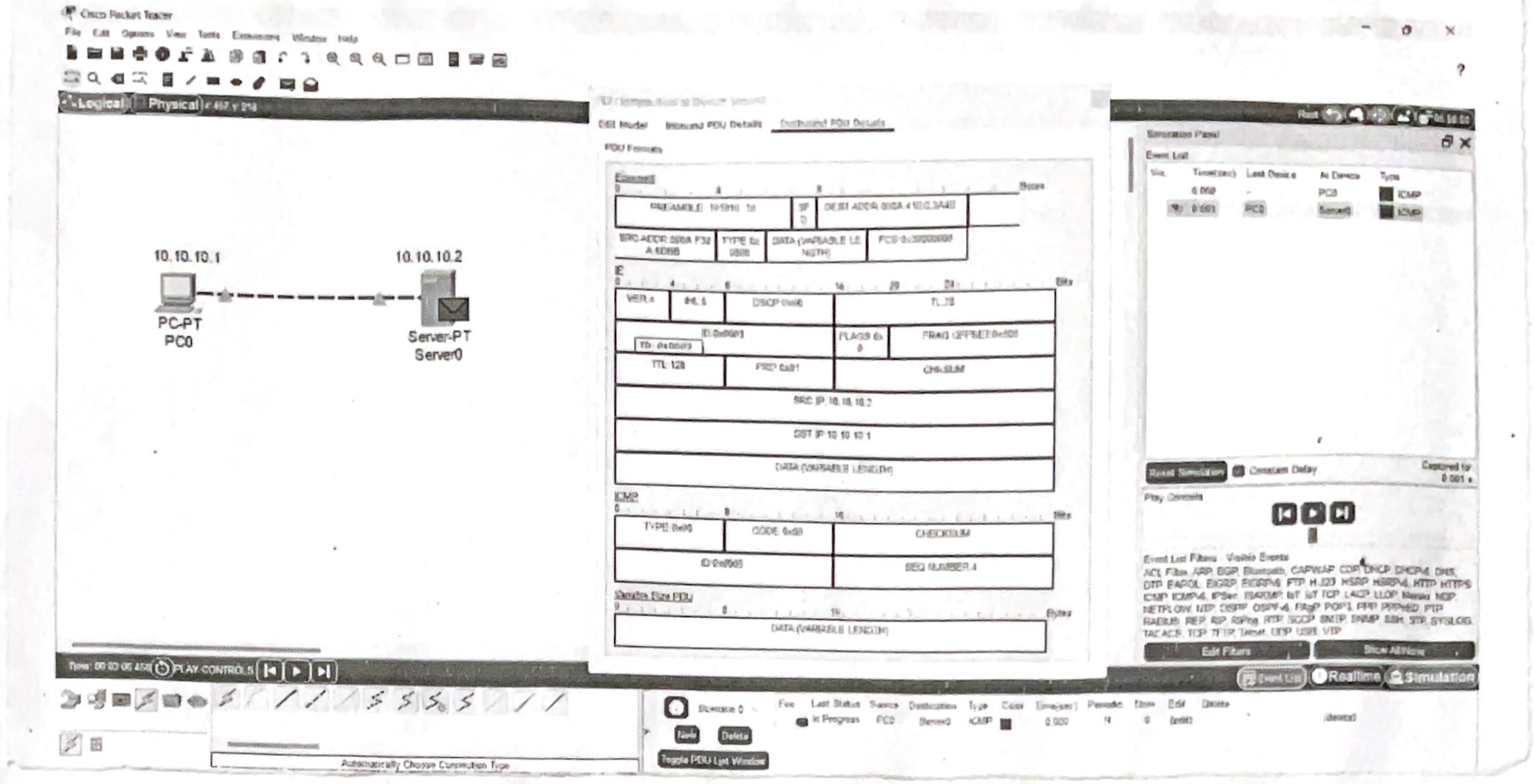
a) Connection between a host and a server by assigning both of them a IP address

i) Transferring a bit of message to the server.

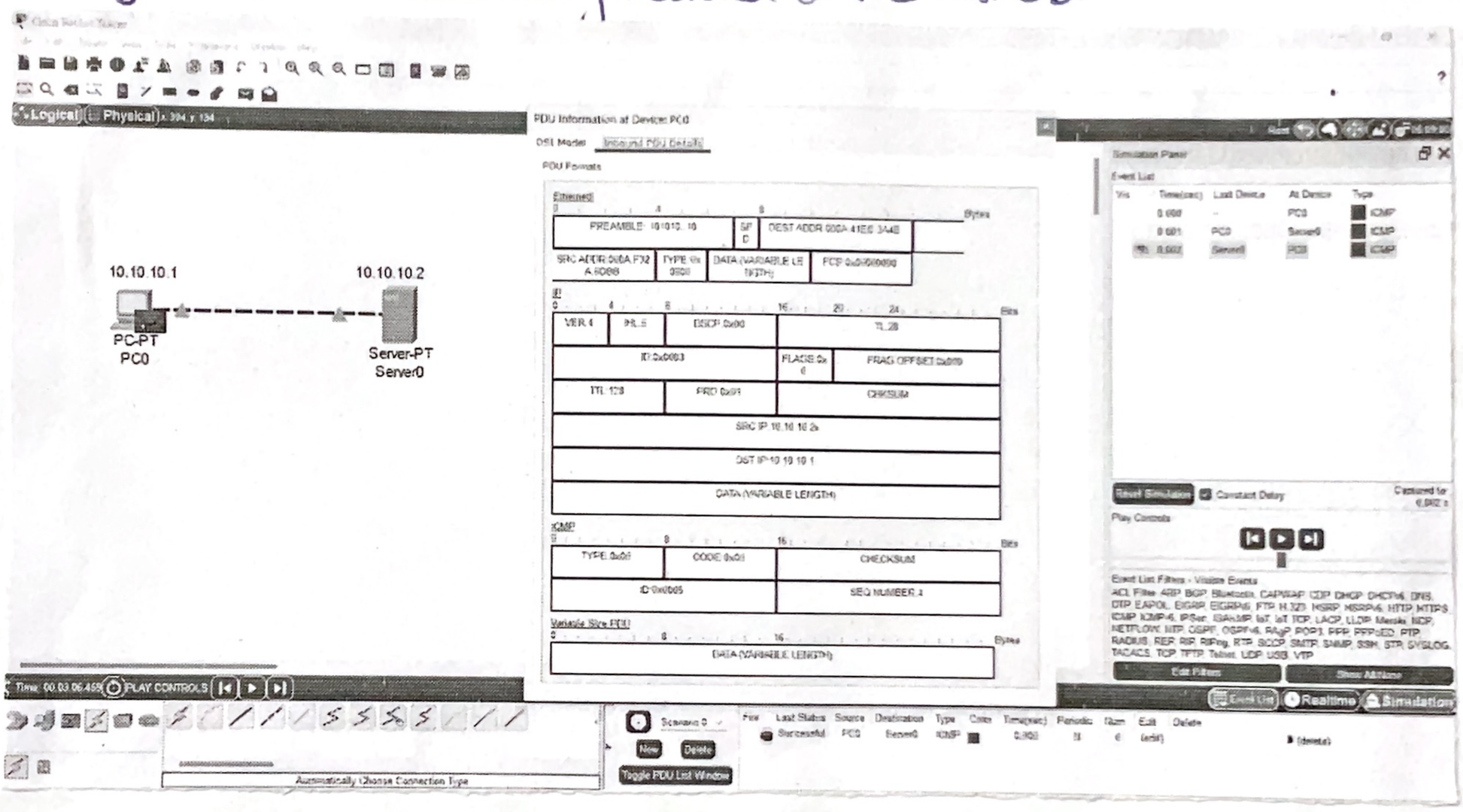


ii) Recieving the message from the host





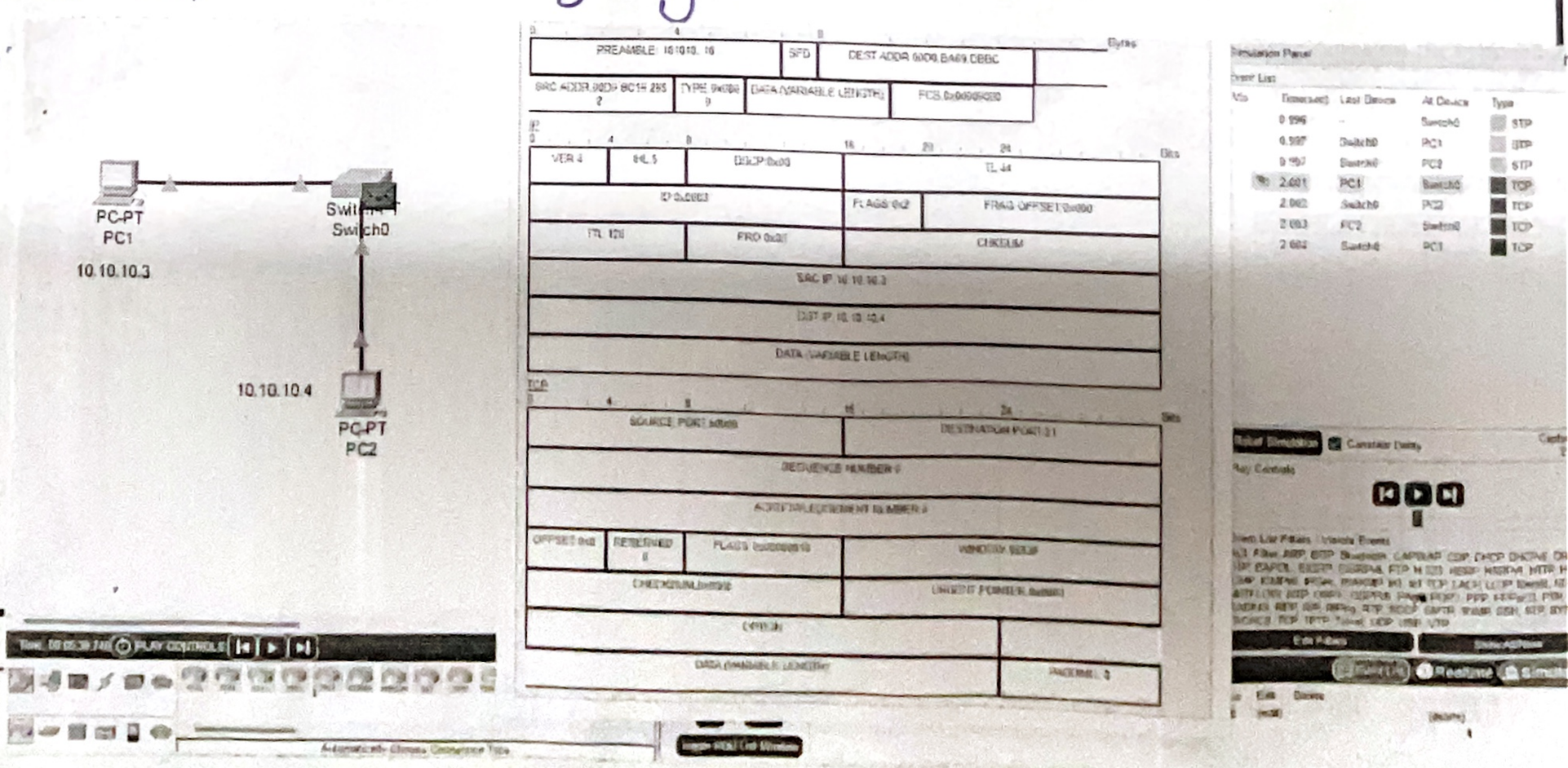
b) Message has been successfully recieved at the hostend.



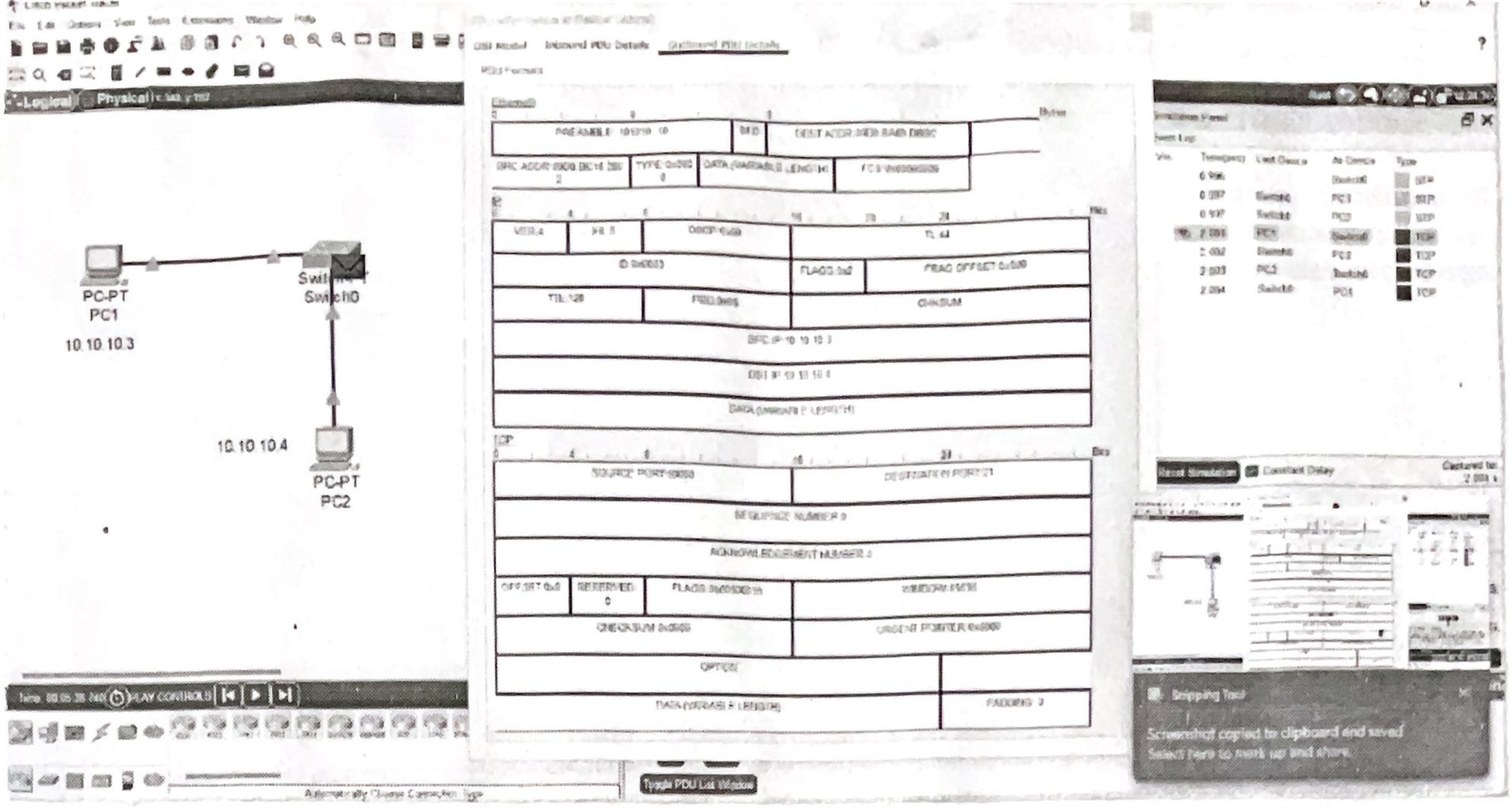
Objective 3 → Simulating the Ethernet by transmitting ICMP, FTP and TFTP messages between two end devices.

a) Connection between two host PCs by using a switch between them with different IP address.

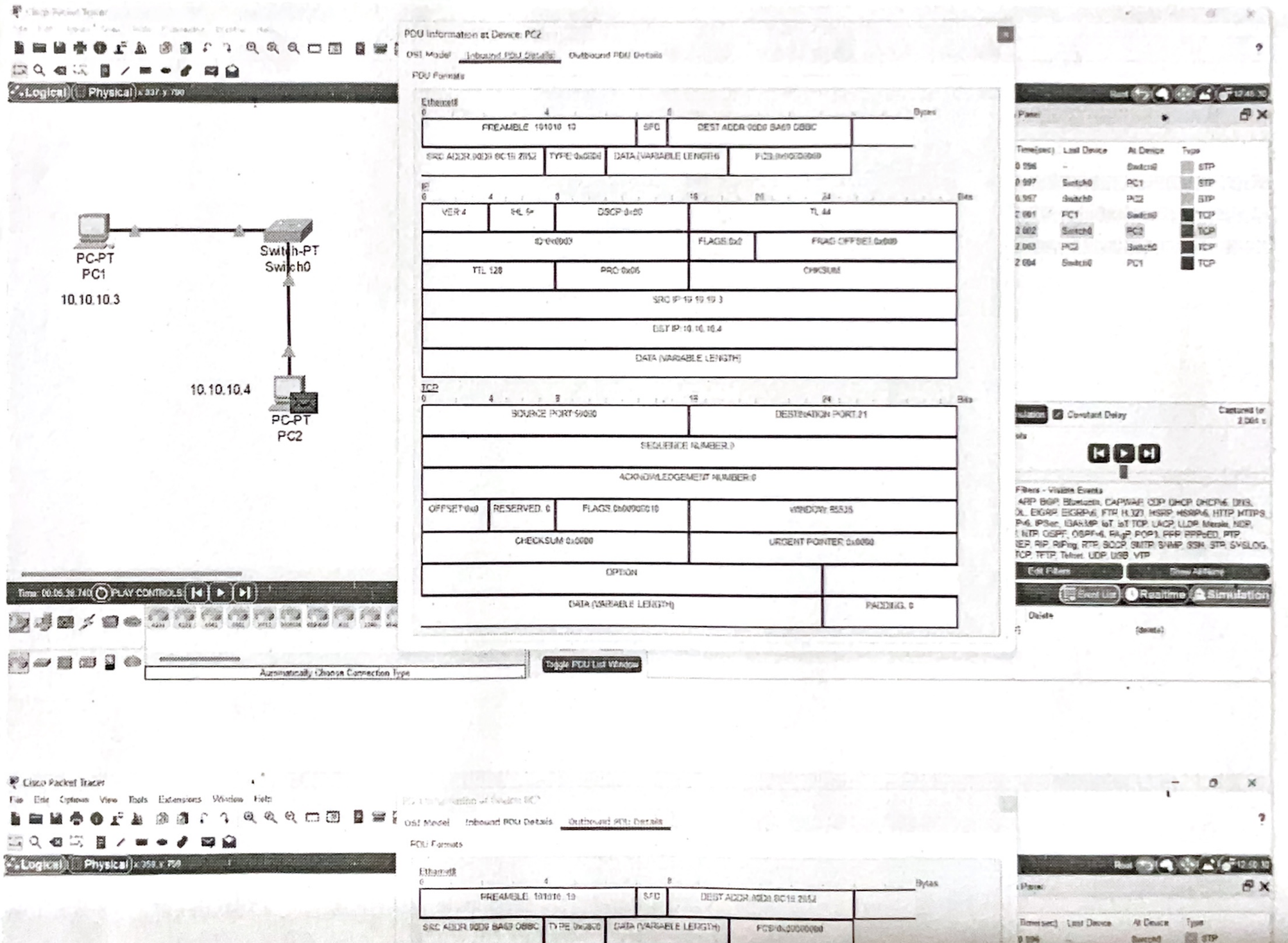
Through FTP protocol

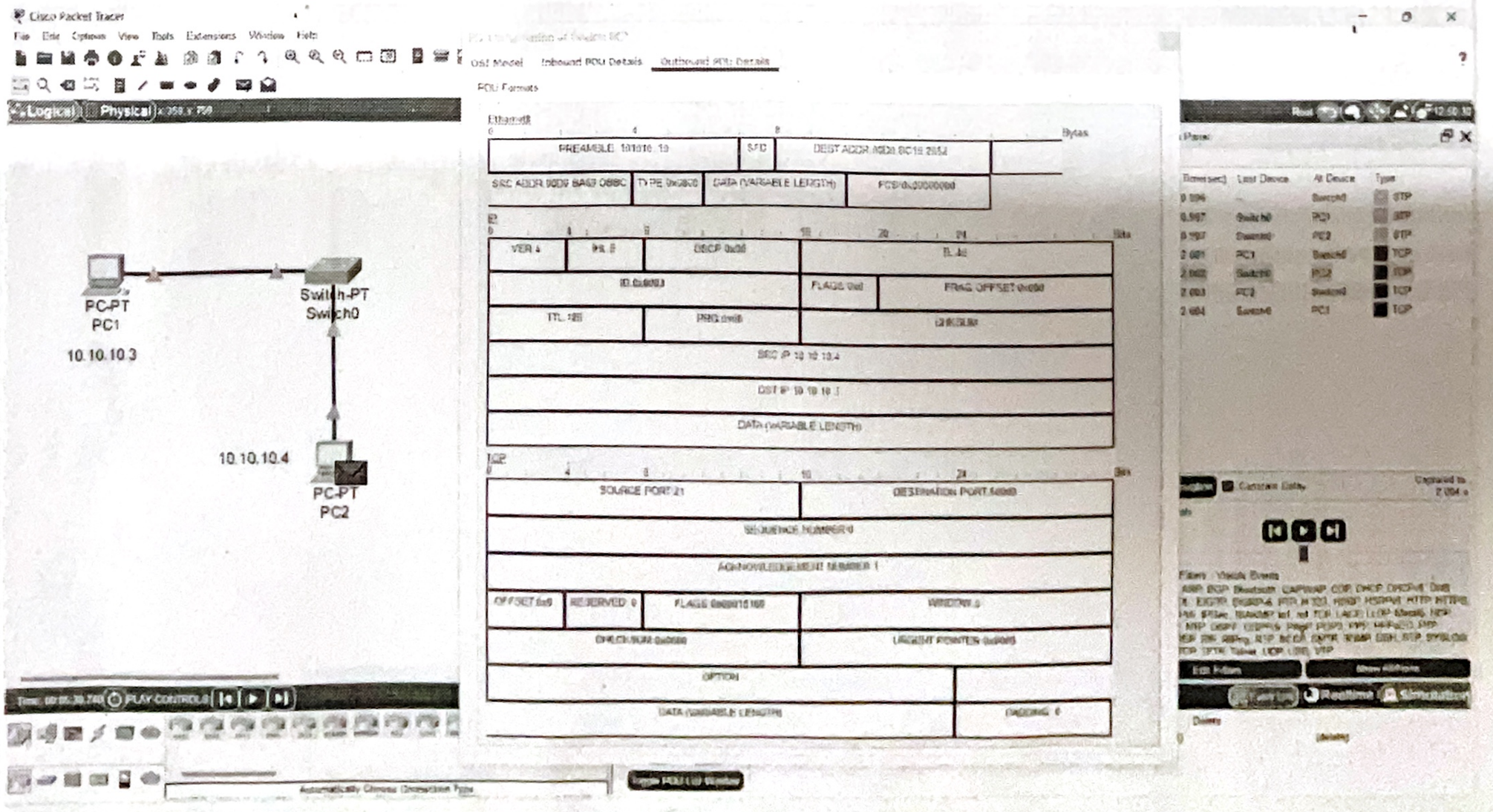


Name: ———

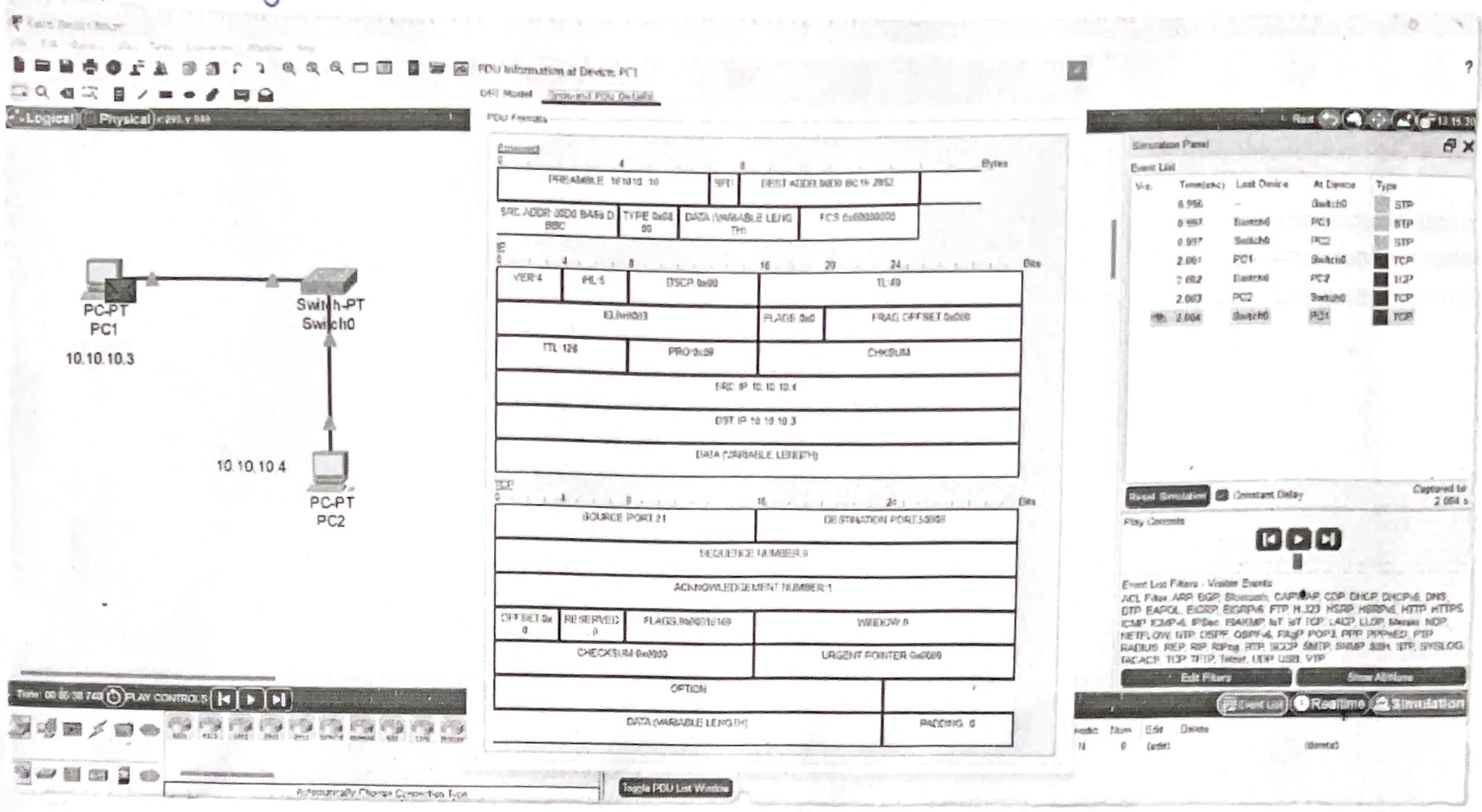


b) Transfer of message from Server to host 2

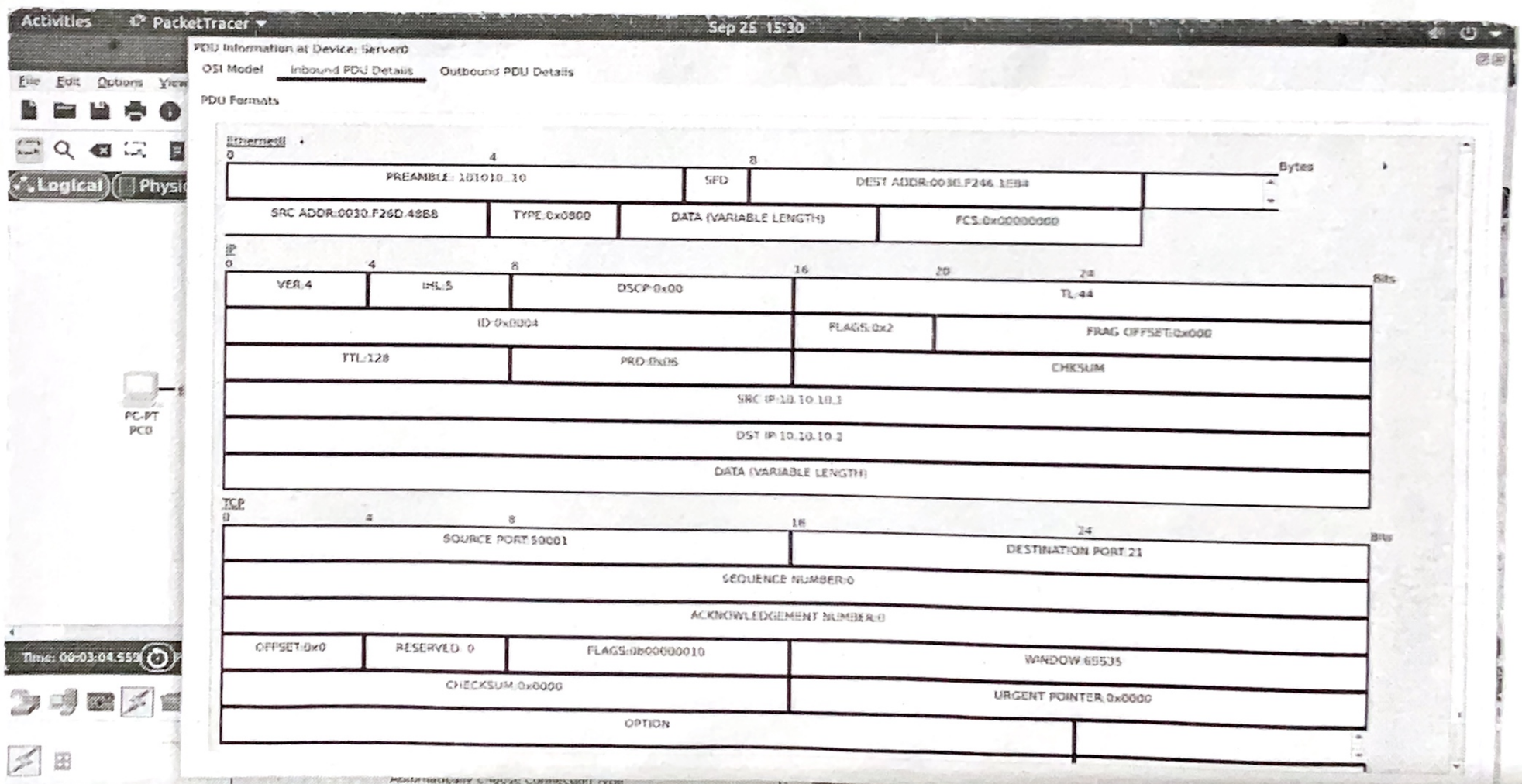


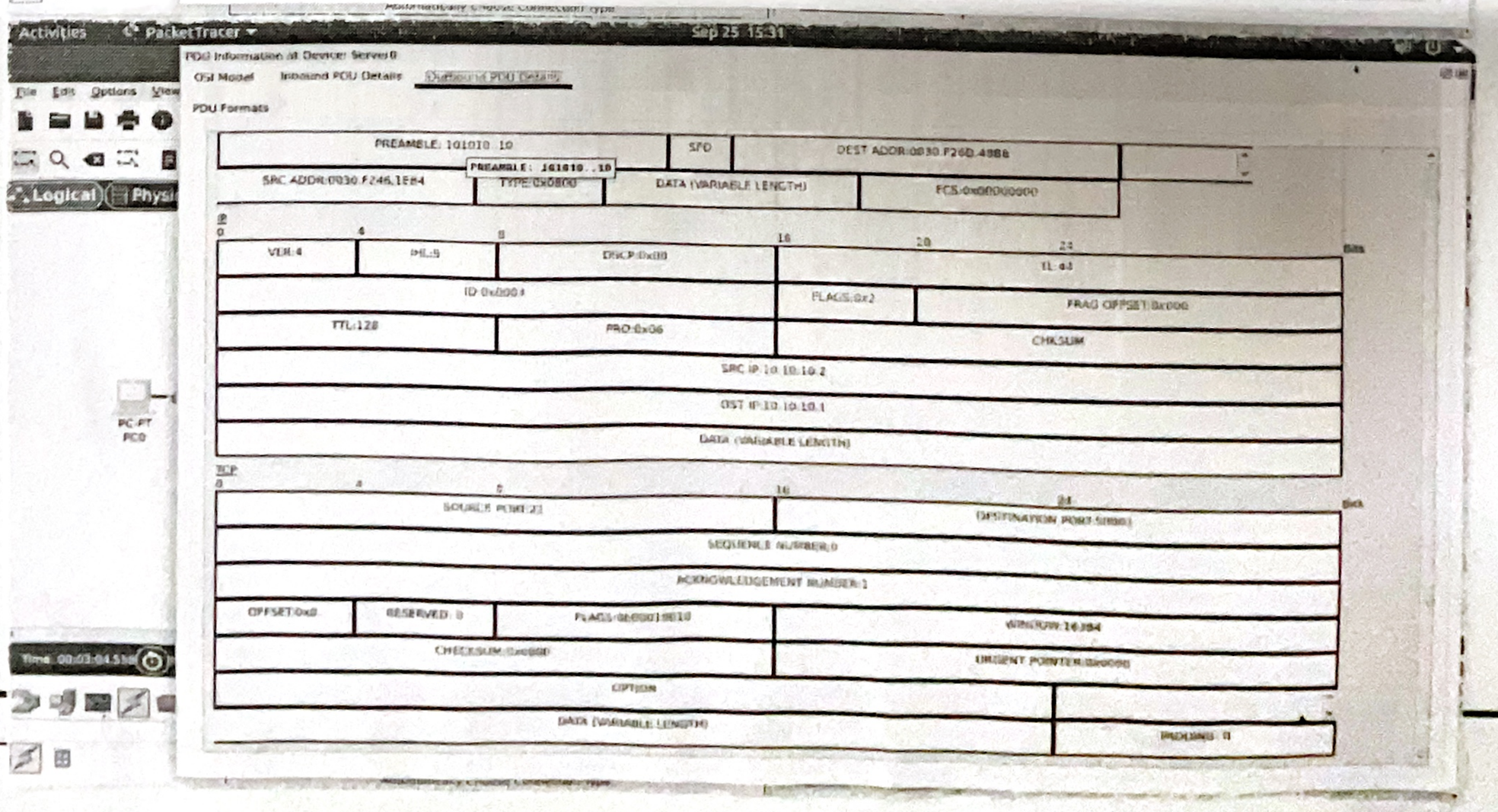


c) Finally message recieved in Host 1



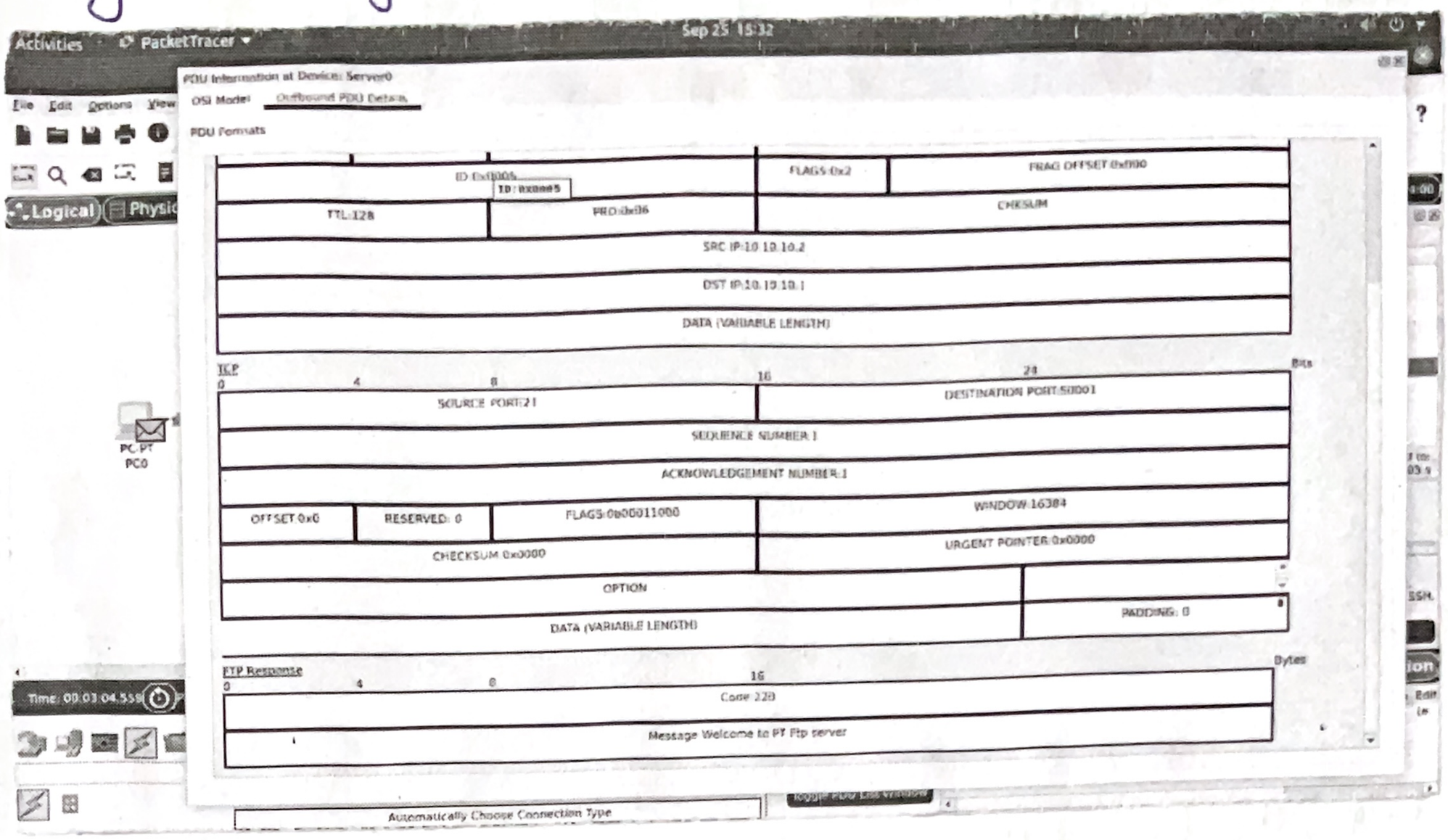
d) Connection between 2host PCs using server in between through TFTP protocol →





Name: —

e) Recieving the message back in Host 1



Objective 4 → Understanding and analyzing different fields of IP, TCP and UDP headers after simulation.

→ Packet ~~Fraudsr~~ Inspection → Use packet tracere simulation mode or wince to capture packets This allows you to view the header in real time.

→ For IP headers: Check the source and destination IP address to verify routing and connectivity.

→ For TCP headers? Analyze the sequence and acknowledge numbers to understand the flow of data and ensure reliable delivery.

→ For protocol identification use the protocol field in the IP header to determine if the data using TCP or UDP, which impacts how data is managed and transmitted.

→ This knowledge is foundational for anyone working in networking and network administration.

Conclusion → Implementing basic ethernet using Cisco Packet Tracer provides practical experience in configuring network devices and understanding communication protocols. This hands-on approach enables detailed analysis of IP, TCP, and UDP headers, enhancing knowledge of data transmission and error handling.

Exercises →

Q1) Given the value available in "fragment offset" field of IP header is 100. What is the number of bytes ahead of this fragment?

Ans → Given that, IP header = 100

The offset is measured in 8-byte blocks.

So, bytes = 100 × 8 = 800 bytes.

Q2) An IP packet has arrived with the first 8 bits as 01000010. What is the version and the header length?

Ans → Given, IP Packets : 0100 0010

Here, the first 4 bits represent the corresponds to version 4 (0100) that IP version (IPv4)

→ For header length: 0010 represent the header length in 32-bit words.

$(0010)_{\text{e2}} = (2)_{10}$

Header length = 2 × 4 = 8 bytes

Q3) A TCP header in hexadecimal format is given as below:

05320017 00000001 00000000 500207ff 00000000

a) What is the source port number?

Ans → The first 16 bits (4-hexadecimal) digits are:

$0532 = 2 \times 16^0 + 3 \times 16^1 + 5 \times 16^2 + 0 \times 16^3$

$= 2 + 48 + 1280$

$= 1330$

b) What is the destination port number?

Ans → Here, next 16 bits are

$0017 = 7 \times 16^0 + 1 \times 16^1 + 0 \times 16^2 + 0 \times 16^3$

$= 7 + 16$

$= 23$

c) What is the length of the header?

Ans→ Here, header is = 5002

1st hex digit = 5 = (0101)

Header length = 5 x 4 = 20 bytes

d) What is the window size?

Ans→ Window size found in the next 16-bits after header length.

$07ff = f \times 16^0 + f \times 16^1 + 7 \times 16^2 + 0 \times 16^3$

$= 15 + 240 + 1792$

$= 2047$

4) Given a UDP header in hexadecimal format 06 32 00 0D 00 1C E2 17. Find the following:

a) Source port number.

Ans→ The first 16-bit digit are: 0632 = $2 \times 16^0 + 3 \times 16^1 + 6 \times 16^2 + 0 \times 16^3$

$= 2 + 48 + 1536$

$= 1586$

b) Destination Port number.

Ans→ Next 16-bit after source port are: 000D = $D \times 16^0 + 0 + 0 + 0$

$= 13$

c) Length of User Datagram.

Ans→ Next 16-bits are 001C = $C \times 16^0 + 1 \times 16^1 + 0 + 0$

$= 12 + 16$

$= 28$ bytes

d) Length of the data.

Ans→ Length of the data = Total length − Header length

$= 28 - 8$

$= 8$ bytes