Lab Exercise 3: Using Wireshark to Analyze a Packet Capture File (15 pts.)

What You Need

- A Computer running any OS. I wrote the instructions for Windows 7.

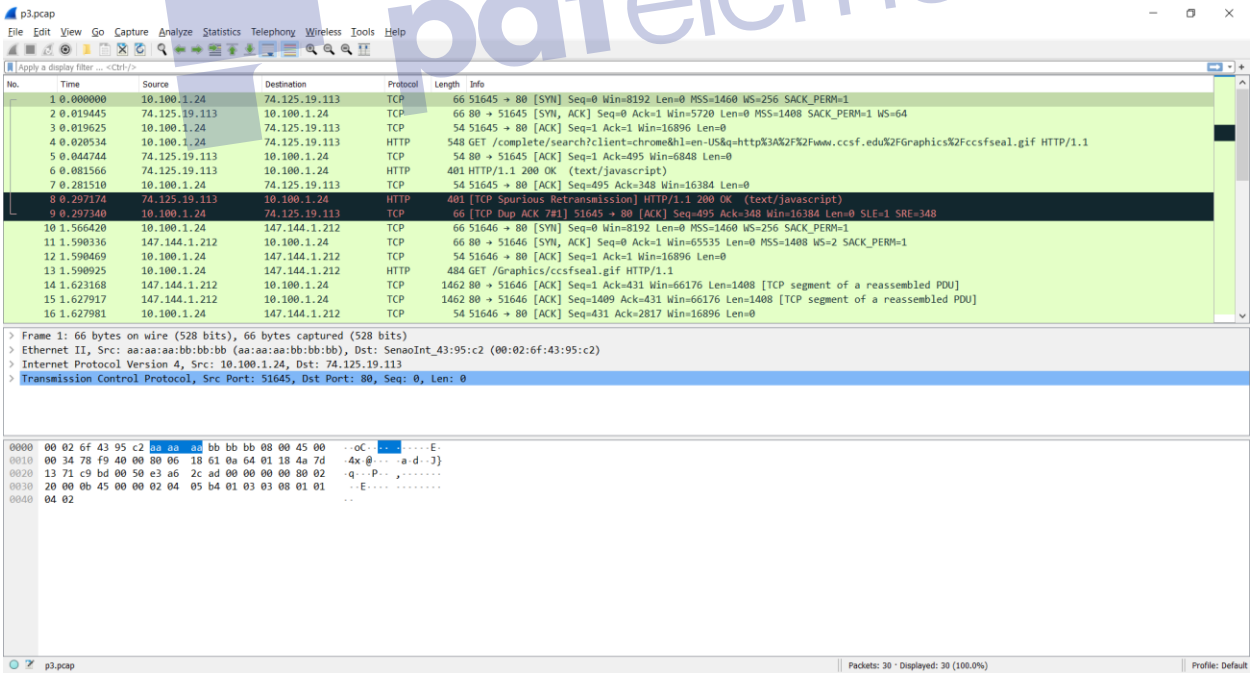
Purpose

You will be examining a saved packet capture file with Wireshark, to practice finding information from it.

Downloading the Packet Capture File

Click the link presented on the instruction and save the capture file on your desktop.

On your desktop, double-click the **p3.pcap** file. The file opens in Wireshark, as shown below on this page.



Analyzing the Packet Capture File

Examine the wireshark window and find answers to the following questions:

A. This packet capture file contains two TCP handshakes. Find the first handshake and write down the packet numbers of those packets (the column labeled "No.").

Answer:

1	0.000000	10.100.1.24	74.125.19.113	TCP	66 51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 80 → 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0

B. In this session, a client machine initiated a connection to a server and then downloaded a file. What is the client's IP address?

Answer: 10.100.1.24

C. How many HTTP GET request packets are there?

Answer: 2

D. Find the first HTTP GET request packet. What was the server's IP address? (The server is the Destination).

Answer: 74.125.19.113

E. Examine the first packet. Look at the center pane in Wireshark. How many bytes were sent on the wire to form this packet?

Answer: 32 bytes

Turning in Your Project

Save this file using the format **LabExer3_[YourName]** and upload to Canvas.