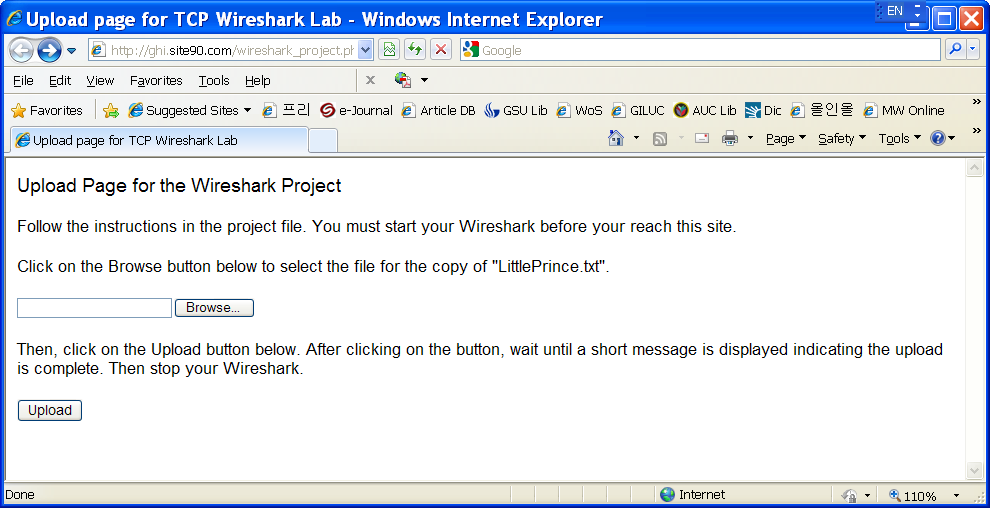
Wireshark Project

Instructions:

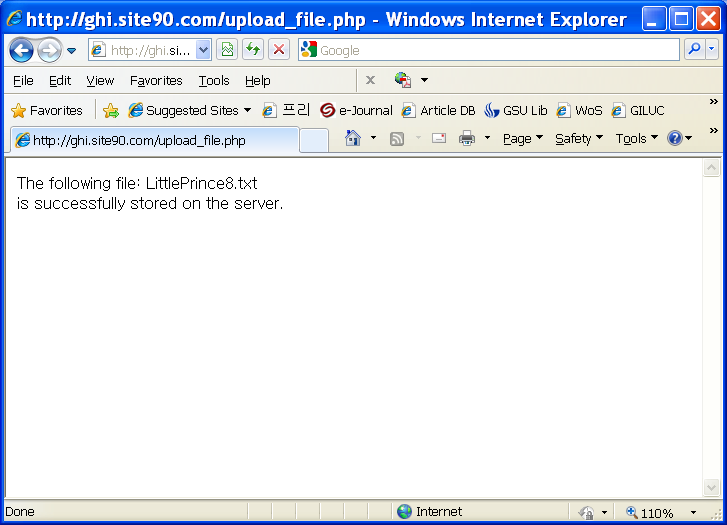
1. Use a computer in your home. Your computer must be connected to the Internet using a LAN cable. To capture live wireless traffic, you need to install airpcap driver with cost. If you use a computer in the Davidson 304, you will get traffic that contains lots of noise and have a hard time in filtering out the background traffic.
2. Use the attached file (LittlePrince.txt) to upload. Change the file name to LittlePrince\_###.txt, where ### is your first initial and last name. If you should upload multiple times, change the file name by adding a number (e.g., LittlePrince\_gim\_1.txt, LittlePrince\_gim\_2.txt). The website does not accept the same file name.
3. When you capture the traffic, capture all traffic and do not use Capture Filters.
4. Submit the original pcap file that contains the whole traffic. Follow the naming convention (wireshark\_###.pcap, where ### is your first initial and last name; e.g., wireshark\_gim.pcap)
5. Answer the questions below and submit your answers in a word file. Follow the naming convention (wireshark\_###.docx, where ### is your first initial and last name; e.g., wireshark\_gim.docx)
6. Submit your answers online and bring a hard copy to the class on Monday, Oct 4th.
7. Submit using Assignments / Wireshark Project link. *No email submission, please!!*
8. This is an individual assignment and collaboration is not allowed.
9. In the lab session, we haven’t covered all the necessary features in Wireshark that are necessary to answer some of the questions below. You are asked to navigate the menus and figure out the solutions by yourself.
10. FYI, I attached DisplayFilter.pdf on the project section. Review it quickly to understand how you can use filters to isolate the unnecessary traffic. You can use Capture Filter at the time of capturing the live traffic. However, in general, capture all and analyze later using Display Filters. Capture and Display Filters work similarly.
11. Refer to “WireShark\_Lab.docx” posted on the Wireshark Lab section as necessary.
12. Contact me if you need clarification.

Do the following:

1. Retrieve the “LittlePrince.txt” file from the Blackboard and change the file name to yours.
2. Start your Wireshark. Go to Capture / Interface / Select your LAN and Start.
3. Start your browser and go to <http://ghi.site90.com/wireshark_project.php>. Do not go to this site in advance. If you do, you will not capture the DNS traffic.



1. Click on the Browse button to select the file.
2. Then, click on the Upload button.
3. After clicking on the button, wait until a short message is displayed indicating the upload is complete. Then stop your Wireshark on Capture Interfaces by clicking on Close.
4. Save the pcap file on your hard drive.



Answer all the questions.

1. What is the IP address and TCP port number used by your computer (client)? What is the IP address and TCP port number used by the server? (6 points)

Client IP: 192.168.131.129

Client Port: 49485

Server IP: 208.122.28.11

Server Port: 80

1. Can you read the content of the file “LittlePrince.txt” through the packet(s) that you captured? (6 points)

Yes, in packet number 232 there are complete uploads of the entire file.

1. Take from the initial three TCP packets (SYN, SYN/ACK, ACK) to the second HTTP packet (i.e., HTTP/1.1 200 OK). Explain how the sequence and acknowledgement numbers for these packets are arranged? Explain them using absolute sequence numbers. (10 points)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Packet no** | **Protocol** | **SYN no** | **ACK no** | **Description** |
| 11 | TCP | 0 | 0 | Cannot find the Absolute Number for these due to the program |
| 12 | TCP | 1 | 414 |  |
| 13 | TCP | 1 | 414 |  |
| 14 | TCP | 1461 | 414 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. We see a lot of the TCP segments of a reassembled PDU. Examine only the TCP segments related to the file uploading. Are these reassembled eventually? (6 points)

Yes, in the packet number 232 all of the segments are located in the same frame.

1. Can you isolate the TCP stream that is related to the uploading of the text file? What filter do you use to achieve this? (6 points)

Yes, the filer is tcp.stream eq 3

1. In your TCP packets, how many errors and warnings did you receive? (6 points)

I had 14 Errors and 46 warnings

1. How do you know round trip time (RTT) of the TCP stream? RTT is the time between the data packet to the corresponding ACK packet. Can you display it? You don’t need to calculate the exact RTT. (6 points)

My round trip time graph was unavailable although I have taken a screen shot and attached it to the assignment on blackboard.