CSCE 560
Homework / Wireshark Instructions

Submit the homework and lab as separate documents. In other words, you will submit two stapled documents—one homework solution and one Wireshark solution.

Homework

You must include the questions in your submitted solution. Your submission must include the question listed followed immediately (inline) by your solution with the answer clearly indicated (e.g., put a box or circle around the final answer). You cannot simply staple my list of questions to the end of your answers.

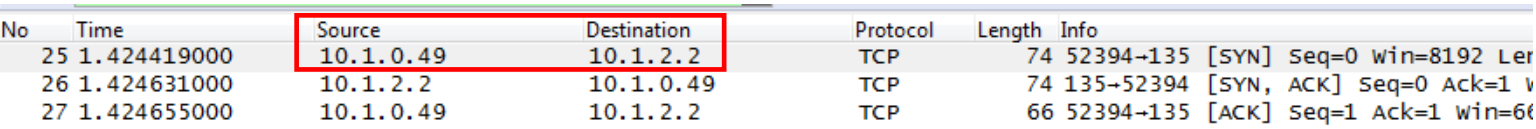
Wireshark Labs

You must include the questions from the handout in your submitted solution. Your submission must include the question listed followed immediately (inline) by your solution with the answer clearly indicated (e.g., put a box or circle around the final answer).

Provide screenshots of the packets you used to answer the questions. A screenshot is not a printout of the packet. Crop and size the image so it is legible. Highlight the pertinent information with color or a red box.

For example, if the question is "What is the source and destination IP address?", you must explicitly answer the question in your own words followed by the screenshot as shown:

What is the source and destination IP address?
The source IP address is 10.1.0.49, and the destination IP address is 10.1.2.2.



No	Time	Source	Destination	Protocol	Length	Info
25	1.424419000	10.1.0.49	10.1.2.2	TCP	74	52394→135 [SYN] Seq=0 Win=8192 Len
26	1.424631000	10.1.2.2	10.1.0.49	TCP	74	135→52394 [SYN, ACK] Seq=0 Ack=1 W
27	1.424655000	10.1.0.49	10.1.2.2	TCP	66	52394→135 [ACK] Seq=1 Ack=1 Win=66

You cannot load Wireshark on AFIT EDU machines because you must have administrator rights. I suggest you load and run it on your home computer. Besides completing the assignment, you'll be able to see the traffic entering and leaving your home system.

If you are unable or unwilling to load it on your home system, see me. I'll let you use our CDN network. I think you'll find your home network much easier to use however since the volume of traffic is significantly less. For example, a typical CDN computer will see at least 15 packets per second! That's a lot of unnecessary clutter.