DFSC1316: Digital Forensic and Information Assurance I

Lab 1 (Due 9/29/2017 23:59:99)

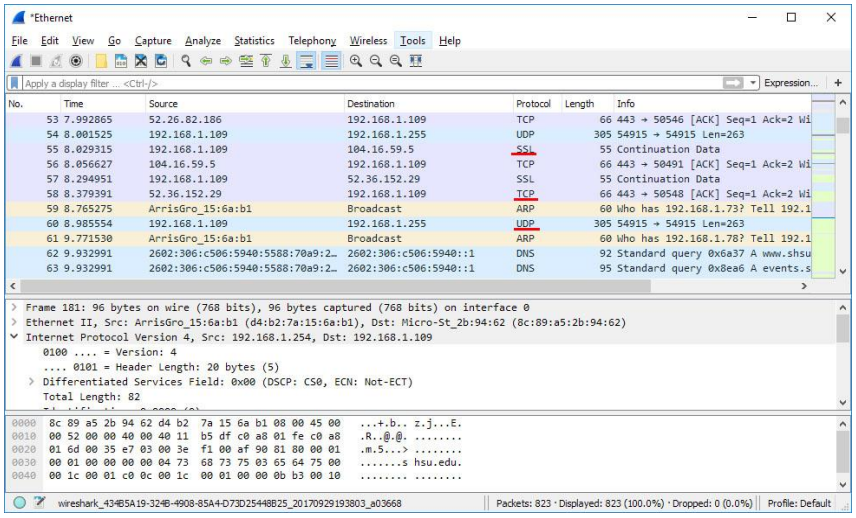
Rules:

1. All you answers will be typed unless otherwise being advised.
2. Submit you assignment in PDF version (Office word can be directly saved as PDF, or you can use virtual PDF printer to 'print' it as pdf).

---

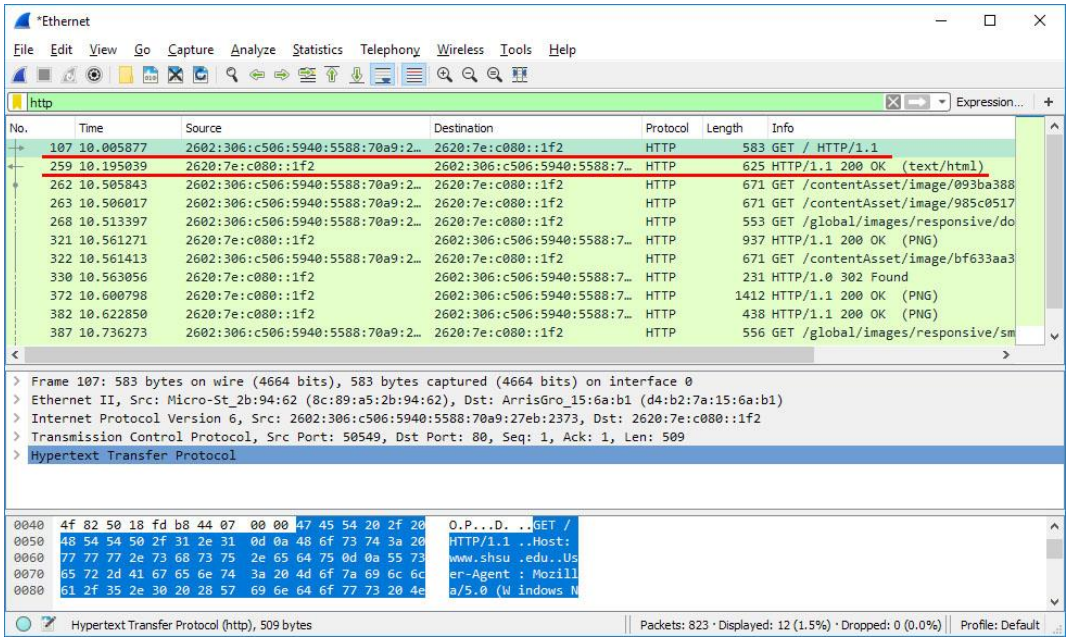
1. **(25pts) List 3 different protocols that appear in the protocol column in the unfiltered packetlisting window in step 7 above. Mark them in the screenshot.**

   TCP, UDP, SSL.



2. **(25pts) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? Clearly mark the packets in the screenshot (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.)**

   It took 0.189169 seconds between packets.



3. **(25 pts) What is the Internet address of www.shsu.edu? What is the Internet address of your computer?**

   www.shsu.edu is: 2620:7e:c080::1f2
   my computer is: 2602:306:c506:5940:5588:70a9:27eb:2373

4. **(25pts) Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only*" and *"Print as displayed"* radial buttons, and choose to print as a PDF file. If you do not have a PDF printer on your computer, you may need to install one, such as Foxit PDF reader/printer.**

   Attached in file upload

5. **(Optional, no points) Find one message at your choice, other than a HTTP message, find out what is the source and/or destination, and try to explain why this message has been sent (e.g., what application may have sent it, where it was sent to, etc.)**