**CSCI 530: Security Systems**

**Lab Assignment 5: Wireshark, Due: November 1st, 2024**

**Name: Anne Sai Venkata Naga Saketh**

**USC Email:** [**annes@usc.edu**](mailto:annes@usc.edu)

**USC ID: 3725520208**

**Assignment Questions:**

1. The number of bytes in the echo protocol exchange in section 4 above, according to the "Follow TCP Stream" window, is ***\_14 bytes\_***
2. The number of bytes in the echo protocol exchange in section 4 above, according to the Statistics/Conversation List/TCP window, is ***\_888 Bytes \_***
3. The iptables command syntax to create a firewall rule prohibiting use of the standard echo protocol (Section 6 above) is:

A screenshot of a computer

Description automatically generated

1. ***OMITTED - Do not answer this question.***
2. The number of frames in section 9's data stream was ***\_\_1350\_\_***
3. The average length/size (in bytes) of the frames in section 9's DataStream was  ***\_\_1012.45\_\_***
4. The most common frame size among the frames in section 9's DataStream was ***\_\_1513.96 (~1514 bytes)\_\_***
5. The maximum frame size among the frames in section 9's DataStream was ***\_\_1513.96 (~1514 bytes)\_\_***
6. For any of those max-sized frames, the size of  its ethernet payload portion was ***\_\_\_1500\_\_\_***
7. For that frame, the size of the remainder of the packet (i.e., its header) was ***\_\_14\_\_***
8. For that frame (and all the others like it) Wireshark names its highest-level payload (see the packet details pane). It's ***\_\_\_\_FTP\_\_\_\_***
9. The observed value of the maximum frame size is interesting. It could not be any larger because (consider the reference graphic that follows):

***Answer: The standard maximum transmission unit (MTU) for Ethernet frames, which is 1500 bytes for the payload + 14 bytes for the Ethernet header, is represented by the observed maximum frame size of 1514 bytes, making it noteworthy. Because it complies with the Ethernet MTU, the frame size limit specified by the Ethernet standard, this maximum frame size could not be greater.***

For reference, question 12:

A screenshot of a computer

Description automatically generated

1. At the bottom of your file, insert two screen captures you made:  
      - the one you generated in section 7 above (telnet login showing cleartext password)  
      - the one you generated in section 10 ("snakeoil" tls decrypt)

**Section 7 Screenshot with the password:**

A screenshot of a computer

Description automatically generated

**Section 10 Screenshot with the decrypted TLS Stream:**A screenshot of a computer

Description automatically generated