SY205 – Net: OPS & Analysis Name(s): _____

Alpha(s): _____

Assignment Type:	Assignment	Collaboration Policy:	Default
Assignment Title:	Packet Analysis Fundamentals		

Wireshark Introduction

1. (5) Complete the below regarding Wireshark under Ubuntu 18.04 LTS in the networking lab room.

   a. [2 / __ / 0] What is the full path for Wireshark?

   b. [3 / __ / 0] What version of Wireshark is installed under Ubuntu 18.04 LTS?

2. (5) Complete the below regarding Wireshark using the provided pcap.

   a. [3 / __ / 0] The hexadecimal section of the *packet bytes* pane in Wireshark contains two groupings of hex values. How many bytes are represented in a single grouping of hex values?

   b. [2 / __ / 0] In the *packet bytes* pane, what character is displayed if the associated byte is not a printable or is an invalid ASCII character?

3. (5) Complete the below regarding Wireshark using the provided pcap. The background of the bytes in the *packet bytes* pane change color based on data selected within Wireshark.

   a. [2 / __ / 0] What does the background color of the protocol bytes change to when a protocol field (not an entire protocol) is selected in the *packet details* pane?

   b. [3 / __ / 0] What does the background color of the protocol field bytes change to when a protocol field (not an entire protocol) is selected in the *packet details* pane?

4. (5) Select the first packet (Frame 1) in the provided pcap, and complete the below.

a. [2 / __ / 0] In the Ethernet frame, how many bytes does the *type* protocol field take up?

b. [1 / __ / 0] In the Ethernet frame, what are the byte offsets of the *type* protocol field? Hint: Look at the information provided in the status bar at the bottom of the Wireshark window.

c. [2 / __ / 0] What are the associated byte values for *IPv4* in the Ethernet frame type protocol field?

5. [5 / __ / 0] In your own words explain what information changed in the *packet list* pane. Explain what resource Wireshark was using to determine the information displayed. Use complete sentences, spelling and grammar count.

6. [5 / __ / 0] In your own words explain what information changed in the *packet list* pane. Explain what information changed in the *packet details* pane. Use complete sentences, spelling and grammar count.

Packet Filtering and Analysis

7. (5) Complete the below using the `arp-only.pcapng` pcap file.

a. [2 / __ / 0] How many bytes are in the pcap file?

b. [3 / __ / 0] What is the first packet number in the pcap file?

8. (5) Complete the below based on the display filter generated in Wireshark.

a. [2 / __ / 0] Write the display filter that was generated, i.e. currently listed, in the filter bar.

b. [3 / __ / 0] In your own words explain whether, and why, you think the Wireshark developers intend for Wireshark users to have or to *not* have some (even a little) programming experience. Use complete sentences, spelling and grammar count.

9. (5) Complete the below based on the applied display filter.

a. [2 / __ / 0] How many packets meet the filter criteria; i.e. how many packets are displayed while the filter is applied?

b. [3 / __ / 0] What percentage of packets within the entire pcap are destined for MAC address `ff:ff:ff:ff:ff:ff`?

10. [5 / __ / 0] This is an applied question. Regarding a broadcast message, what resource utilization benefits are there with a receiving host not replying to a broadcast query that they do not know the answer to?

11. [5 / __ / 0] Read the packet information, and analyze the data in the protocol fields of the ARP request. Why does it make sense that the *Target MAC address* field is all 0's in the ARP request message? Use a complete sentence, spelling and grammar count.

12. (5) Complete the below based on the `eth.type == 0x0800` display filter entered in Wireshark.

a. [2 / __ / 0] How many packets are displayed when the filter is applied?

b. [3 / __ / 0] In your own words, explain what the filter means? Use a complete sentence, spelling and grammar count.

13. (5) Complete the below based on the display filter you created and applied.

a. [2 / __ / 0] Write the display filter you created below.

b. [1 / __ / 0] How many packets met your display filter criteria?

c. [1 / __ / 0] What is the highest layer protocol all of those packets have in common?

d. [1 / __ / 0] What TCP/IP Stack layer does that protocol operate at? You don't need to look up information about the protocol to answer this question. Hint: What address schemes do we use at the different layers of the TCP/IP Stack?

14. (5) Complete the below based on the statistics reports for the pcap file.

a. [2 / __ / 0] What packets include comments?

b. [1 / __ / 0] What report provides an overview of the protocols used in the pcap?

c. [2 / __ / 0] What report can be used to analyze pairs of communicating hosts?

Packet Capturing

15. (5) Complete the below based on the HTTP display filter while capturing packets on the Ethernet interface.

a. [2 / __ / 0] When did Wireshark start displaying packets in the packet list?

b. [1 / __ / 0] Based on the HTTP traffic, what is the IP address of the webserver?

c. [2 / __ / 0] Which stream should be followed to see the website source material in a human readable format?

16. [5 / __ / 0] Write a command line to display unique pairings of Ethernet addresses from the HTTP traffic that is sorted.

17. [5 / __ / 0] Compare the results with the command sequence from the previous question with the contents of `httpHostARPCache.txt`. What is the IP address of the remote host that the packets are being sent to at the Data Link layer (local network).

18. [5 / __ / 0] Write a command line to display unique pairings of HTTP host names and IP addresses from the HTTP traffic that is sorted.

19. [5 / __ / 0] Based on the HTTP traffic, what is the host name of the webserver?

20. [5 / __ / 0] Based on `dig`, what is the host name of the webserver? Hint: Review previous assignment activities to refresh your memory of `dig` options, or read the man page.