SY310 Lab - Wireshark Intro

1. (5 points) In the main window, why do the MAC addresses change when you select/de-select the resolve MAC address option? How does Wireshark know how to make this resolution? Note: To see the changes without closing the preferences-window, hit apply.

The MAC address changes when you select/deselect the MAC address to a format where some of the numerical values are turned into a more readable format. Wireshark makes this resolution by having a memory of common MAC addresses for example broadcasting.

2. (5 points) What changed in the Packet List pane? Why did it change?

When I used this function the destinations that were broadcast changed color to a light grey. It was the only broadcast address that changed. They changed because they are an ARP protocol so the function blurs out these addresses.

3. (5 points) How many bytes is the arp packet file you saved?

60 bytes

4. (5 points) What is currently displayed in the Filter Window?

The current display darkens frame 2 which is the Ethernet II address

5. (5 points) What did this do? What type of address is this? Hint: Look at the filter.

When I apply the filter it only displays frame two, which is the Ethernet II address

6. (5 points) How many total packets are in this pcap? How many are currently displayed?

When selecting the source IP for packet 7, 16 packages are displayed

7. What is the protocol? How many packets contained this protocol in our pcap?

This is still the Internet Protocol Version 4, there are 12 packets contained in this protocol

8. (5 points) What does that filter mean?

The filter is the EtherType is the last two bytes in the Ethernet/IEEE 802.3 header, meaning that the next byte in the stream will be the first byte in the header of the next higher protocol.

9. (5 points) What is the difference in the two query results (eth.type != 0x800 and eth.type == 0x800)?

The difference between the two query's is display EtherTypes and displaying non EtherTypes

10. (5 points) Create a filter for all IP traffic coming from the IP address 24.6.170.101 and not going to destination MAC address ff:ff:ff:ff:ff:ff. What is the filter? What is the name of the Protocol for the resulting frames/packets?

This filter allows for the IP traffic of the specific address 24.6.170.101, but it does not display the broadcasting addresses. This is a ARP protocol

11. (5 points) How many bytes were highlighted? What field was highlighted in the Packet Details pane? What was highlighted in the ASCII portion of the Packet Bytes pane?

6 bytes were highlighted. In the packet detail pane that was highlighted is under the Ethernet II and it is the individual address (unicast). The highlighted ASCII portion is .#T

12. (5 points) Which tool provides an overview of the protocol usage seen in the packet capture? Which tool is useful for identifying common source and destination pairs (two devices communicating with each other)?

The tool that provides the overview of the protocol usage is the Protocol Hierarchy Statistics. The tool useful for identifying common source and destination pairs is the conversations tool