Eddie Mazariegos
Professor Edward Crowley
CIS 3347

Wireshark Video

1. **Who is Gearld Combs?**

- He is the inventor of Wireshark

2. **What does a protocol analyzer like Wireshark do?**

- Wireshark reads the raw data from a network and translates it into a readable format. These data can then be interpreted an analyzed.

3. In the Wireshark Interface, what is the Packet List?

- The packet list displays the summary of each packet captured

4. In the Wireshark Interface, what is the Packet Detail?

- The packet details give more detail to the selected packet.

5. What privileges do you need to run Wireshark? Why?

- You need administrator privileges to run Wireshark. Wireshark analyses network adapters and that requires a high authority.

6. What is a Wireshark display filter?

- Display filter shows the packet that make up that particular stream

7. If you right click on a packet, what are you presented with?

- If you right click on a packet, you are presented with a menu that all allows you do things with the packets

8. Describe the display filter employed when you right click and select "Follow TCP Stream?"

- The display filters shows the conversation between server and web browser.

9. Where can you go to find more information about packet capture with Wireshark?

- You can go to the status bar to find more information about packet capture.