Introduction to Wireshark

Questions:

1. Who is Gearld Combs?

   Gearld Combs is the lead developer of Wireshark and the director of CACE Technologies.

2. What does a protocol analyzer like Wireshark do?

   A protocol analyzer like Wireshark can capture number traffic and show it to us.

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

   The Packet List is the list of packets that are DNS, TCP, and HTTP.

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

   The Packet Detail shows details about the packet such as the host, type, source, and destination.

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

   You need administrative privileges to run Wireshark because without them you won't have access to packet information.

6. What is a Wireshark display filter?

   A Wireshark display filter is a rule such a rule such as coloring that can highlight potential problem.

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

   When you right click on a packet, you are presented with a menu that lets you do things, such as showing you a conversation between the browser and the server.

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

   The display filter employed when you select "Follow TCP Stream" is a window that shows you a conversation between the web browser and the server.

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

   You can go to Wireshark's website to find more information about packet capturing.