Wireshark

1. Who is Gerald Combs?

Combs is the lead developer of Wireshark.

2. What does a protocol analyzer like Wireshark do?

Network capturing device

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

List of each item that was captured on the network

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

Detail information about the selected package

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

Virtual Machines and different operating systems so that your computer stays secure and you don't exploit or compromise the whole system.

6. What is a Wireshark display filter?

Wireshark uses display filters for general packet filtering wile viewing

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

A menu list that lets you perform actions to the packet.

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

It gives you a window that shows you only the packets of all captured that follow a TCP stream.

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

The Wireshark website below can give more information on packet capture. http://www.wireshark.org/docs