Assignment

Introduction to Wireshark

	In this video, Gerald Combs provides a conceptual overview of Wireshark as well as a 'hands on' packet capture demonstration. During the video, Gerald explains how Wireshark can be used for network troubleshooting. Topics include: • Starting Wireshark. • Display filters. • Packet detail. • Color and filter syntax rules. • Capturing packets.

Table 1 *Gerald Combs Introduction to Wireshark Video.*

Wireshark is the world's foremost network protocol analyzer. It allows you to capture, save, and analyze your network's packet traffic. In essence, it changes your network from a black box to something that you can baseline and monitor.

You can find the Introduction to Wireshark video at:
http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/

You can find more information about Wireshark at:
http://www.wireshark.org/docs/

Laura Chappell also has an excellent set of Protocol Analysis resources and videos at:
http://www.wiresharkbook.com/resources.html

Instructions
For this Assignment, you will watch the Introduction to Wireshark Video. Based on that video, please briefly answer the following questions.

When you have completed your answers, save the files to post later to your online portfolio..

Questions

1. Who is Gearld Combs?
2. What does a protocol analyzer like Wireshark do?
3. In the Wireshark Interface, what is the Packet List?
4. In the Wireshark Interface, what is the Packet Detail?
5. What privileges do you need to run Wireshark? Why?
6. What is a Wireshark display filter?
7. If you right click on a packet, what are you presented with?
8. Describe the display filter employed when you right click and select "Follow TCP Stream?"
9. Where can you go to find more information about packet capture with Wireshark?