Assessment Worksheet

Analyzing Protocols with Wireshark

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you exercised a wide variety of capabilities of the Wireshark packet capture and analysis software. In the first part of the lab, you learned about probe placement, clocking and timing issues, Wireshark traffic capture, and the use of filters. In the second part of the lab, you utilized a capture file to answer basic questions about key IP protocols and the basic configuration of the IP hosts from which traffic is captured. Finally, in the third part of the lab, you explored Wireshark on your own to answer a set of challenge questions.

Lab Assessment Questions & Answers

1. What are some causes of the number of bytes on the wire exceeding the number of bytes being captured?

2. What are the source and destination MAC address in Frame 546?

3. What is the manufacturer's specific ID for Intel Core?

4. What is the MAC address used for IPv4 multicast?

5. What version of IP is present in Frame 546? What is the source IP address?

6. At what times do the various steps of the Google three-step TCP handshake occur?

7. A DNS query failure is referred to a higher level Domain Name Server under what condition?

8. The descriptive text that accompanies the packet analysis is provided by Wireshark. True or False?