Case Name: Lab\_17

Course Name: CYB-107

Professor: Webb

Date: MM/DD/YYYY

Examiner Name: Noah Lewis

**Introduction:**

In this lab the students will learn how to operate the software known as “WireShark”. The students will also learn about things such as a packet sniffer, protocols, and overall learn more about packets.

**Analysis:**

1. Start your favorite web browser.

A screenshot of a computer

Description automatically generated

1. Startup WireShark.

A screenshot of a computer

Description automatically generated

1. Capture interface.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Start interface.

A screenshot of a computer

Description automatically generated

1. http://

A screenshot of a computer

Description automatically generated

1. Open link in a browser.

A computer screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

1. More going on that meets the eye.

A screenshot of a computer

Description automatically generated

1. Wireshark-lab Hypertext Transfer Protocol

A screenshot of a computer

Description automatically generated

1. Get

A screenshot of a computer

Description automatically generated

1. Exit WireShark.

A screenshot of a computer

Description automatically generated

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Three protocols that appear in this lab were TCP, UDP, and http.

1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

It took 37.677467 seconds from the Get to the OK.

1. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

The internet address of the gaia.cs.umass.edu is “10.11.115.155”. And my internet address is “128.119.245.12”.

1. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only”* and *“Print as displayed”* radial buttons, and then click OK. Show that you are able to print the messages.

Get “83 14:24:28.956806 10.11.115.155 128.119.245.12 HTTP 638 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1”

OK “328 14:24:43.251309 104.117.182.50 10.11.115.155 HTTP 241 HTTP/1.1 200 OK (text/plain)”

**Conclusion:**

From this lab the students learned how to use WireShark and just some of the things it is capable of doing. The students also developed a deeper understanding about how packets work and what they are. The students also learned more about different internet protocols.