**CS 3873: Net-Centric Computing**

Lab 1: Examining HTTP with Wireshark

Student Name: \_Mahmoud Moustafa Student Number: 3648276

**[Mandatory]** Declaration: “I warrant that this is my own work.”

Signed by Mahmoud Moustafa

[Optional] “I hereby give my permission for this work to be used (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes.”

Signed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report for Lab Exercise 1:

Examining HTTP with Wireshark

**LAB ACTIVITIES: TODO**

In this lab, we learnt how to capture packet traces with Wireshark. In particular, we used Wireshark to examine the details of the hypertext transfer protocol (HTTP).

**ANSWERS TO LAB QUESTIONS:**

The following gives you one example on how to draft your answer to the lab questions.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.  
   **Answer:** As seen in Fig. 1, 3 of the different protocols are TCP, ARP, and UDP

Table

Description automatically generated

Fig. 1. Different protocols that appear in the protocol column

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*.)  
     
   **Answer:** As seen in Fig. 2, the HTTP get message is captured 18.220895 seconds after starting Wireshark, while the first HTTP response is received at 18.260484 seconds after starting Wireshark. It took (18.260484 - 18.220895 = 0.039589) seconds.

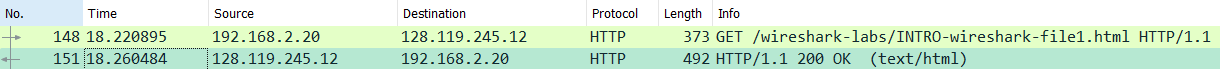


Fig .2. HTTP GET and Response messages in the captured trace

1. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?  
     
   **Answer:** As shown in Fig. 2 and 3, my internet address is 192.168.2.20 and the internet address of gaia.cs.umass.edu is 128.119.245.12.



Fig .3. My internet address

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.  
     
   Text, letter

   Description automatically generated  
     
   Text

   Description automatically generated
2. Based on the above trace, answer the following questions:
3. Select the first HTTP message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the HTTP server. When you select the HTTP GET message, the Ethernet or Ethernet II frame, IPv4 datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. How long did it take from when the HTTP GET message was sent until the first HTTP response was received?

**Answer:** As seen in Fig. 4, the HTTP GET message is captured at time 4.342727, while the first HTTP response is received at time 4.392253. It takes (4.392253-4.342727 = 0.049526) seconds.



Fig. 4. Certain HTTP GET and Response messages in the captured trace.