HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY

FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COURSE: COMPUTER NETWORK

LAB 1B: INTRODUCTION OF WIRESHARK PACKET SNIFFER TOOL

Supervisor : Nguyễn Lê Duy Lai.

Author : Nguyễn Quang Long.

ID : 1812917.

Monday, October 05th , 2020

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

Answer:

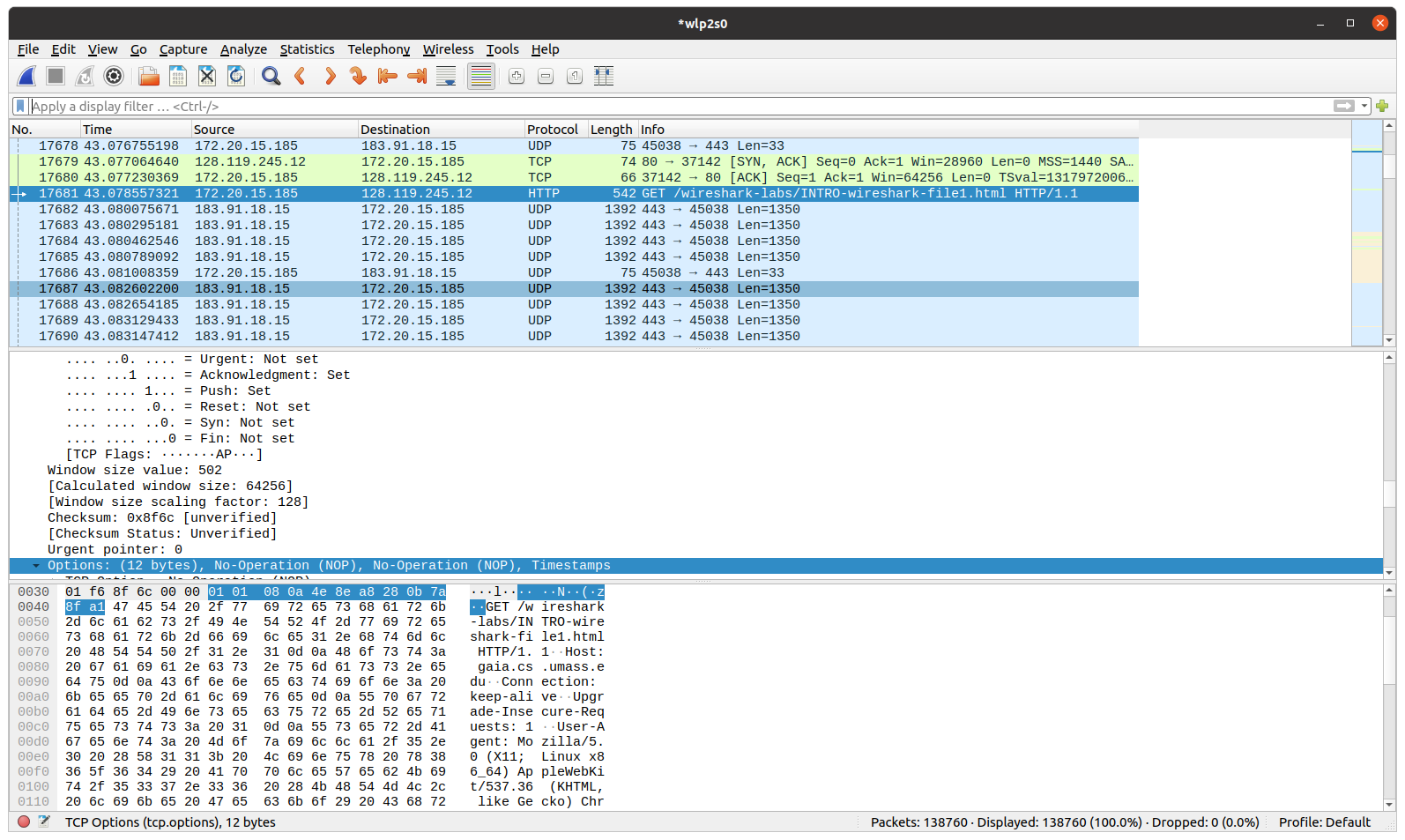
 As we can see in figure 1, three different protocols (maybe more) was listed in the protocol column which are:

Figure :exampe of protocols

* TCP.
* HTTP.
* UDP.

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 packetlisting 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:

In figure 2, the time when the GET message was sent is 43.078557321 and then the OK reply was received at 43.322719862. With a quick math we can figure out that it took 0.244162541s from when the HTTP GET message was sent until the HTTP OK reply was received.

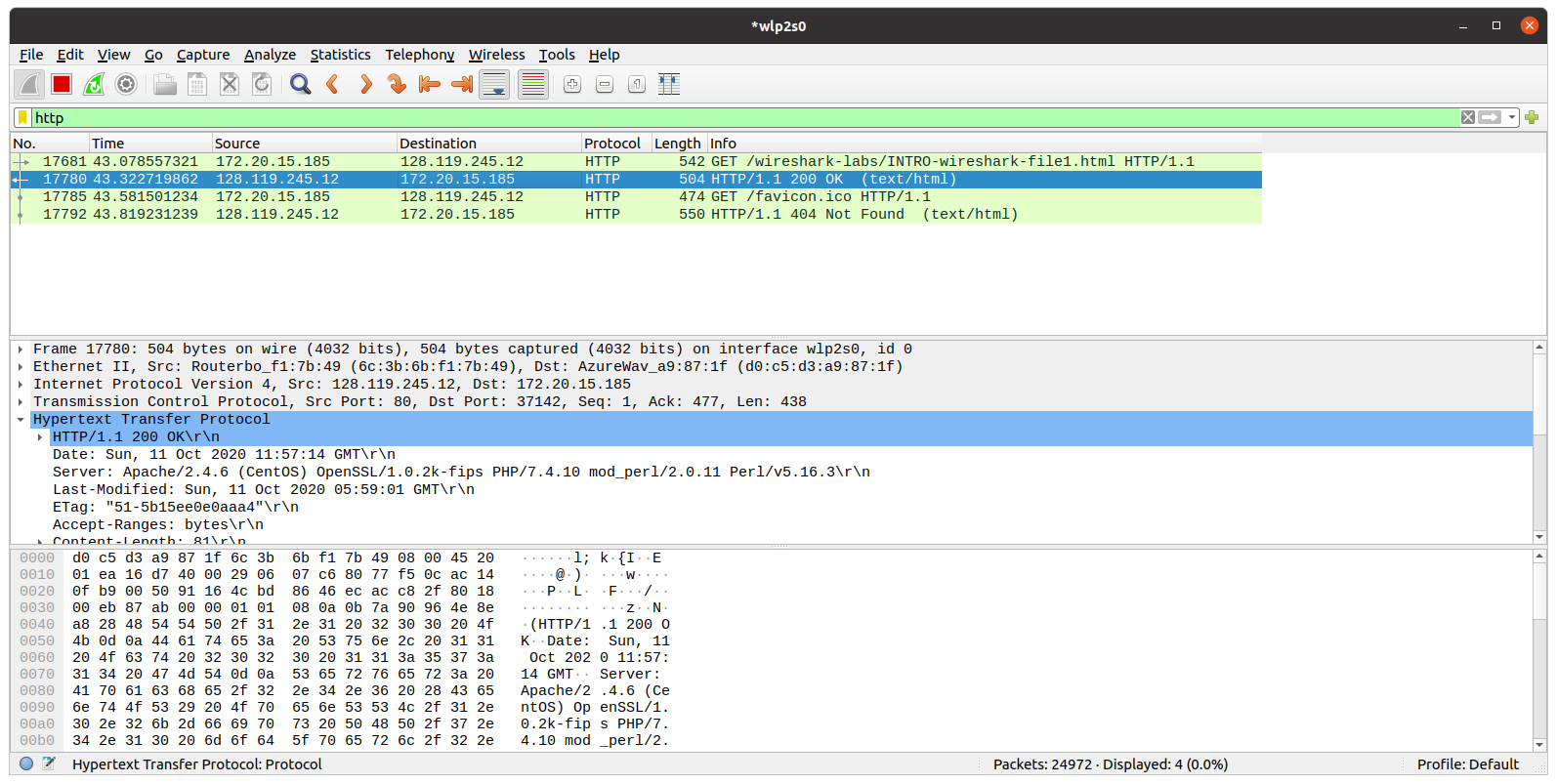
* 

Figure : package's time

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 :

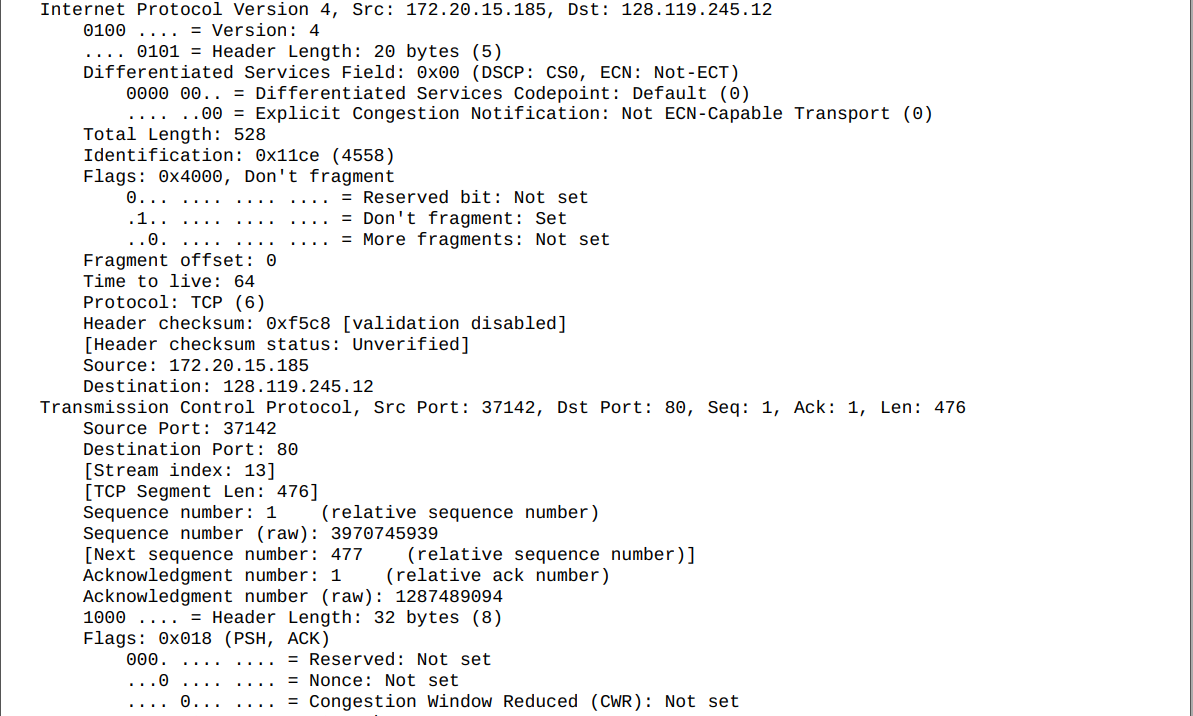
In figure 2, consider the GET message, we can see that there are 2 IP addresses was listed which are 172.20.15.185 (source) and 128.119.245.12 (destination). The source IP represense my computer ip and the Destination is the Internet address of the gaia.cs.umass.edu.

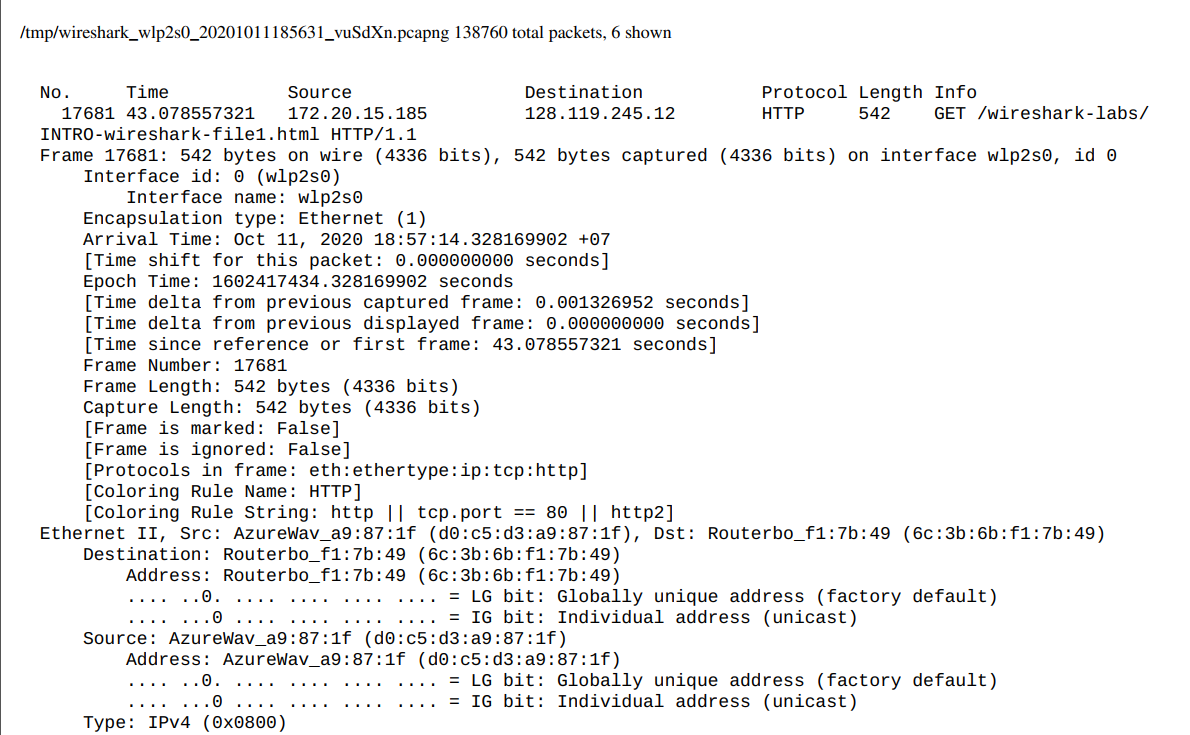
If we take a closer look at the OK reply, it was sent from gaia.cs.umass.edu to my computer so the source would be 128.119.245.12 and destination would be 172.20.15.185.

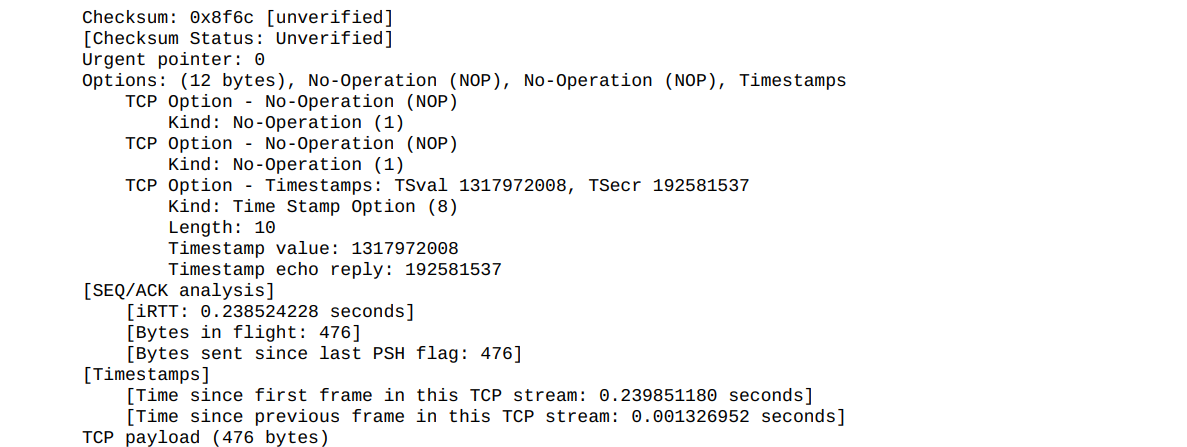
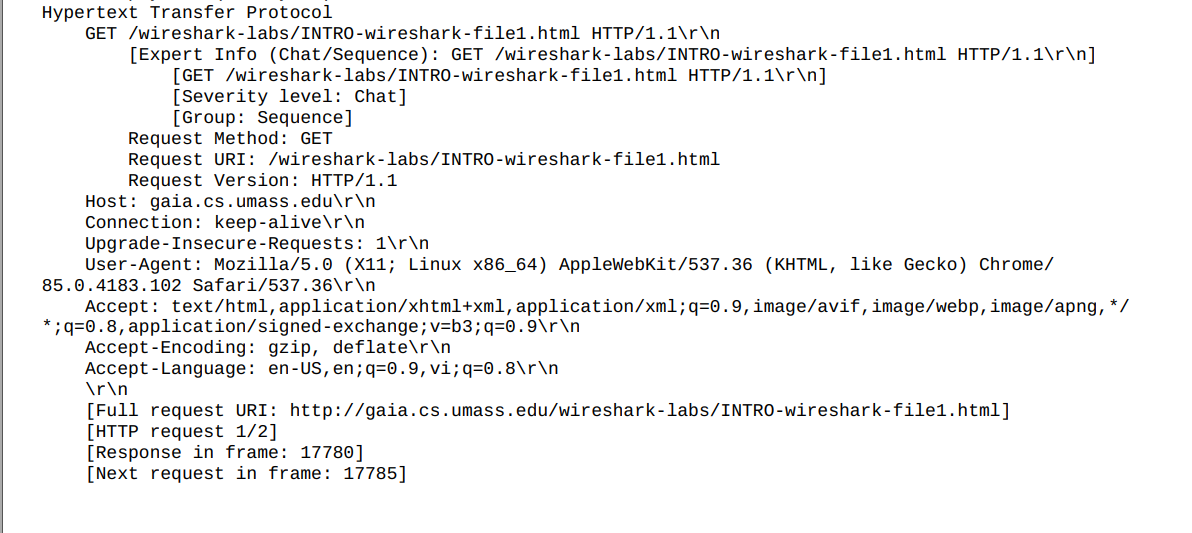
1. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only”* and *“Print as displayed”* radial buttons, and then click OK.

Answer:

* The result when I printed the GET message:







* The result of ok message:

