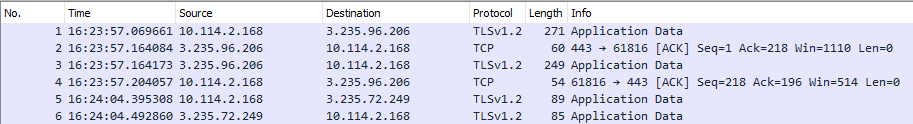
Anthony Chavez

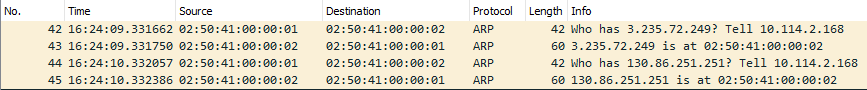
Professor Sun

Wireshark Lab

Question 1



In the beginning of the capture, the TLSv1.2 and the TCP protocol can be seen in the screenshot above. According to keycdn.com, “TLS stands for Transport Layer Security, which is a cryptographic protocol used to increase security over computer networks. Transmission Control Protocol is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data (https://searchnetworking.techtarget.com/definition/TCP).



ARP can be seen in the above screenshot. “Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN).” (https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP)

Question 2



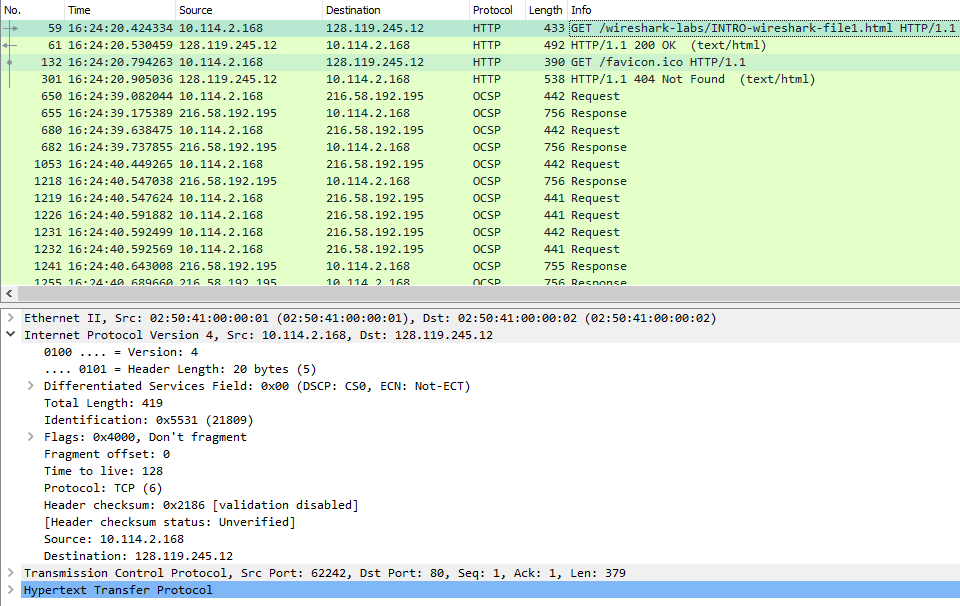
The HTTP GET message was sent at 16:24:20.424334 and the HTTP OK reply was received at 16:24:20.530459. Therefore 20.530459s – 20.424334s = 0.106125 seconds.

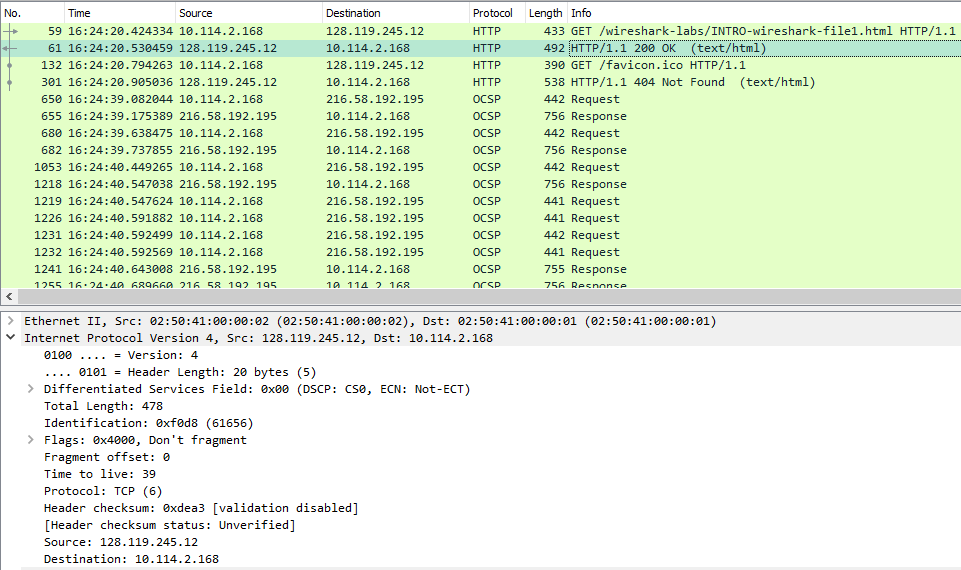
Question 3

There are two options of determining the Internet address of the gaia.cs.umass.edu and my computer.



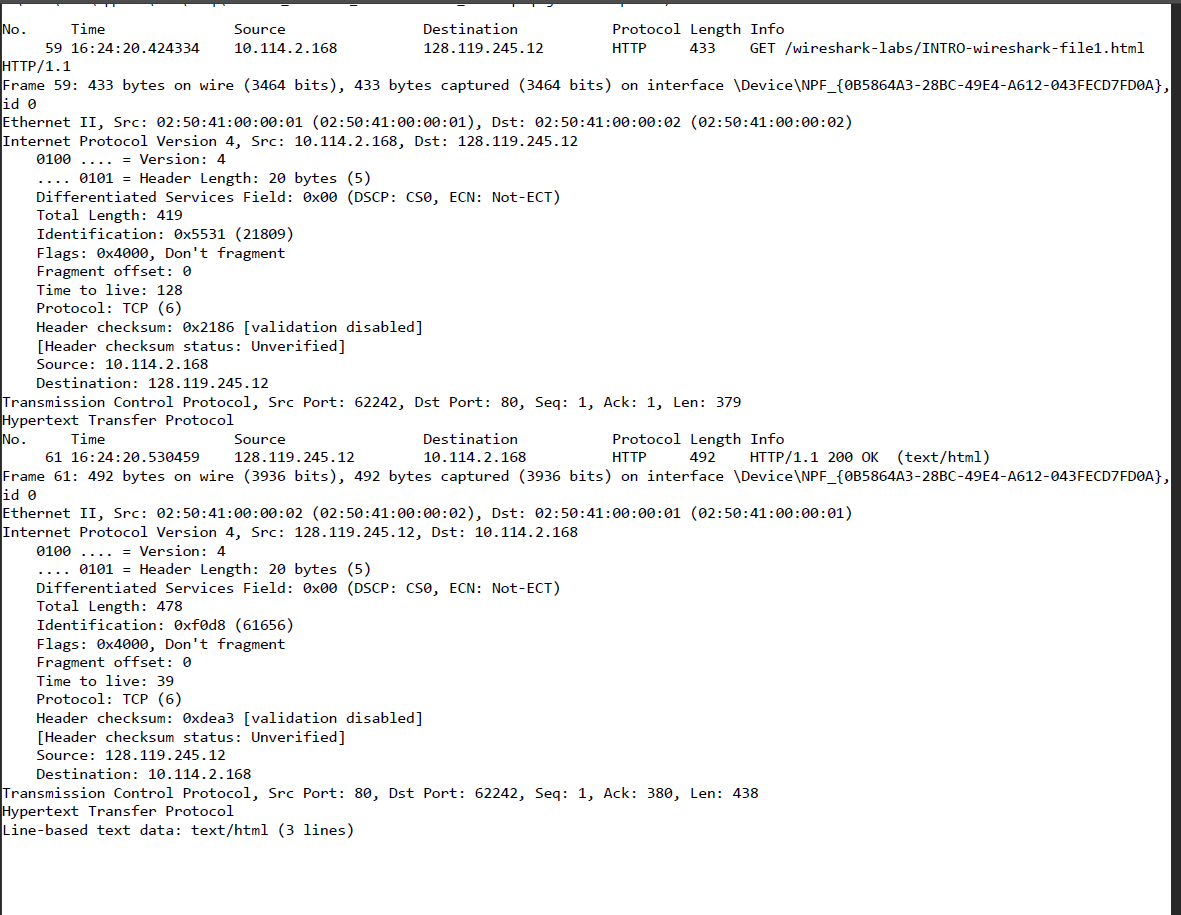
For the HTTP GET message, you can see under the Destination column that the Internet address of gaia.cs.umass.edu is “128.119.245.12” and under the Source column my Internet address is “10.114.2.168”. This is because my computer is sending the HTTP GET message to gaia.cs.umass.edu. On the other hand, the HTTP OK reply is sent by gaia.cs.umass.edu, so gaia.cs.umass.edu has its Internet address as the source and my computer is the destination.





Alternatively, you can select one packet capture at a time and open the “Internet Protocol Version 4” segment. The HTTP GET message is sent by my computer, so the source is my computer’s Internet address. This message is being received by gaia, so the destination is gaia’s Internet address. (See first screenshot) When the HTTP OK reply is sent, the source becomes gaia’s Internet address and the destination becomes my computer’s Internet address. (See second screenshot)

Question 4



This is a printout of the HTTP GET and HTTP OK packet from my Wireshark capture.