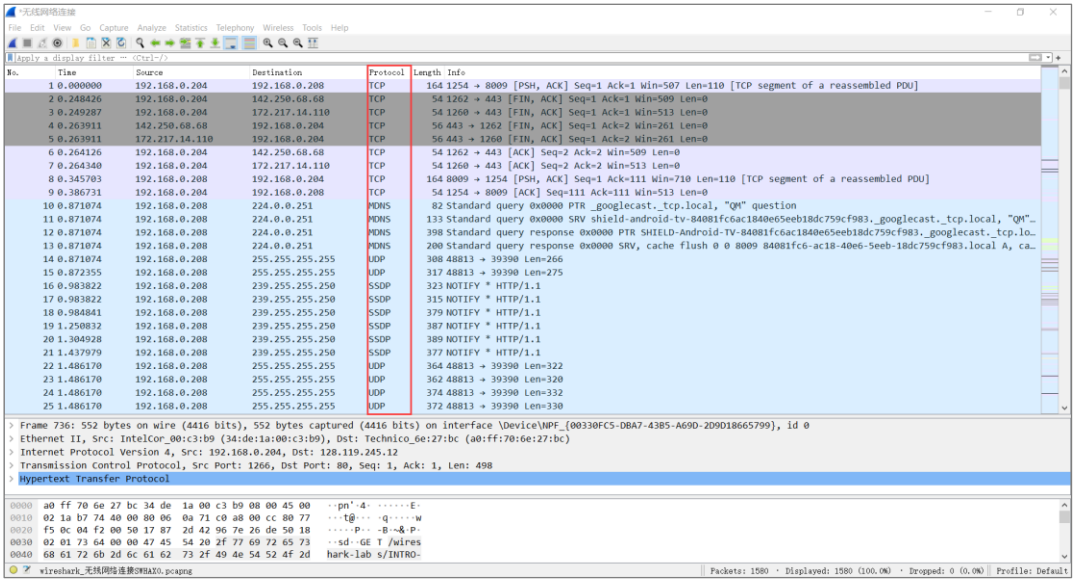
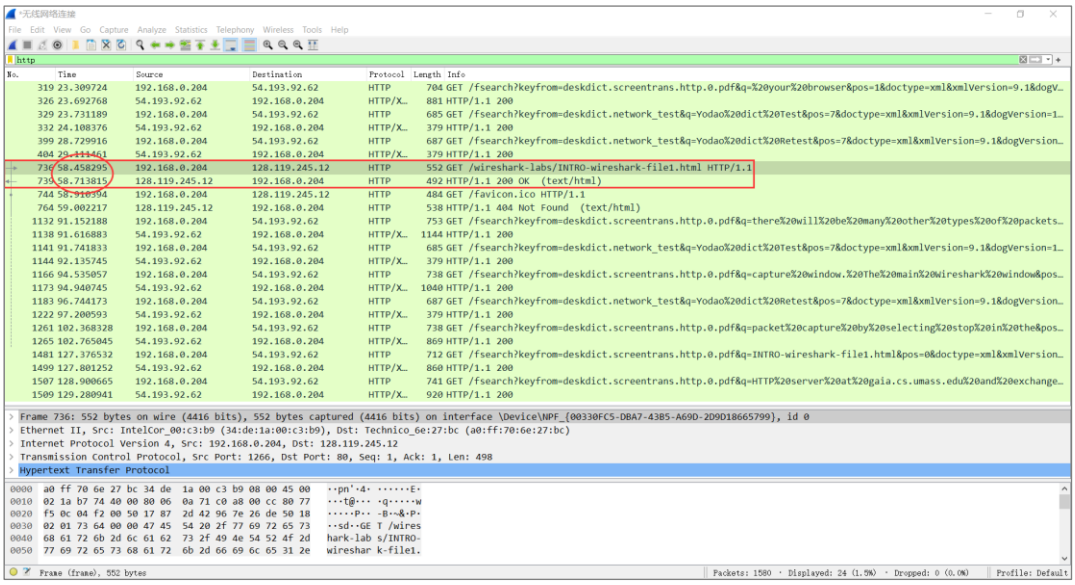
Wireshark Lab 1 - Introduction to Wireshark
Xiaoying Li

1. List 3 different protocols that appear in the protocol column in the unfiltered packet listing pane in step 7 above: TCP, MDNS, UDP.



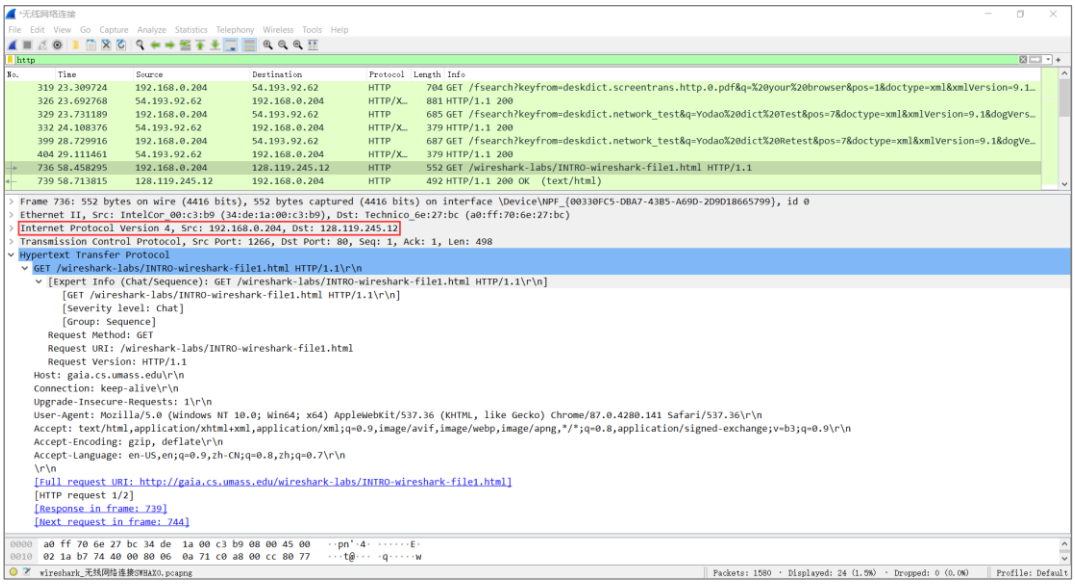
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began.)

The HTTP GET message was sent: 58.458295 seconds since Wireshark tracing began.
The HTTP OK reply was received: 58.713815 seconds since Wireshark tracing began.
Therefore, it takes $58.713815 - 58.458295 = 0.25552$ seconds from when the HTTP GET message was sent until the HTTP OK reply was received.



3. *What is the Internet Protocol (IP) address of the gaia.cs.umass.edu? What is the Internet Protocol (IP) address of your computer?*

Internet Protocol (IP) address of the gaia.cs.umass.edu: 128.119.245.12
Internet Protocol (IP) address of my computer: 192.168.0.204



4. Include screenshots of the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include at least: Arrival Time, Total Length, Protocol, Source IP address, and Destination IP address.

No.	Time	Source	Destination	Protocol	Length	Info
736	58.458295	192.168.0.204	128.119.245.12	HTTP	552	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
739	58.713815	128.119.245.12	192.168.0.204	HTTP	492	HTTP/1.1 200 OK (text/html)

NOTE: The Chinese character "无线网络连接" in the top left corner and bottom left corner of first three screenshots means "Wi-Fi". Since I don't know how to set it to show English and it might confuse you, I wrote this note. Thanks.