

Fatmata Kargbo  
CSCI 3761 H01 Lab 1

## Deliverables

1. Answer four questions on the last page of this lab description.
2. Attached screenshot of the captured packet for each question with your answer.

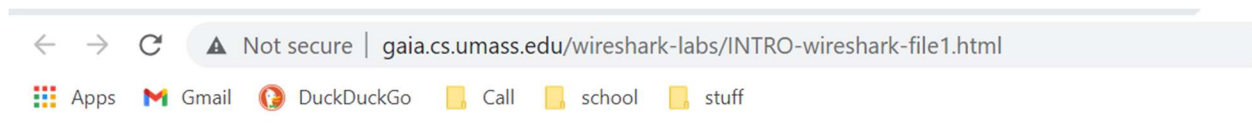
The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar is present with the text "Apply a display filter ... <Ctrl-/>".

The main window is divided into two sections: "Capture" and "Learn".

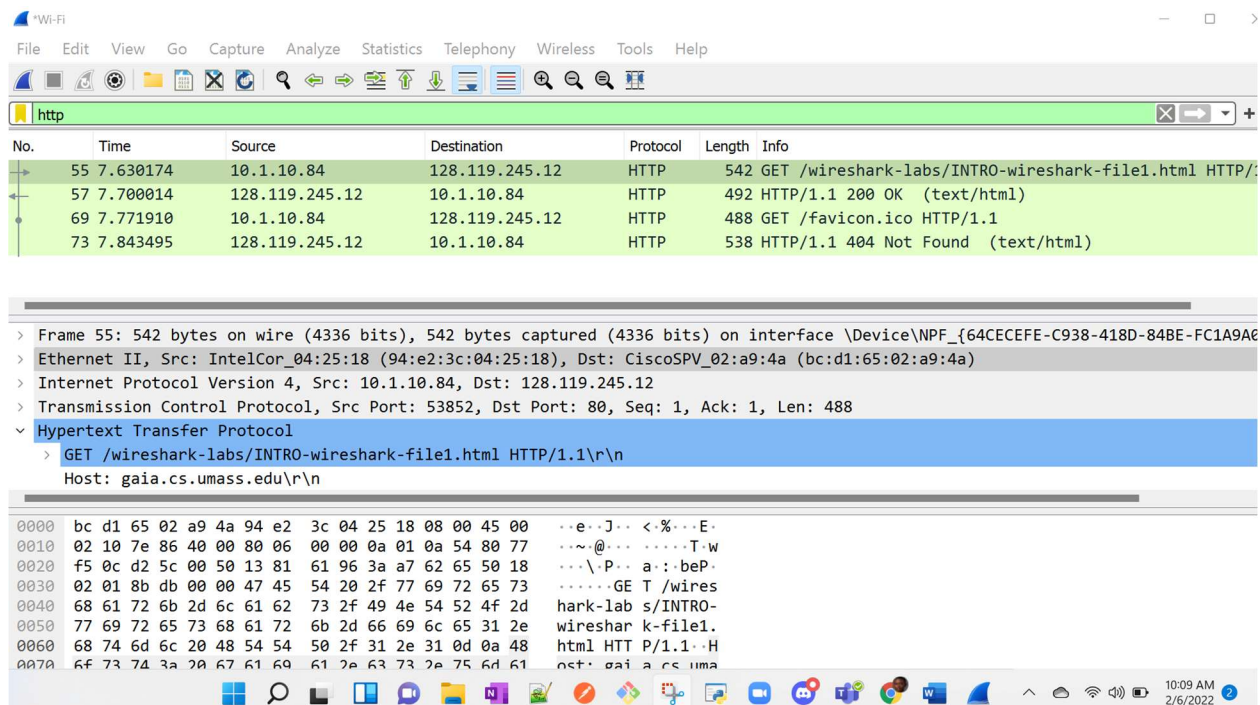
**Capture Section:** A "Welcome to Wireshark" message is displayed. Below it, the "Capture" section shows a list of network interfaces with their corresponding capture status. The interfaces listed are: Local Area Connection\* 11, Local Area Connection\* 10, Local Area Connection\* 9, Bluetooth Network Connection, Wi-Fi, Local Area Connection\* 12, Local Area Connection\* 3, VirtualBox Host-Only Network, and Adapter for loopback traffic capture. The Wi-Fi interface is selected, and its capture status is indicated by a green line.

**Learn Section:** The "Learn" section provides links to the User's Guide, Wiki, Questions and Answers, and Mailing Lists. It also displays the version of Wireshark being used: "You are running Wireshark 3.6.1 (v3.6.1-0-ga0a473c7c1ba). You receive automatic updates."

The bottom section of the interface shows a packet capture table with columns for No., Time, Source, Destination, Protocol, Length, and Info. The table contains several rows of captured packets, including TCP, SSDP, TLSv1.3, and UDP. The selected packet (No. 523) is highlighted in blue. Below the table, the packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII format.



Congratulations! You've downloaded the first Wireshark lab file!



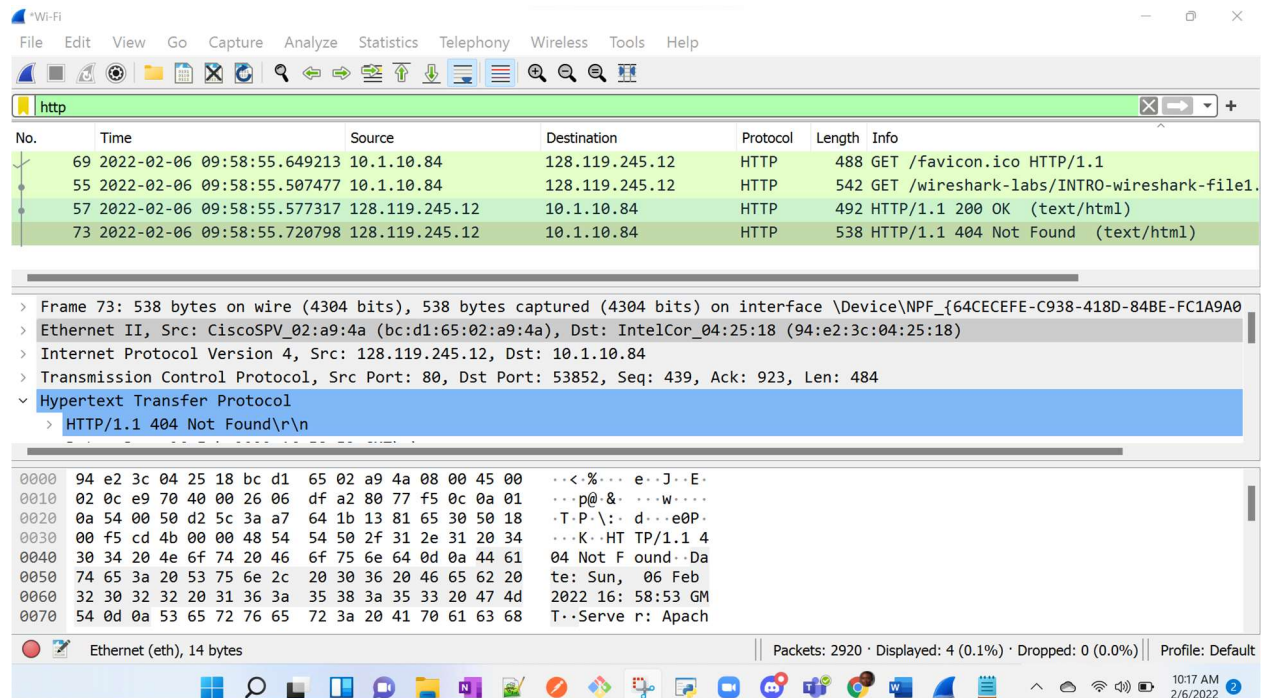
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

HTTP

TCP

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. 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.)



3. 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?

My computer 10.1.10.84

website 128.119.245.12

4. 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.

SEE PDF