# Wireshark Lab 1 - Introduction

Started: Sep 26 at 1:13a.m.

# Quiz Instructions

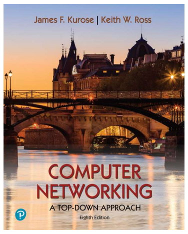
**Wireshark_Intro_v8.1.pdf** (https://q.utoronto.ca/courses/281681/files/22129438/download?download_frd=1)

## Question 1

10 pts

**Intro Lab: Q01 Introduction and protocols seen in trace**

This LMS module allows you to enter answers for the questions posed in the **introductory Wireshark lab writeup (http://gaia.cs.umass.edu/wireshark-labs)** that accompanies the textbook *Computer Networking: A Top-down Approach, 8th edition*. The Wireshark lab description, questions, context, helpful hints, and more are in the introductory Wireshark lab writeup. So that writeup is a *must-read*, before answering these questions.



The answers to the questions in this LMS module (which match those in the Wireshark lab writeup) are based on packets in the trace file intro-wireshark-trace-1, which can be extracted from the zip file **http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip (http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip)** *So make sure you have this specific trace file open in Wireshark when you answer these questions!*

Which of the following protocols appear (i.e., are listed in the Wireshark “protocol” column) in the trace file?

☑ TCP

☐ QUIC

☑ HTTP

☐ DNS

☐ UDP

☑ TLSv1.2

## Question 2

10 pts

**Intro Lab: Q02 HTTP response time.** 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.

Enter your answer in the form of "0.*xyz*" (without quotes) where *xyz* are the three first decimal places (in subseconds) of the HTTP response time. Calculate your answer using the six decimal places of subsecond time precision, and then enter your answer rounded (not truncated) to three subsecond decimal places, 0.*xyz*:

0.029

## Question 3

10 pts

**Intro Lab: Q03.1 Server IP address.** What is the Internet (IP) address of the web server gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? Enter the address in so-called dotted decimal notation of the form *w.x.y.z,* where *w, x, y*, and *z* are integers between 0 and 255. Omit leading zeros (except if the value of *w, x, y* or *z* is zero); include the periods in your answer:

128.119.245.12

## Question 4

10 pts

**Intro Lab: Q03.2 Client IP address.** What is the Internet (IP) address of the client that sent the HTTP request to the gaia.cs.umass.edu server? Enter the client's address in so-called dotted decimal notation of the form *w.x.y.z,* where *w, x, y*, and *z* are integers between 0 and 255. Omit leading zeros (except if the value of *w, x, y* or *z* is zero); include the periods in your answer:

10.0.0.44

## Question 5

**10 pts**

**Intro Lab: Q04 Which web browser?**

Expand the information about the HTTP message in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the "User-Agent:" field in the expanded HTTP message display.

○ Safari

● Firefox

○ Microsoft Edge

○ None of these answers.

## Question 6

**10 pts**

**Intro Lab: Q05 What port number?** Expand the information about the Transmission Control Protocol in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent?

● 80

○ 23

○ 242

○ 53962

Quiz saved at 1:25am Submit Quiz