

Wireshark Lab 3

- Due Apr 2 at 11:59pm
- Points 5
- Questions 5
- Available Mar 21 at 5pm - May 1 at 11:59pm
- Time Limit None
- Allowed Attempts 5

Instructions


Hello everyone,

To answer questions 1 through 5, please first download the **Wireshark Trace file** and then respond to the questions.

Wireshark Trace: [Wireshark-Lab3.pcapng \(https://canvas.uh.edu/courses/20819/files/6365043?wrap=1\)](https://canvas.uh.edu/courses/20819/files/6365043?wrap=1) 
(https://canvas.uh.edu/courses/20819/files/6365043/download?download_frd=1)

[Take the Quiz Again](#)

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	247 minutes	5 out of 5
<div>ⓘ Correct answers are hidden.</div> <div>Score for this attempt: 5 out of 5</div> <div>Submitted Mar 21 at 10:29pm</div> <div>This attempt took 247 minutes.</div> <div>⋮</div> <div>Question 1</div> <div>1 / 1 pts</div> <div>Question Note: First download the Wireshark-Lab3.pcapng (https://canvas.uh.edu/courses/20819/files/6365043?wrap=1)  (https://canvas.uh.edu/courses/20819/files/6365043/download?download_frd=1) and then respond to the questions.</div> <div>In frame 233, the user has sent data using the TLS protocol (over TCP). The requested values help to identify the source and the size of the message. Please complete the required fields below:</div> <div><ul style="list-style-type: none">• Field 1: Source IP address XXX.XXX.XXX.XXX<div>192.168.128.69</div><ul style="list-style-type: none">• Field 2: Packet length (in bytes)<div>113</div><div>Answer 1:</div><div>192.168.128.69</div><div>Answer 2:</div><div>113</div></div>			



Question 2

1 / 1 pts

Question Note: Based on the downloaded file, complete the exercise and provide your answers.

In frame 247, the user initiated a connection with the server by sending a **TCP SYN packet**. The **Maximum Segment Size** value in the TCP options and the **Destination IP address** are of particular importance. Please provide these values:

- Field 1: Maximum Segment Size

- Field 2: Destination IP address XXX.XXX.XXX.XXX

Answer 1:

1460

Answer 2:

206.188.192.81



Question 3

1 / 1 pts

Question Note: Based on the downloaded file, complete the exercise and provide your answers.

In the frame range 362 to 370, it is observed that the server (IP: 206.188.192.81) sends multiple TCP packets containing data to the device (IP: 192.168.128.69). Which option describes what is happening?

- ☐ Initiating DNS lookup
- ☒ Transmitting large amounts of data using PSH, ACK packets followed by acknowledgments
- ☐ Closing the TCP connection with FIN and ACK packets
- ☐ Establishing an encrypted connection



Question 4

1 / 1 pts

Question Note: Based on the downloaded file, complete the exercise and provide your answers.

In frame 36, one of the QUIC protocol packets (using UDP) is observed. From the UDP header, the source port number and packet length are extracted to determine which side initiated the connection. What is the UDP source port number?

- ☐ 788
- ☐ 53102
- ☒ 443
- ☐ 6304



Question 5

1 / 1 pts

Question Note: Based on the downloaded file, complete the exercise and provide your answers.

In frames 3219 to 3225 from the captured file, which of the following events occurred?

- ☐ Initial DNS query exchange between client and server.
- ☒ Exchange of QUIC protocol messages, including initial handshake and protected data (Protected Payload/KP0) transfer.
- ☐ Establishing a DNS connection.
- ☐ Sending ICMP messages to indicate “Destination Unreachable.”

Quiz Score: 5 out of 5