
Middle East Technical University


Department of Computer Engineering

CENG 435

Data Communications and Networking
Fall 2020–2021
Wireshark Take Home Exam 1

Due date: 25/11/2020 - Wednesday, 23:59

1 Objective

In this assignment, you are expected to examine the network traffic by using *Wireshark* and exercise basics of some application layer protocols. As you all know, *Wireshark* is the network capture & analysis tool that we will use in this course and at the end of this assignment you are expected to be familiar with *HTTP*, *HTTPS*, *TLS* and *DNS* protocols.

2 Instructions

This homework includes two parts in which you will capture the network traffic at first and then answer the given questions in your assignment report. Please note that, if you are asked to explain what is the reason, **you MUST explain briefly with your own words in at most 5-6 sentences**. Finally, you will submit your assignment report and capture files.

2.1 HTTP & DNS

2.1.1 Capture the Network Traffic

In order to get a clean capture;

- Open Wireshark and check if it's capturing packets in your network.
- Close all programs including browsers that create network traffic.
- Clean the cookies and site data of your browser that you will use while capturing the network traffic before capturing.
- Before starting the capture, open one browser and one tab, then go to `http://ceng.metu.edu.tr`, mind the *http*.
- In the next step, while capturing, you **MUST** refresh the page by overriding the locally cached version of the page. This process can be done by different key combinations in different operating systems and browsers,
  - On Windows and Linux,
    - On "Mozilla Firefox", "Google Chrome", "Microsoft Edge" and "Internet Explorer": Hold the "**Ctrl**" key and press the "**F5**" key.

  - On macOS,
    * On "Mozilla Firefox", "Google Chrome" and "Safari": Hold the "**Shift**" key and click the "**Reload**" button on the navigation toolbar.

- In Wireshark, start the capture, switch to browser and using the appropriate key combination for our operating system and browser reload the page. You will see that the page is refreshed.
- After the page is loaded, stop capturing the packets in Wireshark.
- Save the capture dump as **e<your_student_id(7 digit)>-http-dns.pcap** file (Ex: **e1234567-http-dns.pcap**) to a safe place because you will send it to us while uploading your homework and answer the corresponding questions by using this "pcap" file.

2.1.2 Answer the Questions (70 Points)

1. How many queries were sent from your computer to the DNS server to get the "**http://ceng.metu.edu.tr**" server address? Take a screenshot that shows the DNS query packets in Wireshark window. **(8 Points)**
2. What is/are the destination address(es) of the server(s) where the DNS queries were sent and answered? **(10 Points)**
   Bonus: By looking the destination address(es) of the server(s) where the DNS queries were sent and answered, can you say from where the server address was found and whether it was cached? **(10 Bonus Points)**
3. In which queries, were the first request sent to the "**http://ceng.metu.edu.tr**" server and the first response received from it (write the numbers which can be shown in "No." fields in Wireshark and attach a screenshot that shows the packets in Wireshark window)? Explain why it was not a HTTP request and response pair (Explain briefly.)? **(15 Points)**
4. In the first HTTP request to "**http://ceng.metu.edu.tr**" server, was any cookie sent with this request? If it was sent, prove it by a screenshot which is taken from Wireshark about how you get that result. **(15 Points)**
5. In any HTTP request to "**http://ceng.metu.edu.tr**" server
   (a) What is the user-agent string? Take a screenshot of the Wireshark packet inspection window that shows user-agent string? **(7 Points)**
   (b) Does the user-agent string include the browser you are using? Is any other browser mentioned? If so, why is that the case (Explain briefly.)? **(15 Points)**

2.2 HTTPS & TLS

2.2.1 Capture the Network Traffic

Follow the steps given in Subsection 2.1.1 with **two *crucial* differences**;

- After starting the capture in Wireshark, switch to browser and this time go to `https://odtuclass.metu.edu.tr`. You **do not** need to refresh the page by overriding the locally cached version of the page, navigating to the URL while capturing the packets is enough.
- Save the capture dump as **e<your_student_id(7 digit)>-https-tls.pcap**, (Ex: **e1234567-https-tls.pcap**)

2.2.2 Answer the Questions (30 Points)

1. Find the first successful request and response pair between your computer and ODTUClass server. Take a screenshot of the Wireshark window that shows the successful packet pair. What is the time difference between the request and the response queries in seconds? **(10 Points)**

2. Regarding the first TLS request and its response, what is written in their "Info" field (column) in the Wireshark? Can you tell which part of the communication the server and the client are in by looking at that "Info" field? **(10 Points)**

3. How many times were the "hello" message sent from client and server? If it is more than once, why (Explain briefly)? **(10 Points)**

3 Other Specifications

- **This is an individual assignment. Using any piece of code, discussion, explanation etc. that is not your own is strictly forbidden and constitutes as cheating. This includes friends, previous homeworks, or the Internet. The violators will be punished according to the department regulations.**
- **Late Submission: Late submission is allowed as stated in the course syllabus.**
- Follow the course page on ODTUClass for any updates and clarifications. Please ask your questions on ODTUClass instead of e-mailing if the question does not contain code or solution.

4 Submission

- Your assignment report's name and format **MUST** be **e<your_student_id(7 digit)>-report.pdf** (Ex: **e1234567-report.pdf**).
- You **MUST** write your report on the computer. Handwriting and scanning submissions will **NOT** be accepted. "**e1234567-report.tex**" file was shared with you in ODTUClass as a template for your report. Please **use this template** while preparing your report and be sure that the screenshots you have put in your report are readable.
- You **MUST** have **three files** to submit (Ex: **e1234567-http-dns.pcap**, **e1234567-https-tls.pcap**, **e1234567-report.pdf**) and there are two place to submit your files in ODTUClass. You **MUST** submit your report pdf file to "**Wireshark Take Home Exam 1 - Report (Turnitin)**". Then, you **MUST** compress two pcap files in **.zip** format called **e<your_student_id(7 digit)>.zip** (Ex: **e1234567.zip**) and submit to "**Wireshark Take Home Exam 1**".