Middle East Technical University

Department of Computer Engineering

CENG 435

Data Communications and Networking

Fall 2022–2023

THE - 1

Due date: 2022-11-07 23:59

1 Introduction

This assignment will cover application layer protocols and will serve as an introduction to networking tools and Wireshark. Use your findings to prepare a report for the final submission. For each question, explain your answer in detail using your own words. Overall submission will include the `.pcap` file you have used to show your capture as well as the `.pdf` report, see Section 5 for details.

2 HTTP

In this section, you will capture & analyze HTTP traffic. Do not forget to save the captures you have used to answer this section as `.pcap` files for submission. For every question, support your answer using screenshots from the Wireshark window and, if necessary, the browser you have used.

2.1 Capture the Network Traffic

- Before starting the capture, open a browser tab, then go to `http://ceng.metu.edu.tr`, mind the *http*.
- For the next step, we will "hard reload" the page to disregard the cache of the browser, there are different ways to do this depending on your setup;
  - On Windows and Linux,
    - On "Mozilla Firefox": `Ctrl+Shift+R`
    - On "Google Chrome" and "Microsoft Edge": Right-click the "refresh" button on the toolbar and select "Empty Cache and Hard Reload"
  - 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 the browser and using the key combination for your operating system and browser, reload the page. The page will refresh.
- After the page has fully loaded, you can stop the capture.

- You might repeat this multiple times depending on the quality of your capture. Do not forget to save the version you used to answer the questions. The name of the `.pcap` file should be `e<your_student_id(7 digits)>.pcap`
- If you are unable to bypass your browser or your OS to answer the following questions as required, you can try incognito mode on your browser, different browsers (e.g. `lynx`) or different OS configurations (e.g. Docker).

2.2 Questions

1. How many queries were sent from your computer to DNS server(s) to get the `http://ceng.metu.edu.tr`'s IP address? Ignore the DNS requests for unrelated domain names. (The answer *should not* be zero, make sure you followed the steps described above)
2. How many servers were queried for the DNS request?
3. What are the IP addresses of the queried DNS server(s)?
4. Inspect the DNS request and response packets on Wireshark. Can you tell whether the response was cached or not by looking at them?
5. Find the first successful request and response pair between your computer and the `http://ceng.metu.edu.tr`'s server. Take a screenshot of the Wireshark window that shows the successful packet pair
   (a) What is the protocol of these requests?
   (b) Explain the reason why this protocol is used for the first request/response pair.
   (c) What is the time difference between the request and the response queries in seconds?
6. During the first HTTP request to `http://ceng.metu.edu.tr`'s server, was there any cookies sent with the request?
7. Using any of the HTTP requests to `http://ceng.metu.edu.tr`'s server;
   (a) What is the user-agent string of the request?
   (b) Does the user-agent string include the browser you are using? Are any other browsers mentioned? If so, why?

3 DNS

1. I have *important* and *urgent* news I have to share with Angela Merkel, the former Chancellor of Germany. Since I am in a rush, can I just send an e-mail to her through merkel@de? Please explain your answer (either way) thoroughly.

   Hint and clarification: Please do not try to send e-mails to that address, you can figure out the answer through other means *much* easier.

4 Other Specifications

- Feel free to ask questions through ODTUClass discussions.
- See the course syllabus for the late submission policy.
- This is an individual assignment. Using any piece of code, discussion, explanation etc. that is not your own without proper attribution is strictly forbidden and constitutes as cheating. This includes friends, previous homework, or the Internet. The violators will be punished according to the department regulations. You are allowed to refer to external sources using citation, though.

5 Submission

- Upload your assignment report in `pdf` format to the ODTUClass *Report Submission*.
- Submit your `.pcap` file through *Pcap Submission* on ODTUClass. The name of the `.pcap` file should be `e<your_student_id(7 digits)>.pcap`

5.1 Grading

- Please ensure that the screenshots in your report are legible. When in doubt, put your screen a meter away from you and see if you can still read the text or consult a friend with bad eyesight. I shouldn't have to be mentioning this
- Answers without explanations or screenshots to support them (e.g. answering just "3" to a "How many..." question) will get no grade.