Wireshark Assignment 1: Application Layer

Objective

In this assignment, you will examine network traffic using Wireshark and exercise the basics of application layer protocols.

Instructions

1. Start up your favorite browser and Wireshark. On wireshark start capturing packets over the interface with the Internet connection.
2. Visit `http://ceng.metu.edu.tr` on your browser, wait for the website to finish loading and then stop the packet capture on Wireshark and save the packet capture (you will submit it).
3. Answer the questions below.

Tip: Before you start doing the exercises, it is highly recommended to close all programs that communicate over network to make the task easier for yourself.

Questions

1. Did your browser perform any DNS queries to resolve the IP address of http://ceng.metu.edu.tr? If so answer the questions below. If not, why it might be the case?
    - How many DNS queries did it take to resolve the domain name?
    - What is the destination IP for the first DNS query?
    - What is the transaction ID for your query(-ies) and its response(s)?
2. What are the Number and Time of the first 5 HTTP request packets sent to server?
3. What is your browser's User-Agent string, what languages does it accept on response?
4. Did you send any Cookies with your first GET request to server?
5. How could a request and response packet be matched on a Wireshark environment?
6. How many parallel connections does your browser use? Explain briefly.

Bonus Question

We have captured the network traffic of a high profile target. We know that he accessed a super important zip file. Can you please retrieve the username&password of the target as well as the contents of the zip file.

(Tip: You are looking for something in the format of "ceng435{.....}")

Deliverables

You are expected to submit your answers as a one-page-long softcopy solution to "Wireshark Turnitin Assignment #1: Application Layer" section and your packet capture file (.pcap) to "Wireshark Assignment #1: Application Layer - PCAP Submission" section before the deadline. Please refer to course syllabus for late submission terms and follow Odtuclass system for further announcements.

Late delivery

Late delivery will be accepted for assignments. Your submission will be assessed out of 100 if it is delivered until the deadline. Late delivery will only be possible for two days after the deadlines. Your grade will be assessed out of 90 points on the first day of late delivery and out of 80 points on the second day. Beyond two days, your submission will not be counted as a valid submission and the NA policy will be applied.

Cheating Policy

We have zero tolerance policy for cheating. People involved in cheating will be punished according to the university regulations.