Due Date:17.04.2023 23:55

CENG 312-Computer Networks

Spring 2023

Assignment 1- HTTP and DNS

Before starting this assignment, we expect you to first review the introductory lab provided by the author and install wireshark software on your computer.
Please see the link below and follow the instructions in the first lab ("Lab topic:Getting Started"):

Wireshark Labs - Jim Kurose Homepage

NOTE:As part of your assignment, you are not responsible for the questions in the "What to hand in" section.

Part 1: HTTP

We will explore the http protocol: GET and POST methods.

1. **The Basic HTTP GET/response interaction**

You will do a GET request to a website (not HTTPs) of your choice. Please do not use the urls in the author's lab. Do the following:

1. Start up your web browser.

2. Then, begin Wireshark packet capture. Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

3. Make a GET request to the website.

4. Do not close the Wireshark for the next operations.

2. **The Basic POST request**

Before doing this part, make sure you have cURL installed on your computer. (**cURL** is a command-line tool that lets you transfer data to/from a server using various protocols. In this case, the curl command will establish a communication to POST to server over **HTTP**)

Now, let's send a simple post request. Do the following:

1. Enter the following to your terminal or command line according to your OS:

```
curl -X POST
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
--user "userid:password" -H "Content-Type: application/json"  -d
"productId=123456&quantity=100"
```

2. Stop Wireshark packet capture.

Answer the following questions:

1. By inspecting the data in the packet content window, what is the difference between GET and POST requests ?
2. What do you see in the authorization section in the post request?
3. Is it safe to send credentials using a post request in this way?Explain why?
4. Provide screenshot(s).(There is an example of how to do this at the end of the file.).

Part 2:

Open the "assignment1.pcapng" file in Wireshark and answer the following questions.

1. What is the protocol type of packets?
2. What is this protocol used for?
3. What is the name and the type of the transferred file over the protocol?
4. Investigate the request and response flows. Please explain what we are trying to do in this scenario.
5. Provide screenshot(s).

Part 3: DNS

In this section we will play with nslookup.

Section 1

- Start packet capture on Wireshark.
- Do an nslookup on ip address 193.140.248.136

Answer the following questions:

1. What is the name of this operation writing IP address instead of DNS name?
2. This operation is generally not recommended. Why? Please explain.
3. Examine the DNS query message on Wireshark. What "Type" of DNS query is it?
4. Examine the DNS response message on Wireshark. What is the DNS name of this ip address?
5. Provide screenshot(s).

Section 2

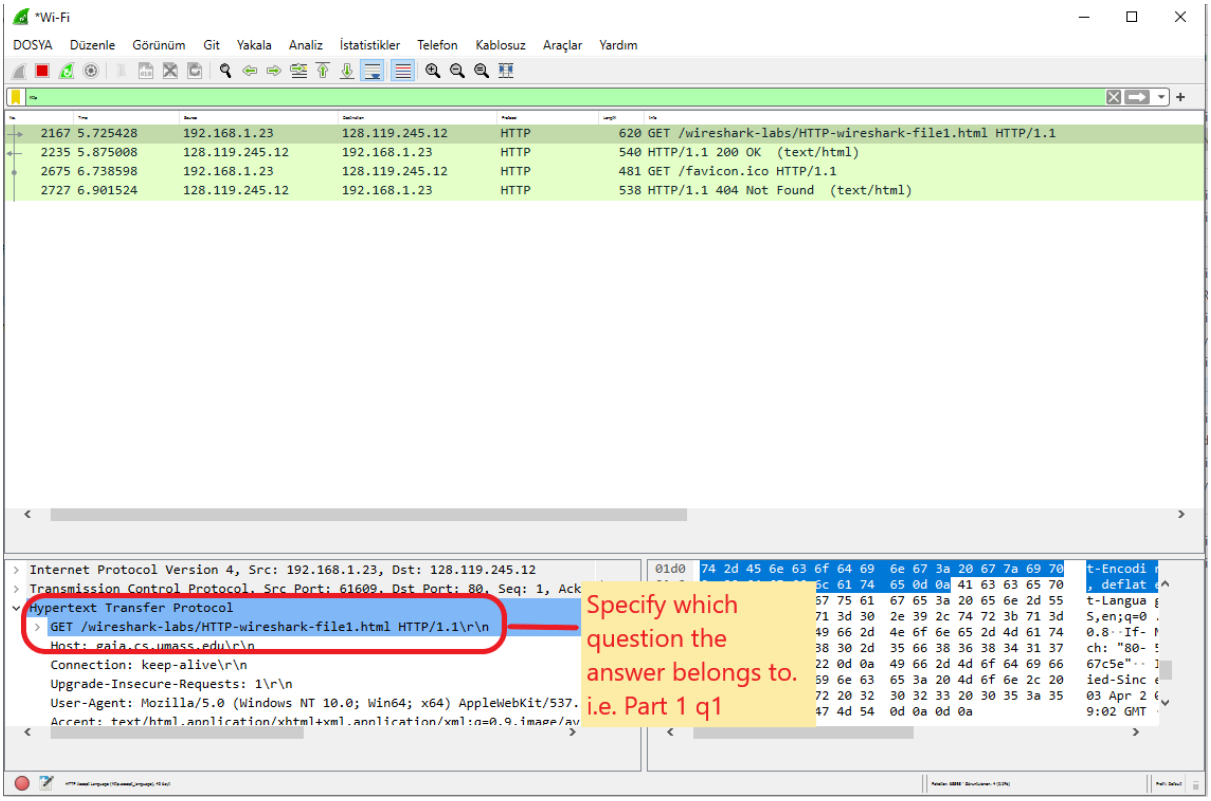
- Open the command prompt/terminal and Wireshark.
- Begin Wireshark packet capture and type **dns** into the display filter field.
- Start packet capture in Wireshark and run the following command in the command prompt.

```
nslookup www.microsoft.com
```

Answer the following questions.

1. What types of DNS queries do you see as a result of this command? Explain the details of these DNS types.
2. Make a DNS request to www.microsoft.com using a different DNS server of your choice instead of your local DNS server.
3. Provide screenshot(s).

Submission rules: When answering the questions, you should take the screenshot of wireshark or terminal (if necessary) and indicate where in the message you've found the information that answers the following questions. When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g.,annotate electronic copies with text in a colored font).
Example output:



- All submissions must be performed via **Microsoft Teams.**
- You must submit a single pdf file containing the answers to the questions. Do not send separate files, screenshots for each question. All materials related to your answer should be included in a single pdf file. And your filename must follow the following rules:

StudentNo_StudentName_Assignment1.pdf (i.e. 12345_BusraCalmaz_Assignment1.pdf)

- Submissions that do not comply with the rules above are penalized.