METU EE444 Introduction to Computer Networks

HW1 - Wireshark

Due: May 29, 2021, 23:55

You are going to submit your homework via **ODTUCLASS** as a **.pdf** file**, including required screen prints**. Name your document as "HW1_studentid.pdf" (ex: "HW1_1234567.pdf").

Using images or texts directly from any kind of resource is prohibited. Cheating will result in zero grade, whereas disciplinary actions may also be taken. Late submissions are not allowed.

To get results easier and correctly:

Before starting Wireshark captures, stopping applications with excessive bandwidth use (like Dropbox etc.) will ease your analysis.

If you've displayed the analyzed web site or image previously, you may not get the expected results sometimes. Therefore, delete the cache and cookies of your browser (you can use your non-favorite browser for example) before starting the capture of each session. *For the interested, "elinks" is a command-line browser alternative if you are on Linux.*

Please keep in mind that you may not have all the knowledge to reply the questions immediately. It is always encouraged to do some research on the internet or on Wireshark itself to learn about new things**.**

Brief Introduction

Wireshark, is a software tool that analyzes all the network packets entering or leaving a computer. It allows the live capture of network traffic and includes many powerful tools to examine, analyze, filter and otherwise manipulate the data. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In this homework, you will learn how to examine network packets via Wireshark. Before starting your homework, install Wireshark to your computer. You will need to install **Npcap** in the process, but you can skip the installation of **USBPCap** when asked.

To be able to capture internet traffic, always run Wireshark in administrator mode if you are on Windows.

Part 1 - Getting Familiar with Wireshark

Q.1.1) You should first specify which interface you are using to connect to the internet (Ethernet, wireless etc.). After that, start capturing packets. Capture the packets about 20 seconds and stop capturing. **Take a screen print** similar to Figure 1. On the capture screen, observe different communication protocols you are familiar with. Write the names of those protocols. (At least 5 of them)

For example; ARP: Address Resolution Protocol

Figure 1 - A sample screen print of Wireshark

Part 2 – HTTP, TCP, DNS

Q.2.1) Open a web browser (Firefox, Chrome, Explorer etc.). Now, we will analyze HTTP traffic. Start Wireshark capturing. Display the picture on METU server

http://www.eee.metu.edu.tr/sites/eee.metu.edu.tr/files/images/eehistory.jpg

via your browser. Stop capturing just after the browser finishes downloading the image. Look at the different types of protocols. What happens in the process? Explain "briefly". Please note that the middle box in Wireshark window provides information related to all the protocols involved for each highlighted action. **You will make use of the fields in this box a lot for other questions.**

Q.2.2) Type "http" (without quotes) to the **filter** box and press enter. This applies a filter to observe http traffic only. You can see a number of HTTP messages here. What is the IP address and port number of the actual source of the image file? What is your IP address? What is the tcp stream index related to the download of the image? Show all of these in a single **screen print**.

Q.2.3) The stream index is an internal Wireshark mapping to: **[IP address A, TCP port A, IP address B, TCP port B].** All the packets for the same tcp.stream value should have the same values for these fields. Apply a filter "tcp.stream eq ____". You should write the number of tcp stream you observed for the download of the image into the blank space. Take a **screen print**. Show the 3-way handshake for this TCP connection by explaining each packet.

Q.2.4) Pick the longest frame for that stream. How many bytes are used for the encapsulation of that **frame**? You can either calculate it just by looking at the TCP requests and replies or by counting the headers in a single frame. Write both methods and show the calculations.

Q.2.5) How can you find the throughput (bytes transferred per unit time) of a TCP connection by analyzing TCP packets without using Wireshark calculators? Calculate the throughput for this TCP stream.

Q.2.6) Now find the throughput of the TCP connection with Wireshark functions. Go to Statistics > TCP Stream Graphs > Throughput and take a **screen print** of the throughput for the stream to download the image file. (Please note that the starting time is falsely set to 0, which leads to a miscalculation of the throughput in the initial stages.)

Q.2.7) Click the HTTP frames associated with the download of the image. How can you understand whether the HTTP is persistent or non-persistent?

Q.2.8) Start a new capture and enter

http://eee.metu.edu.tr/sites/eee.metu.edu.tr/files/images/eehistory.jpeg

to your browser. Find the status code (the number of the error) which states the inexistence of the file. Show the related fields on a **screen print**. Generate two other status codes by performing some actions on the internet to illustrate other possible values of these fields. Provide **screen prints** together with the web addresses.

Q.2.9) Start a new capture and apply multiple filters to visualize frames including cookies. Enter

http://www.odtuyayincilik.com.tr/

and add a book to the basket. Which fields contain unique IDs for you? How long will the web site will save the basket for you? Provide **screen prints** corresponding to your answers.

Q.2.10) If you visited the sites below, clear your DNS cache ("ipconfig /flushdns" for Windows, "sudo systemd-resolve --flush-caches" *for most Linux*). Start a new capture and enter

https://www.ece.cmu.edu/ and https://www.ece.cmu.edu.tr/

to your browser. What is the length of a DNS header and transaction ID? Which flag bit and what values signifies whether the DNS message is a query or response? What are the differences between the responses for the above addresses? Provide **screen prints** corresponding to your answers.
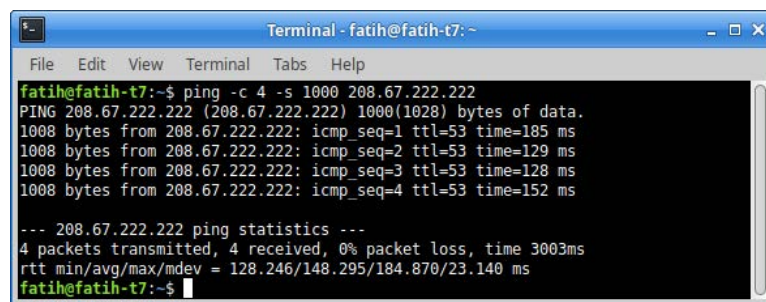
Part 3 – ICMP

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss. The results of the test are printed in form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

Q.3.1) Open command prompt and apply following functions (not at the same time). Explain each command and its output briefly. (*For* `ping` *on Linux, search flags* `-c, -s, -b;` *and* `traceroute`)

- `ping -l 1000 208.67.222.222`
- `ping -l 2000 208.67.222.222`
- `ping -l 9001 208.67.222.222` (hint: what is a "jumboframe"?)
- `ping 0.0.0.0`
- `ping 127.0.0.0`
- `ping 255.255.255.255`
- `tracert twitter.com` (You can also make another traceroute with ODTU VPN and compare the results)

Figure 2 - A sample screen print for ping function

The traceroute program can be used to figure out the path a packet takes from source to destination. In Windows, the source sends a series of ICMP packets (the first packet with TTL=1, the second packet with TTL=2, and so on) to the target destination. Recall that a router will decrement a packet's TTL value as the packet passes through the router. When a packet arrives at a router with TTL=1, the router sends an ICMP error packet back to the source. In this part, the native Windows *tracert* will be used.

Start the Wireshark live capture again. Apply a filter to observe ICMP traffic only. Open command prompt and apply `tracert www.google.com.tr` . Stop Wireshark tracing when the process is over.

Q.3.2) Select the first ICMP Echo Request messages that were sent by your computer for "traceroute", and expand the Internet Protocol part of the packet in the packet details window. What is the name in the upper layer protocol field, within the IP packet header? How many bytes are in the IP header? How many bytes are in the payload of the *IP datagram*? Explain how you calculated the number of payload bytes.

Q.3.3) Which fields of the IP datagram *always* change from one to the next? Which of the fields *must* stay constant?

Q.3.4) How many packets are sent with the same TTL? What is the reason for it?

Q.3.5) Find the ICMP TTL- exceeded replies sent to your computer. What are the changing and constant fields among the same router's replies? Which constant fields' values change when the source router changes? Explain the logic of each changing field.