Assignment 1: Wireshark, Ping, and Traceroute

The HiddenLife of Networks: Network Measurements

Deadline: 27/10/2023
Professor: Maria Papadopouli
TA: Katerina Lionta
mailing list: hy335a-list@csd.uoc.gr
TA: klionta@csd.uoc.gr

The objective of this assignment is to get familiar with passive network measurements, examine the format of packets, and start becoming more familiar with various network protocols (e.g., UDP, ICMP) that we have been discussing in class. Specifically, we will experiment with Wireshark, ping, traceroute, and examine packets, their IP addresses, size and estimate simple statistics.

You will employ **Wireshark**, a popular open-source packet capture and network analysis tool, widely used by network administrators, security professionals, and developers to analyze, troubleshoot, and capture network traffic.

Part 1: Wireshark (50pts)

Objective:

1.1 Open the Wireshark and choose the Wi-Fi interface (if you are connected with an Ethernet cable choose the interface that you observe traffic). Visit some websites like:

https://edition.cnn.com/
https://www.bbc.com/

Wait 5 minutes to ensure you have captured a sufficient number of packets.

a. How many packets have you captured? (5 pts)

b. ***UDP*** *(User Datagram Protocol) is a connectionless transport layer protocol in the Internet Protocol (IP). UDP does not establish a connection before sending data and does not guarantee delivery or order of packets. It is often used for real-time applications, such as streaming media and online gaming, where low latency and quick data transmission are more critical than ensuring every piece of data arrives intact.*
How many **UDP** packets have you captured? (5pts)

c. *An **IP (Internet Protocol)** address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. An IPv4 address is typically represented as a series of four numbers separated by dots (a.b.c.d). Each number is called an octet and represents 8 bits*.
Which is your **IP address**? How many packets were sent from your IP? How many packets were received by your IP? (10pts)

Include screenshots in your report and export the results of the Wireshark to a CSV file (File-> Export Packet Dissections-> As CSV…).

To find your IP address, in the following platforms:

- **Windows**: Open the command prompt type `ipconfig /all` and find the IPv4 Address field
- **Linux**: Open the terminal and type `hostname -I` and your IP address will be displayed just below the command.

1.2 The two datasets you will use are in this drive folder datasets_CS335a. These are two output files of specific Wireshark runs in CSV format. The fields of the datasets are:

No.: the serial number of the packet
Time: the time of the transmission/receiving of the packet (starts from 0, the moment that the capturing started) in seconds
Source: the source IP address
Destination: the destination IP address
Protocol: the protocol used
Length: the length of the packets in bytes
Info: extra information about the packet (header fields, flags etc)

Use the *pandas library* to open and process the CSV file (example: https://www.geeksforgeeks.org/convert-csv-to-pandas-dataframe/).

Develop a script that accepts a CSV file name as an input through a command line argument.

The script should load the data from the CSV file into a DataFrame and then generate various plots based on this data. (5pts)

1.3 Use the Matplotlib library (https://matplotlib.org/stable/gallery/index) to illustrate your data. Generate the following plots for the two datasets (DATASE1, DATASET2):

a. Create a bar plot that illustrates the top 2 destination IP addresses based on the number of packets they have received. This means you will generate one bar for each of the two IP addresses that received the highest number of packets. (5pts)

b. Generate a pie chart that visually represents the distribution of protocols(except UDP) used for sending the packets. This pie chart should display the percentage of the different protocols employed in the packet communication. (5pts)

c. Produce a bar plot that visually represents the number of packets received by the IP address 63.111.11.187 per second (only the seconds that the IP receives packets included in the plot). This line plot should show how the packet count for this specific IP address varies over time in terms of seconds. (5pts)

d. Generate a histogram that visually represents the distribution of packet lengths. Which is the packet size of the most packets (find the median)? (10pts)

Include in your deliverable the script and include in your report the plots that you generate from the script.
Don't hesitate to utilize any resources that you find helpful. You are not obligated to use the suggested libraries.

Part 2: Ping (25 pts)

The **ping** command is a network 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 source to the destination. It sends a series of **ICMP** (Internet Control Message Protocol) Echo Request messages to the target host and reports the time it takes for each message to be acknowledged.
The Internet Control Message Protocol (**ICMP**) is a network layer protocol within the Internet Protocol (IP) suite. It is responsible for sending error messages, diagnostics, and operational information between network devices. ICMP packets are encapsulated within IP packets and serve various purposes, including error reporting, network testing

2.1 Explain precisely and briefly what is the **Round Trip Time (RTT)**. (5pts)

2.2 Use the ping command to measure the RTTs in the following 3 hosts:

www.google.com
www.youtube.com
www.facebook.com
www.twitter.com

For the packets from which you received a response, estimate and report the minimum, average, and maximum round trip times in milliseconds. (10pts)

Include screenshots of the answers that you received in your report.

2.3 By default the Ping command sends 4 packets of 64 bytes [56 bytes(payload) + 8 bytes (header of the ICMP packet)] to the destination.

Run in the terminal the command `ping -h` to find the suitable flag in order to specify the packet size. Now send pings with 56, 512, and 1024 byte packets to the 4 hosts above. Estimate and report the minimum, average, and maximum round trip times in milliseconds for each of the 12 pings. Why are the minimum round-trip times to the same hosts different when using 56, 512, and 1024 byte packets? (10pts)

Part 3: Traceroute (25pts)

The **traceroute** command is a network diagnostic tool that helps identify the route taken by data packets from a source to a destination across an Internet Protocol (IP) network.

3.1 Run:

For Linux:

```
traceroute www.google.com
```

For Windows:

```
tracert    www.google.com
```

What is the number of hops that the packets had to pass through to reach their destination? (5pts)
Include a screenshot of the answer in your report.

3.2 Can you provide an explanation of how the **Time to live (TTL)** field is utilized by the traceroute command and what issue it aims to resolve? (10pts)

3.3 What is the minimum TTL required for the packets to reach their destination in 3.1? (5pts)

3.4 What could be the potential reasons for the following output received from the traceroute command (write at least two reasons)? (5pts)

```
 2     *        *        *     Request timed out.
 3     *        *        *     Request timed out.
 4     *        *        *     Request timed out.
 5     *        *        *     Request timed out.
```

Format Guidelines:

It is important that each plot **clearly** presents the titles and units of the x-axis and y-axis. It should also include legend(s) (also use grids).

Each Figure that may include one or more plots, should have a number id as well as a caption that clearly describes the main results of the plots.

Your report should have the following format:

- Font: Arial or Times New Roman
- Main text font size: 11pt; Title font: 12pt/bold; Figure caption (first line, in font size 10pt, bold) should include the main finding. A description of each plot should follow.

Submission:

1. Consolidate your report into a **single PDF** file, following the guidelines of the format
2. Include your **Python code** (with a readme) and the **CSVs files**
3. Compress them to a .zip file
4. Send them to **klionta@csd.uoc.gr** with the **subject: 335a_assign1_AM** (deliverables with different subjects will not be accepted)