Grading Guidelines:

A right answer will get full credit when:

1. It is right (worth 25%)
2. It is right **AND** neatly presented making it easy and pleasant to read. (worth an **extra** 15%)
3. There is an **obvious and clear link** between 1) the information provided in the exercise and in class and 2) the final answer. A clear link is built by properly writing, justifying, and documenting an answer (worth an **extra** 60%).
4. Calculation mistakes will be minimally penalized (2 to 5% of full credit) while errors on units will be more heavily penalized.

**Late Submission** : as specified in the syllabus. Days counting starts one minute after the deadline.

**Check Your Submission:**  after submitting, download your submission to check whether it is the right version and it is complete.

You are welcome/encouraged to discuss exercises with other students or the instructor. But, ultimately, **personal** writing is expected.

* USE THIS FILE AS THE STARTING DOCUMENT YOU WILL TURN IN. **KEEP IN THE QUESTIONS** AND INSERT YOUR ANSWERS.
* IF USING HAND WRITING (STRONGLY DISCOURAGED), REWRITE THE QUESTIONS.
* FAILING TO FOLLOW TURN IN DIRECTIONS /GUIDELINES WILL COST A 30% PENALTY.

Objectives of this assignment:

* to learn independently about an important topic
* to answer questions about the independently studied topic
* to empower you: you can learn any networking topic on your own
* to learn independently new concepts

What you need to do:

Answer the questions and/or solve the exercises described below.

KEEP THE GRADING GUIDELINES ABOVE TO REMEMBER THE DIRECTIONS AND HOW THE HOMEWORK IS GRADED. Make sure the show the date. No credit will awarded without showing the date the work was done.

Objective: The objective is to learn independently about *monitoring traffic* on your machine. I invite you to download, install, and use *Wireshark*. Wireshark is a popular sniffing tool that will allow you to monitor the traffic on any interface of your machine. After you figure out the basic functions of Wireshark, you will have to find out what a "secret agent" running on your machine sends out.

Resources:

1. Internet.
2. Wikipedia, Youtube (for short getting started tutorials on Wireshark)
3. Your TA and instructor

**Problem**

A program ***secretSender*** (executable only) is provided with this assignment on Canvas. We know that this program ***secretSender***, if executed, sends a secret message to some node with IP address IPx on Port Px. The objective is to find out

1) the message ***Ms*** sent,

2) the transport protocol used,

3) the IP address IPx of the destination host targeted by *secretSender.*

We know that *secretSender* sends **either** a datagram **or** a segment to Port number = 10076.

and 2) the IP address of the destination host.

You are required to perform the following tasks:

1) Download, install, and execute *Wireshark*.

2) Use any *Wireshark* tutorial for beginners. You will find some tutorials on *Youtube*. Try to learn only basic functions such that you know how to set a simple filter and display/examine a captured packet.

3) (25 points) Take a snapshot showing that you ran *Wireshark* on your machine.

Insert snapshot here .... (The screenshot must show is some way the date you took the snapshot)

Graphical user interface, application

Description automatically generated

4) Prepare *Wireshark* with the right filter to capture the secret message sent by *secretSender*.

Insert snapshot here showing and highlighting the filter used....

Graphical user interface, text, application

Description automatically generated



5) Execute *secretSender* by typing "java secretSender" on your command prompt.

6) (35 points) Take a snapshot that clearly shows the filter expression you used and the packet that contains the secret message ***Ms***. Highlight on the snapshot the filter function.

Insert snapshot here .... (The screenshot must show is some way the date you took the snapshot)

Graphical user interface, text, application

Description automatically generated



7) (20 points) Highlight on the snapshot the information we required you to provide, i.e, the message ***Ms*** sent, the transport protocol used, and the IP address IPx.

Insert snapshot here with the highlighted required information.... (The screenshot must show is some way the date you took the snapshot)

Graphical user interface, text, application

Description automatically generated



8) (20 points) Provide the message ***Ms*** sent, the transport protocol used, the IP address IPx, and the IP address of the machine on which *secretSender* was executed.

Insert snapshot here highlighting the message Ms .... (The screenshot must show the date).

**Graphical user interface, text, application

Description automatically generated**

The Message sent is shown in the bottom right box on the screenshot. It says, “ Peace Eagle.”

The IP address is shown at the top as it is highlighted in green. It says, “ip.addr == 131.204.14.247.”

The IP address from the machine where secretSender was executed is visible in the bottom left box, highlighted in gray. It says, “ Internet Protocol Version 4, Src: 172.19.101.186, Dst: 131.204.14.247.”

**What you need to turn in**:

* Electronic copy of this file (including your answers) (standalone). Submit the file as a Microsoft Word or PDF file.
* Recall that answers must be well written, documented, justified, and presented to get full credit.
* How this assignment will be graded:
* A right answer will get full credit when:
* It is right (worth 25%)
* It is right AND neatly presented making it easy and pleasant to read. (worth 15%)
* There is an obvious and clear link between 1) the information provided in the exercise and in class and 2) the final answer. A clear link is built by properly writing, justifying, and documenting an answer (worth 60%).
* Calculation mistakes will be minimally penalized (2 to 5% of full credit) while errors on units will be more heavily penalized.
* You are welcome/encouraged to discuss exercises with other students or the instructor. But, ultimately, personal writing is expected.