Exercise 1

- Start start a new capture session with wireshark
- Visit a web page
- Discover the ip of your classmate and ping it
- Stop the capture session

Protocols and IP Questions

- Examines and verify that DNS,TCP,HTTP,ICMP are contained.
- There are frames in which you are not the destination?
- How many ip addresses of destination not match your IP address?

UDP and DNS Questions

- Find the first DNS frame.
- What is the IP address of the sender in the packet?
- What is the port of the sender and destination?
- Verify that the length information in UDP is correct.
- Examine the payload of the first dns frame.
- What is the information in the frame that specifies whether it is an answer or a question ?
- Describe the contents of the query.
- How many bytes has the ID of a query?
- Find the response of the query.
- Verify that the ip addresses, the port and the ID are correct.
- What is the biggest datagram between the query and the response?
- How many answers are in the datagram? They have the same TTL?

TCP and HTTP Questions

- Filter the frame of “HTTP GET”.
- How many conversations are used?
- Find the sequence of handshake of initialization and termination of the connection. What are the bit flag that specify the initialization and termination of the connection?
- What is the real sequence number used of the first tcp frame.
- Calculate the length of the first “HTTP GET”
- The number of sequence and acknowledge are correct?

Exercise 2

- Download the java class www.mat.unical.it/ianni/storage/SendMail.java
- Compile class : javac SendMail.Java.
- Start a new capture session with wireshark.
- Send an email with SendMail: java SendMail <mail server> <sender> <reciver> <file>
- Stop the capture
- What is the IP of the mail server?
- Change the receiver in a wrong mail and restart the program. What happened? Use wireshark to reconstruct the smtp conversation.

Exercise 3

Step1. Write a simple script *askScholar* that receives as parameters a sequence of word separated by spaces, for example: *askScholar network security*

The script have to query scholar.google.com with the url: http://scholar.google.com/scholar?hl=en&q=<key word separated by +> and return the number of results that are specified in the output phrase: *"About N results"* .

Step2. Do a script similar to *askScholar* that receive from input a file that contain a list of word to search and for each line the script query scholar.google.com and find the number of result of the words in that line. The output of the script is the file taken from input sorted by number of results.

Example:

File input:

WORD1

WORD1 WORD2 WORD3

WORD1 WORD2

Output file:

WORD1 WORD2 23435

WORD1 1034

WORD1 WORD2 WORD3 35