Assignment 1. Traffic Analysis

Traffic analysis is a fundamental tool for many network management tasks, and has various applications related to computer security, such as identification of insecure protocols, collect information of various kinds, or perform network reconnaissance.

The aim of this work is to develop the ability to analyse traffic and recognize some of the type of traffic usually found in a network. To this end, a set of packet captures (made using **Wireshark**) is given, and you are required to elaborate a report that describes each of the captures in detail. This assignment is to be developed in groups between 2 and 3 elements.

In all cases, try to make your report as objective as possible. Bear in mind that the goal of this class in *security*. Put the information in an organized manner and clearly explain the evidence that led to your conclusions.
The evaluation criteria for each capture differ and all captures are quoted equally.

The captures can be download from Moodle (https://moodle.isep.ipp.pt). The groups must analyse them and write a report that clearly and unequivocally identifies in each of them:

a. The intervenient(s);
b. The main protocol;
c. The performed operations of the main protocol (who starts, who answers, communication characteristics and data if applicable, etc.);
d. Safety problems that may occur and how to mitigate them;
e. [optional] Any other consideration of importance.

Captures should be analysed on your own system and not on the VM assigned to each group/student.

A single student of each group must upload the report in PDF format to Moodle until the date specified in Moodle. The name of the report must comply with the format

Teacher_acronym_Student1#_ Student2#[…]_StudentN#.PDF

as for XXX_9999999_9999998.PDF for a group of a class with teacher XXX with the students 9999999 and 9999998.