VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

Telecommunication Networks Introduction to Computer Networks (homework)

Date: 22. 4. 2020
Author: Ing. Petr Machník, Ph.D.
Contact: petr.machnik@vsb.cz
Subject: Telecommunication Networks

Lesson objectives

The objective of this practical lesson is to capture and analyze network traffic using a protocol analyzer Wireshark.

Study from the lectures before the lesson:

The OSI reference model and TCP/IP protocol model (Chapter 2 - Protocol Models) - names and order of layers of both models, their basic characteristics, the principle of encapsulation, the basic features of IP, TCP and UDP protocols.

Instructions on the practical lesson in the area of computer networks

Wireshark Network Analyzer

The Wireshark programme is used to capture and analyze transmitted data. This may cover not only data intended for the given computer, but also foreign data that arrive at the computer's network interface card and would be normally ignored. The Wireshark is a freeware programme (see www.wireshark.org).

Launching the Wireshark: Open the terminal window, gain the administrator's rights (**`su`** command and type the password used on the lab computers upon request) and type **`wireshark`** there to launch this programme. Choose the icon *Capture options* from the top bar, it will open the window where you can set parameters according to which the traffic capture will take place (e.g. which network interface cards will be involved in capturing, what should be captured, etc.) Select only the network interface card, on which the traffic will be captured and click on *Start*.

The programme will start capturing all the traffic near the network interface card from that moment. Now, it is possible to generate own traffic (by the command **`ping`**, by opening the website, etc.). Clicking on the icon *Stop capturing packets* will stop capturing traffic.

Now, we can analyze the captured frames. The Wireshark window consists of three separate sections (see Figure 1). In the first part there is a brief description of all captured data frames. In the second part, you can see the details regarding the frame selected in the first part of the window. Information is divided based on the layers of the TCP/IP model. You can get more detailed information by clicking on the small triangle at the beginning of the line. The third part shows the exact contents of the frames in the hexadecimal form. Out of all captured frames, it is possible to extract those that are the important for us by means of the filters. Using the *Follow TCP stream* function which is offered by right-clicking of the mouse on the frame in the first part of the window which is a part of the examined connection, it is possible to extract only those out of the captured frames which are related to a specific TCP connection. You will also see all the useful information transferred during this connection (e.g. the source code of the web site).

Tasks

1) Using the network analyzer Wireshark, capture and identify the ICMP (Internet Control Message Protocol) messages – echo request and echo reply (are generated by the command **`ping`**).

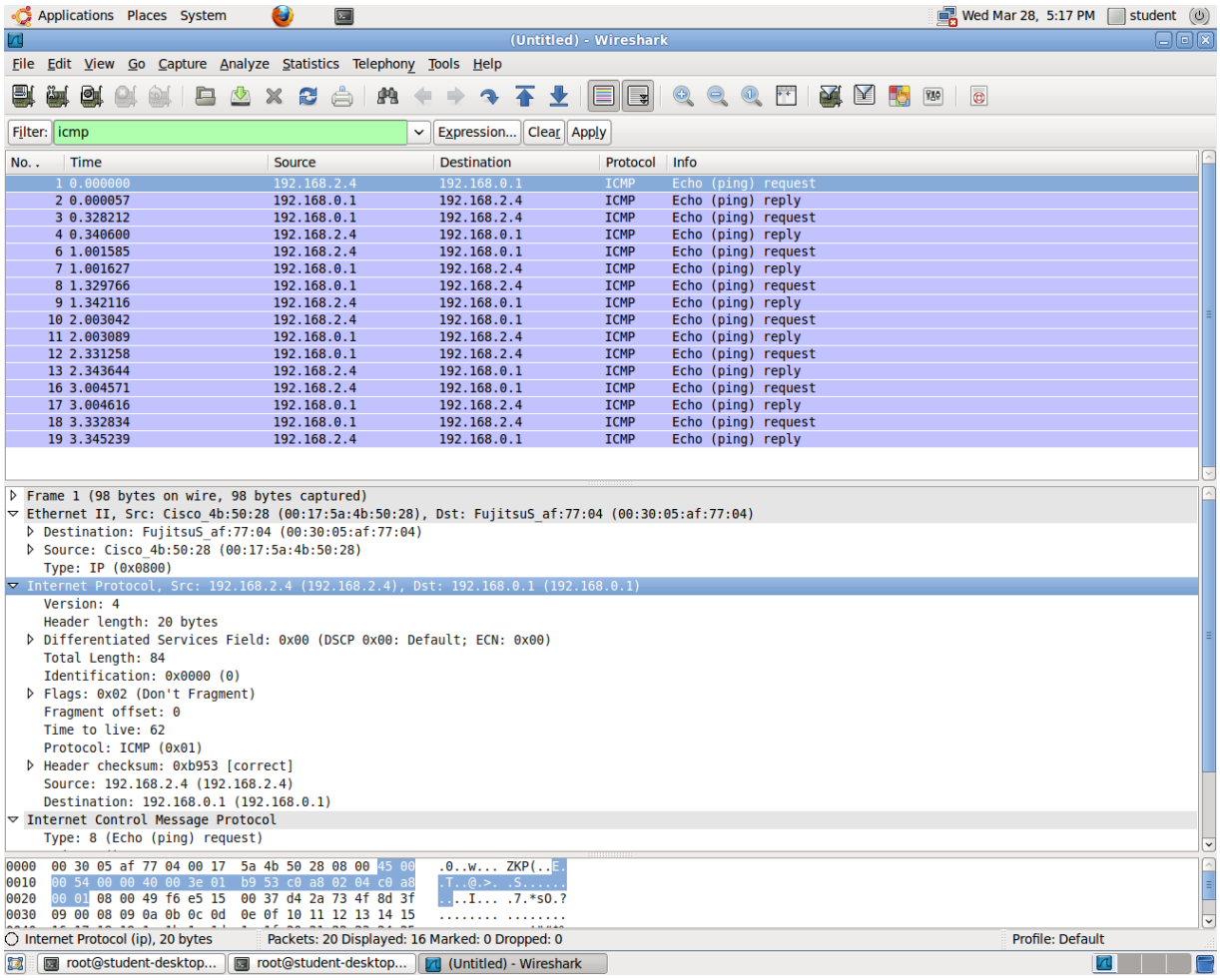

Fig. 1 ICMP messages captured by Wireshark

2) Using Wireshark, capture and identify communication when downloading a web page – HTTP (HyperText Transfer Protocol) at the application layer and TCP (Transmission Control Protocol) at the transport layer. To translate a web address into an IP address, the DNS (Domain Name System) protocol is used.

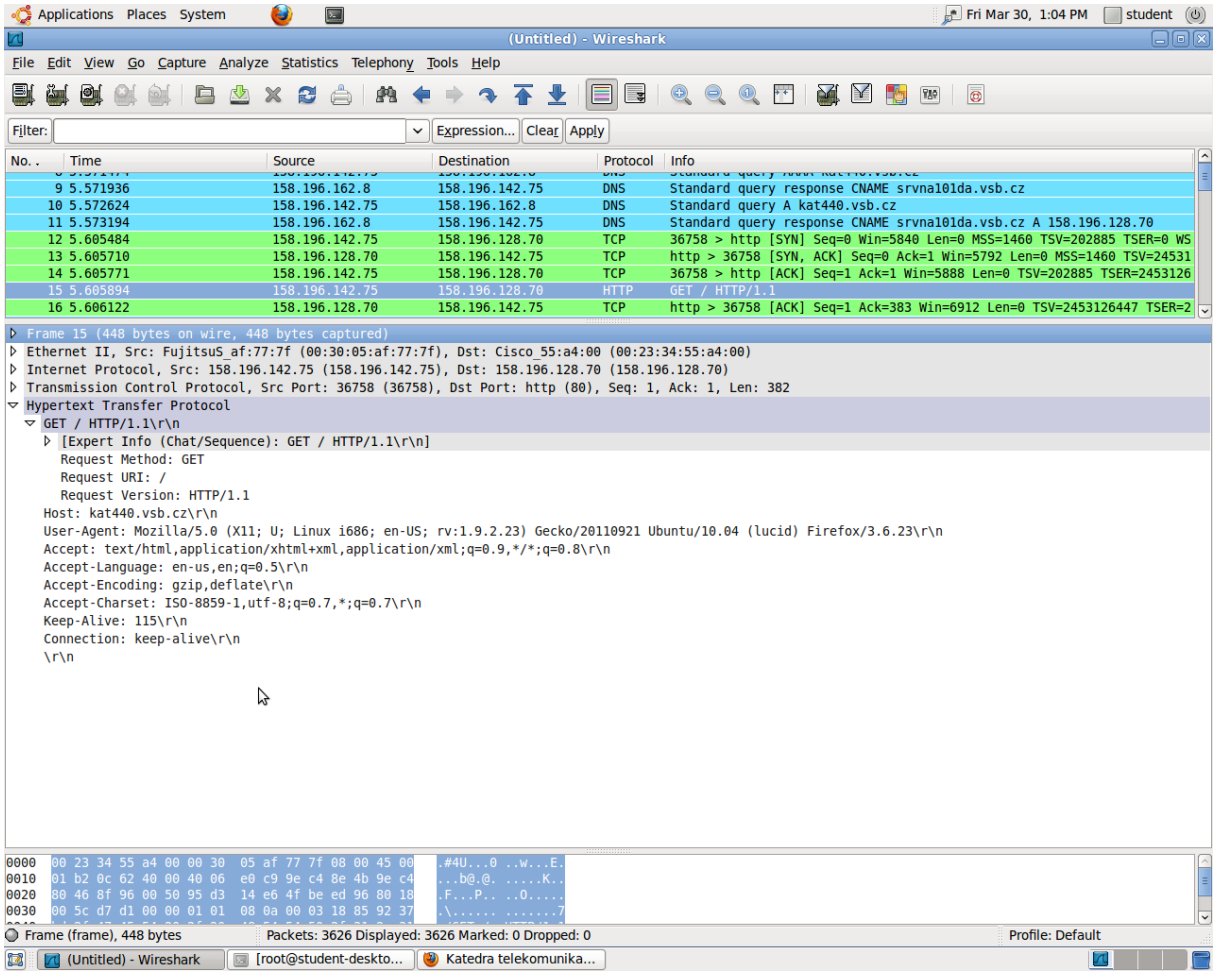

Fig. 2 The process of communication with a web server captured by Wireshark

3) Using Wireshark, capture and identify communication when sending an e-mail. When sending an e-mail via the web interface, HTTP is used. In general, SMTP (Simple Mail Transfer Protocol) is used for sending an e-mail and POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) for downloading an e-mail from the e-mail box.

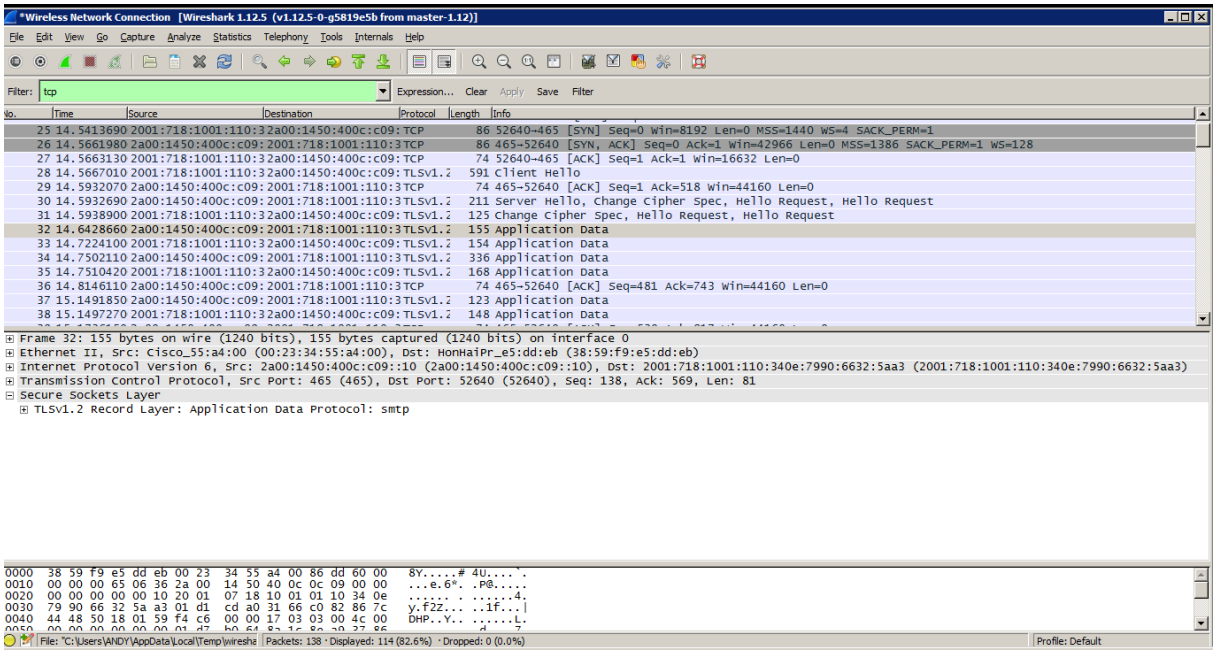

Fig. 3 The process of secure communication when sending an e-mail by SMTP protocol captured by Wireshark

4) Create a report that contains images with an example of captured traffic according to tasks 1) - 3). Follow Fig. 1 - 3. IP addresses and web addresses may of course be different, but try to capture messages of the same protocols - ICMP, DNS, TCP, HTTP, TLS, etc. Briefly describe the captured communication. Submit the report in PDF format on the website lms.vsb.cz - Telecommunication Networks course.