**LAB 4**

**INTRODUCTION TO WIRESHARK**

In this lab you learn to perform basic actions in Wireshark.

User manual: https://www.wireshark.org/docs/wsug\_html\_chunked/

1. If this has not yet happened: Download the latest and stable 64 bit version of the network protocol analyzer software **Wireshark** at <http://www.wireshark.org/>

With this open source software, you can capture and view the details of network packets entering or leaving your network card.

Install Wireshark **and make sure WinPcap is installed with it.** USBPcap may optionally be installed as well, but is not required.

1. Download the file **Capture1.pcapng** (PCAPNG = Packet Capture Next Generation) from Leho and open it by double clicking on it.
2. The opened file contains a number of packets that were sent to/from a computer’s network card during a capturing session.

How many packets were captured?

19055 packets

The main window of Wireshark consists of the following components from top to bottom:

* The menu
* The toolbar
* The filter toolbar
* The packet list panel
* The packet list detail panel
* The packet list byte panel
* The status bar

1. The captured packets are colored according to specified rules by default.

What kind of packets have a light green color?

HTTP-packets

What kind of packets have a light blue color?

UDP-packets

What color are the ICMP packets?

They have a pink color

Hint: use the View > Coloring Rules menu to find the answer.

1. Usually you are not interested in all packets, but only a certain kind of packets. You can limit the number of packets by using a **display filter** that you need to type into the filter toolbar (under the regular toolbar).

With a display filter, make sure that only the DNS packets are shown in the packet list panel.

dns

How many such packets are there? You can find this number in one of the components of the Wireshark window...

182

1. Save these filtered packets in a separate file named ***dns-packets.***

Then open this new file to make sure it contains only DNS packets.

1. Then close the DNS packets file and return to the capture1 file.

Remove the display filter so that you can see all the packets again.

1. In Wireshark you can also use the search function to search for specific packets.

What key combination can you use for this?

CTRL+F

Use this to track all ICMP packets and write down their numbers below.

**Packet numbers =** 205 and 2352

1. You can also search within the data field of a packet for a specific **string** (word, text,...), provided that you explicitly indicate this in the field before the search box (see figure below).

This way, look for the string *user* in the **packet bytes** of the capture file.

Hint: use the following selections:



What is the number of the first packet that meets your search conditions?

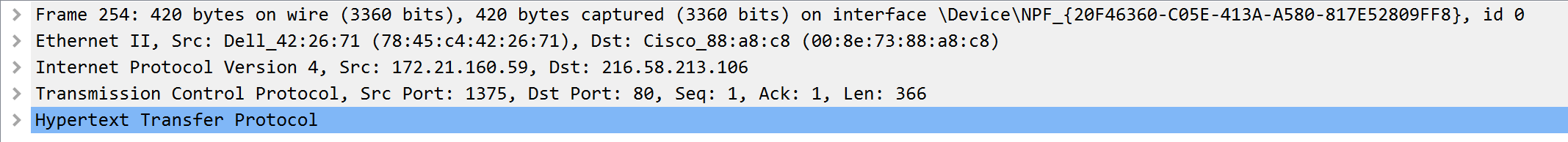
**Packet number =** 206

1. Select Packet **No 254**. Do this by pressing a key combination. Which one?

Hint: Open the ***Go*** menu.

**Keyboard combination =** CTRL+G

1. Paste below the detail pane of this packet.



This detail pane consists of 5 lines that can be folded open (by clicking on the bigger-than-sign) to see even more detail info.

* The first line contains general information about the packet.
* The second line contains *Network Access Layer* (OSI layer 1 and 2: *Physical* and *Data Link*) header information.
* The third line contains *Internet Layer* (OSI layer 3: *Network*) header information.
* The fourth line contains *Transport Layer* (OSI layer 4: *Transport*) header information.
* The fifth line contains the *Application Layer* (OSI layer 5 till 7: *Session, Presentation & Application*) header information and packet data.

1. What 4 protocols are used in that frame (No 254)? Situate these protocols **in the TCP/IP model** by entering their names in the 2nd column of the table below.

|  |  |
| --- | --- |
| **TCP/IP layer** | **Protocol name** |
| Application Layer | HTTP |
| Transport Layer | TCP |
| Internet Layer | IP |
| Network Access Layer | Ethernet |

1. In the first table below, enter the names of the protocol headers that are *before* the HTTP data field of this frame (No 254), in the correct order. Also note under each field how many bytes that header is. (Replace every ‘??’)

|  |  |  |  |
| --- | --- | --- | --- |
| **Ethernet** HEADER | **IP** HEADER | **TCP** HEADER | HTTP DATA |
| **14** bytes | 20 bytes | 20 bytes | 366 bytes |

Note that some protocols use some kind of ‘addresses’ or ‘ports’ (more details in next lectures). IP addresses are written in 4 ‘dotted’ decimal numbers and MAC addresses consist of 12 hexadecimal digits (see previous labs). Ports are written as one decimal number.

There are 2 ports, 2 IP addresses and 2 MAC addresses in this frame. What are their values? And in which order do they appear in the frame?

Dest. Addr Src. Addr. Src. Addr. Dest. Addr Src. Port Dest. Port.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 00:8E:73:88:A8:C8 | 78:45:C4:42:26:71 | 172.21.160.59 | 216.58.213.106 | 1375 | 80 | HTTP DATA |

1. Who manufactured the network cards of the transmitter and the receiver of frame number 206?

Hint: this is Network Access information.

**Manufacturer NIC of the transmitter =** Dell

**Manufacturer NIC of the receiver =** Cisco

1. Wireshark can also be used for capturing live.

To do this, proceed as follows to capture the packets sent out and received by a PING command.

* In Wireshark, close the opened file (without closing Wireshark).
* Double-click in the welcome screen of Wireshark under “Capture” on your (wireless) NIC to start capturing.
* Go to the command prompt of your host and ping (not surfing but pinging) to www.howest.be. Wait till you get all the replies.
* Go back to Wireshark and stop capturing it. This can be done very quickly with the red button in the toolbar.

1. It may well be that not all captured packets are a result of your PING command.

The PING command is based on the use of the ICMP protocol. Therefore, only show the ICMP packets resulting from your PING command.

How many ICMP packets were captured?

8

Explain why this number of ICMP packets was captured.

It is the request and the response x the amount of packages that were sent.

Is the destination MAC address in the captured echo request packets, the MAC address of the computer we are pinging (i.e. the Howest web server in our scenario), or is that the MAC address of the default gateway?

Explain your answer. Give enough explanation!

It is the default gateway. Since we are not pinging in the same network, the device sends the packages to the default gateway of the other network. We can see this by looking at the IP address from the home computer and the Howest server.

1. Also check out the data part of such an ICMP packet in the packet list byte panel. What kind of data is in there?

Letters of the alphabet