



Middle East Technical University



Department of Computer Engineering

CENG 435

Data Communications and Networking

Fall 2020–2021

Wireshark Take Home Exam 4

Due date: 14 January 2021 - Thursday

1 Introduction

In this assignment, you will get some knowledge about the *Network Layer - Control Plane* and *ICMP (Internet Control Message Protocol)*. You will analyze the network packets using the *Wireshark* tool, as you did before in the previous assignments. Please follow the steps below

1. Capture the network traffic with the required packets.
2. Take the required screenshots as described with the examples.
3. Answer the questions.

Before starting, there are some important reminders below,

Important Reminder 1: For this homework, Linux based operating systems are strongly advised instead of Windows operating system.

Important Reminder 2 (for Windows Users): Completing the “capturing the network traffic” parts in Windows is strongly not recommended for this homework. Even if you close all the browsers or applications that create traffic in the network, there could be many applications in the background that create traffic in the network for Windows. Therefore, you may not capture the required packets or although you capture the required packets, you may not get clean captures and these could cause some problems. The commands in the rest of the homework are terminal commands (Linux terminal) and in the parentheses as you will see there are also command prompt (Windows) equivalents of these commands, you can use them in Windows, however, for your “Windows-specific issues”, please firstly prefer to search on the Internet.

Important Reminder 3: The packets that you are expected to capture are explained with some example screenshots in the sections, you must see these packets to answer the questions. If you do not see some of them, try to capture again.

Important Reminder 4: In this assignment, you will use only the “Wireshark” tool and “terminal” (or “command prompt” in Windows). Do NOT use any browser or application that creates traffic in the network, so before capturing, close any other program which is related to network traffic including browsers.

Important Reminder 5: It is advised to connect to the Internet via Wi-Fi and in “Wireshark”, capture the traffic with the interface that you connect to the Internet (NOT loopback interface, etc.).

Important Reminder 6: After capturing the network traffic, save the “.pcap” file in a safe place, you will send us as you did in the previous assignments.

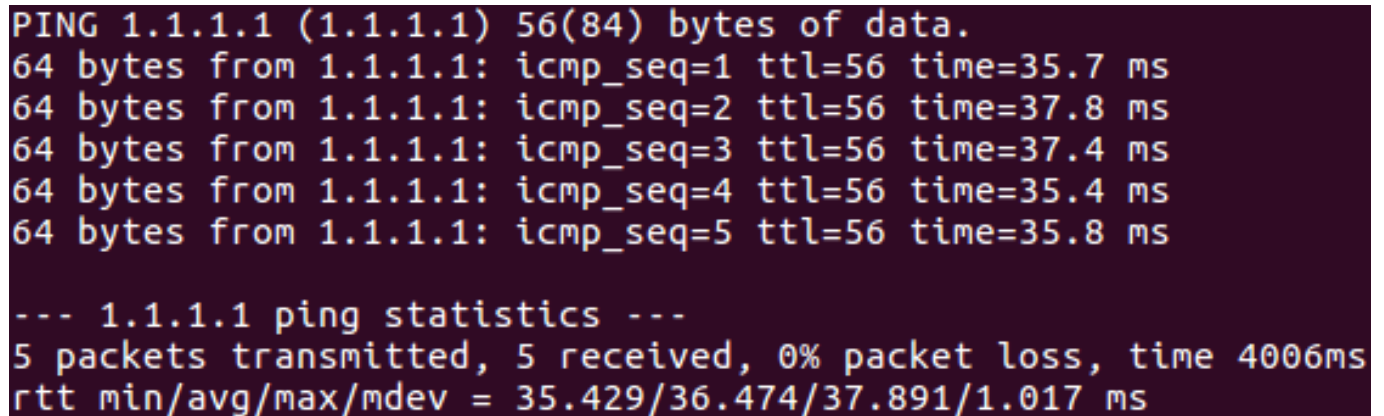
2 ICMP Packet Analysis & Routing Rules

2.1 Capture the Network Traffic

1. Close all programs and applications that create traffic in the network including browsers.
2. Open a terminal (command prompt in Windows).
3. Open “Wireshark” and start to capture the interface that you connect to the Internet.
4. Switch to the terminal and run the ping command below,

```
ping -c 5 1.1.1.1  
For Command Prompt (Windows): ping -n 5 1.1.1.1
```

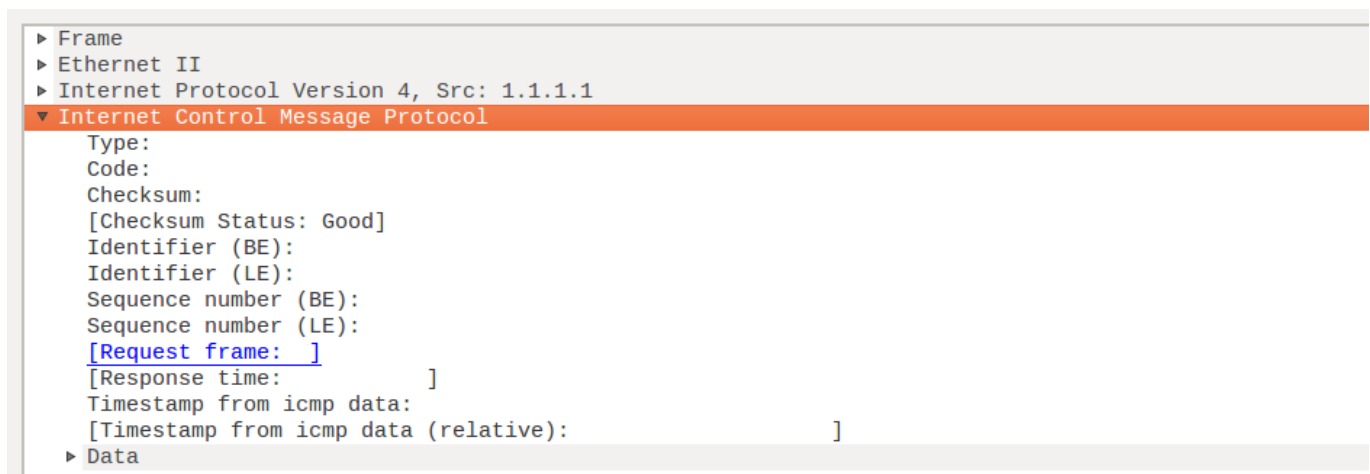
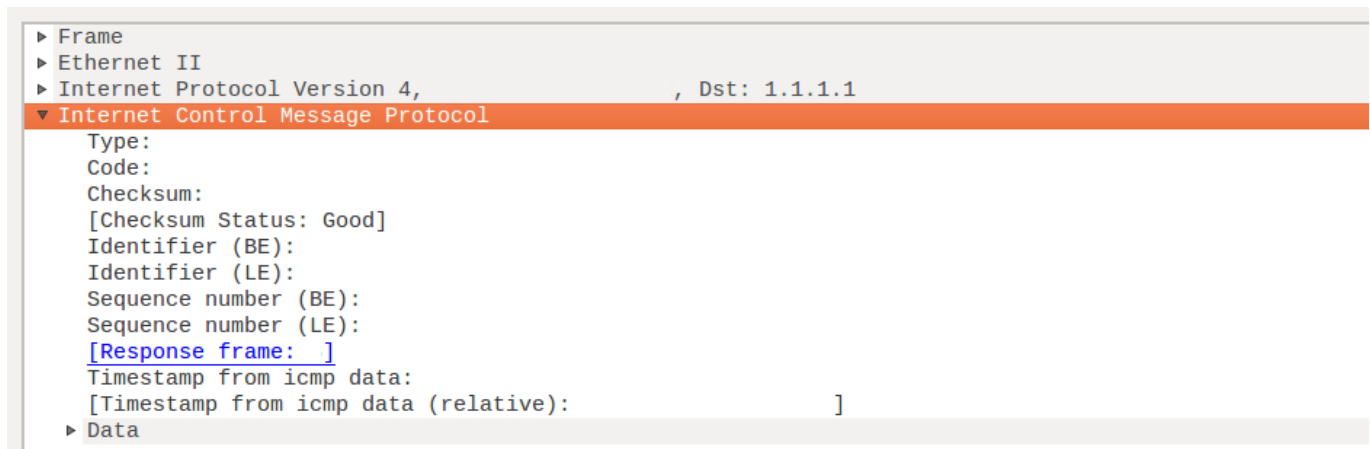
5. In the terminal, you have to see the result similar to the image below (If the packet loss is NOT 0%, repeat from the step three above.) (Command prompt (Windows) users have to see a similar output but not exactly the same output.).



```
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.  
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=35.7 ms  
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=37.8 ms  
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=37.4 ms  
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=35.4 ms  
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=35.8 ms  
  
--- 1.1.1.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4006ms  
rtt min/avg/max/mdev = 35.429/36.474/37.891/1.017 ms
```

Example “ping” Result

6. Stop the capture in Wireshark and save the capture dump as **e<your_student_id(7 digits)>-ping.pcap** file (Ex: **e1234567-ping.pcap**) to a safe place because you will upload it to the system while uploading your homework.
7. You must see 5 “ICMP” requests and 5 “ICMP” responses (If you cannot see them there could be a problem with the interface you have chosen, repeat from the step three above with choosing a different interface.).
8. Double click to a successful “**ICMP request**” packet to open its “Packet Details” window.
9. You will see four headings (the last one must be “Internet Control Message Protocol”) at the upper side of the window and you will see “Packet Bytes” pane at the lower side of the window.
10. Click to expand the last heading which is “Internet Control Message Protocol”. Be sure it is expanded and take a screenshot of that state of the “Packet Details” window’s upper side.
11. This time double click to a successful “**ICMP reply**” packet to open its “Packet Details” window. Do again the step nine and ten above and then take a screenshot as explained in the step ten for the “ICMP reply” packet this time.
12. The example screenshots for ICMP request and reply packets are below,



13. Of course, most of the information is hidden in these screenshots, however, the state of the “Packet Details” window must be the same as in the screenshot.
14. Then, go back to the terminal (command prompt in Windows), run the following command and find your routing table,

15. The column headings of the tables must be like in the screenshots below for Linux or Windows users and, of course, there must be some rows (rules) in the tables.

IPv4 Route Table				
=====				
Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric

Example Routing Table (Windows)

16. Then, take a screenshot of your routing table.
17. Put these screenshots in your report pdf and answer the questions below.

2.2 Questions

1. What are the IP addresses of the source host and the destination host for both of the request and reply packets? **(10 Points)**
2. As you can see, in the packet information of both request and reply packets, there is not any port number information. Why does not an ICMP packet have a source and destination port? **(20 Points)**
3. Look at the “type” and “code” fields in the request and reply packets.
 - (a) For what purpose are these “type” and “code” fields used? Explain briefly. **(15 Points)**
 - (b) As you can see there are some numbers in these “type” and “code” fields in the ICMP request and response packets. What is written in these fields and what do they mean? **(15 Points)**
4. By looking at the ICMP request packet information, find how many bytes are transferred in total. Then, explain where these bytes are used or what is the information do they carry? At final, sum them up and find total transferred bytes (For the previous headers before ICMP, you do not have to explain in detail. Writing how many bytes are used for these headers is enough. However, in the ICMP packet, you have to explain these bytes field by field.). **(20 Points)**
 For example, “a” bytes are used for protocol “b”s header + ... + “c” bytes are used for the “d” field of ICMP packet + ... = “e” total bytes
5. By considering your answer for the first question and routing table screenshot above, which rule should we remove so that the outgoing packets will be dropped and, thus, as a result, we cannot send any ping request? Explain why? **(20 Points)**

3 Other Specifications

- **This is an individual assignment. Using any piece of code, discussion, explanation, etc. that is not your own is strictly forbidden and constitutes as cheating. This includes friends, previous homework, or the Internet. The violators will be punished according to the department regulations.**
- **Late Submission: Late submission is allowed as stated in the course syllabus.**
- Follow the announcements on our ODTUClass page for any updates and clarifications. Please use the discussion forum on ODTUClass first for your questions instead of e-mailing if the question does not contain code or a solution. Your question might have already been answered or the answer you get might help your peers.

4 Submission

- Your assignment report's name and format **MUST** be **e<your_student_id(7 digits)>-report.pdf** (Ex: **e1234567-report.pdf**).
- You **MUST** write your report on the computer. Handwriting and scanning submissions will **NOT** be accepted. “**e1234567-report.tex**” file was shared with you in ODTUClass as a template for your report. Please **use this template** while preparing your report and be sure that the screenshots you have put in your report are readable.
- You **MUST** have **two files** to submit (Ex: **e1234567-ping.pcap**, **e1234567-report.pdf**) and there are two place to submit your files in ODTUClass. You **MUST** submit your **report pdf** file to “**Wireshark Take Home Exam 4 - Report (Turnitin)**” and your “**.pcap**” file to “**Wireshark Take Home Exam 4**”.