

**VILNIUS UNIVERSITY  
SIAULIAI ACADEMY**

PROGRAMŲ SISTEMOS BACHELOR STUDY PROGRAMME

Software engineering

**ANNA KUTOVA**

**Computer Networks**

**Laboratory work No.5**

**ICMP**

Šiauliai, 2025

# **Laboratory Work Report**

# Table of contents

[1. ICMP and Ping 3](#_Toc198917855)

[2. ICMP and Traceroute 6](#_Toc198917856)

[3. Extra Credit 12](#_Toc198917857)

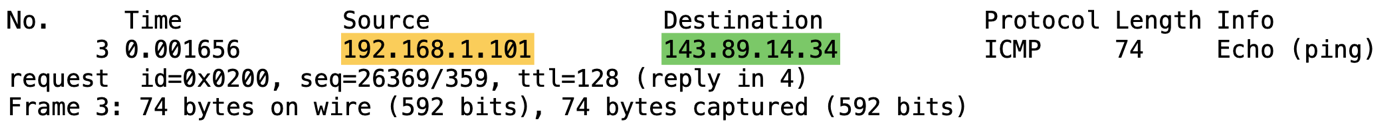
This lab report is based on a combination of live-captured packets on **macOS** and provided trace files from the official Wireshark lab materials.

To maintain consistency and address the differences between platforms, I used the following packet traces for each part:

* **ICMP and Ping (Questions 1–4):**  
  Analysed using the provided trace file **icmp-ethereal-trace-1**.
* **ICMP and Traceroute (Questions 5–6):**  
  Performed on my **macOS system**. Since macOS uses **UDP packets** for traceroute, these responses were used to answer platform-specific questions.
* **ICMP Echo and Error Packet Details (Questions 7–9):**  
  To observe **ICMP Echo Request, TTL-Exceeded, and Destination Unreachable** messages in a **Windows-style traceroute (ICMP-based)**, I used the trace file **icmp-ethereal-trace-2**, as instructed in the lab manual.
* **Question 10:** Performed on my **macOS system**

## ICMP and Ping

1. *What is the IP address of your host? What is the IP address of the destination host?*

**

**Answer:**

* 1. Source IP address (author’s host): **192.168.1.101**
  2. Destination IP address (target host): **143.89.14.34**

1. *Why is it that an ICMP packet does not have source and destination port numbers?*

**Answer:** Because ICMP is in network layer:

🡪 ICMP operates at the network layer (Layer 3) of the OSI model, while ports are a feature of transport-layer protocols like TCP and UDP (Layer 4).

🡪 ICMP does not need ports because it is not used to identify application processes, but rather to send control messages and diagnostics (e.g., Ping, TTL exceeded).

🡪 So ICMP messages do not include source or destination port numbers.

1. *Examine one of the ping request packets sent by your host.*

*What are the ICMP type and code numbers?*

*What other fields does this ICMP packet have?*

*How many bytes are the checksum, sequence number and identifier fields?*

*A screenshot of a computer

AI-generated content may be incorrect.*

*A screenshot of a computer program

AI-generated content may be incorrect.*

**Answer:**

* 1. ICMP Type: **8**

ICMP Code: **0**

* 1. Other fields present:

- Checksum: 2 bytes (0xe45a)

- Identifier: 2 bytes (0x0200)

- Sequence Number: 2 bytes (0x6701)

* 1. Each field (Checksum, Identifier, Sequence Number) is 16 bits = 2 bytes

1. *Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?*

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer code

AI-generated content may be incorrect.**

**Answer:**

* 1. ICMP Type: **0**

ICMP Code: **0**

* 1. Other fields present:

- Checksum: 2 bytes (0xec5a)

- Identifier: 2 bytes (0x0200)

- Sequence Number: 2 bytes (0x6701)

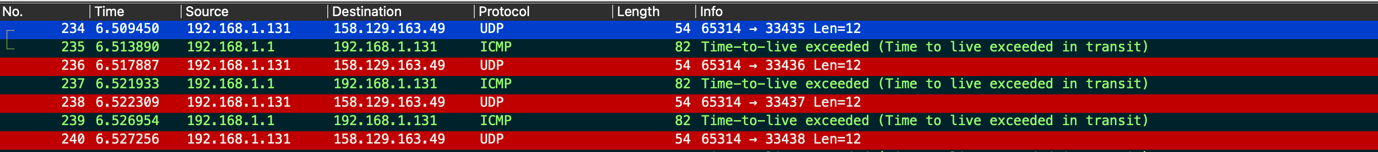
* 1. Each field (Checksum, Identifier, Sequence Number) is 16 bits = 2 bytes

## 2. ICMP and Traceroute

A screenshot of a computer

AI-generated content may be incorrect.

1. *What is the IP address of your host? What is the IP address of the target destination host?*

**

**Answer:**

* 1. Source IP address (my host): **192.168.1.131**
  2. Destination IP address (target host): **158.129.163.49**

1. *If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?*

*A screenshot of a computer

AI-generated content may be incorrect.*

**Answer:** Since this trace was captured on a Unix-like system (macOS), the traceroute utility uses UDP packets instead of ICMP for probes.

As a result, the IP protocol field is set to 17, which is the protocol number for UDP, not 1 (which corresponds to ICMP).

1. *Examine the ICMP echo packet in your screenshot.*

*Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?*

*A computer screen shot of a program

AI-generated content may be incorrect.*

**Answer:** *as I noticed in previous task, I use macOS, so for this task I will use ICMP-ethereal-trace-2, starting from this question.*

*A screenshot of a computer

AI-generated content may be incorrect.A computer screen shot of a computer code

AI-generated content may be incorrect.*

Yes, this ICMP echo packet is slightly different from the ping query packets analyzed in the first part of the lab.

In the first part (*from* *icmp-ethereal-trace-1*), the ping queries had a TTL value of 128, while in this packet (Frame 1 *from icmp-ethereal-trace-2*), the TTL is set to 1.  
 Other fields remain consistent with a normal ICMP Echo Request structure.

1. *Examine the ICMP error packet in your screenshot.*

*It has more fields than the ICMP echo packet.*

*What is included in those fields?*

**Frame 1:***A screenshot of a computer

AI-generated content may be incorrect.*

**Frame 2:***A computer screen with text and numbers

AI-generated content may be incorrect.*

**Answer:** Yes, the ICMP error packet (Frame 2) includes more fields than a standard query ICMP Echo packet. It contains both the IP header and the first 8 bytes of the original ICMP packet that caused the error. This helps the sender identify which packet triggered the response.

It’s possible to see this in Frame 2, where the ICMP message includes:

* + - The original IP header (from 192.168.1.101 to 138.96.146.2)
    - The embedded ICMP Echo Request (Type 8, Identifier 0x0200, Sequence Number 0xa401)

1. *Examine the last three ICMP packets received by the source host.*

*How are these packets different from the ICMP error packets?*

*Why are they different?*

*A screenshot of a computer

AI-generated content may be incorrect.*

*A purple rectangular object with black text

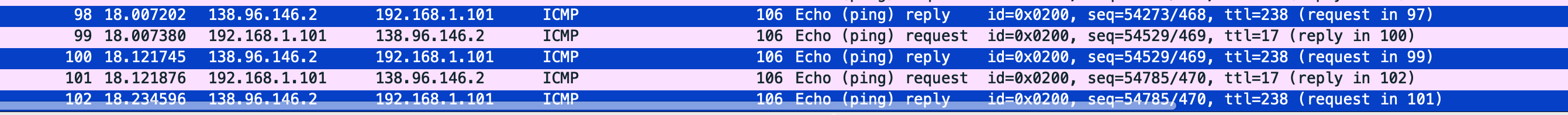
AI-generated content may be incorrect.A green and black text

AI-generated content may be incorrect.*

*A yellow and black text

AI-generated content may be incorrect.*

**Answer:**

The last three ICMP packets received by the source host are:

* + - Frame 98
    - Frame 100
    - Frame 102

1. **Differences:**

| **Field** | **Echo Reply (e.g. Frame 98)** | **ICMP Error (e.g. Frame 2)** |
| --- | --- | --- |
| **ICMP Type** | 0 (Echo Reply) | 11 (Time Exceeded) |
| **Direction** | From **destination host** (138.96.146.2) | From **intermediate router** (e.g. 10.216.228.1) |
| **Purpose** | Shows packet **successfully reached** the target | Shows packet **expired** mid-route |
| **Contains Embedded Data?** | Just ping reply payload | Includes the **original IP header + 8 bytes of original data** |

1. These last three packets are ICMP Echo Replies, meaning the probes successfully reached the destination. Their TTL is high (238), and they include only standard reply fields. Unlike ICMP error messages (Type 11), they don’t contain the original IP header, since no error occurred.
2. *Within the tracert measurements, is there a link whose delay is significantly longer than others?*

*Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others?*

*On the basis of the router names, can you guess the location of the two routers on the end of this link?*

**Answer:**

a. My traceroute results:  
**A screenshot of a computer

AI-generated content may be incorrect.**

Yes, there is a noticeable delay increase between hop 5 and hop 6.

Hop 5 (10.15.1.14) has round-trip times around 20–21 ms.

Hop 6 (mad-b4-link.ip.twelve99.net (213.155.129.70)) jumps to around 48 ms, which is more than double.

b. Figure 4: A screenshot of a computer

AI-generated content may be incorrect.

Yes, from 9 to 10 in figure 4.

In figure 4 the first location is NYC and the second is Pastourelle.

## 3. Extra Credit