4

VILNIUS UNIVERSITY
SIAULIAI ACADEMY

PROGRAMŲ SISTEMOS BACHELOR STUDY PROGRAMME

Software engineering

ANNA KUTOVA

Computer Networks

Laboratory work No.4

IP

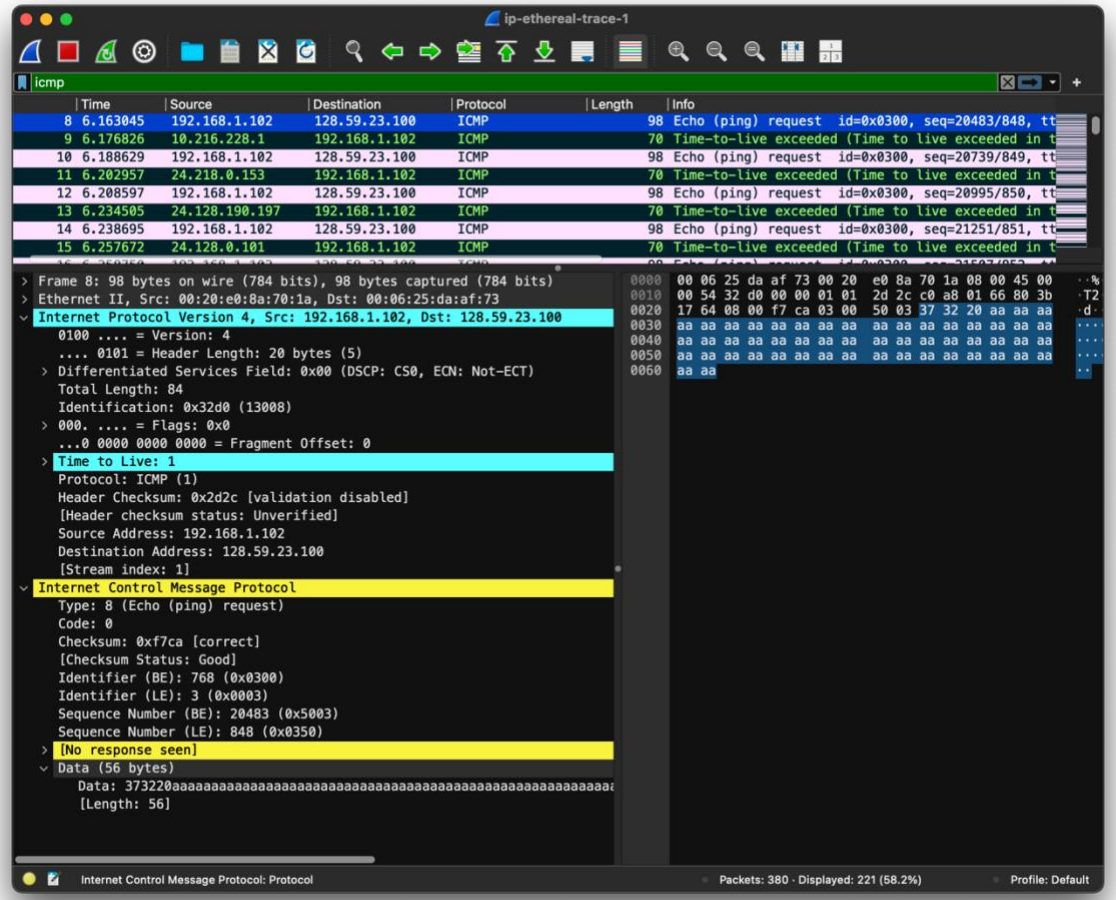
Šiauliai, 2025

Laboratory Work Report

Table of contents

1. Capturing packets from an execution of traceroute

2. A first look at the captured trace



1. *Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.*
   What is the IP address of your computer?

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping)

Answer: the IP address of my computer is **192.168.1.102**

2. *Within the IP packet header, what is the value in the upper layer protocol field?*

```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: 00:20:e0:8a:70:1a, Dst: 00:06:25:da:af:73
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
```

```
Time to Live: 1
Protocol: ICMP (1)
```

Answer: ICMP (1)

3. *How many bytes are in the IP header?*
   How many bytes are in the payload of the IP datagram?
   Explain how you determined the number of payload bytes.

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
```

Answer:

a. Bytes in the IP header : **20 bytes**
b. Bytes in payload : **64 bytes**

c. 84 – 20 = 64 ((Total – header) length)

4. *Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.*

```
 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment Offset: 0
```

Answer:

a. No, this IP datagram hasn't been fragmented.

b. The **Flags field is 0x0**, and the **Fragment Offset is 0**, which means fragmentation did not occur.

5. *Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?*

Answer:

- Identification,
- Destination Port (in UDP),
- TTL

6. *Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?*

Answer:

a. **Stay constant:**
   - Version : IPv4
   - Header length : The IP header remains fixed at 20 bytes for ICMP packets
   - Source IP Address: All packets originate from the same host
   - Destination IP : All packets target the same destination
   - Differentiated Service : all packet use ICMP)
   - Upper Layer Protocol : Always ICMP in this trace

b. **Change**:
   - Identification: Each IP datagram gets a unique ID to allow proper reassembly in case of fragmentation
   - TTL : Traceroute increases TTL with each new packet to discover the next hop in the route
   - Header Checksum: since header changes, so must checksum

7. *Describe the pattern you see in the values in the Identification field of the IP datagram*

   Answer: IP header Identification fields increment with wach ICMP Echo request

8. *What is the value in the Identification field and the TTL field?*

```
Identification: 0x334a (13130)
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 13
```

   Answer:

   Identification: 0x334a (13130)

   TTL: 13

9. *Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?*

```
Identification: 0x0951 (2385)
010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 242
```

```
Identification: 0x0952 (2386)
010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 242
```

```
Identification: 0x0953 (2387)
010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 242
```

   Answer:

   a. The Identification field is different in each ICMP TTL-exceeded reply because it is assigned uniquely to every IP datagram. If two datagrams share the same identification

value, it indicates that they are fragments of a single large IP datagram.

B. The TTL field remains the same in all these replies because the TTL value set for the first-hop router does not change.

3. Fragmentation

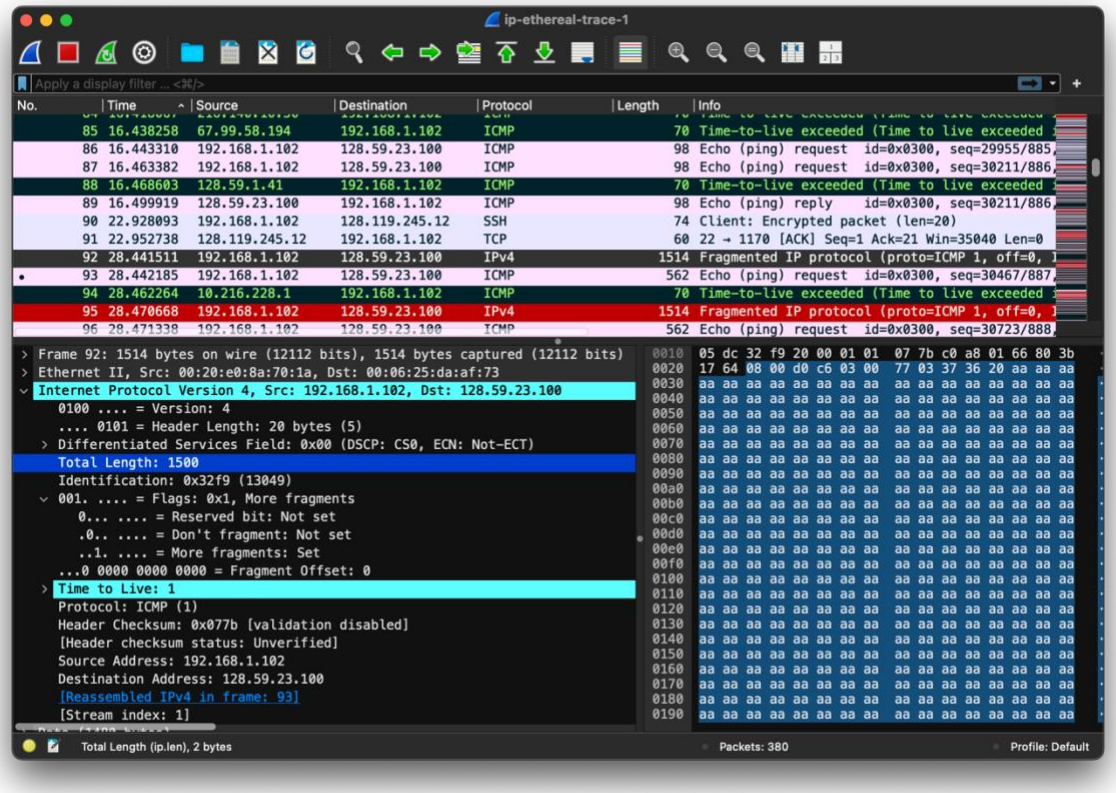
10. *Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000.*
Has that message been fragmented across more than one IP datagram?
[Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ip- ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]

```
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
```

Answer: Yes, the ICMP Echo Request message has been fragmented into two IP datagrams.

11. *Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first*

fragment versus a latter fragment? How long is this IP datagram?



Answer:

The first fragment of the fragmented IP datagram is found in Frame 92.

a. What indicates that the datagram has been fragmented?

The IP header in Frame 92 contains the following fragmentation-related fields:

Flags: More Fragments = 1, which means more fragments follow.

Total Length = 1500, which exceeds the typical Ethernet MTU, confirming fragmentation.

b. How to identify this is the first fragment?

The Fragment Offset = 0, meaning this fragment starts at the beginning of the original datagram.

This confirms Frame 92 is the first fragment.

c. How long is the full IP datagram?

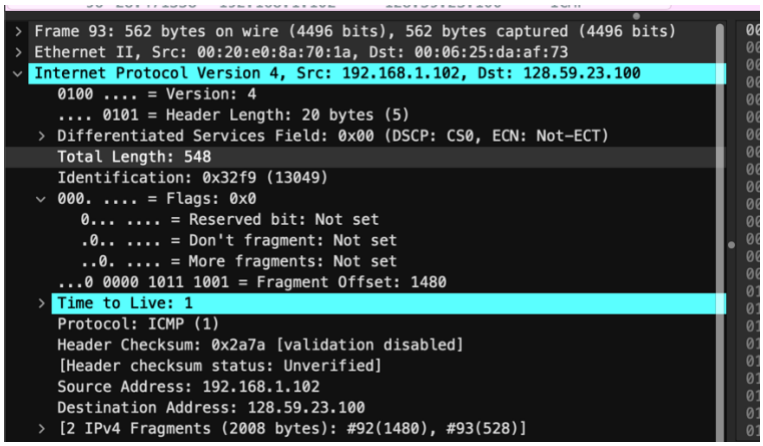
According to Wireshark:

```
Identification: 0x32f9 (13049)
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

"[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]"

The total IP datagram size is 2008 bytes.

12. *Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?*




```
Identification: 0x32f9 (13049)
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
```

Answer:

a. The IP header contains:
   Fragment Offset = 1480
   This means this fragment starts 1480 bytes into the original datagram, so it is not the first
b. No, this is the last fragment

c. The "More Fragments" (MF) flag = 0, which indicates that no further fragments follow

13. What fields change in the IP header between the first and second fragment?

```
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: 00:20:e0:8a:70:1a, Dst: 00:06:25:da:af:73
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
    001. .... = Flags: 0x1, More fragments
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
```

```
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: 00:20:e0:8a:70:1a, Dst: 00:06:25:da:af:73
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
    000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
```

Answer:

1) Fragment Offset

First fragment: Fragment Offset = 0

Second fragment: Fragment Offset = 1480

→ Indicates the byte position where the fragment's data starts within the original datagram.

2) More Fragments (MF) flag

First fragment: MF = 1 (more fragments follow)

Second fragment: MF = 0 (this is the last fragment)

3) Total Length

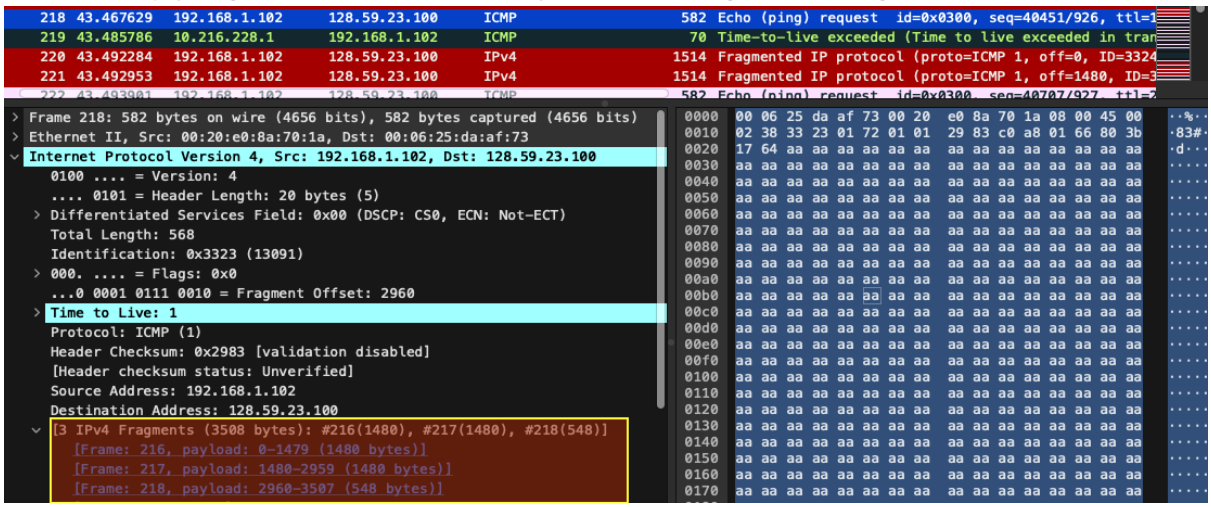
First fragment: Total Length = 1500 (includes max payload size)

Second fragment: Total Length = 548 (only 528 bytes of data + 20-byte header)

4) Header Checksum

Changes due to changes in header fields.

14. How many fragments were created from the original datagram?



Answer: The ICMP Echo Request datagram of 3500 bytes was fragmented into 3 IP fragments.

15. What fields change in the IP header among the fragments?

Answer: The following fields change across the three IP fragments:

Field	Frame 216	Frame 217	Frame 218	Description
Fragment Offset	0	1480	2960	Indicates position of this fragment in the original datagram
Flags (MF bit)	More Fragments = 1	More Fragments = 1	More Fragments = 0	Last fragment has MF=0, others have MF=1
Total Length	1500	1500	568	Different sizes due to how payload is split
Header Checksum	0x0751	0x0698	0x2983	Automatically recalculated because the header content changes