

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА  
Факультет електроніки і комп'ютерних технологій  
Кафедра системного проектування

**Звіт**

про виконання лабораторної роботи № 7  
«Протоколи мережного рівня – IP та ICMP»

**Виконав:**

студент групи ФЕП-13

Карсанашвілі А.Р.

**Викладач:**

Продивус А.М.

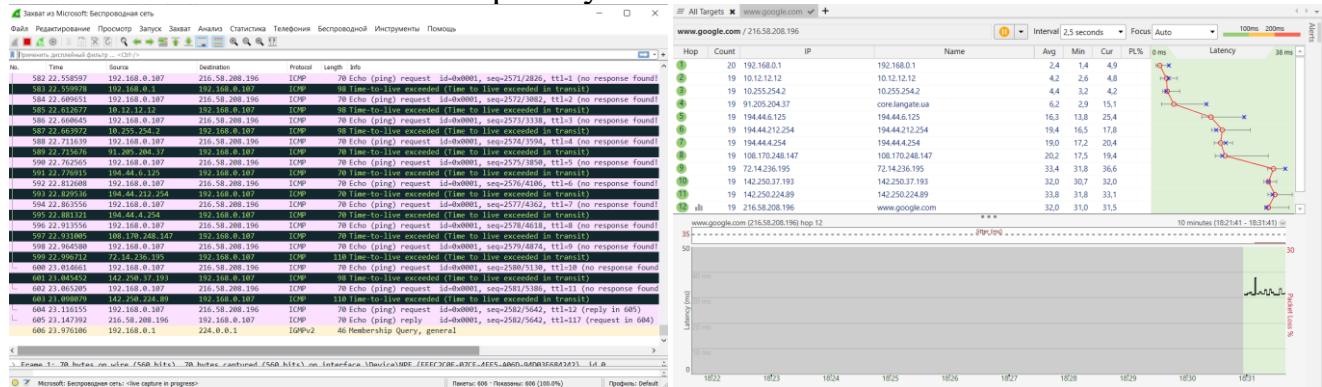
**Львів 2020**

**Мета:** вивчити протокол IP, зокрема, формат IP-дейтаграми. Вивчити деякі аспекти протоколу ICMP, формат та зміст ICMP-повідомлень

## Хід роботи

### Перехоплення пакетів IP програми pingplotter

1. Запускаю *Wireshark* і запускаю перехоплення пакетів
2. Запускаю *pingplotter* та обираю адресу призначення (я обрав [www.google.com](http://www.google.com) – 216.58.214.228), розмір обираю за замовчуванням, тобто 56 байтів та починаю роботу.



### Дослідження перехоплених пакетів IP

Обираю перший ехо – запит та відкриваю деталі заголовку IP

The screenshot shows the details of the first ICMP Echo (ping) request packet in Wireshark. The packet is 70 bytes long and is an ICMP Echo (ping) request with ID 0x0001, sequence number 2374, and TTL 255. The destination IP is 216.58.208.196. The packet is captured on the 'Microsoft: Беспроводная сеть' interface.

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{EEEC2C0F-07CF-4EE5-A06D-94D03E684242}, id 0

Ethernet II, Src: IntelCor\_0c:cf:88 (e0:d4:e8:0c:cf:88), Dst: Tp-LinkT\_ac:fc:dc (50:d4:f7:ac:fc:dc)

Internet Protocol Version 4, Src: 192.168.0.107, Dst: 216.58.208.196

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xcfc8c (53132)

Flags: 0x0000

Fragment offset: 0

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.107

Destination: 216.58.208.196

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x2cf7 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 2374 (0x0946)

1. IP-адреса мого комп'ютера – 192.168.0.107
2. Значення поля протоколу вищого рівня – ICMP

3. Розмір заголовку дорівнює 20 байт, розмір пакету дорівнює – 56 байт. Це можна визначити з полів Header Length та Total Length.
4. Ні, дана дейтаграма не фрагментована, тому що фрагментація IP-дейтаграми необхідна, коли її розмір перевищує розмір максимально припустимого пакета даних, тобто 1500 байт.
5. Ідентифікатор пакету і контрольна сума – ці поля IP-дейтаграми завжди змінюються.
6. Всі решта поля не змінюються та, у випадку з більшими пакетами, прапорців залишаються незмінними.
7. Поле Time-to-live має значення 64

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.107	216.58.208.196	ICMP	70	Echo (ping) request id=0x0001, seq=2374/17929, ttl=255 (reply in 2)
2	0.030791	216.58.208.196	192.168.0.107	ICMP	70	Echo (ping) reply id=0x0001, seq=2374/17929, ttl=117 (request in 1)
3	0.050774	192.168.0.107	216.58.208.196	ICMP	70	Echo (ping) request id=0x0001, seq=2375/18185, ttl=1 (no response found!)
4	0.052025	192.168.0.107	192.168.0.107	ICMP	98	time to live exceeded (time to live exceeded in transit)
5	0.100805	192.168.0.107	216.58.208.196	ICMP	70	Echo (ping) request id=0x0001, seq=2376/18441, ttl=2 (no response found!)
6	0.104505	192.168.0.107	192.168.0.107	ICMP	98	time to live exceeded (time to live exceeded in transit)

> Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF\_{EEEC2C0F-07CF-4EE5-A06D-94D03E684242}, id 0

> Ethernet II, Src: Tp-LinkT\_ac:fc:dc (50:d4:f7:ac:fc:dc), Dst: IntelCor\_0c:cf:88 (e0:d4:e8:0c:cf:88)

✓ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.107

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 84

Identification: 0xfc97 (64663)

> Flags: 0x0000

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0xfb94 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.1

Destination: 192.168.0.107

> Internet Control Message Protocol

8. Цей параметр змінювався залежно від відправника пакету, так як відстань від відправника до мого комп'ютера в стрибках може відрізнятись.

## Фрагментація

9. Знаходжу свій перший ICMP Echo Request після того, як розмір пакета було змінено на 2000 байт. Це повідомлення фрагментоване на декілька дейтаграм.

[illegible]

Дане повідомлення було поділено на декілька дейтаграм. В одному повідомленні було передано 1480 байт, а в іншому 500.

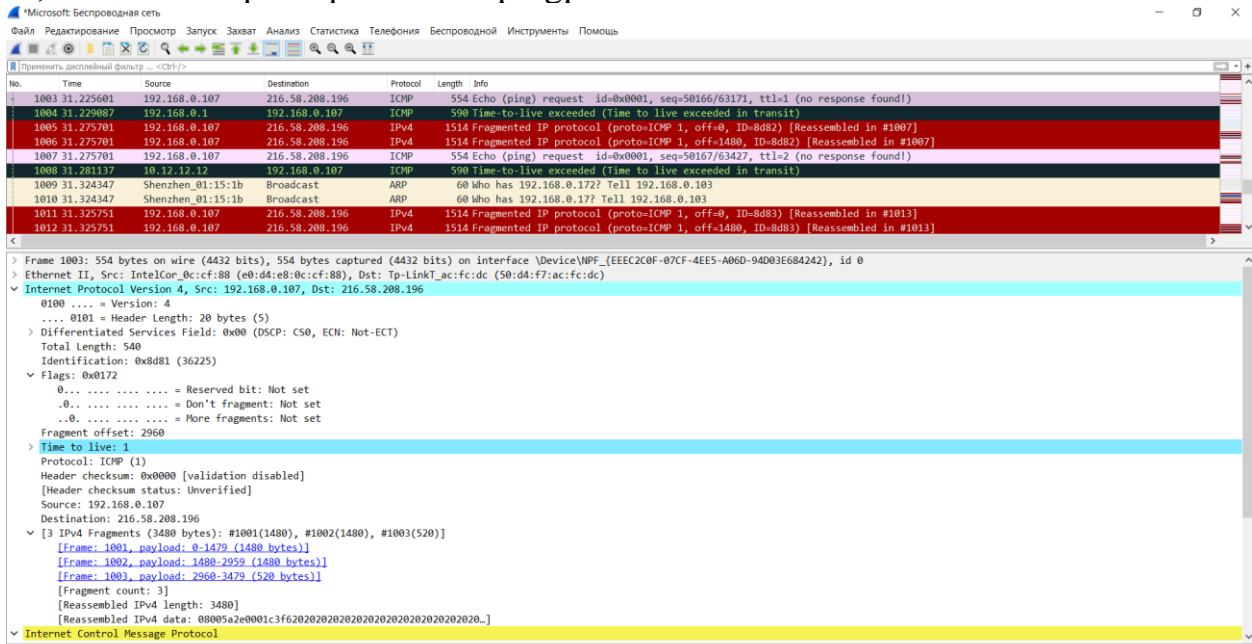
Про фрагментування можна дізнатись з поля Flags.

Якщо зміщення фрагмента рівне 0, це свідчить, що в фрагменті міститься початок великого пакету. Другий пакет має зміщення 185.

$$185 \times 8 = 1480 \text{ байт.}$$

В заголовку змінювались поля – Flags, Fragment Offset, Length, Checksum.

Знайшов перший ICMP Echo Request, який було надіслано на мій комп'ютер після того, як я змінив розмір пакета в pingplotter на 3500.



13. Дейтаграма була фрагментована на 3 пакета. Два пакети містили 1480 байт і останній 520.

14. В заголовку змінювались поля – Flags, Fragment Offset, Length, Checksum.

### Дослідження протоколу ICMP

1. Згенерую ICMP – повідомлення за допомогою утиліти ping.

Ввожу команду: `ping -n 10 216.58.214.228`

Аргумент 10 відповідає за кількість пакетів які мають бути відправлені.

Відповіді на запитання:

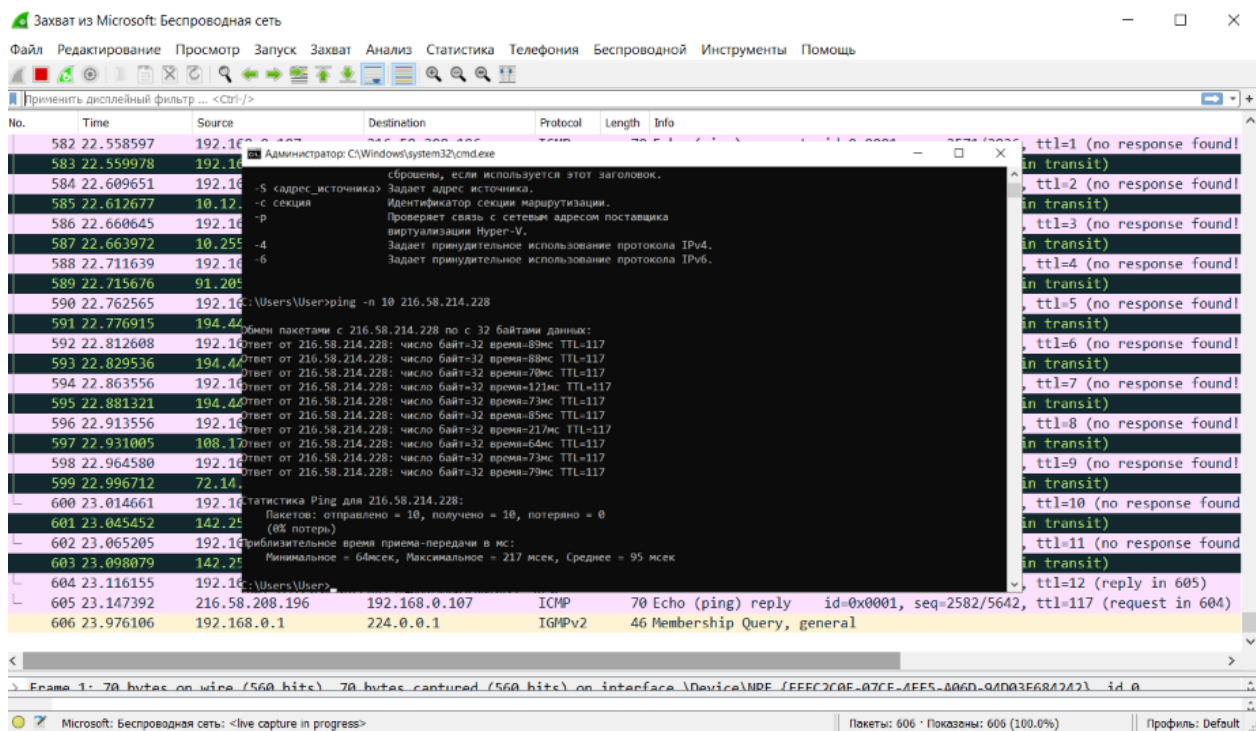
1) IP-адреса хосту призначення – 216.58.214.228

IP-адреса мого комп'ютера – 192.168.0.107

2) ICMP пакети не містять портів відправника та призначення, бо даний протокол є керуючим, а не транспортним.

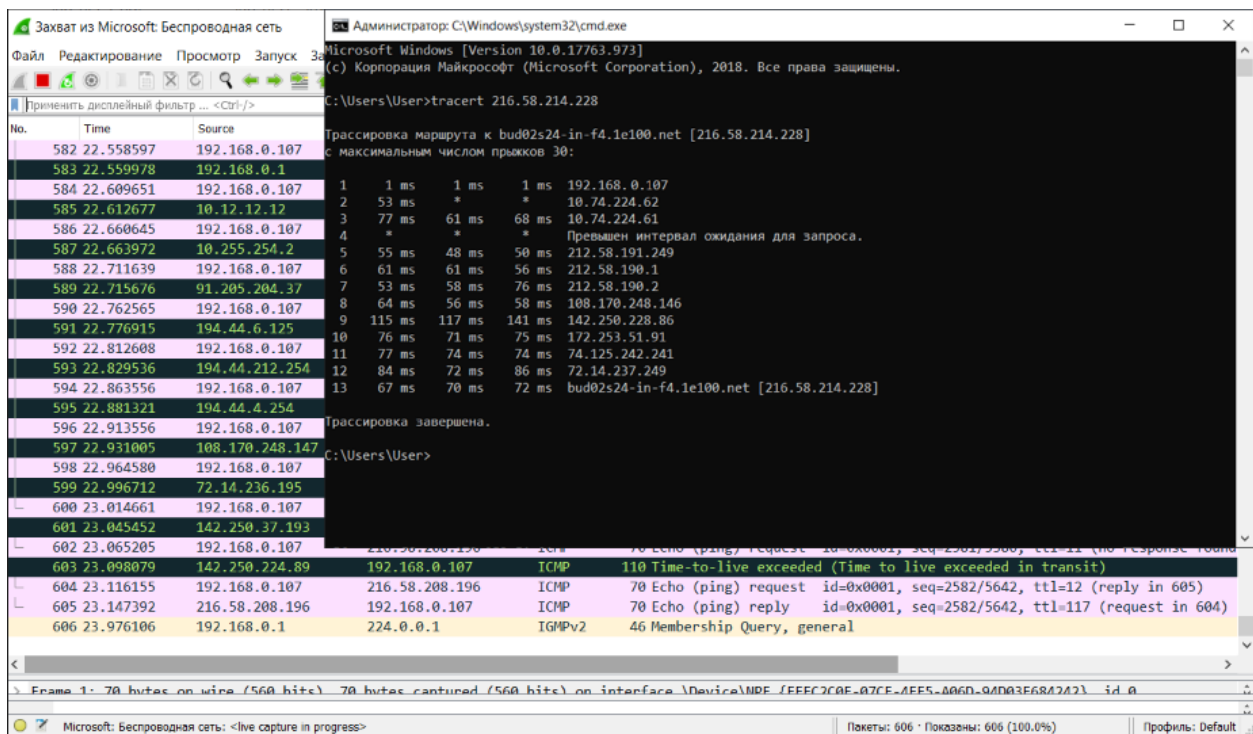
3) Відправлений мною ICMP пакет мав тип 8 (ехо запит) та код 0.

4) Отриманий у відповідь ICMP пакет мав тип 0 (ехо відповідь) та код 0.



Порти відправника та призначення містять протоколи, що належать до транспортного рівня. А ICMP належить до керуючого рівня. Ехо запит мав запит 8 та код 0. Ехо відповідь мала запит та код – 0.

## 2. ICMP-повідомлення, які генерується програмою traceroute; Вводжу команду tracert 216.58.214.228



Відповіді на запитання:

- 5) IP-адреса хосту призначення – 216.58.214.228
- IP-адреса мого комп'ютера – 192.168.0.107

- 6) Надіслані UDP пакети матимуть номер протоколу рівний номеру UDP протоколу, тобто 17.
- 7) Пакети надіслані за утилітою tracert мають тип 11 та код 0. Тип 11 означає, що пакет перевищив TTL.
- 8) Відмінність полягає в типі ICMP пакетів.
- 9) З наведених даних tracert можна дізнатися, який з каналів маршруту мав затримку з відповіддю значно довшу, ніж інші, так як він виводить затримку в мс.

**Висновок:** виконуючи дану лабораторну роботу я вивчив протокол IP, зокрема, формат IP - дейтаграми. А також, ознайомилась з деякими аспектами протоколу ICMP, формат та зміст ICMP – повідомлень.