

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО
АНАЛІЗУ

Лабораторна робота №5

З дисципліни «Комп'ютерні мережі»

Виконала: студентка 3-го курсу

гр. КА-77

Гоголя О.О.

Прийняв: *Кухарєв С.О*

Київ 2020р.

Командная строка

```
C:\Users\alexa>ping -l 2000 gaia.cs.umass.edu

Обмен пакетами с gaia.cs.umass.edu [128.119.245.12] с 2000 байтами данных:
Ответ от 128.119.245.12: число байт=2000 время=203мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=123мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=121мс TTL=42
Ответ от 128.119.245.12: число байт=2000 время=124мс TTL=42

Статистика Ping для 128.119.245.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 121мсек, Максимальное = 203 мсек, Среднее = 142 мсек

C:\Users\alexa>
```

*Wi-Fi

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
103	13.515453	128.119.245.12	192.168.1.6	IPv4	1514	Fragmented IP protocol
104	13.515455	128.119.245.12	192.168.1.6	ICMP	562	Echo (ping) reply
105	13.915834	149.154.167.51	192.168.1.6	SSL	159	Continuation Data
106	14.129067	192.168.1.6	149.154.167.51	TCP	54	54825 → 443 [ACK] Seq
107	14.381575	192.168.1.6	128.119.245.12	IPv4	1514	Fragmented IP protocol
108	14.381576	192.168.1.6	128.119.245.12	ICMP	562	Echo (ping) request
109	14.527528	128.119.245.12	192.168.1.6	IPv4	1514	Fragmented IP protocol
110	14.527529	128.119.245.12	192.168.1.6	ICMP	562	Echo (ping) reply
111	15.388995	192.168.1.6	128.119.245.12	IPv4	1514	Fragmented IP protocol
112	15.388996	192.168.1.6	128.119.245.12	ICMP	562	Echo (ping) request
113	15.533447	128.119.245.12	192.168.1.6	IPv4	1514	Fragmented IP protocol
114	15.533449	128.119.245.12	192.168.1.6	ICMP	562	Echo (ping) reply

> Frame 1: 956 bytes on wire (7648 bits), 956 bytes captured (7648 bits) on interface \Device\NPF_{28914A...}

> Ethernet II, Src: LiteonTe_12:30:a6 (3c:a0:67:12:30:a6), Dst: HuaweiTe_70:0d:6c (bc:76:70:70:0d:6c)

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 54.200.63.64

> Transmission Control Protocol, Src Port: 55551, Dst Port: 443, Seq: 1, Ack: 1, Len: 902

> Transport Layer Security

0000 bc 76 70 70 0d 6c 3c a0 67 12 30 a6 08 00 45 00 -vpp-l< g-0...E-

0010 03 ae 8c e1 40 00 80 06 32 b2 c0 a8 01 06 36 c8@... 2....6-

0020 3f 40 d8 ff 01 bb 5e fa 23 56 69 75 93 3f 50 18 ?@...^ #Viu-?P-

0030 01 01 ac c9 00 00 17 03 03 03 81 00 00 00 00 00

0040 00 00 04 44 86 92 20 e8 c1 7e ef cd 0e fb f4 18 ...D... ~.....

0050 8b b8 c1 f3 eb 2b ec e1 fb 15 e2 42 51 22 10 71+... ..BQ"-q

0060 29 57 15 ac 8e 7f 73 06 ca 04 a4 cd 11 51 c1 29)W....s-Q-)

0070 95 e0 cb 44 b8 ea 35 15 86 76 fe 36 83 55 0e 20 ...D..5- ..v-6-U-

0080 39 19 f0 9f 79 1a 7c bb ec 05 47 fd f7 04 9c 1c 9...y-|..-G.....

wireshark_Wi-Fi_20200416214044_a08016.pcapng

Пакеты: 133 · Показаны: 133 (100.0%) | Профиль: Default

Відповіді на контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій.

Моя: 192.168.1.170, цільова: 128.119.245.12

2. Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?

No.	Time	Source	Destination	Protocol	Length	Info
138	26.368540	192.168.1.170	128.119.245.12	ICMP	562	Echo (ping) request id=0x0
140	26.571608	128.119.245.12	192.168.1.170	ICMP	562	Echo (ping) reply id=0x0
142	27.372031	192.168.1.170	128.119.245.12	ICMP	562	Echo (ping) request id=0x0
144	27.495274	128.119.245.12	192.168.1.170	ICMP	562	Echo (ping) reply id=0x0
146	28.375802	192.168.1.170	128.119.245.12	ICMP	562	Echo (ping) request id=0x0
148	28.497677	128.119.245.12	192.168.1.170	ICMP	562	Echo (ping) reply id=0x0
151	29.379349	192.168.1.170	128.119.245.12	ICMP	562	Echo (ping) request id=0x0
153	29.503760	128.119.245.12	192.168.1.170	ICMP	562	Echo (ping) reply id=0x0

3. Скільки байт займає заголовок IP першого пакету із запитом ICMP? Скільки байт займає корисна інформація (payload) пакету? Поясніть як ви встановили кількість байт корисної інформації.

bytes, $548 - 20 = 528$ bytes of payload

```

✓ Ethernet II, Src: AzureWav_00:05:8C:00:05:15, Dst: ASUS-TEK_00:80:04:10:51:01:00:80:04
✓ Internet Protocol Version 4, Src: 192.168.1.170, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x3c09 (15369)
  > Flags: 0x00b9
    Fragment offset: 1480
    Time to live: 128
    Protocol: ICMP (1)

```

4. Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?

Так, пакет фрагментований. Номер фрагменту можна встановити за допомогою Flags

```

✓ Flags: 0x00b9
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment offset: 1480

```

5. Знайдіть наступний фрагмент датаграми IP. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?

```

✓ Flags: 0x00b9
  0... .. = Reserved bit: Not set
  .0.. .. = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment offset: 1480
  Time to live: 128

```

6. Які поля протоколу IP відрізняють перший фрагмент від другого? Flags- у кожного фрагменту він різний.

7. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?

Identification, Header checksum

8. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?

Identification, Header checksum - ці поля повинні змінюватися для того, щоб розрізняти пакети та перевіряти їх на непошкодженість. Інше - за потребою.

9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.

Збільшується на один

10. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?

id=0x0001, ttl=128

11. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL? Чи змінюються ці значення для різних пакетів у послідовності? Чому? Identification змінюється, а TTL - ні, бо за допомогою ідентифікатора визначається той чи інший пакет, а час життя визначається джерелом передачі.

Висновки: В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи IP та було проведено аналіз деталей роботи даних протоколів.