МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №5

з курсу «Комп'ютерні мережі»

Виконав: студент 3-го курсу
групи КА-73
Борисюк Я.А.
Прийняв: Кухарєв С.О.

Київ – 2020

Мета роботи: аналіз деталей роботи протоколу IP.

Хід виконання роботи

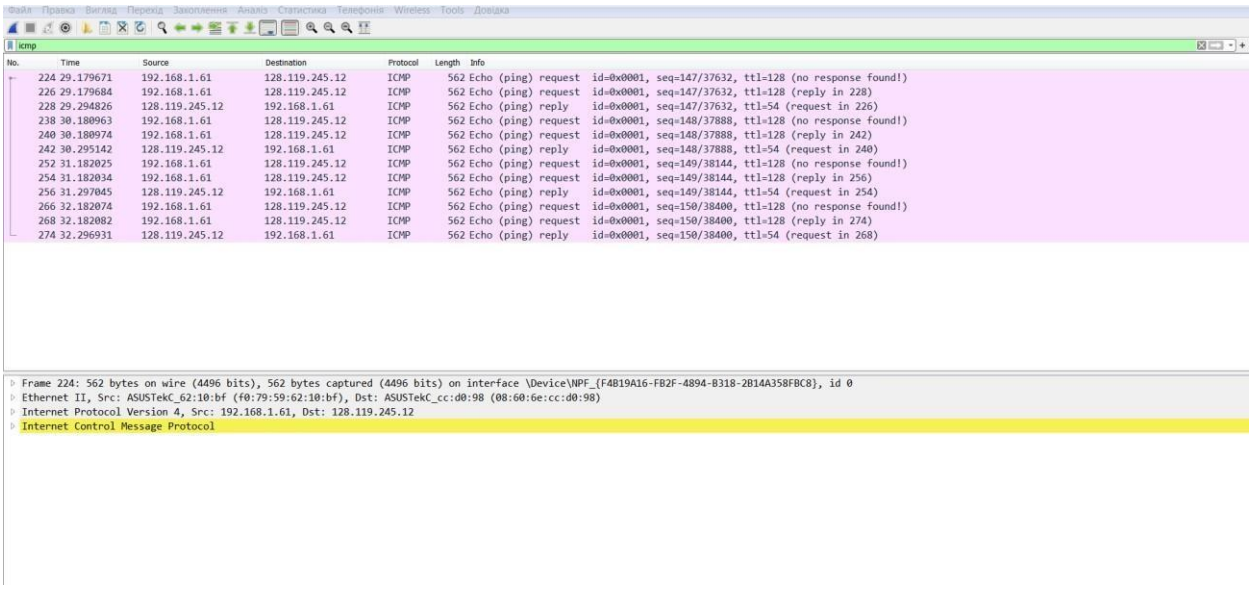
```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\User>ping -l 2000 gaia.cs.umass.edu
При проверке связи не удалось обнаружить узел -1.
Проверьте имя узла и повторите попытку.

C:\Users\User>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=115мс TTL=54
Ответ от 128.119.245.12: число байт=2000 время=114мс TTL=54
Ответ от 128.119.245.12: число байт=2000 время=115мс TTL=54
Ответ от 128.119.245.12: число байт=2000 время=114мс TTL=54

Статистика Ping для 128.119.245.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 114мсек, Максимальное = 115 мсек, Среднее = 114 мсек
```



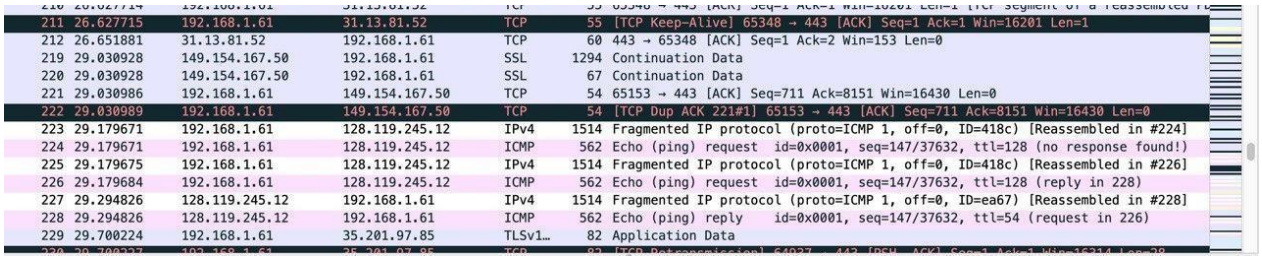
Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій. IP адреси:
    a Моя: 192.168.1.61

b Цільова: 128.119.245.12.

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

a 224.

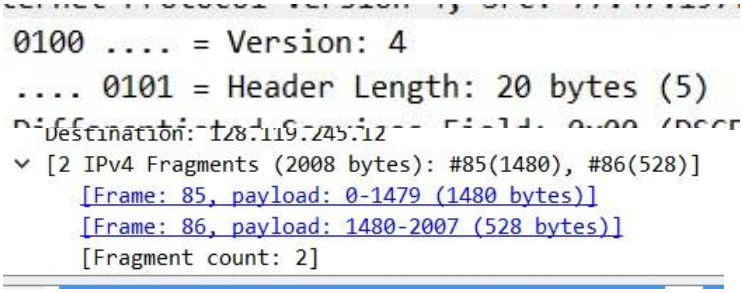


211	26.627715	192.168.1.61	31.13.81.52	TCP	55	[TCP Keep-Alive] 65348 → 443 [ACK] Seq=1 Ack=1 Win=16201 Len=1
212	26.651881	31.13.81.52	192.168.1.61	TCP	60	443 → 65348 [ACK] Seq=1 Ack=2 Win=153 Len=0
219	29.030928	149.154.167.50	192.168.1.61	SSL	1294	Continuation Data
220	29.030928	149.154.167.50	192.168.1.61	SSL	67	Continuation Data
221	29.030986	192.168.1.61	149.154.167.50	TCP	54	65153 → 443 [ACK] Seq=711 Ack=8151 Win=16430 Len=0
222	29.030989	192.168.1.61	149.154.167.50	TCP	54	[TCP Dup ACK 221#1] 65153 → 443 [ACK] Seq=711 Ack=8151 Win=16430 Len=0
223	29.179671	192.168.1.61	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=418c) [Reassembled in #224]
224	29.179671	192.168.1.61	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (no response found!)
225	29.179675	192.168.1.61	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=418c) [Reassembled in #226]
226	29.179684	192.168.1.61	128.119.245.12	ICMP	562	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply in 228)
227	29.294826	128.119.245.12	192.168.1.61	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ea67) [Reassembled in #228]
228	29.294826	128.119.245.12	192.168.1.61	ICMP	562	Echo (ping) reply id=0x0001, seq=147/37632, ttl=54 (request in 226)
229	29.700224	192.168.1.61	35.201.97.85	TLSv1…	82	Application Data

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.

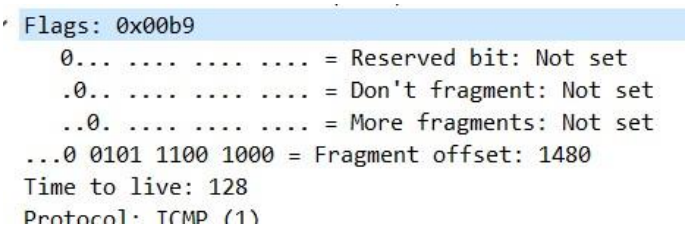
a 2008 bytes – payload.

b



```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Destination: 128.119.245.12
[2 IPv4 Fragments (2008 bytes): #85(1480), #86(528)]
    [Frame: 85, payload: 0-1479 (1480 bytes)]
    [Frame: 86, payload: 1480-2007 (528 bytes)]
    [Fragment count: 2]
```

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? Пакет фрагментований.

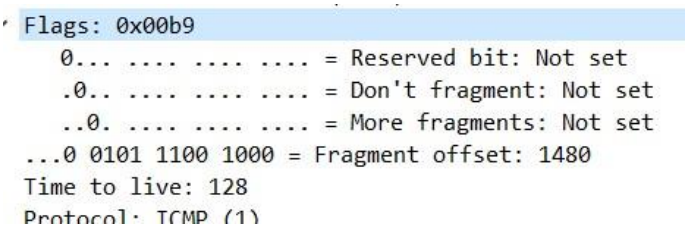


```
Flags: 0x00b9
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
...0 0101 1100 1000 = Fragment offset: 1480
Time to live: 128
Protocol: ICMP (1)
```

a

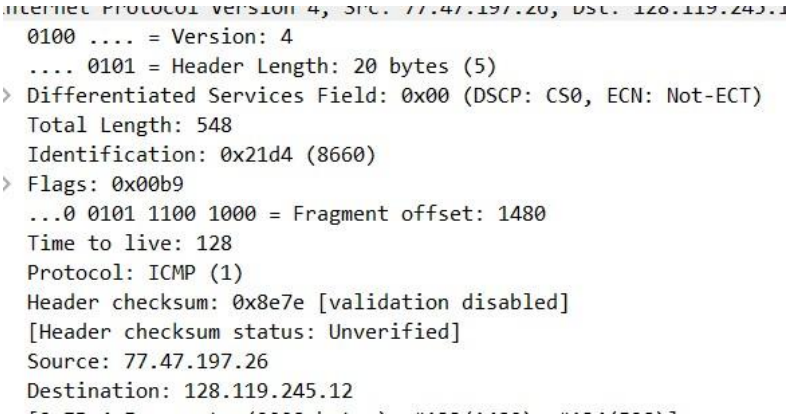
b За допомогою Flags, який передається.

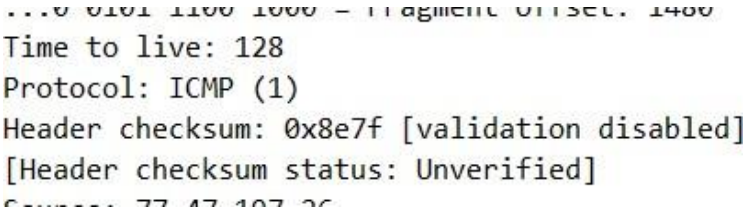
5. Знайдіть наступний фрагмент датаграми IP. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?



```
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
Protocol: ICMP (1)
```

a

6. Як поля протоколу IP відрізняють перший фрагмент від другого?
    a Фрагменти відрізняються Flags- у кожного фрагменту він різний.
7. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?
    a Завжди змінюється поле Identification.
8. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?
    a 

    b Окрім поля Identification, воно повинно змінюватися, бо кожного разу ми ідентифікуємо інший запит.
9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.
    a Кожного разу додається одиниця до коду.
10. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?
    a 

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?
    a Так змінються, тому що validation disabled різний для всіх протоколів.

Висновок

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.