

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 4
З дисципліни: Комп'ютерні мережі

Протокол ІСМР

Виконав:
Студент III курсу
Групи КА-74
Микитенко О.В.
Перевірив: Кухарєв С. О.

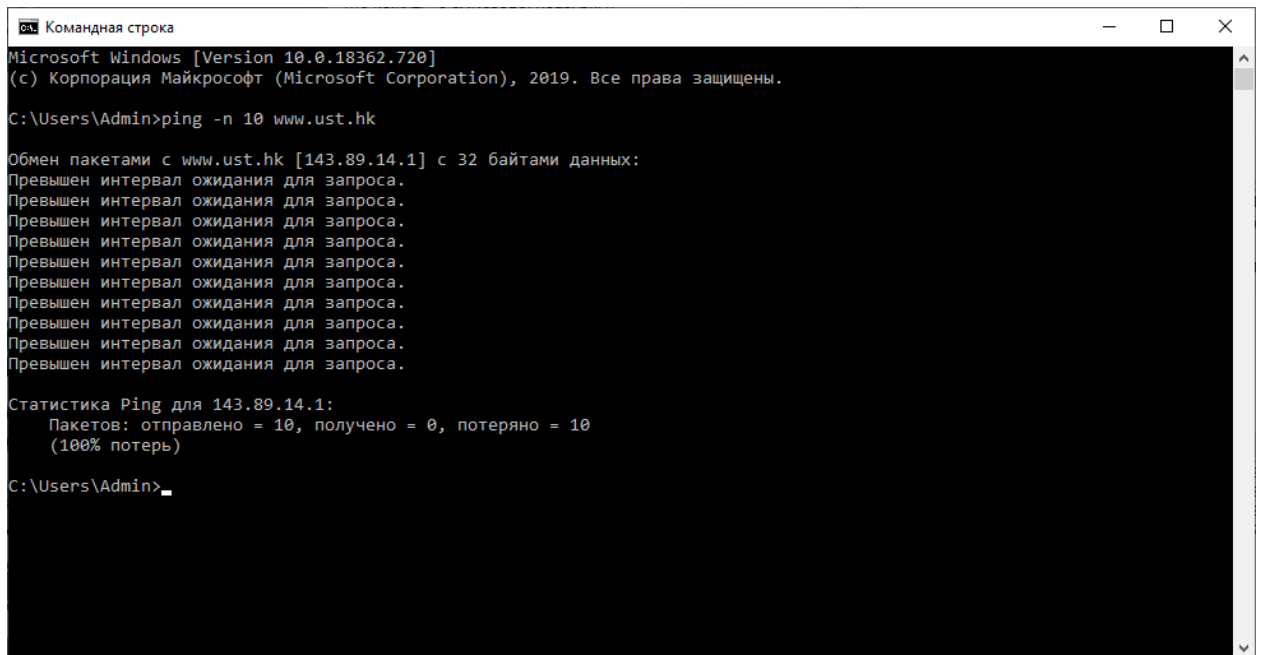
Київ 2020

Мета роботи: аналіз деталей роботи протоколу ICMP.

Хід роботи

Необхідно виконати наступні дії:

- ✓ Відкрийте командний термінал
- ✓ Запустіть Wireshark, почніть захоплення пакетів.
- ✓ Виконайте команду
 - windows: ping -n 10 www.ust.hk
 - linux: ping -c 10 www.ust.hk



```
Командная строка
Microsoft Windows [Version 10.0.18362.720]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

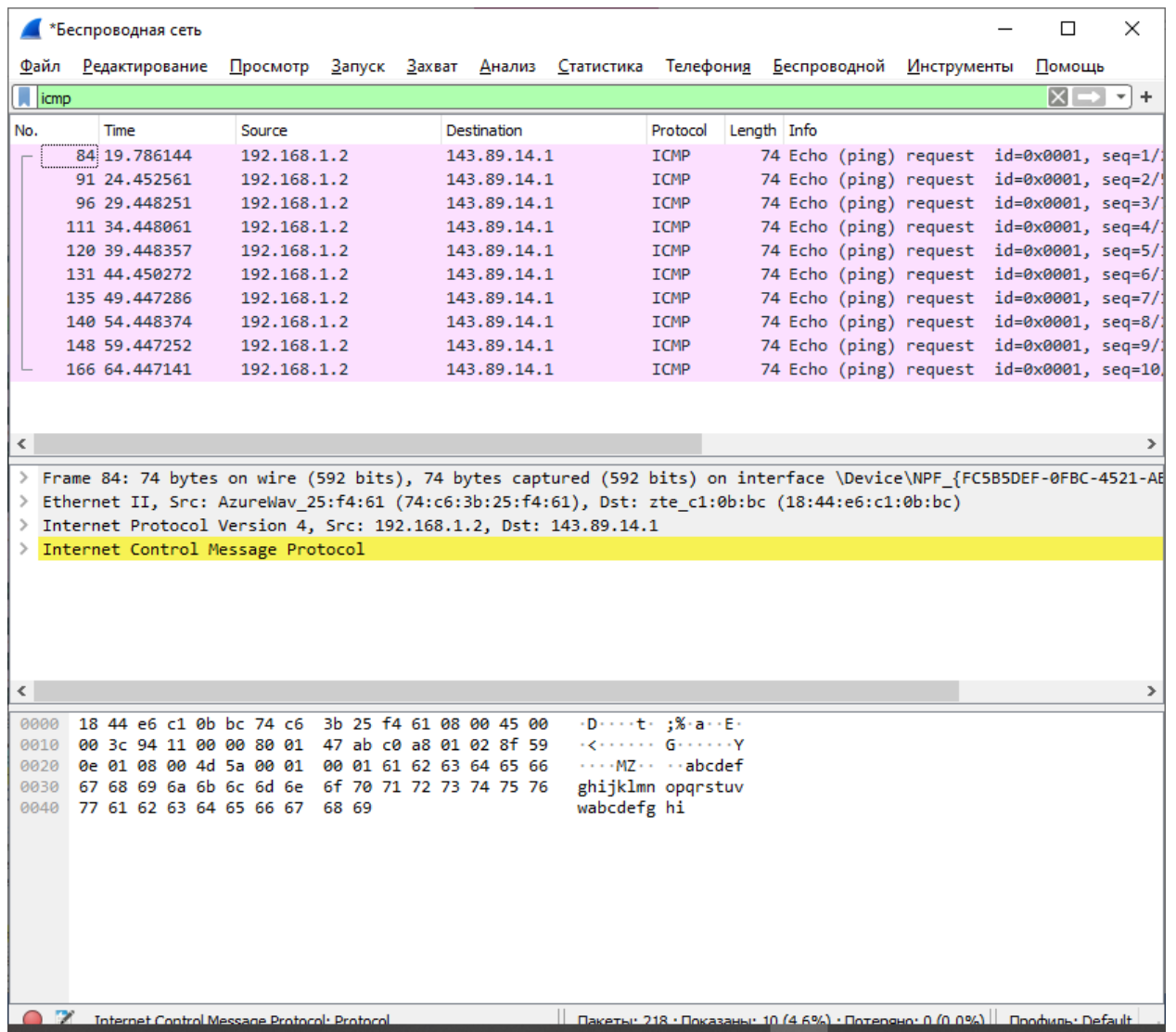
C:\Users\Admin>ping -n 10 www.ust.hk

Обмен пакетами с www.ust.hk [143.89.14.1] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

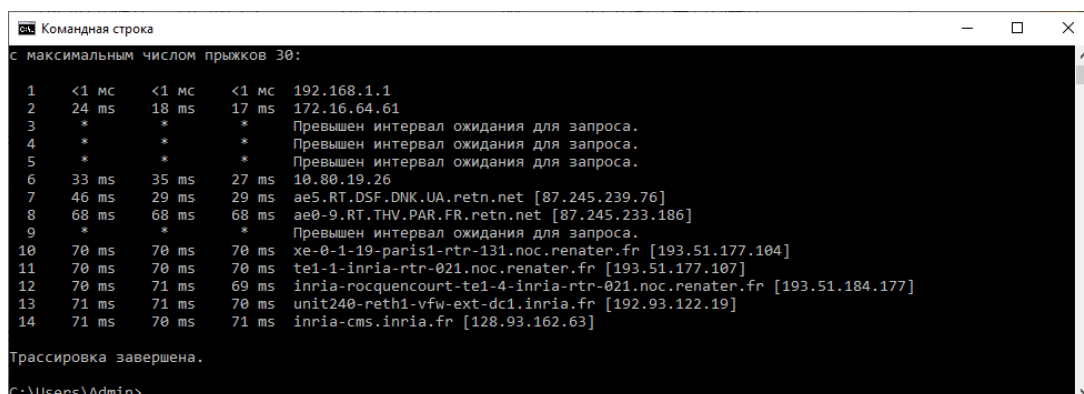
Статистика Ping для 143.89.14.1:
    Пакетов: отправлено = 10, получено = 0, потеряно = 10
              (100% потерь)

C:\Users\Admin>
```

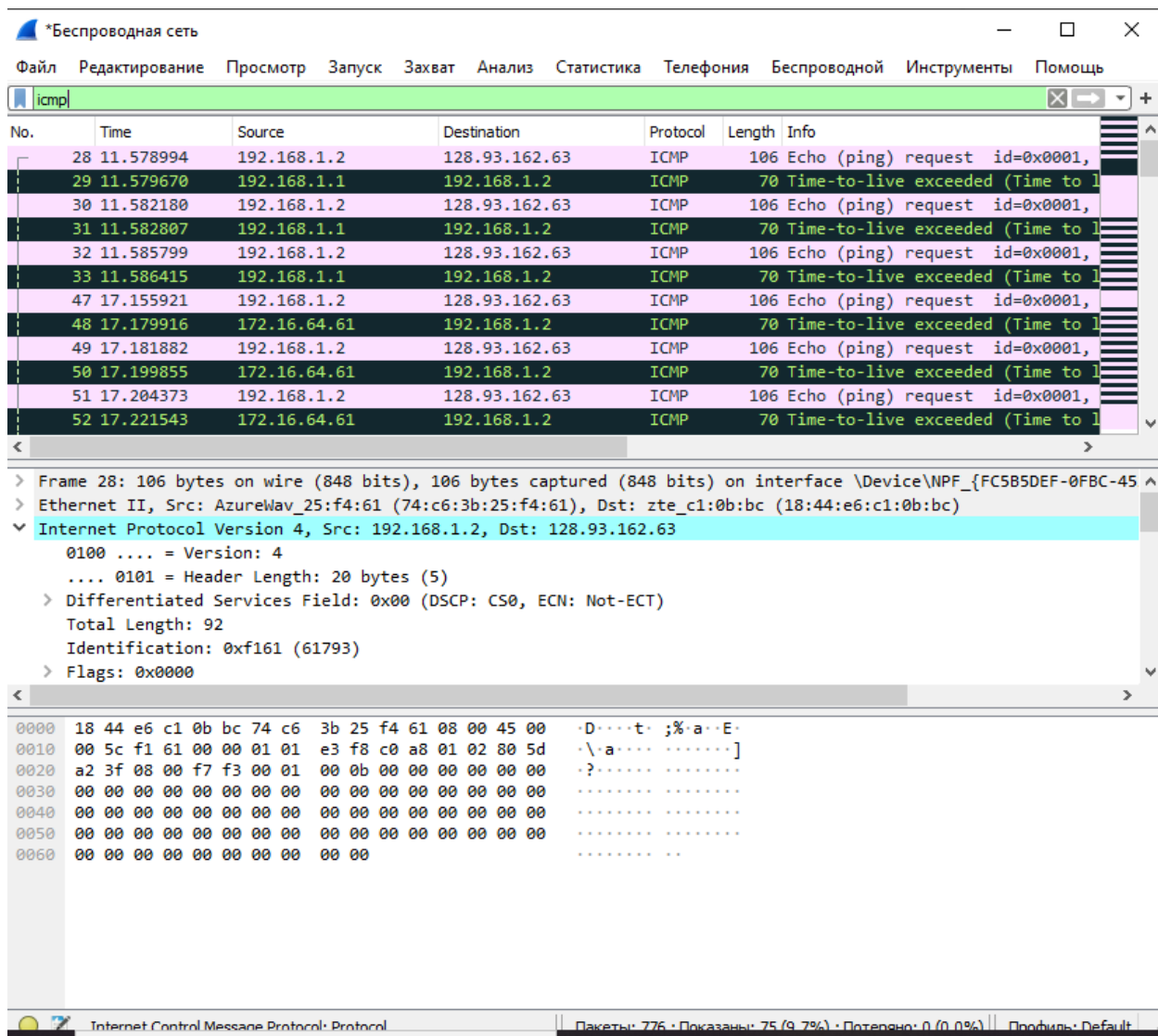
- ✓ Зупиніть захоплення пакетів.
- ✓ Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім IP/ICMP (за допомогою знаків +/-).



- ✓ Приготуйте відповіді на контрольні запитання 1-4, роздрукуйте необхідні для цього пакети.
- ✓ Почніть захоплення пакетів.
- ✓ Виконайте команду
 - windows: `tracert www.inria.fr`
 - linux: `traceroute -I www.inria.fr`



✓ Зупинить захоплення пакетів.



✓ Приготуйте відповіді на контрольні запитання 5-11, роздрукуйте необхідні для цього пакети.

✓ Закрийте Wireshark.

✓ Закрийте командний термінал.

Контрольні питання

1. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.2

Цільова: 143.89.14.1

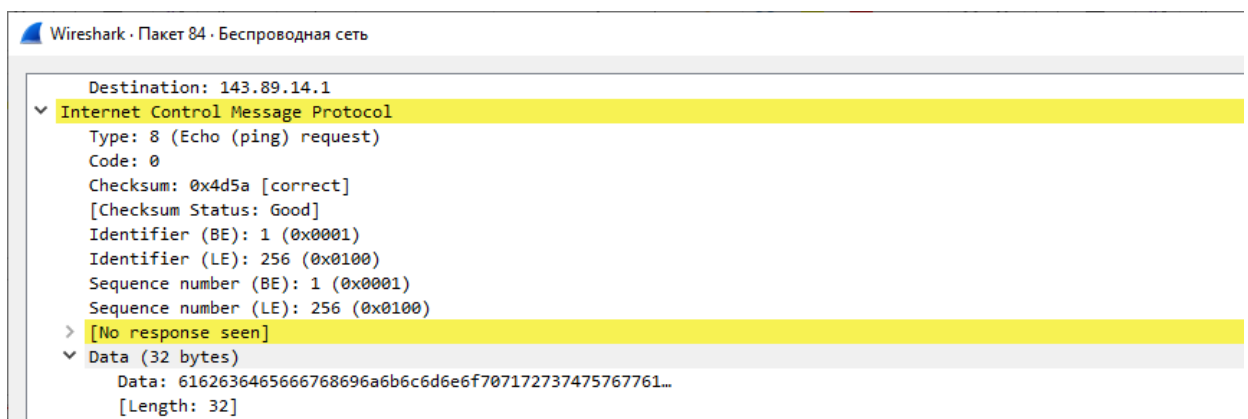
2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?

Тому, що ICMP використовує мережевий рівень, а не транспортний, як порти.

```
Header checksum: 0x47ab [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.2
Destination: 143.89.14.1
> Internet Control Message Protocol
```

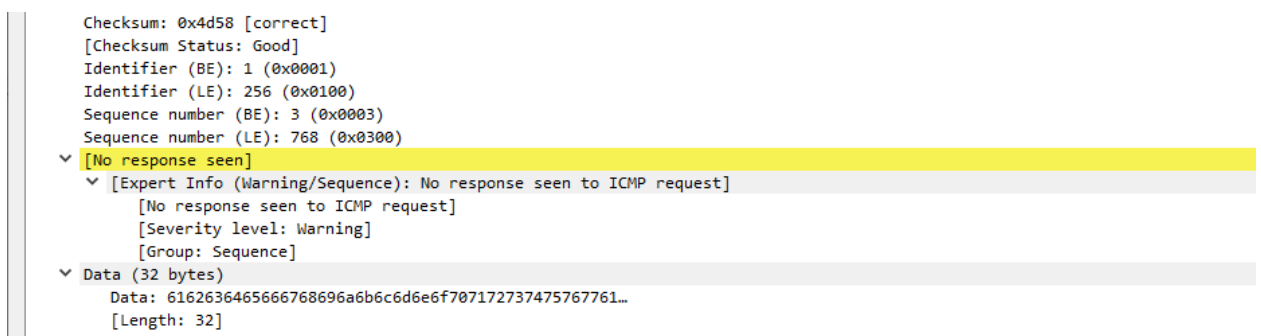
3. Дослідіть один з пакетів-запитів ICMP. Які тип та код зазначені у цьому пакеті?

Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?



4. Дослідіть відповідний пакет з відповіддю на пакет із пункту 3. Які тип та код зазначені у цьому пакеті? Які інші поля має цей пакет? Скільки байтів займають поля контрольної суми, номера послідовності та ідентифікатору?

Відповіді я не отримала.



5. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.1.2

Цільова: 128.93.162.63

6. Який номер протоколу IP використовується програмою?

Version: 4.

7. Чи відрізняється пакет із запитом програми traceroute від пакету із запитом програми ping? Якщо так, наведіть приклади.

Команда ping дає можливість перевірити доступність певного ресурсу мережі: подає на вказаний хост пакет заданого розміру, що згодом повертається назад.

У нашому випадку відповідь не була отримана на жоден із 10 відправлених пакетів.

Команда traceroute також надсилає пакет до вказаного ресурсу, ще й послідовно запитує і вимірює час затримку між маршрутизаторами на шляху пакета.

Таким чином, можна визначити інтервал найбільших затримок. Також, при використанні команди traceroute з адресом, що вказаним символьно, автоматично перевіряється робота DNS сервісу, який вертає IP адресу заданого ресурсу мережі.

No.	Time	Source	Destination	Protocol	Length	Info
28	11.578994	192.168.1.2	128.93.162.63	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=1 (no re
29	11.579670	192.168.1.1	192.168.1.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

8. Проаналізуйте пакет ICMP з повідомленням про помилку. Чи є у ньому деякі додаткові поля, які не зазначаються у повідомленні з підтвердженням. Якщо є – які саме поля і яку інформацію вони вміщують?

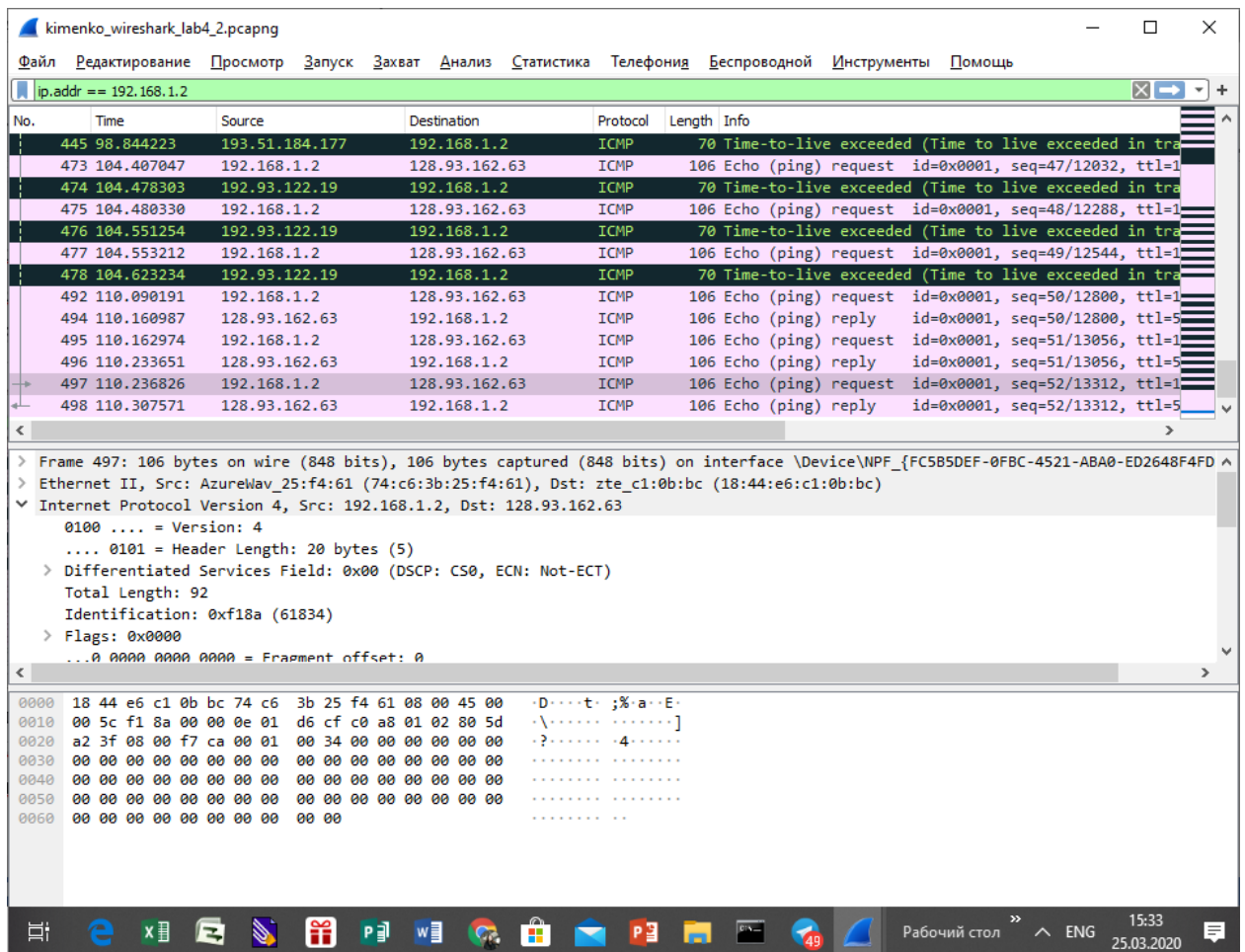
Wireshark · Пакет 28 · kimenko_wireshark_lab4_2.pcapng

Identification: 0xf161 (61793)
> Flags: 0x0000
...0 0000 0000 0000 = Fragment offset: 0
> Time to live: 1
Protocol: ICMP (1)
Header checksum: 0xe3f8 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.2
Destination: 128.93.162.63
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7f3 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 11 (0x000b)
Sequence number (LE): 2816 (0x0b00)
> [No response seen]
> Data (64 bytes)

0000 18 44 e6 c1 0b bc 74 c6 3b 25 f4 61 08 00 45 00 .D...t.;%a..E.
0010 00 5c f1 61 08 00 01 01 e3 f8 c0 a8 01 02 80 5d .\a...[
0020 a2 3f 08 00 f7 f3 00 01 00 0b 00 00 00 00 00 .?...?
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Close Help

9. Проаналізуйте три останні відповіді протоколу ICMP, які отримала ваша робоча станція. Як ці пакети відрізняються від пакетів з повідомленням про помилку? Чому вони відрізняються?



Тому що, у пакетах з помилкою не було отримано відповіді.

10. Знайдіть етап ретрансляції повідомлень з найбільшою середньою затримкою. Чи є можливість оцінити географічну відстань між маршрутизаторами на цьому етапі?

Так, за допомогою довжини даних.

Висновок

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