**Лабораторна робота № 5 з предмету «Комп’ютерні інформаційні мережі»**

Виконав:

студент групи ПМІ-32

Юрас Назар

Львів-2022

**Тема:** Аналіз повідомлень канального рівня Ethernet засобами Wireshark

**Мета:** Здобути практичні навички з інтерпретації Ethernet-кадрів. Ознайомтеся на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).

Хід роботи

Виконайте наступні дії саме у такій послідовності:

1.Від'єднайтеся від мережі.

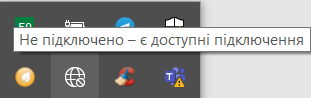
2.Запустіть аналізатор мережевих пакетів Wireshark від імені адміністратора.

3.З’єднайтесь з мережею.

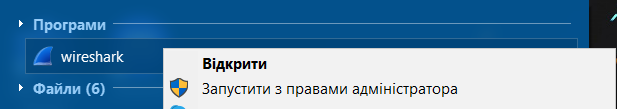
4.Захопіть кадри впродовж приблизно 30 секунд, здійснюючи активність в браузері або передаючи файли локальною мережею.

5.Виберіть будь-який пакет (кадр) для аналізу (оскільки усі без винятку пакети інкапсулюються в кадри):

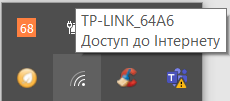
1. **Від’єднався від мережі**



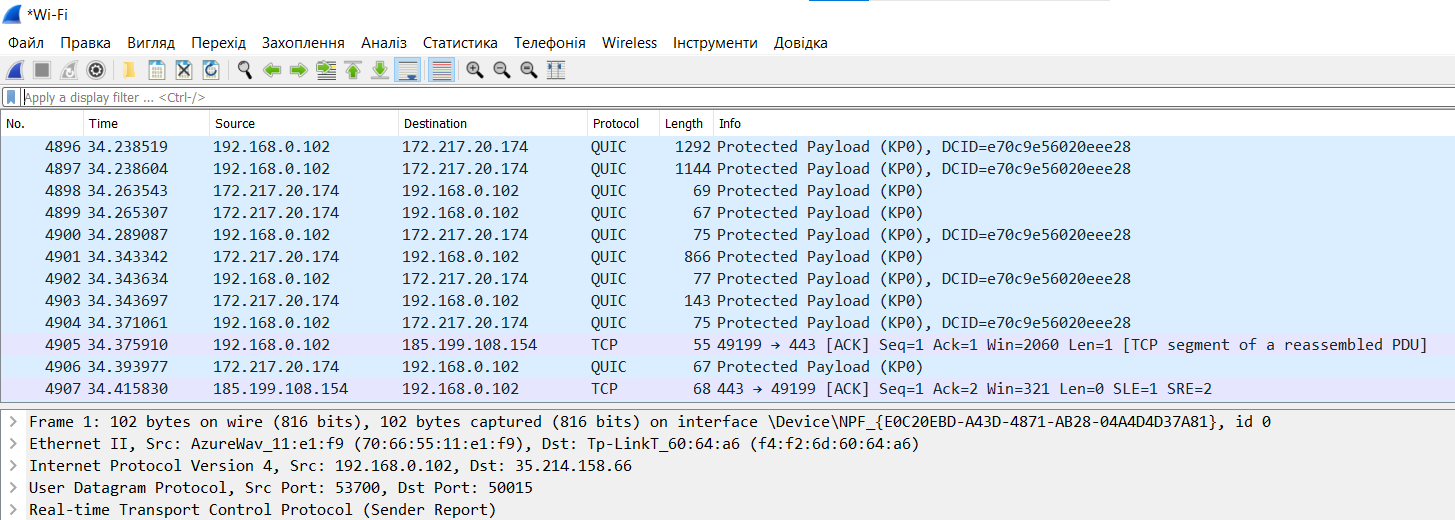
1. **Запустив аналізатор пакетів Wireshark від імені адміністратора.**



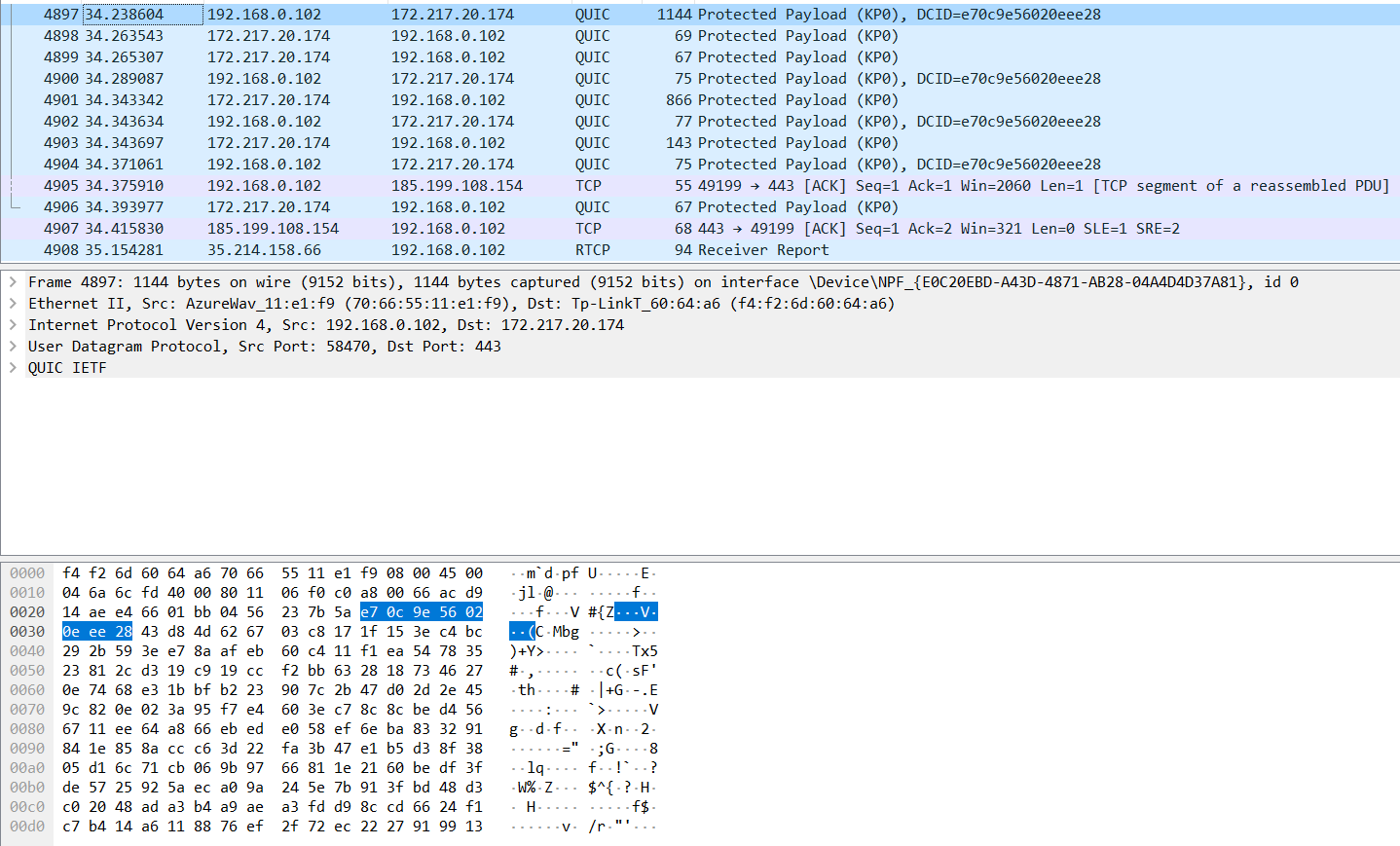
1. **Підключився до своєї мережі Wi-Fi**



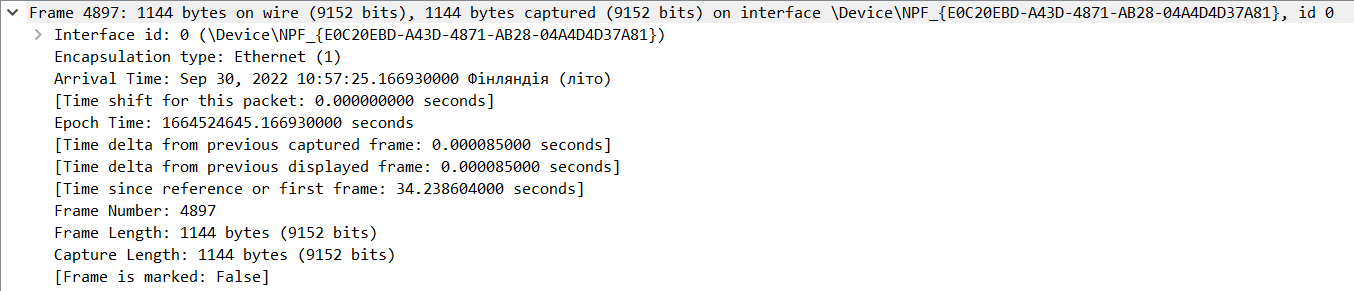
1. **Запустив захоплення пакетів і зробив певну активність в браузері, заходячи на сайти, переключаючись між вкладками, тощо, зупинив захоплення пакетів**



1. **Обрав кадр №4897, розмір – 1144 байт (9152 біт)**



1. **Час захоплення: Sep 30, 2022 10:57:25**



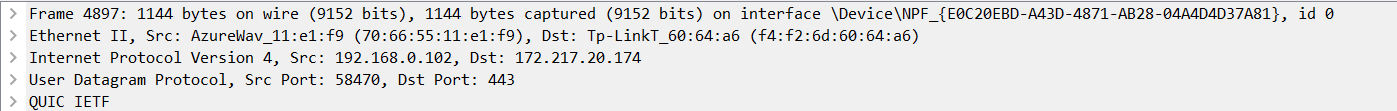
**Ієрархія протоколів:**

**Ethernet-кадр**

**IP-пакет:**

**UDP-сегмент**,

**QUIC-повідомлення** (Quick UDP Internet Connection) – транспортний мережевий протокол, який розвивається компанією Google з 2013 року як альтернатива зв'язці TCP + TLS для веб



1. **Заголовок кадру та його характеристики:**

Розмір: 14 байт

****

**Отримувач**: мережевий адаптер, МАС-адреса: f4:f2:6d:60:64:a6



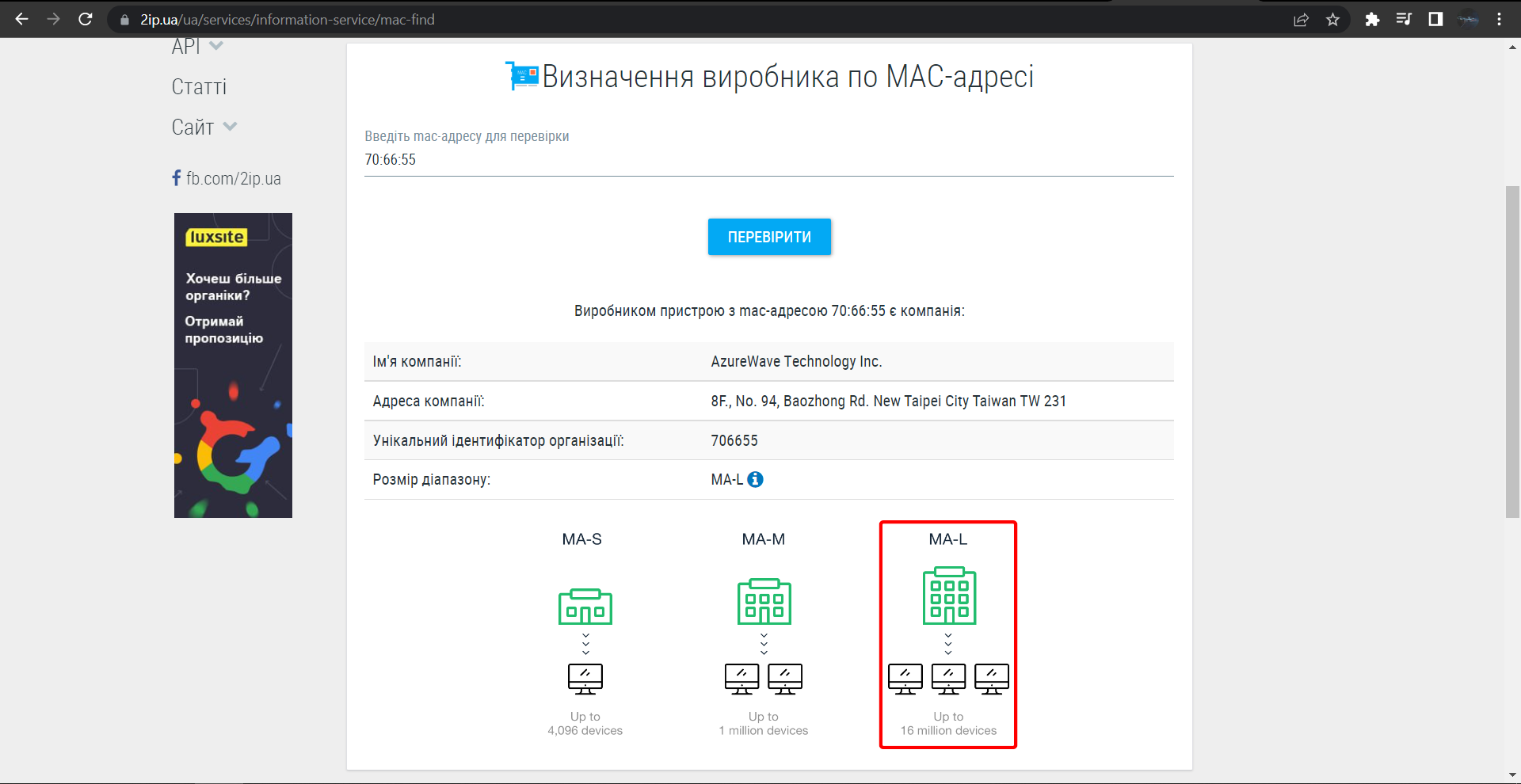
**Відправник**: маршрутизатор, МАС-адреса: 70:66:55:11:e1:f9



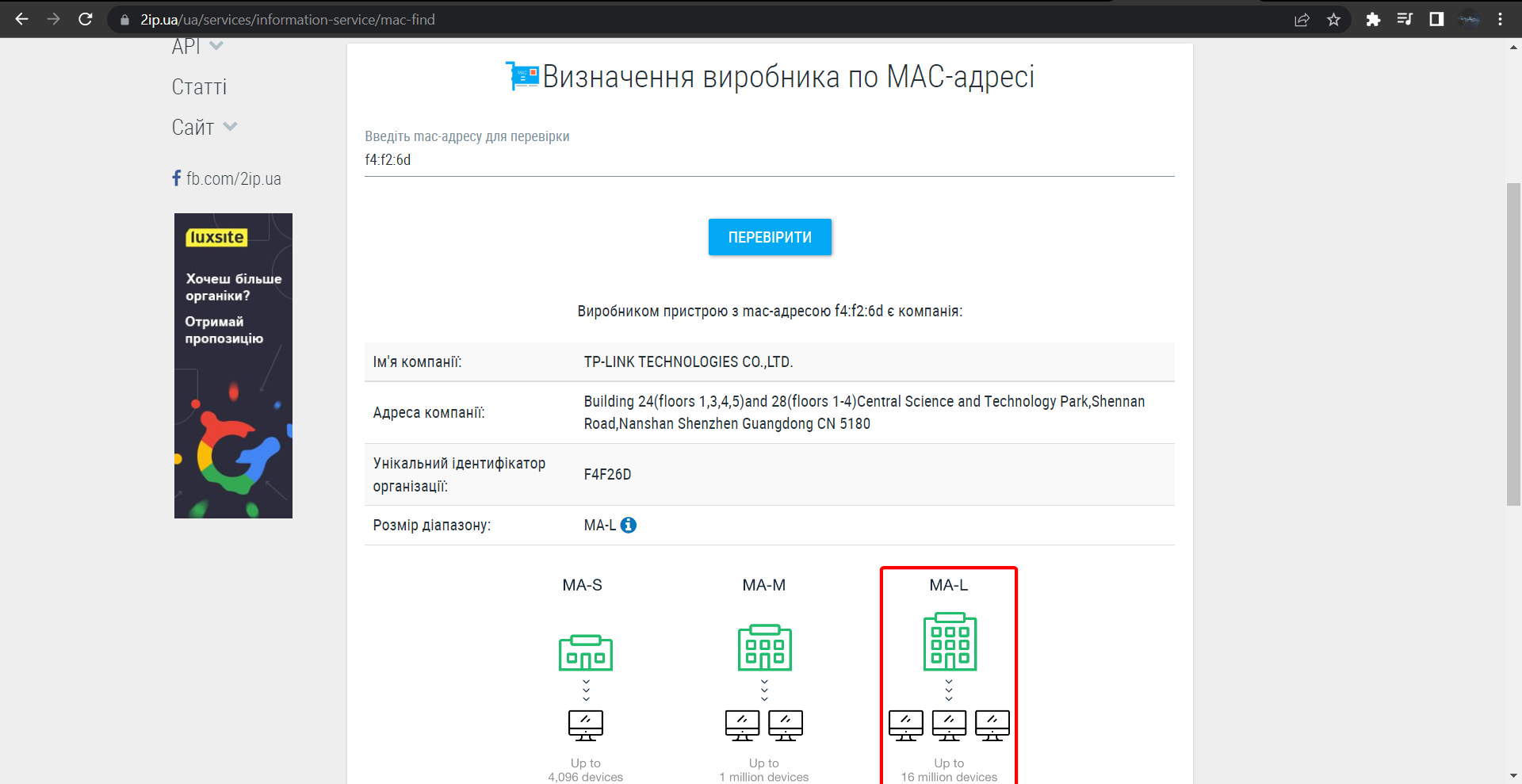
Вкладений протокол, що передається: **IPv4** 

1. **За першими половинами МАС-адрес отримав інформацію про виробників пристроїв відправника та отримувача:**

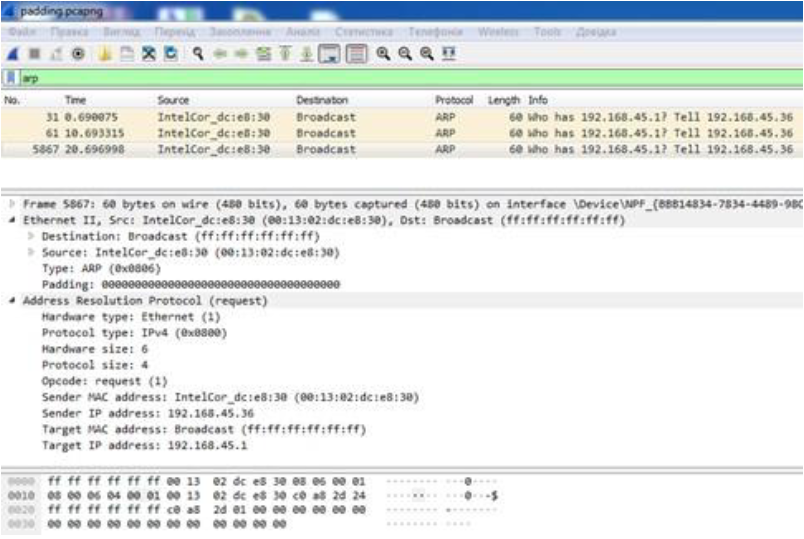
**Інформація про виробника пристрою-відправника:**



**Інформація про виробника пристрою-отримувача**:



1. **Спробував відшукати за допомогою фільтру кадри, які переносять повідомлення протоколу ARP, однак у мене його не виявилось, тому поясню по скріну з методички:**

****

**Що ж таке Padding?** Це додаткові (зазвичай нульові) байти у повідомленні, які використовуються для того, щоб вирівняти певні поля чи розмір всього повідомлення до певної довжини.

**Чому у захопленому кадрі немає кінцевика?** Справа в тому, що кінцевик, що використовується для перевірки правильності даних, на даному етапі видаляється, бо корисної інформації не несе, тому дані з запиту передаються на інший рівень.

**Висновок:** на цій лабораторній роботі я здобув практичні навички з інтерпретації Ethernet-кадрів, а також знайомився на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).