ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі
ЛАБОРАТОРНА РОБОТА №4

Тема: «Аналіз повідомлень канального рівня Ethernet засобами Wireshark. Утиліти для діагностики мережі на канальному рівні».

Виконала:
Ст. *Пелещак Вероніка*
ПМІ-35с

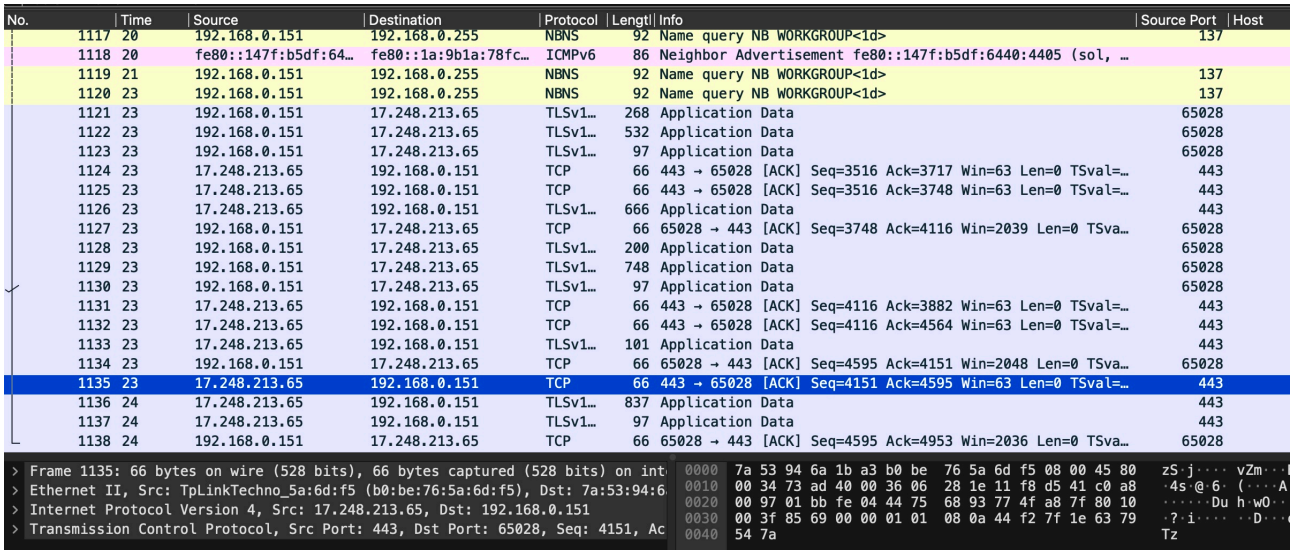
2025

Тема: Аналіз повідомлень канального рівня Ethernet засобами Wireshark. Утиліти для діагностики мережі на канальному рівні.

Мета: Здобути практичні навички з інтерпретації Ethernet-кадрів та використання консольних утиліт для діагностики мережі на рівні мережевих інтерфейсів.

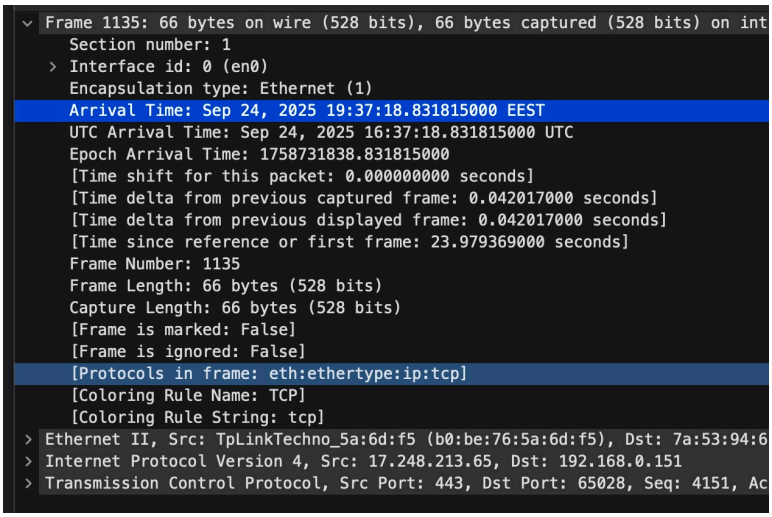
Хід роботи:

1. Спочатку я від'єдналась від мережі, запустила Wireshark від імені адміністратора і з'єдналася з мережою. Захопила кадри, здійснюючи активність у браузері.



Кадр: №1135, Розмір: 66 байтів (528 бітів).

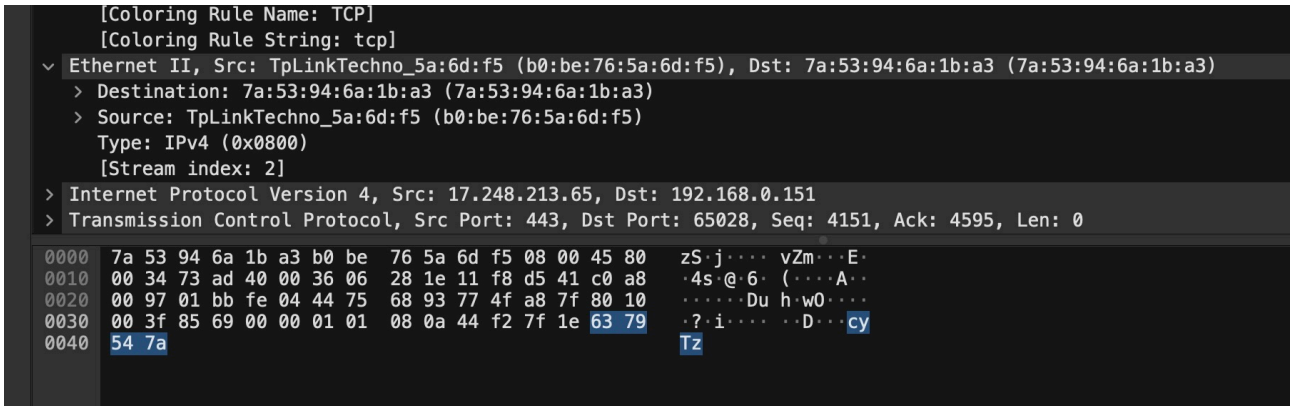
2. Інформація про кадр:



Час захоплення: 24.09.2025 19:37:18.

Ієрархія протоколів: кадр Ethernet → IP-пакет → TCP-сегмент.

3. Основні складові заголовку кадра:



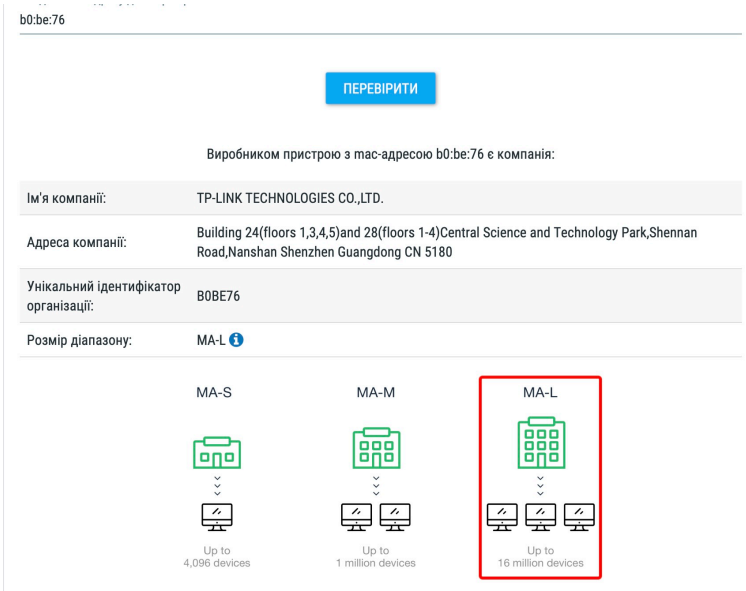
Розмір: 14 байтів

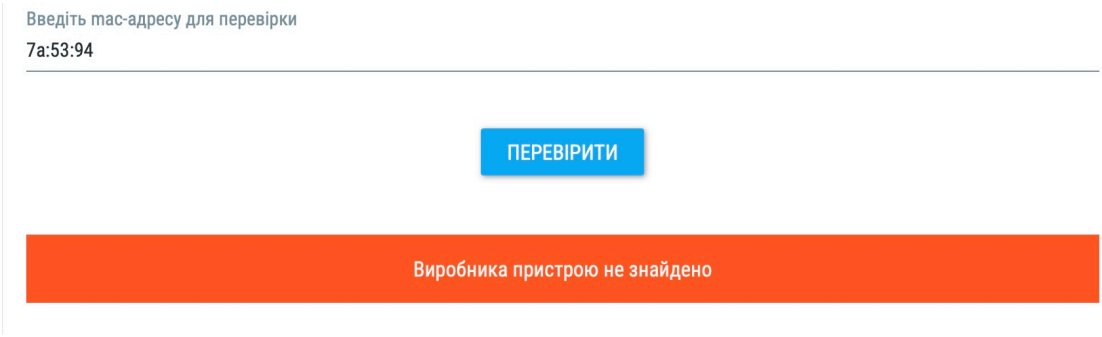
Відправник: мережевий адаптер (MAC b0:be:76:5a:6d:f5)

Отримувач: маршрутизатор (MAC 7a:53:94:6a:1b:a3)

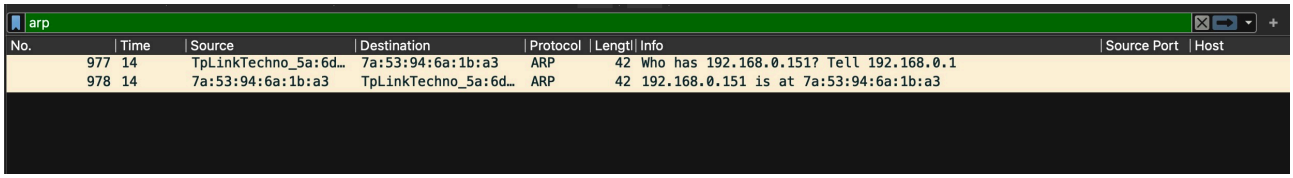
Вкладений протокол: IPv4

4. За допомогою MAC адреси дізналась інформацію про виробника відправника:

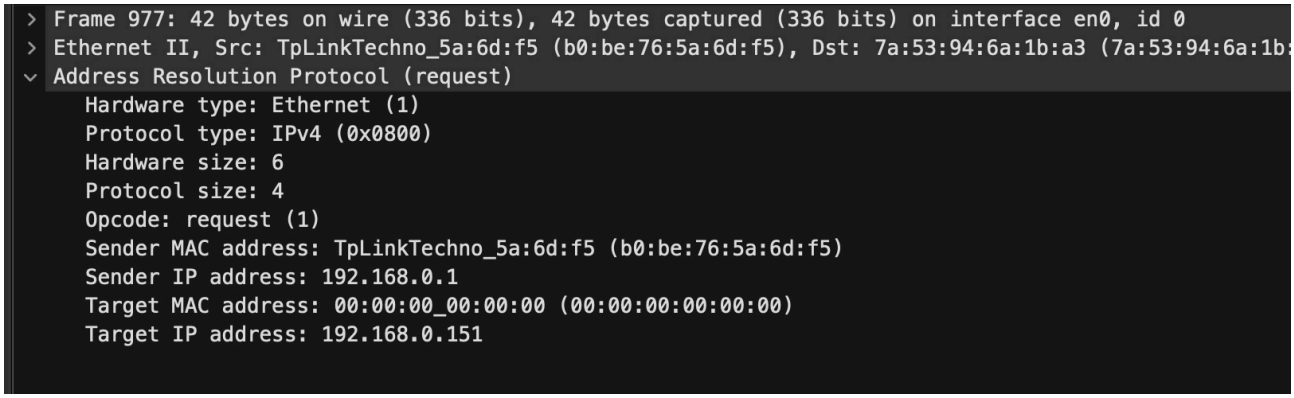




5. Дослідила протокол ARP і скористалась однойменним фільтром arp:



6. ARP-запит:



Hardware type: Ethernet (1) *— використовується Ethernet.*

Protocol type: IPv4 (0x0800) *— визначається IP-протокол версії 4.*

Hardware size: 6 *— довжина MAC-адреси 6 байт.*

Protocol size: 4 *— довжина IP-адреси 4 байти.*

Opcode: request (1) *— це ARP-запит.*

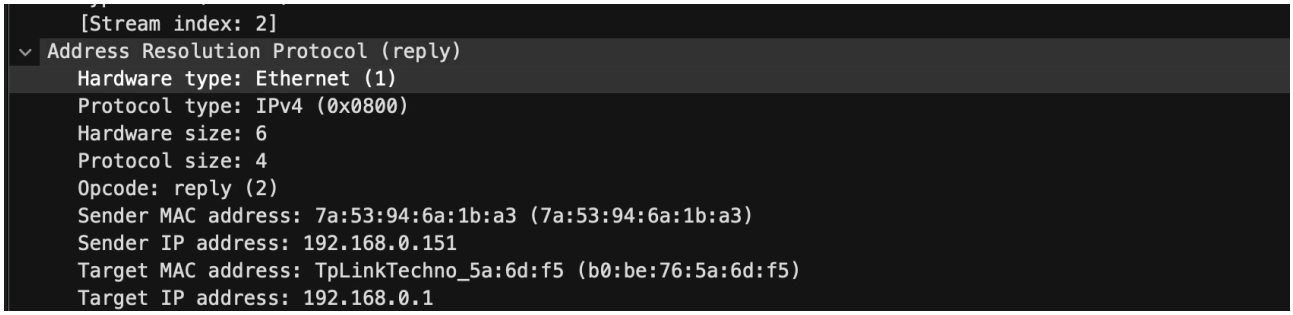
Sender MAC address: b0:be:76:5a:6d:f5 *— MAC-адреса відправника.*

Sender IP address: 192.168.0.1 *— IP-адреса відправника.*

Target MAC address: 00:00:00:00:00:00 *— MAC-адреса цілі невідома.*

Target IP address: 192.168.0.151 — *IP-адреса, чию MAC-адресу шукають.*

7. ARP-відповідь:



Hardware type: Ethernet (1) *— використовується Ethernet.*

Protocol type: IPv4 (0x0800) *— протокол – IPv4.*

Hardware size: 6 *— MAC-адреса має 6 байт.*

Protocol size: 4 *— IP-адреса має 4 байти.*

Opcode: reply (2) *— це ARP-відповідь.*

Sender MAC address: 7a:53:94:6a:1b:a3 *— MAC-адреса відправника.*

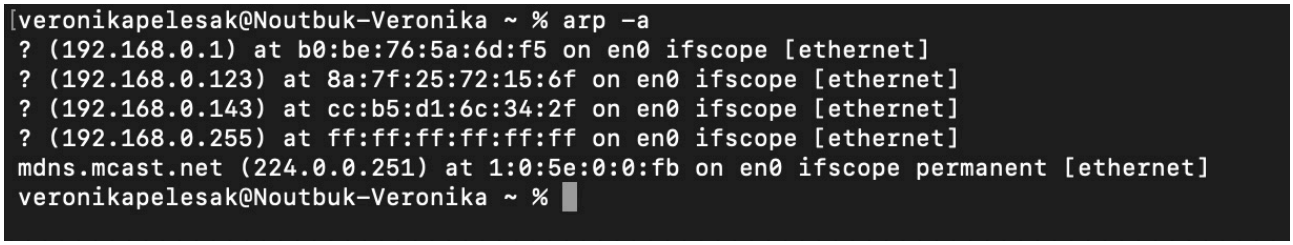
Sender IP address: 192.168.0.151 *— IP-адреса відправника.*

Target MAC address: b0:be:76:5a:6d:f5 *— MAC-адреса запитувача.*

Target IP address: 192.168.0.1 *— IP-адреса запитувача.*

8. **Padding:** У Ethernet-кадрі мінімальна довжина повинна бути 64 байти. Якщо ARP-повідомлення менше, ніж ця довжина, то в кінець кадру додається Padding (заповнення нулями), щоб «добити» розмір. Якщо поле Padding відсутнє, то це означає, що загальна довжина кадру і так досягла мінімально необхідних 64 байт.

9. Виконала команду arp -a у Terminal:



10. Чому у захоплених кадрах немає кінцевика?

У захоплених кадрах Wireshark немає кінцевика, бо цей елемент кадру перевіряється апаратно мережею та не передається операційній системі. Мережеві карти відкидають його ще до того, як дані потрапляють у Wireshark. Тому програма показує тільки основну частину кадру, і це нормальна поведінка, яка не впливає на аналіз мережевого трафіку.

Висновок: Під час роботи проаналізовано Ethernet-кадри та протокол ARP за допомогою Wireshark і консольних утиліт. Визначено розмір кадру, MAC-адреси, вкладений протокол, обмін ARP-запитами та відповідями, пояснено призначення поля Padding і відсутність кінцевика (FCS). Робота закріпила практичні навички аналізу мережевих повідомлень.