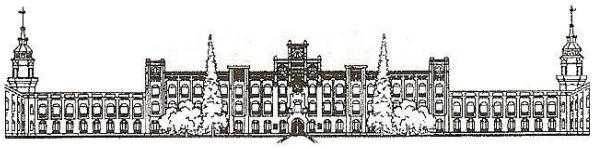

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №1

з дисципліни «Комп'ютерні мережі»

«Стеки мережевих протоколів. Аналізатор мережевого трафіку Wireshark»

Виконав студент групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Мета роботи

Засвоєння функцій модулів різних рівнів еталонної моделі OSI, процедури інкапсуляції та формування повідомлень для передачі в мережу; ознайомлення та вивчення аналізатора мережевого трафіку Wireshark.

План виконання лабораторної роботи

1. Ознайомитися та засвоїти теоретичні відомості про еталонну модель взаємодії відкритих систем OSI та стек мережевих протоколів TCP/IP.
2. Ознайомитися з можливостями аналізатора мережевого трафіку Wireshark.
3. За допомогою аналізатора Wireshark виконати захоплення та провести аналіз мережевих пакетів.

Завдання

1. При виконанні роботи використовується програмне забезпечення для аналізу протоколів комп'ютерних мереж Wireshark. Запустити відповідну програму.
2. Вибрати інтерфейс для захоплення трафіку (меню Capture/Interface) та активізувати режим захоплення.
3. Скопіювати через мережу файл розміром кілька десятків Мбайт.
4. Завершити захоплення трафіку та перейти до режиму аналізу. В захопленому фрагменті виберіть кадр, який містить пакет TCP. Виділіть складові частини кадру. Знайдіть в кадрі транспортні, логічні та фізичні адреси відправника та отримувача.

Теоретичні відомості

Модель OSI

Модель OSI (Open System Interconnect) є еталонною моделлю взаємодії комп'ютерних систем через мережу. Вона розділяє процес передачі даних на 7 рівнів, кожен з яких виконує специфічні функції: від взаємодії з користувачем (прикладний рівень) до передачі сигналів (фізичний рівень). Кожен рівень взаємодіє лише з сусідніми рівнями, забезпечуючи абстрагування складних процесів обміну даними.

TCP/IP

На відміну від OSI, модель TCP/IP (Department of Defense) складається з 4 рівнів і більше орієнтована на реальні потреби передачі даних. Вона використовується у мережах Інтернету і охоплює транспортний рівень, який забезпечує надійність передачі даних, та мережевий рівень, який відповідає за маршрутизацію.

Інкапсуляція

Процедура інкапсуляції — це процес додавання службової інформації до даних кожного рівня під час їхнього переміщення від верхніх рівнів до фізичного. Вона дозволяє мережевим пристроям коректно передавати і приймати дані.

Аналізатор Wireshark

Wireshark — це популярний інструмент для перехоплення та аналізу мережевого трафіку. Він дозволяє досліджувати пакети на різних рівнях, фільтрувати їх за протоколами або умовами, що дозволяє знаходити проблеми в мережі або аналізувати шкідливий трафік.

Хід роботи

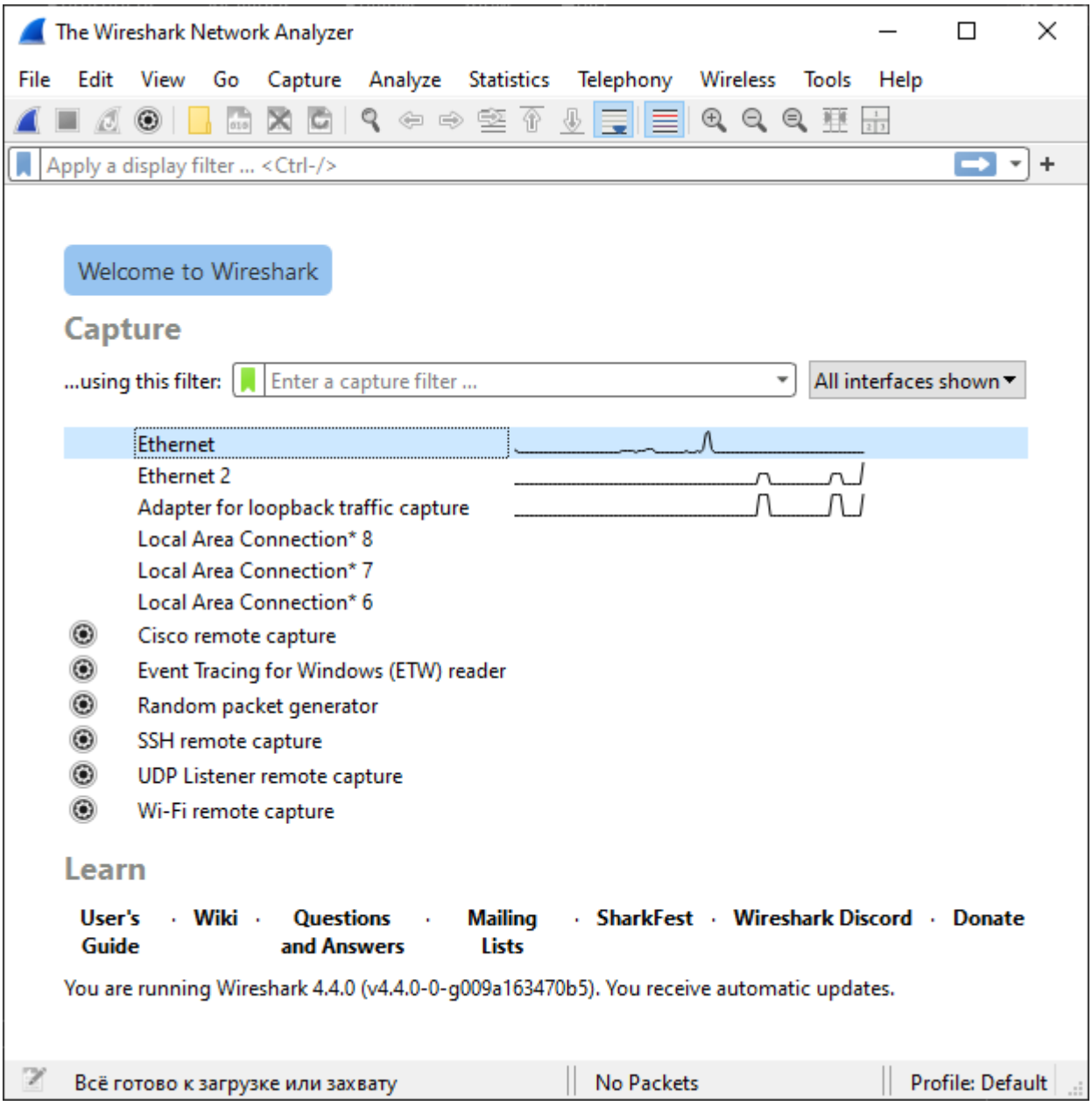

Рис. 1 – Головне вікно програми Wireshark

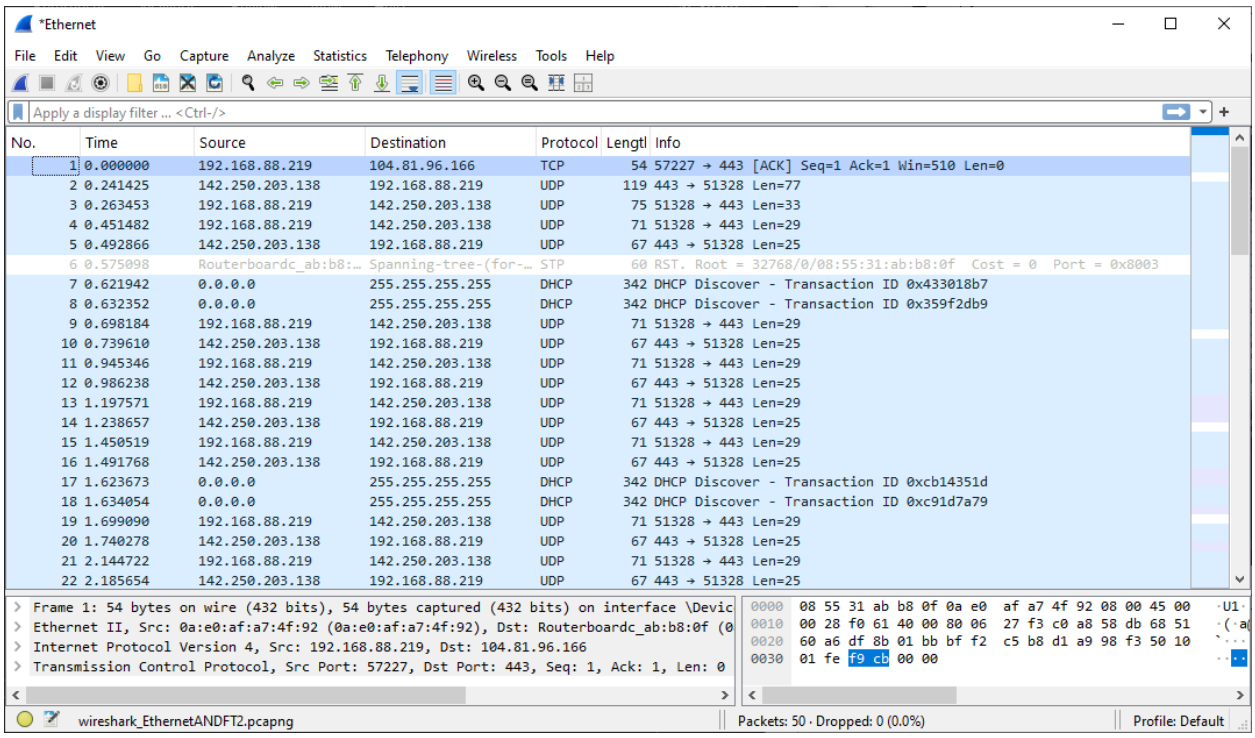

Рис. 2 – Результат сканування інтерфейсу Ethernet

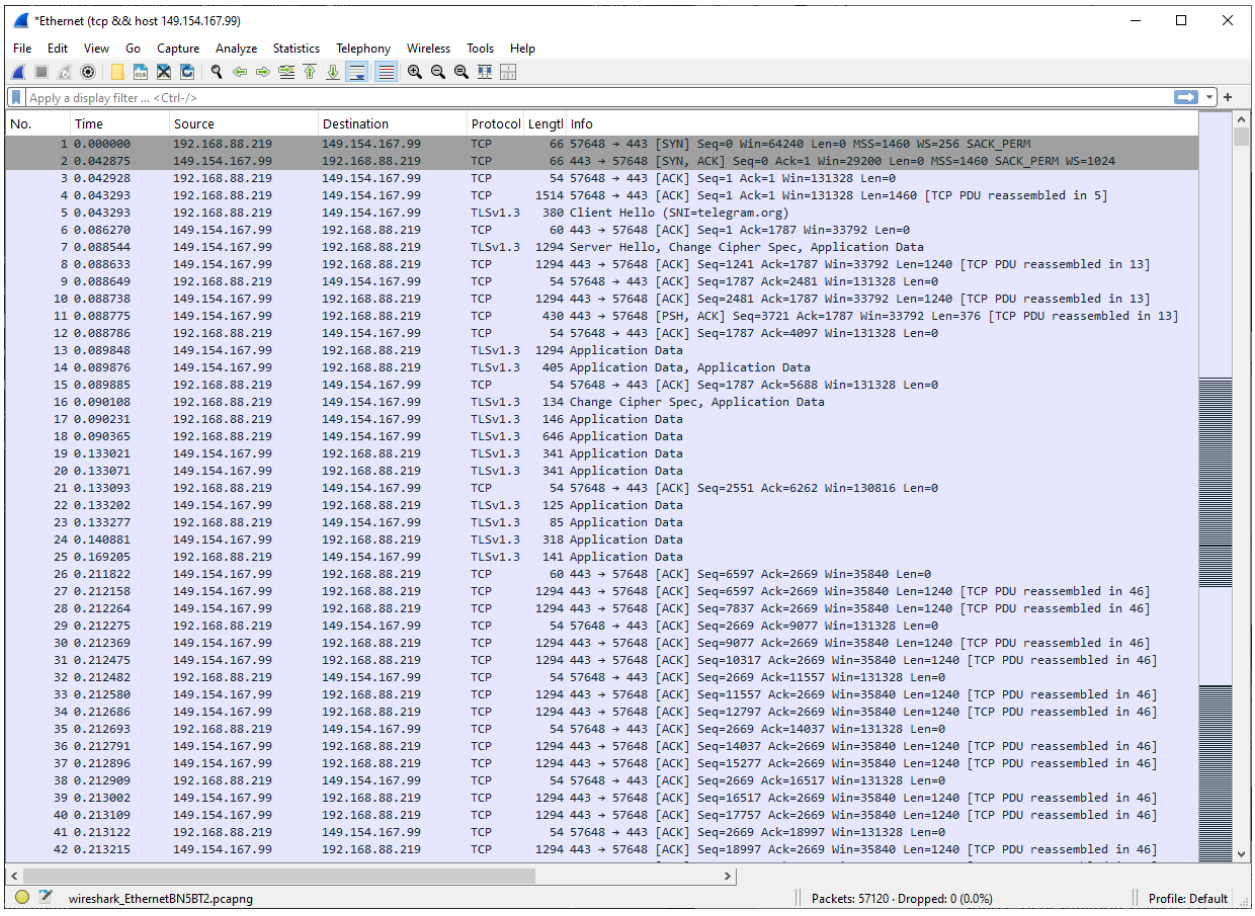

Рис. 3 – Результат сканування інтерфейсу Ethernet під час завантаження файлу

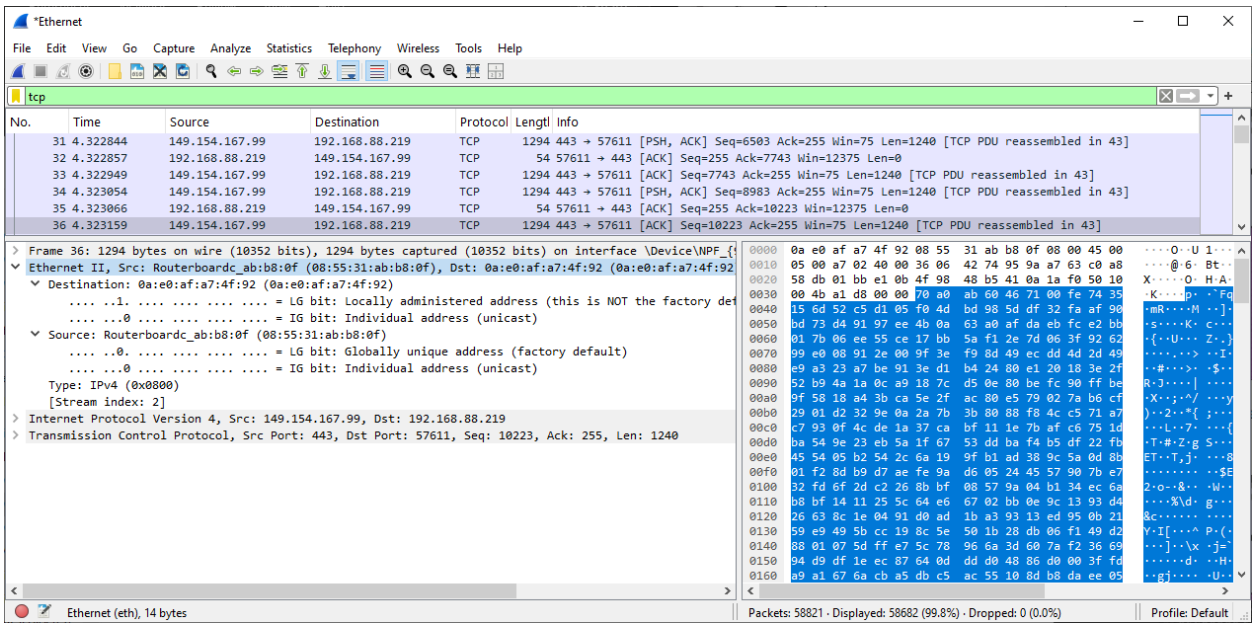

Рис. 4 – Ethernet заголовок пакету

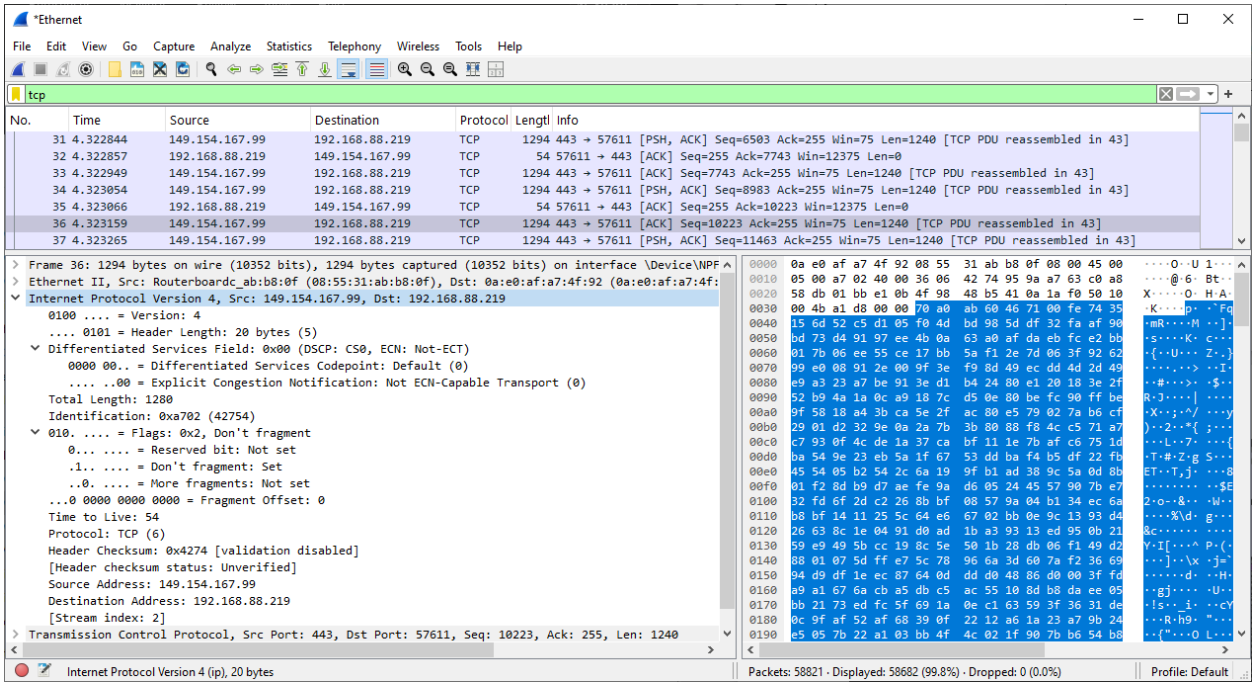

Рис. 5 – IP заголовок пакету

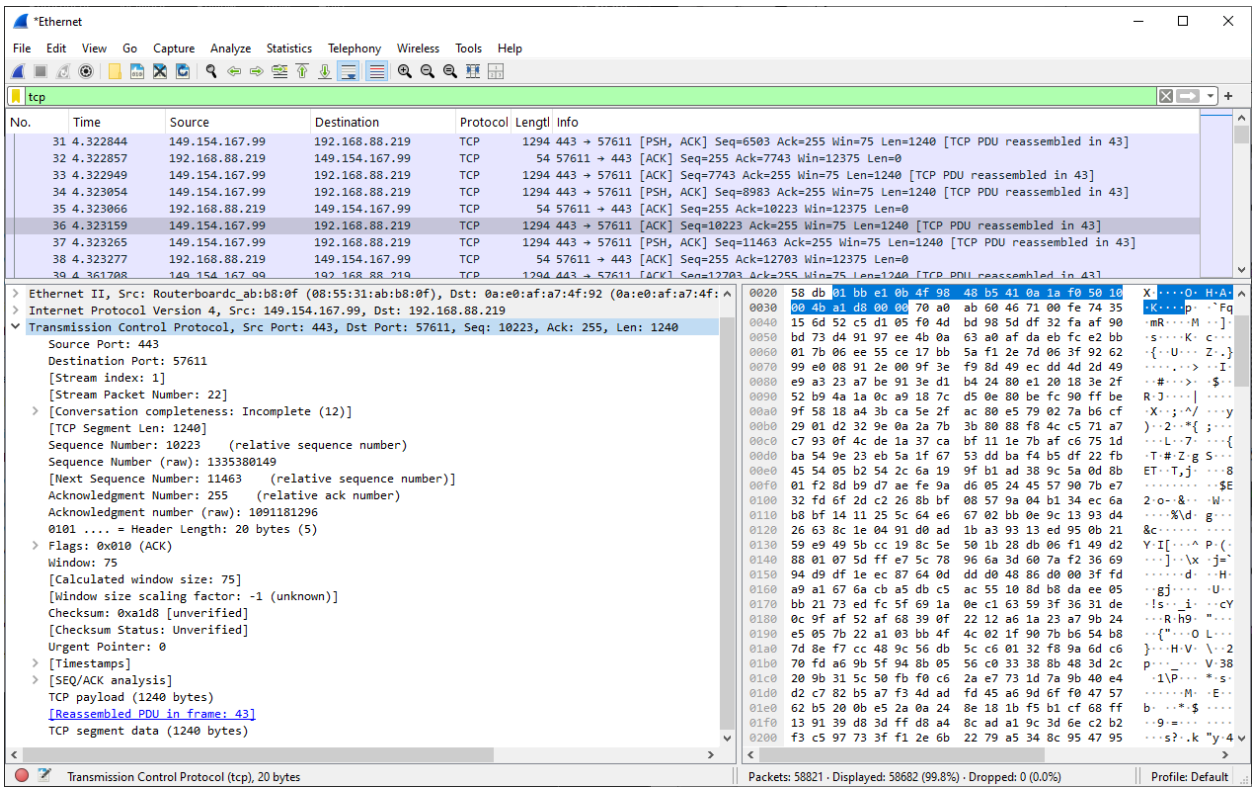

Рис. 6 – TCP заголовок пакету

На рис. 4, рис. 5, рис. 6 можна побачити транспортну, фізичну та логічну адреси відправника та отримувача, а саме:

- MAC адреса маршрутизатора: 08:55:31:ab:b8:0f
- MAC адреса локального пристрою: 0a:e0:af:a7:4f:92
- IP адреса серверу: 149.154.167.99
- IP адреса локального пристрою: 192.168.88.219(локальна адреса)
- Порт серверу: 443
- Порт отримувача(назначений NAT): 57611

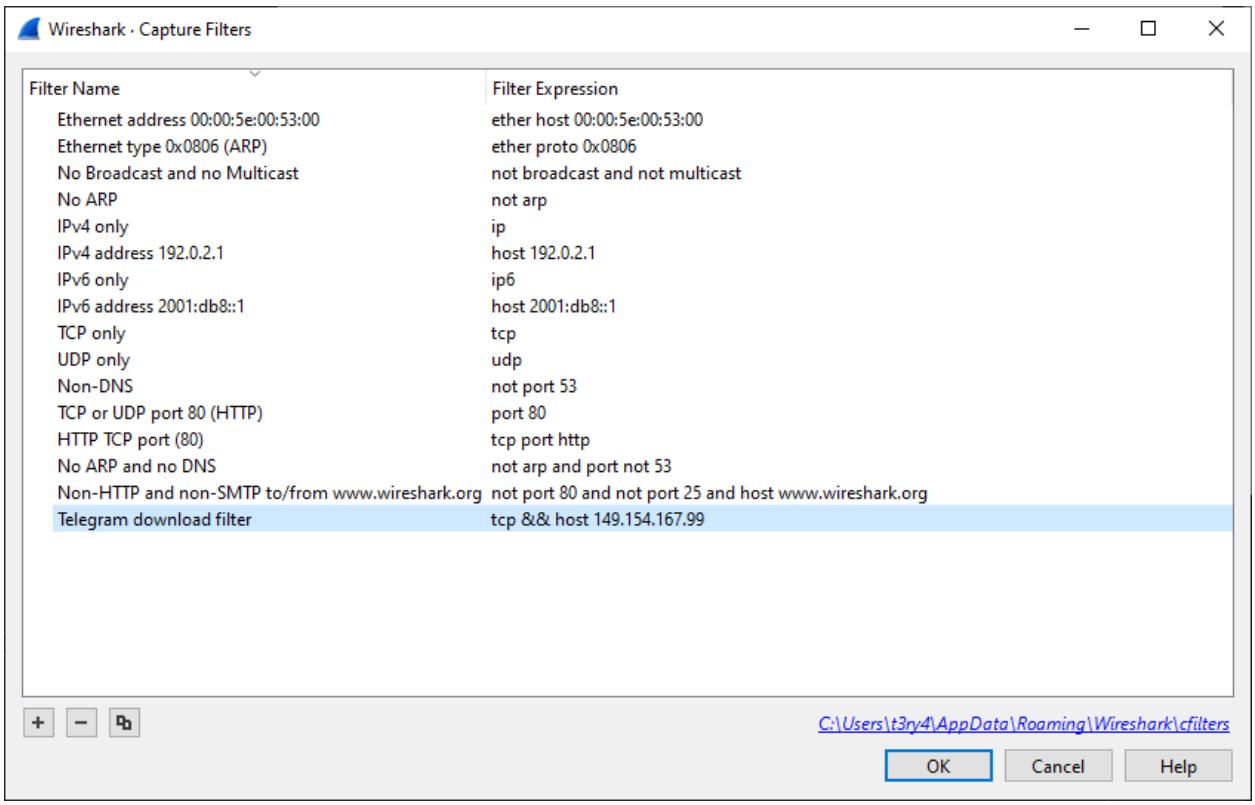

Рис. 7 – Створення фільтру захоплення пакетів TCP з IP адреси 149.154.167.99

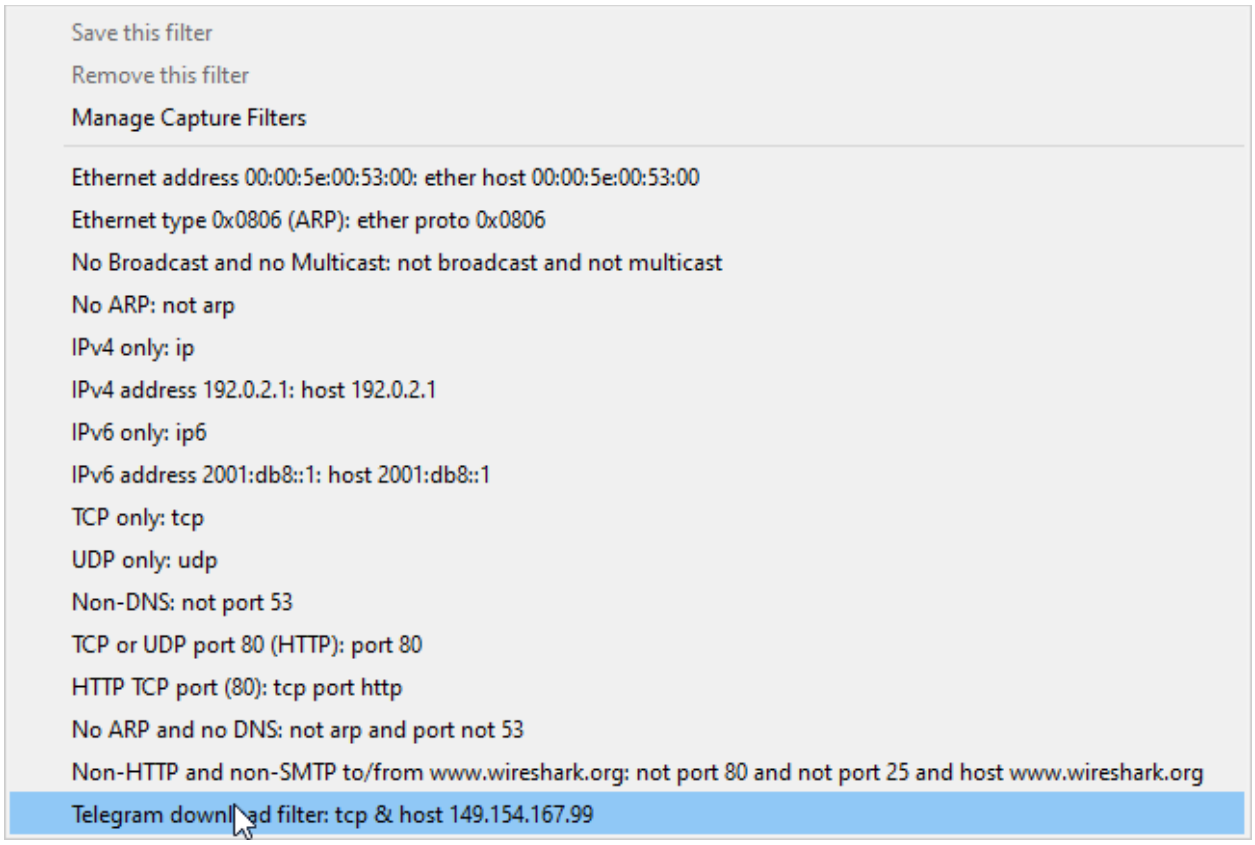

Рис. 8 – Застосування фільтру

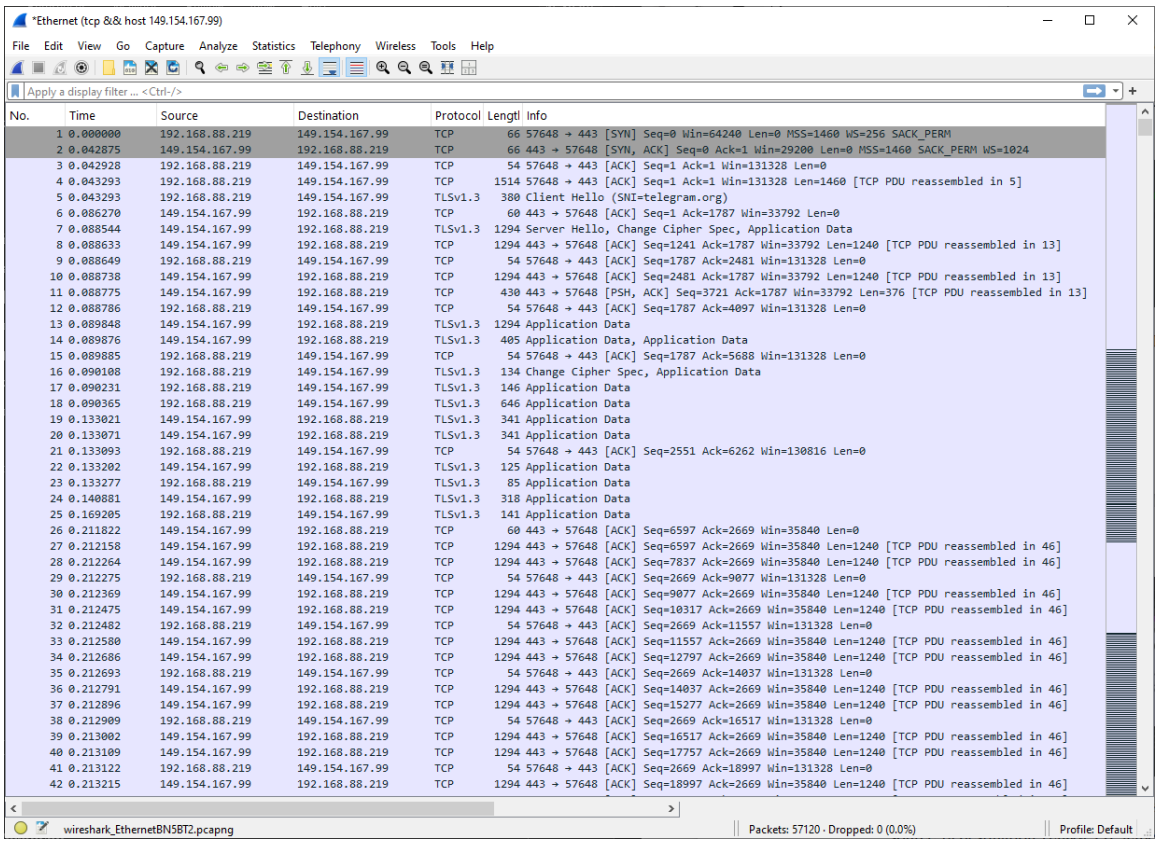

Рис. 9 – Результати захоплення зі застосуванням фільтру

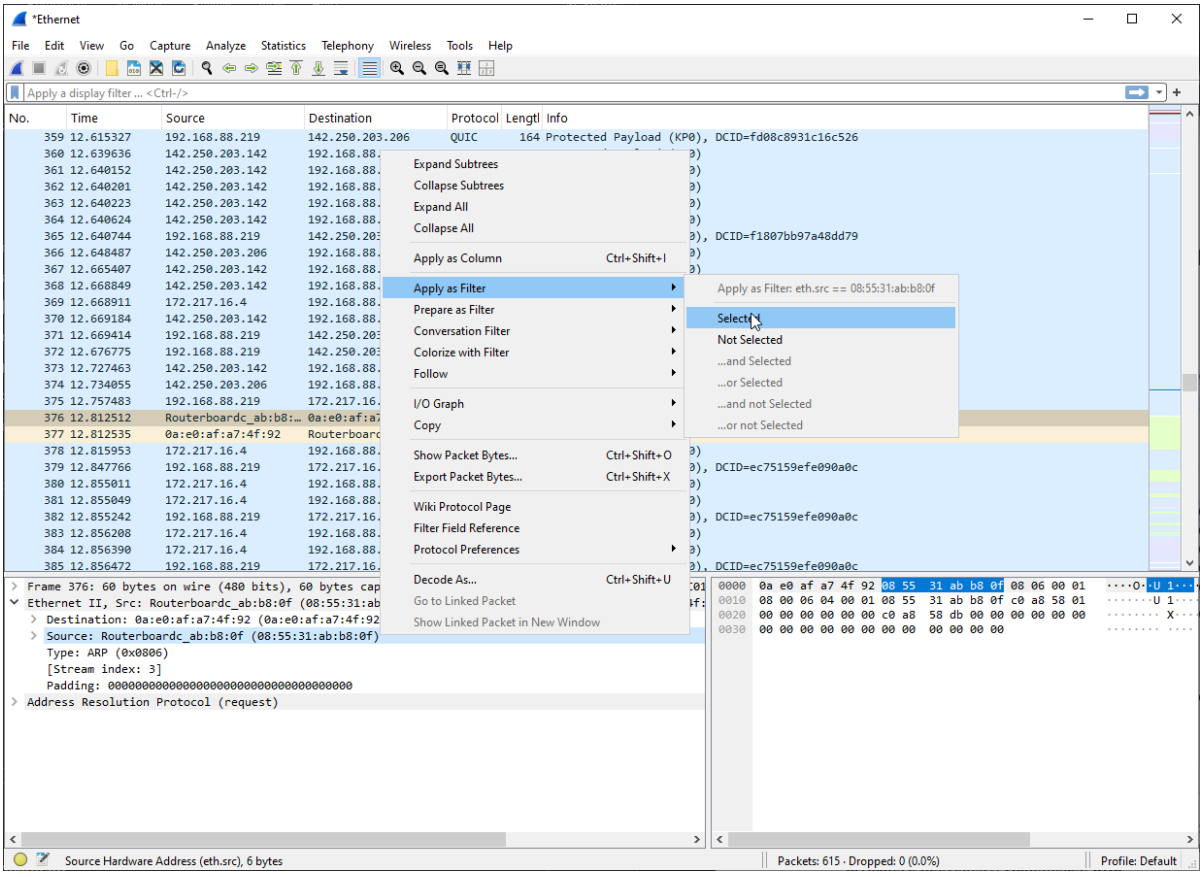

Рис. 10 – Застосування фільтру за MAC адресою з заголовку Ethernet

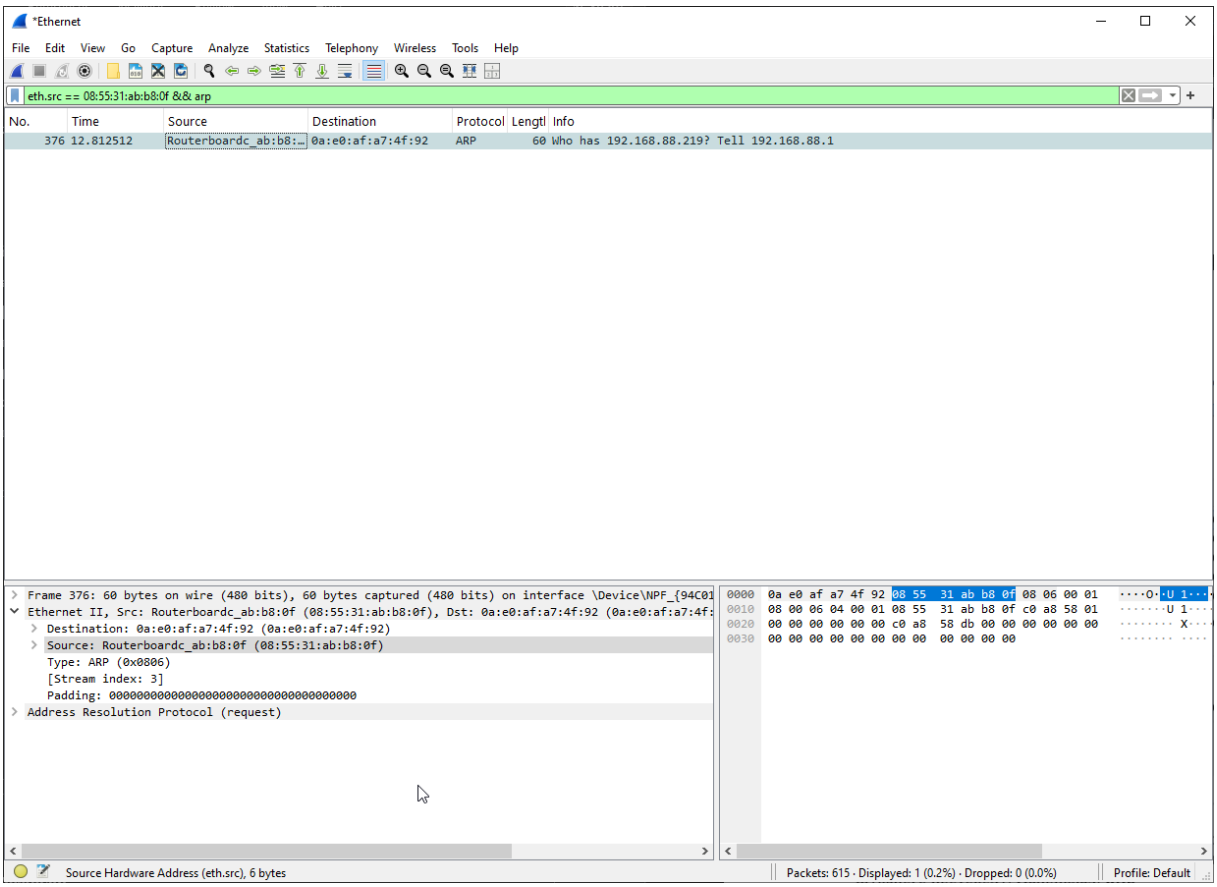

Рис. 11 – Захоплені пакети зі застосуванням фільтру та доданою фільтрацією arp

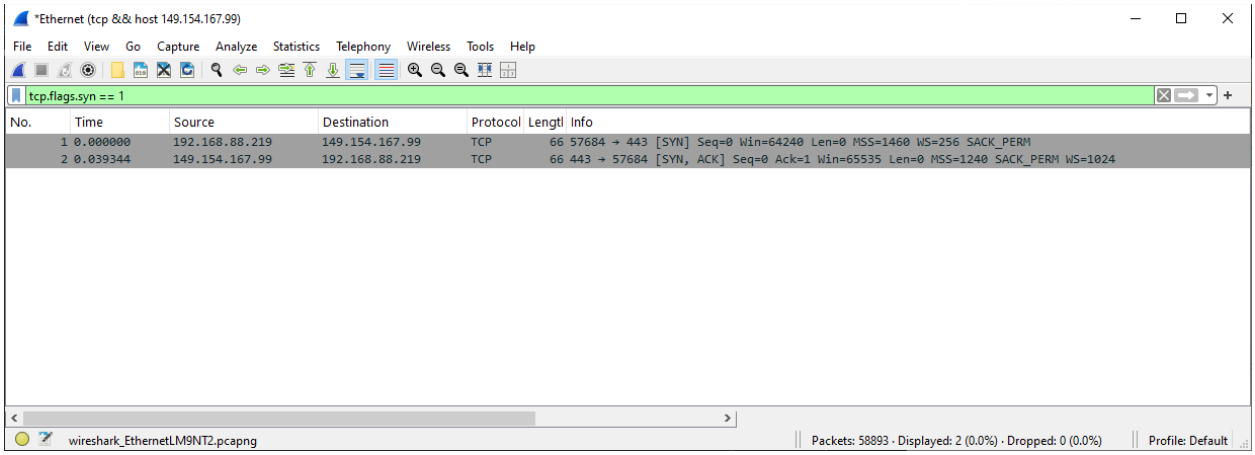

Рис. 12 – Захоплені пакети з прапорцем SYN під час завантаження файлу та доданим раніше фільтром захоплення

Висновки

Ознайомились з функціональними можливостями Wireshark для аналізу мережевого трафіку, зокрема з процесом застосування фільтрів. Використання фільтрів дозволило ефективно відсіяти зайвий трафік та зосередитися на аналізі конкретних протоколів, таких як TCP та IP, або на пакетах за певними критеріями. Це значно полегшило процес аналізу великого обсягу даних. Метою роботи було навчитися використовувати фільтри для точного визначення необхідних пакетів за заданими параметрами, такими як IP-адреси або порти. Було проведено аналіз інкапсуляції даних на різних рівнях мережевої моделі OSI та вивчено взаємодію між транспортним і мережевим рівнями.