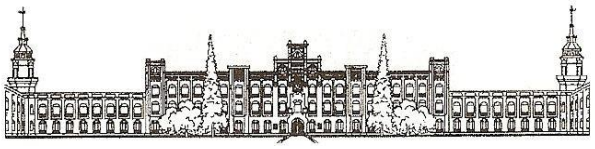

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

**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.

## *Хід роботи*

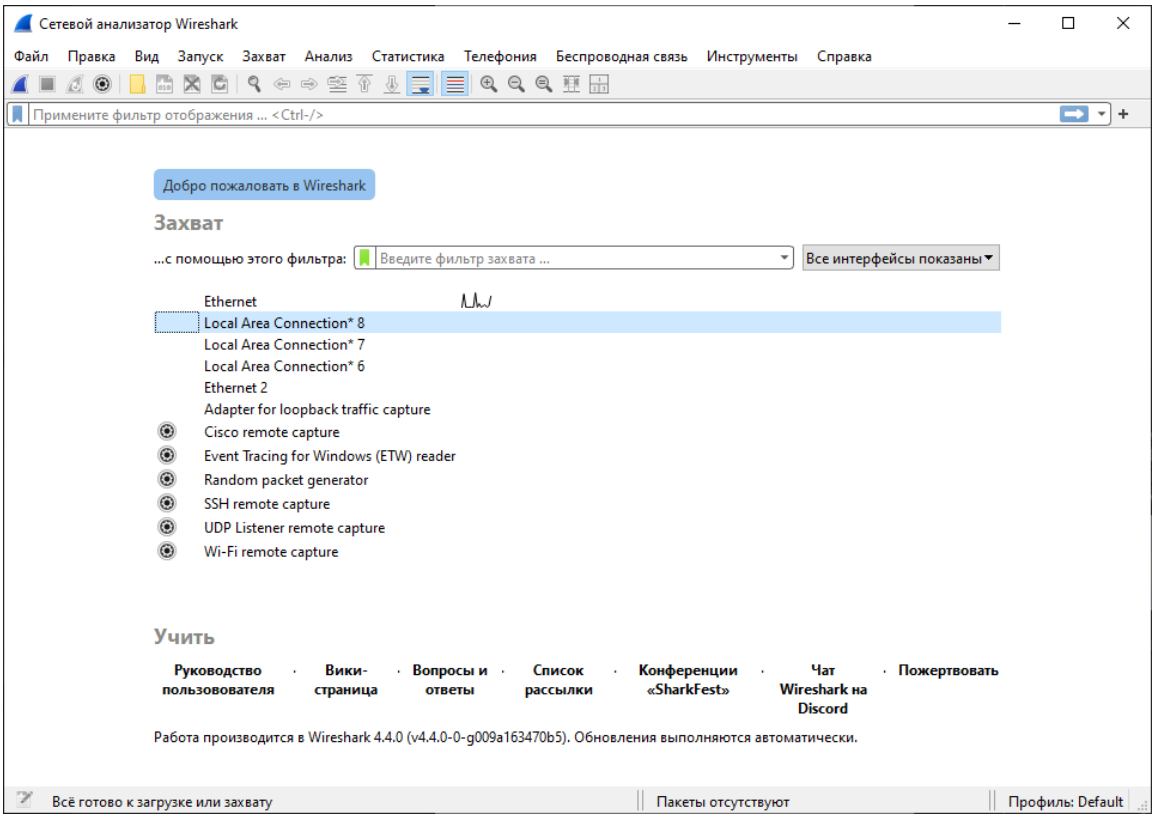


Рис. 1 – Початкове вікно Wireshark

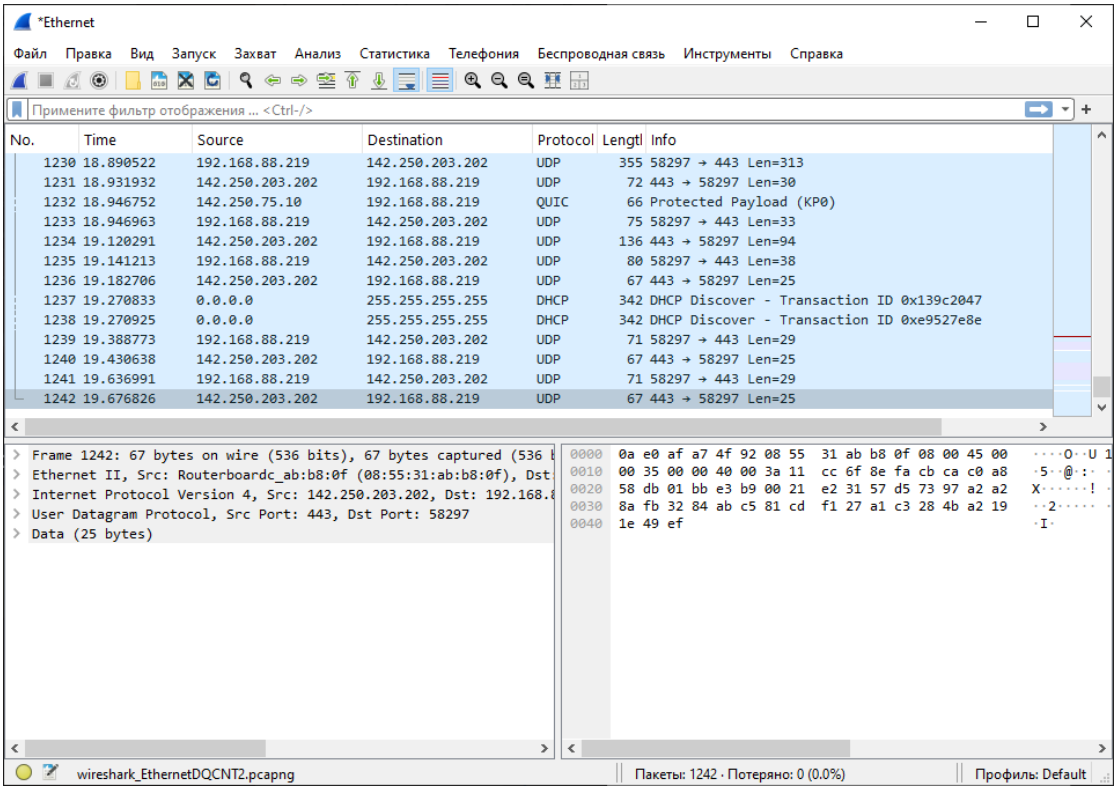


Рис. 2 – Головне вікно Wireshark

З метою копіювання файлу через мережу для подальшого захоплення, був завантажений інтернет додаток, відповідно захоплена мережа Ethernet.

Рис. 3 – Аналіз пакету Wireshark з прапором SYN

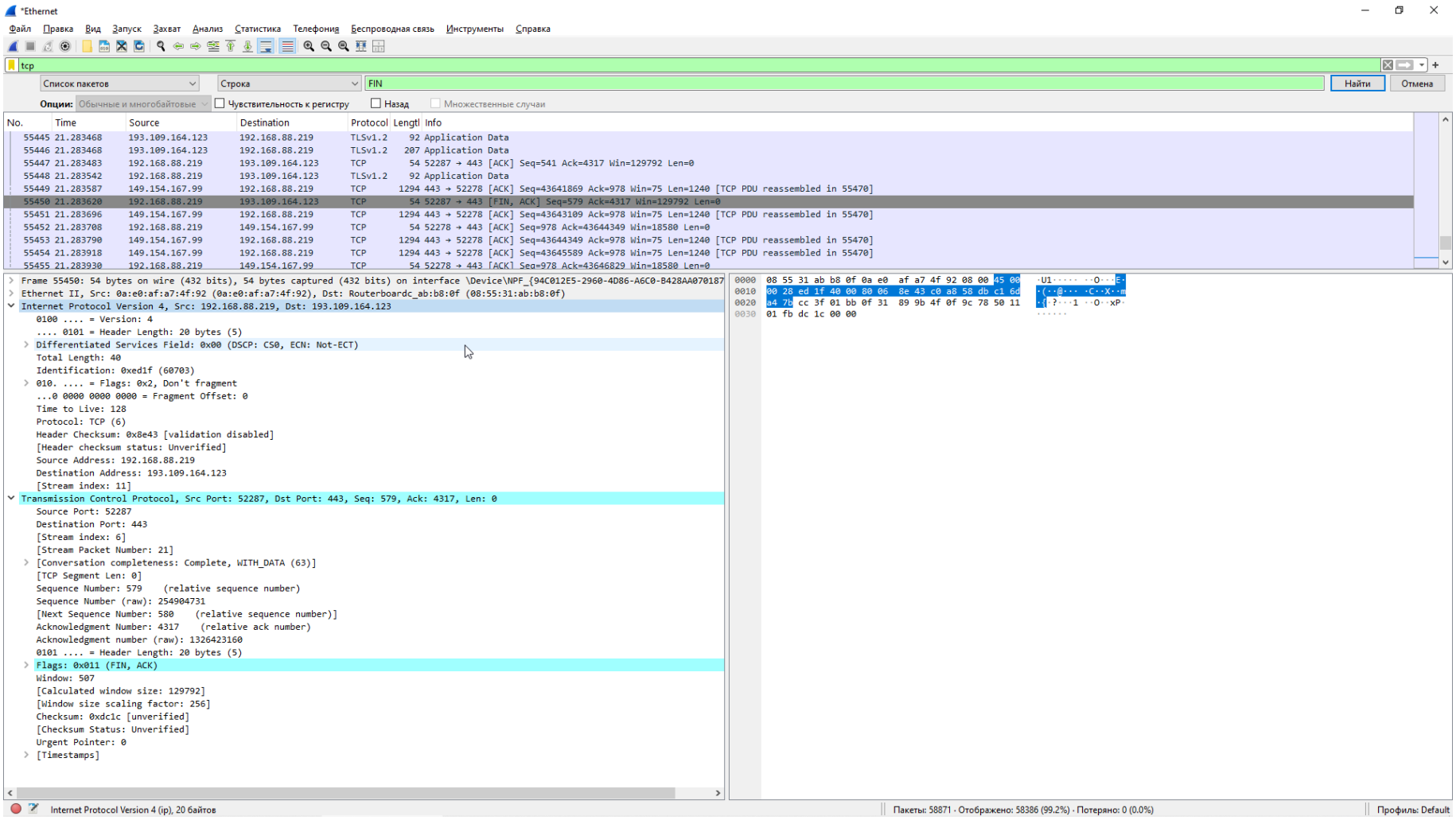


Рис. 4 – Аналіз пакету Wireshark з прапором FIN

На рис. 3 зображено триходове рукостискання(3-Way Handhake: SYN, SYN-ACK, ACK). Під час передачі даних файл був розділений на окремі TCP-сегменти, що були успішно зібрані в повну одиницю передачі даних PDU або Protocol Data Unit, на що відповідно вказує Wireshark в розділі Info для пакетів за допомогою повідомлення “TCP segment of a reassembled PDU”. На рис. 4, де зображено пакет з прапорцями FIN, ACK, що вказують на закінчення з’єднання між двома пристроями. Пакет з такими прапорцями відправляють обидва пристрої, щоб підтвердити готовність закрити з’єднання.

Також на рис. 3 та на рис. 4 можна побачити фізичні, логічні та транспортні адреси. В першому випадку, де відправник – сервер з якого завантажували файл, а в другому – пристрій з локальної мережі.

*Сервер мав такі адреси:*

Фізична адреса(MAC) - 08:55:31:ab:b8:0f

Логічна адреса(IP) - 193.109.164.123

Транспортна адреса(порт) – 52287

*Пристрій з локальної мережі:*

Фізична адреса(MAC) - 0a:e0:af:a7:4f:92

Логічна адреса(IP) - 192.168.88.219

Транспортна адреса(порт) – 443

У випадку з пристроєм з локальної мережі ми бачимо локальну IP адресу, а у серверу – публічну.