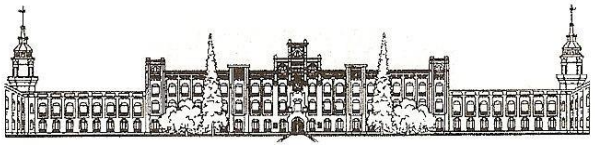

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №2

з дисципліни «Комп'ютерні мережі»

«Аналіз просування даних по стеку TCP/IP з використанням аналізатора трафіку Wireshark. Транспортний і мережевий рівні»

Виконав студент групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Мета роботи

Засвоєння функцій модулів транспортного та мережевого рівнів стеку протоколів TCP/IP, структури заголовків протоколів TCP та UDP, псевдозаголовку, аналіз фрагментів протоколу TCP за допомогою аналізатора мережевого трафіку Wireshark.

План виконання лабораторної роботи

1. Ознайомитися та засвоїти теоретичні відомості, викладені в методичному посібнику до лабораторної роботи.

2. Виконати завдання до лабораторної роботи.

Завдання

№1

За допомогою програми Wireshark необхідно виконати захоплення даних сеансу FTP і визначити значення полів заголовків протоколу TCP при передачі файлів з використанням протоколу FTP між хост-комп'ютером і анонімним FTP-сервером. Під'єднання до анонімного FTP-серверу і завантаження файлу виконується за допомогою браузера.

1. Активізувати режим захоплення даних з використанням програми Wireshark.
2. Завантажити файл довідки README.TXT.

2.1. Під 'єднатися до FTP-сервера центру FreeBSD:

ftp://ftp3.ie.freebsd.org.

2.2. В розділі pub/FreeBSD знайти і завантажити файл README.TXT (рисунок 2.10).

2.3. Після завершення завантаження файлу зупинити захоплення даних програмою Wireshark.

3. Відкрити головне вікно програми Wireshark.
4. Проаналізувати поля заголовків сегментів TCP.

№2

1. Ознайомитись з можливостями фільтрації даних за різними ознаками, зокрема, за MAC-адресою відправника і отримувача. Фільтр створюється за описаною вище методикою. Відповідно до рекомендачій викладача сформувати фільтр за MAC-адресою.

2. Розглянути результат інкапсуляції при передачі даних. В захоплених пакетах виділити службову інформацію (заголовки) всіх блоків даних, а також, за наявністю, кінцевика.

3. Використовуючи фільтр відображення tcp.flags.syn = = 1 відібрати сегменти-запити, які містять встановлений прапорець SYN у заголовку та сегменти-відповіді, які містять встановлені прапорці SYN та ACK. Провести аналіз поля Options заголовку TCP. Яке значення MSS використовується в з'єднанні, що аналізується?

4. За допомогою меню «Statistics» необхідно отримати і додати до звіту таку інформацію:

- кількість захоплених пакетів та байтів;
- середня швидкість передачі даних (в бітах за секунду);
- середній розмір пакета;
- час, протягом якого здійснювалось захоплення трафіку;
- вивести таблицю Ethernet Conversations та пояснити вміст її рядків;
- вивести IO Grafs, за допомогою якого визначити пікову швидкість передачі даних протягом інтервалу, що підлягає аналізу.

5. За результатами роботи зробити висновки.

Хід роботи

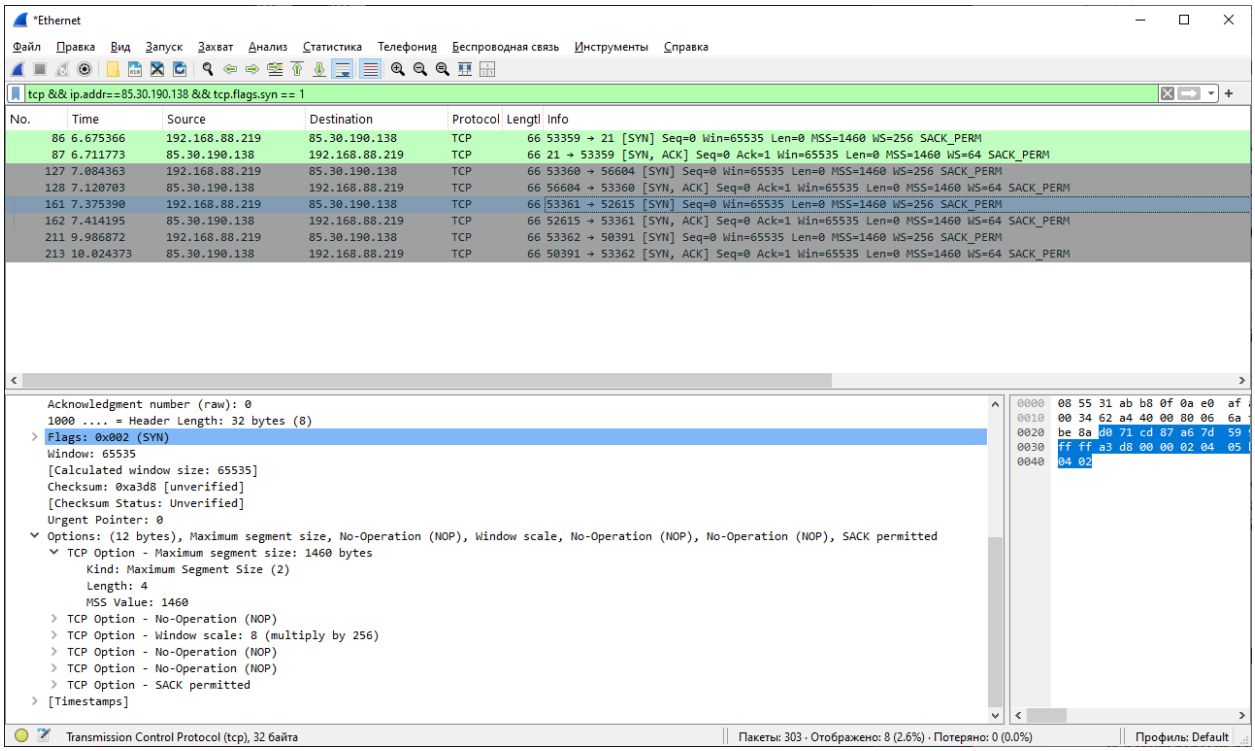

Рис.1 – Розгорнутий фрагмент TCP, встановлення зв’язку [SYN], [SYN, ACK], [SYN]

На рис. 1 можна побачити розгорнутий фрагмент TCP після завантаження файлу з FTP серверу, пакети були відфільтровані за протоколом TCP, IP адресою серверу та за прапором SYN.

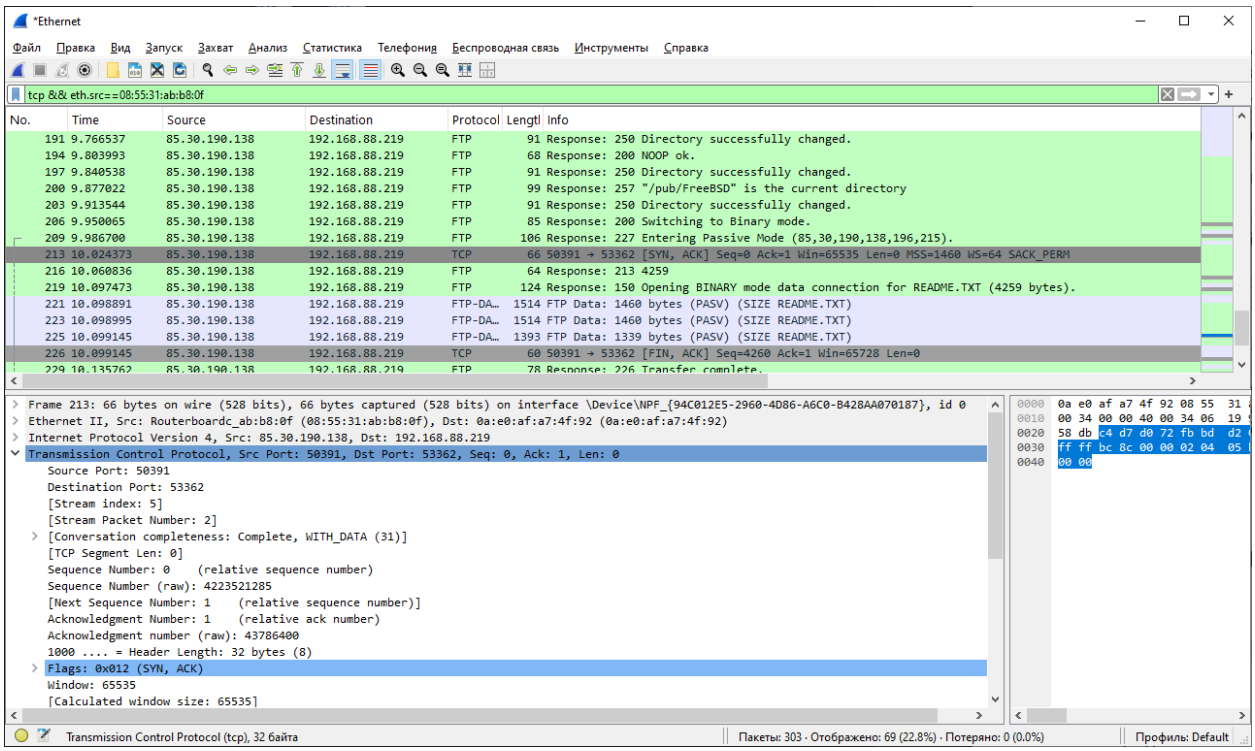

Рис.2 – Розгорнутий фрагмент TCP, пакети відфільтровані за MAC-адресою

На рис. 2 можна побачити приклад фільтрації пакетів за MAC-адресою, а також побачити розмір MSS, що становить 1460.

Фрагмент TCP містить наступні поля:

Порт відправника: 33449;

Порт одержувача: 80 (стандартний для FTP-з’єднань);

Порядковий номер: 0 (перший октет у сегменті TCP);

Номер підтвердження: 0 (також перший октет у сегменті TCP);

Прапорці: встановлено прапорець SYN (синхронізація);

Розмір вікна: 62240 байт;

Максимальний розмір сегменту (MSS): 1460 байт (MTU – 1484 байт, IP та TCP заголовки займають 12 байт, додаткових опцій немає, тому MSS = 1484 - 12 - 12 = 1460).

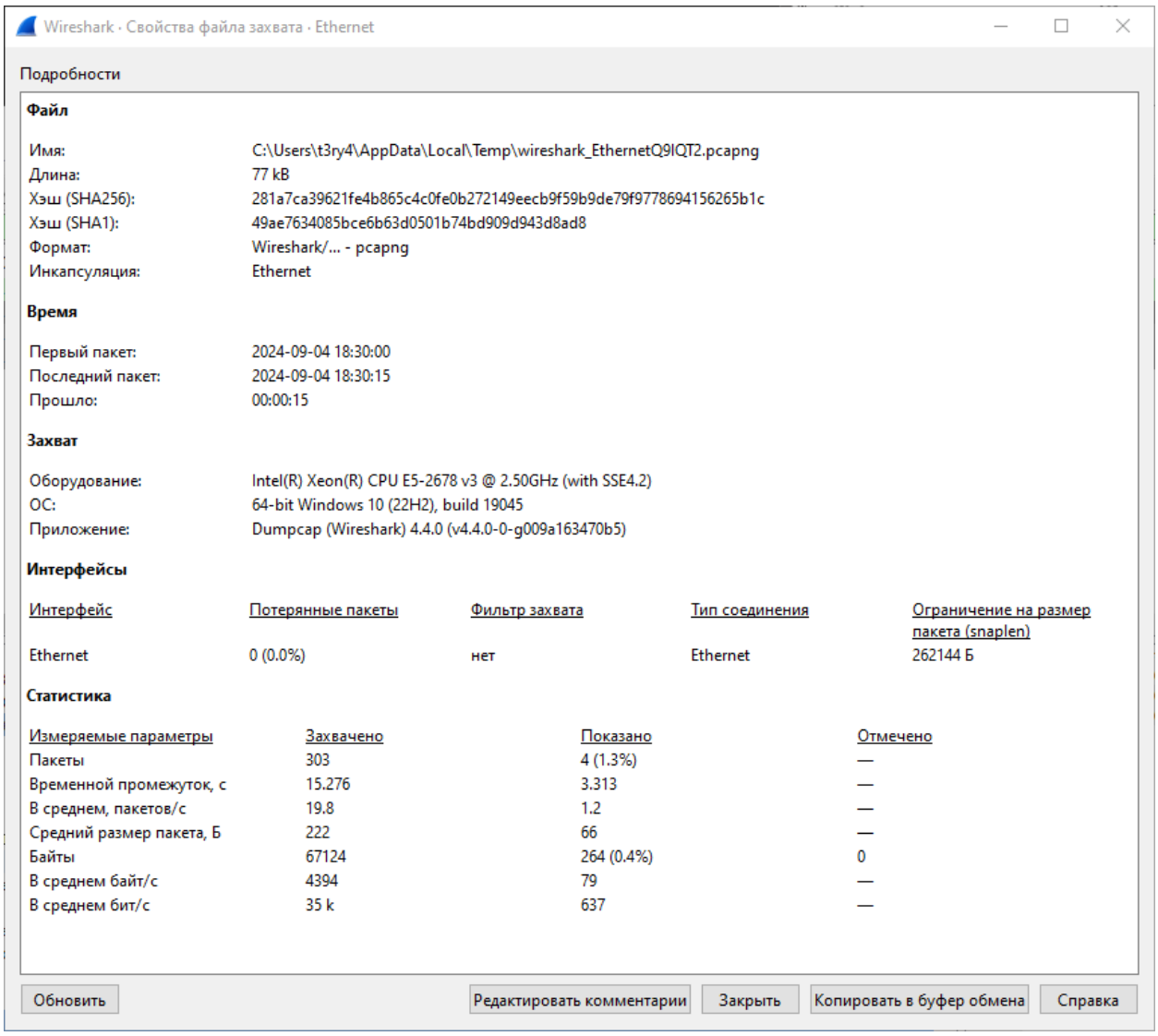

Рис. 3 – Статистика захоплення пакетів Wireshark

З рис. 3 можна отримати основну статистику.

Кількість захоплених пакетів та байтів: 303 пакети та 67124 байти

Середня швидкість передачі даних(біти/секунда): 19.8 бітів за секунду

Середній розмір пакету: 222 байти

Час, протягом якого здійснювалось захоплення трафіку: 15.276 секунд

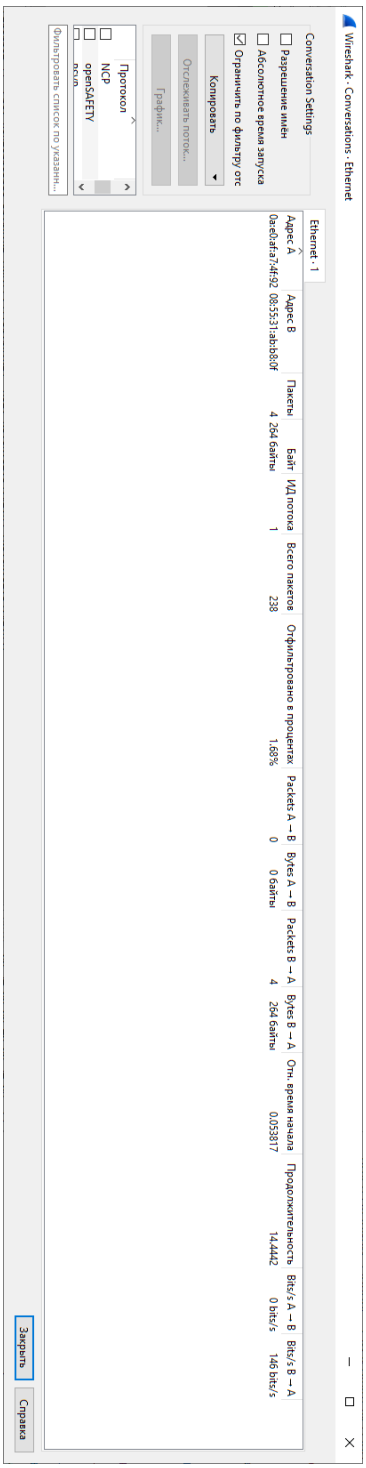

Рис. 4 – Таблиця Ethernet Conversations

На рис. 4 зображено таблицю Ethernet Conversations. Кожен рядок у цьому списку містить дані про:

- MAC-адреси відправника і отримувача – унікальні апаратні адреси пристроїв, які беруть участь у передачі даних.
- Кількість пакетів – скільки пакетів було надіслано з одного пристрою на інший і назад (якщо є двосторонній зв'язок).
- Загальний обсяг даних – скільки байтів було передано між пристроями.
- Тривалість – час, протягом якого відбувалася передача даних між цими двома пристроями.

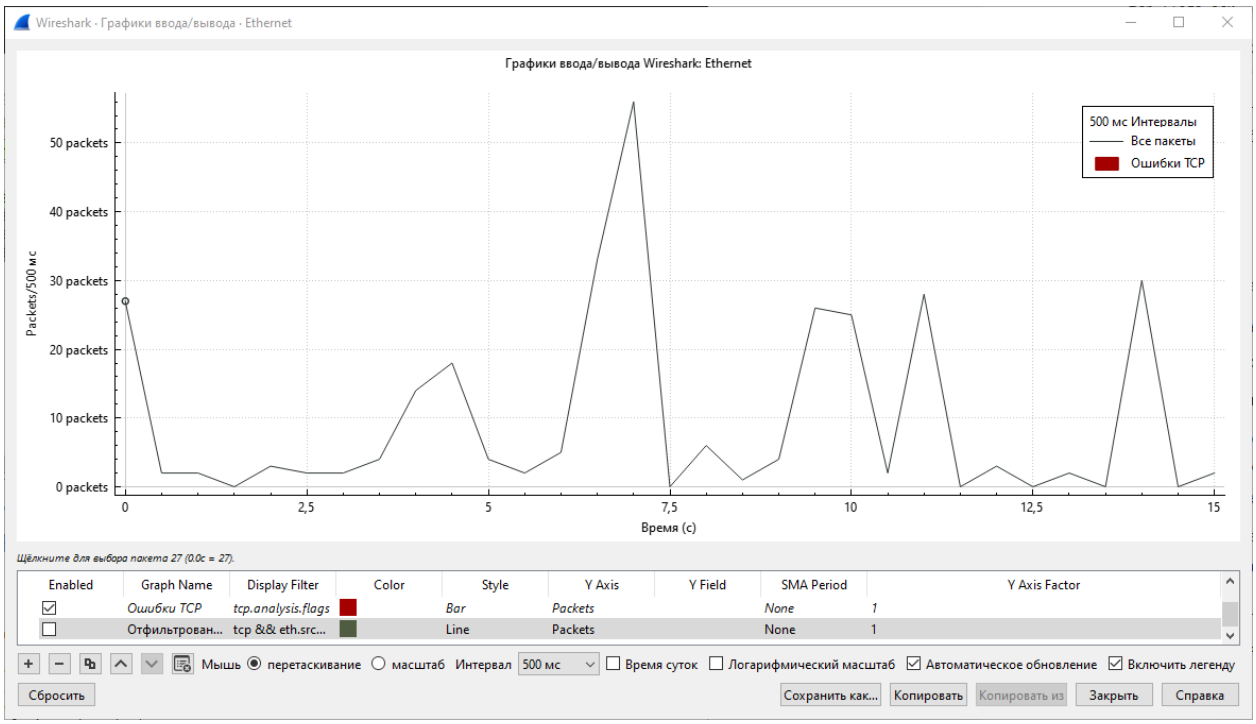

Рис. 5 – IO Graphs, графік вводу/виводу

На рис. 5 зображений графік зміни обсягу переданих даних(пакетів) у часі, можна побачити, що на 7-ій секунді було пікове навантаження, а саме 56 пакетів.

Висновок

Під час лабораторної роботи було проведено дослідження передачі даних за стеком протоколів TCP/IP за допомогою Wireshark. Дослідження було зосереджено на ролях транспортного та мережевого рівнів, проаналізовано заголовки протоколів TCP і UDP і проведено фільтрацію даних на основі MAC-адрес.

Аналіз також включав сегменти TCP, зокрема ті, що містять прапори SYN та ACK, під час визначення параметрів з’єднання MSS. Крім того, дослідження таблиці розмов Ethernet і графіків вводу/виводу показало пікові навантаження, що виникають під час передачі даних.

Загалом покращили розуміння принципів мережевого трафіку, а також удосконалили вміння використовувати Wireshark для аналізу мережевих з’єднань.