1. Мета роботи

Метою даної лабораторної роботи є оволодіння методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

2. Хід роботи

Під час виконання лабораторної роботи виконано наступні дії:

1. Запущено веб-браузер.

2. Запущено Wireshark.

3. В Wireshark активовано діалог вибору мережевого інтерфейсу для захоплення: ‘Capture >> Interfaces’.

4. Обрано інтерфейс, для якого відображається найбільша кількість захоплених пакетів, - ‘Wi-Fi: en0’ та натиснуто кнопку Start навпроти нього.

5. Відкрито в браузері сторінку за наступною адресою: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Пакети зі вмістом зазначеної веб-сторінки були захоплені Wireshark.

6. Зупинено захоплення пакетів за допомогою команди ’Capture >> Stop’.

7. Введено текст «http» в поле фільтрації та натиснуто Apply. У вікні лістингу пакетів залишилися тільки ті, які були створені протоколом HTTP.

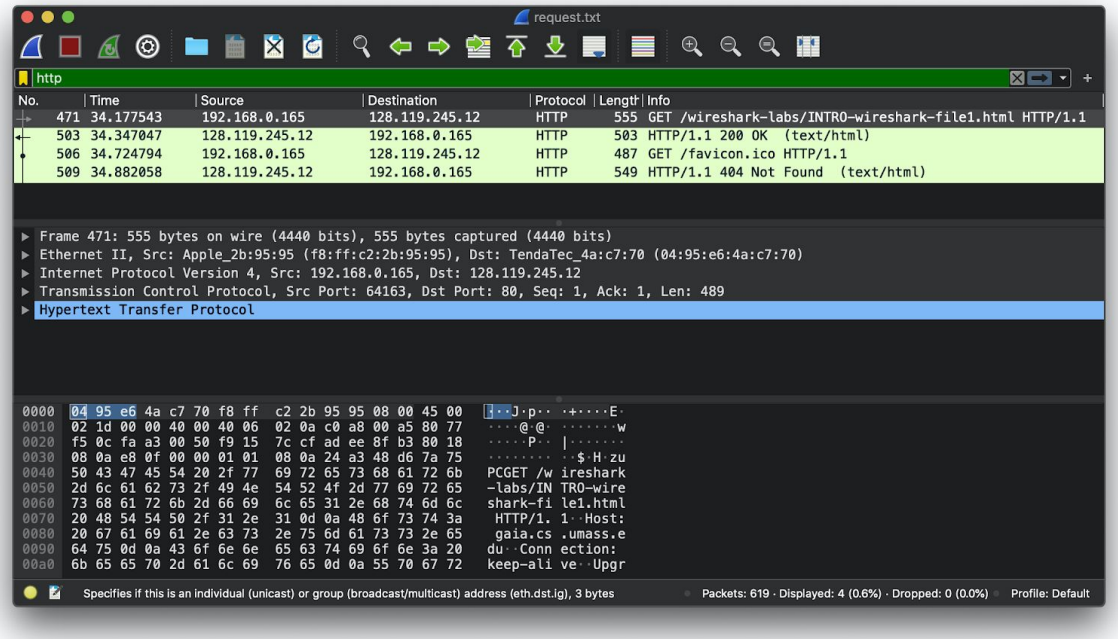

Рис. 1. Результат застосування фільтру http

8. Обрано перший пакет HTTP, який відобразився у вікні лістингу, це було повідомлення GET протоколу HTTP. Також цей пакет вміщував інформацію про інші протоколи нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрито деталі, пов’язані з протоколом HTTP та скрито детальну інформацію про інші протоколи.

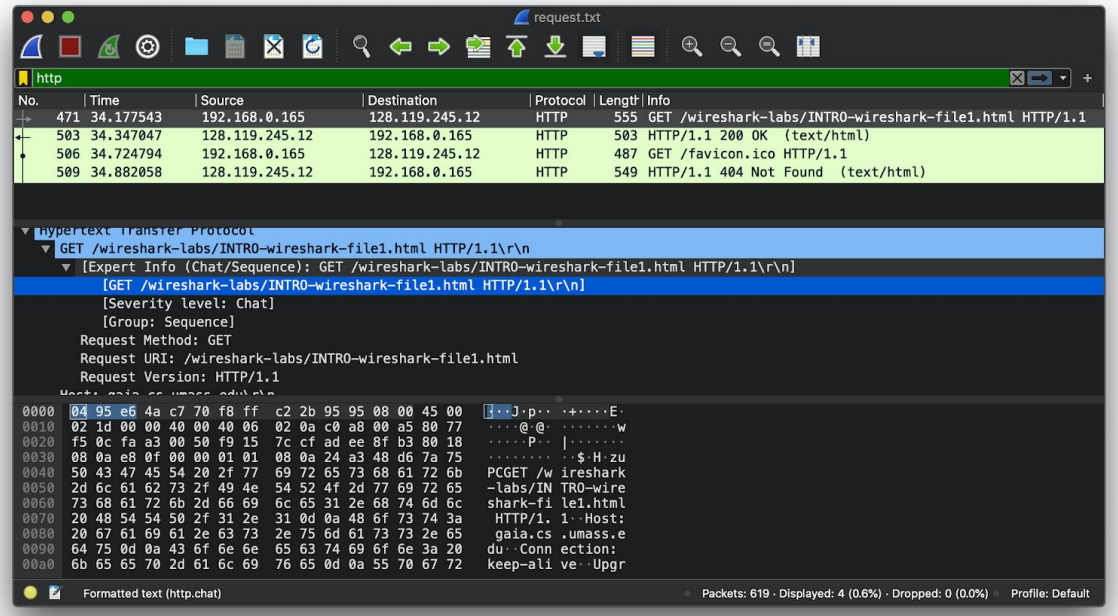

Рис. 2. Деталі заголовку запиту

10. Збережено перші пакети запиту та відповіді у відповідні файли:

Vysotskyi_Request_INTRO-wireshark.txt та

Vysotskyi-Response_INTRO-wireshark.txt.

11. Перевірено, що у збережених файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколи.

3. Відповіді на контрольні питання

3.1 Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

У вікні лістингу протоколів до включення фільтрації відображалися наступні протоколи: TCP, UDP, DNS, TLSv1.2, HTTP, та інші.

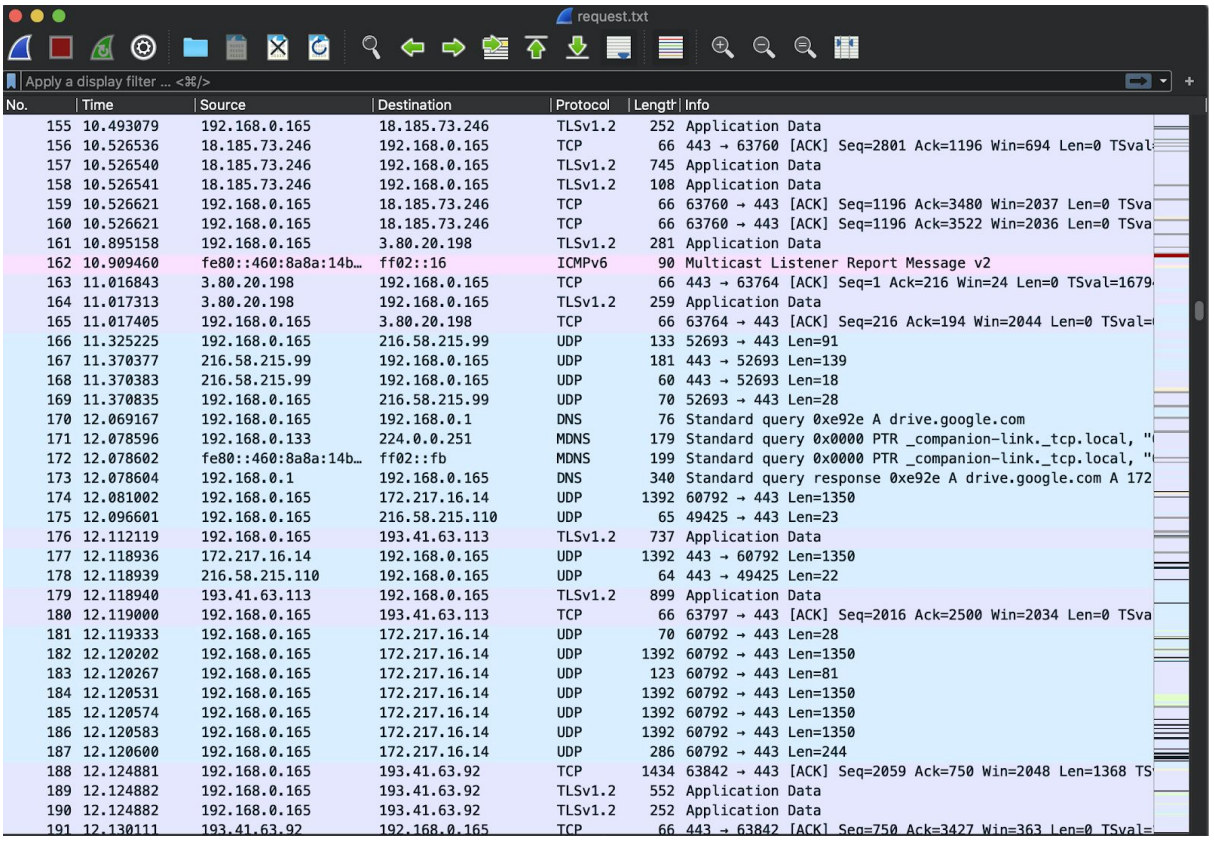

Рис. 3. Інформація про протоколи до включення фільтрації

3.2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

У пакеті запиту використовувались - eth:ethertype:ip:tcp:http протоколи, у пакеті відповіді - eth:ethertype:ip:tcp:http:data-text-lines протоколи.

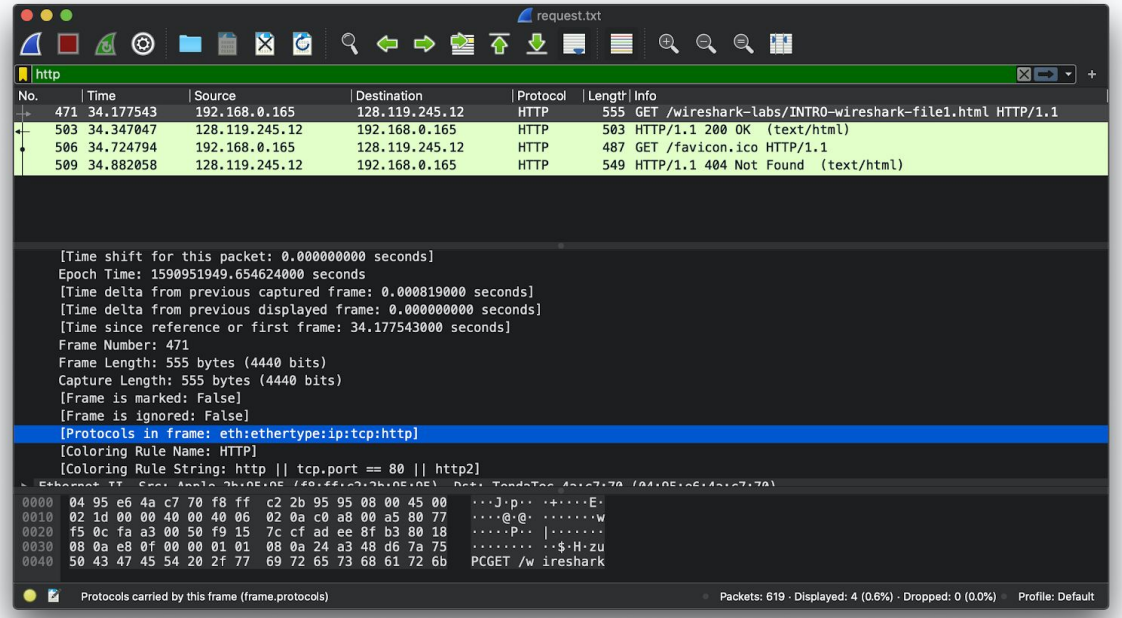

Рис. 4. Протоколи, які використовувались у пакеті запиту

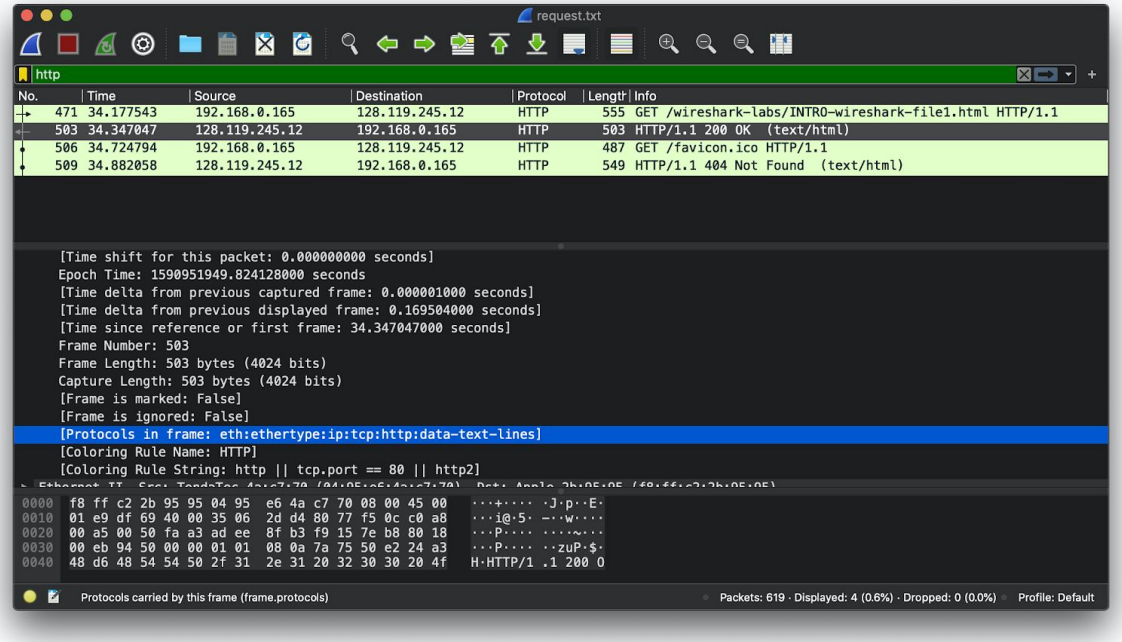

Рис. 5. Протоколи, які використовувались у пакеті відповіді

3.3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Час відправки пакету запиту - 22:05:49.654624000 EEST, час отримання пакету відповіді 22:05:49.824128000 EEST, період часу між пакетом запиту та відповіді склав приблизно 0.17 с.

3.4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Для пакету запиту:

Source - 192.168.0.165, Destination - 128.119.245.12;

Для пакету відповіді:

Source - 128.119.245.12, Destination - 192.168.0.165.

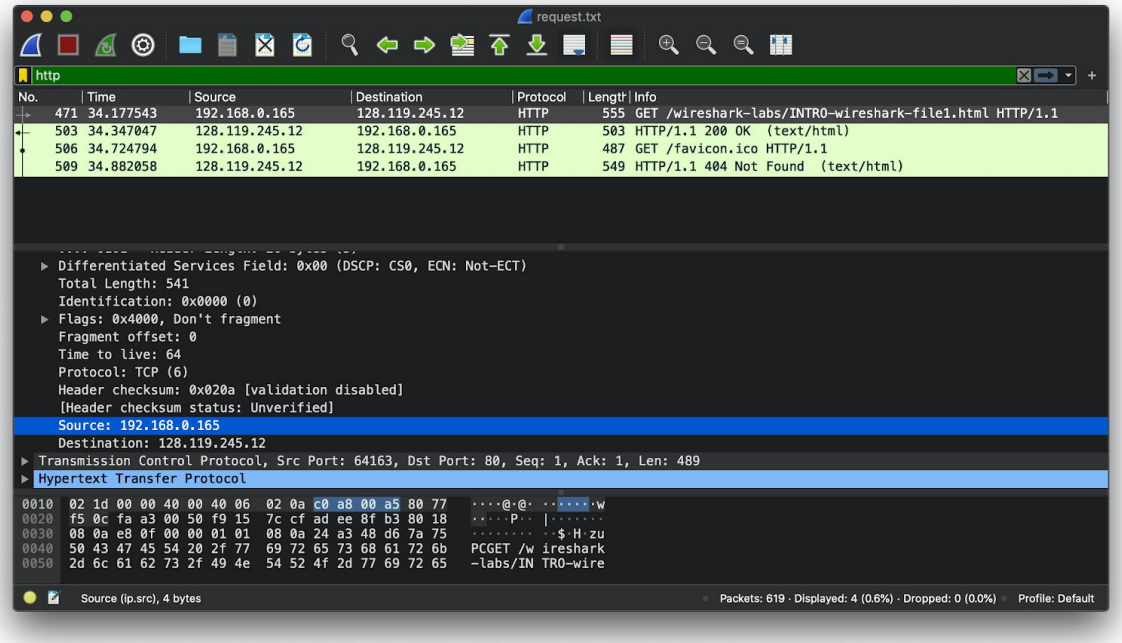

Рис. 6. Інформація про вихідні та цільові адреси пакетів із запитом

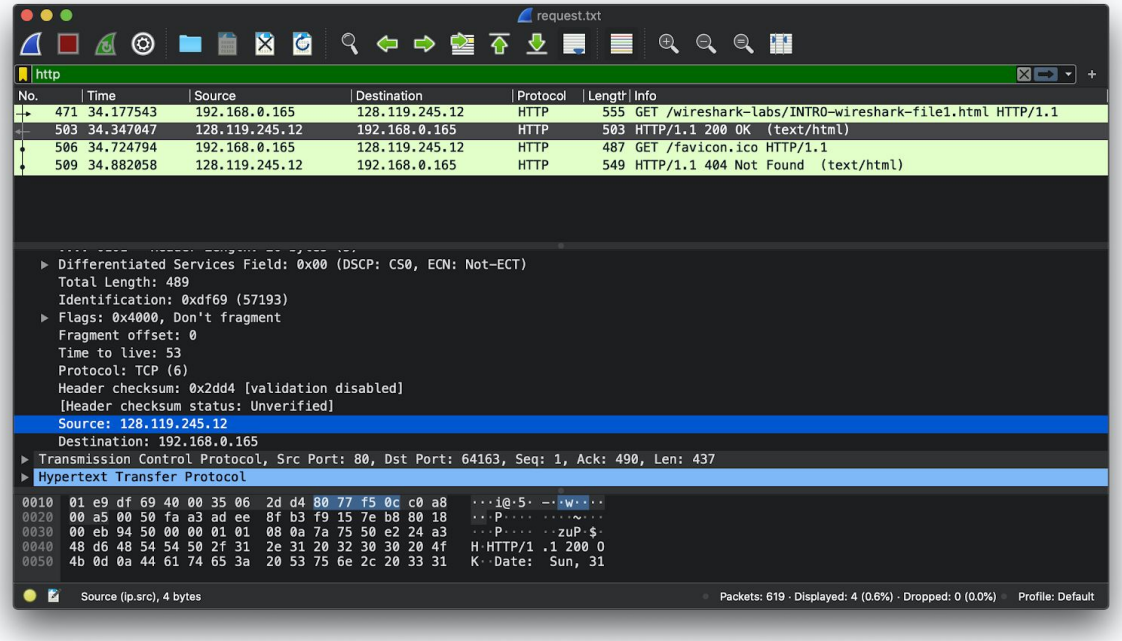

Рис. 7. Інформація про вихідні та цільові адреси пакетів із відповіддю

3.5. Яким був перший рядок запиту на рівні протоколу HTTP?

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

3.6. Яким був перший рядок відповіді на рівні протоколу HTTP?

HTTP/1.1 200 OK\r\n