МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Комп’ютерні інформаційні мережі**

**Лабораторна робота №8**

Виконала:

студентка групи ПМі-31

Харитонова Анастасія

Львів 2024

**Тема:** Аналіз ТСР-сегментів та UDP-датаграм засобами Wireshark

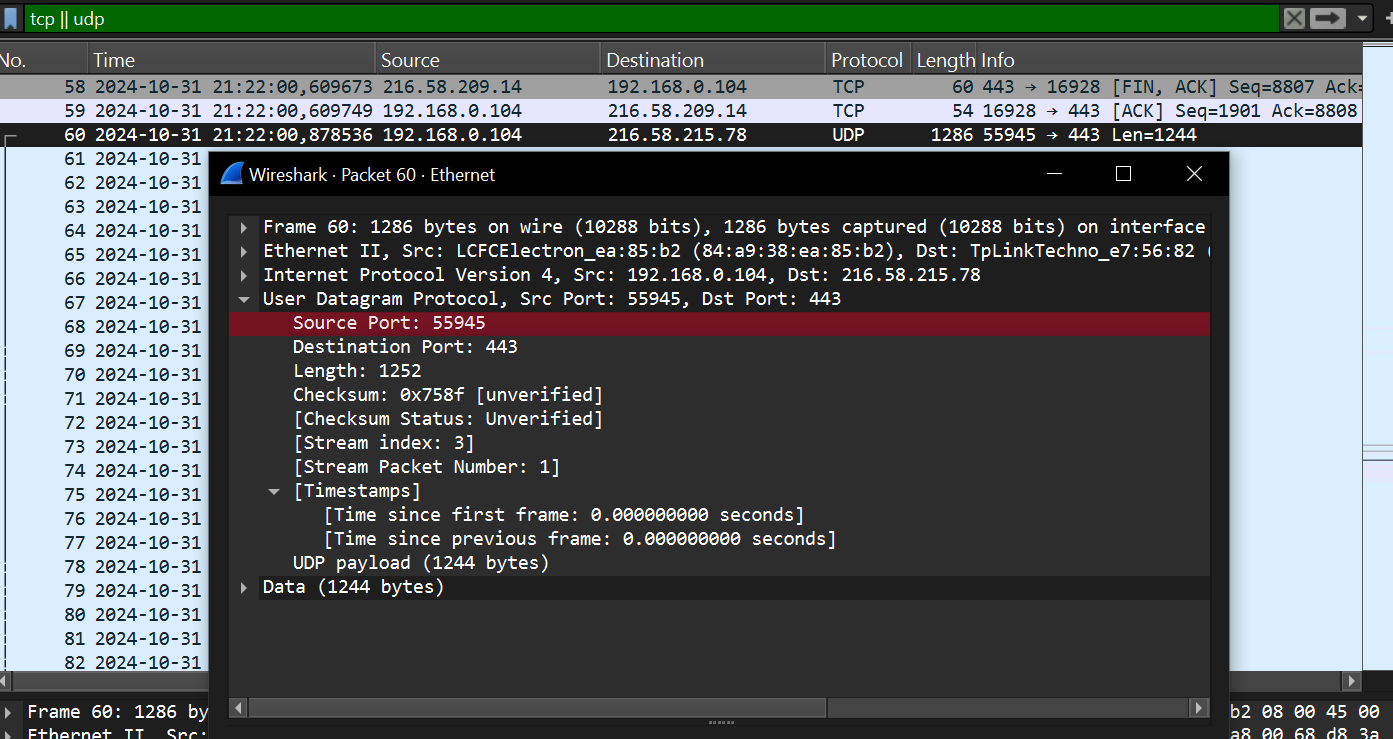
**Мета:** Здобути практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку ТСР/ІР.

**Хід роботи:**

1. Захопила пакети під час здійснення активності в браузері який працює за протоколом http.
2. Відфільтрувала пакети. DNS та HTTP відображаються тому, що:

-DNS зазвичай використовує порт UDP для передачі запитів (також може використовувати ТСР для обміну повідомленнями більше 512 байт).

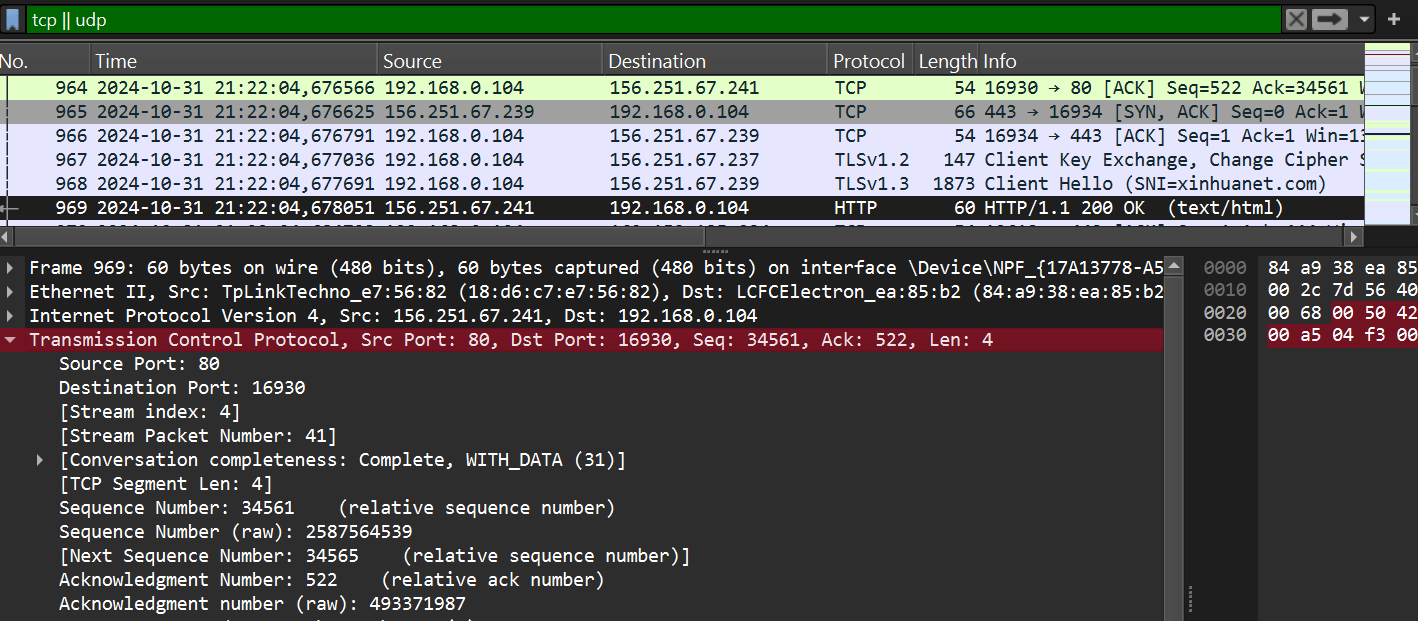
-HTTP повідомлення передаються через TCP з’єднання.



Порт відправника – 55945: динамічний порт, згенерований системою.

Порт одержувача – 443: закріплений за протоколом, порт для веб-браузерів.

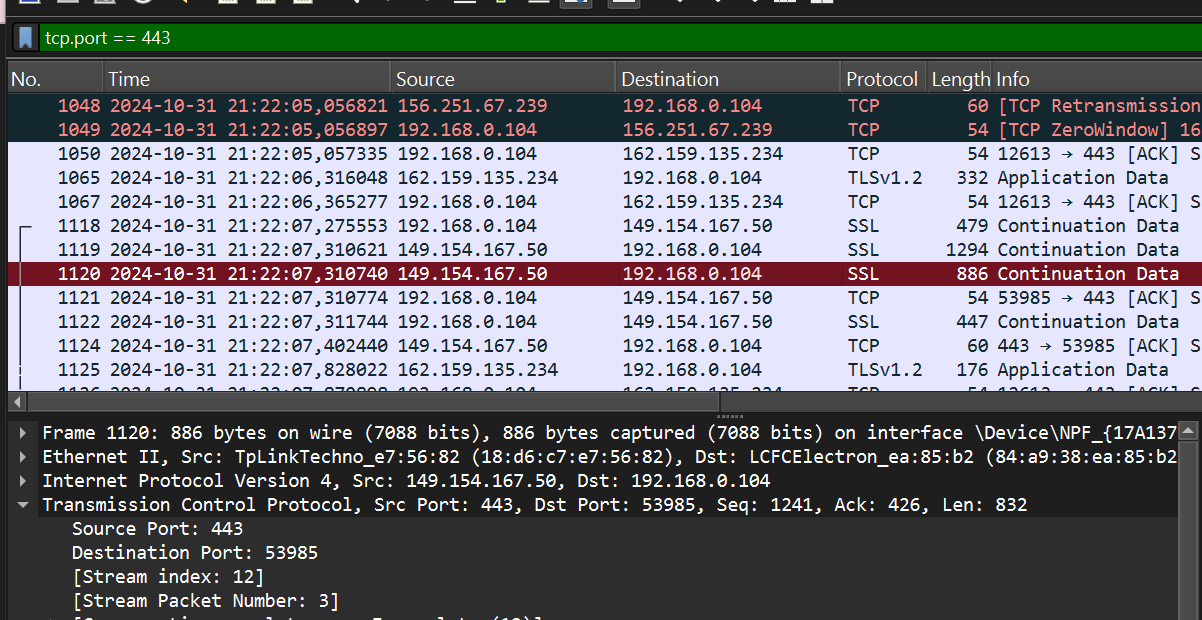
**4.**



Порт відправника – 80: закріплений (зв’язок між браузером і веб-сервером).

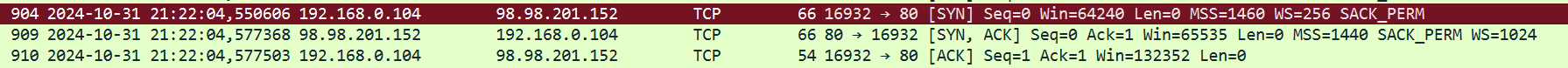
Порт одержувача – 16930: згенерований.

**5.** Відфільтрувала пакети (tcp.port==443)



TLS та SSL використовується для шифрування трафіку. Дозволяє розрізнити звичайний HTTP (який передається у відкритому вигляді), та HTTPS.

**6.** Знайшла послідовність пакетів процедури ‘потрійного рукостискання’.

****

**7.**

**-------------------------------------------------------------------------------------------------------**

**Source Port: 16932 –** порт відправника

**Destination Port: 80 –** порт призначення, на якому працює сервер.

**[Stream index: 6] –** 6 'розмова' (потік)

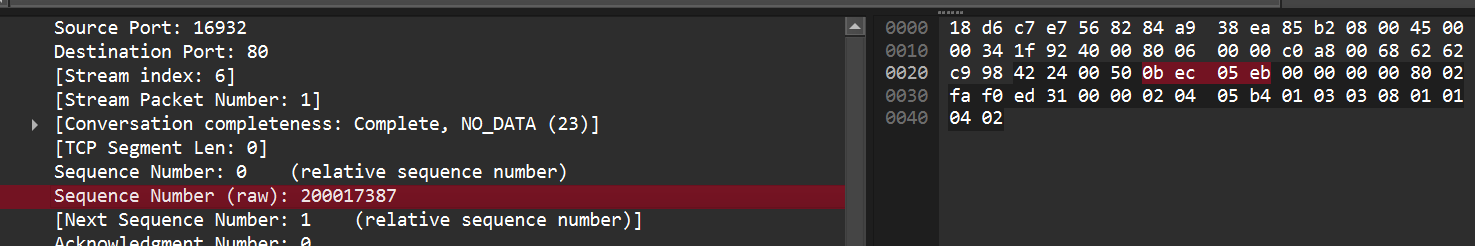
**[Stream Packet Number: 1] –** номер пакета у списку (1)

**[Conversation completeness: Complete, NO\_DATA (23)] -** потік завершено, і у ньому немає даних.

**[TCP Segment Len: 0] –** довжина сегмента ТСР, 0 байт, бо SYN призначений лише для встановлення з’єднання.

**Sequence Number: 0 (relative sequence number) –** відносний номер послідовності.

**Sequence Number (raw): 200017387 -** справжній номер, випадково згенерований протоколом ТСР під час ініціалізації з’єднання.



Число 200017387 записане в 16-му вигляді = b ec 05 eb (4 байти).

**[Next Sequence Number: 1 (relative sequence number)] –** наступний номер послідовності, який буде відправлений

**Acknowledgment Number: 0 / Acknowledgment number (raw): 0 –** в SYN пакеті завжди 0, бо не містить даних (клієнт не отримав жодних даних від сервера).

**Header Length: 32 bytes (8) –** загальна довжина заголовка ТСР у байтах

**Flags: 0x002 (SYN) –** прапор SYN, вказує на початок процесу встановлення з’єднання.

**Window: 64240 –** максимальний розмір вікна, який клієнт пропонує для цього з’єднання

**Checksum: 0xed31 [unverified] –** контрольна сума, яку використано для перевірки цілісності сегменту. Статус **unverified** означає що сума не перевірено.

**Urgent Pointer: 0 –** використовується для вказівки пріоритетних даних.

**Options: (12 bytes)** – додаткові опції, розмір 12 байт. **Maximum segment size** максимальний розмір сегмента**, No-Operation (NOP) –** для вирівнювання розміру заголовка, щоб зробити його кратним 4, **Window scale –** дозволяє збільшити розмір віка, для підтримки високошвидкісних з’єднань, **SACK permitted –** дозволяє використовувати вибіркове підтвердження. (ретрансляція лише втрачених даних).

**-------------------------------------------------------------------------------------------------------**

**Source Port: 80 –** порт відправника (сервера).

**Destination Port: 16932 –** порт одержувача (клієнта).

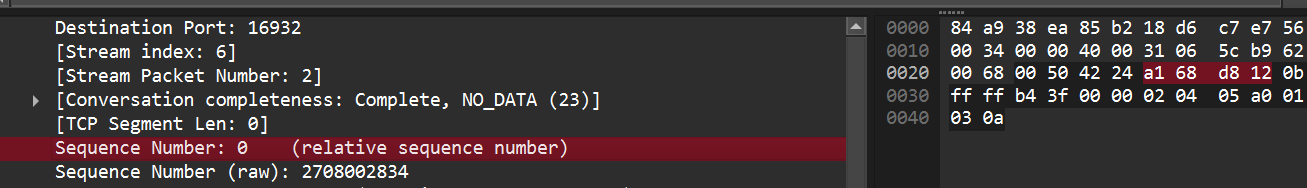
**[Stream index: 6] –** індекс потоку.

**[Stream Packet Number: 2] –** порядковий номер пакета (2).

**[Conversation completeness: Complete, NO\_DATA (23)] –** означає, що цей потік завершено, і у ньому немає даних

**Sequence Number: 0 (relative sequence number) –** відносний номер.

**Sequence Number (raw): 2708002834 –** справжній номер (4 байти).



**[Next Sequence Number: 1 (relative sequence number)] –** наступний номер послідовності

**Acknowledgment Number: 1 (relative ack number) –** відносний номер підтвердження (тут підтвердження першого байтаБ надісланого клієнтом).

**Acknowledgment number (raw): 200017388 –** справжнє значення номера підтвердження.

**Header Length: 32 bytes (8) –** довжина заголовка (32 байти, 8 32-бітних слів).

**Flags: 0x012 (SYN, ACK) –** SYN – для початку нового з’єднання між клієнтом і сервером.

ACK – для підтвердження отримання.

**Window: 65535 –** розмір вікна.

**Checksum: 0xb43f [unverified] –** контрольна сума для перевірки цілісності.

**Urgent Pointer: 0 –** для вказівки пріоритетних даних.

**[Timestamps] –** додає часові мітки, які використовуються для вимірювання затримки між пакетом і підтвердженням.

**[SEQ/ACK analysis] –** аналіз номерів послідовності та підтверджень (відстеження правильності порядку передачі та підтверджень пакетів у потоці).

**---‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑‑-------------------------**

**Source Port: 16932 –** порт відправника

**Destination Port: 80 –** порт призначення, на якому працює сервер.

**[Stream index: 6] –** 6 'розмова' (потік)

**[Stream Packet Number: 1] –** номер пакета у списку (3).

**[Conversation completeness: Complete, NO\_DATA (23)]**

**[TCP Segment Len: 0]**

**Sequence Number: 1 (relative sequence number) –** номер першого байта сегменту в потоці.

**Sequence Number (raw): 200017388 –** справжнє значення.

**[Next Sequence Number: 1 (relative sequence number)]**

**Acknowledgment Number: 1 (relative ack number) –** відносний номер підтвердження (1 означає підтвердження отримання SYN пакета).

**Acknowledgment number (raw): 2708002835 –** справжнє значення номера підтвердження.

**Header Length: 20 bytes (5) –** довжина заголовка (20 байт).

**Flags: 0x010 (ACK) –** прапорець підтверджує отримання SYN-АСК пакета від сервера.

**Window: 517 –** позначає максимальну кількість байтів, яку клієнт готовий прийняти.

**[Calculated window size: 132352] –** обрахований розмір вікна (517\*256)

**[Window size scaling factor: 256] –** коефіцієнт масштабування вікна, дозволяє підтримувати більшу пропускну здатність.

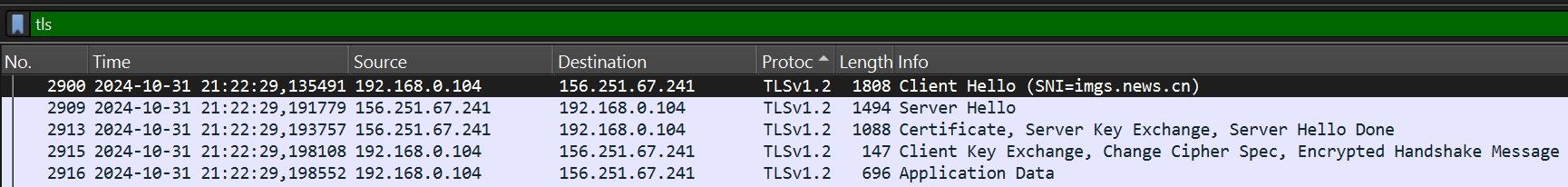
**Checksum: 0xed25 [unverified] -** контрольна сума для перевірки цілісності.

**Urgent Pointer: 0 –** для вказівки пріоритетних даних.

**[Timestamps] –** додає часові мітки, які використовуються для вимірювання затримки між пакетом і підтвердженням.

**[SEQ/ACK analysis] –** аналіз номерів послідовності та підтверджень (відстеження правильності порядку передачі та підтверджень пакетів у потоці).

**8 – 9.**  Відфільтрувала пакети, використовуючи фільтр tls, знайшла пакети, які стосуються пакетів TLS-рукостискання.

****

**Client Hello –** клієнт ініціює ‘рукостискання’ (надсилає повідомлення **‘Hello’**). В повідомленні вказано версію TLS, яку підтримує клієнт, набори шифрів і рядок випадкових байтів (для генерації ключів шифрування).

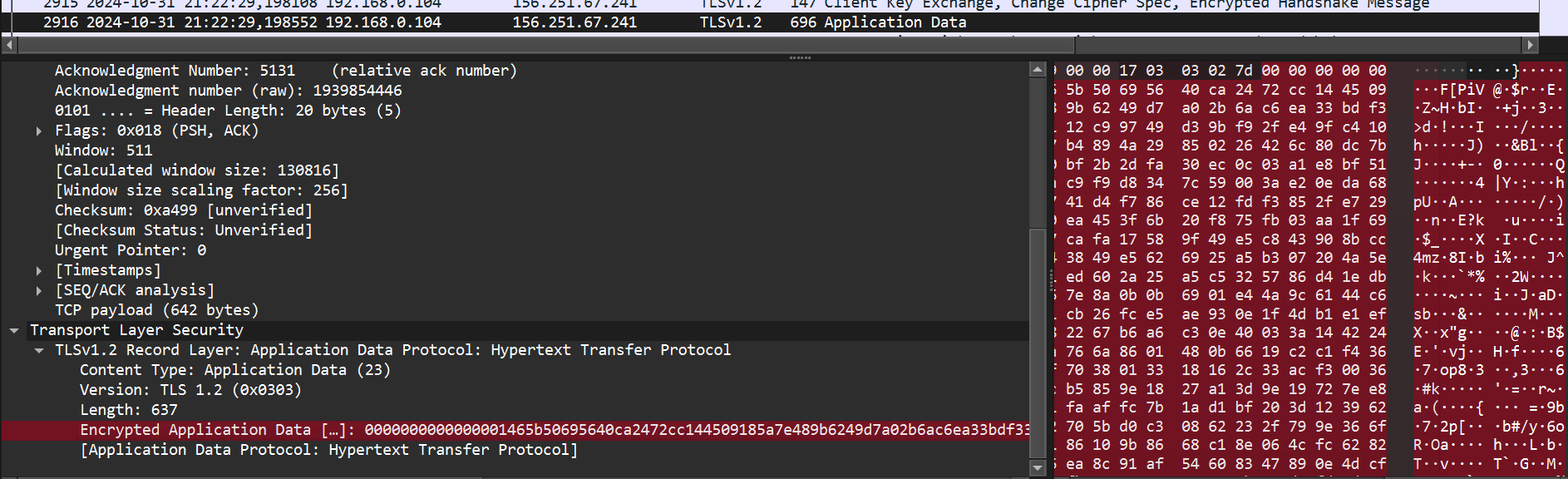
**Server Hello –** сервер відповідає, надсилає повідомлення в якому – вибраний набір шифрів, рядок випадкових байтів, згенерованих сервером і SSL сертифікат.

**Certificate -** сертифікат**, Server Key Exchange –** додаткові дані для обміну ключами (якщо алгоритм вимагає)**, Server Hello Done –** сигналізує, що рукостискання завершене.

**Client Key exchange –** клієнт надсилає пакет з даними, необхідними для обміну ключами**, Change Cypher Spec –** клієнт надсилає, щоб вказати що всі дані будуть зашифровані вибраним набором шифрів**, Encrypted Handshake message –** підтвердження завершення рукостискання з боку клієнта.

**Application Data –** обмін даними.

**10.**

****

Видно, що дані зашифровані.

**Висновок:** здобула практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку ТСР/ІР.