Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра програмування

Звіт

до лабораторної роботи №8

з теми

**“Аналіз ТСР-сегментів та UDP-датаграм засобами Wireshark”**

Підготував:

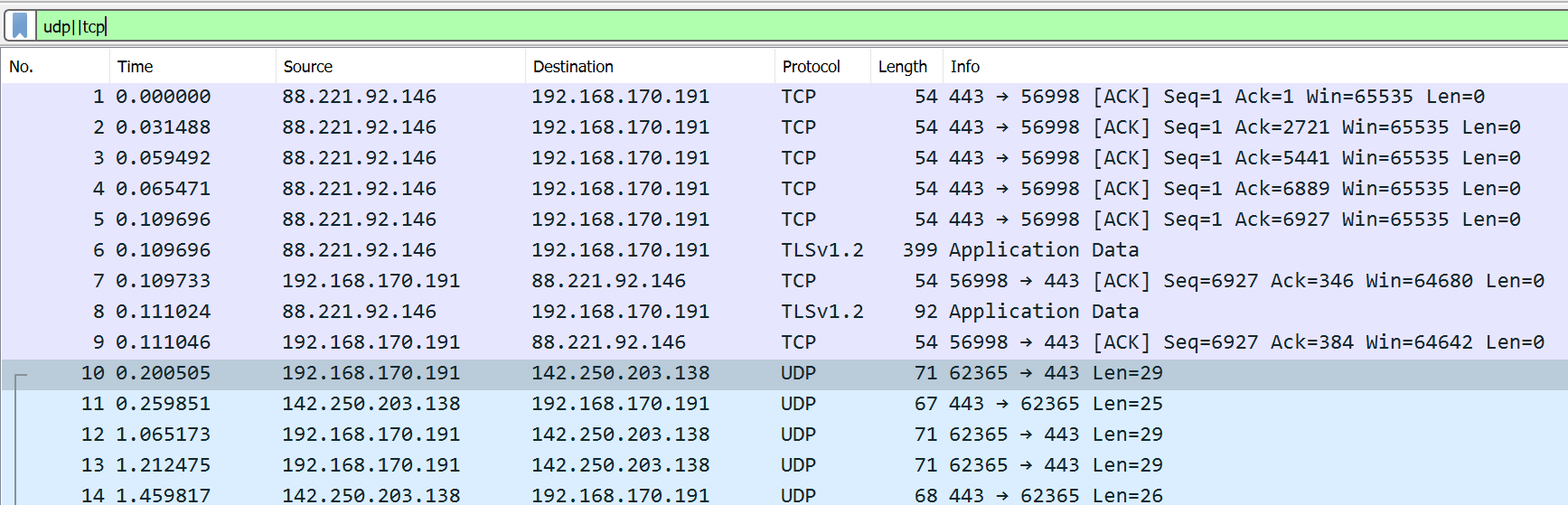
cтудент ПМІ-31

Процьків Назарій

Львів 2023

**Хід роботи**

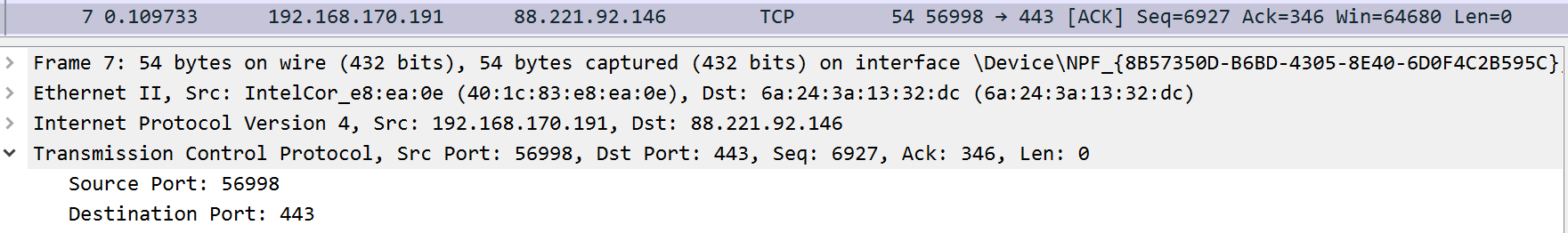
1. Захопив пакети відповідно до вказівок в описі лабораторної роботи.



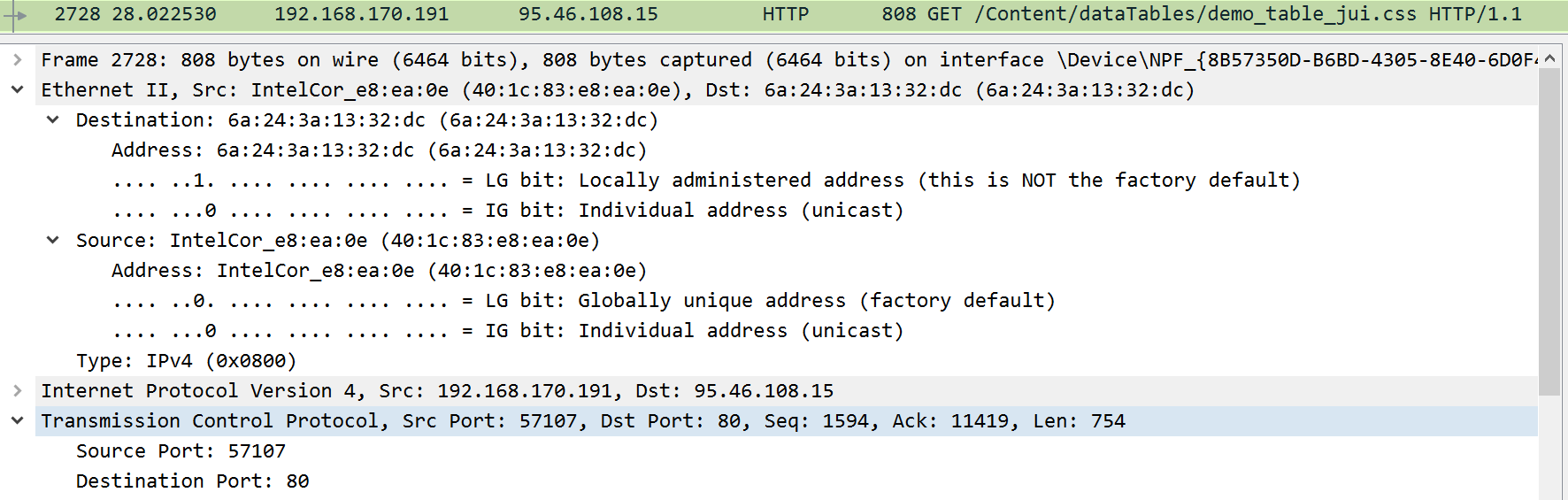
1. Протоколи HTTP функціонують на рівні застосунків та мають призначений порт, який може бути визначений стандартом або налаштований адміністратором мережі. Під час обміну даними між пристроями на різних мережевих вузлах інформація проходить через верхні рівні OSI-моделі та доходить до рівня зв'язку даними. Тут дані розбиваються на пакети, які передаються протоколу транспортного рівня, такому як TCP або UDP.

TCP, як протокол транспортного рівня, отримує ці пакети даних від протоколів верхнього рівня. Кожен пакет має визначений номер порту, що ідентифікує застосунок на приймачі. Таким чином, фільтруючи пакети за допомогою умови tcp || udp, можна відслідковувати передачу HTTP, оскільки цей протокол часто використовує TCP для обміну даними.

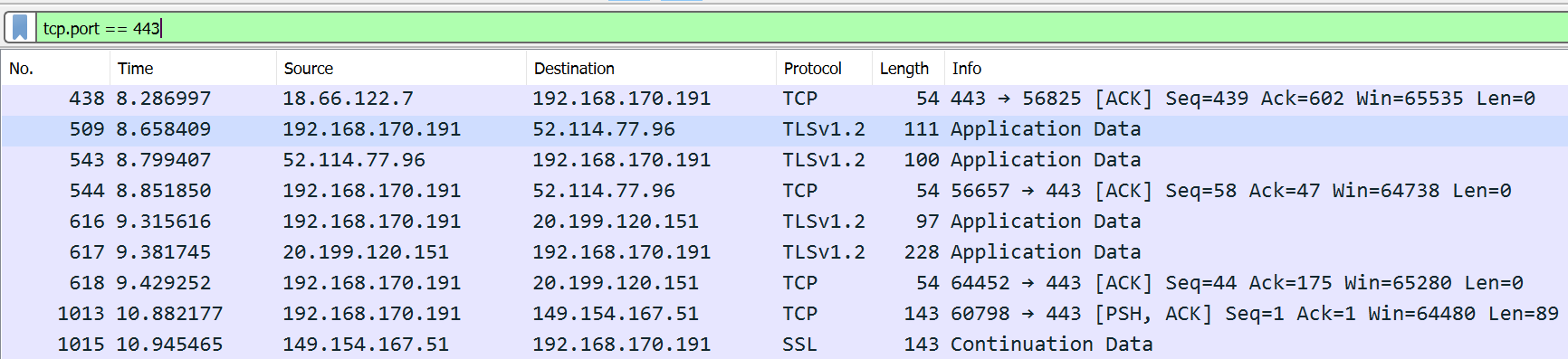
1. Порт 56998 є портом відправника, а порт 443 є портом отримувача. Порт отримувача – закріплений за протоколом, а порт відправника – згенерований автоматично.



1. Порт 57107 є портом відправника. Він згенерований джерелом. Порт 80 є портом отримувача, він зазвичай використовується для HTTP-запитів.



1. За допомогою фільтру знайшов пакети протоколу HTTPS. Пакети протоколу HTTPS в Wireshark відображаються через протоколи транспортного та криптографічного рівнів.
   1. TCP (Transmission Control Protocol): HTTPS використовує TCP для передачі зашифрованих даних.
   2. TLS (Transport Layer Security) або SSL (Secure Sockets Layer): Транспортний рівень, який забезпечує шифрування та забезпечення конфіденційності та цілісності даних. В залежності від версії протоколу може бути позначено як "TLS" або "SSL".



1. Знайшов послідовність пакетів процедури “потрійного рукостискання”.



1. Порти:
   1. Джерело – 59313
   2. Призначення – 80

Прапорці:

* 1. SYN: Встановлено (1), вказує на початок з’єднання

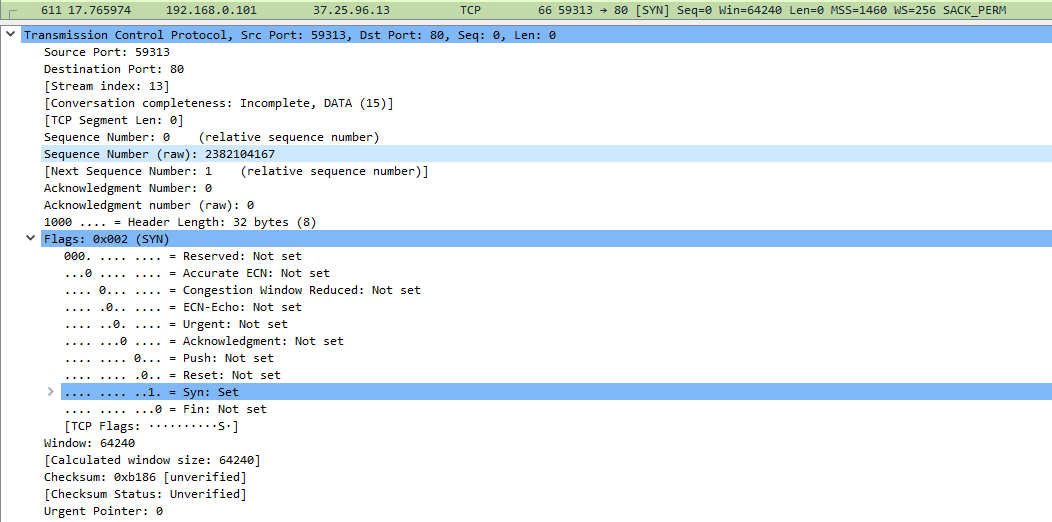
Порядковий номер послідовності: 2382104167(8dfc0667)

Вікно: Вказує кількість байтів, яку відправник може передати, не очікуючи підтвердження - 64240.

TCP Options:

1. Maximum Segment Size: Максимальний розмір сегмента, який відправник може приймати. У цьому випадку, MSS = 1460 байтів.
2. Window Scale: Вказує на масштабування вікна. У цьому випадку, Window Scale = 8.
3. SACK Permitted: Вказує, що опція Selective Acknowledgment (SACK) дозволена.

Timestamps: Ця опція використовується для визначення часу, коли був створений пакет. У цьому випадку, відміток часу не показано.



1. Порти:
   1. Джерело – 80
   2. Призначення – 59313

Порядковий номер послідовності для цього пакету: 2184071592(822e49a8).

Порядковий номер підтвердження для цього пакету, який вказує на наступний очікуваний байт в послідовності даних від відправника: 2382104168(8dfc0667).  
Прапорці:

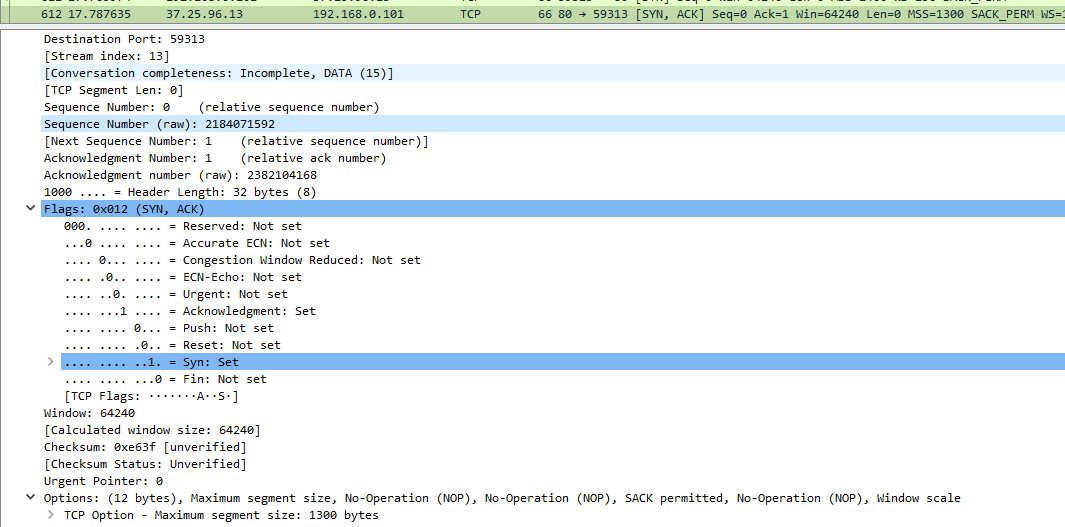
1. SYN, ACK: Вказує, що цей пакет одночасно (SYN) встановлює з'єднання і підтверджує (ACK) отримання першого пакету.

Вікно: Вказує кількість байтів, яку відправник може передати, не очікуючи підтвердження і дорівнює 64240.

TCP Options:

1. Maximum Segment Size: Максимальний розмір сегмента, який відправник може приймати. У цьому випадку, MSS = 1300 байтів.
2. Window Scale: Вказує на масштабування вікна. У цьому випадку, Window Scale = 7.
3. SACK Permitted: Вказує, що опція Selective Acknowledgment (SACK) дозволена.

Timestamps: Ця опція використовується для визначення часу, коли був створений пакет. У цьому випадку, відміток часу не показано.



1. Порти:
   1. Джерело – 59313
   2. Призначення – 80

Порядковий номер послідовності для цього пакету: 2382104168.

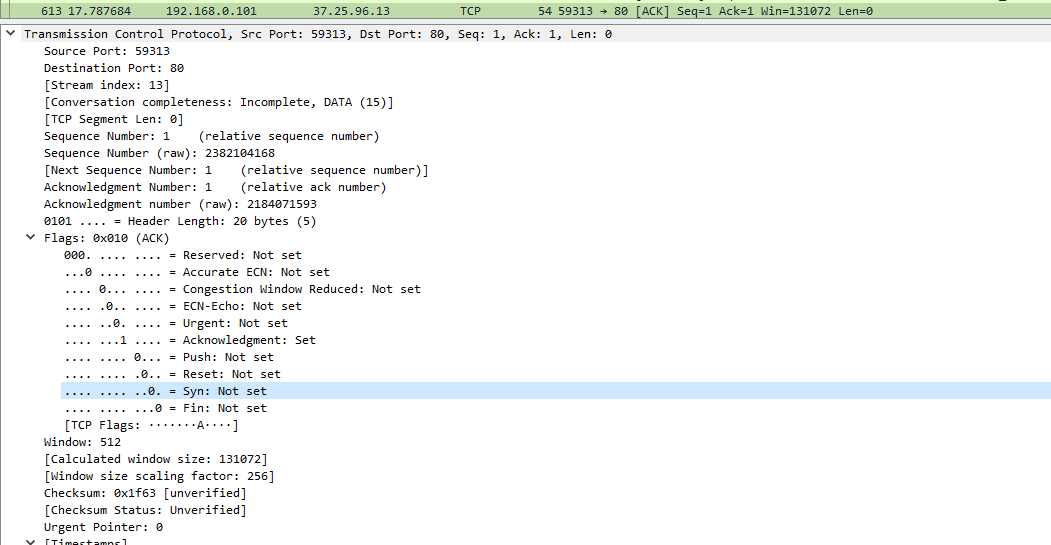
Порядковий номер підтвердження для цього пакету: 2184071593.  
Прапорці:

1. ACK: Вказує, що цей пакет є підтвердженням. ACK встановлено.

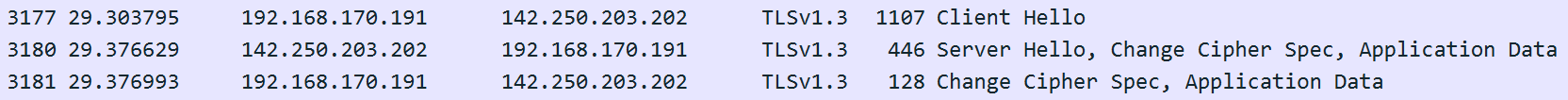
Вікно: Вказує кількість байтів, яку відправник може передати, не очікуючи підтвердження і дорівнює 512.

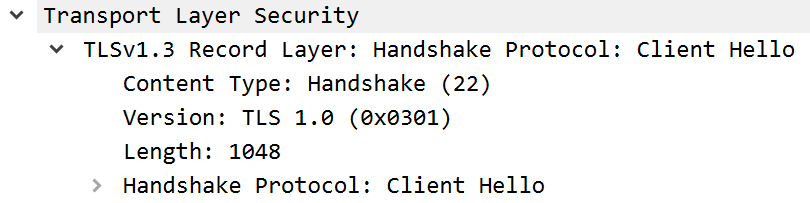
Контрольна сума: Контрольна сума для валідації цілісності пакету.

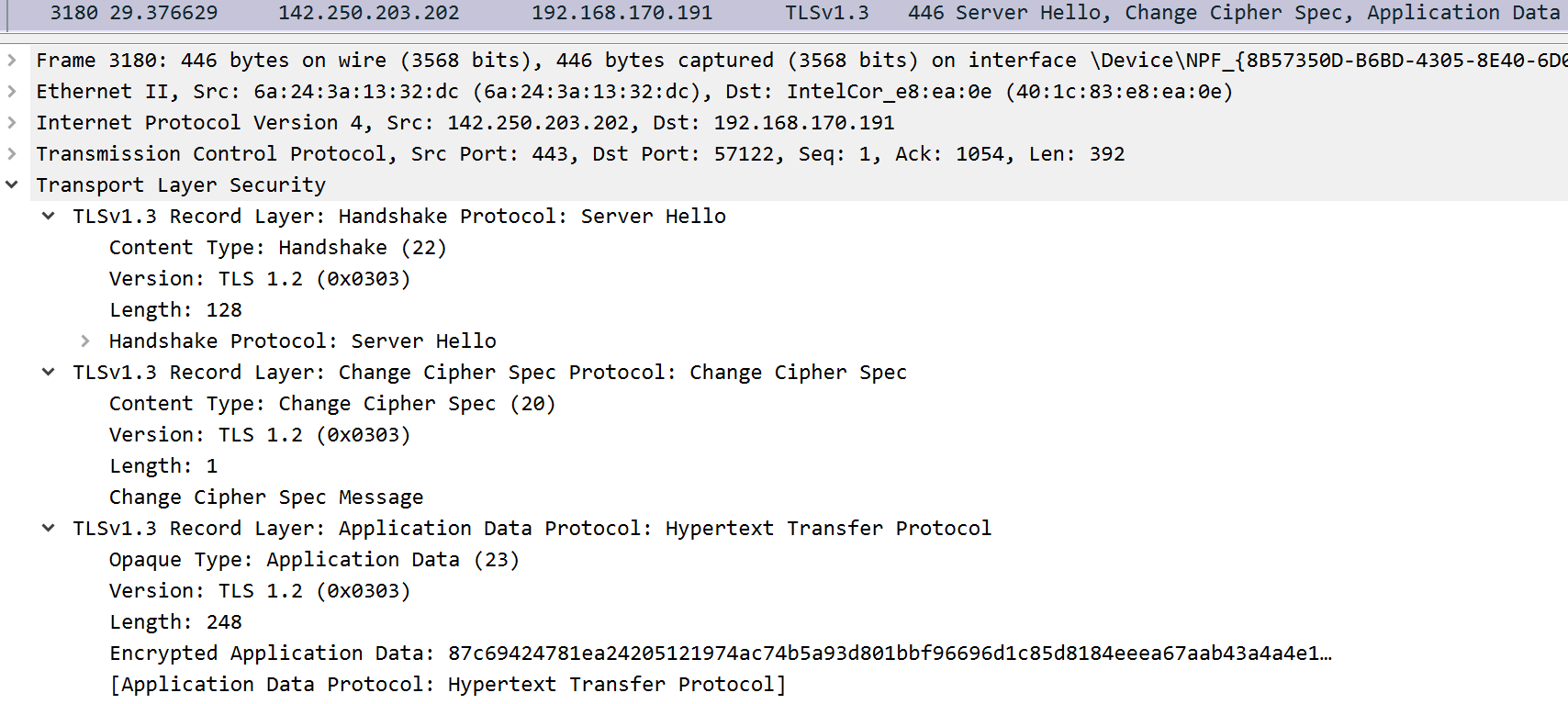
Timestamps: Ця опція використовується для визначення часу, коли був створений пакет. У цьому випадку, відміток часу не показано.

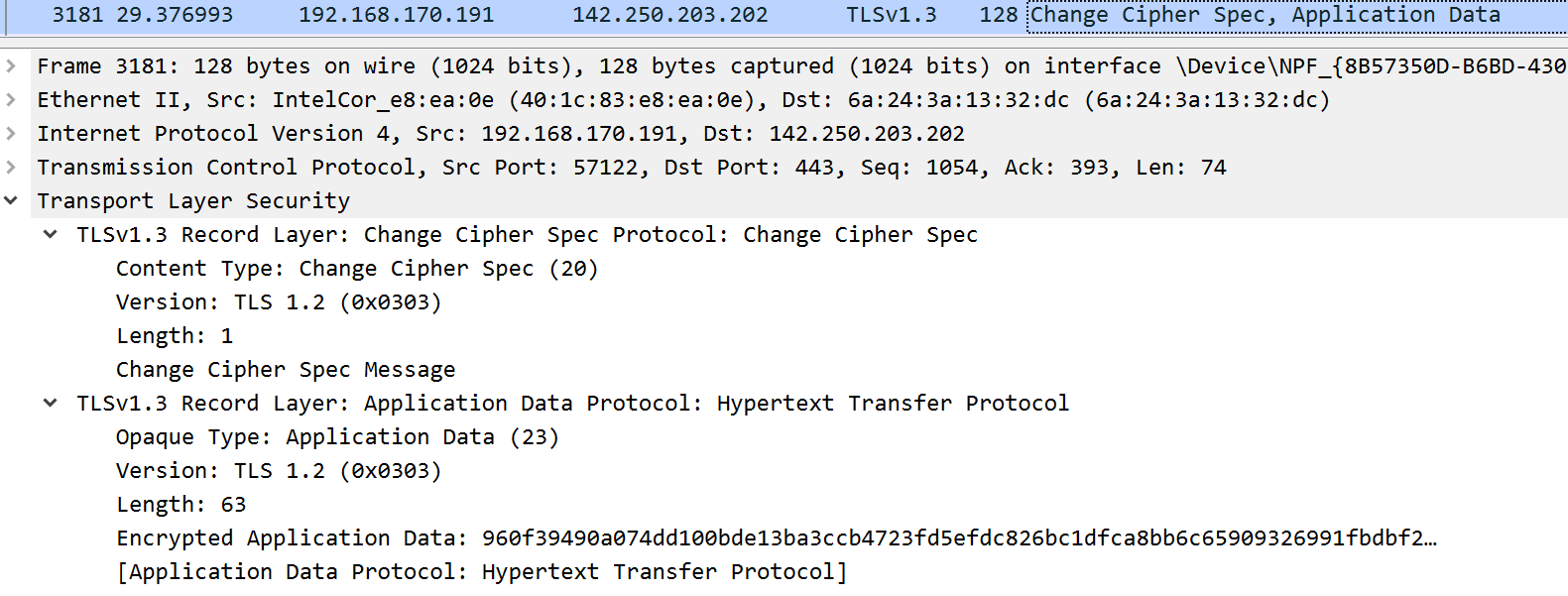


1. Відшукав пакети, які стосуються TLS-рукостискань







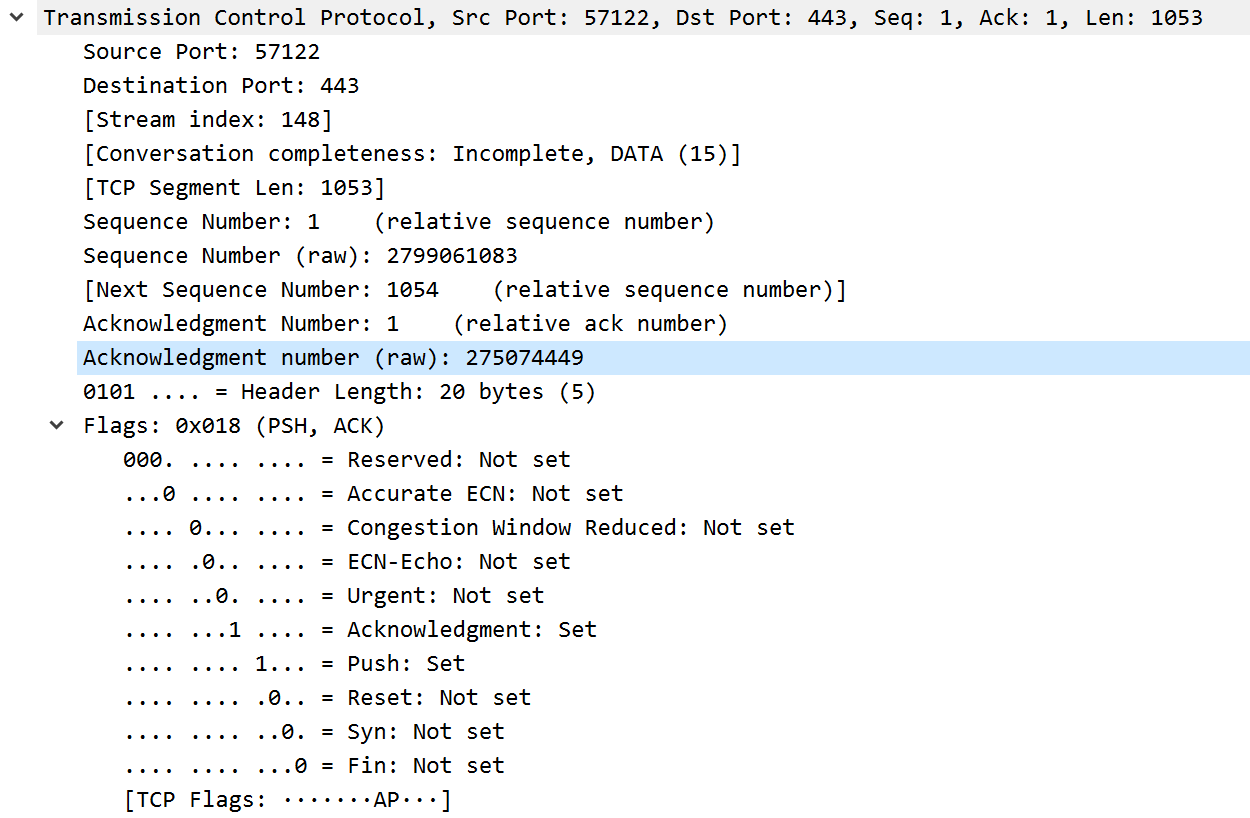


1. Порти:
   1. Джерело – 57122
   2. Призначення – 443

Порядковий номер послідовності для цього пакету: 2799061083.

Порядковий номер підтвердження для цього пакету: 275074449.  
Прапорці:

1. ACK: Вказує, що цей пакет є підтвердженням. ACK встановлено.

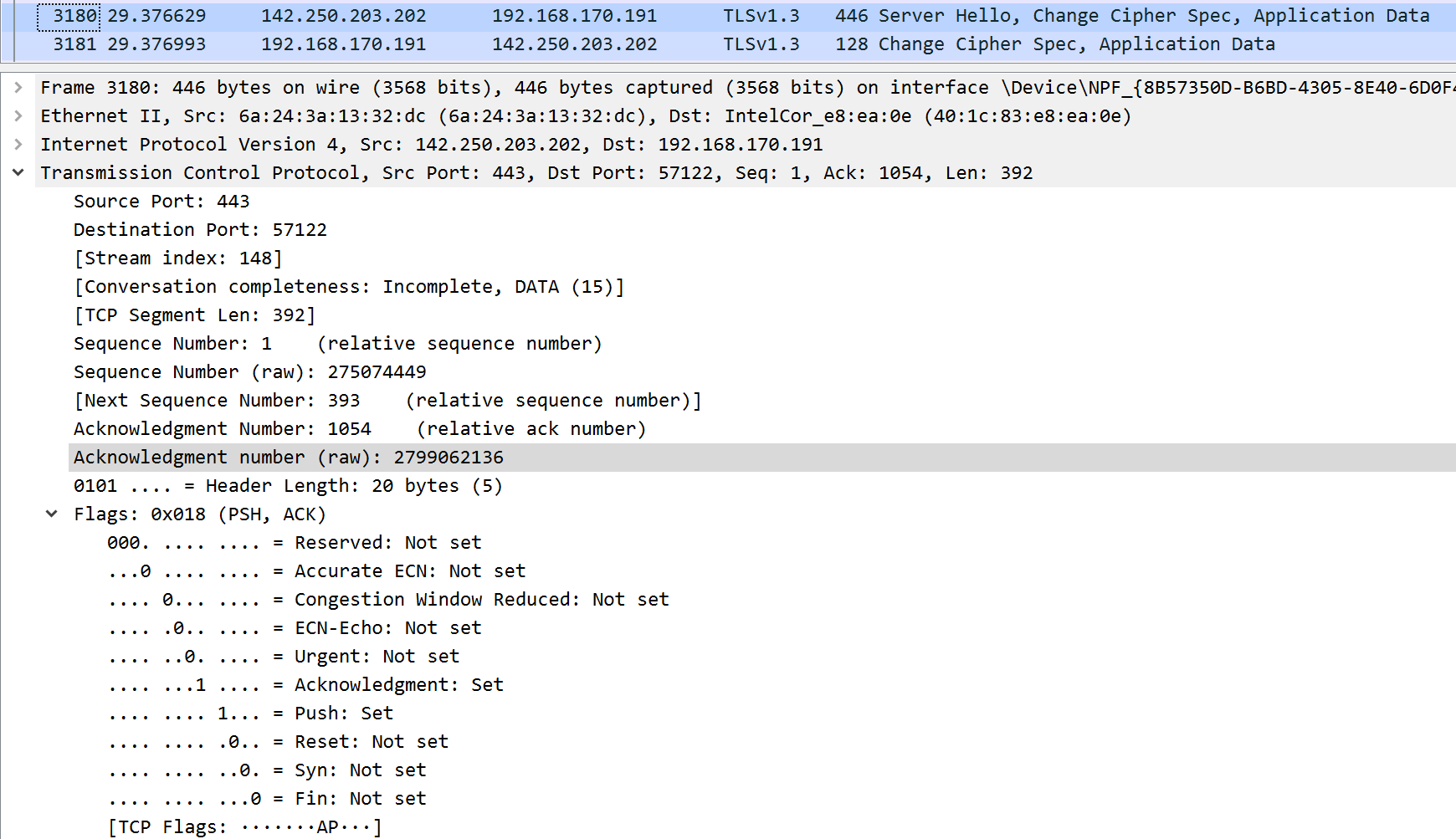


1. Порти:
   1. Джерело – 443
   2. Призначення – 57122

Порядковий номер послідовності для цього пакету: 275074449.

Порядковий номер підтвердження для цього пакету: 2799062136.  
Прапорці:

1. Прапорець Push вказує на те, що дані, які включаються в цей пакет, повинні бути передані вищому рівню без очікування підтвердження (ACK) від отримувача.
2. ACK: Вказує, що цей пакет є підтвердженням. ACK встановлено.



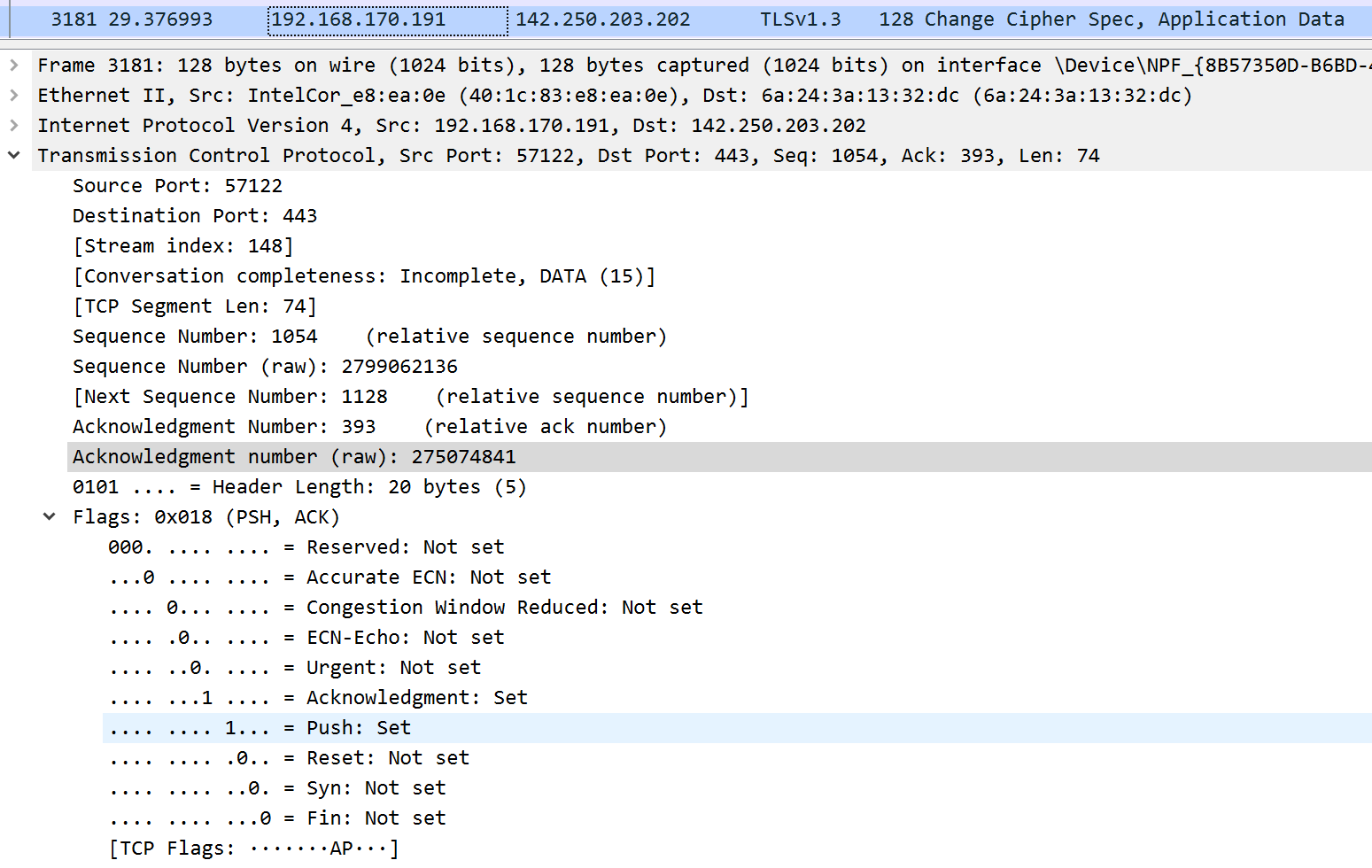
1. Порти:
   1. Джерело – 57122
   2. Призначення – 443

Порядковий номер послідовності: 2799062136.

Порядковий номер підтвердження: 275074841.

Прапорці:

* 1. Прапорець Push вказує на те, що дані, які включаються в цей пакет, повинні бути передані вищому рівню без очікування підтвердження (ACK) від отримувача.
  2. ACK: Вказує, що цей пакет є підтвердженням. ACK встановлено.



1. Побачив, що дані зашифровані.

