Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра дискретного аналізу

**Комп’ютерні інформаційні мережі**

**Лабораторна робота №8**

Виконав:

Студент групи ПМі-33

Тимчишин Ярема

Прийняв:

Ас. Жировецький В.В.

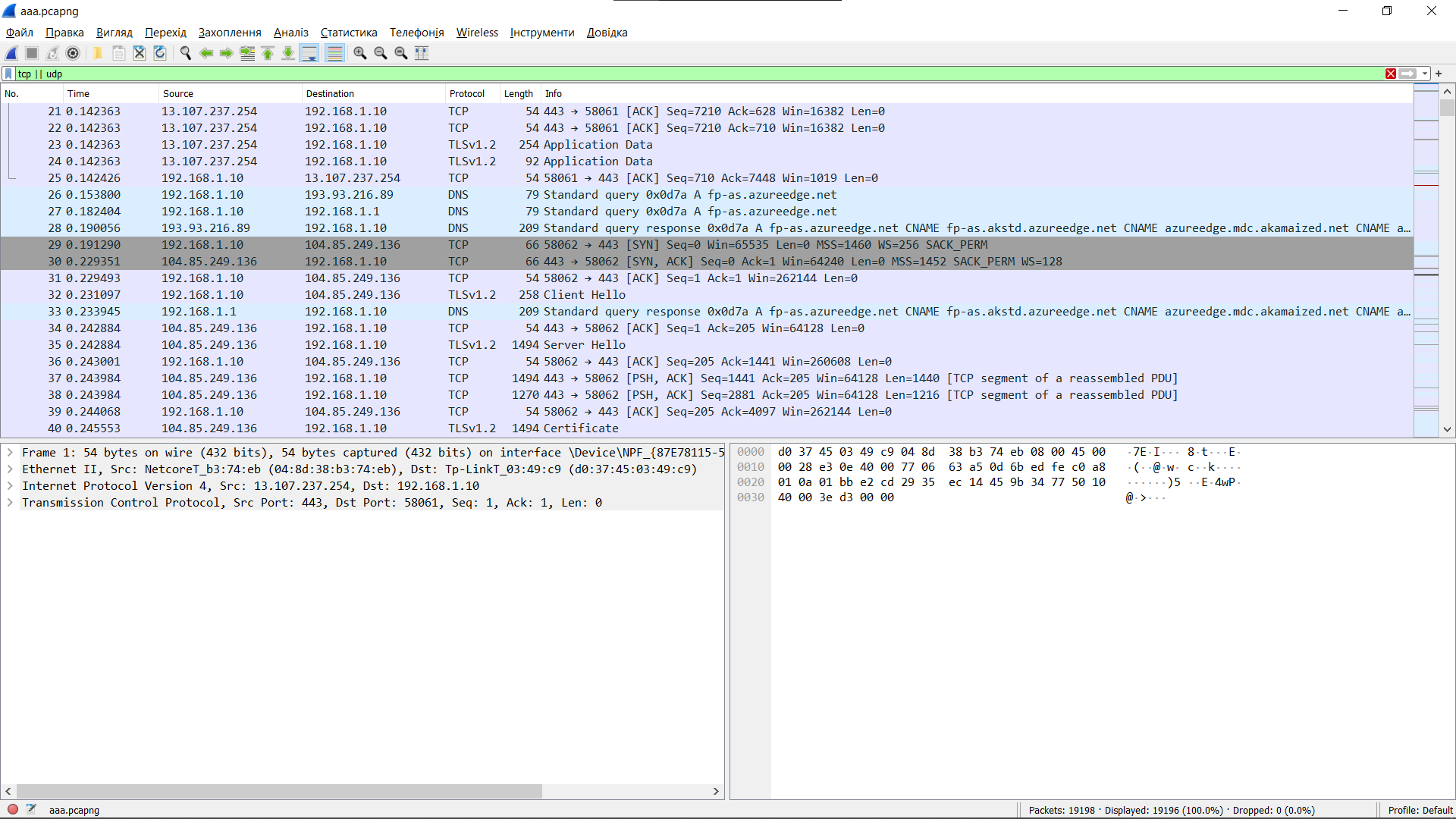
Львів 2023

**Тема:** Wireshark (Transport Layer).

**Мета роботи:** Здобути практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку TCP/IP.

**Хід роботи**

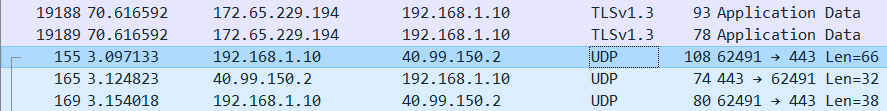
1. Використовуючи Wireshark, захопив пакети, здійснюючи активність в браузері, серед якої перейшов на сайт, який працює за протоколом http, а також завантажив файл розміром 5.7 мегабайт.
2. Встановив фільтр tcp || udp.



Пояснив чому крім вказаних протоколів (ТСР та UDP) відображаються і інші, наприклад, DNS і HTTP.

* HTTP та DNS - це протоколи, які використовують TCP або UDP для передачі даних, тому вони також можуть відображатися з фільтром tcp || udp. Тому що цей фільтр включає всі транспортні протоколи, але не обов'язково фільтрує пакети на рівні протоколів прикладного рівня, таких як HTTP або DNS.

1. Вибрав пакет, який використовує протокол UDP.



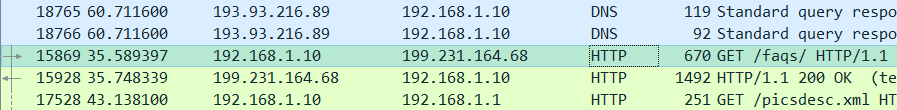
Вказав порти відправника та одержувача.



Дав відповідь на питання “Який з цих портів згенерований автоматично операційною системою, а який закріплений за протоколом?”.

* У моєму випадку, порт відправника (62491) генерується автоматично операційною системою. Коли клієнт (в даному випадку, це мій комп'ютер) ініціює з'єднання, то операційна система вибирає порт автоматично. Тоді як порт одержувача (443) є закріплений за конкретним протоколом.

1. Вибрав пакет, який використовує протокол HTTP.



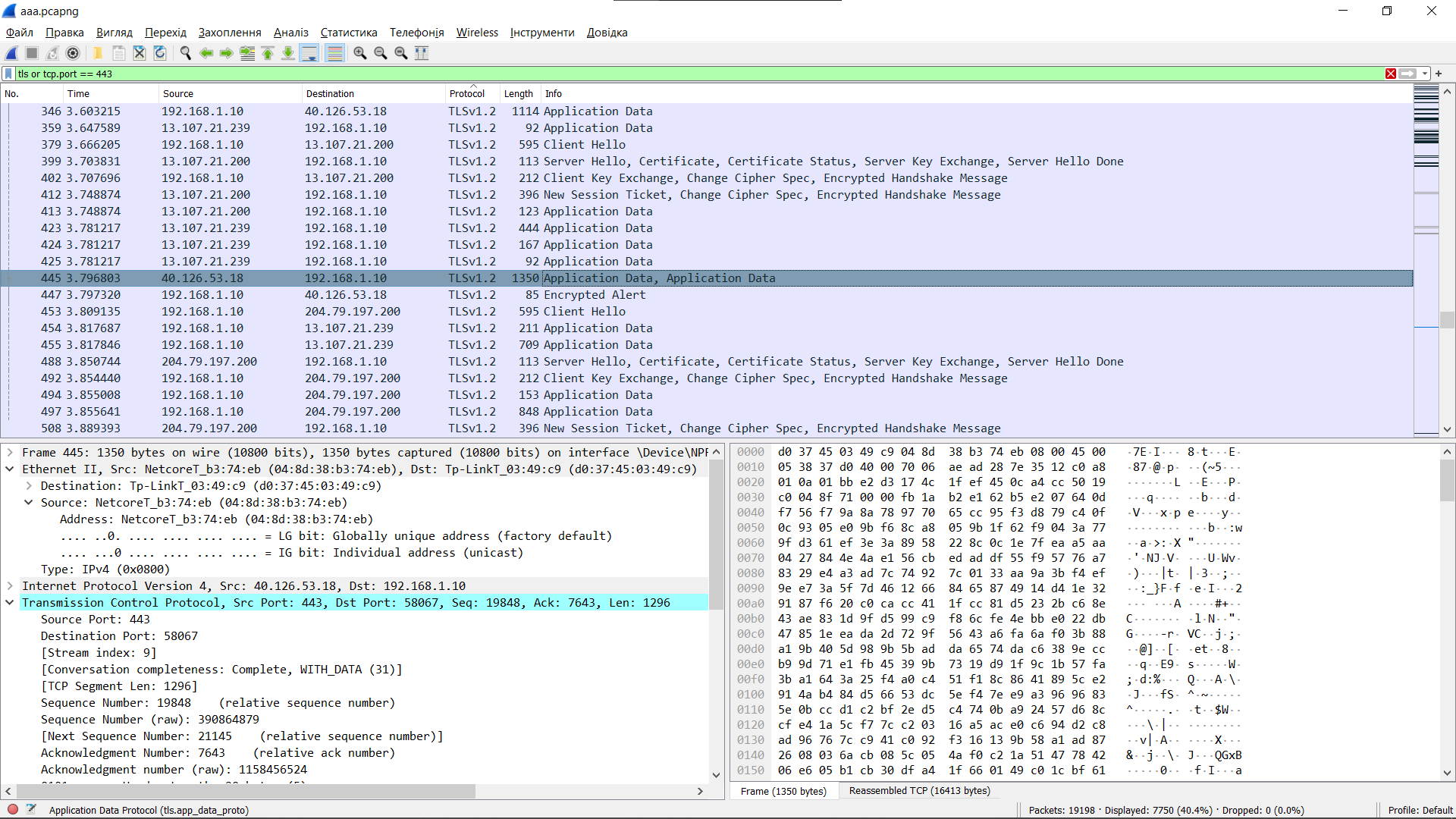
Вказав порти відправника та одержувача.



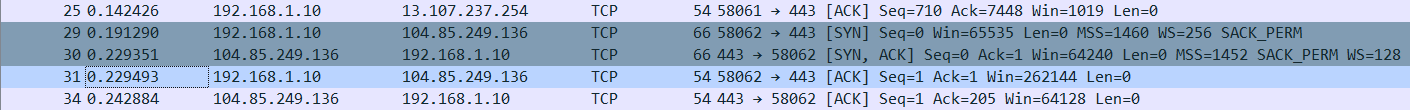
Дав відповідь на питання “Який з цих портів згенерований автоматично операційною системою, а який закріплений за протоколом?”.

* У моєму випадку, порт відправника (58201) був вибраний операційною системою, а порт одержувача (80) є стандартним портом для протоколу HTTP без шифрування (незашифрованого з'єднання).

1. Знаючи закріплений за НTTPS порт (443), знайшов пакети цього протоколу. Wireshark відображає цей протокол в стовпці “Протокол” як пакет “TLS”. Це пов'язано з тим, що HTTPS використовує TLS для забезпечення шифрування даних.



1. Відшукав послідовність пакетів процедури “потрійного рукостискання”.



1. Описав вміст кожного сегменту з попереднього пункту (порти, прапорці, номери послідовностей).

* Пакет 29:
  + Порт відправника: 58062
  + Порт одержувача: 443
  + Прапорці: [SYN]
  + Номер послідовності (Seq): 0
* Пакет 30:
  + Порт відправника: 443
  + Порт одержувача: 58062
  + Прапорці: [SYN, ACK]
  + Номер послідовності (Seq): 0
  + Номер підтвердження (Ack): 1
* Пакет 31:
  + Порт відправника: 58062
  + Порт одержувача: 443
  + Прапорці: [ACK]
  + Номер послідовності (Seq): 1
  + Номер підтвердження (Ack): 1

Користуючись нижнім полем побітового представлення, вказав справжнє десяткове значення номерів послідовності та пояснив, звідки беруться ці значення.

* Пакет 29:



* Пакет 30:





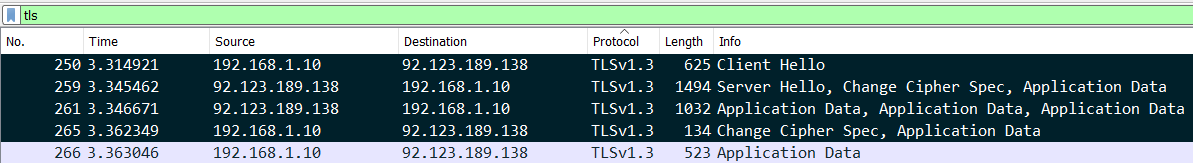
* Пакет 31:





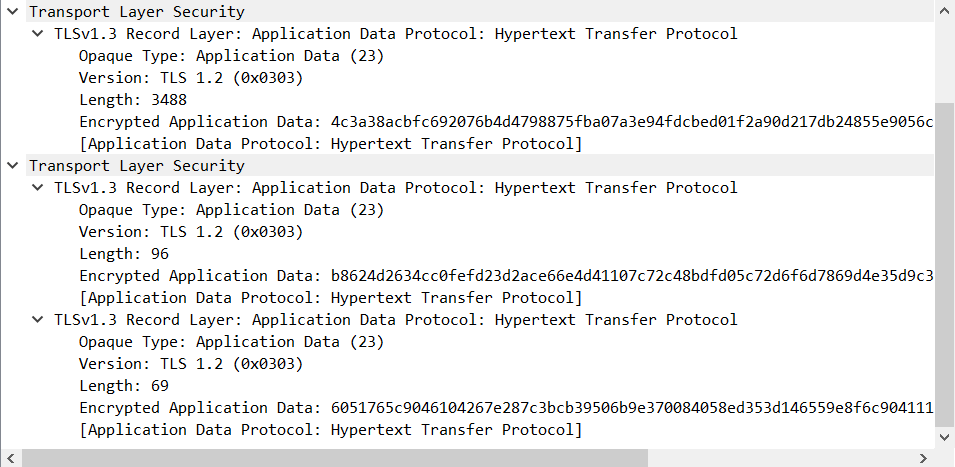
Справжні десяткові значення номерів послідовності в TCP визначаються самим протоколом і представляють собою порядкові номери байтів в потоці даних. Ці номери визначають, які саме байти у потоці даних є предметом обміну між сторонами. Кожен новий пакет починається з номера, який вказує на перший байт даних в даному пакеті. Під час передачі даних цей номер збільшується, і номер підтвердження вказує на номер байту, який очікується від іншої сторони.

1. Використовуючи фільтр tls, отримав пакети криптографічного протоколу TLS.
2. Відшукав пакети, які стосуються процедури TLS-рукостискання та описав їх.



* Пакет 250: Клієнт ініціює рукостискання, відправляючи "Client Hello" серверу.
* Пакет 259: Сервер відповідає "Server Hello", вводить "Change Cipher Spec", що означає початок застосування нових параметрів шифрування і починає передачу "Application Data".
* Пакет 261: Сервер продовжує відправляти "Application Data".
* Пакет 265: Клієнт відповідає "Change Cipher Spec", підтверджуючи зміни в шифруванні, і починає відправляти свої дані "Application Data".

1. Вибравши пакет з даними, переконався, що вони зашифровані:



**Висновок:** Під час виконання цієї лабораторної роботи, я здобув практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку TCP/IP.