ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп’ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №8

Аналіз ТСР-сегментів та UDP-датаграм засобами Wireshark

Виконав:

Студент групи ПМі-31

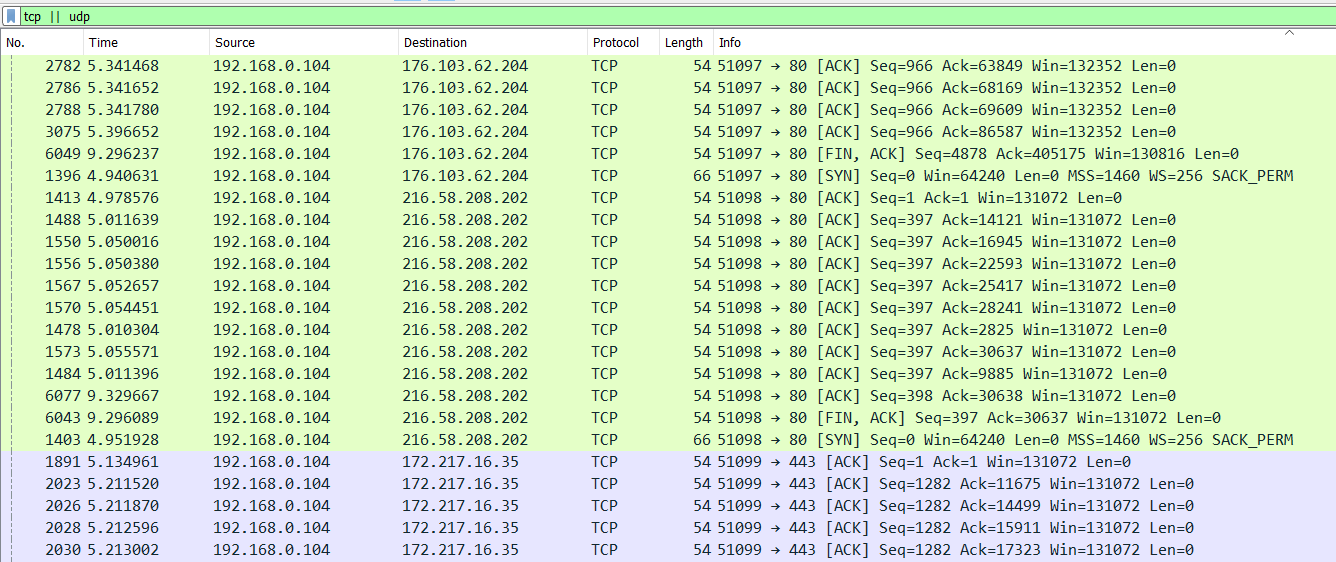
Яцуляк Андрій

2023

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

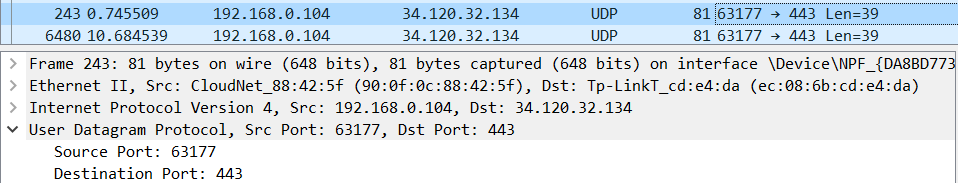
**Хід роботи**

1. Опрацював теоретичний матеріал.
2. Використовуючи Wireshark, почав захоплення пакетів. Здійснив активність в браузері, зокрема на сайтах, що працюють за протоколом http, завантажив файл.
3. Зупинив захоплення пакетів. Встановив фільтр tcp || udp:



Фільтр tcp || udp фільтрує пакети на основі вказаних критеріїв, але не виключає пакети, що містять протоколи вищого рівня, інкапсульовані в TCP або UDP. Іншими словами, фільтр tcp || udp захоплює пакети TCP або UDP, але не відфільтровує пакети, які мають TCP або UDP як транспортні протоколи, а також містять протоколи вищого рівня, такі як DNS або HTTP.

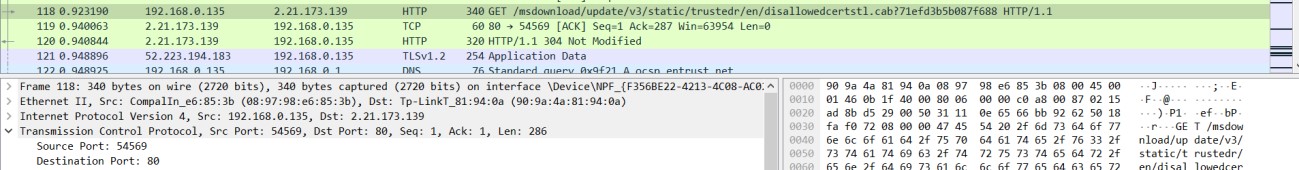
1. Вибрав пакет, що використовує протокол UPD:

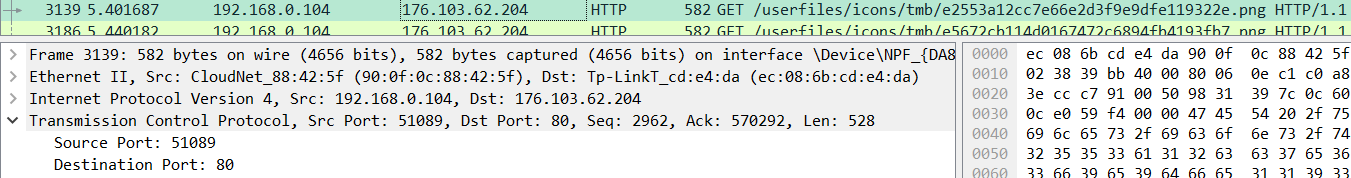


Порт відправника 63177 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв’язок.

Порт отримувача 443 є фіксованим і вибирається на основі протоколу чи служби, що використовується.

1. Вибрав пакет, що використовує протокол HTTP:

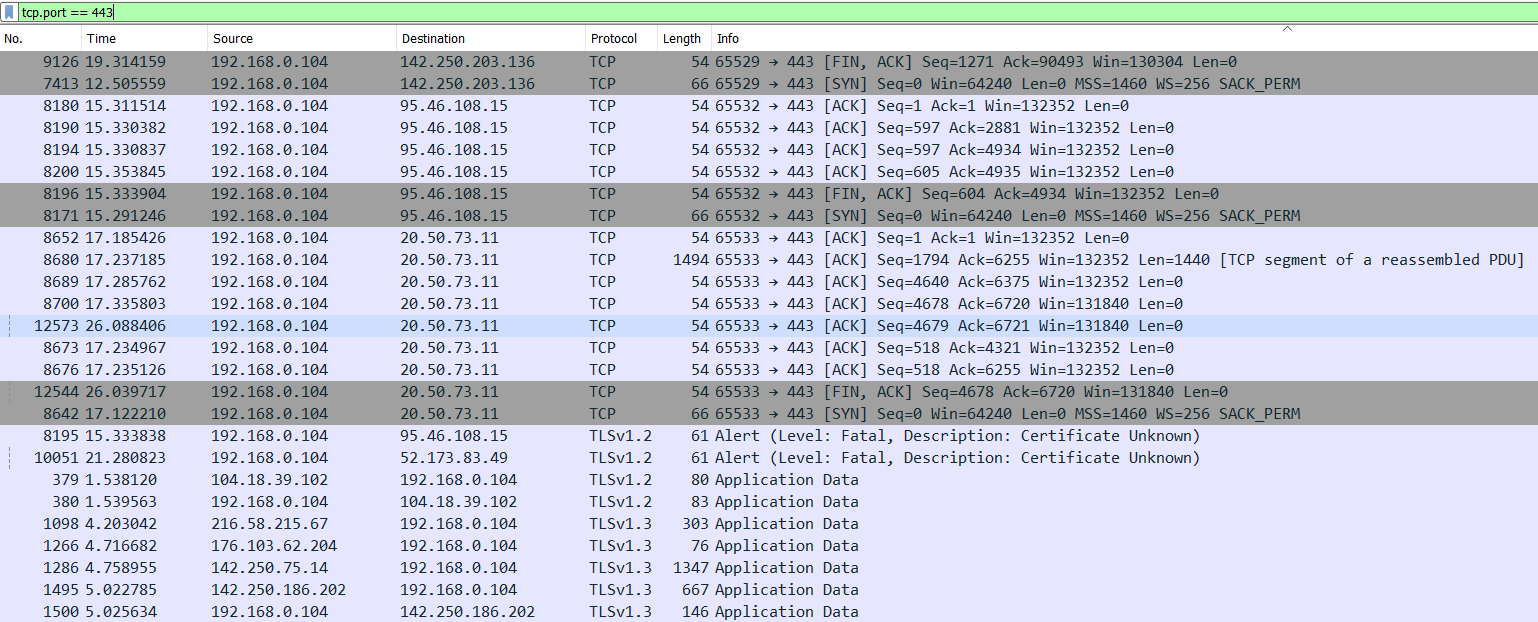




Порт відправника 51089 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв’язок.

Порт отримувача 80 є добре відомим портом для HTTP. Це фіксований порт, призначений для протоколу HTTP.

1. Знаючи закріплений за НTTPS порт (443), знайшов пакети цього протоколу:



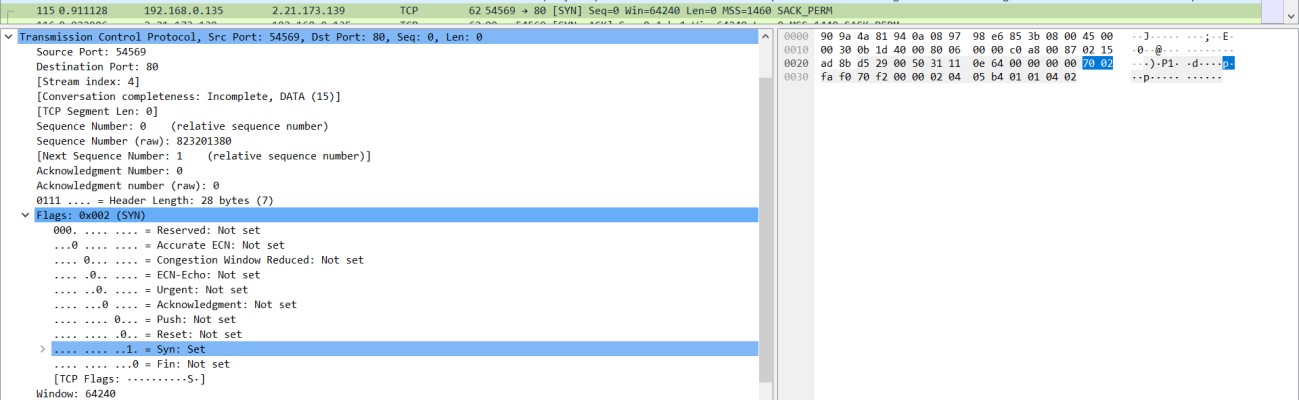
Бачу різні протоколи, зокрема TCP та TLSv1.2, TLSv1.3. Це пов’язано з тим, що мережевий трафік часто передбачає кілька рівнів інкапсуляції, а

Wireshark відображає протоколи на основі доступних. Отже, сам вміст HTTPS може бути не відразу видимим, якщо трафік зашифровано, і для його розшифровки для аналізу потрібні додаткові кроки.

1. Відшукав послідовність пакетів процедури “потрійного рукостискання”:



1. Аналіз пакетів з попереднього пункту: 1) Пакет №115:



Порт відправника – 54569, а порт отримувача – 80, який є портом за замовчуванням для HTTP.

Sequence Number (Relative): 0 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 823201380 - є фактичним 32-бітним порядковим номером.

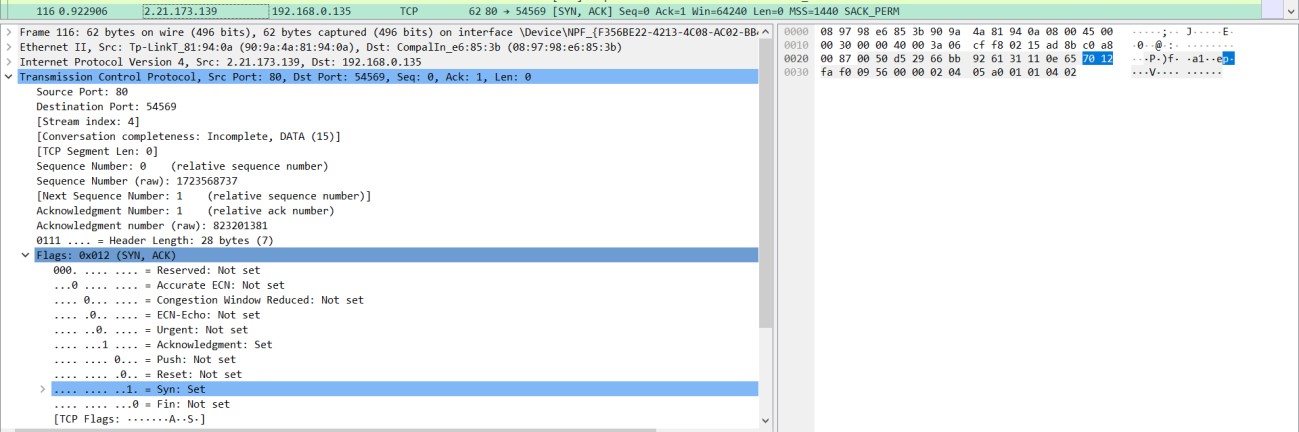
Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 0 - відправник не отримав жодних даних від іншої сторони.

Acknowledgment Number (Raw): 0.

Прапорець 0x002 (SYN) вказує на початок нового TCP-з'єднання. Інші прапорці не встановлені (не використовуються в цьому пакеті).

2) Пакет №116:



Порт відправника – 80, який є портом за замовчуванням для HTTP, а порт отримувача – 54569.

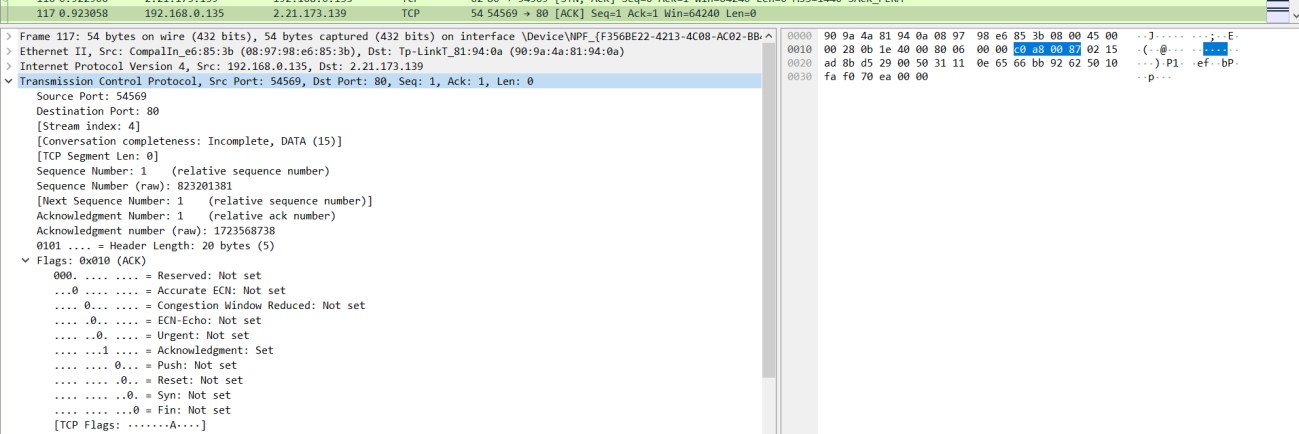
Sequence Number (Relative): 0 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 1723568737- є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 1 - вказує на те, що відправник отримав перший пакет (з порядковим номером 0). Acknowledgment Number (Raw): 823201381.

Прапорці 0x012 (SYN, ACK) вказують, що це пакет SYN-ACK, який підтверджує отриманий SYN. Інші прапорці не встановлені (не використовуються в цьому пакеті). 3) Пакет №117:



Порт відправника – 54569, а порт отримувача – 80, який є портом за замовчуванням для HTTP.

Sequence Number (Relative): 1 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 823201380 - є фактичним 32-бітним порядковим номером.

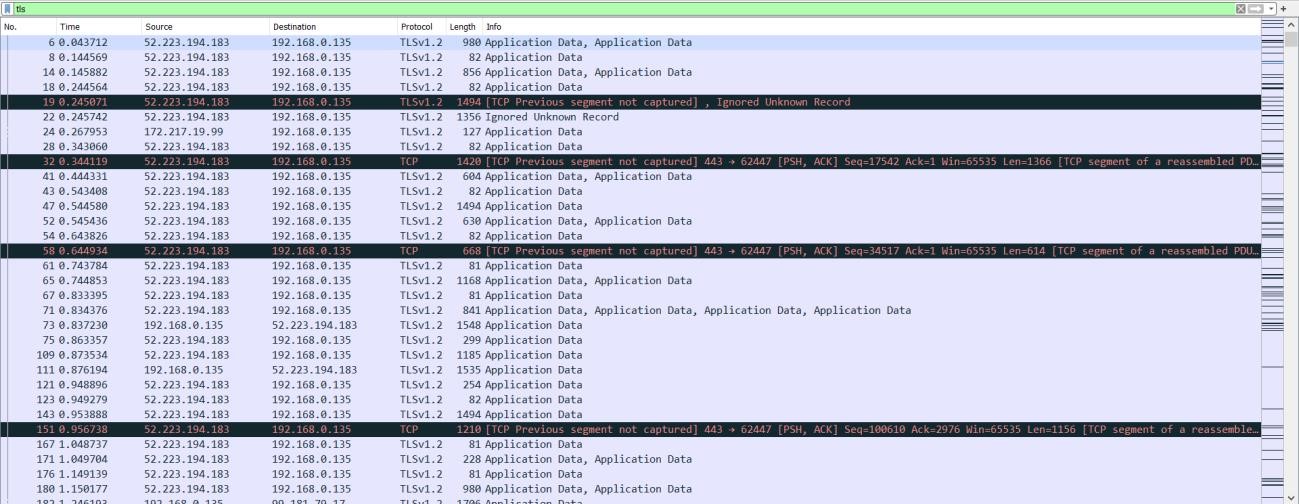
Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

Acknowledgment Number (Relative): 1 – вказує на те, що відправник отримав пакет SYN-ACK (з порядковим номером 0) і підтверджує його.

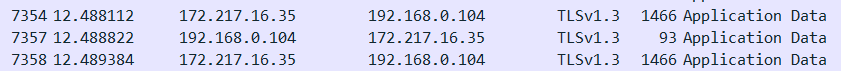
Acknowledgment Number (Raw): 1723568738.

Прапорець 0x010 (ACK) вказує на те, що це пакет ACK, який підтверджує отриманий SYN-ACK. Інші прапорці не встановлені (не використовуються в цьому пакеті).

1. Використовуючи фільтр tls, отримав пакети криптографічного протоколу TLS:

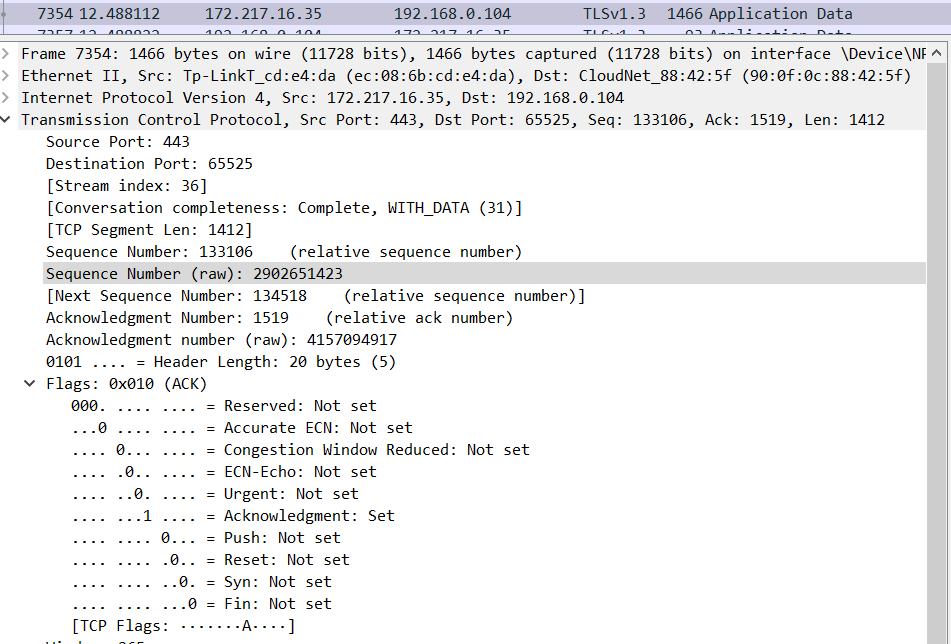


1. Обрав пакети, що стосуються процедури TLS-рукостискання:



Аналіз пакетів:

1) Пакет № 7354:



Порт відправника – 443, який є портом за замовчуванням для HTTPS, а порт отримувача – 65525.

Sequence Number (Relative): 133106 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 2902651423 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 134518 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 134518.

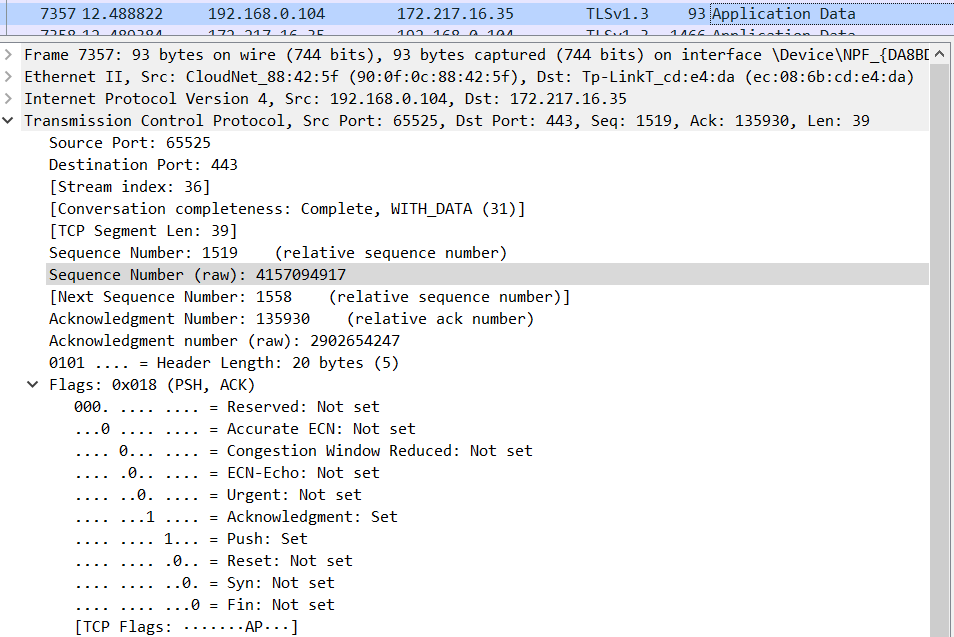
Acknowledgment Number (Relative): 1519 – вказує на те, що відправник отримав дані до порядкового номера 1519 і підтверджує це.

Acknowledgment Number (Raw): 4157094917.

Прапорці 0x010 (ACK) вказують на те, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

2) Пакет № 7357:



Порт відправника – 65525, а порт отримувача – 443, який є портом за замовчуванням для HTTPS.

Sequence Number (Relative): 1519 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 4157094917 - є фактичним 32-бітним порядковим номером.

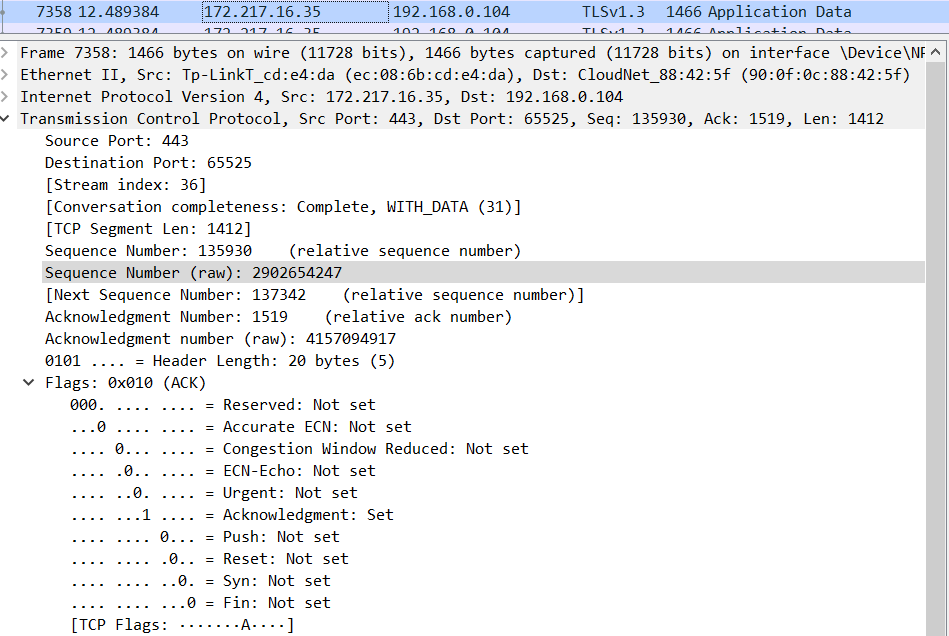
Next Sequence Number (Relative): 1558 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1558.

Acknowledgment Number (Relative): 135930 – вказує на те, що відправник отримав дані до порядкового номера 135930 і підтверджує це. Acknowledgment Number (Raw): 2902654247.

Прапорці 0x018 (PSH, ACK) вказують на те, що це кадр підтвердження з функцією push, припускаючи, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

3) Пакет № 7358:



Порт відправника – 443, який є портом за замовчуванням для HTTPS, а порт отримувача – 65525.

Sequence Number (Relative): 135930 - відноситься до початкового порядкового номера підключення.

Sequence Number (Raw): 2902654247 - є фактичним 32-бітним порядковим номером.

Next Sequence Number (Relative): 137342 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 137342.

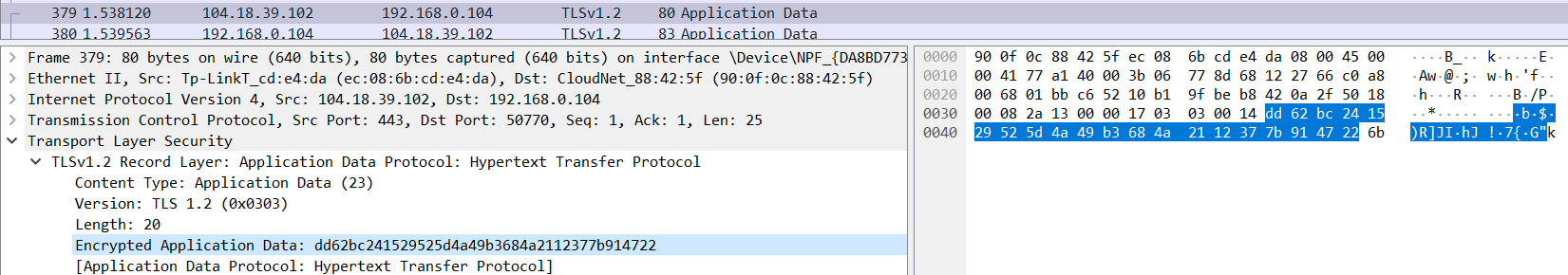
Acknowledgment Number (Relative): 1519– вказує на те, що відправник отримав дані до порядкового номера 1519 і підтверджує це.

Acknowledgment Number (Raw): 4157094917.

Прапорці 0x010 (ACK) вказують на те, що дані надсилаються на прикладний рівень.

Інші прапорці не встановлені (не використовуються в цьому пакеті).

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



**Висново**: Під час виконання лабораторної роботи я здобув практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку ТСР/ІР.