ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Факультет прикладної математики та інформатики

Комп’ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №8

Аналіз TCP-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 TCP/IP.

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:

tcp || udp

No.	Time	Source	Destination	Protocol	Length	Info
2782	5.341468	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=63849 Win=132352 Len=0
2786	5.341652	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=68169 Win=132352 Len=0
2788	5.341780	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=69609 Win=132352 Len=0
3075	5.396652	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [ACK] Seq=966 Ack=86587 Win=132352 Len=0
6049	9.296237	192.168.0.104	176.103.62.204	TCP	54	51097 → 80 [FIN, ACK] Seq=4878 Ack=405175 Win=130816 Len=0
1396	4.940631	192.168.0.104	176.103.62.204	TCP	66	51097 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1413	4.978576	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1488	5.011639	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=14121 Win=131072 Len=0
1550	5.050016	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=16945 Win=131072 Len=0
1556	5.050380	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=22593 Win=131072 Len=0
1567	5.052657	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=25417 Win=131072 Len=0
1570	5.054451	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=28241 Win=131072 Len=0
1478	5.010304	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=2825 Win=131072 Len=0
1573	5.055571	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=30637 Win=131072 Len=0
1484	5.011396	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=397 Ack=9885 Win=131072 Len=0
6077	9.329667	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [ACK] Seq=398 Ack=30638 Win=131072 Len=0
6043	9.296089	192.168.0.104	216.58.208.202	TCP	54	51098 → 80 [FIN, ACK] Seq=397 Ack=30637 Win=131072 Len=0
1403	4.951928	192.168.0.104	216.58.208.202	TCP	66	51098 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1891	5.134961	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
2023	5.211520	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=11675 Win=131072 Len=0
2026	5.211870	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=14499 Win=131072 Len=0
2028	5.212596	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=15911 Win=131072 Len=0
2030	5.213002	192.168.0.104	172.217.16.35	TCP	54	51099 → 443 [ACK] Seq=1282 Ack=17323 Win=131072 Len=0

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.

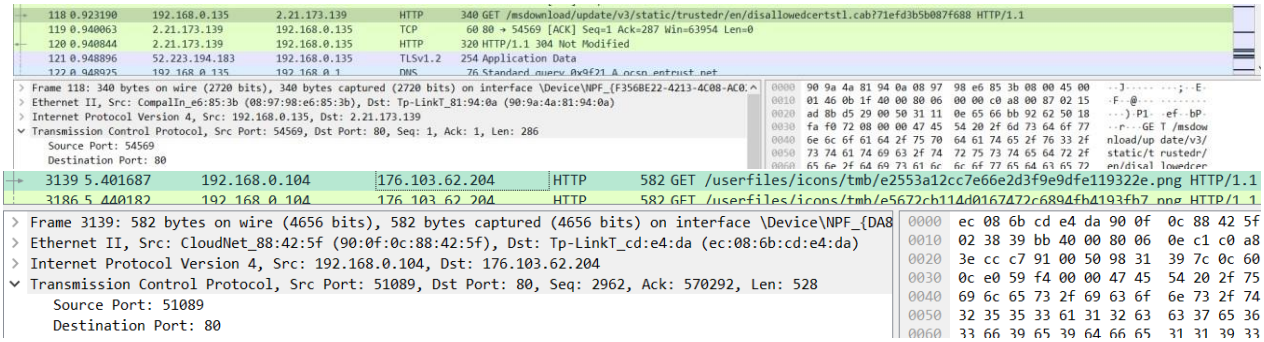
4. Вибрав пакет, що використовує протокол UPD:

243	0.745509	192.168.0.104	34.120.32.134	UDP	81	63177 → 443 Len=39
6480	10.684539	192.168.0.104	34.120.32.134	UDP	81	63177 → 443 Len=39

```
> Frame 243: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{DA8BD773
> Ethernet II, Src: CloudNet_88:42:5f (90:0f:0c:88:42:5f), Dst: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 34.120.32.134
v User Datagram Protocol, Src Port: 63177, Dst Port: 443
    Source Port: 63177
    Destination Port: 443
```

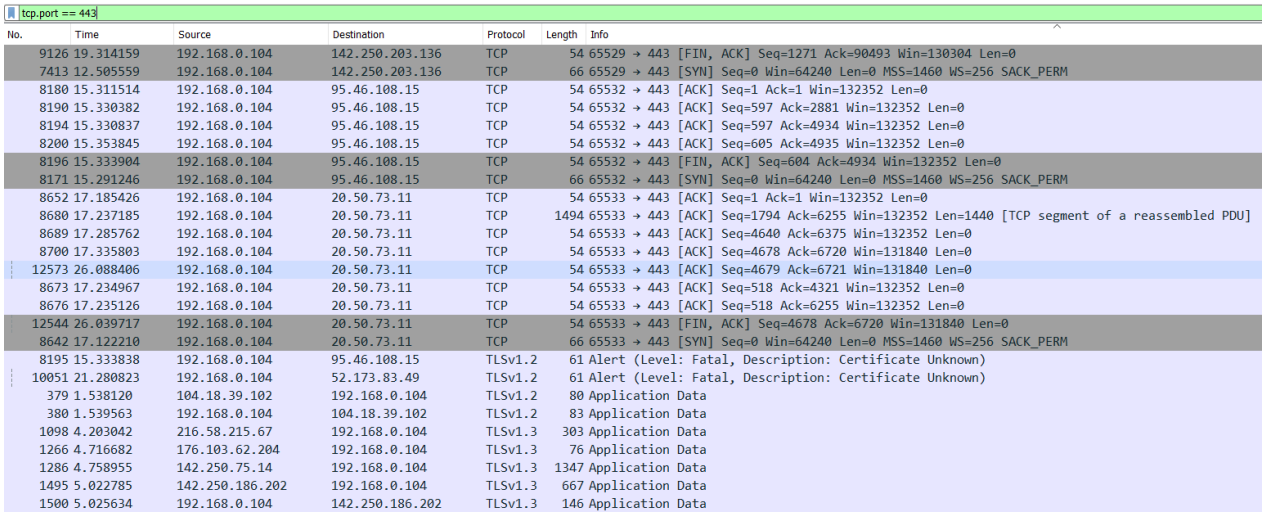
Порт відправника 63177 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв’язок.
Порт отримувача 443 є фіксованим і вибирається на основі протоколу чи служби, що використовується.

5. Вибрав пакет, що використовує протокол HTTP:



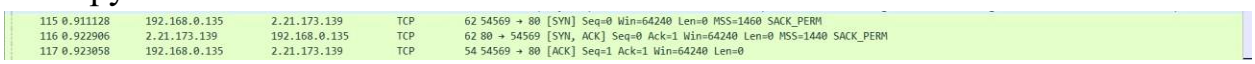
Порт відправника 51089 динамічно або випадково призначається операційною системою або програмою, яка ініціює зв’язок.
Порт отримувача 80 є добре відомим портом для HTTP. Це фіксований порт, призначений для протоколу HTTP.

6. Знаючи закріплений за HTTPS порт (443), знайшов пакети цього протоколу:

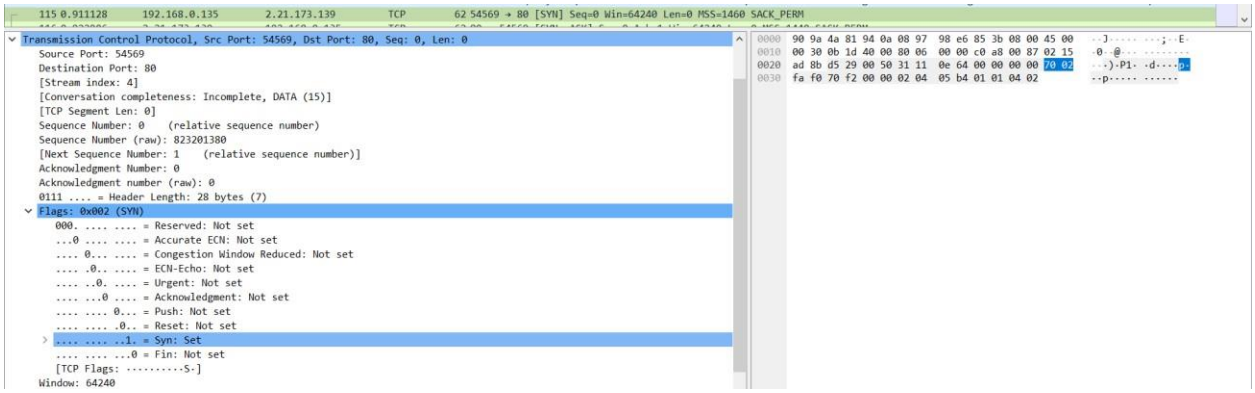


Бачу різні протоколи, зокрема TCP та TLSv1.2, TLSv1.3. Це пов’язано з тим, що мережевий трафік часто передбачає кілька рівнів інкапсуляції, а Wireshark відображає протоколи на основі доступних. Отже, сам вміст HTTPS може бути не відразу видимим, якщо трафік зашифровано, і для його розшифровки для аналізу потрібні додаткові кроки.

7. Відшукав послідовність пакетів процедури “потрійного рукостискання”:



8. 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.

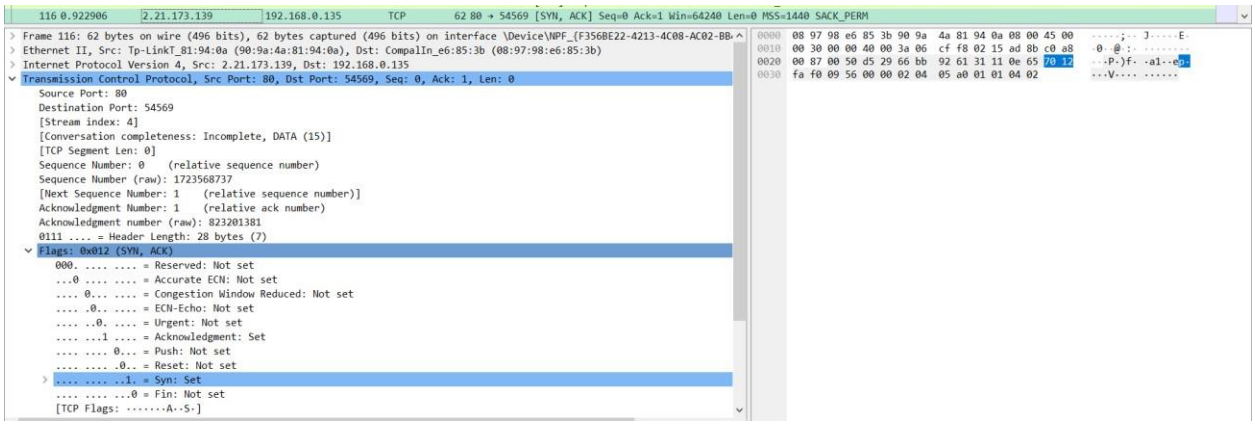
Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

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:



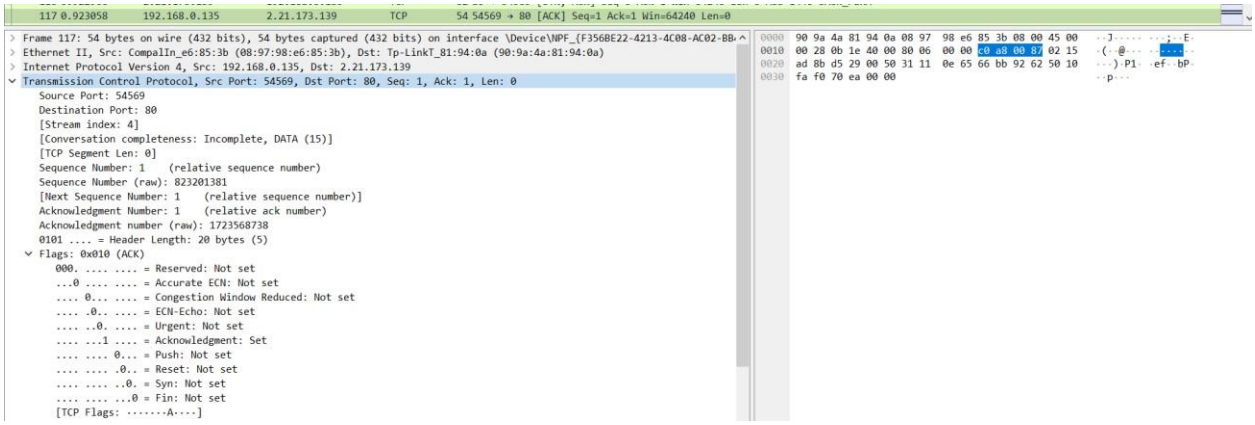
Порт відправника – 80, який є портом за замовчуванням для HTTP, а порт отримувача – 54569.

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

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

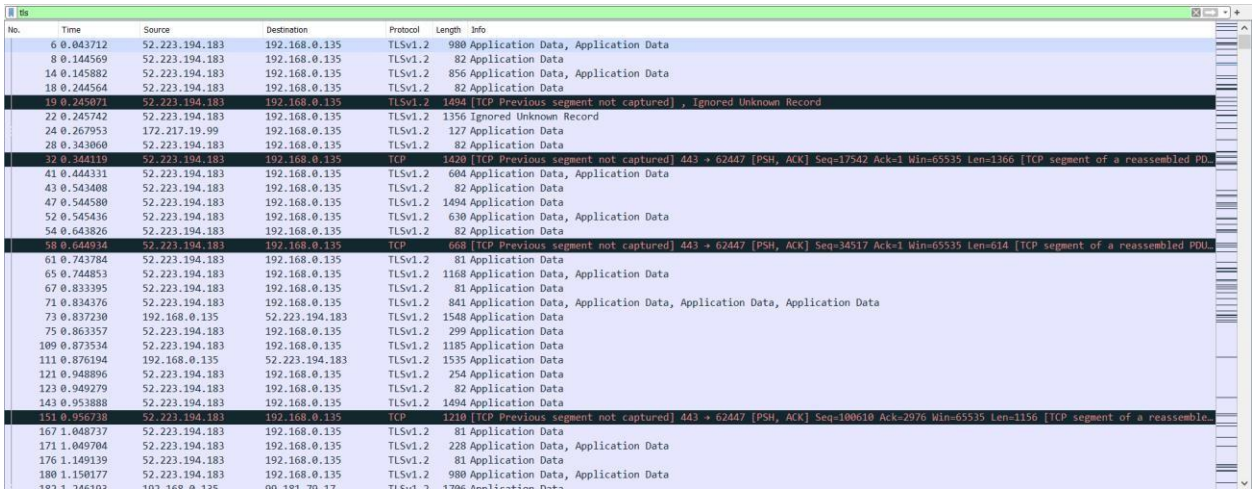
Next Sequence Number (Relative): 1 - вказує на те, що відправник очікує, що наступний пакет матиме порядковий номер 1.

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).

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



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

```
7354 12.488112    172.217.16.35    192.168.0.104    TLSv1.3   1466 Application Data
7357 12.488822    192.168.0.104    172.217.16.35    TLSv1.3     93 Application Data
7358 12.489384    172.217.16.35    192.168.0.104    TLSv1.3   1466 Application Data
```

Аналіз пакетів:

1) Пакет № 7354:

```
7354 12.488112    172.217.16.35    192.168.0.104    TLSv1.3   1466 Application Data
```

```
> Frame 7354: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Device\NF
> Ethernet II, Src: Tp-LinkT_cd:e4:da (ec:08:6b:cd:e4:da), Dst: CloudNet_88:42:5f (90:0f:0c:88:42:5f)
> Internet Protocol Version 4, Src: 172.217.16.35, Dst: 192.168.0.104
v Transmission Control Protocol, Src Port: 443, Dst Port: 65525, Seq: 133106, Ack: 1519, Len: 1412
    Source Port: 443
    Destination Port: 65525
    [Stream index: 36]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1412]
    Sequence Number: 133106    (relative sequence number)
    Sequence Number (raw): 2902651423
    [Next Sequence Number: 134518    (relative sequence number)]
    Acknowledgment Number: 1519    (relative ack number)
    Acknowledgment number (raw): 4157094917
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A····]
```

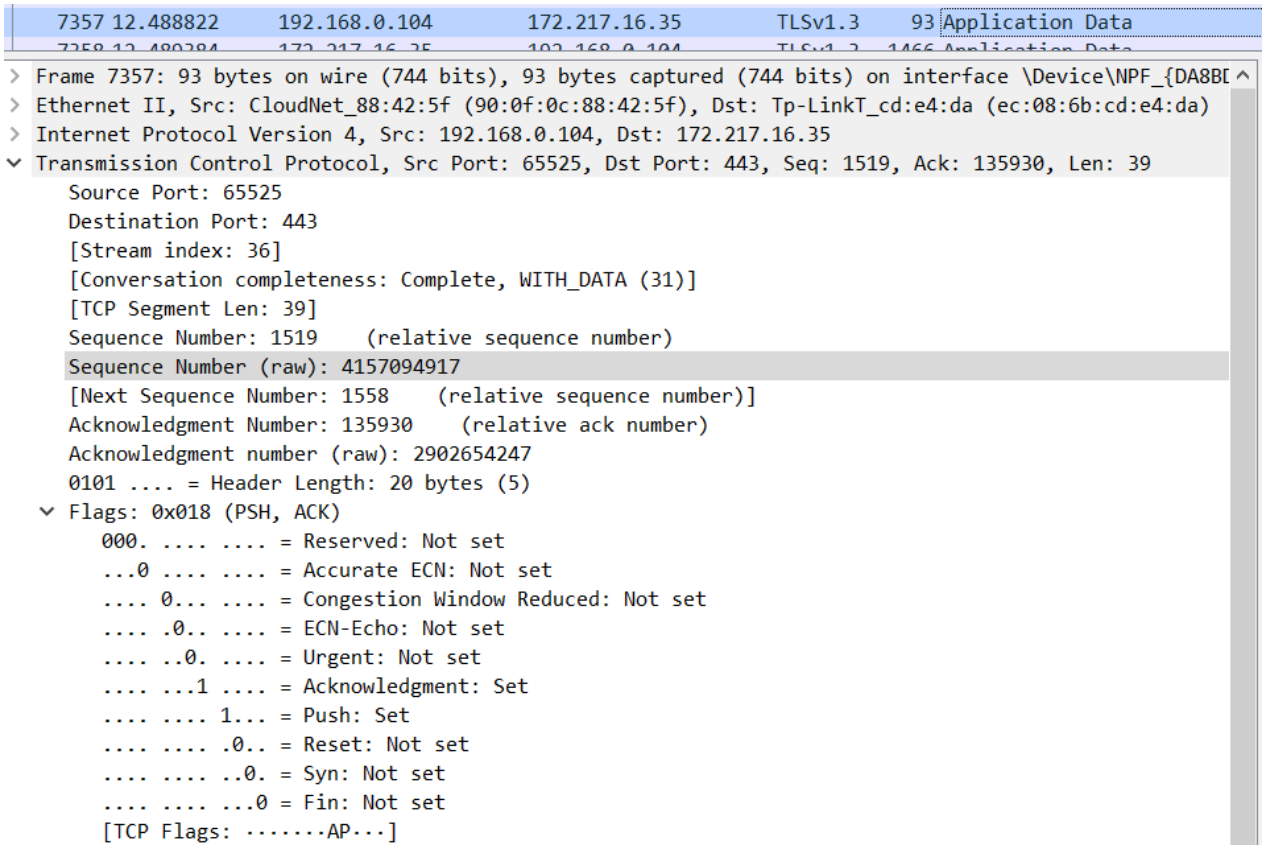
Порт відправника – 443, який є портом за замовчуванням для HTTPS, а порт отримувача – 65525.

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).

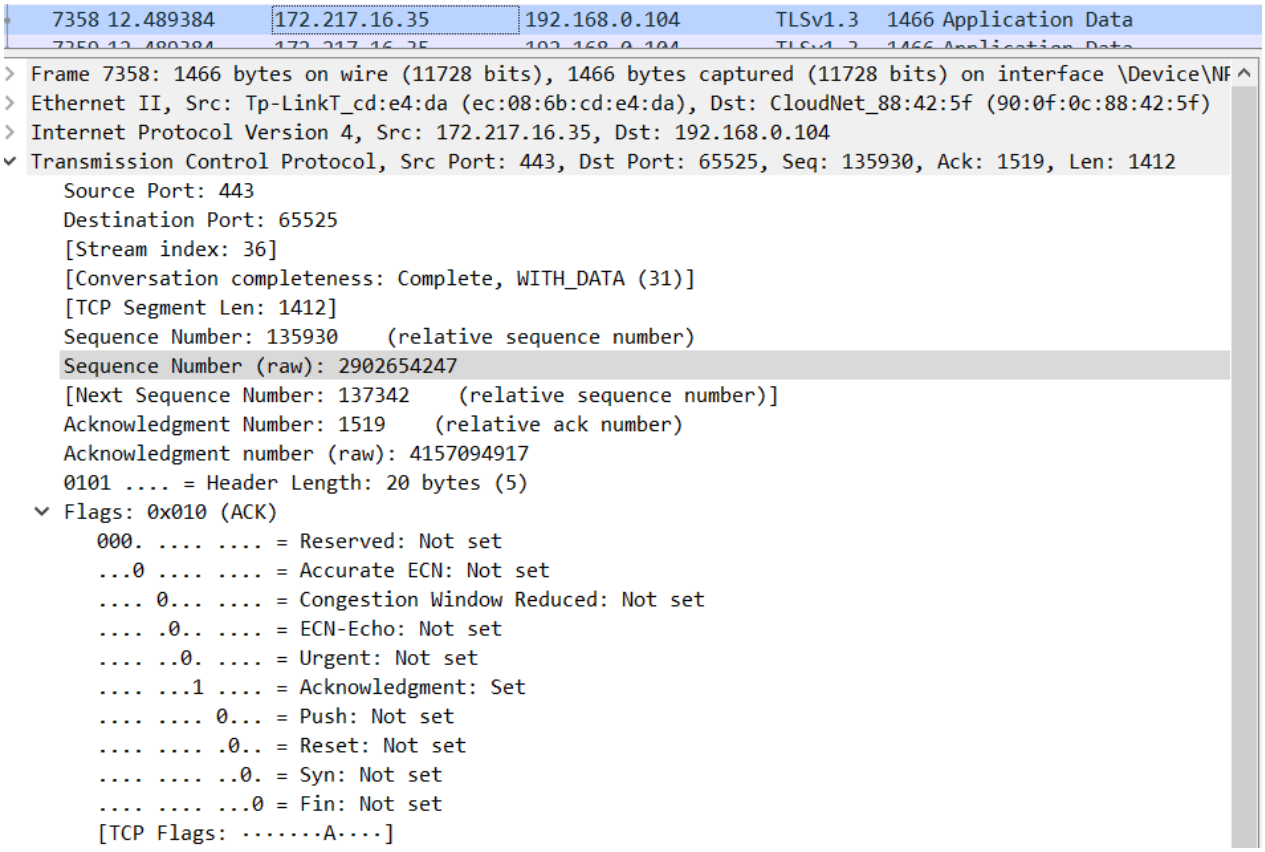
2) Пакет № 7357:



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.

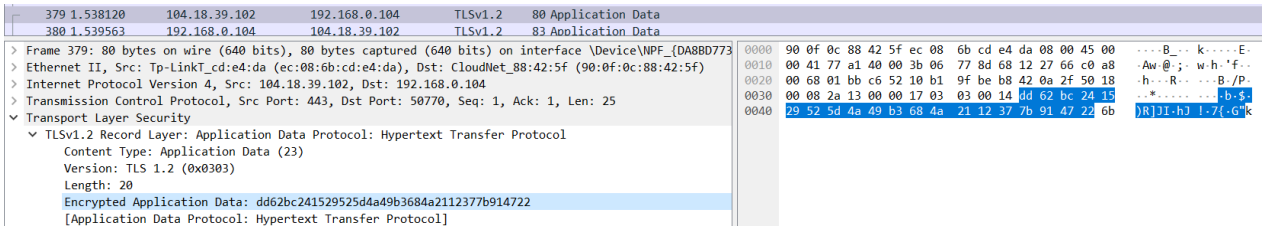
Acknowledgment Number (Relative): 1519– вказує на те, що відправник отримав дані до порядкового номера 1519 і підтверджує це.

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 TCP/IP.