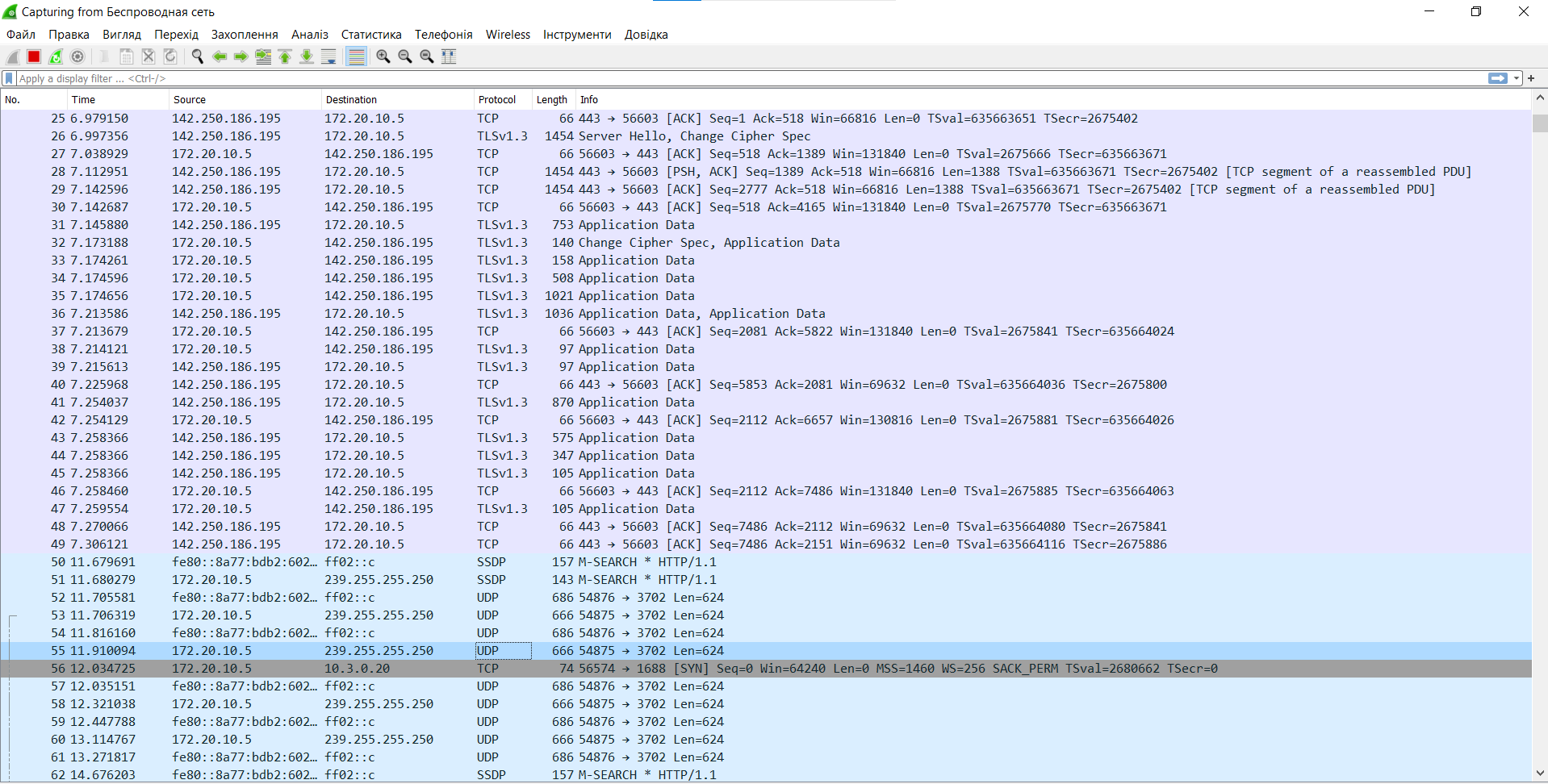
ЗВІТ КОМАНДИРА С-04 ГРУПИ

СТАРШИЙ СЕРЖАНТ ФЕСЕНКО ІВАН ОЛЕКСІЙОВИЧ

UDP and TCP

Скріншоти використання **WireShark** на **Windows**



*Одразу обрав TCP та UDP на віндовс*  
  
TCP (Transmission Control Protocol) та UDP (User Datagram Protocol) - це два основних протоколи передачі даних у комп'ютерних мережах.

Основна різниця між TCP та UDP полягає у способах передачі даних та рівні надійності.

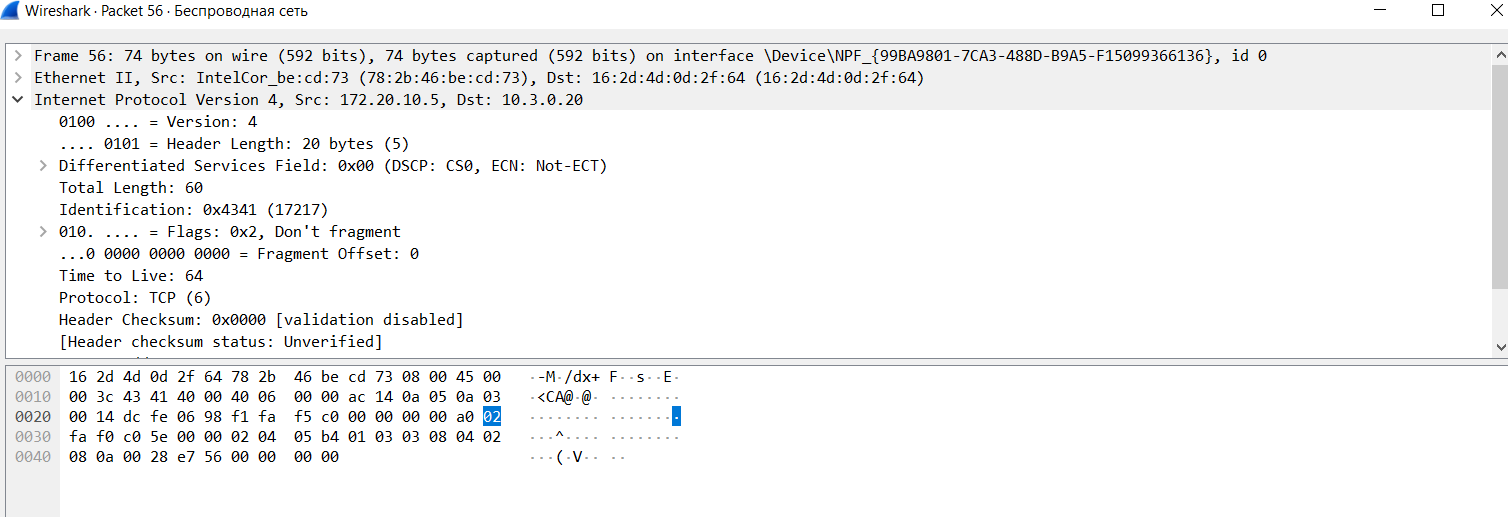
TCP - це з'єднувальний та надійний протокол. Він забезпечує передачу даних шляхом встановлення з'єднання між відправником та отримувачем. TCP гарантує, що дані будуть доставлені в правильному порядку, без втрат та дублювання. Якщо пакети втрачаються або пошкоджуються під час передачі, TCP повторно відправляє втрачені пакети для забезпечення повної доставки. Це робить TCP надійним, але додає певну накладну вартість у вигляді затримок.

UDP - це безз'єднувальний та ненадійний протокол. Він передає дані без встановлення з'єднання та не гарантує доставку даних в правильному порядку або без втрат. UDP швидший та має меншу накладну вартість порівняно з TCP. Він використовується там, де невелика втрата даних не критична, наприклад, у відео- та голосових додатках, де важлива швидкість передачі.

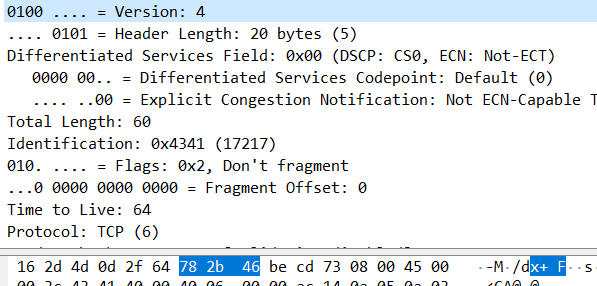
Таким чином, TCP надає надійну передачу даних з контролем порядку та відновленням пакетів, а UDP надає швидку, безз'єднувальну передачу даних без надійності та контролю порядку. Вибір між TCP та UDP залежить від потреб конкретного додатка та вимог до надійності та швидкості передачі даних.

Отже повериаємось до нашого TCP

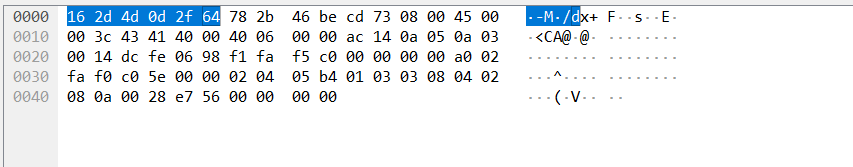




Версія 4



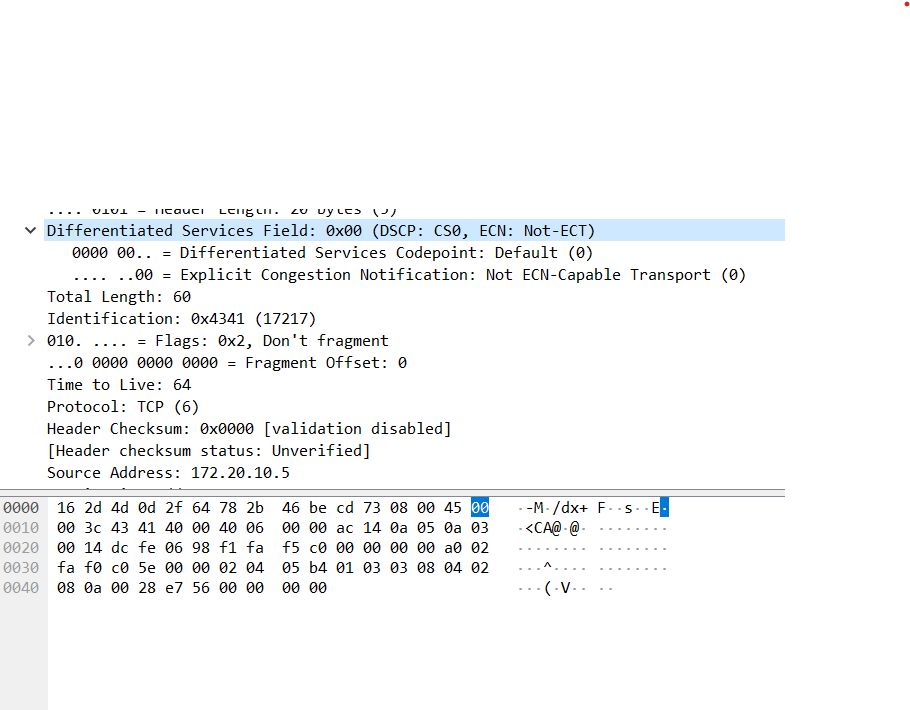
Адрес:



///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

Header Length – 20 байтів

**Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)**



Поле Differentiated Services Field (DS-Field) в заголовку пакета IP використовується для встановлення рівня обслуговування (Quality of Service - QoS) для пакета в комп'ютерних мережах. Значення "0x00" у DS-Field означає, що пакет має DSCP (Differentiated Services Code Point) значення "CS0" та ECN (Explicit Congestion Notification) значення "Not-ECT". Давайте розшифруємо ці значення:

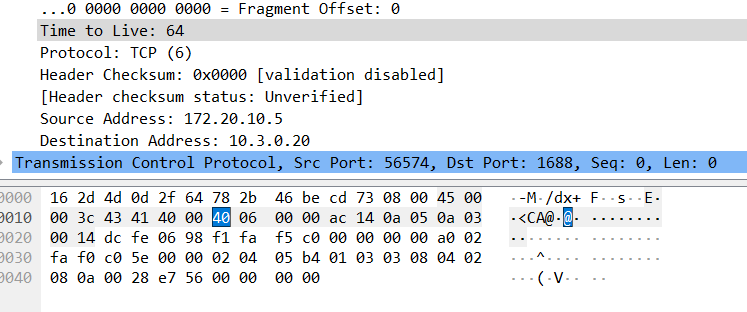
DSCP "CS0" (Class Selector 0) вказує, що пакет не має особливого пріоритету або класифікації обслуговування. Це значення використовується, коли немає потреби в диференційованому обслуговуванні пакетів і всі пакети можуть бути оброблені однаково.

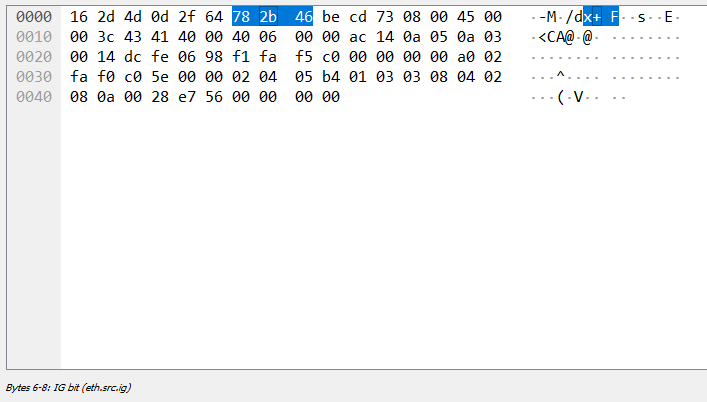
ECN "Not-ECT" (Not ECN-Capable Transport) вказує, що пакет не підтримує механізм явної індикації припливу (Explicit Congestion Notification). Цей механізм дозволяє відправникам та отримувачам пакетів співпрацювати у виявленні та уникненні перевантаження мережі шляхом позначення та передачі інформації про стан загрузки маршрутизаторів.

Загалом, значення "0x00" (DSCP: CS0, ECN: Not-ECT) вказує на відсутність диференційованого обслуговування та відсутність підтримки ECN для пакета. Такі пакети можуть бути оброблені стандартним чином, без особливих пріоритетів чи інших додаткових функцій QoS

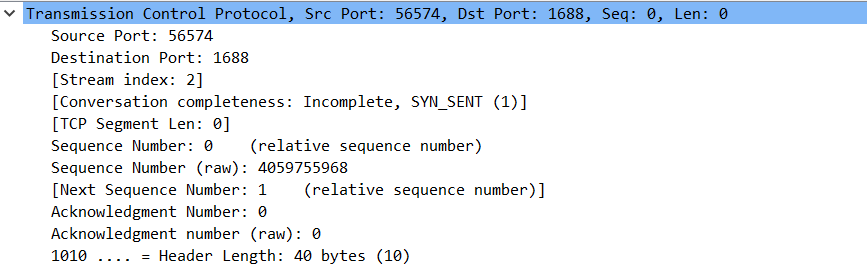
Total Length – 60 байт

Identification: 0x4341 (17217)





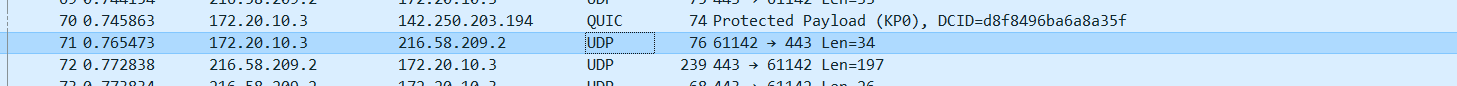
В Wireshark, "IG bit" відноситься до полів "IGMPv2" (Internet Group Management Protocol version 2) в заголовку пакета. IGMP використовується для керування мультикастовим трафіком в IP-мережах. Поле "IG bit" вказує тип повідомлення IGMPv2, яким можуть бути "Membership Query" (запит на участь у групі) або "Membership Report" (звіт про участь у групі). Це поле допомагає ідентифікувати та аналізувати мультикастовий трафік у Wireshark.

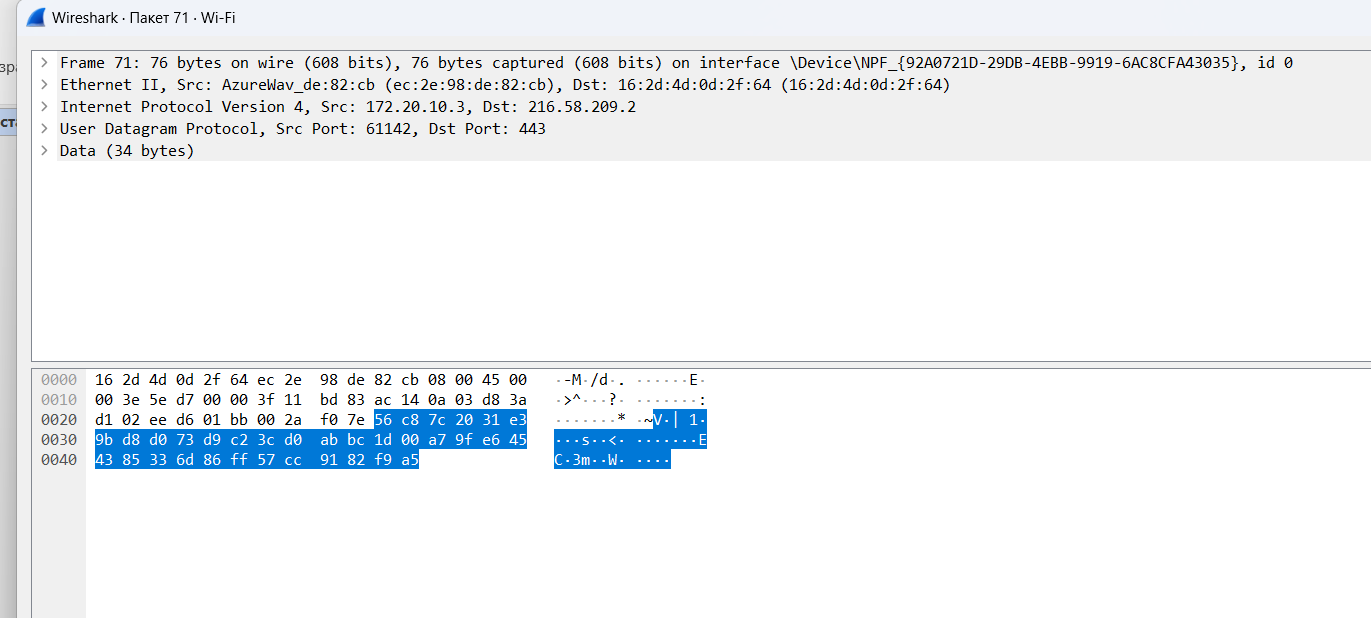


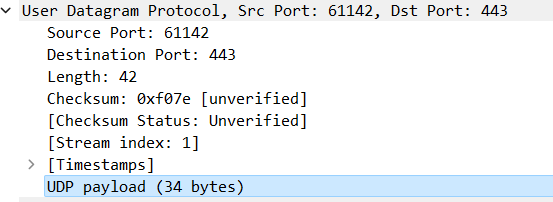
***Сама TCP:***

* Source Port: 56574 - номер порту, з якого відправляється пакет.
* Destination Port: 1688 - номер порту, до якого адресований пакет.
* Stream index: 2 - індекс потоку, який вказує на конкретний потік зв'язку між відправником та отримувачем.
* Conversation completeness: Incomplete, SYN\_SENT (1) - статус розмови, яка поки не завершена, і наразі в процесі встановлення з'єднання. SYN\_SENT означає, що відправлено синхронізаційний (SYN) сигнал, і очікується підтвердження (ACK) від отримувача.
* TCP Segment Len: 0 - довжина сегмента TCP в байтах, в даному випадку дорівнює 0, що означає, що пакет не містить додаткових данних.
* Sequence Number: 0 - послідовний номер (sequence number) пакета, який вказує на порядковий номер байту в потоці даних.
* Sequence Number (raw): 4059755968 - значення послідовного номера пакета у вигляді сирого числа без перетворень.
* Next Sequence Number: 1 - наступний послідовний номер (sequence number), який вказує на очікуваний порядковий номер байту в наступному пакеті.
* Acknowledgment Number: 0 - номер підтвердження (acknowledgment number), що вказує на послідовний номер пакета, на який відправник очікує підтвердження від отримувача.
* Acknowledgment number (raw): 0 - значення номера підтвердження у вигляді сирого числа без перетворень.
* 1010 .... = Header Length: 40 bytes (10) - довжина заголовка TCP у байтах, в даному випадку становить 40 байт, що відповідає значенню 10 в десятковому форм

**UDP**



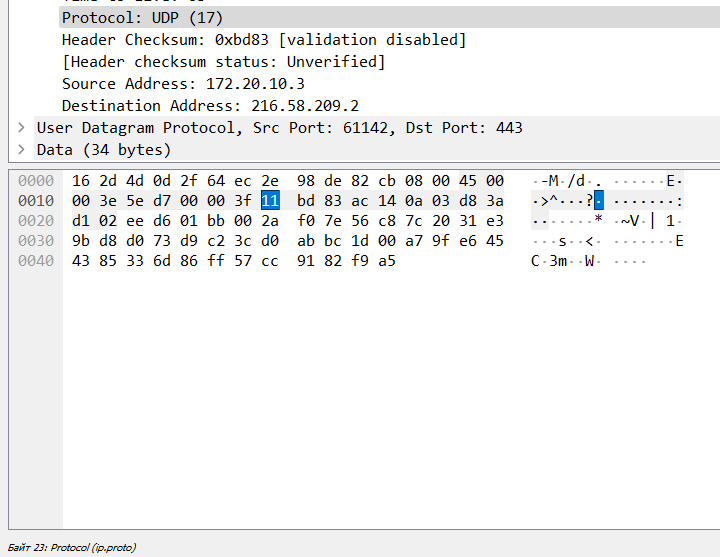




Короткий опис даних UDP-пакету:

* Source Port: Порт відправника UDP-пакету - 61142.
* Destination Port: Порт одержувача UDP-пакета – 443 (зазвичай використовується для HTTPS-з'єднань).
* Length: Довжина UDP-пакету в байтах, в даному випадку 42 байти.
* Checksum: Контрольна сума UDP-пакету дорівнює 0xf07e. (Статус перевірки контрольної суми не підтверджено).
* Stream index: Індекс потоку, у разі 1.
* UDP payload (34 bytes): Навантаження UDP-пакета, що містить 34 байти даних. Це дані, які передаються через UDP-з'єднання.

Зверніть увагу, що цей описовий текст є зведенням основної інформації про UDP-пакет, засновану на наданих даних. Детальний аналіз UDP-пакету може вимагати більш детального розгляду його вмісту, такого як IP-адреси та дані всередині навантаження UDP.



* Протокол: UDP (User Datagram Protocol, номер 17)
* Фрагментація: Прапори фрагментації встановлені на "0", що вказує на те, що цей UDP-пакет не фрагментований. Зміщення фрагмента дорівнює 0.
* Час життя (TTL): Значення часу життя пакета (TTL) дорівнює 63. Це означає, що пакет може пройти через 63 маршрутизатори перед тим, як буде відкинуто.
* Контрольна сума заголовка: Значення контрольної суми заголовка пакета дорівнює 0xbd83. Статус перевірки контрольної суми не підтверджено (валідацію вимкнено).
* Адреса відправника: IP-адреса відправника пакета – 172.20.10.3.
* Адреса одержувача: IP-адреса одержувача пакета – 216.58.209.2.

Це зведення основних полів IP-заголовка для цього UDP-пакета. Зверніть увагу, що в цьому описі не міститься інформація про вміст UDP-пакету, оскільки це стосується лише IP-заголовка.