ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»

**ЗВІТ**

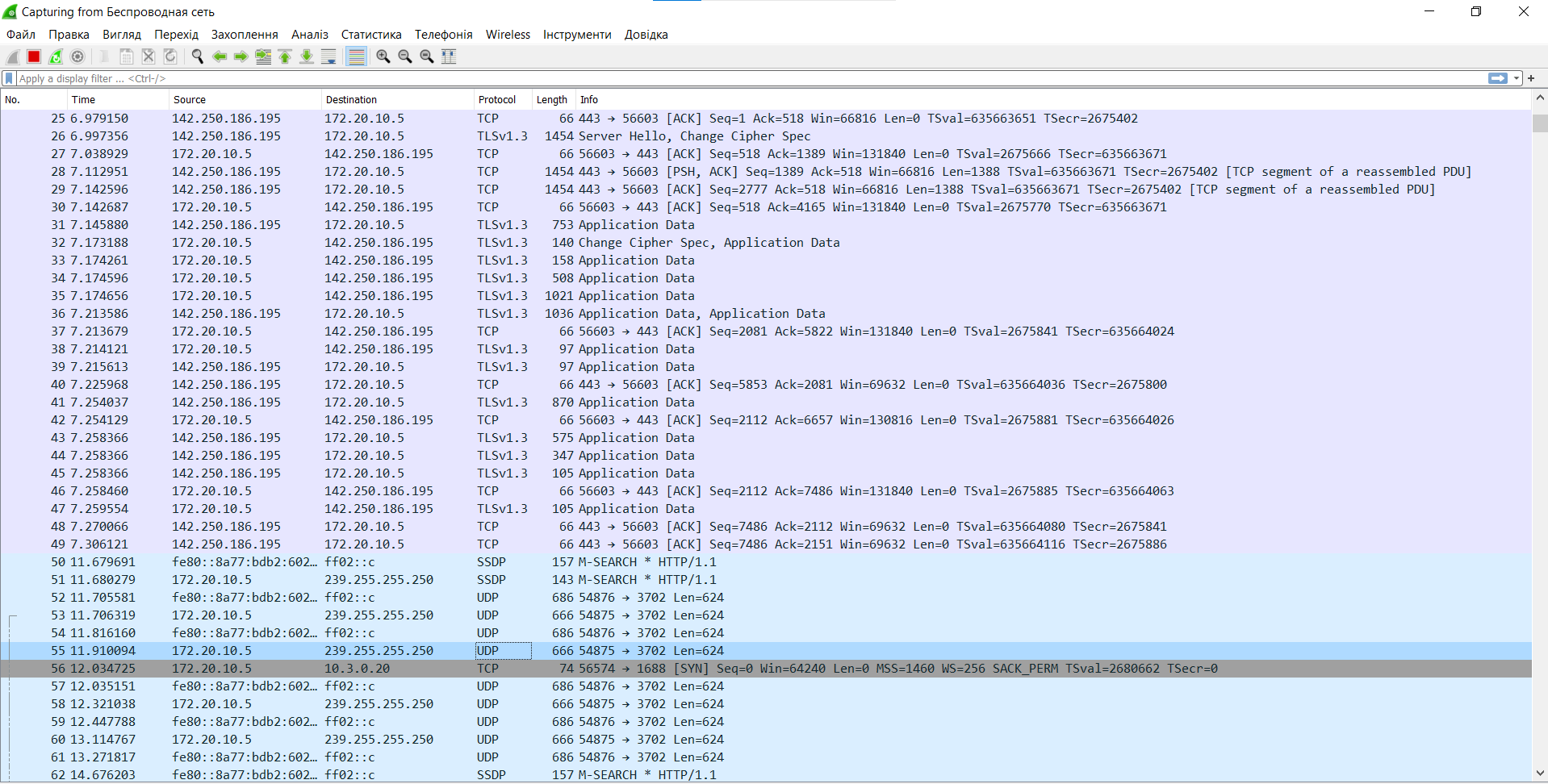
з дисципліни «ЗККЗІ»

Виконaв: командир І відділення С-05 групи

молодший сержант Владислав КУЩ

КИЇВ 2023

**TCP (Transmission Control Protocol) та UDP (User Datagram Protocol)**

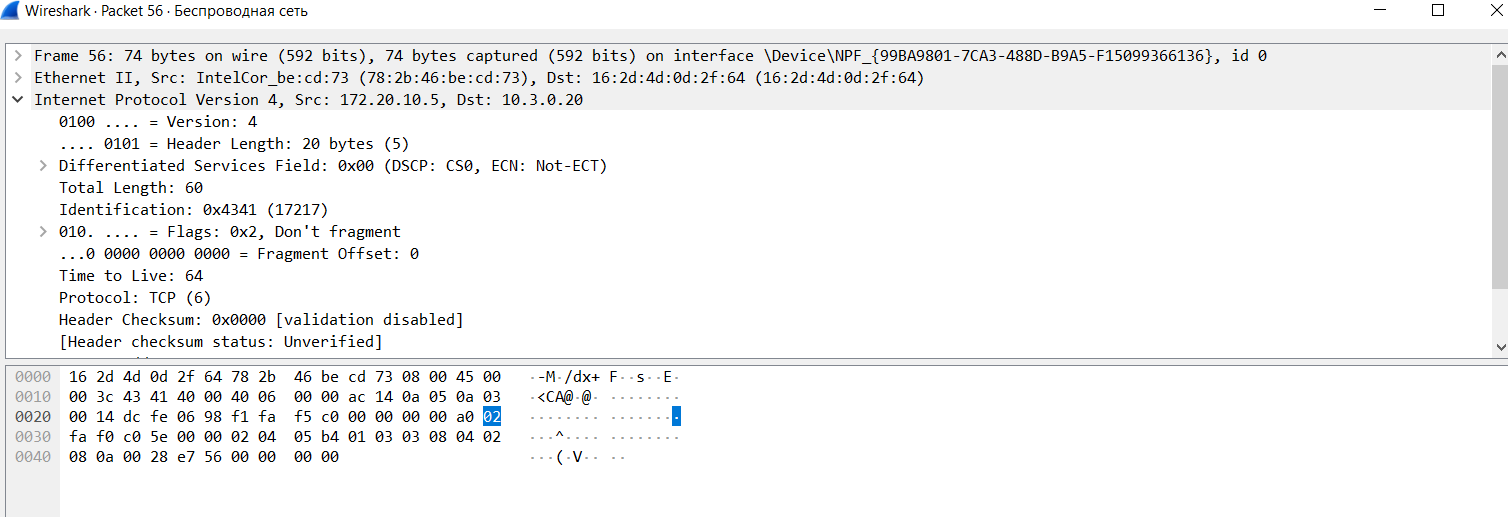


TCP (Transmission Control Protocol) та UDP (User Datagram Protocol) є двома основними протоколами транспортного рівня в комп'ютерних мережах. Обидва протоколи використовуються для передачі даних, але вони мають різні особливості та використовуються в різних сценаріях.

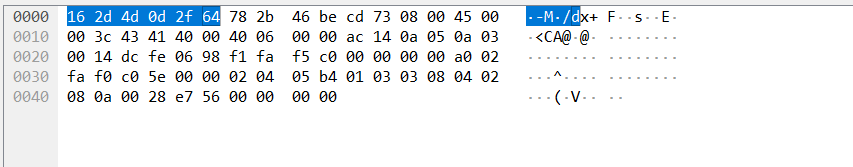
Основні відмінності між TCP та UDP:

1. З'єднання проти безз'єднаній комунікації: TCP забезпечує надійне, з'єднане передавання даних. Він встановлює віртуальне з'єднання між відправником і отримувачем перед передачею даних. У порівнянні з цим, UDP є безз'єднаним протоколом, який не встановлює з'єднання перед передачею даних. Кожен пакет даних відправляється окремо і може бути доставлений в будь-якому порядку або взагалі не бути доставленим.
2. Надійність: TCP забезпечує механізми перевірки доставки, виявлення та відновлення втрачених пакетів даних. Він гарантує, що всі дані будуть доставлені в правильному порядку та без помилок. UDP не надає такої надійності і не має механізмів перевірки доставки або відновлення втрачених пакетів. Це робить UDP швидшим, але менш надійним протоколом.
3. Затримка та пропускна здатність: Внаслідок свого надлишкового контролю та механізмів надійності, TCP може мати більшу затримку передачі даних порівняно з UDP. UDP, як стрімінг аудіо або відео.
4. Контроль потоку: TCP має вбудований механізм контролю потоку, що дозволяє регулювати швидкість передачі даних між відправником і отримувачем. Він гарантує, що отримувач може впоратися зі швидкістю передачі та не буде перевантажений. UDP не має механізму контролю потоку, тому передача даних відбувається на максимально можливій швидкості без будь-якого регулювання.
5. Залишковий ризик: TCP має механізм підтвердження отримання даних, що зменшує залишковий ризик передачі. Якщо якийсь пакет даних втрачений або пошкоджений, TCP спробує відновити його передачу. У випадку UDP, якщо пакет даних втрачений, він не буде автоматично відновлюватися, і отримувач повинен самостійно вирішити, як з ним поводитись.
6. Використання: TCP широко використовується в додатках, де надійність та порядок доставки даних є важливими, таких як веб-переглядачі, електронна пошта та передача файлів. UDP використовується в додатках, які більш толерантні до втрати даних, наприклад, стрімінг медіа, відеодзвінки та онлайн-ігри.

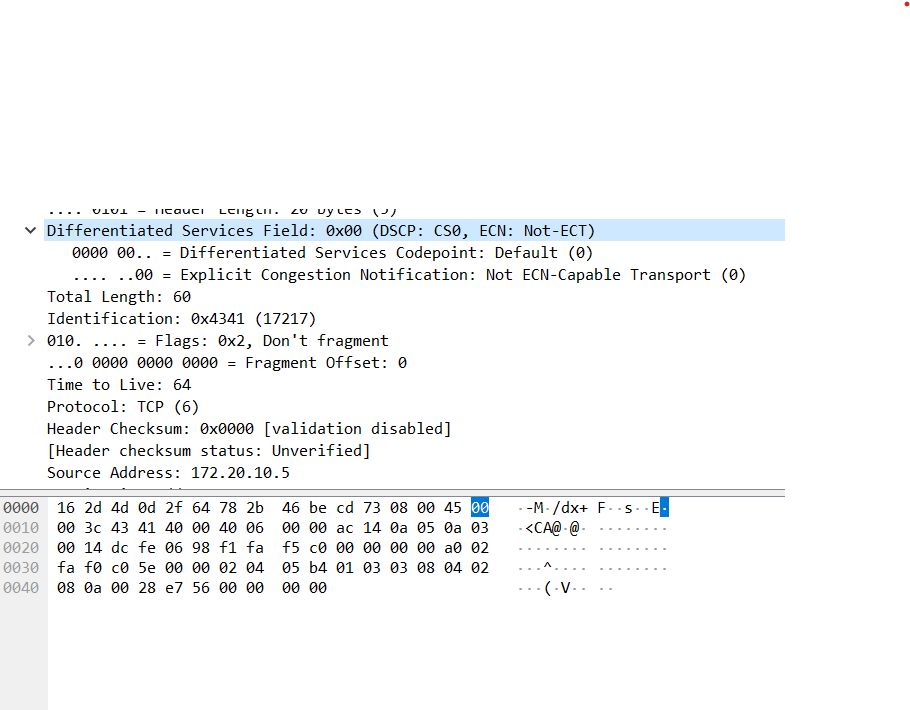
Отже, TCP та UDP мають свої відмінності в термінах надійності, затримки, контролю потоку та використання. Вибір між ними залежить від конкретних потреб вашої програми чи додатка, де ви розглядаєте їх використання.



Адрес:



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



Поле Differentiated Services Field (DS-Field) в заголовку IP-пакета 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". Розшифровуючи ці значення:

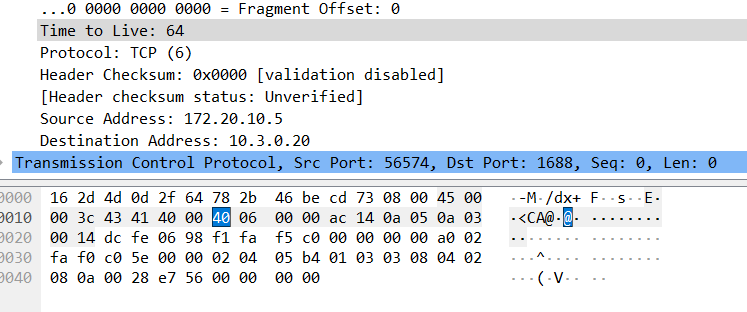
DSCP "CS0" (Class Selector 0) вказує, що пакет не має особливого пріоритету або класифікації обслуговування. Це значення використовується, коли немає потреби у диференційованому обслуговуванні пакетів, і всі пакети можуть бути оброблені однаково.

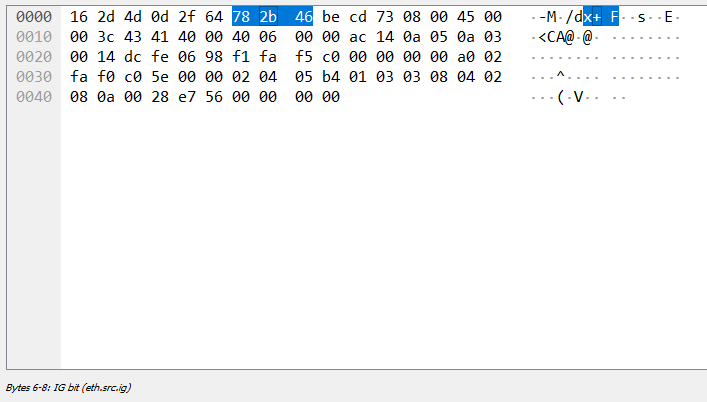
ECN "Not-ECT" (Not ECN-Capable Transport) вказує, що пакет не підтримує механізм явної індикації припливу (Explicit Congestion Notification). Цей механізм дозволяє відправникам та отримувачам пакетів співпрацювати у виявленні та уникненні перевантаження мережі шляхом позначення та передачі інформації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

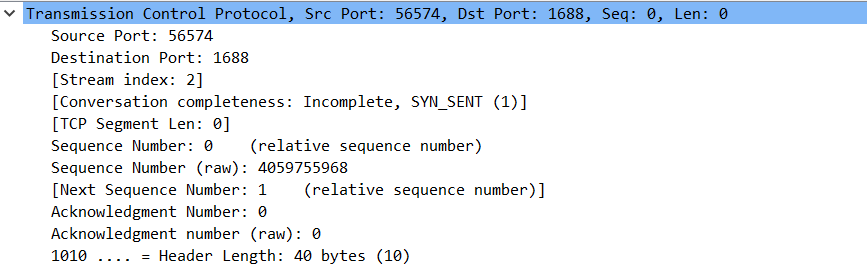
Щодо поля "Total Length", його значення - 60 байт, вказує на загальну довжину IP-пакета в байтах, включаючи заголовок та дані пакета.

Поле "Identification" зі значенням "0x4341" (17217) є ідентифікатором пакета і використовується для відстеження та збирання фрагментів пакета, якщо він був розбитий на менші





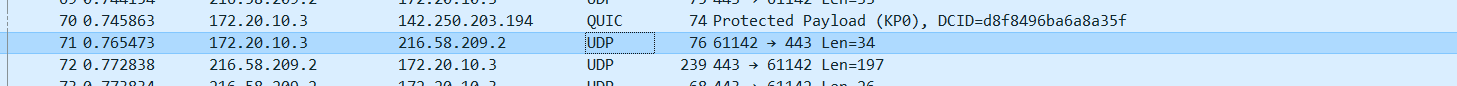
У програмі Wireshark, поле "IG bit" відноситься до полів "IGMPv2" (Internet Group Management Protocol версія 2) у заголовку пакета. Протокол IGMP використовується для керування мультикастовим трафіком в IP-мережах. Поле "IG bit" вказує на тип повідомлення IGMPv2, яким можуть бути "Membership Query" (запит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

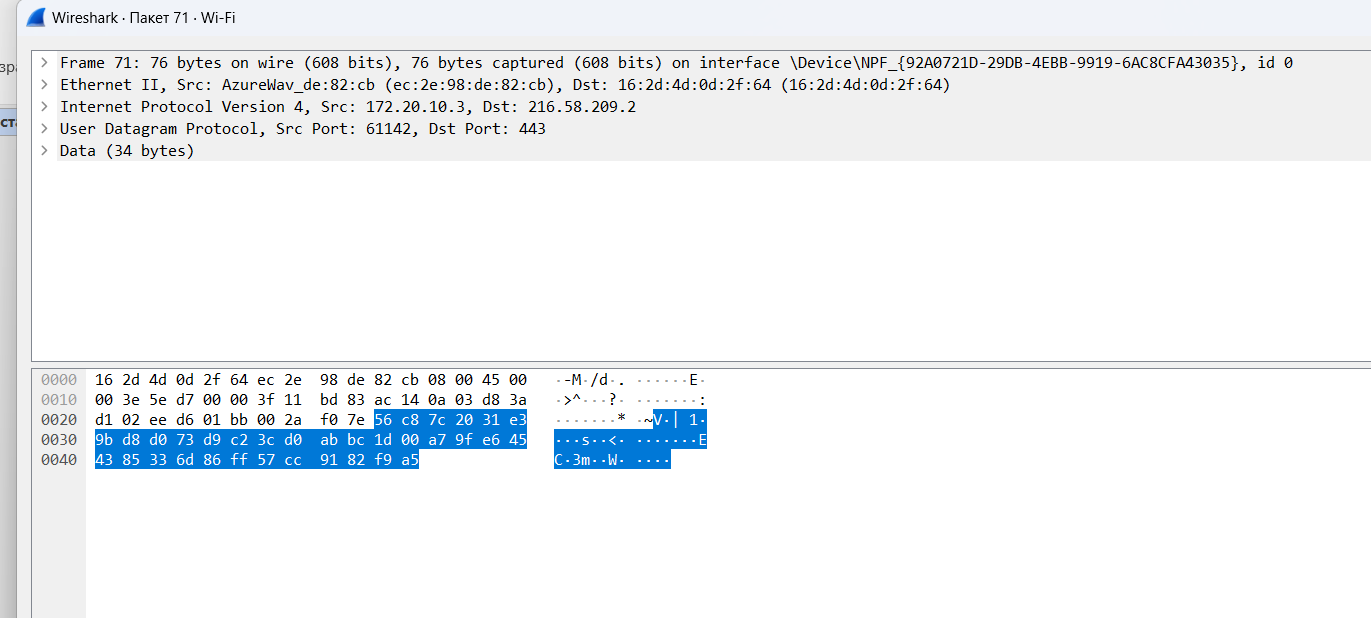


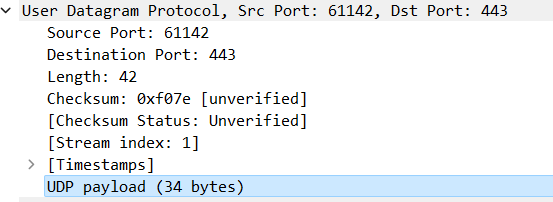
***Сама TCP:***

* 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 десятковій формі

**UDP**







Це короткий опис даних UDP-пакету:

- Порт відправника UDP-пакету: 61142.

- Порт одержувача UDP-пакету: 443 (зазвичай використовується для HTTPS-з'єднань).

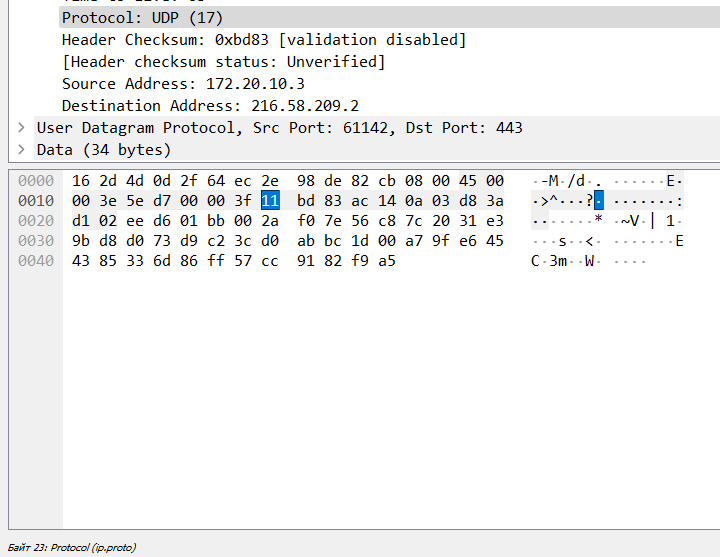
- Довжина UDP-пакету: 42 байти.

- Контрольна сума UDP-пакету: 0xf07e (Статус перевірки контрольної суми не підтверджено).

- Індекс потоку: 1.

- Навантаження UDP-пакету (34 байти): Дані, які передаються через UDP-з'єднання.

Цей опис надає загальну інформацію про UDP-пакет на основі доступних даних. Для детального аналізу UDP-пакету може знадобитися розгляд його вмісту, такого як IP-адреси та дані всередині навантаження UDP.



Ось короткий опис основних полів IP-заголовка для даного UDP-пакету:

* Протокол: UDP (User Datagram Protocol, номер 17).
* Фрагментація: Прапори фрагментації встановлені на "0", що свідчить про те, що цей UDP-пакет не фрагментований. Зміщення фрагмента дорівнює 0.
* Час життя (TTL): Значення часу життя пакета (TTL) становить 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 (валідація вимкнена).
* Адреса відправника: IP-адреса відправника пакета - 172.20.10.3.
* Адреса одержувача: IP-адреса одержувача пакета - 216.58.209.2.

Цей опис надає загальну інформацію про основні поля IP-заголовка для даного UDP-пакету. Зверніть увагу, що в цьому описі не включена інформація про вміст UDP-пакету, оскільки опис стосується лише полів IP-заголовка.