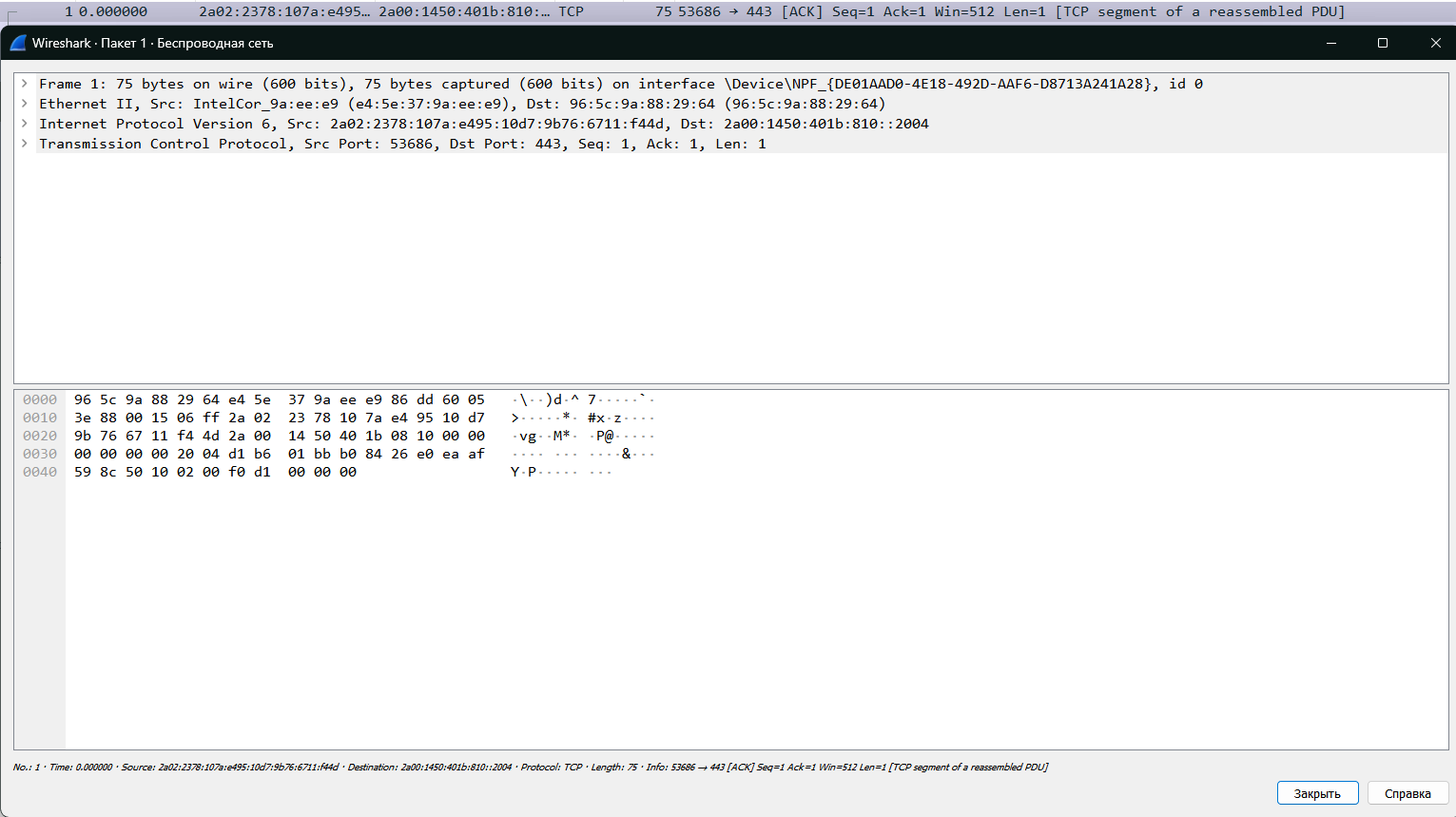
**Звіт**

Тема: Аналіз пакетів TCP (Transmission Control Protocol) та UDP (User Datagram Protocol)

Виконав: курсант С-04 групи Бондаренко О.Р

КИЇВ – 2023

TCP

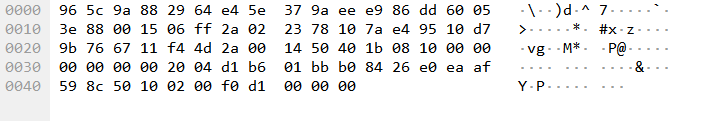


Значення полів у Frame 1, який був захоплений у Wireshark:

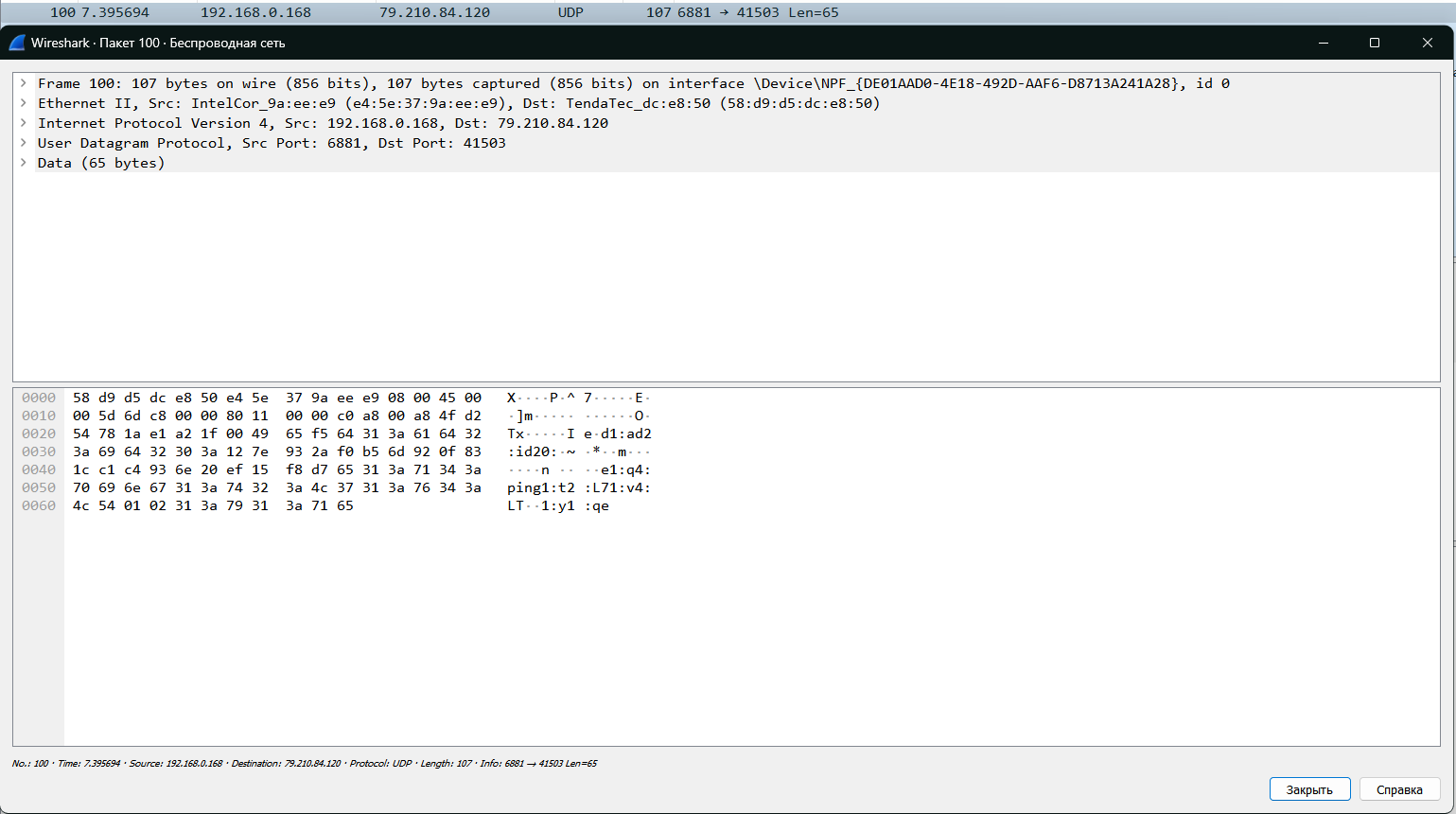
* Розмір пакету: 75 байт (600 біт)
* Ethernet II: DIX Ethernet використовується для передачі даних
* Src: e4:5e:37:9a:ee:e9 (IntelCor\_9a:ee:e9) – MAC-адреса відправника
* Dst: 96:5c:9a:88:29:64 – MAC-адреса отримувача
* Internet Protocol Version 6 (IPv6): протокол мережевої адресації
* Src: 2a02:2378:107a:e495:10d7:9b76:6711:f44d – IP-адреса відправника
* Dst: 2a00:1450:401b:810::2004 – IP-адреса отримувача
* TCP (Transmission Control Protocol): протокол транспортного рівня для надійної передачі даних у мережах.
* Src порт: 53686 відправника
* Dst порт: 443 отримувача

Цей пакет відображає початок комунікації між двома вузлами мережі. Відправник має IP-адресу 2a02:2378:107a:e495:10d7:9b76:6711:f44d, а отримувач - IP-адресу 2a00:1450:401b:810::2004. Комунікація відбувається через протокол TCP з використанням портів 63076 і 15154. У заголовку TCP вказано, що передаються дані, починаючи з послідовності номера 1 і маючи довжину 1 байт.

Шістнадцяткове представлення пакету:



UDP

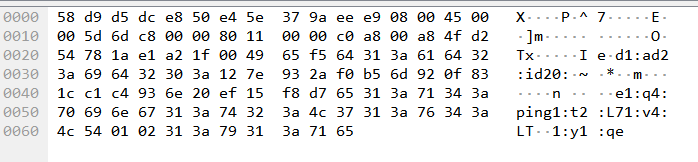


Internet Protocol Version 4, Src: 192.168.0.168, Dst: 79.210.84.120

Значення полів у Frame 100, який був захоплений у Wireshark:

* Розмір пакету: 107 байт (856 біт)
* Ethernet II: DIX Ethernet використовується для передачі даних
* Src: e4:5e:37:9a:ee:e9 (IntelCor\_9a:ee:e9) – MAC-адреса відправника
* Dst: 58:d9:d5:dc:e8:50 (TendaTec\_dc:e8:50) – MAC-адреса отримувача
* Internet Protocol Version 4 (IPv4): протокол мережевої адресації
* Src: 192.168.0.168– IP-адреса відправника
* Dst: 79.210.84.120 – IP-адреса отримувача
* UDP (User Datagram Protocol): протокол транспортного рівня для незабезпеченої передачі даних у мережах..
* Src порт: 6881
* Dst порт: 41503
* Data (65 bytes): в даному пакеті присутні дані загальним обсягом 65 байтів. Ця частина пакету відображає полезну навантаження або дані, які передаються через протокол UDP в мережі. Конкретний зміст цих даних може варіюватися в залежності від застосування або протоколу, який використовується поверх UDP..

Шістнадцяткове представлення пакету:



Основні відмінності між протоколами TCP (Transmission Control Protocol) та UDP (User Datagram Protocol) включають наступне:

1.Надійність доставки: TCP забезпечує надійну доставку даних шляхом встановлення з'єднання, впровадження механізму підтвердження отримання та автоматичного повторного надсилання в разі втрати пакетів.

2.Контроль потоку: TCP забезпечує контроль потоку, регулюючи швидкість передачі даних, щоб уникнути перевантаження мережі або отримувача.

3. TCP використовує послідовність номерів для ідентифікації та керування потоком даних. Кожен TCP-пакет має поле в заголовку, відоме як "номер послідовності"

4. TCP здійснює контроль обміну даними, що може зробити трафік меншим у порівнянні з UDP.

5. Затримка та ефективність: UDP має нижчу накладну частоту, оскільки не виконує додаткових механізмів надійності та контролю потоку, що робить його швидшим.

Відправка власного TCP пакету та захоплення його у Wireshark.

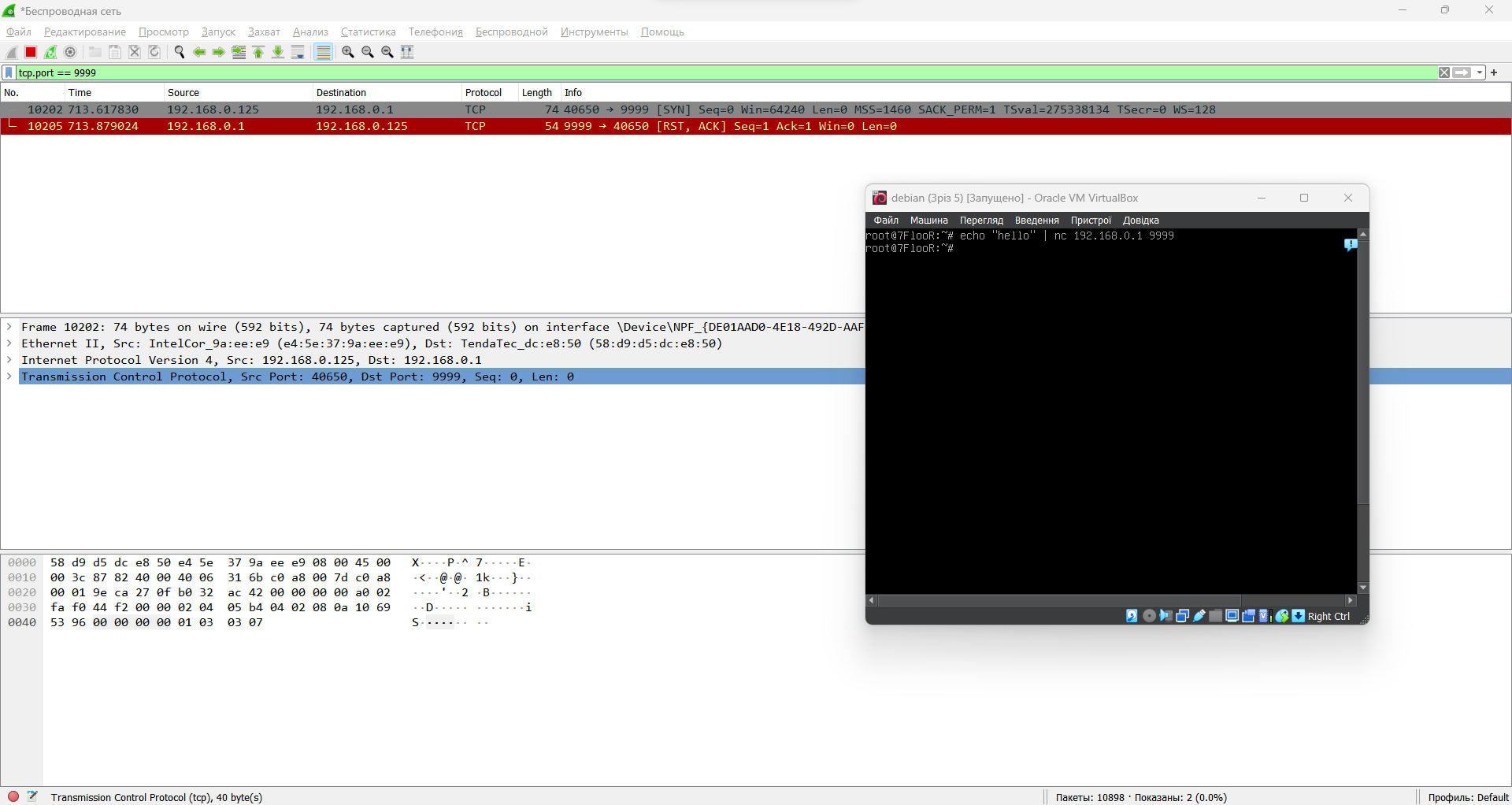
За допомогою фільтрів визначаємо порт 9999 для перехоплення в Wireshark



За допомогою netcat відправляємо пакет на IP адресу Windows та на порт 9999.



Після цього бачимо наші пакети

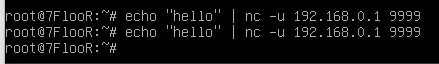


Відправка власного UDP пакету та захоплення його у Wireshark.

За допомогою фільтрів визначаємо порт 9999 для перехоплення в Wireshark



За допомогою netcat відправляємо пакет на IP адресу Windows та на порт 9999.



Після цього бачимо наші пакети

