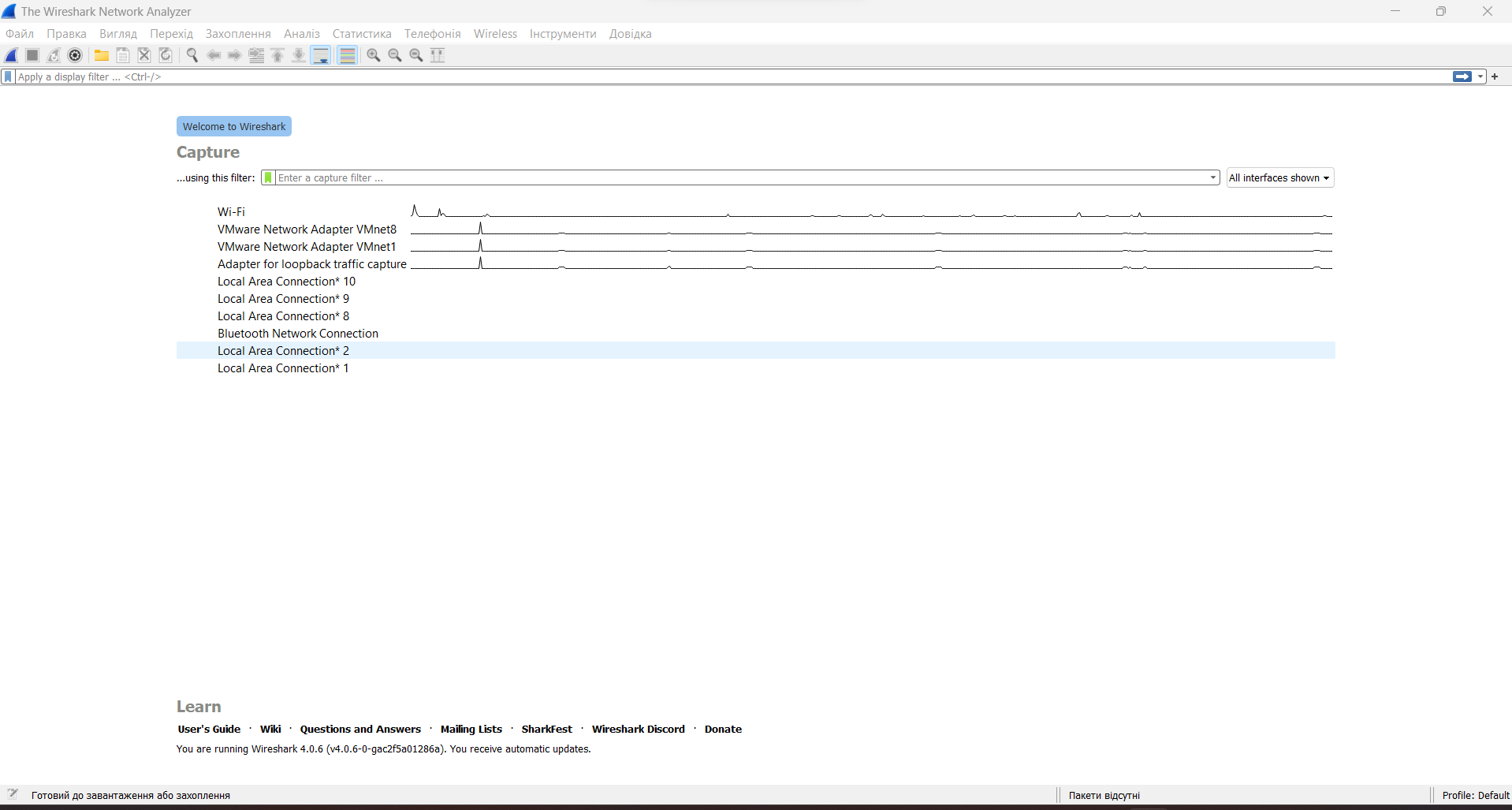
**Wireshark**

Підготував курсант групи С-05 Бойко Наталія

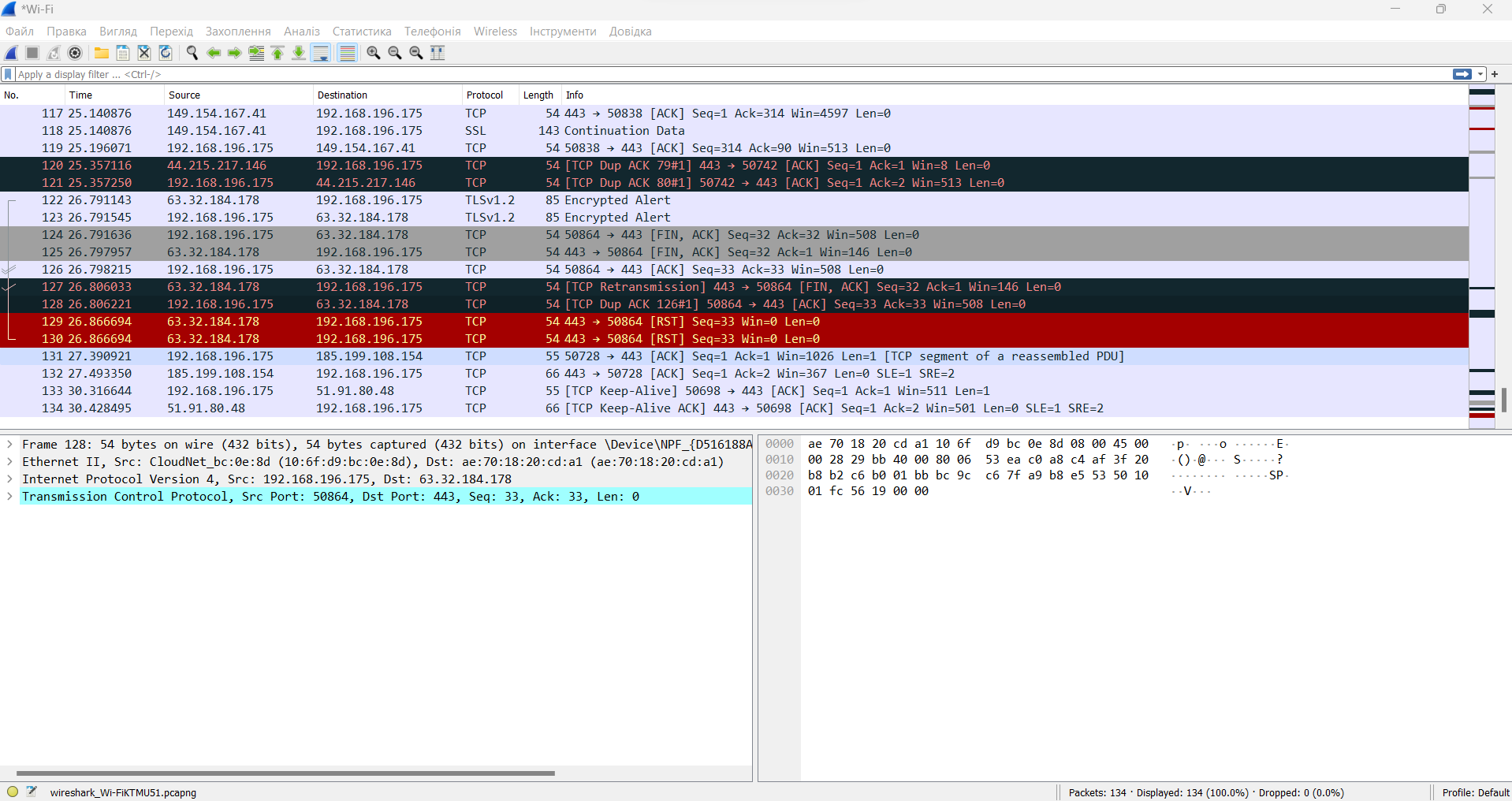
Початок роботи



Після встановлення та запуску програми можна побачити загальний інтерфейс програми.

Тут ви побачите список мережевих інтерфейсів, доступних на комп'ютері користувача. На цьому комп'ютері їх дев'ять. Графік праворуч від назви показує, які інтерфейси в даний момент надсилають і приймають пакети даних. Наразі ми розглянемо бездротову мережу (WIFI).

Загальний інтерфейс



TCP (протокол управління передачею)

Протокол управління передачею (TCP) - один з основних протоколів передачі даних у комп'ютерних мережах. Він забезпечує надійну та безперебійну передачу даних між пристроями в Інтернеті.

Основними характеристиками TCP є:

1. 1. надійність: TCP забезпечує надійну передачу даних. Він використовує механізми підтвердження і повторної передачі, щоб гарантувати, що дані будуть доставлені без втрат і збоїв.

2. 2. з'єднання: TCP встановлює з'єднання між відправником і одержувачем перед передачею даних. Це з'єднання дозволяє обом пристроям синхронізуватися та обмінюватися інформацією про передачу даних.

3. 3. Контроль потоку: TCP використовує вікна передачі для контролю потоку даних. Відправник не надсилає дані швидше, ніж одержувач може їх обробити, таким чином уникаючи перевантажень і втрати даних.

4. 4. Контроль помилок: TCP містить механізми для виявлення та виправлення помилок при передачі даних. Контрольні суми можуть бути використані для перевірки цілісності даних і відновлення втрачених або пошкоджених пакетів.

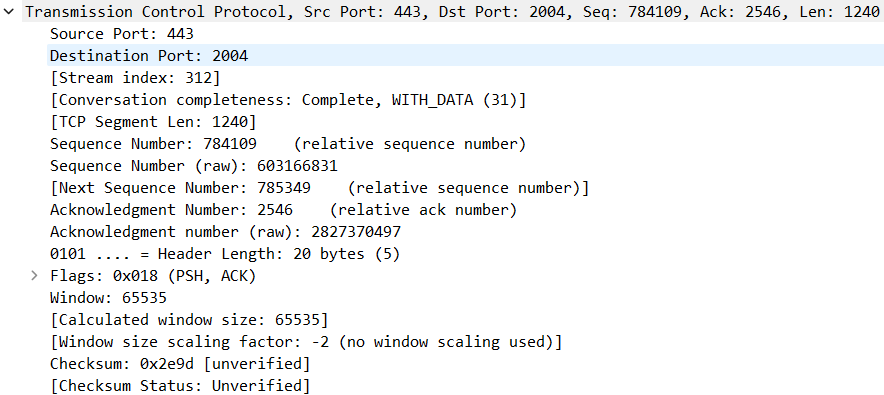
5. 5. орієнтований на потік: TCP розбиває передачу даних на потоки байтів, що дозволяє передавати дані навіть тоді, коли мережеві шляхи та умови обробки змінюються.

6. 6. пунктуація: TCP додає заголовок до кожного пакету даних, щоб одержувач міг правильно зібрати отримані пакети.

7. TCP використовує систему портів для ідентифікації програм, що взаємодіють через нього. Кожна програма може мати унікальний номер порту на стороні відправника та отримувача, що дозволяє TCP правильно адресувати дані.

TCP є одним з основних протоколів в Інтернеті і використовується багатьма програмами, такими як веб-браузери, електронна пошта, передача файлів та інші мережеві сервіси, де важлива надійність і порядок передачі даних.

Заголовок TCP



1. Порт відправника (16 біт): Вказує номер порту відправника даних.
2. Порт отримувача (16 біт): Вказує номер порту отримувача, до якого адресовані дані.
3. Послідовний номер (32 біти): Використовується для впорядкування та відновлення пакетів на стороні отримувача.
4. Номер підтвердження (32 біти): Вказує на наступний очікуваний номер послідовного байту, який отримувач очікує від відправника.
5. Довжина заголовка (4 біти): Вказує довжину заголовка TCP.
6. Флаги (6 біт): Використовуються для керування з'єднанням, наприклад, для встановлення, підтвердження або закриття з'єднання.
7. Вікно (16 біт): Визначає кількість байтів, які отримувач може приймати, перед тим як вимагати підтвердження.
8. Контрольна сума (16 біт): Використовується для перевірки цілісності даних в заголовку та тілі пакета.
9. Важливість та пріоритет (3 біти): Використовується для встановлення пріоритету пакета.
10. Відстежування з'єднання (32 біти): Використовується для відстеження стану з'єднання, зокрема для керування потоком даних.

UDP

User Datagram Protocol (UDP) - це протокол передачі даних для комп'ютерних мереж. Він забезпечує простий і швидкий спосіб передачі даних без забезпечення надійності або з'єднання.

Основними особливостями UDP є

1. він не потребує з'єднання: UDP передає дані без встановлення та керування з'єднанням між відправником та отримувачем. Тому він характеризується високою швидкістю і низькими мережевими накладними витратами.

2. ненадійний протокол UDP не передбачає механізмів підтвердження, повторної передачі або контролю потоку даних. Це може призвести до втрати або неправильної передачі даних без автоматичної корекції.

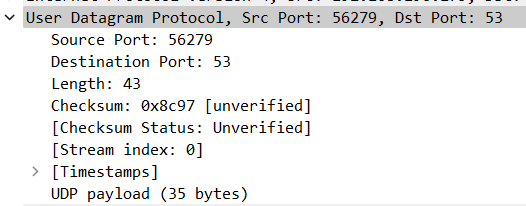
3. мінімальний заголовок: UDP має простий заголовок, що складається з 8 байт. Цей заголовок містить таку інформацію, як порти джерела та призначення, довжина дейтаграми та контрольна сума.

4. відсутність контролю потоку: в UDP немає вбудованого механізму контролю потоку даних. Це означає, що відправники можуть надсилати дані швидше, ніж одержувач може їх обробити, що може призвести до втрати даних і перевантаження одержувача.

5. використання в режимі реального часу UDP часто використовується в додатках, де швидкість і низька затримка є важливими, наприклад, у додатках для передачі відео та голосу в режимі реального часу.

UDP є менш складним протоколом, ніж TCP, і тому найкраще підходить для ситуацій, коли надійність доставки не критична, але важлива швидкість і ефективність передачі даних При використанні UDP розробникам додатків може знадобитися реалізувати управління надійністю, перевірку цілісності і повторну передачу даних, якщо це потрібно для конкретного додатка Необхідно впровадити додаткові механізми.

Заголовок UDP



1. відправника (16 біт): Вказує номер порту відправника даних.
2. Порт отримувача (16 біт): Вказує номер порту отримувача, до якого адресовані дані.
3. Довжина (16 біт): Вказує загальну довжину пакета, включаючи заголовок та дані.
4. Порт Контрольна сума заголовку (16 біт): Використовується для перевірки цілісності даних в пакеті.

Порівняння TCP та UDP

TCP (Transmission Control Protocol) та UDP (User Datagram Protocol) - це два основних протоколи передачі даних в комп'ютерних мережах. Вони використовуються для передачі пакетів даних між пристроями, але мають деякі суттєві відмінності.

Основні відмінності між TCP та UDP:

1 Надійність передачі: TCP забезпечує надійну передачу даних. Він гарантує, що дані будуть доставлені відправнику без втрати, дублювання або порушення порядку. UDP, натомість, не забезпечує надійності передачі. Він може втрачати пакети або доставляти їх не в тому порядку, в якому вони були відправлені.

2 Контроль з'єднання: TCP встановлює з'єднання між відправником і отримувачем перед передачею даних. Він використовує трьохв'язкове рукостискання (three-way handshake) для встановлення з'єднання та використовує потокову модель передачі даних. UDP не використовує з'єднання та працює на основі безз'єднаної моделі, кожен пакет розглядається як окреме повідомлення.

3 Контроль помилок: TCP використовує механізми виявлення та виправлення помилок, такі як перевірка суми контролю (checksum) та повторна передача пакетів, які були пошкоджені або втрачені. UDP не має вбудованих механізмів виправлення помилок, і якщо пакет втрачений або пошкоджений, він просто відкидається.