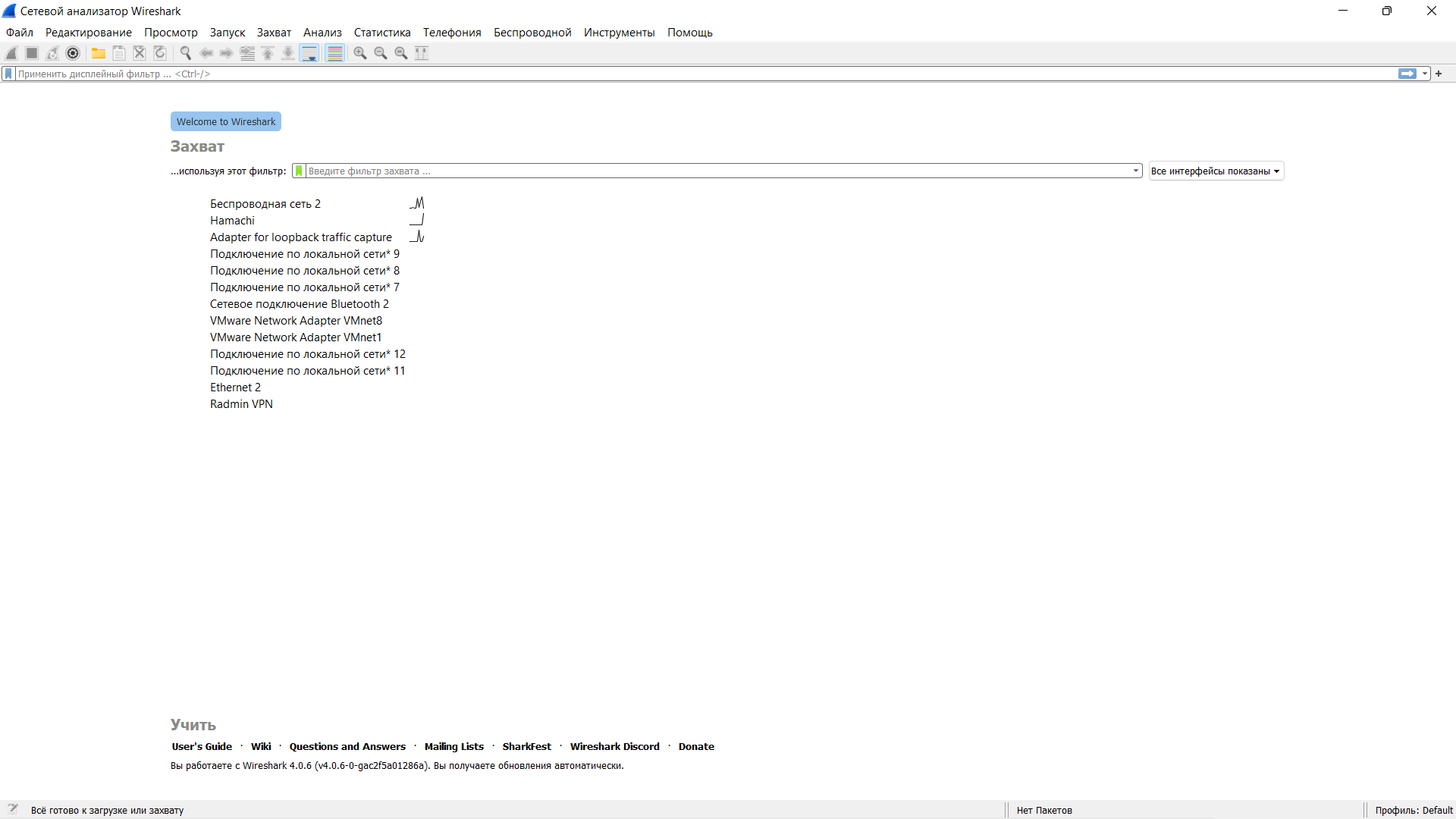
**Програма-аналізатор Wireshark**

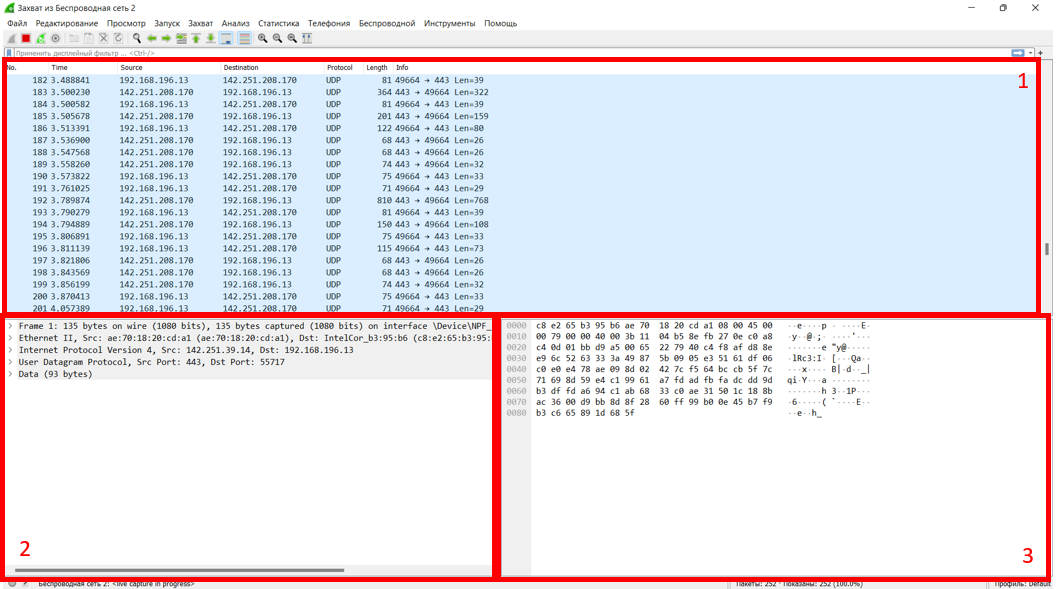
Підготував курсант групи С-05 Остапенко Максим

Початок роботи



Після встановлення та запуску програми, загальний інтерфейс програми стає доступним. Тут можна переглянути перелік мережевих інтерфейсів, які присутні на комп'ютері користувача. На цьому конкретному комп'ютері їх кількість становить 13. За допомогою графіків, розташованих праворуч від назв, можна візуально визначити, які інтерфейси наразі передають та отримують пакети даних. Зараз розглядатиметься бездротова мережа (Wi-Fi).

Загальний інтерфейс



Після запуску бездротової мережі можна побачити три розділи:

Після активації бездротової мережі, з'являються три розділи:

1. "Packet List" (Список пакетів): В цьому розділі відображаються пакети, що передаються з нашого комп'ютера у мережу та надходять з неї. Кожен пакет має такі характеристики:

а) No.: номер пакету.

б) Time: час, що пройшов від моменту захоплення першого пакету (наприклад, пакет №184 був захоплений через 3.5 секунди після пакету №1). Цей параметр можна налаштувати щодо формату та точності відображення.

в) Source: IP-адреса або ідентифікатор джерела, з якого відправлено пакет.

г) Destination: IP-адреса або ідентифікатор призначення, до якого адресовано пакет.

д) Protocol: протокол, використовуваний для передачі/прийому даних.

е) Length: загальна довжина пакета у байтах.

є) Info: коротке описове повідомлення, яке надає інформацію про пакет, таку як назву протоколу, виконувану дію або додаткові деталі.

2. "Packet Details" (Деталі пакета): У цьому розділі можна побачити докладну інформацію про вибраний пакет зі списку. Розділ містить розширену інформацію про пакет, яка залежить від протоколу та типу пакета. Його складові включають:

а) Frame: загальна інформація про фізичний кадр, така як номер кадру, довжина, індекс маскування та інші параметри.

б) Ethernet: якщо пакет використовує протокол Ethernet, то цей розділ показує деталі, пов'язані з Ethernet-заголовком, такі як MAC-адреси джерела та призначення, тип фрейму тощо.

в) Internet Protocol: надає деталі про IP-заголовок, включаючи версію IP, дж

ерело та призначення IP-адреси, TTL (Time to Live), тип служби тощо.

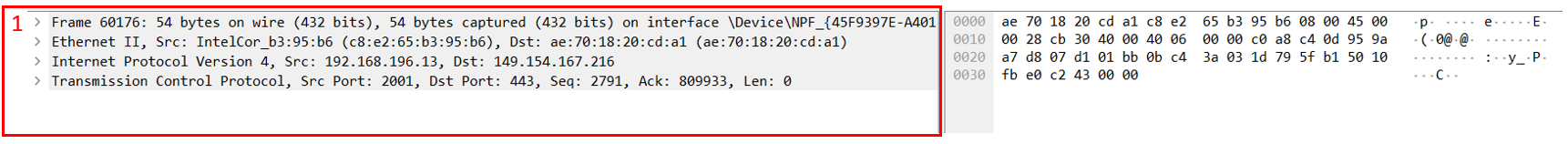
г) Transmission Control Protocol: якщо пакет використовує TCP, то цей розділ показує додаткову інформацію про TCP-заголовок, таку як порти джерела та призначення, номери послідовностей, прапорці, контрольна сума тощо.

д) User Datagram Protocol: для пакетів, що використовують UDP, цей розділ відображає інформацію про UDP-заголовок, таку як порти джерела та призначення, довжину дейтаграми, контрольну суму тощо.

е) Data: вміст самого пакета, що передається по мережі. Цей розділ показує біти або октети, що складають пакет, і відображає їх у різних форматах.

3. "Packet Bytes" (Байти пакета): У цьому розділі відображається шістнадцяткове представлення байтів вибраних пакетів. Кожен байт пакета представлений двома шістнадцятковими цифрами. Це дозволяє детально переглядати та аналізувати вміст пакета на нижньому рівні.

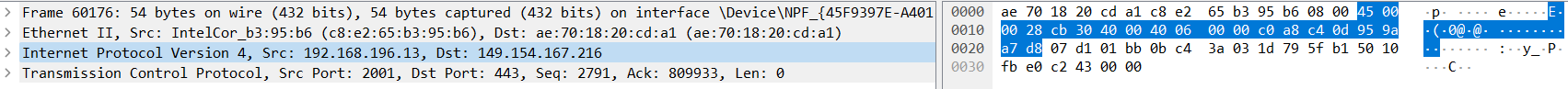
Розбір конкретного пакету



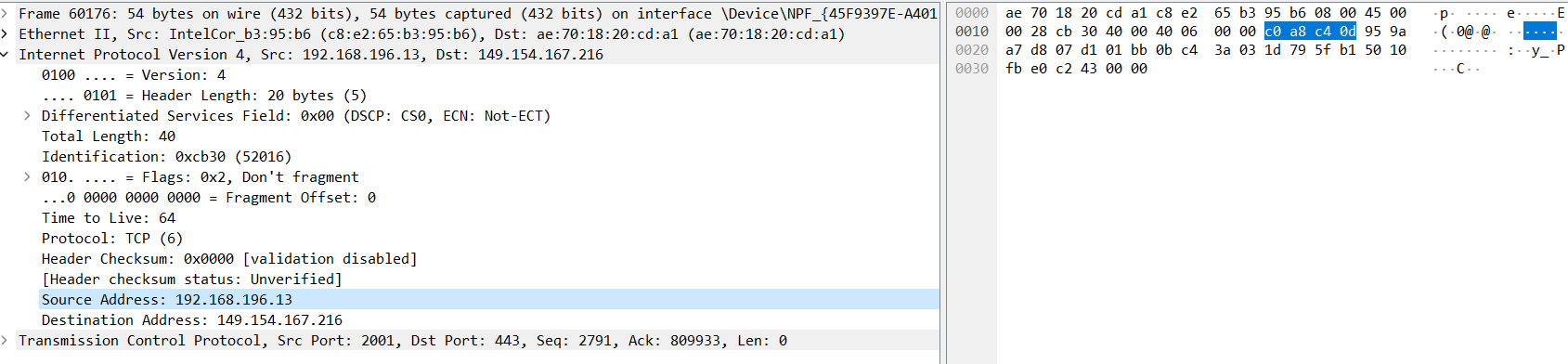
Для прикладу було взято випадковий пакет даних.

На зображенні 1 представлені заголовки протоколів різних рівнів. Frame є фізичним рівнем. Ethernet II протокол канального рівня. Internet Protocol мережевого рівня. TCP транспортного рівня.

Коли вибраний якийсь протокол то його заголовок в розділі "Packet Details" підсвічується



В разі якщо потрібно більш детальна інформація щодо певного протоколу, то його можна знайти всередині(наприклад потрібна IP-адреса відправника) та після вибору буде підсвічена відповідна частина в розділі "Packet Details".



TCP

TCP, відомий як Transmission Control Protocol (протокол керування передачею), є одним з основних протоколів, що використовуються для передачі даних в комп'ютерних мережах. Він забезпечує надійну та з'єднану передачу даних між пристроями у мережі Інтернет.

Основні характеристики TCP:

1. Надійність: TCP забезпечує надійну передачу даних, використовуючи підтвердження та повторну відправку, щоб гарантувати, що дані доставляються без втрати або порушення порядку.

2. З'єднання: TCP встановлює з'єднання між відправником та отримувачем перед передачею даних. Це з'єднання дозволяє пристроям синхронізуватись та обмінюватись інформацією про передачу даних.

3. Контроль потоку: TCP використовує вікна передачі для контролю потоку даних. Відправник не передає дані швидше, ніж може обробити отримувач, що допомагає уникнути перевантаження та втрати даних.

4. Контроль помилок: TCP має механізми виявлення та виправлення помилок у передачі даних. Він використовує контрольну суму для перевірки цілісності даних та може відновлювати втрачені або пошкоджені пакети.

5. Орієнтованість на поток: TCP розбиває передачу даних на потоки байтів, що дозволяє передавати дані в умовах змінного мережевого шляху та обробки.

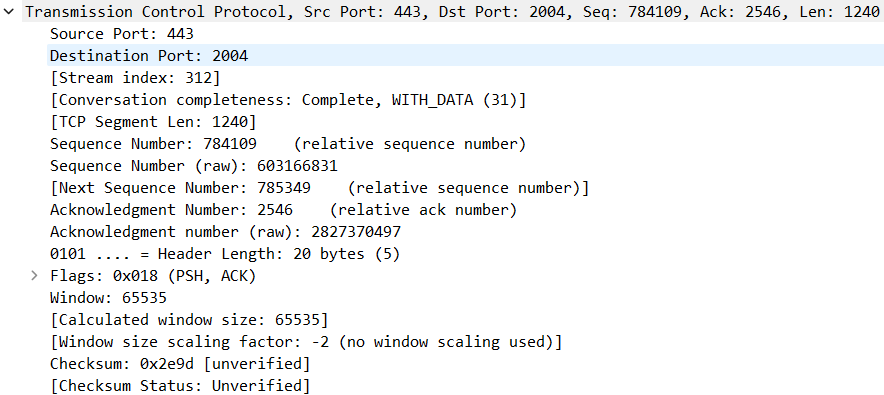
6. Пунктуація: TCP додає заголовки до кожного пакету даних, що допомагає отримувачу правильно скласти отримані пакети.

7. Використання системи портів: TCP використовує систему портів для ідентифікації додатків

, які спілкуються через нього. Кожен додаток може мати унікальний номер порту на відправнику та отримувачу, що дозволяє TCP правильно адресувати дані.

TCP є одним з основних протоколів в Інтернеті і застосовується у багатьох сферах, таких як веб-браузери, електронна пошта, передача файлів та інші мережеві служби, де надійність та порядок передачі даних є важливими.

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

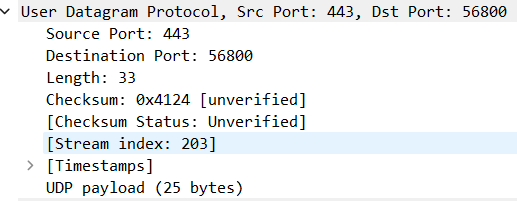
UDP (User Datagram Protocol) є протоколом передачі даних у комп'ютерних мережах. Він надає простий та швидкий спосіб передачі даних без забезпечення надійності та з'єднання.

Основні риси UDP:

1. Без з'єднання: UDP передає дані без встановлення та управління з'єднанням між відправником та отримувачем. Це робить його швидким та малопомітним з точки зору накладних витрат мережі.
2. Ненадійний протокол: UDP не забезпечує механізми підтвердження, повторної передачі чи управління потоком даних. Це означає, що втрати даних або порушення порядку можуть відбуватися без автоматичної корекції.
3. Мінімальний заголовок: UDP має простий заголовок, що складається з 8 байтів. Він містить інформацію про порти джерела та призначення, довжину дейтаграми та контрольну суму.
4. Без управління потоком: UDP не має вбудованих механізмів управління потоком даних. Це означає, що відправник може передавати дані швидше, ніж їх може обробити отримувач, що може призводити до втрати даних або перевантаження отримувача.
5. Використання в реальному часі: UDP часто використовується в застосунках, де важлива швидкість та низька затримка передачі даних, наприклад, відео- та голосових додатках у реальному часі.

UDP є менш складним протоколом порівняно з TCP, і він найбільш підходить для ситуацій, де надійність доставки не є критичною, а важлива швидкість та ефективність передачі даних. Використання UDP вимагає від розробників додатків додаткових механізмів для управління надійністю, перевірки цілісності та повторної передачі даних, якщо це необхідно для конкретного застосування.

Заголовок UDP



1. Порт 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. 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) є двома різними протоколами передачі даних у комп'ютерних мережах. Ось декілька ключових відмінностей між ними:

1. Надійність передачі: TCP забезпечує надійну передачу даних, оскільки він включає механізми підтвердження, повторної передачі та контролю помилок. У випадку втрати пакетів або пошкодження даних, TCP автоматично повторно відправляє втрачені пакети, забезпечуючи доставку даних у правильному порядку. З іншого боку, UDP не забезпечує надійності передачі даних, що означає, що він може втрачати пакети або передавати їх у неправильному порядку без автоматичної корекції.
2. З'єднання: TCP встановлює з'єднання між відправником та отримувачем перед передачею даних. Це з'єднання дозволяє обом пристроям синхронізуватися та обмінюватися інформацією про передачу даних. У випадку UDP з'єднання не встановлюється, і кожен пакет розглядається окремо.
3. Накладні витрати: TCP має більшу накладну частоту у порівнянні з UDP. Це пов'язано з додатковими механізмами, такими як контроль підтверджень, повторна передача та управління потоком. UDP, натомість, має меншу накладну частоту, оскільки йому не потрібно виконувати складні механізми, що забезпечують надійність.
4. Використання в застосунках: TCP широко використовується в застосунках, де надійність передачі та гарантія порядку даних є критичними, таких як веб-сторінки, електронна пошта, передача файлів тощо. UDP використовується в застосунках, де швидкість та ефективність передачі даних мають більший пріоритет, наприклад, відео- та голосових додатках у реальному часі.
5. Розмір заголовків: Заголовок TCP має більший розмір порівняно з заголовком UDP. Це пов'язано з додатковими полями, що використовуються для контролю потоку, номерів підтвердження, управління вікном тощо. Заголовок UDP є простішим та має менший розмір.

Вибір між TCP та UDP залежить від конкретних потреб застосування. Якщо важлива надійність, гарантія порядку та контроль над передачею даних, то TCP може бути кращим вибором. У випадку, коли пріоритет має швидкість, ефективність та низька затримка передачі даних, UDP може бути більш підходящим протоколом.