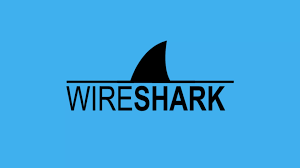
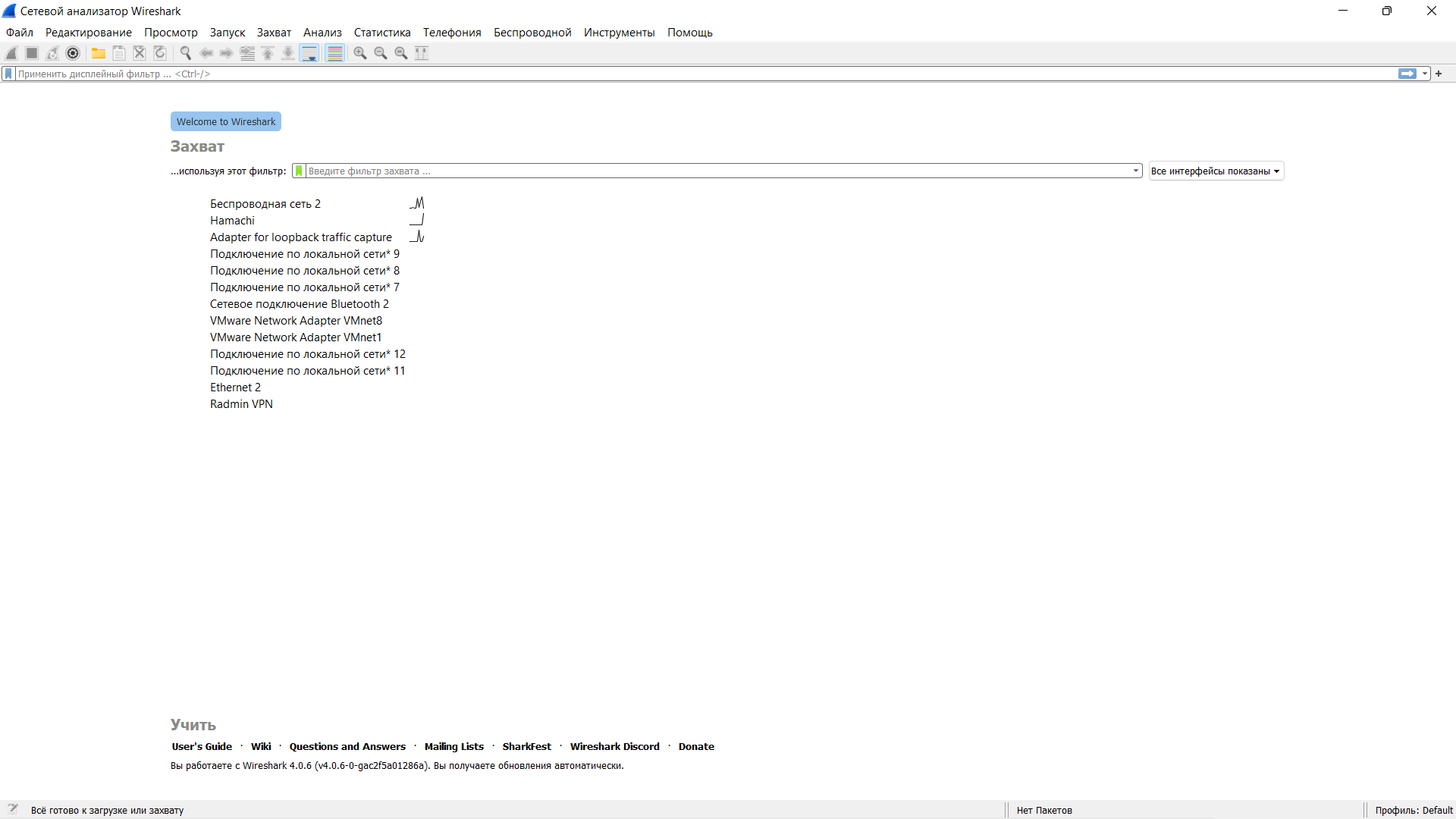
**Програма-аналізатор Wireshark**

Підготував сержант групи С-05 Майстренко Влад



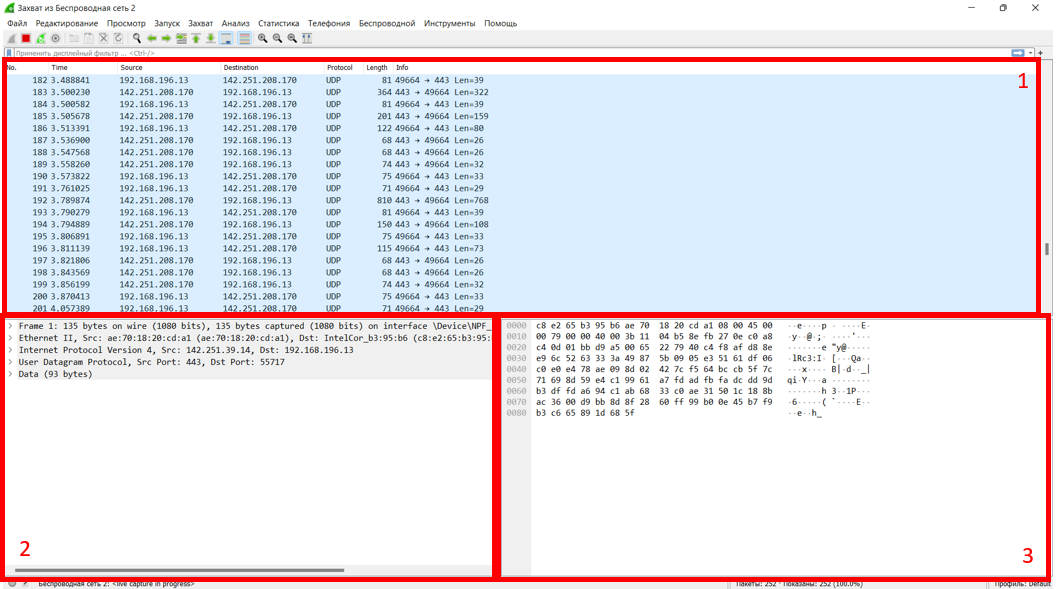
Початок роботи



Після установки та запуску програми можна побачити загальний інтерфейс програми.

Тут можна побачити список мережевих інтерфейсів які є на комп’ютері користувача. На даному комп’ютері їх 13. По графікам справа від назв можна побачити які інтерфейси на даний момент передають та приймають пакети даних. На даний момент буде розглядатися бездротова мережа(wifi).

Загальний інтерфейс



Після запуску бездротової мережі можна побачити три розділи:

1. В даному розділі показані пакети, які передаються з нашого комп’ютера в мережу та приймаються з неї відповідно. Дані в пакеті мають таку класифікацію:

а) No.: номер пакету

б) Time: в даному випадку показується час з моменту захоплення першого пакету(напр. пакет №184 був захоплений через 3.5 секунди після пакету №1). Цей пункт можна змінити в налаштуваннях, як формат так і параметри точності відображення.

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

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

д) Protocol: протокол, за допомогою якого надсилаються/приймаються дані.

е) Length: загальна довжина пакету в байтах.

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

1. Розділ називається "Packet Details" (Деталі пакета). В цьому розділі можна побачити докладну інформацію про обраний пакет, який був вибраний у списку пакетів. Цей розділ містить розширені відомості про пакет, які можуть включати різноманітну інформацію, залежно від протоколу і типу пакета.

Дані в пакеті мають таку класифікацію:

а)Frame: надає загальну інформацію про фізичний кадр, таку як номер кадру, довжина, індекс маскування (masking bit), та інші параметри.

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

в)Internet Protocol: відображає деталі про IP-заголовок, включаючи версію IP, джерело та призначення IP-адреси, TTL (Time to Live), тип служби тощо.

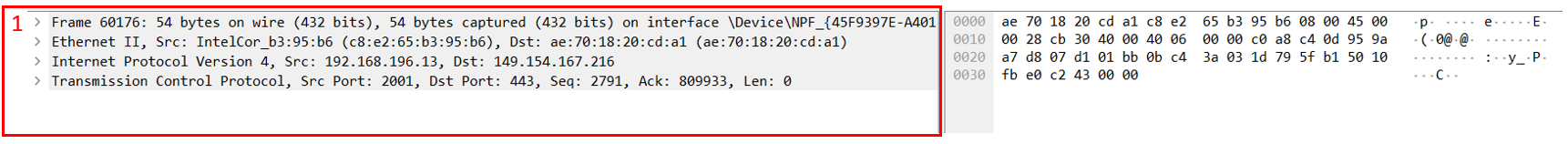
г)Transmission Control Protocol: якщо пакет використовує TCP, то цей розділ показує додаткові відомості про TCP-заголовок, такі як порти джерела та призначення, номери послідовностей, прапорці, контрольна сума тощо.

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

e)Data: відповідає за вміст самого пакету, який був переданий через мережу. Цей розділ показує рівень бітів або октетів, що складають пакет, і відображає його у різних форматах.

1. Розділ називається "Packet Bytes". Цей розділ відображає шістнадцяткове представлення байтів обраних пакетів. Кожен байт пакета відображається двома шістнадцятковими цифрами. Це дозволяє детально переглядати і аналізувати вміст пакета на нижньому рівні.

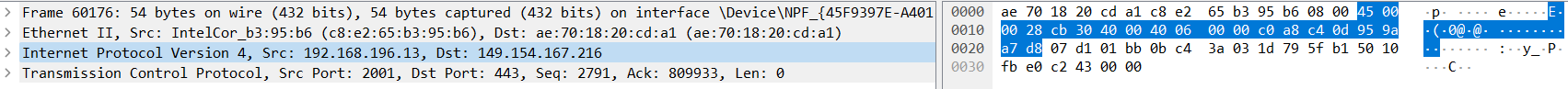
Розбір конкретного пакету



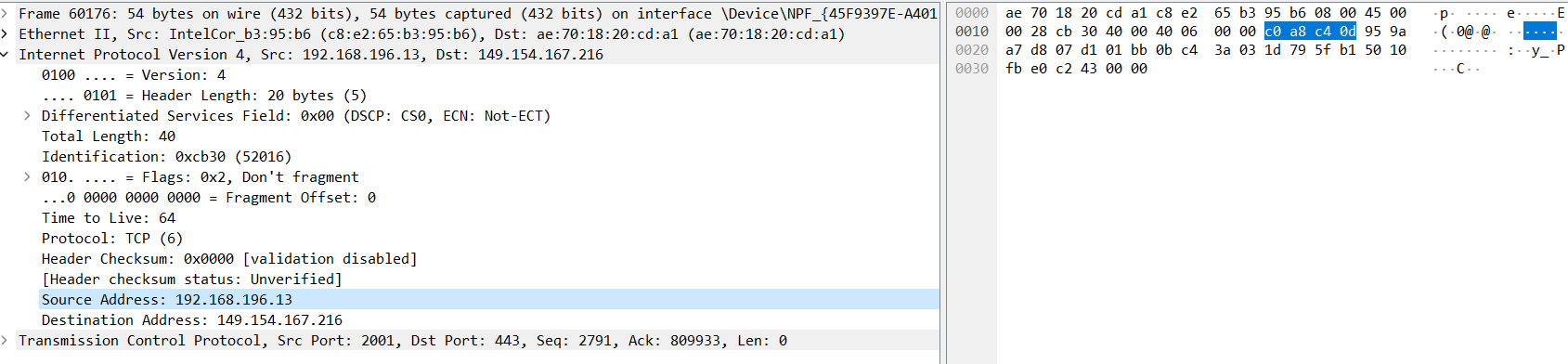
Для прикладу було взято випадковий пакет даних.

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

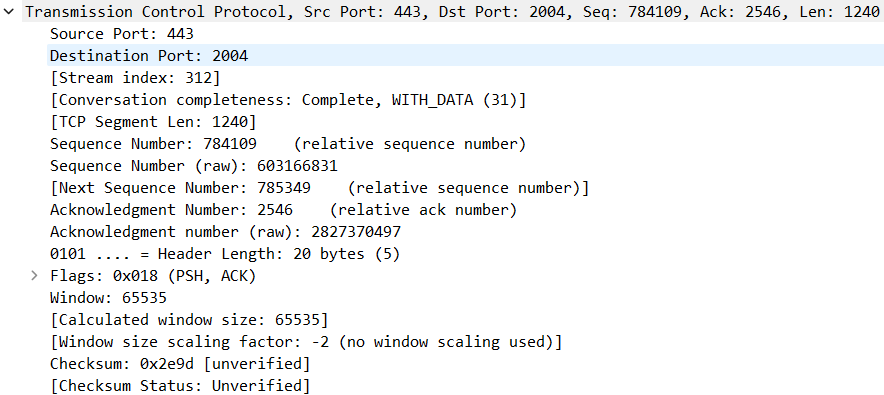
TCP (Transmission Control Protocol) є одним з основних протоколів передачі даних в комп'ютерних мережах. Він забезпечує надійну та з'єднану передачу даних між пристроями у мережі Інтернет.

Основні риси TCP:

1. 1.Надійність: TCP забезпечує надійну передачу даних. Він використовує механізми підтвердження та повторних відправок, щоб гарантувати, що дані доставлені без втрати або порушення порядку.
2. 2.З'єднання: TCP встановлює з'єднання між відправником та отримувачем перед передачею даних. Це з'єднання дозволяє обом пристроям синхронізуватись та обмінюватись інформацією про передачу даних.
3. 3.Контроль потоку: TCP використовує вікна передачі для контролю потоку даних. Відправник не передає дані швидше, ніж може обробити отримувач, що дозволяє уникнути перевантаження та втрати даних.
4. 4.Контроль помилок: TCP включає механізми виявлення та виправлення помилок у передачі даних. Він використовує контрольну суму для перевірки цілісності даних та може відновлювати втрачені або пошкоджені пакети.
5. 5.Орієнтованість на поток: TCP розбиває передачу даних на потоки байтів, що дозволяє передавати дані в умовах змінного мережевого шляху та обробки.
6. 6.Пунктуація: TCP додає заголовки до кожного пакету даних, що дозволяє отримувачу правильно скласти отримані пакети.
7. 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 та використовується в багатьох застосунках, таких як веб-браузери, електронна пошта, передача файлів та інші мережеві служби, де надійність та порядок передачі даних є критичними.

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

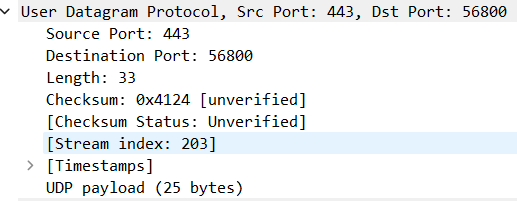
UDP (User Datagram Protocol) є протоколом передачі даних у комп'ютерних мережах. Він надає простий та швидкий спосіб передачі даних без забезпечення надійності та з'єднання.

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.