**Звіт**

Тема: Основи роботи з Wireshark. Аналіз пакетів

КИЇВ – 2023

**Зміст**

|  |  |
| --- | --- |
| **Вступ………………………………………………………………………..** | **3** |
| **Огляд робочого вікна…………………………………………………….** | **4** |
| **Приклади застосування………………………………………………….** | **5** |
| **Візуальне (кольорове) розрізнення……………………………………..** | **13** |
| **Пошук інформації………………………………………………………...** | **14** |
| **Статистика трафіку………………………………………………………** | **15** |
| **Висновок……………………………………………………………………** | **16** |

**Вступ**

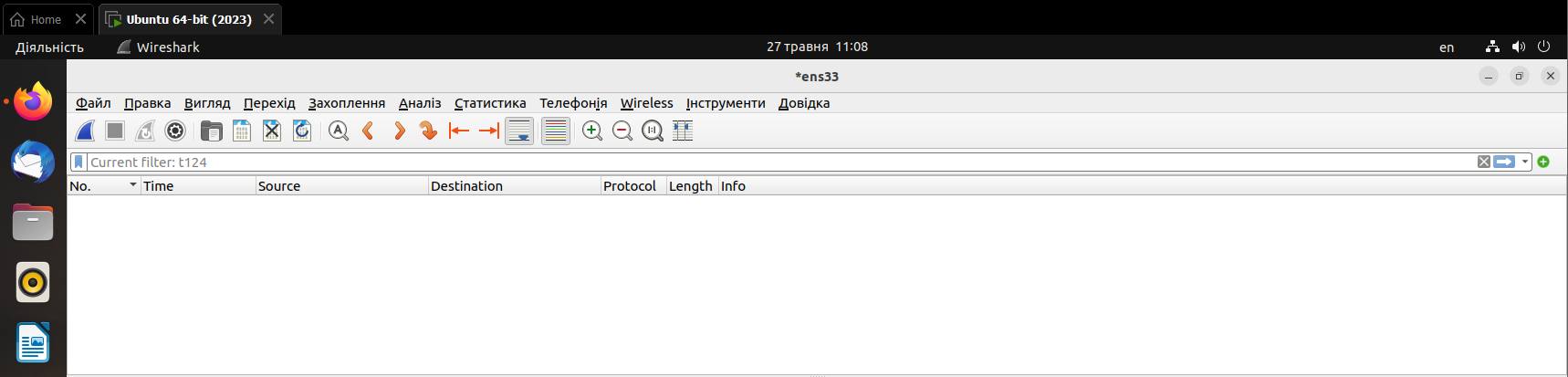
Wireshark є одним з найпопулярніших інструментів для аналізу мережевого трафіку. Він дозволяє захоплювати пакети даних, що пересилаються в мережі, та надає детальну інформацію про ці пакети, що допомагає зрозуміти, як працює ваша мережа і виявити можливі проблеми.

Основи роботи з Wireshark включають наступні етапи:

1. Захоплення пакетів: Wireshark дозволяє захоплювати пакети даних, які проходять через мережевий інтерфейс вашого комп'ютера. Ви можете вибрати конкретний інтерфейс для захоплення або використати опцію "Всі інтерфейси", щоб захопити пакети з усіх доступних інтерфейсів.
2. Аналіз пакетів: Після захоплення пакетів Wireshark відображає їх у вигляді таблиці з різними стовпцями, такими як номер пакету, час, джерело та призначення, протокол, довжина тощо. Ви можете аналізувати ці дані, фільтрувати пакети за різними критеріями та шукати певні події або проблеми.
3. Розшифрування зашифрованого трафіку: Wireshark може розшифрувати зашифрований трафік, такий як SSL або TLS, що дозволяє переглядати його в зрозумілому форматі. Для цього необхідно мати доступ до відповідних приватних ключів або налаштувати Wireshark для розшифрування.
4. Відображення графіків та статистики: Wireshark надає можливість відображати графіки та статистику зібраного трафіку. Графіки можуть показувати розмір пакетів, швидкість передачі даних, затримку тощо, що допомагає візуально аналізувати їх.

**Огляд робочого вікна**

Програма Wireshark є інструментом аналізу мережевого трафіку, який дозволяє перехоплювати та аналізувати пакети даних, що передаються через мережу.



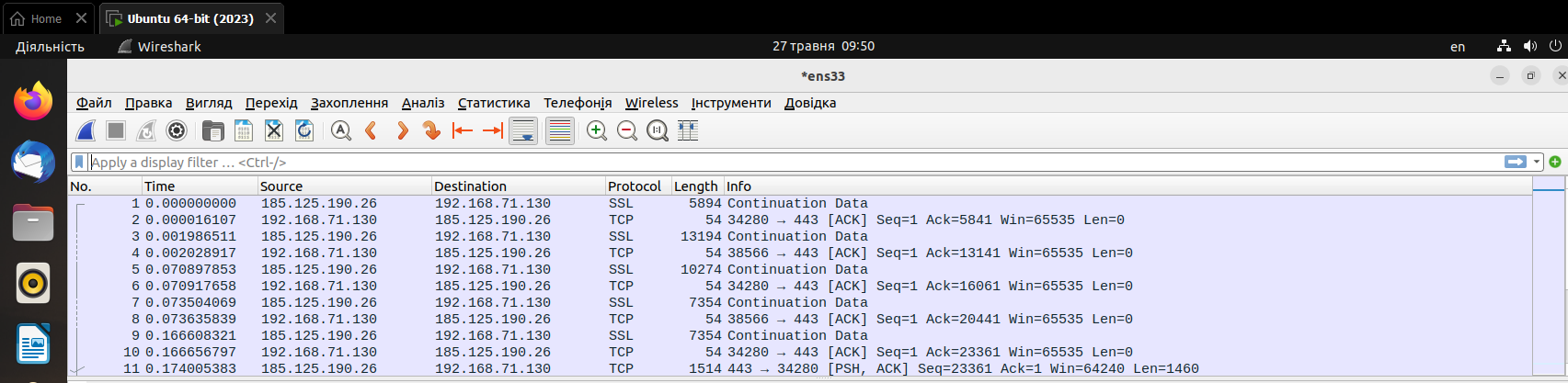
У таблиці Wireshark наведені різні стовпці, які містять інформацію про ці пакети. Ось означення кожного стовпця:

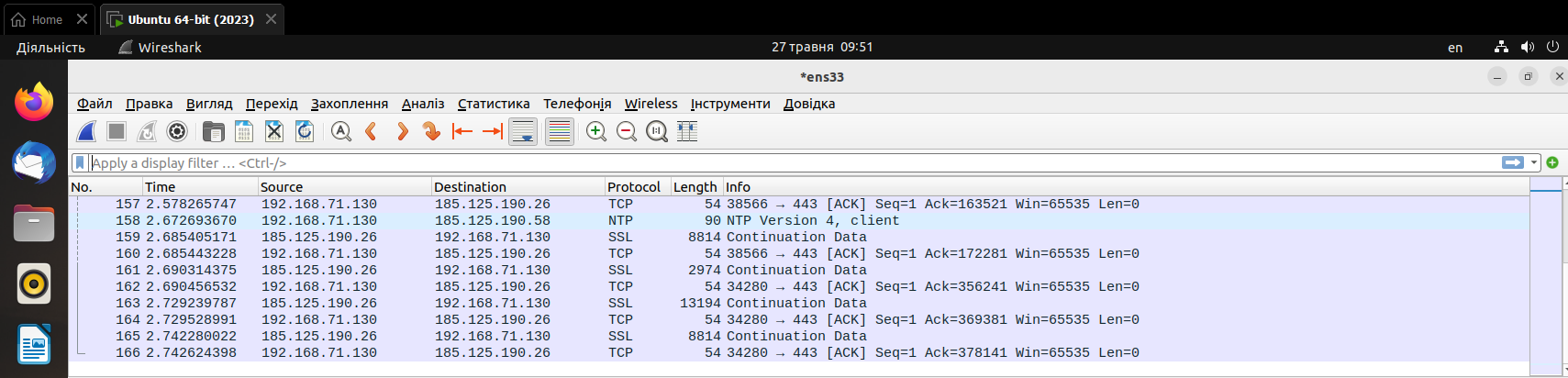
* No. (Номер): Це порядковий номер пакету в списку. Він вказує порядок, в якому пакети були перехоплені.
* Time (Час): Це часова мітка, коли пакет був перехоплений. Час може бути вказаний у форматі годин:хвилин:секунди або у більш детальному форматі, який включає мілісекунди або мікросекунди.
* Source (Джерело): Це IP-адреса або ім'я джерела, з якого був відправлений пакет. Він вказує на те, звідки походить пакет.
* Destination (Призначення): Це IP-адреса або ім'я призначення, до якого був направлений пакет. Він вказує на те, куди був адресований пакет.
* Protocol (Протокол): Це протокол мережевого рівня, який використовується для передачі пакету. Наприклад, це може бути TCP, UDP, HTTP, ICMP і т. д.
* Length (Довжина): Це довжина пакету в байтах. Він вказує на кількість байтів, які містяться в пакеті.
* Info (Інформація): Це короткий опис або заголовок пакету. Ця інформація може містити додаткові деталі про тип пакету, його джерело та призначення, можливі помилки або подібні важливі дані.

Всі ці стовпці надають корисну інформацію для аналізу мережевого трафіку та вивчення взаємодії між пристроями в мережі.

**Приклади застосування**

Загалом маємо перехоплених 166 пакетів.





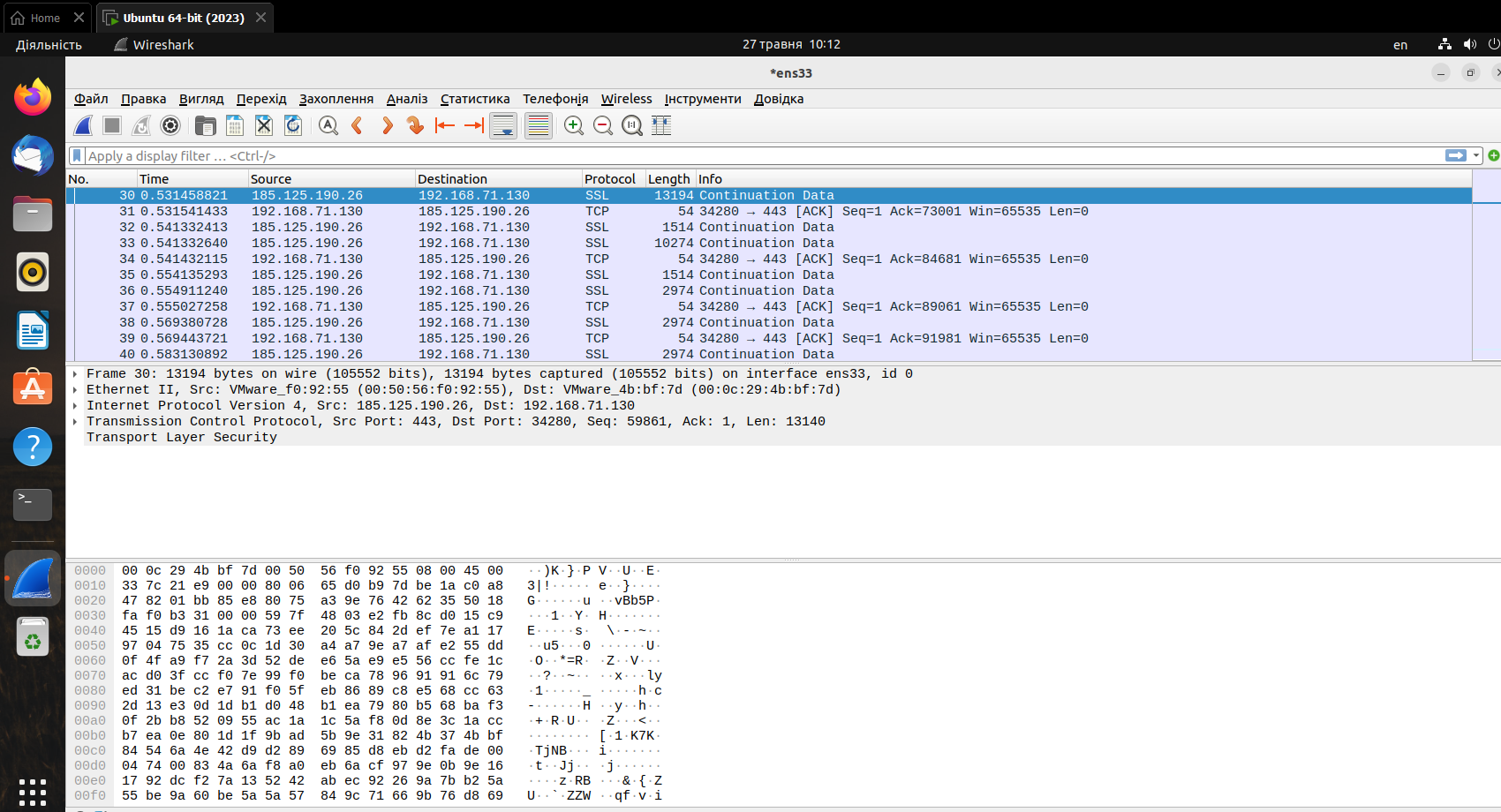
Це можна було побачити завдяки стовпць “№”.

Можемо спостерігати, що перехоплені нами пакети мають два протоколи: TCP та SSL.

* **TCP** **(Transmission Control Protocol)** є одним з основних протоколів транспортного рівня в моделі OSI (Open Systems Interconnection). Він забезпечує надійну доставку даних між двома вузлами в мережі шляхом установлення з'єднання, управління потоком, виявлення та відновлення втрачених пакетів, а також контролю за порядком доставки даних. TCP використовуєся для передачі різноманітних протоколів на вищих рівнях, таких як HTTP (протокол передачі гіпертексту), FTP (протокол передачі файлів) і інші.
* **SSL** **(Secure Sockets Layer)** є протоколом криптографічного захисту, розробленим для забезпечення безпеки комунікацій через мережі. SSL здатен забезпечити шифрування та автентифікацію даних, що передаються між клієнтом і сервером. Він дозволяє забезпечити конфіденційність, цілісність та автентичність даних шляхом застосування криптографічних методів. SSL-захищені з'єднання використовуються в багатьох протоколах, таких як HTTPS (захищений протокол передачі гіпертексту), SMTPS (захищений протокол передачі електронної пошти) і багато інших.

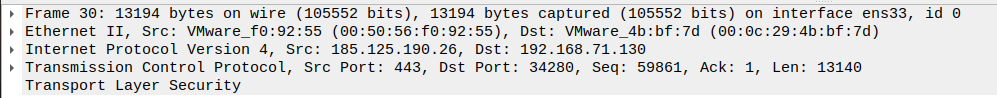
***\* Примітка.***  *Одним з відомих протоколів, що використовують як TCP, так і SSL, є HTTPS. Він використовує TCP для забезпечення надійної доставки даних і SSL для шифрування та захисту цих даних під час передачі через мережу.*

**В якості першого прикладу розглянемо пакет №30 з протоколом SSL.**



* No. (Номер): Пакет має номер 30, що вказує на те, що він є 30-м пакетом, перехопленим або записаним в Wireshark.
* Time (Час): Часова мітка пакету становить 0.531458821. Це може бути виміряно в секундах або в іншій одиниці, в залежності від налаштувань Wireshark.
* Source (Джерело): IP-адреса джерела пакету - 185.125.190.26. Це вказує на те, що пакет був відправлений з цієї конкретної IP-адреси.
* Destination (Призначення): IP-адреса призначення пакету - 192.168.71.130. Це вказує на те, що пакет був призначений для цієї конкретної IP-адреси.
* Protocol (Протокол): Протокол, який використовується в пакеті, - SSL. Це означає, що пакет використовує SSL (Secure Sockets Layer) для криптографічного захисту та безпеки комунікації.
* Length (Довжина): Пакет має довжину 13194 байтів. Це вказує на загальну кількість байтів, що містяться в пакеті.
* Info (Інформація): Значення "Continuation Data" вказує на те, що це пакет є продовженням передачі даних. Інші попередні пакети, можливо, містять початок цих даних, і цей пакет містить продовження цих даних.

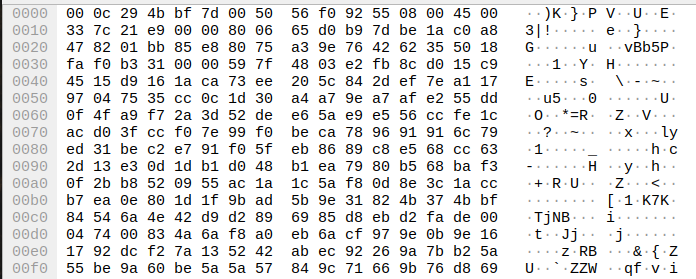
Ці значення стовпців надають певну інформацію про перехоплені пакети і можуть бути використані для подальшого аналізу мережевого трафіку.



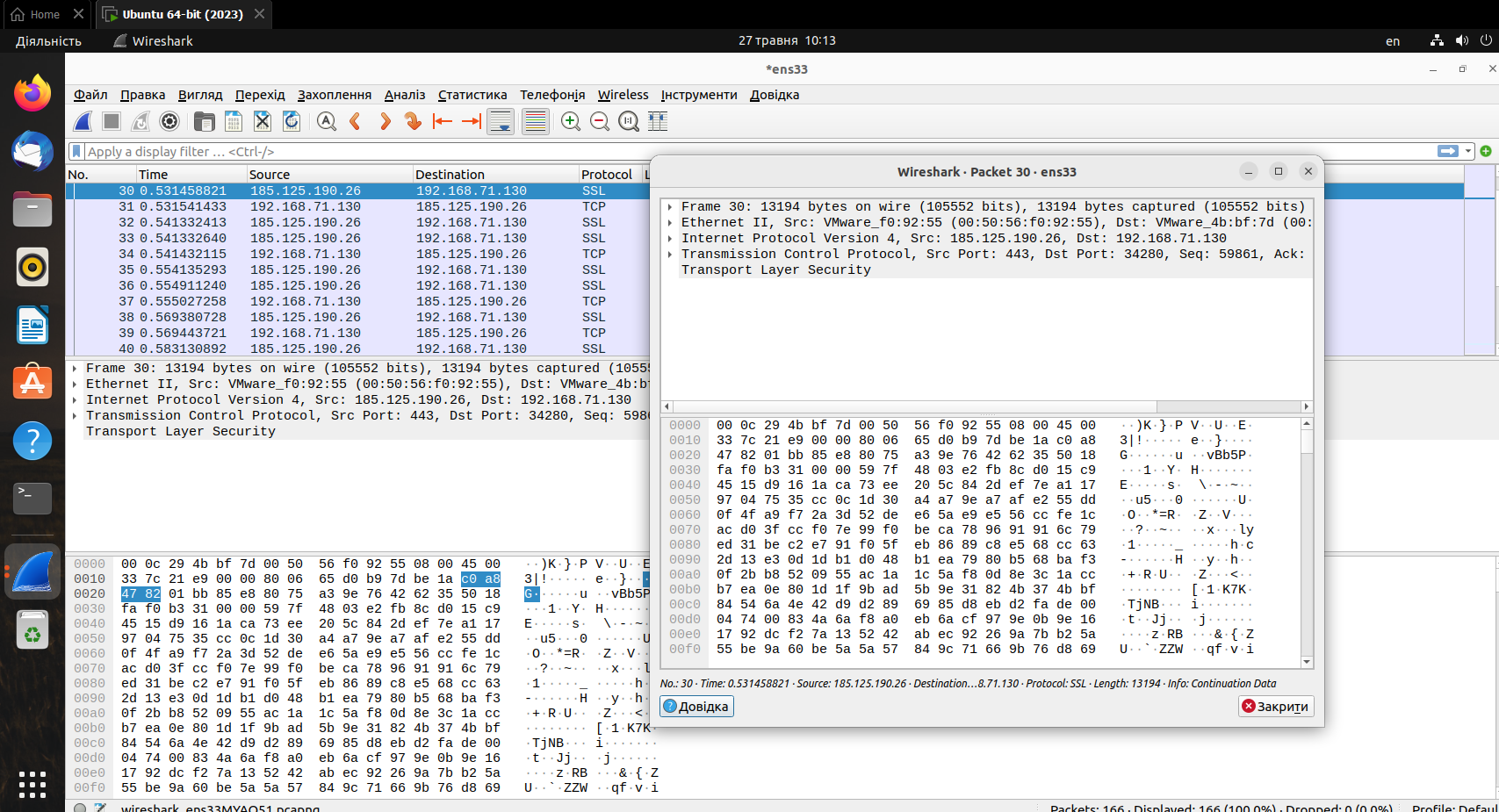
Інформація, яка відображається під таблицею в окремому вікні для пакету Frame 30, надає більш детальний розшифрований опис заголовків різних протоколів, які містяться в цьому пакеті.

* Ethernet II, Src: ..., Dst: ... - Ця частина інформації вказує на використаний протокол мережевого рівня, Ethernet II, та вказує джерело (Src) і призначення (Dst) пакету.
* Ethernet II є протоколом, що використовується для фізичної передачі даних в мережах Ethernet.
* Internet Protocol Version 4, Src: ..., Dst: ... - Ця частина інформації вказує на версію протоколу мережевого рівня, яка використовується в пакеті, в даному випадку, Internet Protocol Version 4 (IPv4). Також вказується джерело (Src) і призначення (Dst) пакету. IPv4 є протоколом мережевого рівня, що використовується для маршрутизації пакетів в мережах.
* Transmission Control Protocol, Src Port: ..., Dst Port: ..., Ack: ..., Len: ... - Ця частина інформації вказує на протокол транспортного рівня, який використовується в пакеті, в даному випадку, Transmission Control Protocol (TCP). Також вказується джерело порту (Src Port) та призначення порту (Dst Port) пакету. Ack вказує на номер підтвердження, а Len вказує на довжину пакету.
* Transport Layer Security - Ця частина інформації вказує на використання протоколу Transport Layer Security (TLS) для захищеної комунікації між джерелом і призначенням. TLS використовується для шифрування та захисту даних під час передачі через мережу.

Маємо можливість дізнатися приховану (більш детальну інформацію про пакет), натиснувши на стрілочку (трикутничок)

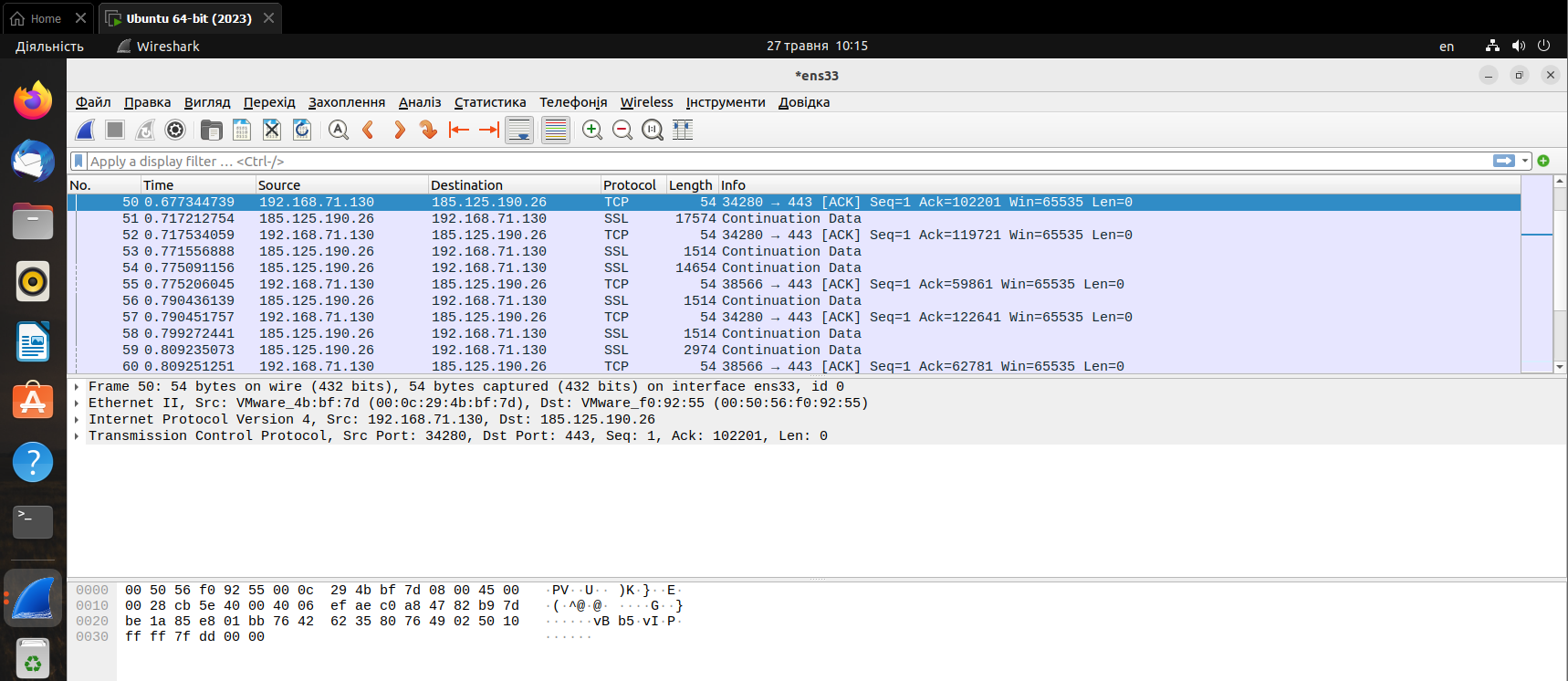


Тут можемо спостерігати закодовану інформацію розміром 13194 байти (або 105552 біти) в 16-ричній формі.

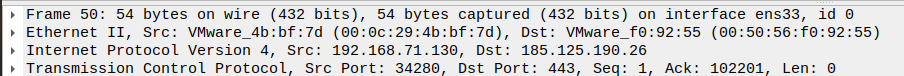


***\* Примітка.*** *При подвійному натисканні на пакет, який нас цікавить, отримуємо аналогічні дані, але вже у окремому вікні. Навівши на будь-яку частину коду можемо дізнатися інформацію, яка тут зашифрована.*

**В якості другого прикладу розглянемо пакет №60 з протоколом TCP.**



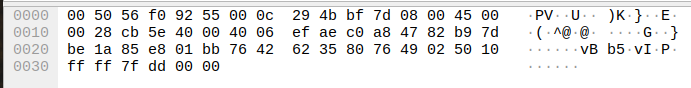
* No. (Номер): Пакет має номер 50, що вказує на те, що він є 50-м пакетом, перехопленим або записаним в Wireshark.
* Time (Час): Часова мітка пакету становить 0.677344739. Це може бути виміряно в секундах або в іншій одиниці, в залежності від налаштувань Wireshark.
* Source (Джерело): IP-адреса джерела пакету - 192.168.71.130. Це вказує на те, що пакет був відправлений з цієї конкретної IP-адреси.
* Destination (Призначення): IP-адреса призначення пакету - 185.125.190.26. Це вказує на те, що пакет був призначений для цієї конкретної IP-адреси.
* Protocol (Протокол): Протокол, який використовується в пакеті, - TCP. Це означає, що пакет використовує TCP (Transmission Control Protocol) для надання надійної доставки даних.
* Length (Довжина): Пакет має довжину 54 байти. Це вказує на загальну кількість байтів, що містяться в пакеті.
* Info (Інформація): Значення "34280 → 443 [ACK] Seq=1 Ack=102201 Win=65535 Len=0" є детальним описом пакету. Ця інформація містить різні атрибути пакету, такі як порти джерела і призначення (34280 → 443), тип підтвердження (ACK), послідовність (Seq=1), підтвердження (Ack=102201), вікно відправника (Win=65535) та довжину (Len=0). Ці дані вказують на деталі процесу обміну даними між джерелом та призначенням через TCP.



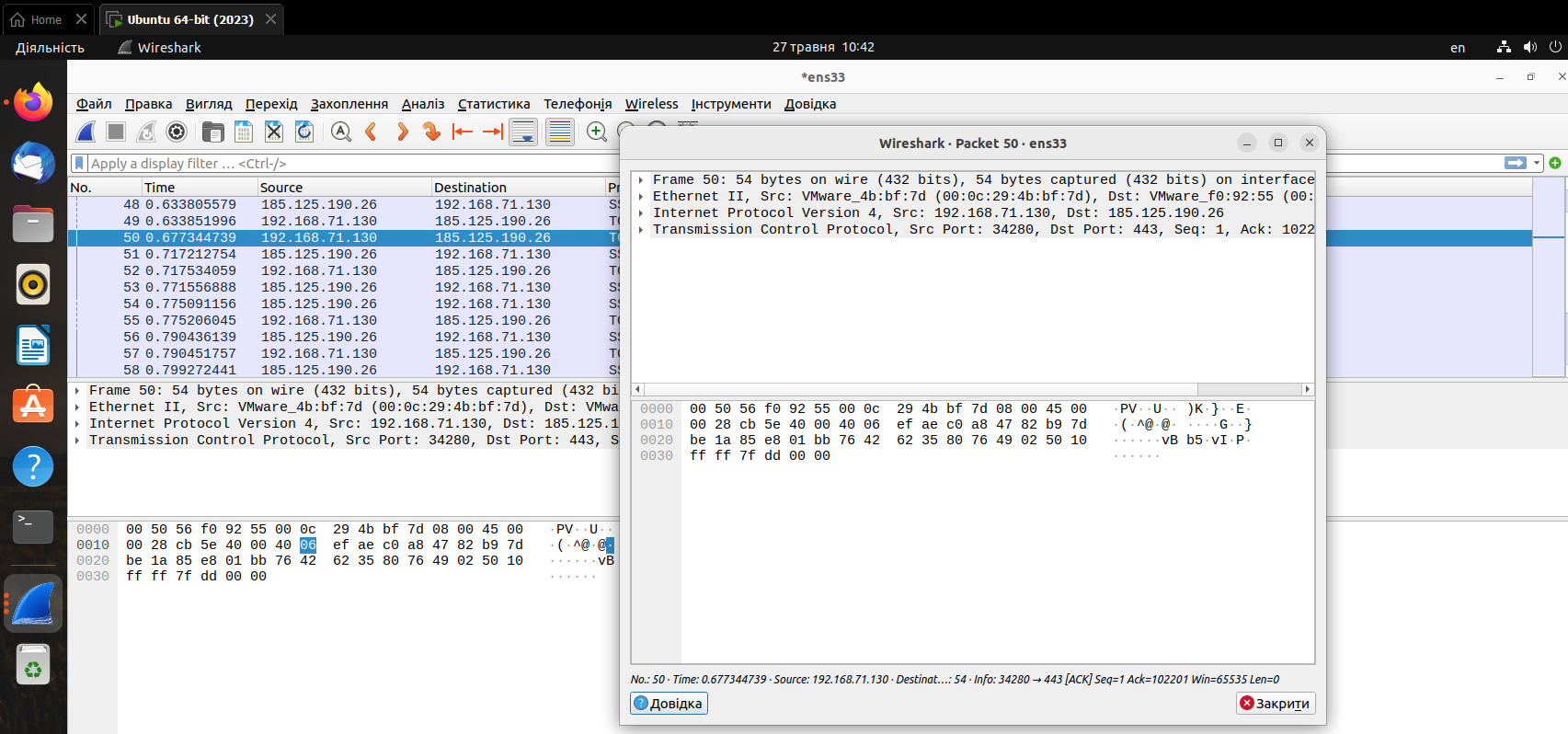
Інформація, яка відображається під таблицею в окремому вікні для пакету Frame 50, надає більш детальний розшифрований опис заголовків різних протоколів, які містяться в цьому пакеті.

* Ethernet II, Src: ..., Dst: ... - Ця частина інформації вказує на використаний протокол мережевого рівня, Ethernet II, та вказує джерело (Src) і призначення (Dst) пакету.
* Ethernet II є протоколом, що використовується для фізичної передачі даних в мережах Ethernet.
* Internet Protocol Version 4, Src: ..., Dst: ... - Ця частина інформації вказує на версію протоколу мережевого рівня, яка використовується в пакеті, в даному випадку, Internet Protocol Version 4 (IPv4). Також вказується джерело (Src) і призначення (Dst) пакету. IPv4 є протоколом мережевого рівня, що використовується для маршрутизації пакетів в мережах.
* Transmission Control Protocol, Src Port: ..., Dst Port: ..., Ack: ..., Len: ... - Ця частина інформації вказує на протокол транспортного рівня, який використовується в пакеті, в даному випадку, Transmission Control Protocol (TCP). Також вказується джерело порту (Src Port) та призначення порту (Dst Port) пакету. Ack вказує на номер підтвердження, а Len вказує на довжину пакету.

Маємо можливість дізнатися приховану (більш детальну інформацію про пакет), натиснувши на стрілочку (трикутничок)

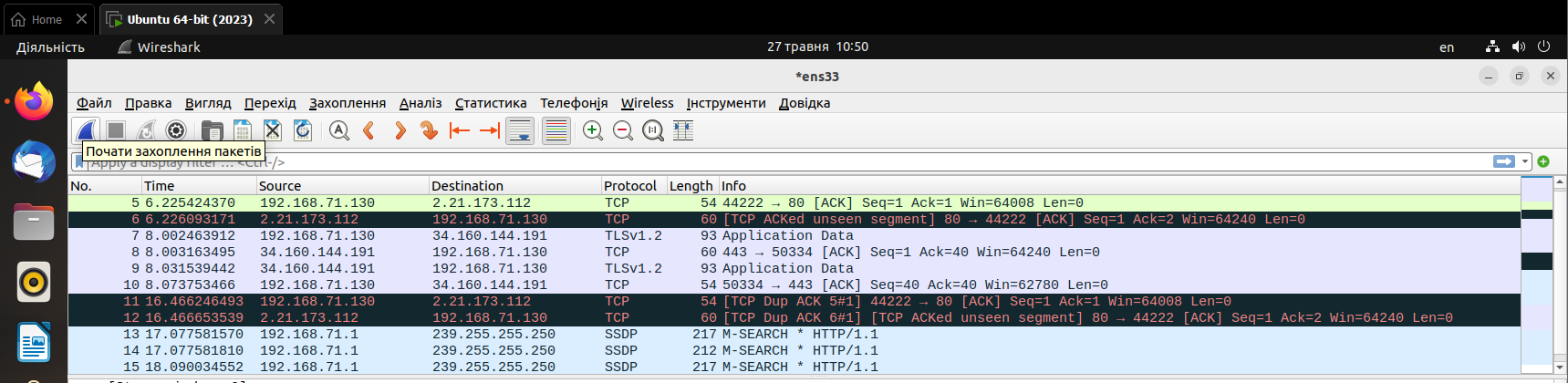


Тут можемо спостерігати закодовану інформацію розміром 54 байти (або 432 біти) в 16-ричній формі.



***\* Примітка.*** *При подвійному натисканні на пакет, який нас цікавить, отримуємо аналогічні дані, але вже у окремому вікні. Навівши на будь-яку частину коду можемо дізнатися інформацію, яка тут зашифрована.*

**Для третього прикладу необхідно ввімкнути браузер Firefox.**



Можемо спостерігати появу нових типів пакетів, вже присутні пакети з протоколами TCP, TLSv1.2, SSDP. Перший ми вже розглянули у прикладах вище, а про два нових відомо наступне:

* **TLSv1.2 (Transport Layer Security version 1.2)**: TLS є криптографічним протоколом, що забезпечує захищену комунікацію в мережі. Версія TLSv1.2 є покращеною версією TLS і надає шифрування, аутентифікацію та цілісність даних, передаваних між двома кінцевими точками. TLS широко використовується для захисту протоколів зв'язку, таких як HTTPS, SMTPS, FTPS та інших.
* **SSDP (Simple Service Discovery Protocol)**: SSDP є протоколом, який використовується для автоматичного виявлення мережевих пристроїв і служб в локальній мережі. Він дозволяє пристроям автоматично анонсувати свою наявність і характеристики в мережі, а також здійснювати пошук і запити для знаходження доступних пристроїв і служб. SSDP часто використовується в пристроях Інтернету речей (IoT), медіаплеєрах і деяких мережевих пристроях для спрощення їх встановлення та взаємодії.

Ці протоколи використовуються для різних цілей в мережевому оточенні: TLS забезпечує безпеку та конфіденційність комунікації, тоді як SSDP допомагає виявляти пристрої та служби в мережі для спрощення їх використання та взаємодії.

**Візуальне (кольорове) розрізнення**

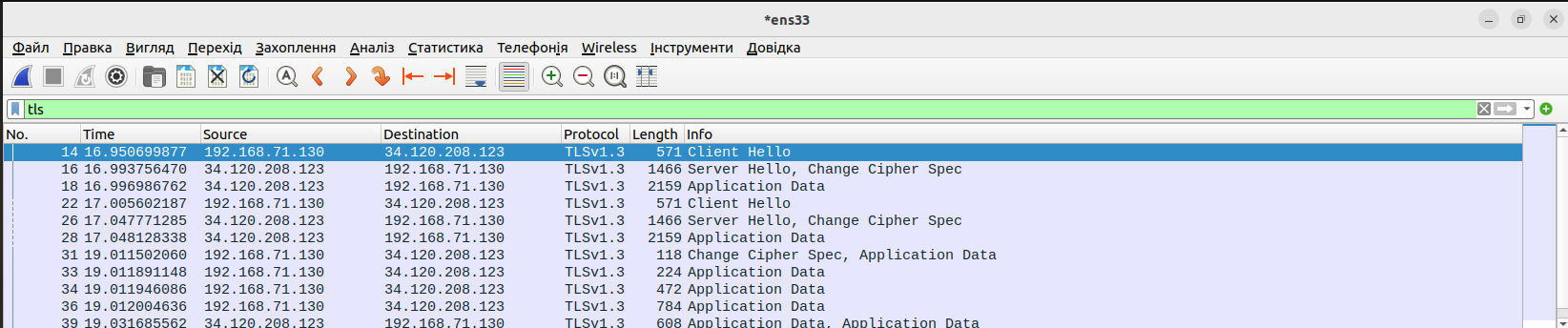
В Wireshark різні кольори протоколів використовуються для візуального розрізнення різних типів пакетів або протоколів у таблиці пакетів.

* Зелений. Зелений колір використовується для пакетів, що містять TCP-протоколи, наприклад HTTP, FTP, SSH тощо. Зелений колір вказує на використання протоколу TCP для цих пакетів.
* Синій. Синій колір також використовується для пакетів з протоколом TCP, таких як HTTP, FTP, SSH тощо.
* Блакитний. Блакитний колір використовується для пакетів, що містять протокол SSDP (Simple Service Discovery Protocol). SSDP - це протокол, який використовується для автоматичного виявлення мережевих пристроїв і служб в локальній мережі.
* Чорний. Чорний колір використовується для пакетів, які не відносяться до зазначених протоколів або які не можуть бути розпізнані Wireshark. Вони можуть представляти різні інші протоколи або пакети з помилками.

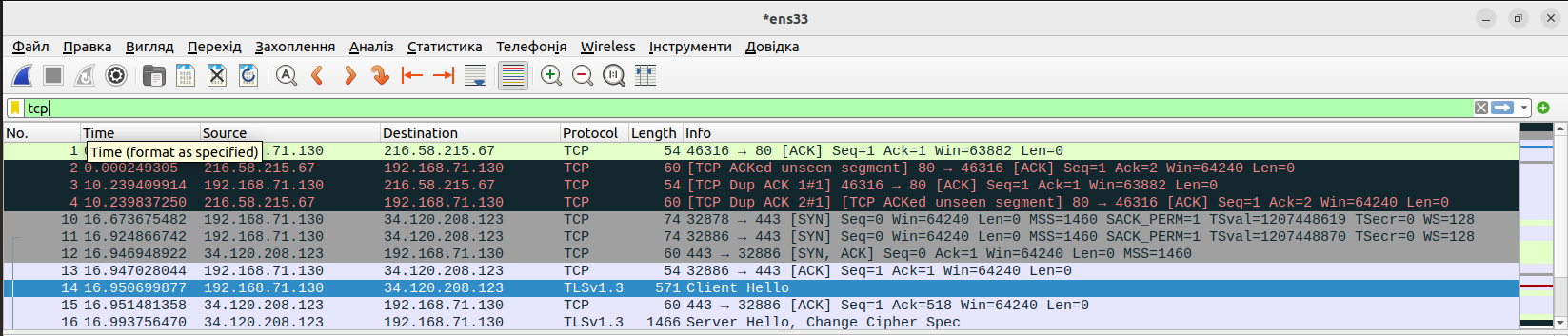
Варто зазначити, що кольори протоколів можуть змінюватися в залежності від налаштувань Wireshark, а також від контексту та специфіки мережевого захоплення.

**Пошук інформації**

Пошук за запитом “TLS”:



Пошук за запитом “TCP”:



Таким чином, можна легко та варіативно фільтрувати пакети за вашим бажанням, тим самим полегшивши процес роботи та аналізу.

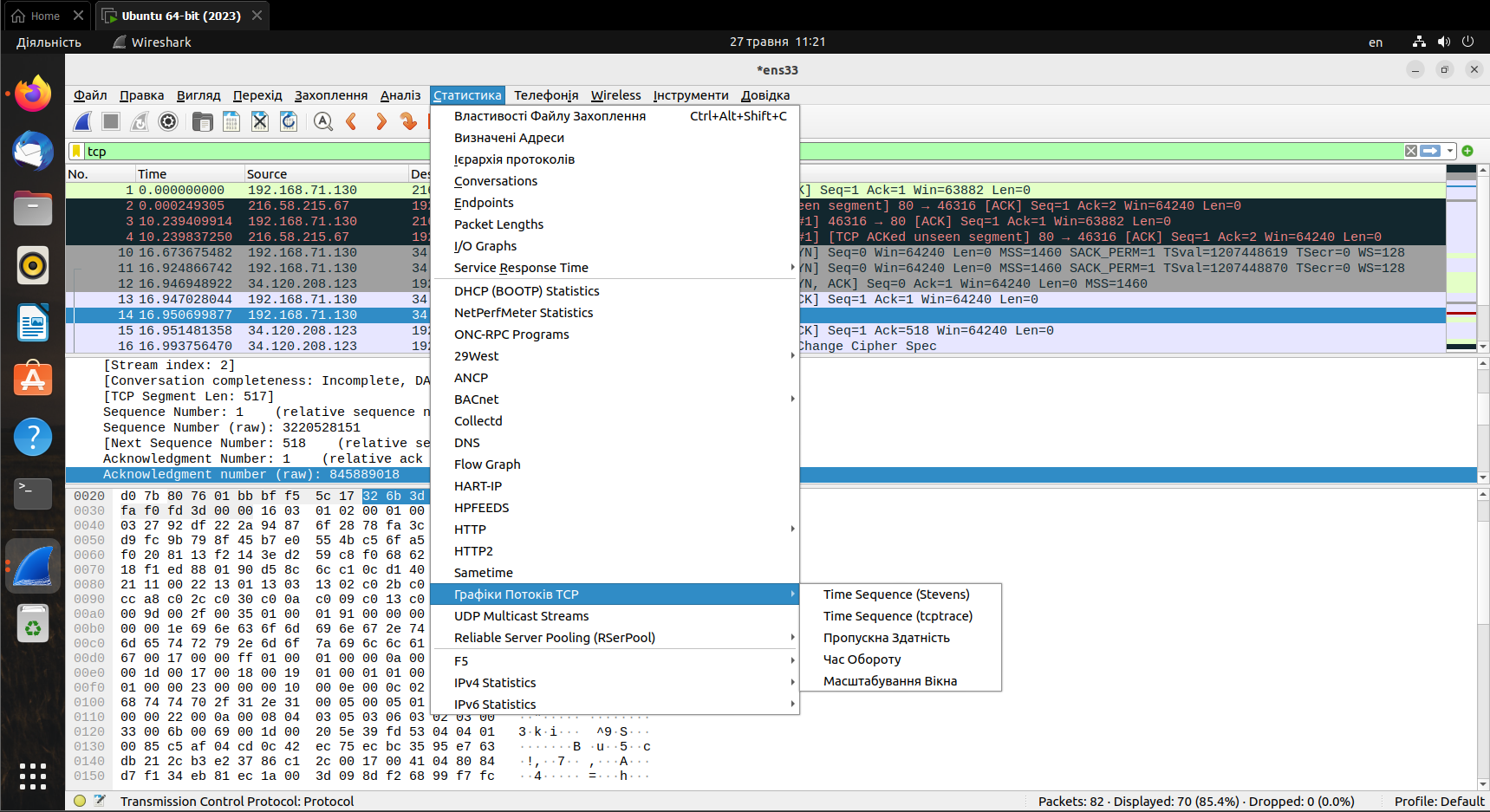
**Статистика трафіку**

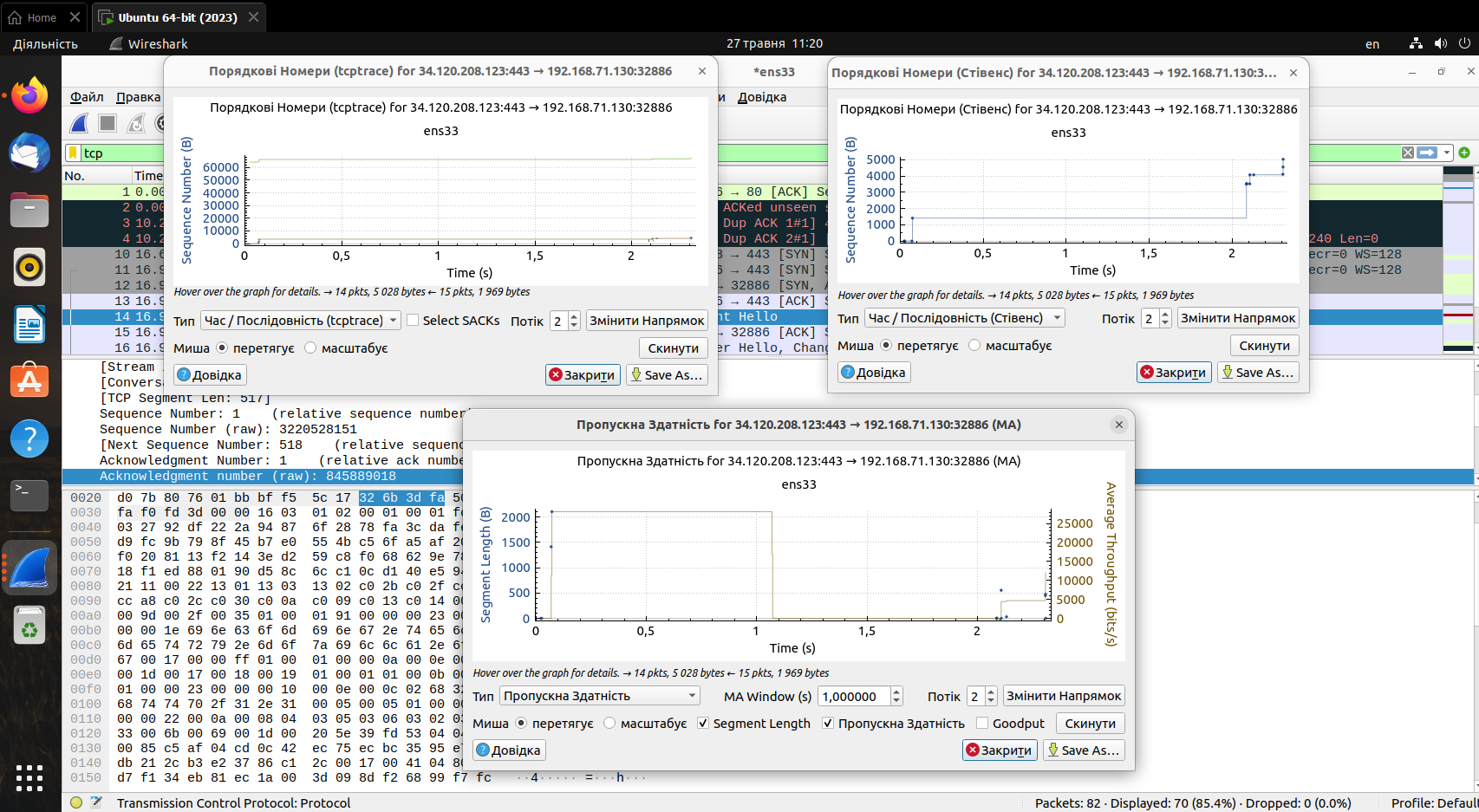
Wireshark надає можливість відображати графіки потоків TCP, які дозволяють вам візуально аналізувати поведінку та характеристики TCP-потоків у вашому захопленні мережевого трафіку. Графіки потоків TCP можуть надати цінну інформацію про розмір пакетів, швидкість передачі даних, час відповіді та інші метрики.

Для побудови графіків потоків TCP у Wireshark можна скористатися такими кроками:

1. Відкрийте захоплення мережевого трафіку у Wireshark.Виберіть пакет з потоком TCP, який вас цікавить.
2. Натисніть на вкладку “Статистика”
3. Тепер можете спостерігати меню вибору статистики (різноманітні властивості, ієрархії, тощо). Проте, нас цікавлять “Графіки протоколів TCP”
4. Натисніть “Графіки протоколів TCP”
5. Оберіть відповідний варіант та інформацію, яка буде представлена на графіку.

Графіки потоків TCP можуть бути корисними для виявлення патернів, аномалій або проблем у поведінці TCP-потоків, а також для порівняння різних потоків у мережі. Вони допомагають зрозуміти пропускну здатність, ефективність та стабільність TCP-з'єднань у вашій мережі.

****

****

**Висновок**

Отже, Wireshark є потужним інструментом для аналізу мережевого трафіку. Він дозволяє захоплювати пакети даних, які пересилаються в мережі, і виводити їх у зручному для розуміння форматі.

Під час роботи з Wireshark у вас є можливість переглядати і аналізувати різні аспекти пакетів, такі як джерело та призначення, протокол, час передачі, довжина тощо. Ці дані допомагають вам розуміти, як працює ваша мережа і як взаємодіють пристрої в ній. Кольорове кодування пакетів в Wireshark допомагає вам швидко виділити пакети різних протоколів або розпізнати спеціальні типи пакетів. Аналіз пакетів у Wireshark дозволяє вам виявити потенційні проблеми або недоліки в мережі, такі як помилки протоколу, надмірна витрата пропускної здатності, некоректна конфігурація тощо. Це допомагає вам зрозуміти, як поліпшити ефективність та безпеку вашої мережі. Wireshark також має багато інших корисних функцій, таких як фільтрація пакетів за різними критеріями, статистика мережевого трафіку, графіки та діаграми для візуалізації даних, підтримка різних форматів файлів тощо.

Загалом надзвичайно зручна та багатофункціональна програма, яка доводить свою ефективність з перших хвилин роботи.