

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

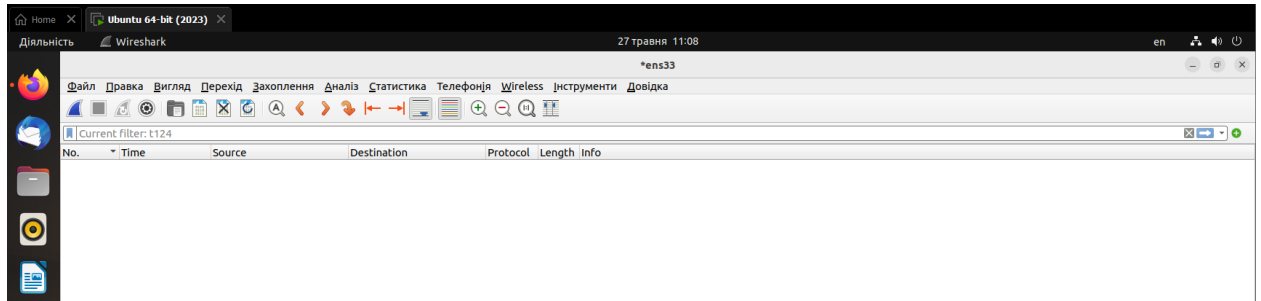
Wireshark є одним з найпопулярніших інструментів для аналізу мережевого трафіку. Він дозволяє захоплювати пакети даних, що пересилаються в мережі, та надає детальну інформацію про ці пакети, що допомагає зрозуміти, як працює ваша мережа і виявити можливі проблеми.

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.



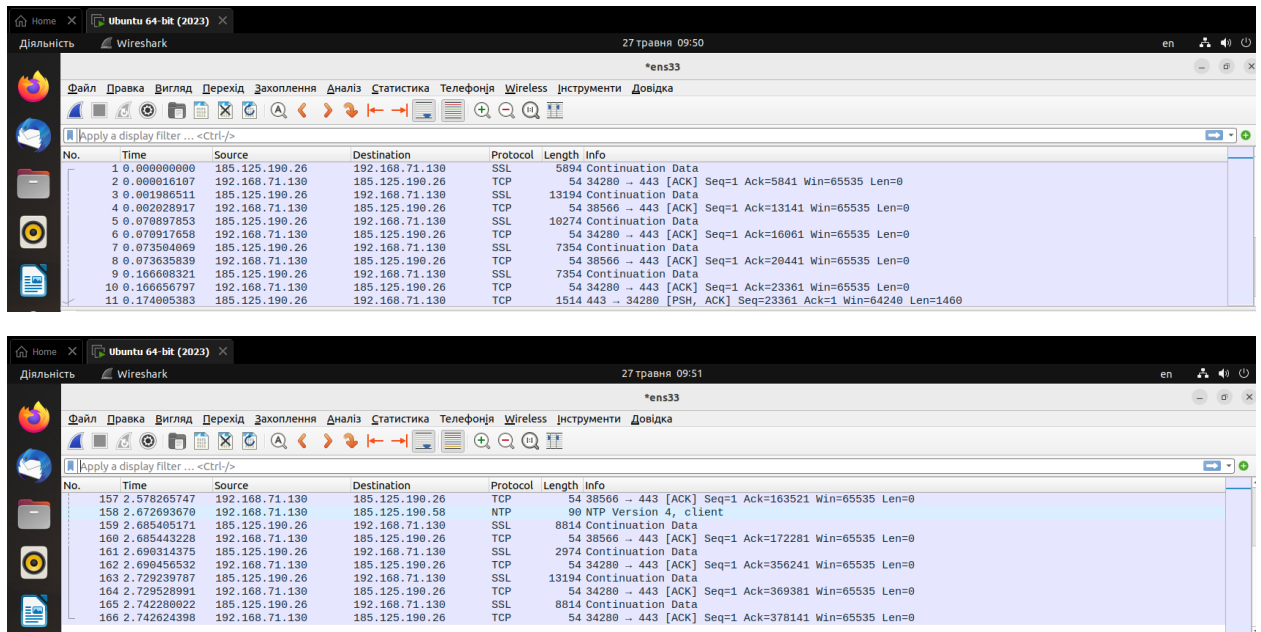
У таблиці Wireshark наведені різні стовпці, які містять інформацію про ці пакети. Ось означення кожного стовпця:

- **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.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	185.125.190.26	192.168.71.130	SSL	5894	Continuation Data
2	0.000016107	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=5841 Win=65535 Len=0
3	0.001986511	185.125.190.26	192.168.71.130	SSL	13194	Continuation Data
4	0.002028917	192.168.71.130	185.125.190.26	TCP	54	38566 → 443 [ACK] Seq=1 Ack=13141 Win=65535 Len=0
5	0.070897853	185.125.190.26	192.168.71.130	SSL	10274	Continuation Data
6	0.070917658	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=16061 Win=65535 Len=0
7	0.073504069	185.125.190.26	192.168.71.130	SSL	7354	Continuation Data
8	0.073635839	192.168.71.130	185.125.190.26	TCP	54	38566 → 443 [ACK] Seq=1 Ack=20441 Win=65535 Len=0
9	0.106608321	185.125.190.26	192.168.71.130	SSL	7354	Continuation Data
10	0.106656797	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=23361 Win=65535 Len=0
11	0.174005383	185.125.190.26	192.168.71.130	TCP	1514	443 → 34280 [PSH, ACK] Seq=23361 Ack=1 Win=64240 Len=1460

No.	Time	Source	Destination	Protocol	Length	Info
157	2.578265747	192.168.71.130	185.125.190.26	TCP	54	38566 → 443 [ACK] Seq=1 Ack=163521 Win=65535 Len=0
158	2.672693670	192.168.71.130	185.125.190.58	NTP	90	NTP Version 4, client
159	2.685405171	185.125.190.26	192.168.71.130	SSL	8814	Continuation Data
160	2.685443228	192.168.71.130	185.125.190.26	TCP	54	38566 → 443 [ACK] Seq=1 Ack=172281 Win=65535 Len=0
161	2.690314375	185.125.190.26	192.168.71.130	SSL	2974	Continuation Data
162	2.690456532	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=356241 Win=65535 Len=0
163	2.729239787	185.125.190.26	192.168.71.130	SSL	13194	Continuation Data
164	2.729528991	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=369381 Win=65535 Len=0
165	2.742280922	185.125.190.26	192.168.71.130	SSL	8814	Continuation Data
166	2.742624398	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=378141 Win=65535 Len=0

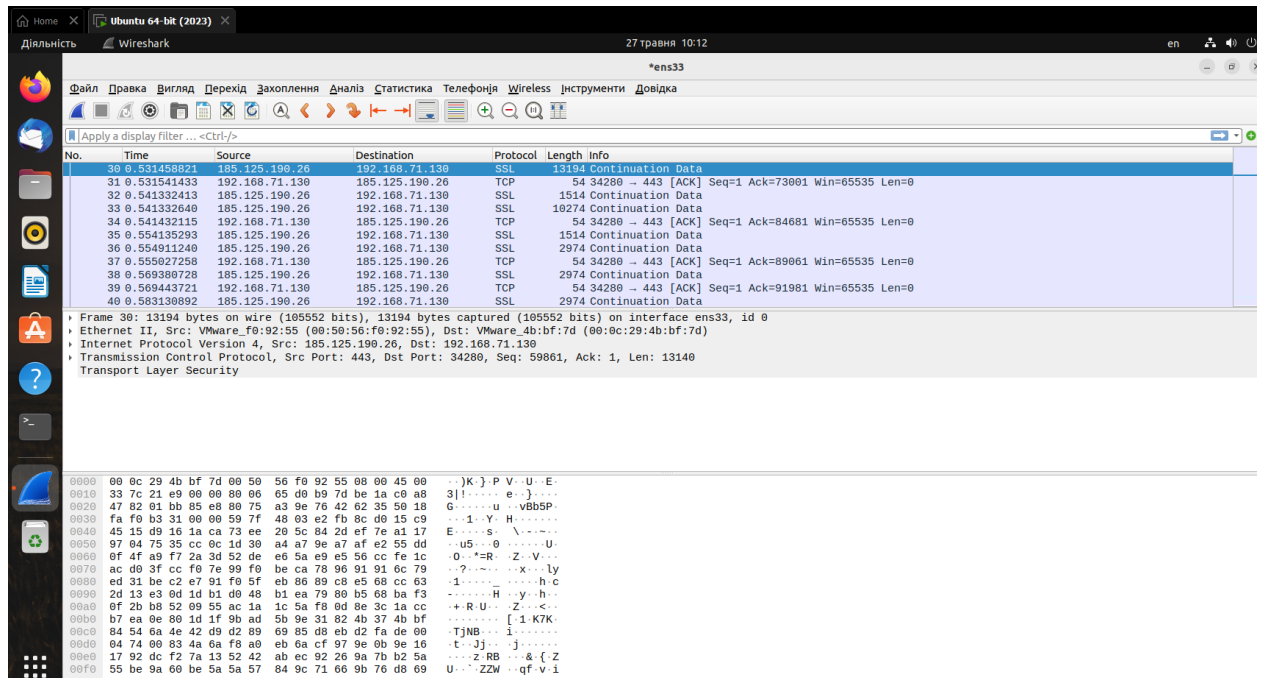
Це можна було побачити завдяки стовпцю “№”.

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 установалення з'єднання, управління потоком, виявлення та відновлення втрачених пакетів, а також контролю за порядком доставки даних. TCP використовується 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.	Time	Source	Destination	Protocol	Length	Info
30	0.531458821	185.125.190.26	192.168.71.130	SSL	13194	Continuation Data
31	0.531541433	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=73001 Win=65535 Len=0
32	0.541332413	185.125.190.26	192.168.71.130	SSL	1514	Continuation Data
33	0.541332640	185.125.190.26	192.168.71.130	SSL	10274	Continuation Data
34	0.541332115	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=84681 Win=65535 Len=0
35	0.554135293	185.125.190.26	192.168.71.130	SSL	1514	Continuation Data
36	0.554911240	185.125.190.26	192.168.71.130	SSL	2974	Continuation Data
37	0.555027258	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=89061 Win=65535 Len=0
38	0.569380728	185.125.190.26	192.168.71.130	SSL	2974	Continuation Data
39	0.569443721	192.168.71.130	185.125.190.26	TCP	54	34280 → 443 [ACK] Seq=1 Ack=91981 Win=65535 Len=0
40	0.583130092	185.125.190.26	192.168.71.130	SSL	2974	Continuation Data

Frame 30: 13194 bytes on wire (105552 bits), 13194 bytes captured (105552 bits) on interface ens33, id 0
Ethernet II, Src: VMware_f0:92:55 (00:50:56:f0:92:55), Dst: VMware_4b:bf:7d (00:0c:29:4b:bf:7d)
Internet Protocol Version 4, Src: 185.125.190.26, Dst: 192.168.71.130
Transmission Control Protocol, Src Port: 443, Dst Port: 34280, Seq: 59861, Ack: 1, Len: 13140
Transport Layer Security

- **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.

```
› Frame 30: 13194 bytes on wire (105552 bits), 13194 bytes captured (105552 bits) on interface ens33, id 0
› Ethernet II, Src: VMware_f0:92:55 (00:50:56:f0:92:55), Dst: VMware_4b:bf:7d (00:0c:29:4b:bf:7d)
› Internet Protocol Version 4, Src: 185.125.190.26, Dst: 192.168.71.130
› Transmission Control Protocol, Src Port: 443, Dst Port: 34280, Seq: 59861, Ack: 1, Len: 13140
  Transport Layer Security
```

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.

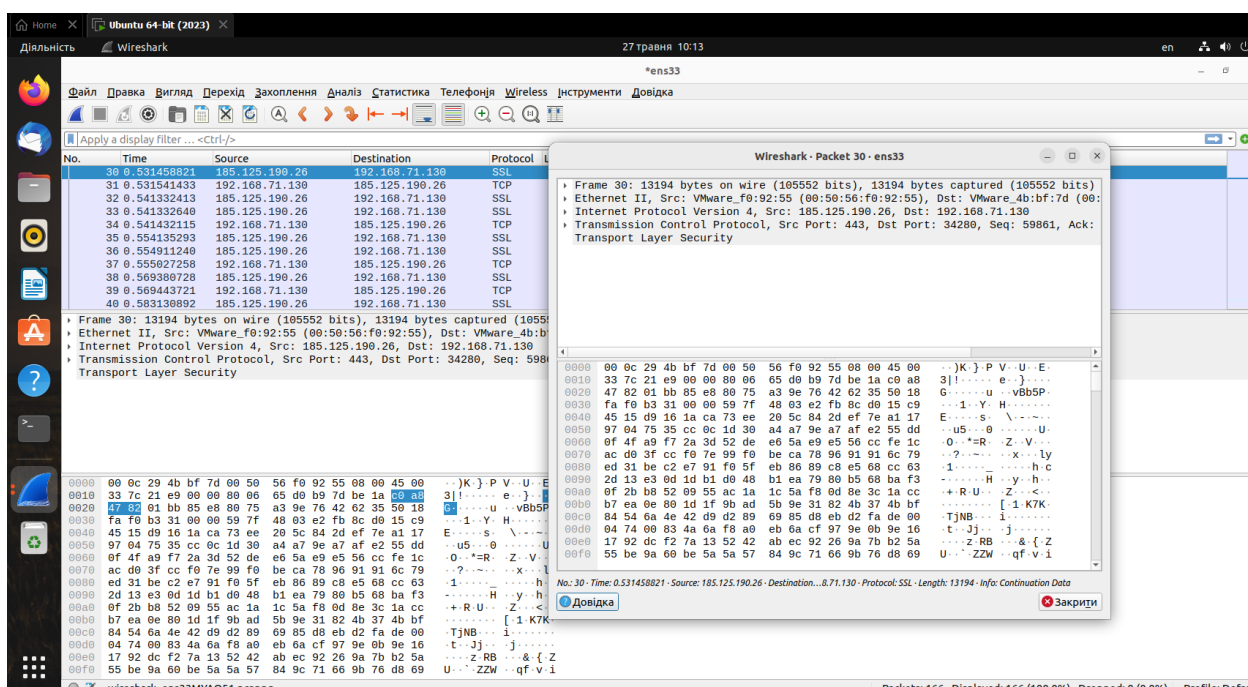
Маємо можливість дізнатися приховану (більш детальну інформацію про пакет), натиснувши на стрілочку (трикутникчик)

```

0000 00 0c 29 4b bf 7d 00 50 56 f0 92 55 08 00 45 00 ..)K}.P V..U..E.
0010 33 7c 21 e9 00 00 80 06 65 d0 b9 7d be 1a c0 a8 3|!.....e..}....
0020 47 82 01 bb 85 e8 80 75 a3 9e 76 42 62 35 50 18 G.....u..vBb5P.
0030 fa f0 b3 31 00 00 59 7f 48 03 e2 fb 8c d0 15 c9 ...1..Y..H.....
0040 45 15 d9 16 1a ca 73 ee 20 5c 84 2d ef 7e a1 17 E.....s.. \..~...
0050 97 04 75 35 cc 0c 1d 30 a4 a7 9e a7 af e2 55 dd ..u5...0.....U.
0060 0f 4f a9 f7 2a 3d 52 de e6 5a e9 e5 56 cc fe 1c .0..*=R..Z..V...
0070 ac d0 3f cc f0 7e 99 f0 be ca 78 96 91 91 6c 79 ..?..~...x...ly
0080 ed 31 be c2 e7 91 f0 5f eb 86 89 c8 e5 68 cc 63 .1....._.....h.c
0090 2d 13 e3 0d 1d b1 d0 48 b1 ea 79 80 b5 68 ba f3 -.....H...y..h..
00a0 0f 2b b8 52 09 55 ac 1a 1c 5a f8 0d 8e 3c 1a cc .+R.U..Z...<...
00b0 b7 ea 0e 80 1d 1f 9b ad 5b 9e 31 82 4b 37 4b bf .....[.1.K7K.
00c0 84 54 6a 4e 42 d9 d2 89 69 85 d8 eb d2 fa de 00 .TjNB...i.....
00d0 04 74 00 83 4a 6a f8 a0 eb 6a cf 97 9e 0b 9e 16 .t..Jj...j.....
00e0 17 92 dc f2 7a 13 52 42 ab ec 92 26 9a 7b b2 5a ...z.RB...&.{.Z
00f0 55 be 9a 60 be 5a 5a 57 84 9c 71 66 9b 76 d8 69 U...ZZW...qf.v.i

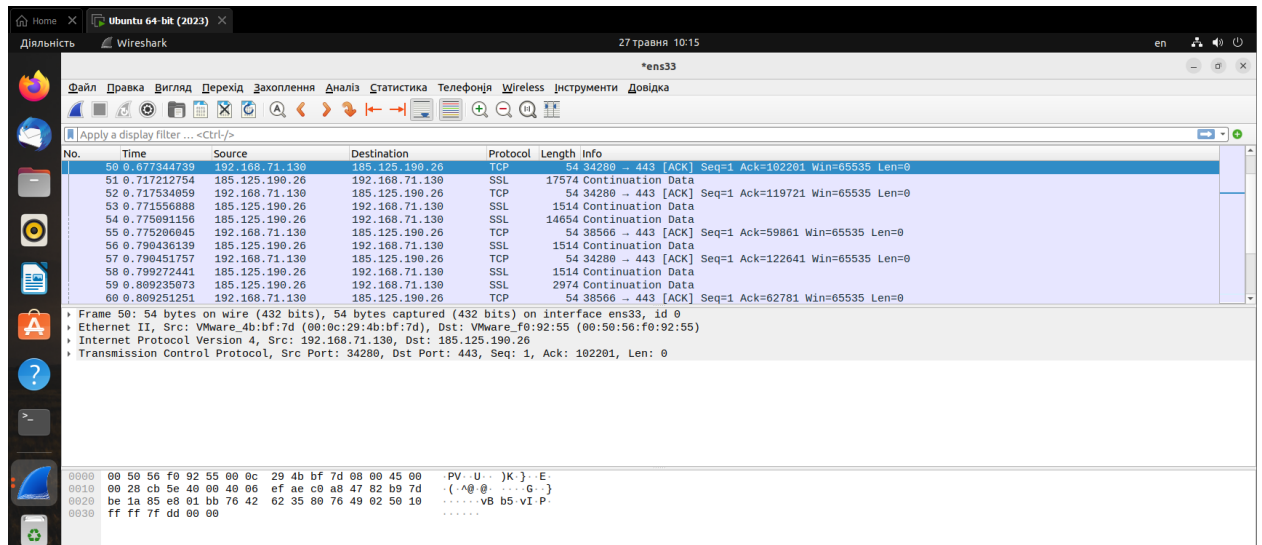
```

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.

```
‣ Frame 50: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface ens33, id 0
‣ Ethernet II, Src: VMware_4b:bf:7d (00:0c:29:4b:bf:7d), Dst: VMware_f0:92:55 (00:50:56:f0:92:55)
‣ Internet Protocol Version 4, Src: 192.168.71.130, Dst: 185.125.190.26
‣ Transmission Control Protocol, Src Port: 34280, Dst Port: 443, Seq: 1, Ack: 102201, Len: 0
```

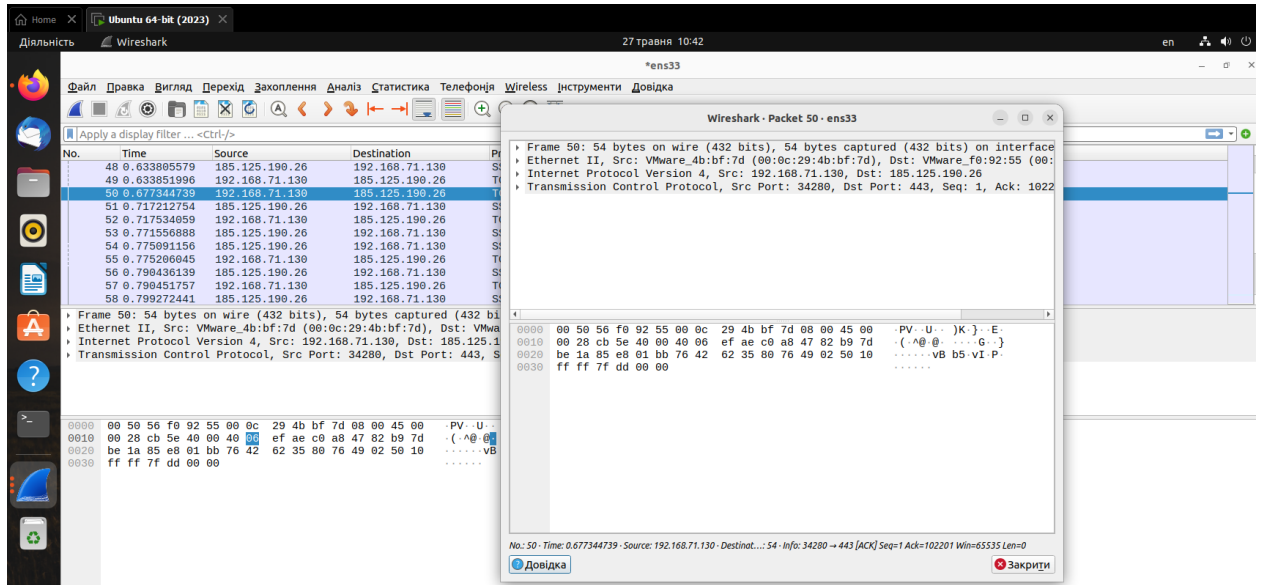
Інформація, яка відображається під таблицею в окремому вікні для пакету Frame 50, надає більш детальний розшифрований опис заголовків різних протоколів, які містяться в цьому пакеті.

- 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 (трикутникчик)

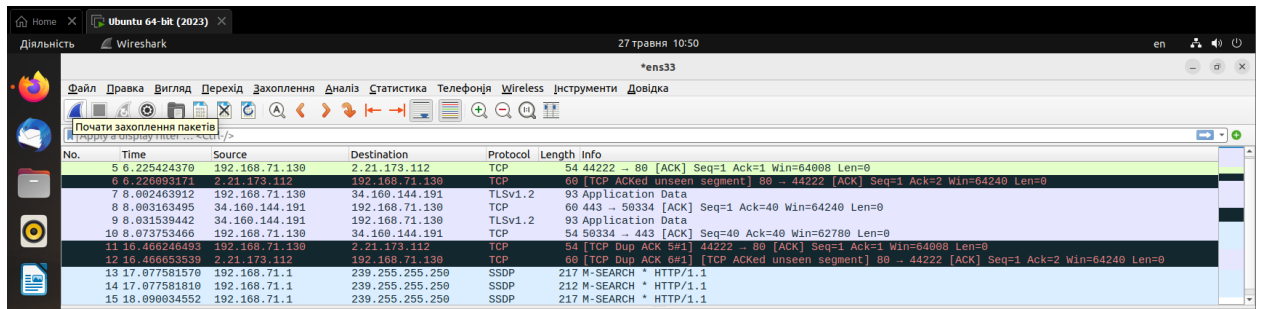
0000	00 50 56 f0 92 55 00 0c	29 4b bf 7d 08 00 45 00	·PV·U·)K·}·E·
0010	00 28 cb 5e 40 00 40 06	ef ae c0 a8 47 82 b9 7d	·(^@·@· ···G·}
0020	be 1a 85 e8 01 bb 76 42	62 35 80 76 49 02 50 10	·····vB b5·vI·P·
0030	ff ff 7f dd 00 00		·····

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

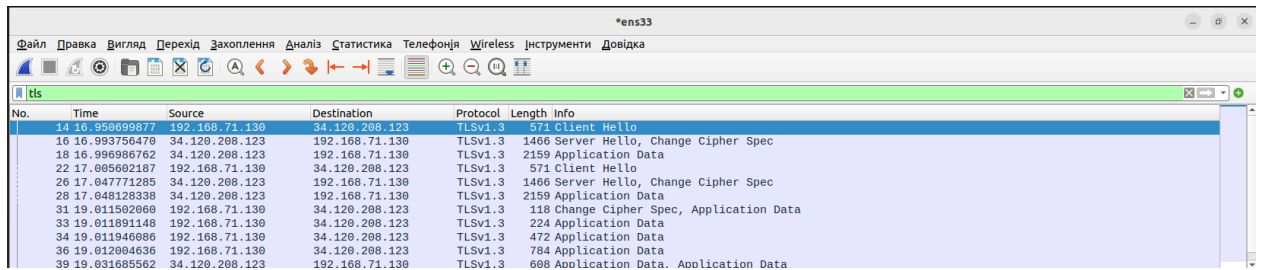
В Wireshark різні кольори протоколів використовуються для візуального розрізнення різних типів пакетів або протоколів у таблиці пакетів.

- **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

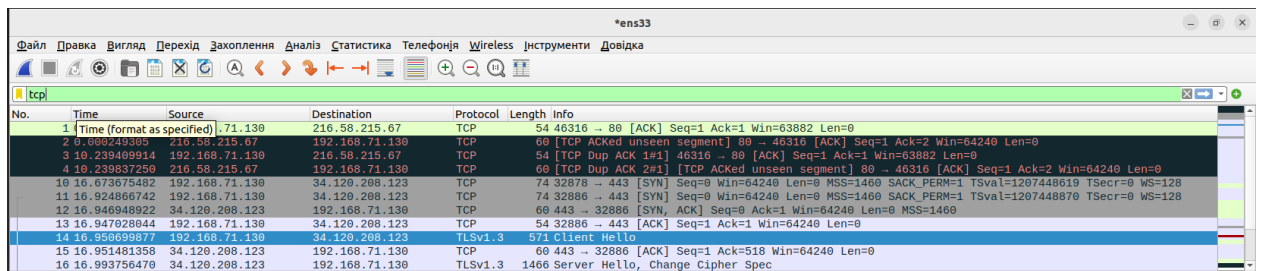
Пошук за запитом “TLS”:



Wireshark capture showing TLS traffic. The filter bar is set to 'tls'. The packet list shows 10 packets, all of which are TLSv1.3. The packet details pane shows the selected packet (No. 14) with its structure: Client Hello, Change Cipher Spec, and Application Data.

No.	Time	Source	Destination	Protocol	Length	Info
14	16.95669877	192.168.71.130	34.120.208.123	TLSv1.3	571	Client Hello
16	16.993756470	34.120.208.123	192.168.71.130	TLSv1.3	1466	Server Hello, Change Cipher Spec
18	16.996986762	34.120.208.123	192.168.71.130	TLSv1.3	2159	Application Data
22	17.005662187	192.168.71.130	34.120.208.123	TLSv1.3	571	Client Hello
26	17.047771285	34.120.208.123	192.168.71.130	TLSv1.3	1466	Server Hello, Change Cipher Spec
28	17.048128338	34.120.208.123	192.168.71.130	TLSv1.3	2159	Application Data
31	19.011502060	192.168.71.130	34.120.208.123	TLSv1.3	118	Change Cipher Spec, Application Data
33	19.011891148	192.168.71.130	34.120.208.123	TLSv1.3	224	Application Data
34	19.011946086	192.168.71.130	34.120.208.123	TLSv1.3	472	Application Data
36	19.012094636	192.168.71.130	34.120.208.123	TLSv1.3	784	Application Data
39	19.031685562	34.120.208.123	192.168.71.130	TLSv1.3	608	Application Data, Application Data

Пошук за запитом “TCP”:



Wireshark capture showing TCP traffic. The filter bar is set to 'tcp'. The packet list shows 10 packets, all of which are TCP. The packet details pane shows the selected packet (No. 1) with its structure: ACK, Seq=1, Ack=1, Win=63882, Len=0.

No.	Time	Source	Destination	Protocol	Length	Info
1	16.95669877	192.168.71.130	34.120.208.123	TCP	54	46316 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
2	16.993756470	34.120.208.123	192.168.71.130	TCP	60	[TCP ACKed unseen segment] 80 → 46316 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3	16.996986762	34.120.208.123	192.168.71.130	TCP	54	[TCP Dup ACK 1st] 46316 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
4	16.996986762	34.120.208.123	192.168.71.130	TCP	60	[TCP Dup ACK 2nd] [TCP ACKed unseen segment] 80 → 46316 [ACK] Seq=1 Ack=2 Win=64240 Len=0
10	16.673675482	192.168.71.130	34.120.208.123	TCP	74	32878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1207448619 TSecr=0 WS=128
11	16.924866742	192.168.71.130	34.120.208.123	TCP	74	32886 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1207448870 TSecr=0 WS=128
12	16.946948922	34.120.208.123	192.168.71.130	TCP	60	443 → 32886 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
13	16.947028044	192.168.71.130	34.120.208.123	TCP	54	32886 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14	16.95669877	192.168.71.130	34.120.208.123	TLSv1.3	571	Client Hello
15	16.951481358	34.120.208.123	192.168.71.130	TCP	60	443 → 32886 [ACK] Seq=1 Ack=518 Win=64240 Len=0
16	16.993756470	34.120.208.123	192.168.71.130	TLSv1.3	1466	Server Hello, Change Cipher Spec

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

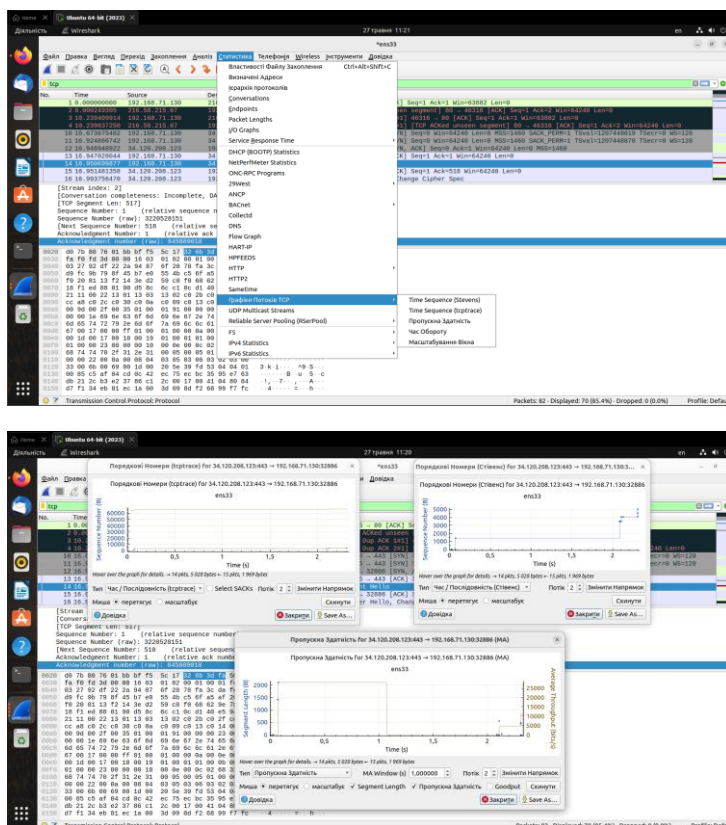
Статистика трафіку

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