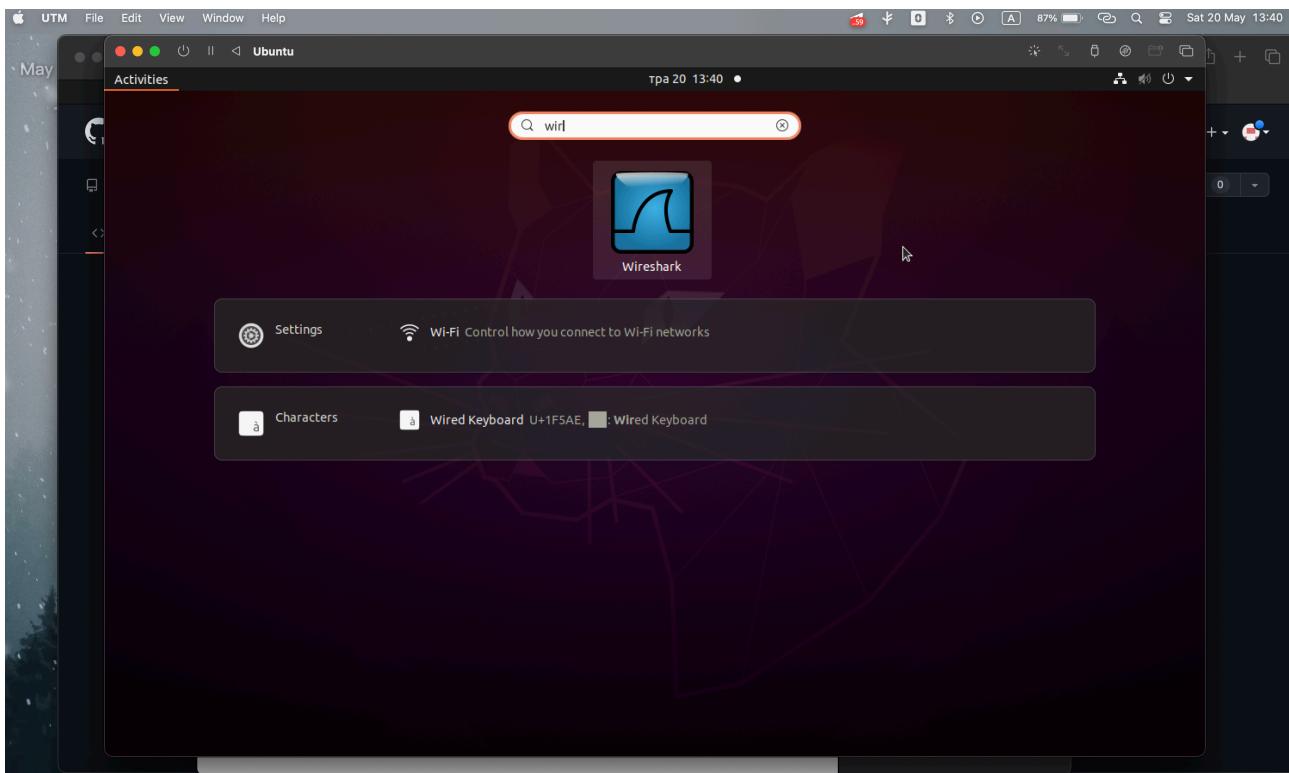
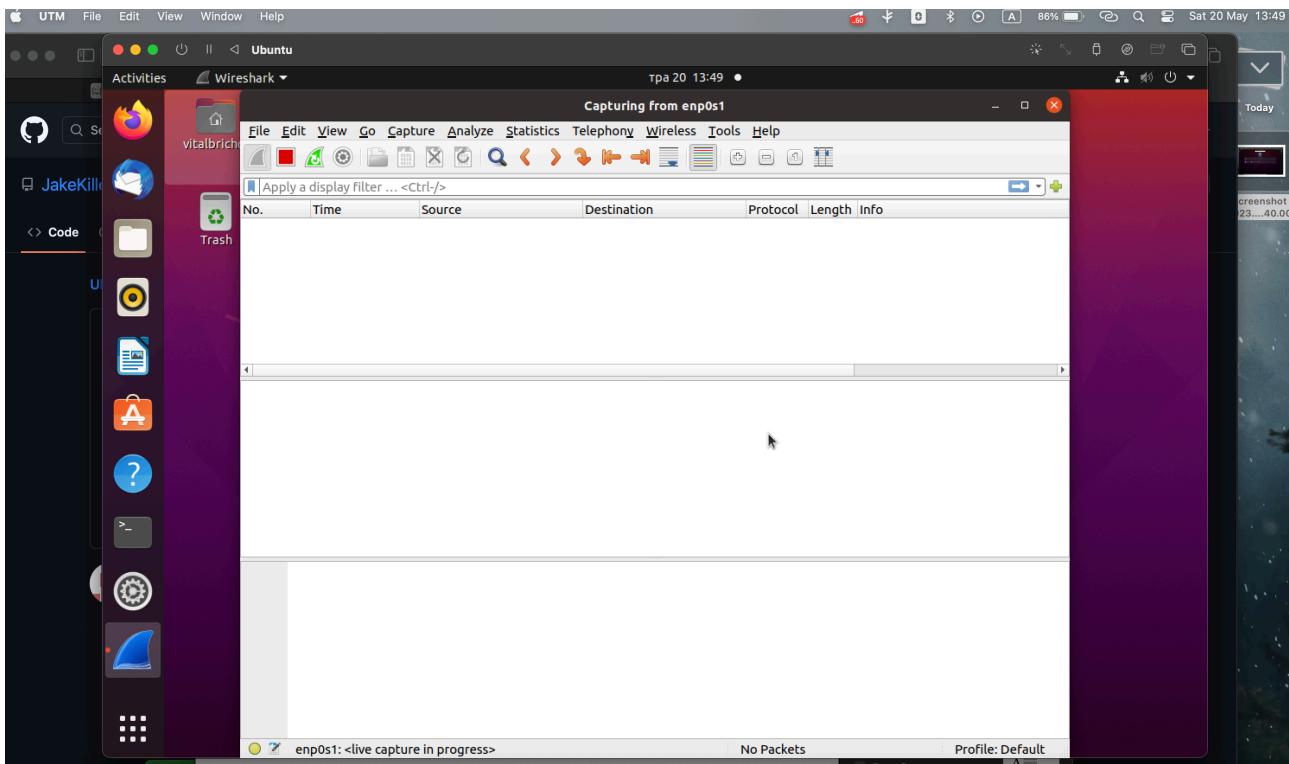


## Робота з Wireshark

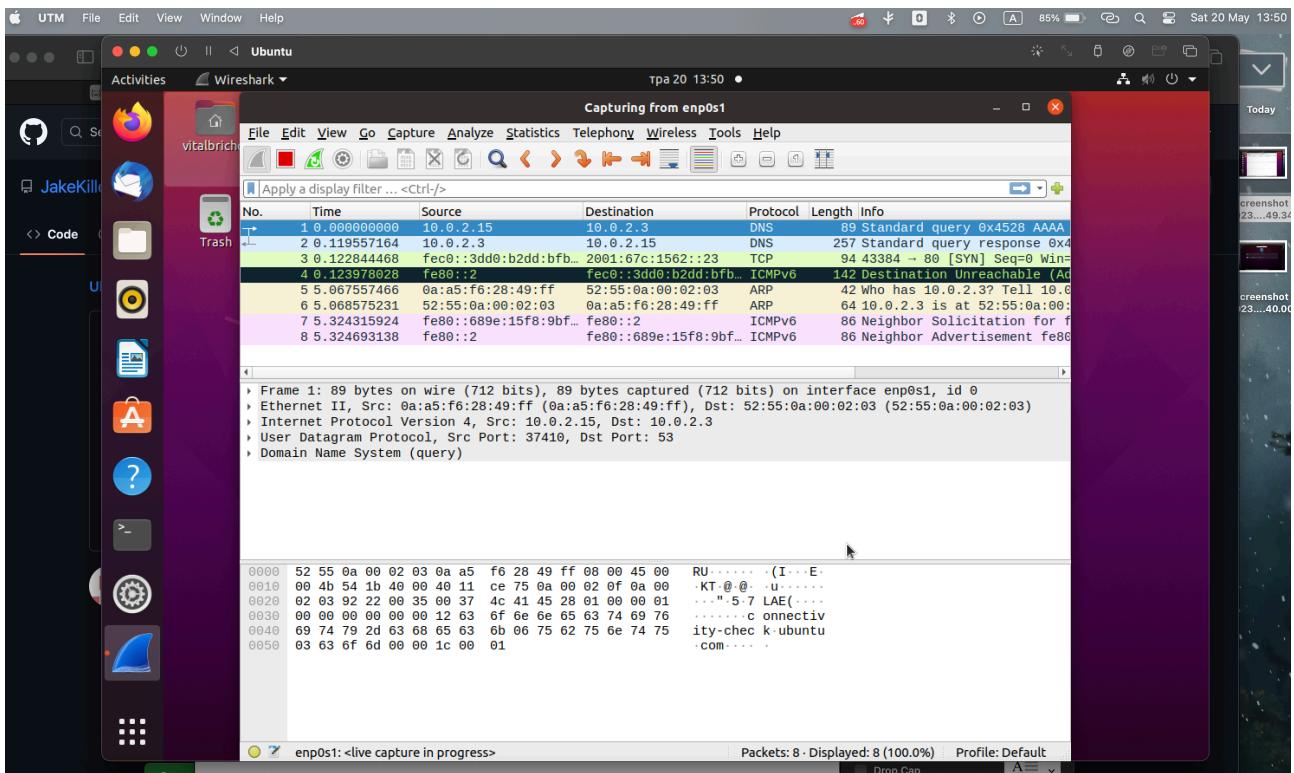
1. Була встановлена програма Wireshark на віртуальну ОС (Ubuntu).



2. Відкрили та запустили програму.



3. Запустили, для приклада, MozillaFirefox.



4. Ми можемо використати фільтр, який буде сортувати отриманні дані та показувати конкретні.

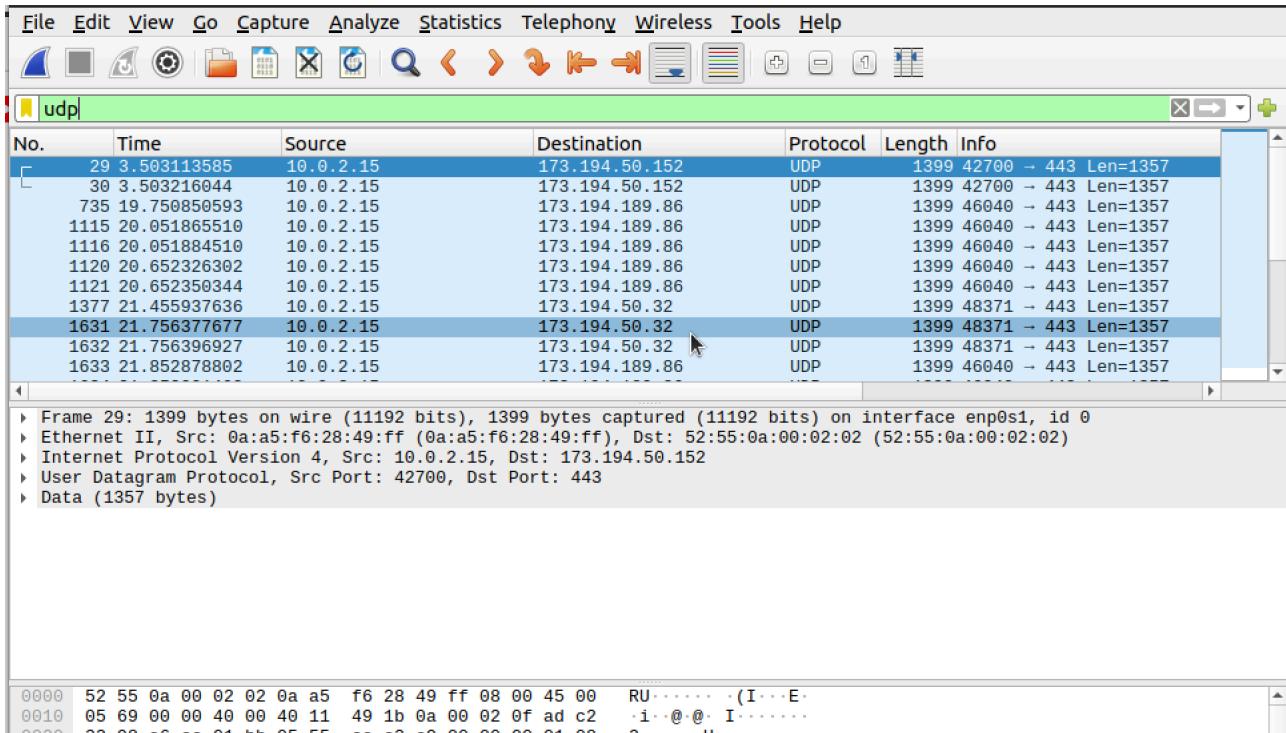
| No. | Time        | Source         | Destination    | Protocol | Length | Info                      |
|-----|-------------|----------------|----------------|----------|--------|---------------------------|
| 5   | 0.532586417 | 35.244.181.201 | 10.0.2.15      | TLSv1.2  | 100    | Application Data          |
| 6   | 0.532601126 | 10.0.2.15      | 35.244.181.201 | TCP      | 54     | 38358 → 443 [ACK] Seq=47  |
| 7   | 1.574875626 | 10.0.2.15      | 34.117.237.239 | TLSv1.2  | 93     | Application Data          |
| 8   | 1.574930959 | 10.0.2.15      | 34.117.65.55   | TLSv1.2  | 93     | Application Data          |
| 9   | 1.575089084 | 10.0.2.15      | 52.222.236.23  | TLSv1.2  | 100    | Application Data          |
| 10  | 1.575562459 | 34.117.237.239 | 10.0.2.15      | TCP      | 54     | 443 → 52562 [ACK] Seq=1 A |

5. В цьому прикладі ми шукаємо всі результати з протоколом TCP.

| No. | Time        | Source         | Destination    | Protocol | Length | Info                      |
|-----|-------------|----------------|----------------|----------|--------|---------------------------|
| 5   | 0.532586417 | 35.244.181.201 | 10.0.2.15      | TLSv1.2  | 100    | Application Data          |
| 6   | 0.532601126 | 10.0.2.15      | 35.244.181.201 | TCP      | 54     | 38358 → 443 [ACK] Seq=47  |
| 7   | 1.574875626 | 10.0.2.15      | 34.117.237.239 | TLSv1.2  | 93     | Application Data          |
| 8   | 1.574930959 | 10.0.2.15      | 34.117.65.55   | TLSv1.2  | 93     | Application Data          |
| 9   | 1.575089084 | 10.0.2.15      | 52.222.236.23  | TLSv1.2  | 100    | Application Data          |
| 10  | 1.575562459 | 34.117.237.239 | 10.0.2.15      | TCP      | 54     | 443 → 52562 [ACK] Seq=1 A |
| 11  | 1.575562959 | 34.117.65.55   | 10.0.2.15      | TCP      | 54     | 443 → 45854 [ACK] Seq=1 A |
| 12  | 1.575563043 | 52.222.236.23  | 10.0.2.15      | TCP      | 54     | 443 → 40346 [ACK] Seq=1 A |
| 13  | 1.575642501 | 10.0.2.15      | 52.222.236.23  | TLSv1.2  | 85     | Encrypted Alert           |
| 14  | 1.575974959 | 52.222.236.23  | 10.0.2.15      | TCP      | 54     | 443 → 40346 [ACK] Seq=1 A |
| 15  | 1.576167126 | 10.0.2.15      | 34.117.65.55   | TLSv1.2  | 78     | Application Data          |

Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp0s1, id 0  
Ethernet II, Src: 0:a5:f6:28:49:ff (0:a5:f6:28:49:ff), Dst: 52:55:0:a:00:02:02 (52:55:0:a:00:02:02)

## 6. Так само з UDP.



### Що таке протоколи UDP та TCP?

Протокол UDP - це швидкий протокол який відправляє пакети на пряму незважаючи хто отримувач, без запитів (але є вірогідність втрати декількох пакетів), зазвичай він використовується для трансляцій де важливий прямий ефір(twitch, YouTube), хоча й можлива втрата декількох фреймів (для людини вони майже непомітні)

Протокол TCP - для протокол, навпаки, важливо щоб дійшли всі пакети, він використовується для пересилання текстових повідомлень, де втрата декількох пакетів може кардинально вплинути на результат.