Adrian Herda 26844

Sprawozdanie 1

**Ping**

Ping to narzędzie do sprawdzania czy podane urządzenie istnieje w naszej sieci innymi słowy do sprawdzania połączenia pomiędzy naszym urządzeniem a serwerem.

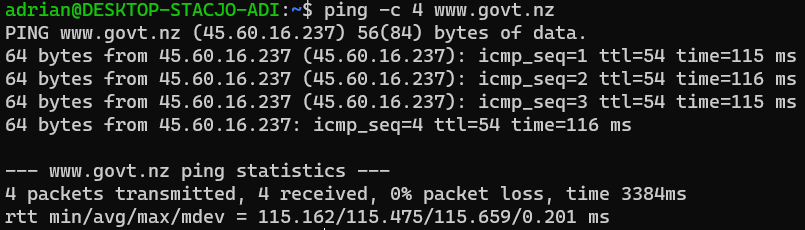
Wybrane możliwe opcje/parametry (Linux):

* **-t <ttl>** - ustawia wartość *time to live*
* **-4** - wymusza używanie IPv4
* **-6** - wymusza używanie IPv6
* **-s <wielkość>** - ustawia rozmiar (w bytach) danych do wysłania
* **-W <czas>** - ustawia czas czekania na odpowiedź
* **-c <ilość>** - zatrzymuje działanie programu po ustawionej ilości odpowiedzi
* **-M <do/dont/want>** - do zapobiega fragmentacji; dont nie zapobiega fragmentacji; want wykonuje badanie MTU, następuje fragmentacja przy dużych pakietach

TTL - to wartość, której główną funkcją jest zapobieganie tworzenia się pętli podczas szukania adresata wysyłanych danych. Jest to maksymalna liczba odwiedzonych serwerów na trasie naszych danych. Każdy serwer przez który przejdą wysłane przez nas dane zmniejsza wartość TTL przez co dane nie mogą krążyć w nieskończoność. Jednocześnie dzięki TTL możemy sprawdzać długość trasy która pokonały.

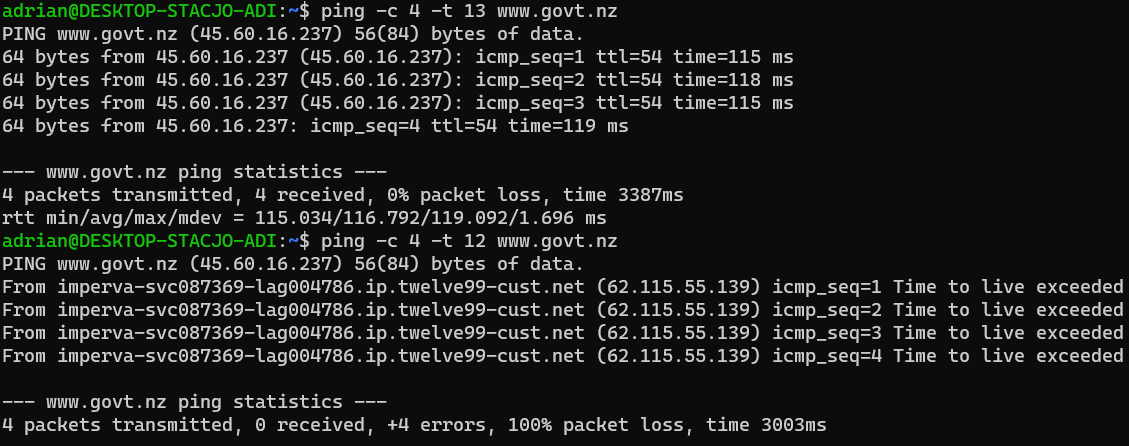
Stratowe wartości TTL róznią się zależnie od systemu operacyjnego, z którego dane zostały wysłane.

* Windows (nowsze wersje) - 128
* Linux, FreeBSD - 64



Na powyższym zrzucie ekranu TTL wynosi 54, oznacza że nasze dane na swojej drodze powrotnej pokonały 64 - 54 = **10** serwerów.

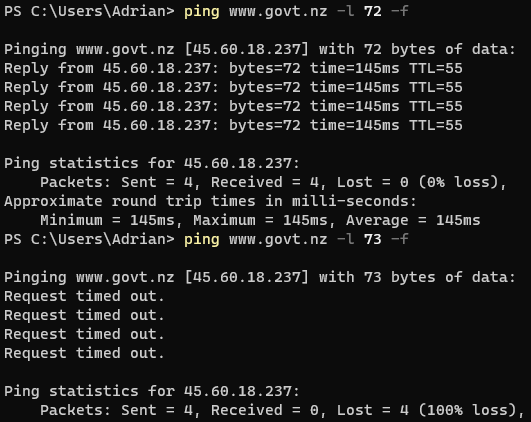
Drogę do serwera musimy znaleźć metodą ,,prób i błedów" wykorzystując opcje ***-t*** programu ping.



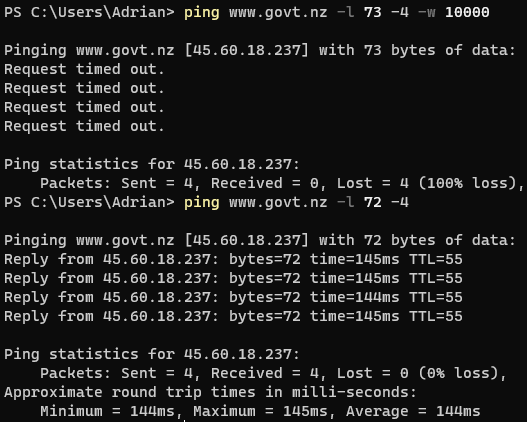
Zamieszony powyżej zrzut ekranu pokazuje że dla początkowego TTL = 13 nasze pakiety dotarły do celu ale już dla TTL = 12, nie powiodło się. Oznacza to że na drodze do serwera docelowego nasze dane pokonały 13 serwerów.

**Zmiana rozmiaru pakietu**

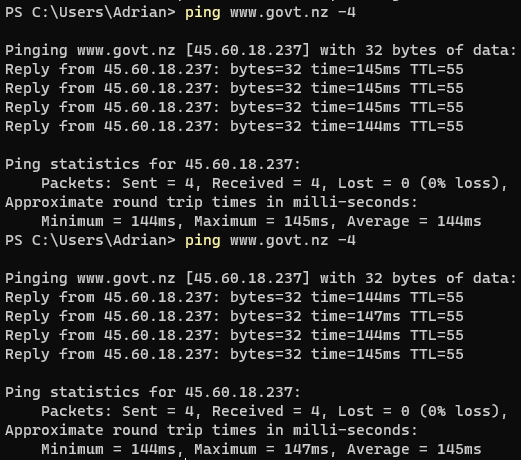
Dla odległego geograficznie serwera największy niefragmentowalny pakiet jaki udało mi się wysłać miał 100 bytów (72 plus 28 nagłówka)



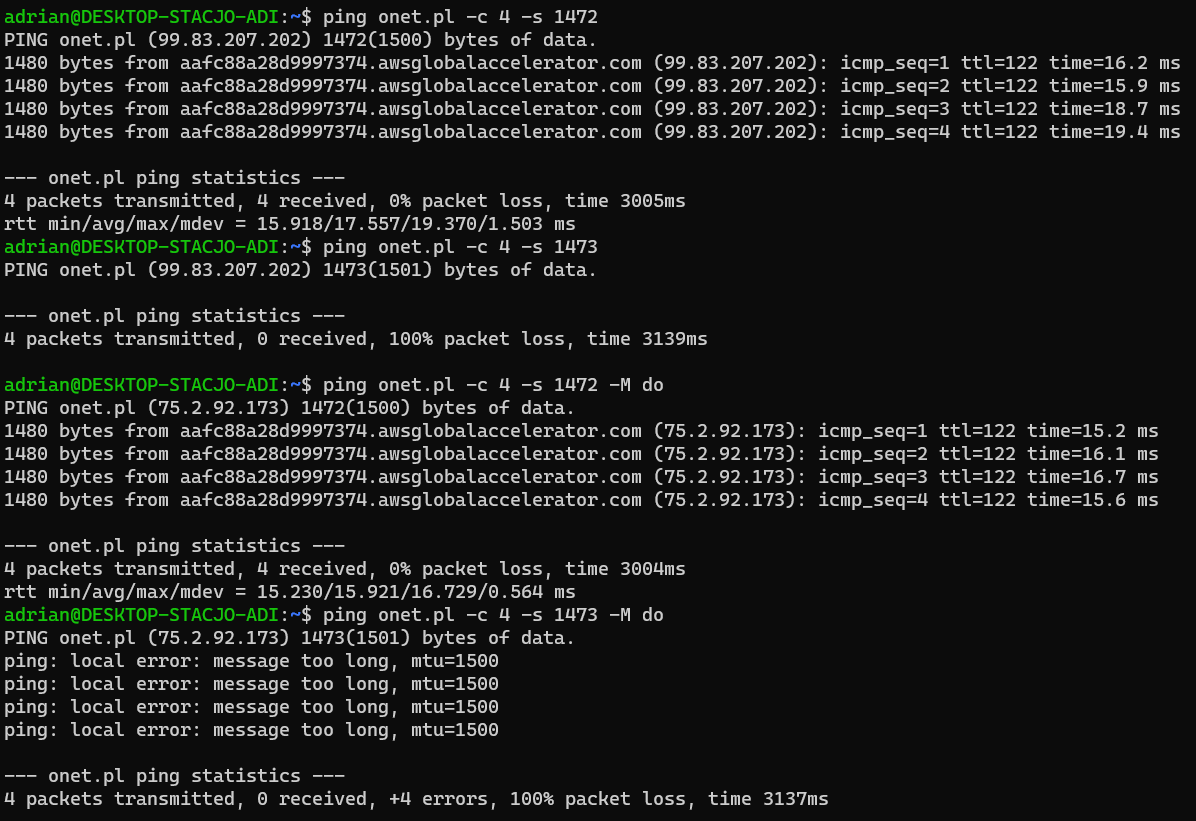
Jest to przy okazji największy plik jaki w ogóle udało mi się wysłać



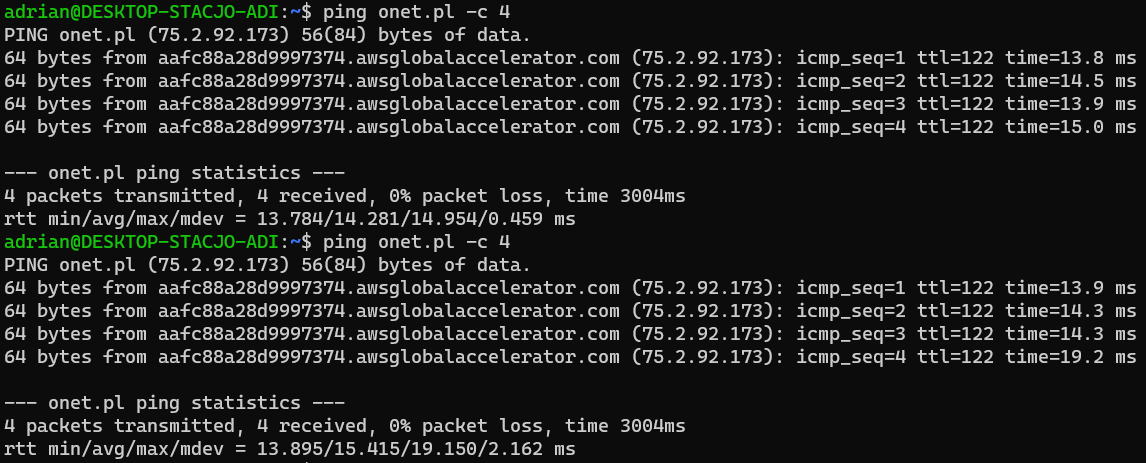
Fakt że pakiet jest niefragmentowany i większy nie zmienia ani trochę czasu ani drogi jaka była podczas próby kontrolnej:



Dla bliskiego geograficznie serwera ponownie największy plik niefragmentowany i fragmentowany wychodzi taki sam, trasa natomiast pozostaje pomiędzy obiema cały czas taka sama. różnica w czasie przesyłania pakietów jest pomijalnie mała (2ms).

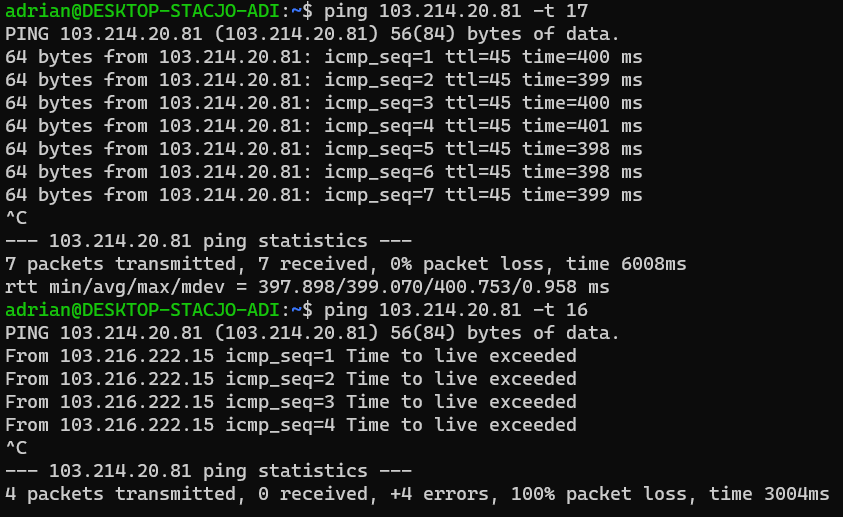


Prównując to z próba kontrolną widzimy że róznice trasach nie istnieją a róznice w czasch przesyłania sa bardzo małe.



**Średnica internetu**

Serwerem z najdłuższa trasą jaką znalazłem jest serwer do gry w minecraft osadzony w nowej zelandii o ip 103.214.20.81



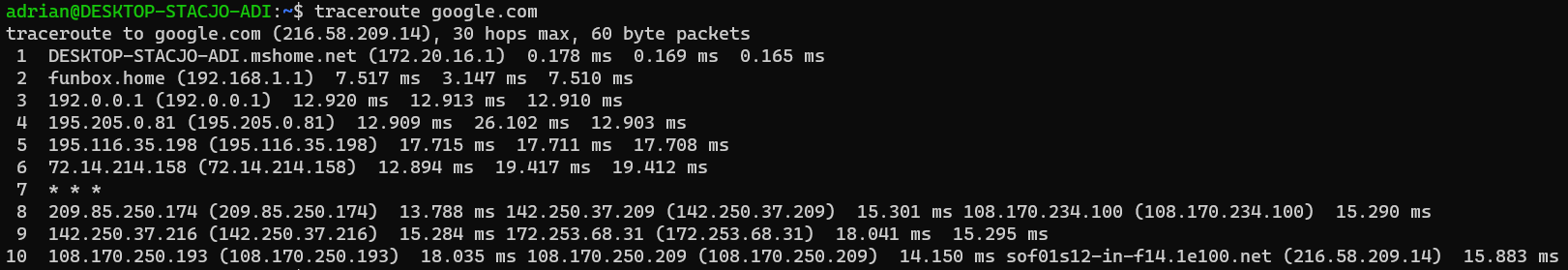
Dane wracając z danego serwera przeszły przez 64 - 45 = **19** serwerów a idąc do wykonały 17 skoków.

**Sieci wirtualne**

Trasy przechodzące przez sieci wirtualne są szczególnie trudne do analizy ponieważ wyżej wymienione sieci zmieniają wartości TTL. Sieci wirtualne można rozpoznać po tym że na przestrzeni czasu ukazują nam się znaczne róznice w wartościach TTL.

**Traceroute**

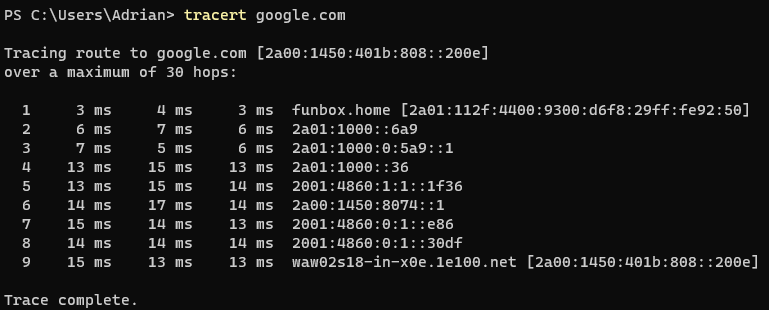
Traceroute to narzędzie służace do badania trasy wysyłanych przez nas danych do wybranego przez nas serwera. Program ten pokaże nam przez jakie serwery przechodzą nasze dane oraz czasy przesyłania ich na odcinkach pomiędzy nimi.



Z powyższego zrzutu ekranu wynika że wysłane przeze mnie dane pokonały trasę 10 serwerów\*.

\*Dane zawyżone o 1 ze względu na korzystanie z wirtualizacji systemu linux

\*\* Zrzut ekranu z windowsowego odpowiednika Tracert:

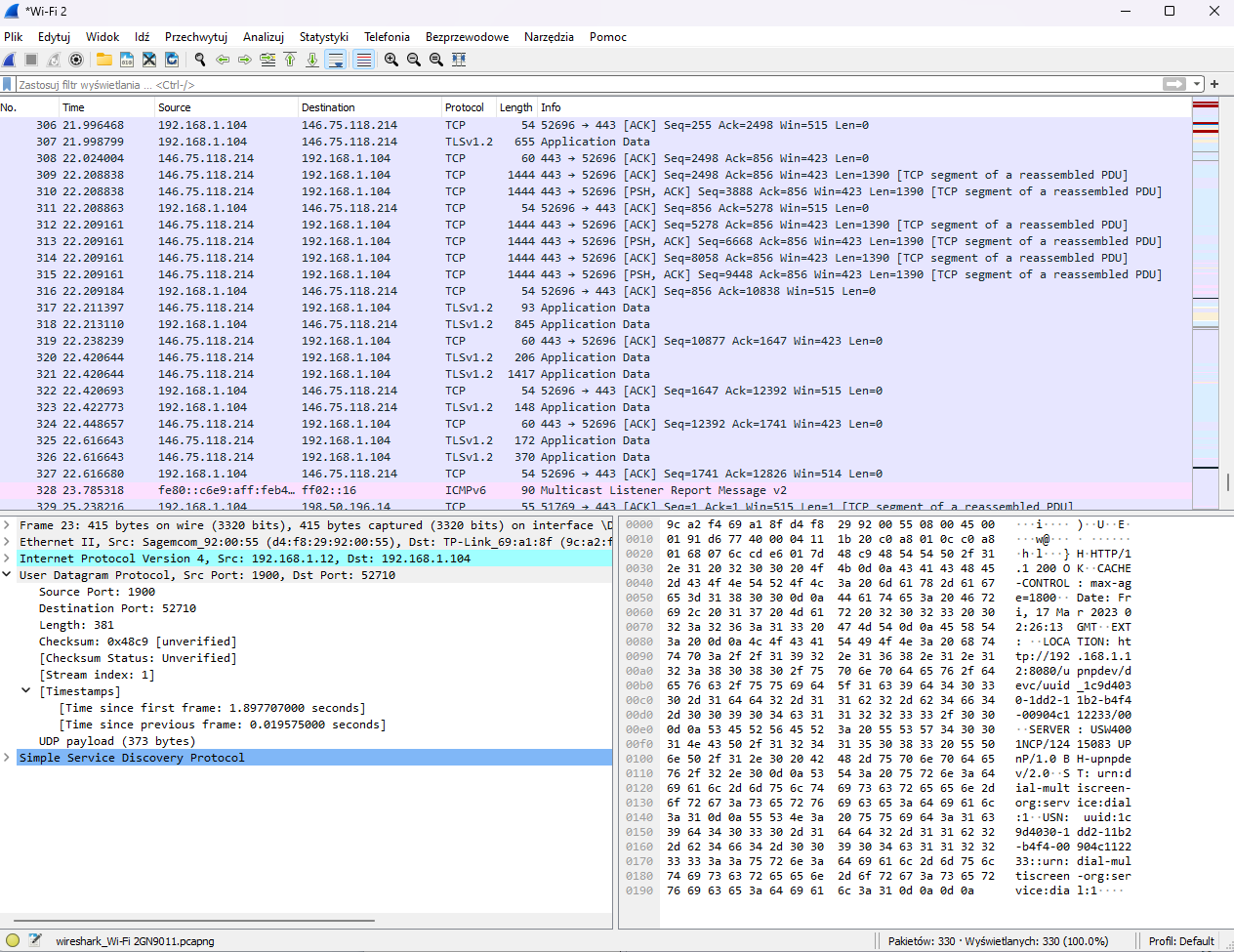


Tajemnicze gwiazdki w zrzucie ekranu oznaczają że serwer, przez który przeszły nasze dane, nie odpowiedział na dany pakiet. Może to wynikać z celowej konfiguracji tego serwera lub z problemami w sieci.

**Wireshark**

Darmowy program open-source do nagrywania, dekodowania oraz analizowania odbieranych pakietów. Program ten służy jedynie do ,,słuchania" i nie wpływa na odbierane dane ani na żadne aplikacje, które również przechwytują te same dane.

Wireshark ma pełno dodatków które bardzo ułatwiają pracę z tym programem. Jest idealnym narzędziem do analizowania użytych protokołów i ich właściwości.

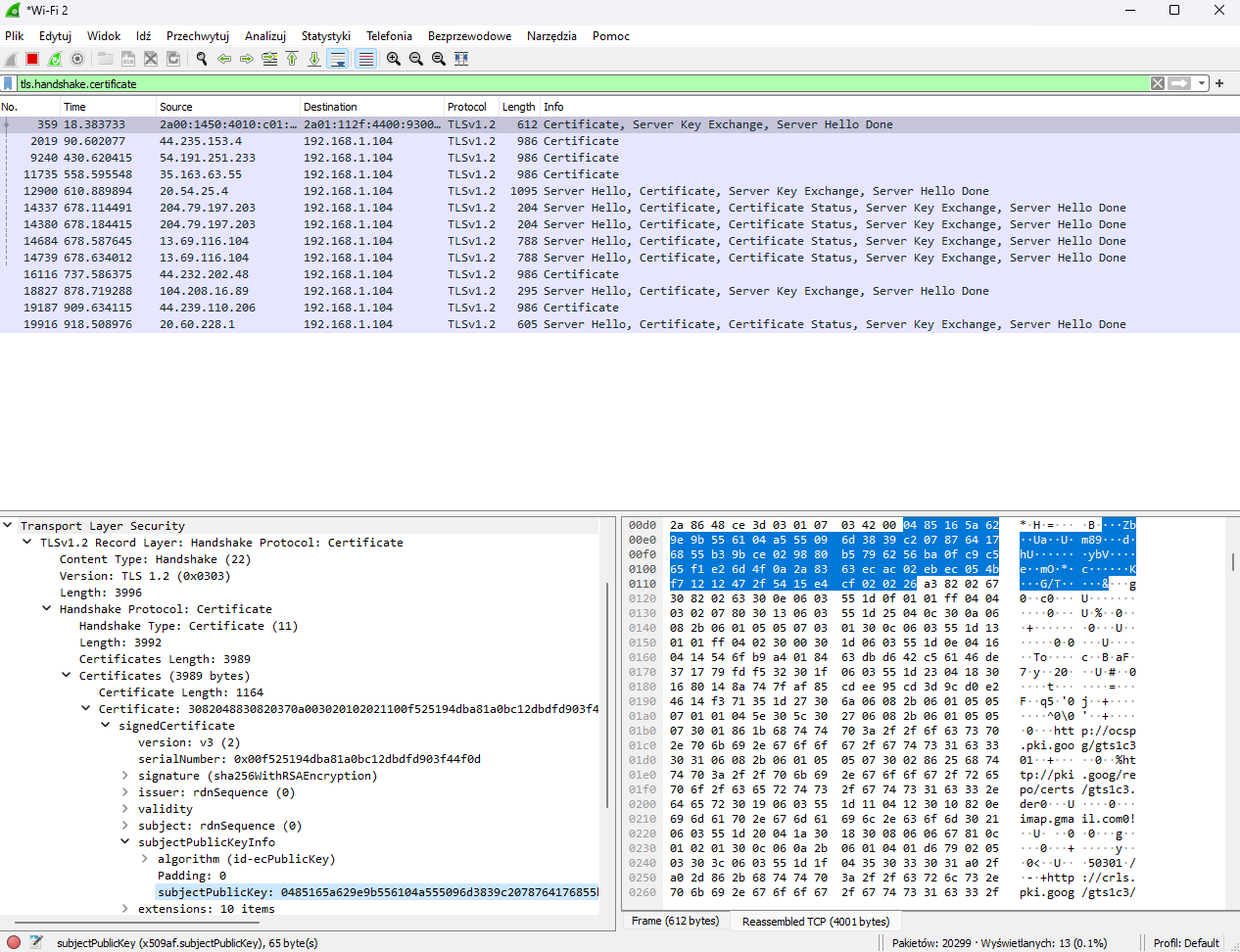


Na powyższym zrzucie ekranu można zobaczyć bardzo dużo informacji: na górze są przechwycone dane z podziałem kolumnowym na:

* Liczba porządkowa
* Czas przechwycenia od rozpoczęcia nagrywania liczony w sekundach
* Adres źródła
* Adres adresata
* Wykorzystany protokół
* Długość informacji liczona w bytach

W lewym dolnym rogu są szczegółowe informacje na temat wybranego pakietu.

W prawym dolnym rogu jest reprezentacja szesnastkowa przechwyconych danych. Na niebiesko jest podświetlona informacja (zaznaczona w lewym dolnym rogu) wybranego pakietu (zaznaczonego w górnej części okna).



Na powyższym zrzucie ekranu jest zaprezentowane jak możemy sprawdzić klucz publiczny z certyfikatu serwera strony z którą się łączymy.