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

```
adrian@DESKTOP-STACJO-ADI:~$ ping -c 4 www.govt.nz
PING www.govt.nz (45.60.16.237) 56(84) bytes of data.
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=1 ttl=54 time=115 ms
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=2 ttl=54 time=116 ms
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=3 ttl=54 time=115 ms
64 bytes from 45.60.16.237: icmp_seq=4 ttl=54 time=116 ms

--- www.govt.nz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3384ms
rtt min/avg/max/mdev = 115.162/115.475/115.659/0.201 ms
```

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.

```
adrian@DESKTOP-STACJO-ADI:~$ ping -c 4 -t 13 www.govt.nz
PING www.govt.nz (45.60.16.237) 56(84) bytes of data.
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=1 ttl=54 time=115 ms
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=2 ttl=54 time=118 ms
64 bytes from 45.60.16.237 (45.60.16.237): icmp_seq=3 ttl=54 time=115 ms
64 bytes from 45.60.16.237: icmp_seq=4 ttl=54 time=119 ms

--- www.govt.nz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3387ms
rtt min/avg/max/mdev = 115.034/116.792/119.092/1.696 ms
adrian@DESKTOP-STACJO-ADI:~$ ping -c 4 -t 12 www.govt.nz
PING www.govt.nz (45.60.16.237) 56(84) bytes of data.
From imperva-svc087369-lag004786.ip.twelve99-cust.net (62.115.55.139) icmp_seq=1 Time to live exceeded
From imperva-svc087369-lag004786.ip.twelve99-cust.net (62.115.55.139) icmp_seq=2 Time to live exceeded
From imperva-svc087369-lag004786.ip.twelve99-cust.net (62.115.55.139) icmp_seq=3 Time to live exceeded
From imperva-svc087369-lag004786.ip.twelve99-cust.net (62.115.55.139) icmp_seq=4 Time to live exceeded

--- www.govt.nz ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3003ms
```

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)

```
PS C:\Users\Adrian> ping www.govt.nz -l 72 -f

Pinging www.govt.nz [45.60.18.237] with 72 bytes of data:
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 145ms, Maximum = 145ms, Average = 145ms
PS C:\Users\Adrian> ping www.govt.nz -l 73 -f

Pinging www.govt.nz [45.60.18.237] with 73 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

```
PS C:\Users\Adrian> ping www.govt.nz -l 73 -4 -w 10000

Pinging www.govt.nz [45.60.18.237] with 73 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Adrian> ping www.govt.nz -l 72 -4

Pinging www.govt.nz [45.60.18.237] with 72 bytes of data:
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55
Reply from 45.60.18.237: bytes=72 time=144ms TTL=55
Reply from 45.60.18.237: bytes=72 time=145ms TTL=55

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 144ms, Maximum = 145ms, Average = 144ms
```

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

```
PS C:\Users\Adrian> ping www.govt.nz -4

Pinging www.govt.nz [45.60.18.237] with 32 bytes of data:
Reply from 45.60.18.237: bytes=32 time=145ms TTL=55
Reply from 45.60.18.237: bytes=32 time=145ms TTL=55
Reply from 45.60.18.237: bytes=32 time=145ms TTL=55
Reply from 45.60.18.237: bytes=32 time=144ms TTL=55

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 144ms, Maximum = 145ms, Average = 144ms
PS C:\Users\Adrian> ping www.govt.nz -4

Pinging www.govt.nz [45.60.18.237] with 32 bytes of data:
Reply from 45.60.18.237: bytes=32 time=144ms TTL=55
Reply from 45.60.18.237: bytes=32 time=147ms TTL=55
Reply from 45.60.18.237: bytes=32 time=144ms TTL=55
Reply from 45.60.18.237: bytes=32 time=145ms TTL=55

Ping statistics for 45.60.18.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 144ms, Maximum = 147ms, Average = 145ms
```

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).

```
adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4 -s 1472
PING onet.pl (99.83.207.202) 1472(1500) bytes of data.
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (99.83.207.202): icmp_seq=1 ttl=122 time=16.2 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (99.83.207.202): icmp_seq=2 ttl=122 time=15.9 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (99.83.207.202): icmp_seq=3 ttl=122 time=18.7 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (99.83.207.202): icmp_seq=4 ttl=122 time=19.4 ms

--- onet.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 15.918/17.557/19.370/1.503 ms
adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4 -s 1473
PING onet.pl (99.83.207.202) 1473(1501) bytes of data.

--- onet.pl ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3139ms

adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4 -s 1472 -M do
PING onet.pl (75.2.92.173) 1472(1500) bytes of data.
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=1 ttl=122 time=15.2 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=2 ttl=122 time=16.1 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=3 ttl=122 time=16.7 ms
1480 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=4 ttl=122 time=15.6 ms

--- onet.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 15.230/15.921/16.729/0.564 ms
adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4 -s 1473 -M do
PING onet.pl (75.2.92.173) 1473(1501) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500

--- onet.pl ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3137ms
```

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

```
adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4
PING onet.pl (75.2.92.173) 56(84) bytes of data.
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=1 ttl=122 time=13.8 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=2 ttl=122 time=14.5 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=3 ttl=122 time=13.9 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=4 ttl=122 time=15.0 ms

--- onet.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 13.784/14.281/14.954/0.459 ms
adrian@DESKTOP-STACJO-ADI:~$ ping onet.pl -c 4
PING onet.pl (75.2.92.173) 56(84) bytes of data.
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=1 ttl=122 time=13.9 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=2 ttl=122 time=14.3 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=3 ttl=122 time=14.3 ms
64 bytes from aafc88a28d9997374.awsglobalaccelerator.com (75.2.92.173): icmp_seq=4 ttl=122 time=19.2 ms

--- onet.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 13.895/15.415/19.150/2.162 ms
```

Średnica internetu

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

```
adrian@DESKTOP-STACJO-ADI:~$ ping 103.214.20.81 -t 17
PING 103.214.20.81 (103.214.20.81) 56(84) bytes of data.
64 bytes from 103.214.20.81: icmp_seq=1 ttl=45 time=400 ms
64 bytes from 103.214.20.81: icmp_seq=2 ttl=45 time=399 ms
64 bytes from 103.214.20.81: icmp_seq=3 ttl=45 time=400 ms
64 bytes from 103.214.20.81: icmp_seq=4 ttl=45 time=401 ms
64 bytes from 103.214.20.81: icmp_seq=5 ttl=45 time=398 ms
64 bytes from 103.214.20.81: icmp_seq=6 ttl=45 time=398 ms
64 bytes from 103.214.20.81: icmp_seq=7 ttl=45 time=399 ms
^C
--- 103.214.20.81 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 397.898/399.070/400.753/0.958 ms
adrian@DESKTOP-STACJO-ADI:~$ ping 103.214.20.81 -t 16
PING 103.214.20.81 (103.214.20.81) 56(84) bytes of data.
From 103.216.222.15 icmp_seq=1 Time to live exceeded
From 103.216.222.15 icmp_seq=2 Time to live exceeded
From 103.216.222.15 icmp_seq=3 Time to live exceeded
From 103.216.222.15 icmp_seq=4 Time to live exceeded
^C
--- 103.214.20.81 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3004ms
```

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

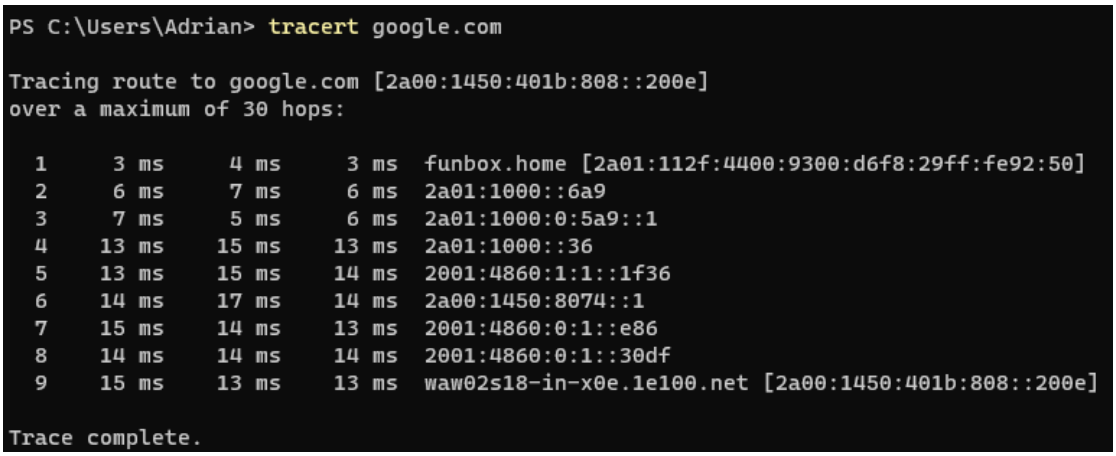
Traceroute to narzędzie służace do badania trasy wysyłanych przez nas danych do wybranego przez nas serwera. Program ten pokaże nam przez jakie serwery przechodzą nasze dane oraz czasy przesyłania ich na odcinkach pomiędzy nimi.

```
adrian@DESKTOP-STACJO-ADI:~$ traceroute google.com
traceroute to google.com (216.58.209.14), 30 hops max, 60 byte packets
 1  DESKTOP-STACJO-ADI.mshome.net (172.20.16.1)  0.178 ms  0.169 ms  0.165 ms
 2  funbox.home (192.168.1.1)  7.517 ms  3.147 ms  7.510 ms
 3  192.0.0.1 (192.0.0.1)  12.920 ms  12.913 ms  12.910 ms
 4  195.205.0.81 (195.205.0.81)  12.909 ms  26.102 ms  12.903 ms
 5  195.116.35.198 (195.116.35.198)  17.715 ms  17.711 ms  17.708 ms
 6  72.14.214.158 (72.14.214.158)  12.894 ms  19.417 ms  19.412 ms
 7  * * *
 8  209.85.250.174 (209.85.250.174)  13.788 ms 142.250.37.209 (142.250.37.209)  15.301 ms 108.170.234.100 (108.170.234.100)  15.290 ms
 9  142.250.37.216 (142.250.37.216)  15.284 ms 172.253.68.31 (172.253.68.31)  18.041 ms  15.295 ms
10  108.170.250.193 (108.170.250.193)  18.035 ms 108.170.250.209 (108.170.250.209)  14.150 ms sof01s12-in-f14.1e100.net (216.58.209.14)  15.883 ms
```

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:

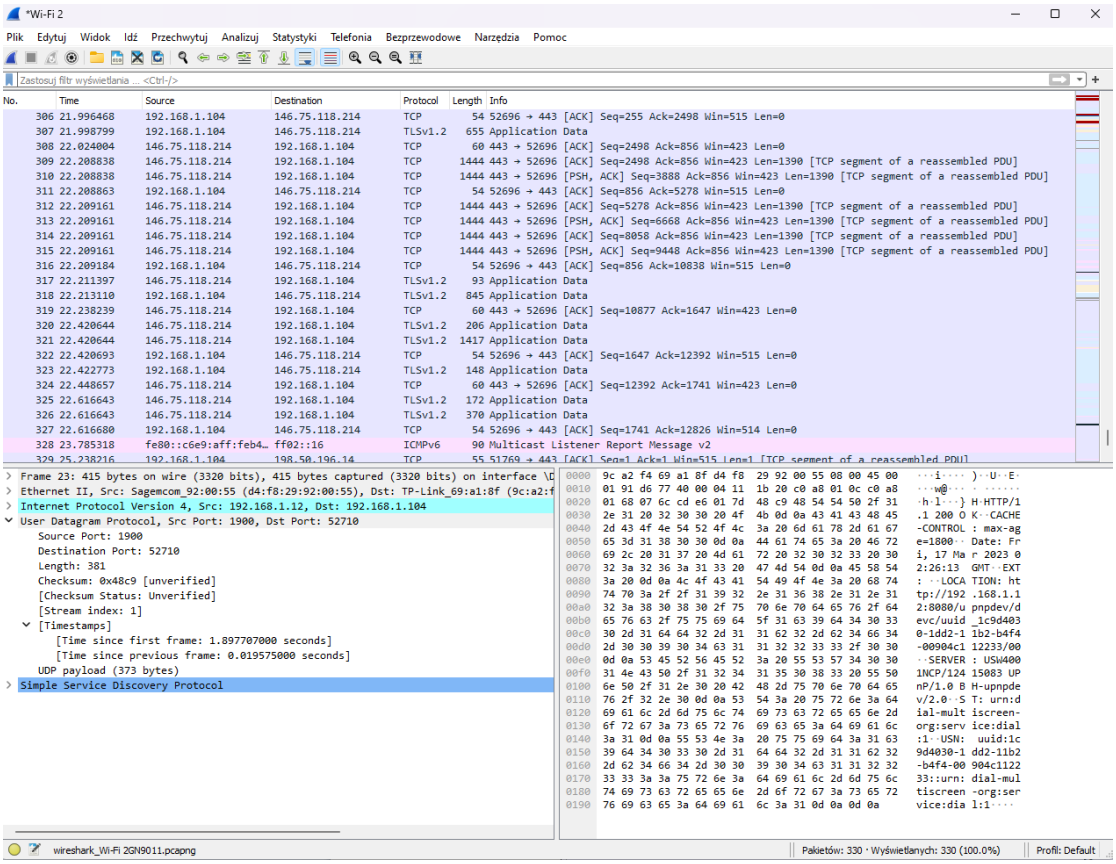


Tajemnicze gwiazdki w zrzucie ekranu oznaczają że serwer, przez który przeszły nasze dane, nie odpowiedział na dany pakiet. Może to wynikać z celowej konfiguracji tego serwera lub z problemami w sieci.

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.

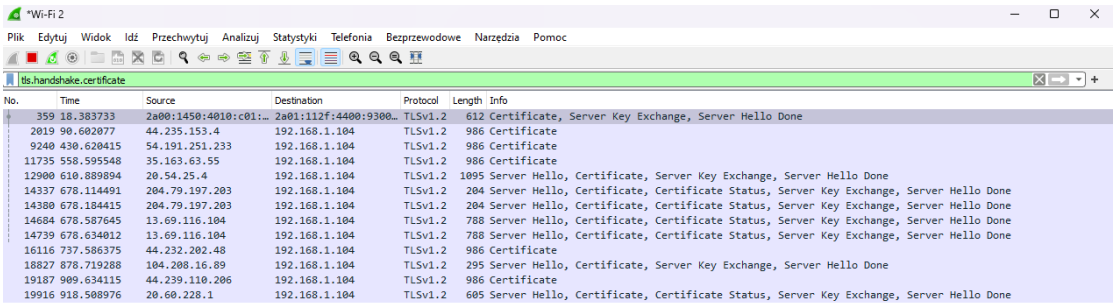


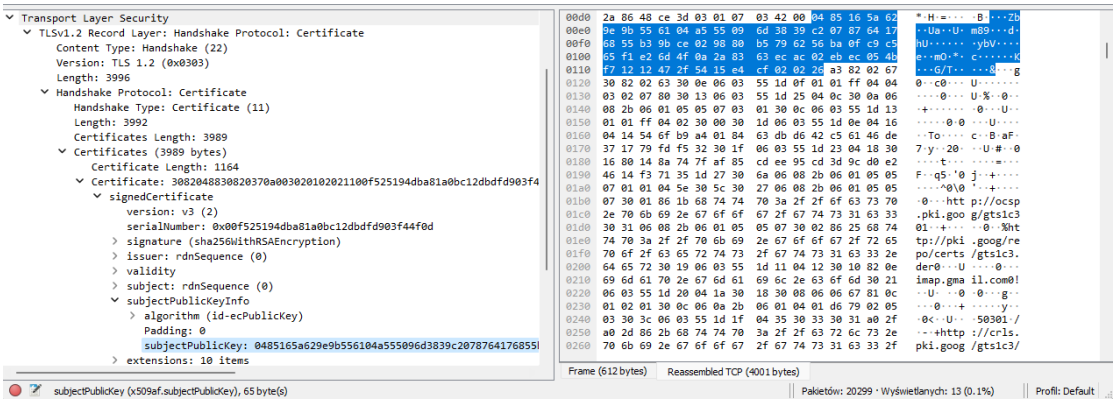
Na powyższym zrzucie ekranu można zobaczyć bardzo dużo informacji: na górze są przechwycone dane z podziałem kolumnowym na:

- 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.