

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 bajtach) danych do wysłania
- **-W <czas>** - ustawia czas czekania na odpowiedź
- **-c <ilość>** - zatrzymuje działanie programu po ustawionej ilości odpowiedzi
- **-M <do/dont/want>** - do zapobiegania 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 różnią 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 rzucie 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 błędów” 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

```

Zamieszczony 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 bajtów (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 próbą kontrolną widzimy że różnice trasach nie istnieją a różnice w czasach 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 najdłuższą 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 różnice w wartościach TTL.

Traceroute

Traceroute to narzędzie służące 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:

```

PS C:\Users\Adrian> tracert google.com

Tracing route to google.com [2a00:1450:401b:808::200e]
over a maximum of 30 hops:

  1    3 ms    4 ms    3 ms  funbox.home [2a01:112f:4400:9300:d6f8:29ff:fe92:50]
  2    6 ms    7 ms    6 ms  2a01:1000::6a9
  3    7 ms    5 ms    6 ms  2a01:1000:0:5a9::1
  4   13 ms   15 ms   13 ms  2a01:1000::36
  5   13 ms   15 ms   14 ms  2001:4860:1:1::1f36
  6   14 ms   17 ms   14 ms  2a00:1450:8074::1
  7   15 ms   14 ms   13 ms  2001:4860:0:1::e86
  8   14 ms   14 ms   14 ms  2001:4860:0:1::30df
  9   15 ms   13 ms   13 ms  waw02s18-in-x0e.1e100.net [2a00:1450:401b:808::200e]

Trace complete.

```

Tajemnicze gwiazdki w rzucie ekranu oznaczają że serwer, przez który przeszedł 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 przechwytyują te same dane.

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

No.	Time	Source	Destination	Protocol	Length	Info
306	21.996468	192.168.1.104	146.75.118.214	TCP	54	52696 → 443 [ACK] Seq=255 Ack=2498 Win=515 Len=0
307	21.998799	192.168.1.104	146.75.118.214	TLSv1.2	655	Application Data
308	22.024004	146.75.118.214	192.168.1.104	TCP	60	443 → 52696 [ACK] Seq=2498 Ack=856 Win=423 Len=0
309	22.208838	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [ACK] Seq=2498 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
310	22.208838	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [PSH, ACK] Seq=3888 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
311	22.208863	192.168.1.104	146.75.118.214	TCP	54	52696 → 443 [ACK] Seq=856 Ack=5278 Win=515 Len=0
312	22.209161	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [ACK] Seq=5278 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
313	22.209161	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [PSH, ACK] Seq=6668 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
314	22.209161	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [ACK] Seq=8058 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
315	22.209161	146.75.118.214	192.168.1.104	TCP	1444	443 → 52696 [PSH, ACK] Seq=9448 Ack=856 Win=423 Len=1390 [TCP segment of a reassembled PDU]
316	22.209184	192.168.1.104	146.75.118.214	TCP	54	52696 → 443 [ACK] Seq=856 Ack=10838 Win=515 Len=0
317	22.211397	146.75.118.214	192.168.1.104	TLSv1.2	93	Application Data
318	22.213118	192.168.1.104	146.75.118.214	TLSv1.2	845	Application Data
319	22.238239	146.75.118.214	192.168.1.104	TCP	60	443 → 52696 [ACK] Seq=10877 Ack=1647 Win=423 Len=0
320	22.420644	146.75.118.214	192.168.1.104	TLSv1.2	206	Application Data
321	22.420644	146.75.118.214	192.168.1.104	TLSv1.2	1417	Application Data
322	22.420693	192.168.1.104	146.75.118.214	TCP	54	52696 → 443 [ACK] Seq=1647 Ack=12392 Win=515 Len=0
323	22.422773	192.168.1.104	146.75.118.214	TLSv1.2	148	Application Data
324	22.448657	146.75.118.214	192.168.1.104	TCP	60	443 → 52696 [ACK] Seq=12392 Ack=1741 Win=423 Len=0
325	22.616643	146.75.118.214	192.168.1.104	TLSv1.2	172	Application Data
326	22.616643	146.75.118.214	192.168.1.104	TLSv1.2	370	Application Data
327	22.616680	192.168.1.104	146.75.118.214	TCP	54	52696 → 443 [ACK] Seq=1741 Ack=12826 Win=514 Len=0
328	23.785318	fe80::c6e9:aff:feb4::f802:16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
329	25.238216	192.168.1.104	198.58.196.14	TCP	55	51269 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=0 [TCP segment of a reassembled PDU]

Frame 23: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface Wi-Fi 2

Ethernet II, Src: Sagemcom_92:00:55 (dc:f8:29:52:00:55), Dst: TP-Link_69:a1:8f (9c:a2:f8:69:a1:8f)

Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.104

User Datagram Protocol, Src Port: 1980, Dst Port: 52710

Source Port: 1980

Destination Port: 52710

Length: 381

Checksum: 0x48c9 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

[Time since first frame: 1.897707000 seconds]

[Time since previous frame: 0.019575000 seconds]

UDP payload (373 bytes)

Simple Service Discovery Protocol

0000 9c a2 f4 69 a1 8f 04 f8 20 92 00 55 00 00 45 00 ...1.... }-U-E

0010 01 91 d6 77 40 00 04 11 1b 20 c0 a8 01 0c c0 a8 ...m8....

0020 01 68 07 6c cd e6 01 7d 48 c9 48 54 50 2f 31 ..h1...} H-HTTP/1

0030 2e 31 20 32 30 30 20 4f 4b 0d 0a 43 41 43 48 45 ..1 200 O K-CACHE

0040 2d 43 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 -CONTROL : max-ag

0050 65 3d 31 38 30 30 0d 0a 44 61 74 65 3a 20 46 72 e=1800 Date: Fr

0060 69 2c 20 31 37 20 4d 61 72 20 32 30 32 30 30 i, 17 Ma 2023 0

0070 32 3a 32 36 3a 31 33 20 47 4d 54 0d 0a 45 50 54 2:26:13 GMT-EXT

0080 3a 20 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 74 :--LOCA TION: ht

0090 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 31 2e 31 tp://192.168.1.1

00a0 32 3a 38 30 38 30 2f 75 70 6e 70 64 65 76 2f 64 2:8080/u pnpdev/d

00b0 65 76 63 2f 75 75 69 64 5f 31 63 39 64 34 30 33 evc/uuid_1c90403

00c0 30 2d 31 64 64 32 2d 31 31 62 32 2d 62 34 66 34 0-1dd2-1 1b2-b4f4

00d0 2d 30 30 39 30 34 63 31 31 32 32 33 33 2f 30 30 -00904c1 12233/00

00e0 0d 0a 53 45 52 56 45 52 3a 20 55 53 57 34 30 30 --SERVER : USW400

00f0 31 4e 43 50 2f 31 32 34 31 35 30 38 33 20 55 50 1NCP/124 15083 UP

0100 6e 50 2f 31 2e 30 20 42 48 2d 75 70 6e 70 64 65 nP/1.0 B H-upnpde

0110 76 2f 32 2e 30 0d 0a 53 54 3a 20 75 72 6e 3a 64 v/2.0 S T: urn:d

0120 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e 2d ial=mult iscreen-

0130 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 6c org:serv ice:dial

0140 3a 31 0d 0a 55 53 4e 3a 20 75 75 69 64 3a 31 63 :1--USN: uuid:1c

0150 39 64 34 30 33 30 2d 31 64 64 32 2d 31 31 62 32 9d4030-1 dd2-11b2

0160 2d 62 34 66 34 2d 30 30 39 30 34 63 31 31 32 32 -b4f4-00 904c1122

0170 33 33 3a 3a 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 33::urn: dial-mul

0180 74 69 73 63 72 65 65 6e 2d 6f 72 67 3a 73 65 72 tiscreen -org:ser

0190 76 69 63 65 3a 64 69 61 6c 3a 31 0d 0a 0d 0a vice:dial 11:....

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 bajtach

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

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

No.	Time	Source	Destination	Protocol	Length	Info
359	18.383733	2a00:1450:4010:c01::	2a01:112f:4400:9300::	TLSv1.2	612	Certificate, Server Key Exchange, Server Hello Done
2019	90.602077	44.235.153.4	192.168.1.104	TLSv1.2	986	Certificate
9240	430.620415	54.191.251.233	192.168.1.104	TLSv1.2	986	Certificate
11735	558.595548	35.163.63.55	192.168.1.104	TLSv1.2	986	Certificate
12900	610.889894	20.54.25.4	192.168.1.104	TLSv1.2	1095	Server Hello, Certificate, Server Key Exchange, Server Hello Done
14337	678.114491	204.79.197.203	192.168.1.104	TLSv1.2	204	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
14380	678.184415	204.79.197.203	192.168.1.104	TLSv1.2	204	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
14684	678.587645	13.69.116.104	192.168.1.104	TLSv1.2	788	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
14739	678.634012	13.69.116.104	192.168.1.104	TLSv1.2	788	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
16116	737.586375	44.232.202.48	192.168.1.104	TLSv1.2	986	Certificate
18827	878.719288	104.200.16.89	192.168.1.104	TLSv1.2	295	Server Hello, Certificate, Server Key Exchange, Server Hello Done
19187	909.634115	44.239.110.206	192.168.1.104	TLSv1.2	986	Certificate
19916	918.508976	20.60.228.1	192.168.1.104	TLSv1.2	605	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done

- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3996
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3992
 - Certificates Length: 3989
 - Certificates (3989 bytes)
 - Certificate Length: 1164
 - Certificate: 3082048830820370a003020102021100f525194da81a0bc12dbddf903f44f0d
 - signedCertificate
 - version: v3 (2)
 - serialNumber: 0x00f525194da81a0bc12dbddf903f44f0d
 - signature (sha256WithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - algorithm (id-ecPublicKey)
 - padding: 0
 - subjectPublicKey: 0485165a629e9b556104a555096d3839c20787641768551
 - extensions: 10 items

```

00d0 2a 86 48 ce 3d 03 01 07 03 42 00 04 85 16 5a 62  *H-----B-----
00e0 0e 8b 55 61 04 a5 55 03 6d 38 39 c2 07 87 64 17  ..Ua..U..a09...d
00f0 68 55 b3 9b ce 02 98 80 b5 79 62 56 ba 0f c9 c5  nu.....ybV...
0100 65 f1 e2 6d 4f 0a 2a 83 63 ec ac 02 eb ec 05 4b  e..m0+..c.....k
0110 f7 12 12 47 2f 54 15 a4 cf 02 02 28 a3 82 02 67  ...G/T...--g
0120 30 82 02 63 30 06 06 03 55 1d 0f 01 01 ff 04 04  0..c0...U.....
0130 03 02 07 00 30 13 06 03 55 1d 25 04 0c 30 0a 06  ...0...U%..0..
0140 08 2b 06 01 05 05 07 03 01 30 0c 06 03 55 1d 13  +-----0...U..
0150 01 01 ff 04 02 30 00 30 1d 06 03 55 1d 0e 04 16  +-----0...U...
0160 04 14 54 6f b9 a4 01 84 63 db d6 42 c5 61 46 de  ..To.....c:B:aF
0170 37 17 79 fd f5 32 30 1f 06 03 55 1d 23 04 18 30  7..y..20...U:#..0
0180 16 00 14 8a 74 7f af 85 c0 ee 95 cd 3d 9c 00 e2  ...t.....
0190 46 14 f3 71 35 1d 27 30 6a 06 08 2b 06 01 05 05  F..q5'0 j..+....
01a0 07 01 01 04 5e 30 5c 30 27 06 08 2b 06 01 05 05  ....0\0 j..+....
01b0 07 30 01 86 1b 68 74 74 70 3a 2f 2f 6f 63 73 70  0...htt p://ocsp
01c0 2e 70 6b 69 2e 67 6f 6f 67 2f 67 74 73 31 63 33  .pki.goo g/gtsic3
01d0 30 31 06 08 2b 06 01 05 05 07 30 02 86 25 68 74  01..+...0 ...hnt
01e0 74 70 3a 2f 2f 70 6b 69 2e 67 6f 6f 67 2f 72 65  tpt//pki .goog/re
01f0 70 6f 2f 63 65 72 74 73 2f 67 74 73 31 63 33 2e  po/certs /gtsic3.
0200 64 65 72 30 19 06 03 55 1d 11 04 12 30 10 82 0e  der0...U ...0...
0210 69 6d 61 70 2e 67 6d 61 69 6c 2e 63 6f 6d 30 21  imap.gma il.com0!
0220 06 03 55 1d 20 04 1a 30 18 30 08 06 06 67 81 0c  ..U...0 ...g..
0230 01 02 01 30 0c 06 0a 2b 06 01 04 01 06 79 02 05  ...0...+...y...
0240 03 30 3c 06 03 55 1d 1f 04 35 30 33 30 31 a0 2f  0<c..U.../50301./
0250 a0 2d 86 2b 68 74 74 70 3a 2f 67 63 72 6c 73 2e  --+http //crls.
0260 70 6b 69 2e 67 6f 6f 67 2f 67 74 73 31 63 33 2f  pki.goog /gtsic3/

```

subjectPublicKey (x509af.subjectPublicKey), 65 byte(s)

Frame (612 bytes) Reassembled TCP (4001 bytes)

Pakietów: 20299 · Wyświetlanych: 13 (0.1%)

Profil: Default

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