**Technologie sieciowe – lista 1**

**Szymon Hładyszewski**

1. Opis programów

1.1 Ping

Ping to narzędzie używane do sprawdzania dostępności hosta w sieci IP. Wysyła pakiety ICMP Echo Request do docelowego hosta i oczekuje na odpowiedź ICMP Echo Reply. Umożliwia ocenę opóźnienia (czasu propagacji) oraz sprawdzenie jakości połączenia sieciowego.

1.2 Traceroute

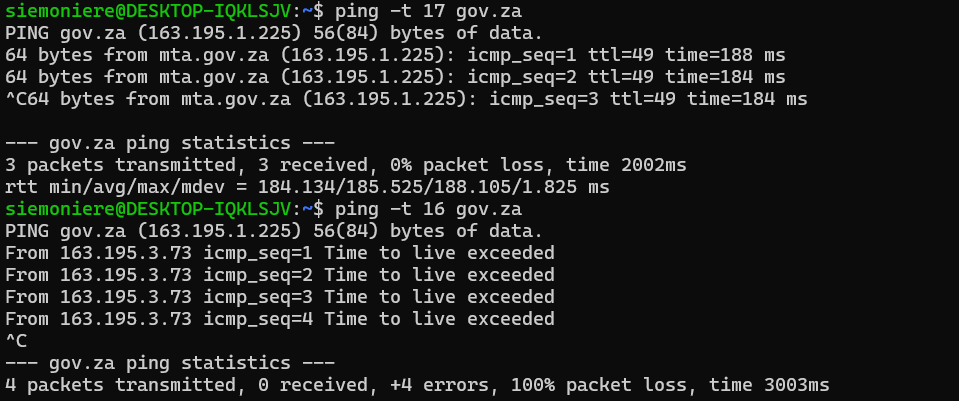
Traceroute to narzędzie służące do identyfikacji trasy, jaką przebywa pakiet z jednego hosta do drugiego w sieci.

1.3 WireShark

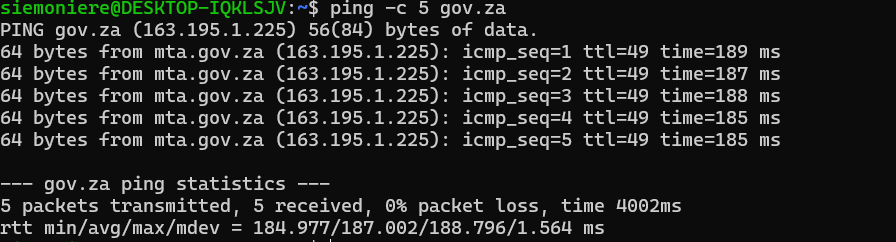
WireShark to narzędzie do analizy ruchu sieciowego, które umożliwia przechwytywanie i szczegółową analizę pakietów przesyłanych w sieci. Wywołania i analiza wyników

2.1.1 Badanie za pomocą Ping

Wybrany przeze mnie serwer: gov.za (RPA)

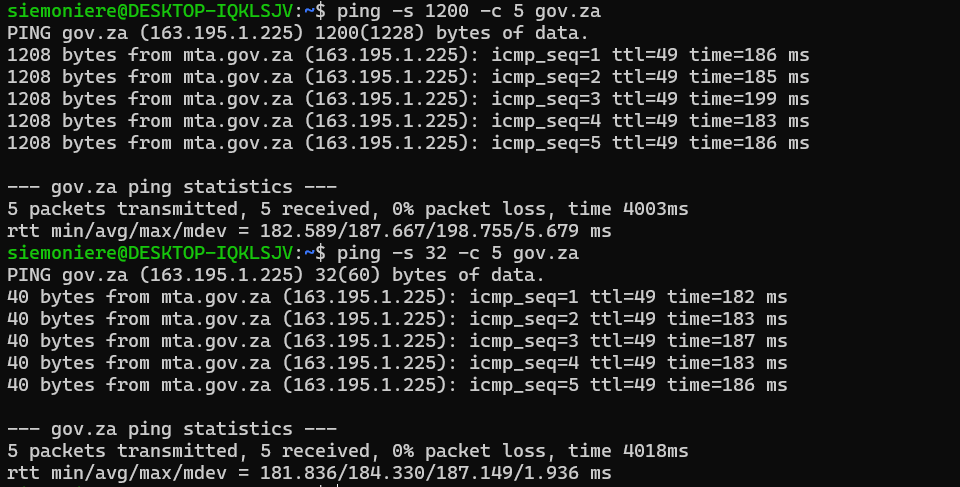


Na podstawie powyższych informacji widzimy, że skoków do tego serwera jest 17, ponieważ dla ttl (Time to live) równego 16 wiadomość nie dociera ze względu na to, że z każdym węzłem ttl maleje o 1.

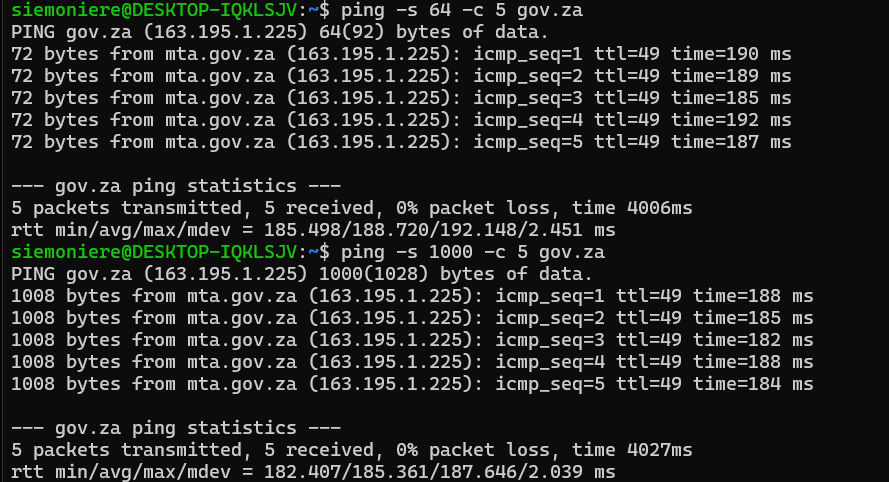


Powyżej przedstawiona jest trasa od serwera. Zostało wysłanych 5 pakietów, każdy z nich dotarł w niecałe 190ms.

2.1.2 Wpływ wielkości pakietu na czas propagacji



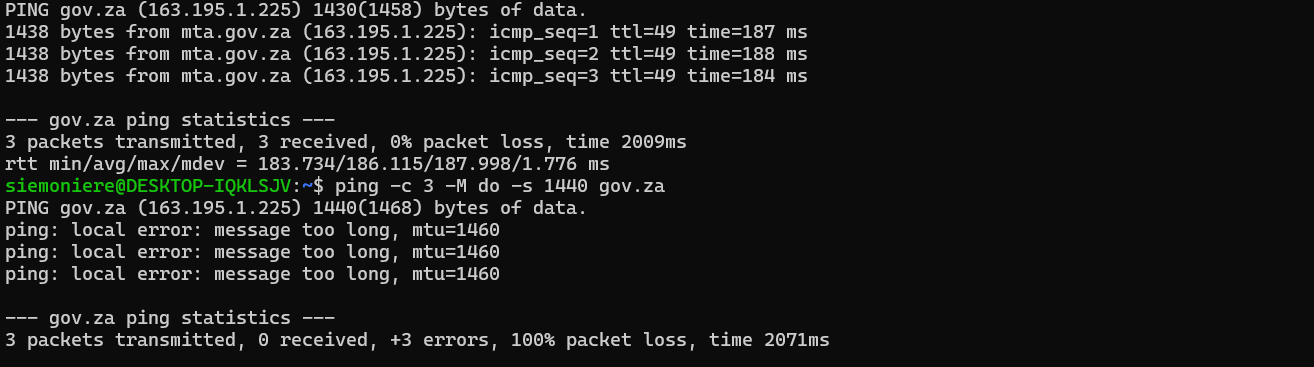
Zgodnie z przewidywaniami, większy pakiet (1200 bajtów) potrzebuje więcej czasu, aby dotrzeć od nadawcy do odbiorcy, choć różnice te są dosyć niewielkie. Na potwierdzenie tego, poniżej znajduje się przypadek, w którym większy pakiet (1000 bajtów) dociera szybciej.



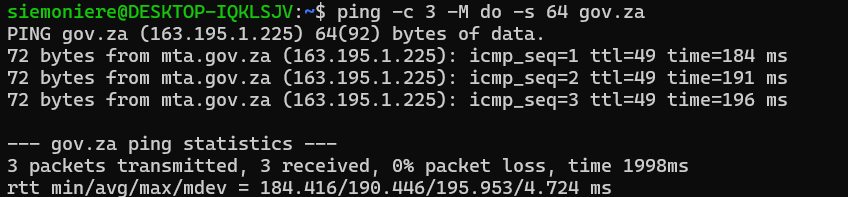
Widzimy tutaj, że avg rtt (Round Trip Time) jest mniejszy w pakiecie 1000 bajtów. Niemniej jednak, mniejsze pakiety są bardziej stabilne – ich czas nie jest aż tak zróżnicowany jak dla większych pakietów.

2.1.3 Maksymalny niefragmentowny pakiet

Standardowy MTU (Maximum Transmission Unit) dla Ethernetu wynosi 1500 bajtów, natomiast w moim przypadku 1468 bajtów (1440 + 28 z nagłówków IP i ICMP) stanowiło już za długą wiadomość. Może to wynikać z używania VPN (nie w moim przypadku), tunelowania lub firewalli.

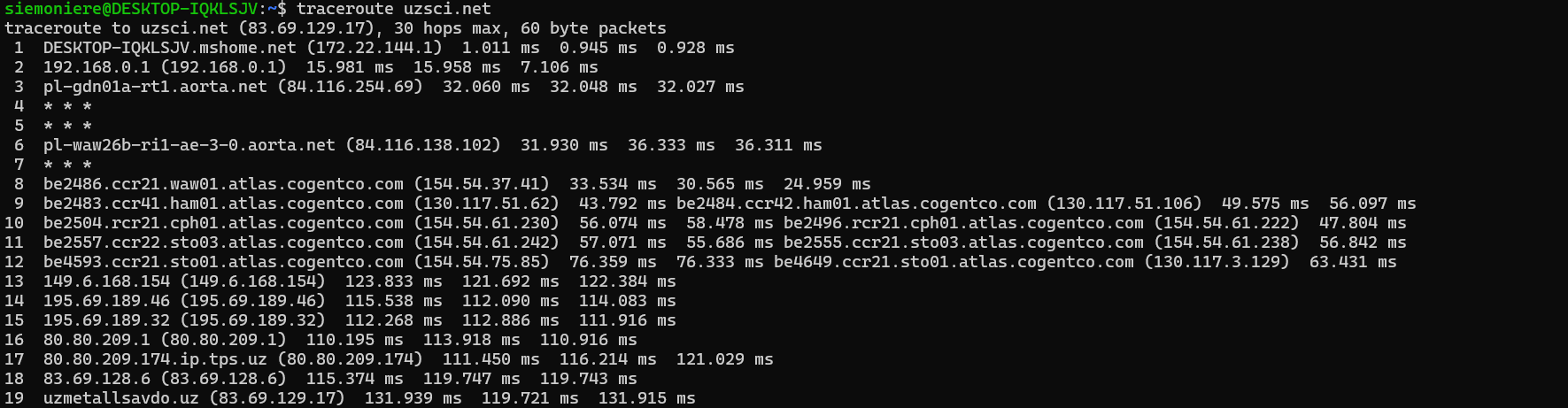


Dla mniejszych pakietów (64 bajty) można zaobserwować nieznacznie krótszy czas trwania operacji:

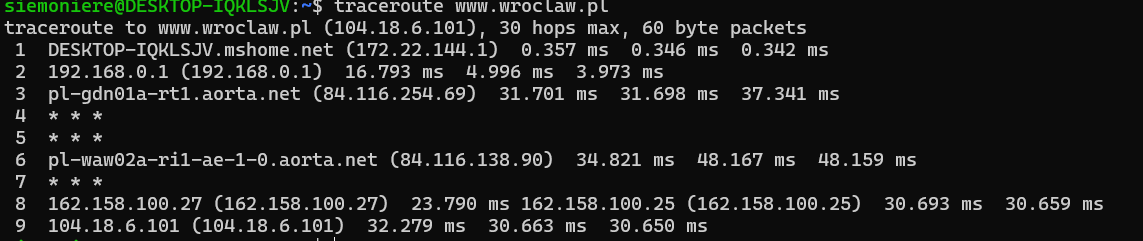


2.2 Badanie średnicy internetu za pomocą Traceroute

Najdłuższa trasa, którą udało mi się znaleźć, dociera do Uzbekistanu. Widoczne w punktach 4., 5. oraz 7. przeskoki świadczą o tym, że pakiet mógł przejść przez sieci wirtualne (sieć VPN lub tunel, który nie odpowiada na ICMP).



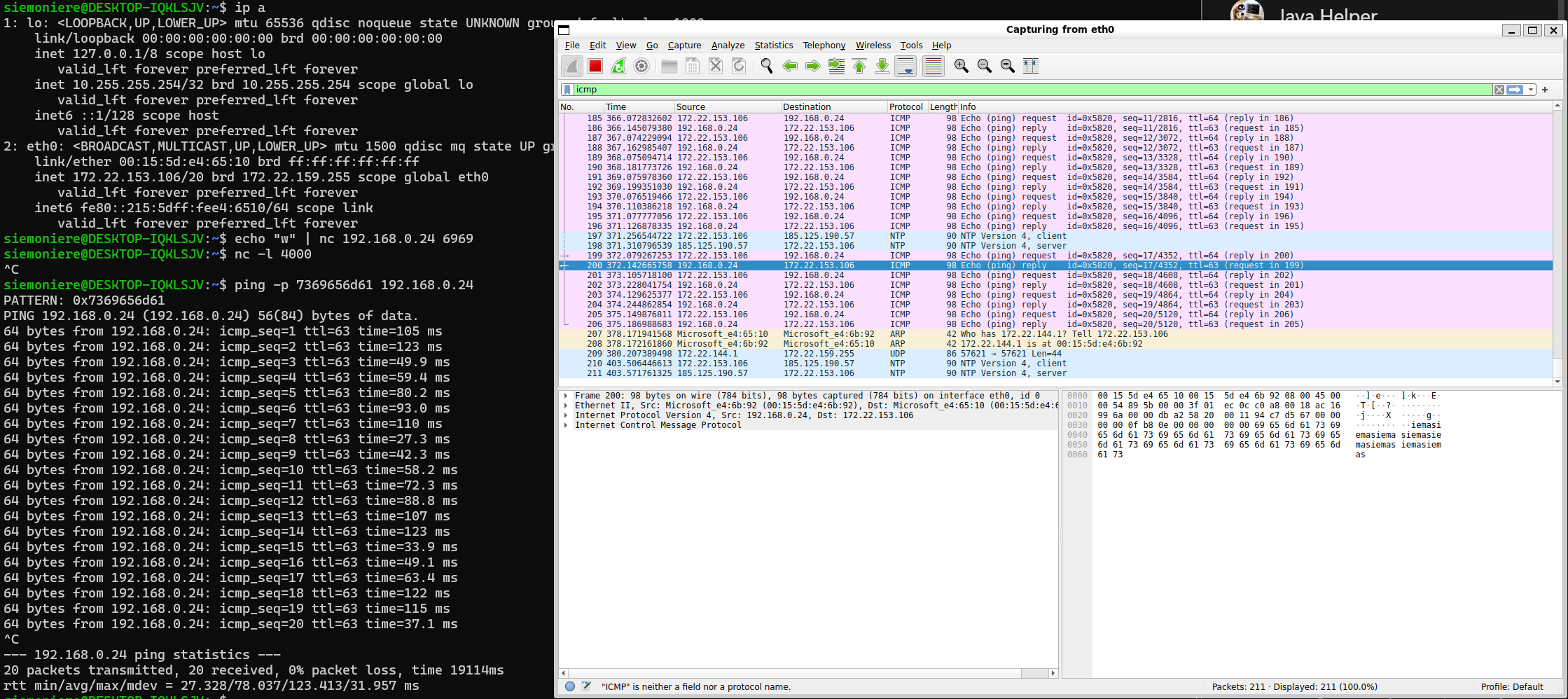
Dla serwerów bliżej geograficznie zgodnie z intuicją mamy do czynienia z krótszą trasą. Dla przykładu dla www.wroclaw.pl mamy:



Ponadto widać, że czas odpowiedzi na każdym przeskoku jest znacznie krótszy (ok. 35 ms) niż dla wyżej wymienionego Uzbekistanu (do 130 ms).

2.3 Analiza za pomocą WireShark

Dzięki WireShark w systemie szesnastkowym przesłaliśmy informację do innego urządzenia w tej samej sieci – w tym przypadku jest to wiadomość „siema”.



3. Wnioski dotyczące przydatności programów

* Ping świetnie nadaje się do szybkiego testowania dostępności hostów i określania wpływu wielkości pakietu na opóźnienie.
* Traceroute pozwala śledzić trasę pakietu i identyfikować sieci wirtualne przez analizę ukrytych przeskoków i opóźnień.
* WireShark umożliwia szczegółową analizę ruchu sieciowego, łącznie z identyfikacją rozmiarów pakietów i protokołów.