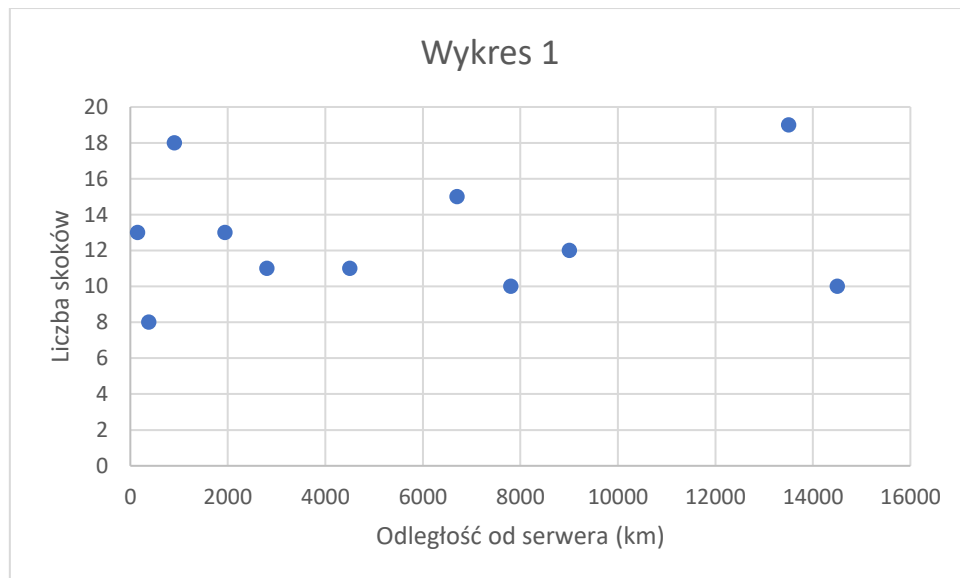


Sprawozdanie

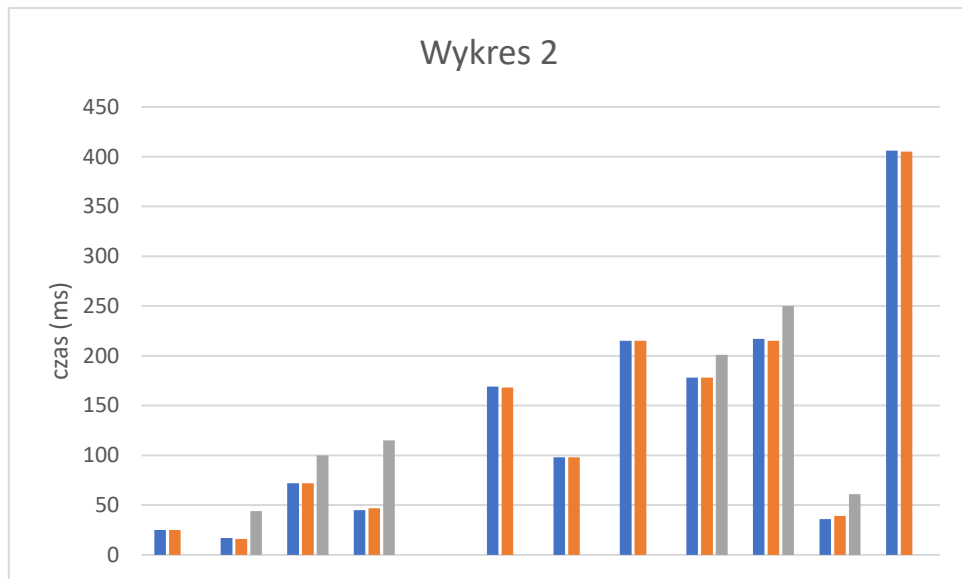
1. Program Ping.



Powyższy wykres przedstawia liczbę skoków w zależności od odległości w linii prostej do serwera dla 32 bajtowego pakietu. Dla każdego sprawdzonego przeze mnie adresu IP liczba skoków do serwera była większa niż liczba skoków z serwera. Nie odnotowałem wpływu rozmiaru pakietu na liczbę skoków. Najdłuższą znaną ścieżką była droga do serwera w mieście Port-Moresby w Nowej Gwinei: 19 skoków do serwera i 18 z powrotem.

Wnioski

- Na podstawie powyższych danych nie stwierdzam wpływu odległości geograficznej na liczbę skoków przesyłanego pakietu.
- Droga pakietu z serwera i do niego przebiegała w większości przypadków różnymi ścieżkami.



Wykres 2 przedstawia czas propagacji wyrażony w milisekundach w zależności od wielkości fragmentowanego pakietu. Niebieskie, pomarańczowe i szare słupki są przyporządkowane do pakietów odpowiednio: 128, 1024 i 65500 bajtów. Ostatni rozmiar jest jednocześnie największym, który mogłem przesać do serwera. W przeprowadzeniu tego doświadczenia użyłem polecenia:

```
C:\Users\Kamil Jeziorny>ping google.com -l 128,
```

Gdzie `google.com` i `128` zastępowałem odpowiednio adresem IP serwera i wybraną wielkością pakietu. W większości badanych przypadków wystąpiła niewielka różnica (rzędu kilku ms) pomiędzy przesyłaniem pakietu fragmentowanego oraz niefragmentowanego, gdzie pakiet fragmentowany przysłał się szybciej. Największy niefragmentowany pakiet, który przesałem, miał wielkość 1472 bajtów. Próba przesłania pakietu do sieci wirtualnej (serwer publiczny w Chinach), dała poniższe rezultaty:

```
C:\Users\Kamil Jeziorny>ping 114.114.114.114

Pinging 114.114.114.114 with 32 bytes of data:
Reply from 114.114.114.114: bytes=32 time=148ms TTL=81
Reply from 114.114.114.114: bytes=32 time=148ms TTL=63
Reply from 114.114.114.114: bytes=32 time=153ms TTL=62
Reply from 114.114.114.114: bytes=32 time=148ms TTL=82
```

Wartość TTL zmieniała się za każdym razem, gdy przysyłałem pakiet.

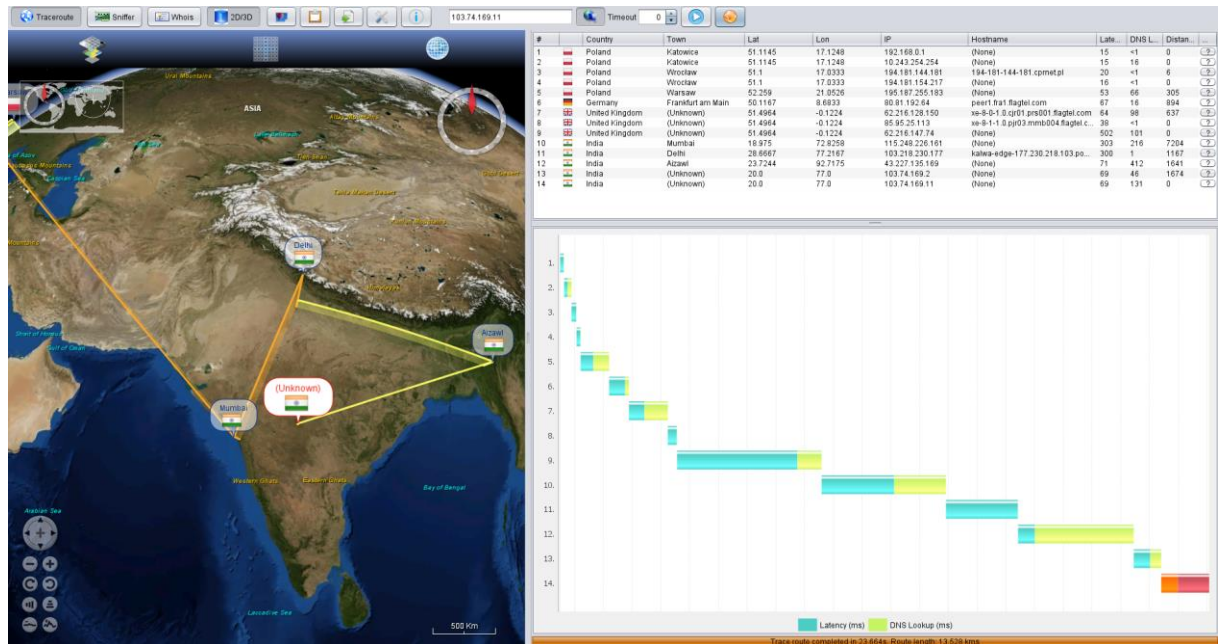
Wniosek

- Wielkość przesyłanych pakietu ma wpływ na czas propagacji.

2. Program Traceroute.

Powyższy program pozwolił mi na analizę drogi, którą był przesyłany pakiet do wybranego serwera.

Screen 2.1



Powyższy screen ukazuje użycie programu Open Visual Traceroute, w którym przeanalizowałem drogę do jednego z serwerów z Indii.

Wnioski:

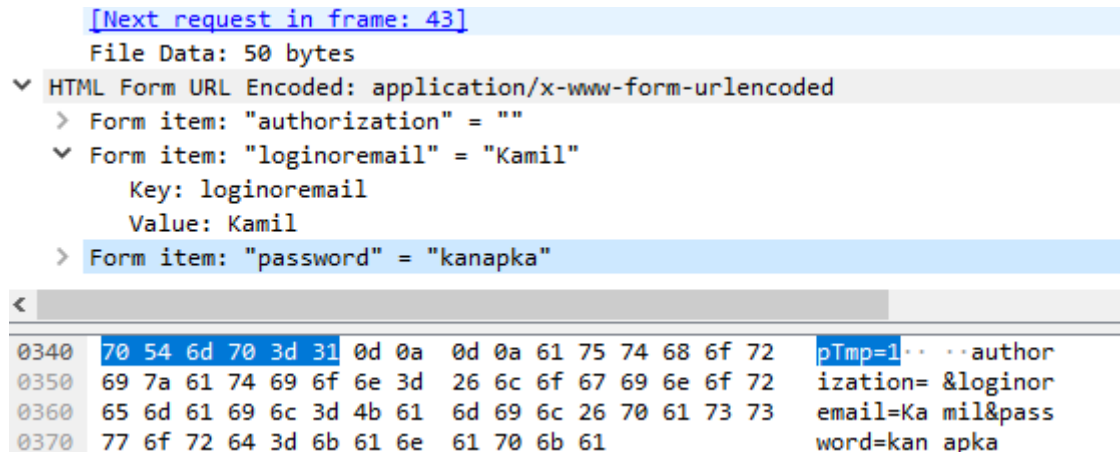
- Przesyłany pakiet nie musi przemieszczać się najkrótszą geograficznie drogą.

3. Program Wireshark.

Pozwala odczytywać informacje o użytkownikach sieci takie jak:

- Docelowy adres IP wysyłanych danych,
- Adres IP użytkownika,
- Typ protokołu,
- Długość przesłanej wiadomości.

Screen 3.1



Screen 3.1 pokazuje udaną próbę przechwycenia loginu i hasła podczas próby zalogowania się na stronę z protokołem http.

Program poprzez przechwytywanie pakietów pozwala również odczytywać dodatkowe informacje o użytkownikach, np. rodzaj przeglądarki, która jest używana pod danym adresem IP, co ukazuje screen 3.2

Screen 3.2

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\nContent-Type: application/x-www-form-urlencoded\r\n

Wnioski końcowe

Ping:

- Łatwość w analizowaniu podstawowych własności sieci.
- Pomocny w diagnozowaniu problemów z siecią.
- Możliwość dobrania odpowiednich parametrów wywołania poszerza funkcjonalność programu.

Traceroute:

- Przejrzysty interfejs w prosty sposób ukazuje przepływ pakietów pomiędzy serwerami.

Wireshark:

- Pozwala przechwytywać pakiety z informacjami.
- W prosty sposób można sprawdzić niektóre informacje o użytkownikach sieci Wi-Fi.
- Łatwość w zbieraniu danych o użytkownikach może przyczyniać się do zwiększenia niebezpieczeństwa w sieci.