Zadanie

- Zadanie
- Sprawozdanie
  - Ping
    - Opis programu
    - Ile jest węzłów na trasie do (i od) wybranego, odległego geograficznie, serwera.
      - Trasa do citygallery.org.nz
      - Trasa od citygallery.org.nz
    - Jak wielkość pakietu wpływa na obserwowane czasy propagacji.
    - Jaki największy niefragmentowany pakiet uda się przesłać.
    - Przeanalizuj te same zagadnienia dla krótkich tras (do serwerów bliskich geograficznie).
    - Określ "średnicę" internetu (najdłuższą scieżkę którą uda sie wyszukać).
    - Czy potraficz wyszukać trasy przebiegające przez sieci wirtualne (zdalne platformy "cloud computing").
    - Ile węzłów mają scieżki w tym przypadku.
  - Traceroute
  - Wireshark
    - Połączenie w sieci lokalnej
    - Netcat
    - Nasłuchiwanie jako serwer nc
    - Nasłuchiwanie jako klient nc


```
Przetestuj działanie programów:
a) Ping: Sprawdź za jego pomocą ile jest węzłów na trasie do (i od)
wybranego, odległego geograficznie, serwera. Uwaga: trasy tam i z powrotem
mogą być różne. Zbadaj jaki wpływ ma na to wielkość pakietu. Zbadaj jak
wielkość pakietu wpływa na obserwowane czasy propagacji. Zbadaj jaki wpływ
na powyższe ma konieczność fragmentacji pakietów. Jaki największy
niefragmentowany pakiet uda się przesłac. Przeanalizuj te same zagadnienia
dla krótkich tras (do serwerów bliskich geograficznie). Określ "średnicę"
internetu (najdłuższą ścieżkę którą uda sie wyszukać). Czy potraficz
wyszukać trasy przebiegające przez sieci wirtualne (zdalne platformy "cloud
computing"). Ile węzłów mają scieżki w tym przypadku.
b) Traceroute,
c) WireShark.
Napisz sprawozdanie zawierające: opis programów, wywołania dla powyższych
zagadnień z analizą wyników, wnioski dotyczące przydatności tych programów.
```

Sprawozdanie

Ping

Opis programu

Ping - program służący do wysyłania zapytan ECHO_REQUEST (ICMP) do urządzeń sieciowych - hostów.

Bazowe użycie:

```
$ ping google.com

PING google.com (142.250.179.142) 56(84) bytes of data.
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=1
ttl=111 time=26.2 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=2
ttl=111 time=27.7 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=3
ttl=111 time=27.7 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 26.229/27.210/27.724/0.693 ms
```

Jak możemy wyczytać z podanych wyników, ping wysłał 3 pakiety do serwera google.com, z których wszystkie zostały odebrane.

Informacje:

- `icmp_seq` - numer sekwencyjny pakietu
- `ttl` - Time To Live, maksymalna liczba skoków jaką pakiet może wykonać
    - Wartość TTL jest zmniejszana o 1 przez każdy router, przez który przechodzi pakiet
    - Jeśli wartość TTL osiągnie 0, pakiet jest odrzucany, a informacja o jego odrzuceniu jest zwracana do nadawcy
- `time` - czas odpowiedzi - od wysłania pakietu do otrzymania odpowiedzi

Spróbujmy zpingować gateway:

```
ip r | grep default
ping 10.182.254.254

PING 10.182.254.254 (10.182.254.254) 56(84) bytes of data.
64 bytes from 10.182.254.254: icmp_seq=1 ttl=64 time=4.96 ms
```

Widzimy, że gateway odpowiada na pinga z `TTL=64`. TTL może mieć wartości w przedziale `[0, 255]`, co oznacza, że pakiet może przejść maksymalnie `255` skoków, zanim zostanie odrzucony.

Ile jest węzłów na trasie do (i od) wybranego, odległego geograficznie, serwera.

Uwaga: trasy tam i z powrotem mogą być różne.

Wybierzmy serwer galerii w Nowe Zelandii `citygallery.org.nz`

Trasa do citygallery.org.nz

```
[~] ping -t 13 citygallery.org.nz
PING citygallery.org.nz (141.193.213.10) 56(84) bytes of data.
64 bytes from 141.193.213.10: icmp_seq=1 ttl=53 time=9.11 ms
^C
--- citygallery.org.nz ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.105/9.105/9.105/0.000 ms
[~] ping -t 12 citygallery.org.nz
PING citygallery.org.nz (141.193.213.10) 56(84) bytes of data.
From 162.158.100.9 icmp_seq=1 Time to live exceeded
From 162.158.100.9 icmp_seq=2 Time to live exceeded
```

Zatem minimalny ttl wynosi 13 - tyle skoków jest na trasie do serwera citygallery.org.nz.

Trasa od citygallery.org.nz

```
ping citygallery.org.nz

PING citygallery.org.nz (141.193.213.11) 56(84) bytes of data.
64 bytes from 141.193.213.11: icmp_seq=1 ttl=53 time=8.67 ms
64 bytes from 141.193.213.11: icmp_seq=2 ttl=53 time=12.0 ms
```

Liczba węzłów na trasie może zostać sprawdzona za pomocą polecenia `traceroute`:

```
traceroute citygallery.org.nz

traceroute to citygallery.org.nz (141.193.213.10), 30 hops max, 60 byte
packets
 1  _gateway (10.182.254.254)  5.021 ms  4.981 ms  4.969 ms
 2  10.3.60.28 (10.3.60.28)  5.141 ms  6.052 ms  5.370 ms
 3  10.3.61.25 (10.3.61.25)  8.415 ms  7.763 ms  9.574 ms
 4  10.3.60.162 (10.3.60.162)  9.565 ms  9.555 ms  9.545 ms
 5  do-wcss.pwr.edu.pl (156.17.147.251)  13.178 ms  13.168 ms  13.154 ms
 6  156.17.252.52 (156.17.252.52)  9.501 ms  3.528 ms  4.271 ms
 7  156.17.252.53 (156.17.252.53)  4.589 ms  18.098 ms  18.057 ms
 8  156.17.254.101 (156.17.254.101)  18.040 ms  18.029 ms  18.019 ms
 9  212.191.238.214 (212.191.238.214)  18.008 ms  17.997 ms  17.986 ms
10  * * *
11  cloudflare.plix.pl (195.182.218.134)  50.638 ms  50.623 ms *
12  162.158.100.7 (162.158.100.7)  8.949 ms 162.158.100.17 (162.158.100.17)
10.143 ms  23.582 ms
13  141.193.213.10 (141.193.213.10)  8.922 ms  23.512 ms  23.496 ms
```

Liczymy tylko L3 (bez ostatniego hopa, bo LAN w traceroute pokazuje się jako 1 hop)

Zobaczmy, że skoro mamy 12 hopów, to mamy 11 węzłów na trasie, a z informacją TTL=53 wiemy, że serwer citygallery.org.nz odpowiada z bazowym TTL (64), co oznacza, że jest 11 skoków od nas.

Jak wielkość pakietu wpływa na obserwowane czasy propagacji.

```
ping -s 1000 -c 10 chatgpt.com
ping -s 64 -c 10 chatgpt.com

[uni] ping -s 1000 -c 10 chatgpt.com

--- chatgpt.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 36.474/48.526/86.066/13.689 ms

[uni] ping -s 64 -c 10 chatgpt.com

[...]

--- chatgpt.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 10.227/11.826/18.821/2.404 ms
```

RTT - Round Trip Time

Widzimy że wartość rtt dla dłuższego pakietu jest większa (48.526s na 1000 bajtów / 11.826s na 64 bajty)

Jaki największy niefragmentowany pakiet uda się przesłać.

Dotyczy on wartości MTU - maximum transmission unit ustalany na 1500 bajtów - pełna ramka, lub 9000 - jumboframe. Przekroczenie tej wartości skutkuje fragmentacją pakietu.

Dla sieci w VPN może wynieść to mniej niż 1500, np. MTU 1440.

Przeanalizuj te same zagadnienia dla krótkich tras (do serwerów bliskich geograficznie).

Dla krótkich tras będziemy obserwować TTL zbliżony do wartości podstawowej:

- pingowanie gatewaya zwraca 64.

Czasy propagacji są mniejsza, a fragmentacja podobna.

Określ "średnicę" internetu (najdłuższą scieżkę którą uda sie wyszukać).

Najdłuższą trasę udało się znaleźć do chile:

```
$ sudo traceroute www.electronicareal.cl
traceroute to www.electronicareal.cl (190.107.177.80), 30 hops max, 60 byte
packets
 1  _gateway (10.182.254.254)  4.338 ms  4.281 ms *
 2  * * *
```

```
 3  * * *
 4  * * *
 5  * * *
 6  * 156.17.252.52 (156.17.252.52)  3.463 ms  2.218 ms
 7  156.17.252.53 (156.17.252.53)  2.161 ms  2.925 ms  3.445 ms
 8  156.17.254.101 (156.17.254.101)  4.948 ms  4.924 ms  4.900 ms
 9  212.191.238.214 (212.191.238.214)  5.134 ms  5.113 ms  4.833 ms
10  * * *
11  * * *
12  40ge1-3.core1.lon2.he.net (195.66.224.21)  32.012 ms  30.477 ms  30.362
ms
13  * * *
14  port-channel27.core2.mia1.he.net (184.104.188.217)  166.160 ms * *
15  cl-phei-as263237.e0-51.switch1.mia1.he.net (216.66.61.2)  309.081 ms
282.597 ms  281.391 ms
16  199.100.16.106 (199.100.16.106)  281.361 ms  297.963 ms  224.836 ms
17  * * *
18  * * *
19  srv2.thehosting.cl (190.107.177.80)  234.116 ms  234.092 ms  234.584 ms
```

Czy potraficz wyszukać trasy przebiegające przez sieci wirtualne (zdalne platformy "cloud computing").

Traceroute do prezydenta brunei `www.pmo.gov.bn` przechodzi przez sieć wirtualną:

```
$ traceroute www.pmo.gov.bn

traceroute to www.pmo.gov.bn (103.4.188.110), 30 hops max, 60 byte packets
 1  _gateway (192.168.32.2)  5.741 ms  6.705 ms  6.608 ms
 2  * * *
 3  172.26.9.14 (172.26.9.14)  33.839 ms 172.26.9.78 (172.26.9.78)  34.799
ms 172.26.9.14 (172.26.9.14)  34.717 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  81.52.179.224 (81.52.179.224)  257.309 ms  257.363 ms  257.273 ms
11  154-255.static.espeed.com.bn (61.6.255.154)  260.748 ms  257.359 ms
307.286 ms
[...]
```

* widoczne na powyższym logu oznaczają przejścia L2, potencjalnie mogą to byc seci wirtualne

Ile węzłów mają scieżki w tym przypadku.

Traceroute

Traceroute do koleżanki w LAN chodzi w L2, zatem:

```
[uni] traceroute 192.168.32.43
traceroute to 192.168.32.43 (192.168.32.43), 30 hops max, 60 byte packets
 1  192.168.32.43 (192.168.32.43)  50.039 ms  50.840 ms  50.778 ms
```

Wireshark

Połączenie w sieci lokalnej

Spróbujmy skomunikować się z netcata.

```
ip a
4: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
    link/ether 54:8d:5a:ef:08:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.233/24
```

Mój adres IP to 192.168.32.233, a adres koleżanki to 192.168.32.43.

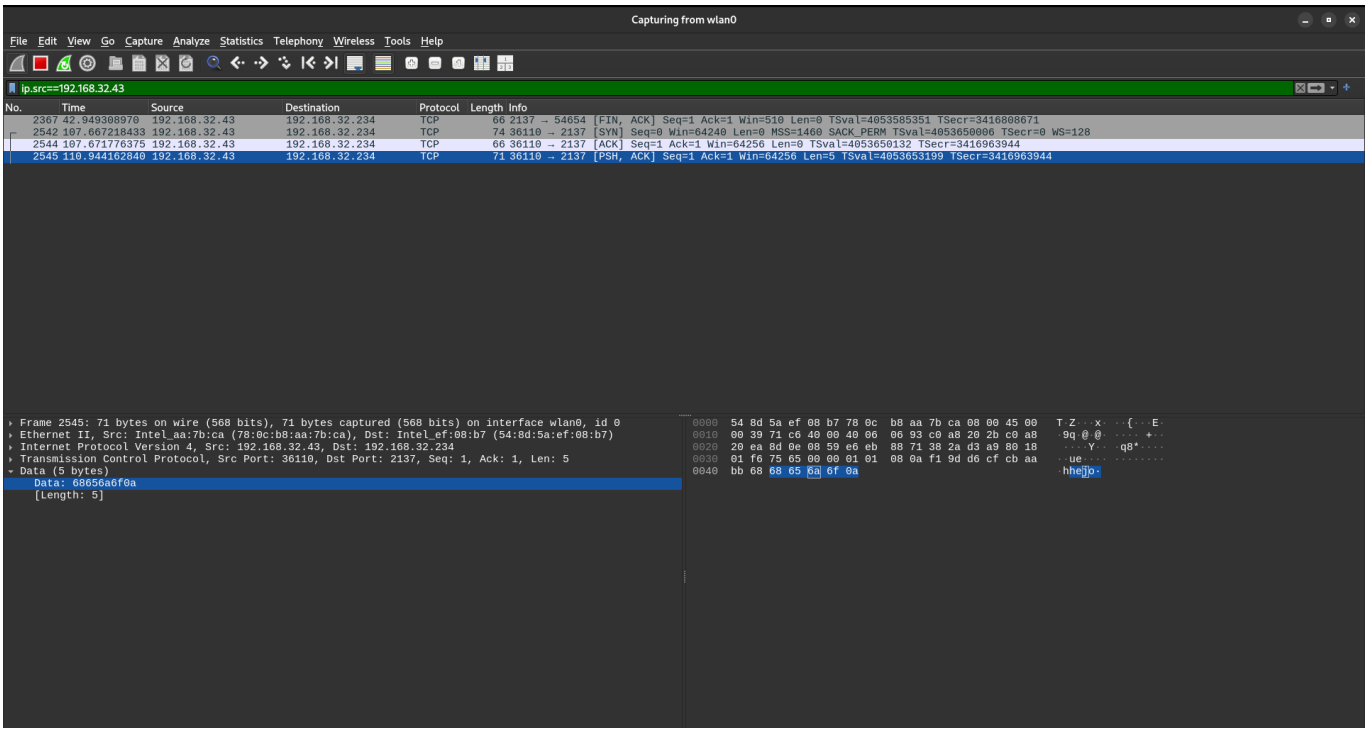
Netcat

Spróbujmy prostą komunikację

```
nc -ltp 2137
nc 192.168.32.43 2137
```

Nasłuchiwanie jako serwer nc

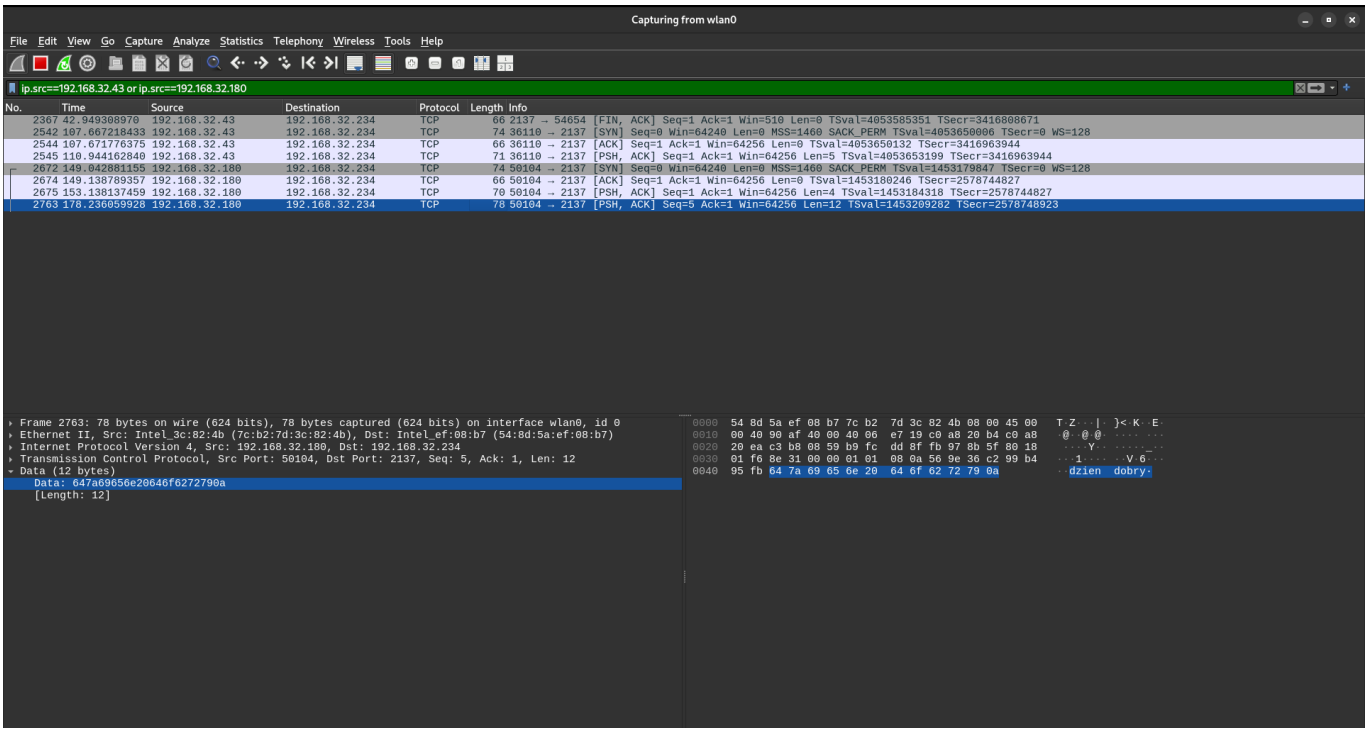
Koleżanka napisała do mnie wiadomość `hejo`



Zobaczmy, że `netcat` odpalony na porcie TCP zwraca jej ACK

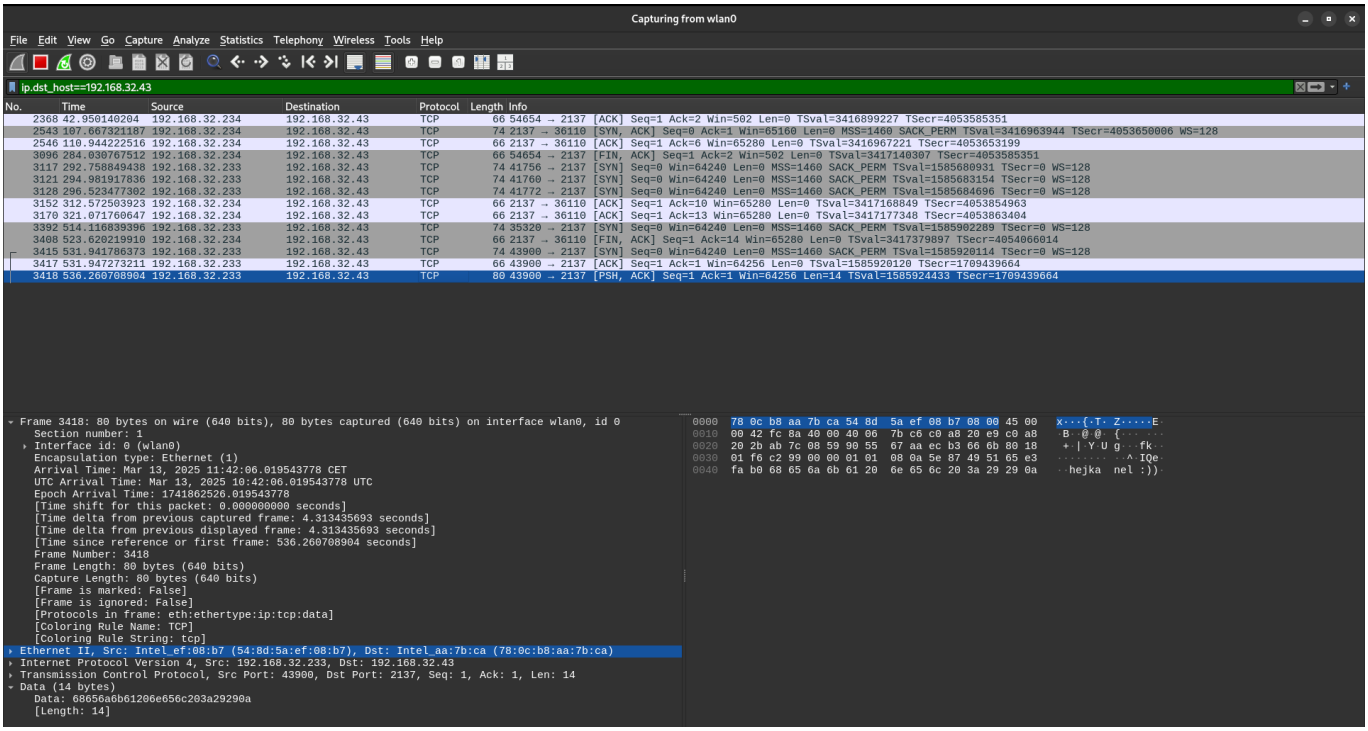
```
2542    107.667218433   192.168.32.43   192.168.32.234  TCP 74  36110 →
2137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4053650006
TSecr=0 WS=128
2544    107.671776375   192.168.32.43   192.168.32.234  TCP 66  36110 →
2137 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4053650132 TSecr=3416963944
2545    110.944162840   192.168.32.43   192.168.32.234  TCP 71  36110 →
2137 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=5 TSval=4053653199
TSecr=3416963944
```

Bartek (192.168.32.180) wysłał mi dzień dobry



Nasłuchiwanie jako klient nc

Napisałem do Nel: `hejka nel :)`




```
3418    536.260708904   192.168.32.233  192.168.32.43   TCP 80  43900 →
2137 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=14 TSval=1585924433
TSecr=1709439664
```