

# Analiza działania polecenia tracert za pomocą aplikacji Wireshark.

Wireshark to aplikacja służąca do analizy pakietów sieciowych, która pozwala na przechwytywanie i analizowanie ruchu sieciowego. Może ona analizować wiele protokołów sieciowych, takich jak TCP, UDP, HTTP, DNS, DHCP, FTP, SMTP i wiele innych. Może być wykorzystywany do różnych celów, w tym do diagnostyki problemów sieciowych, analizy wydajności sieciowej, wykrywania ataków sieciowych oraz do testowania bezpieczeństwa sieci.

Wynik zapytania tracert Helios.et.pu.poznan.pl:

- w wierszu poleceń:

```
Tracing route to helios.et.put.poznan.pl [150.254.11.6]
over a maximum of 30 hops:

  1  30 ms  3 ms  3 ms  10.202.14.1
  2   4 ms  5 ms  4 ms  10.1.5.1
  3   6 ms  6 ms  4 ms  ra.uwm.edu.pl [213.184.0.100]
  4  15 ms 13 ms 16 ms  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  5  14 ms 14 ms 14 ms  z-poznan-gw3.poznan.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  6  14 ms 14 ms 15 ms  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  7  14 ms 15 ms 21 ms  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  8  20 ms 23 ms 27 ms  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
  9  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58] reports: Destination host unreachable.

Trace complete.
```

- w aplikacji Wireshark:

icmp					
No.	Time	Source	Destination	Protocol	Length Info
17	4.158212	10.202.14.160	150.254.11.6	ICMP	106 Echo (ping) request id=0x0001, seq=38/9728, ttl=1 (no response found!)
18	4.162169	10.202.14.1	10.202.14.160	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
19	4.164179	10.202.14.160	150.254.11.6	ICMP	106 Echo (ping) request id=0x0001, seq=39/9984, ttl=1 (no response found!)
20	4.167588	10.202.14.1	10.202.14.160	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
21	4.168763	10.202.14.160	150.254.11.6	ICMP	106 Echo (ping) request id=0x0001, seq=40/10240, ttl=1 (no response found!)
22	4.173071	10.202.14.1	10.202.14.160	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
28	4.248829	10.202.14.1	10.202.14.160	ICMP	70 Destination unreachable (Communication administratively filtered)
36	5.722649	10.202.14.1	10.202.14.160	ICMP	70 Destination unreachable (Communication administratively filtered)
44	7.236390	10.202.14.1	10.202.14.160	ICMP	70 Destination unreachable (Communication administratively filtered)

a) **Ile wiadomości i jakiego typu wysłał komputer?**

Komputer wysłał 1 wiadomość typu tracert.

b) **Ile wiadomości i jakiego typu komputer otrzymał?**

Komputer otrzymał 26 wiadomości typu ICMP.

c) **Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.**

Źródło: o IP: 10.202.14.160 o MAC: fc:f8:ae:77:3f:da Odbiorca: o IP: 150.254.11.6 o MAC: 88:e0:f3:c0:87:f0

d) **Określić wartość parametru TTL?**

Wartość parametru TTL wynosi od 1 do 9.

e) **Narysuj graf przepływu.**

