Analiza działania polecenia pathping 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.

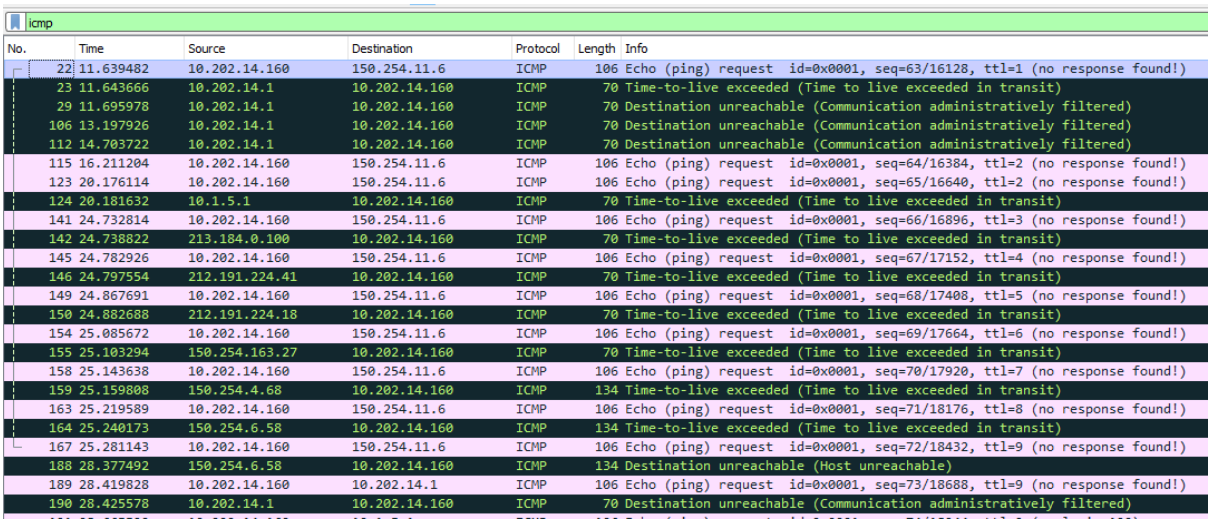
Wynik zapytania pathping Helios.et.put.poznan.pl:

- w wierszu poleceń:

```
Tracing route to Helios.et.put.poznan.pl [150.254.11.6]
over a maximum of 30 hops:
  0  DESKTOP-SSUSOMK.dns-enforcement.man.olsztyn.pl [10.202.14.160]
  1  10.202.14.1
  2     *     10.1.5.1
  3  ra.uwm.edu.pl [213.184.0.100]
  4  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  5  z-poznan-gw3.pozman.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  6  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  7  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  8  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.

Computing statistics for 225 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          DESKTOP-SSUSOMK.dns-enforcement.man.olsztyn.pl [10.202.14.160]
                                   1/ 100 =  1%   |
  1    7ms     6/ 100 =  6%      5/ 100 =  5%  10.202.14.1
                                   0/ 100 =  0%   |
  2   11ms     1/ 100 =  1%      0/ 100 =  0%  10.1.5.1
                                   0/ 100 =  0%   |
  3    8ms     5/ 100 =  5%      4/ 100 =  4%  ra.uwm.edu.pl [213.184.0.100]
                                   0/ 100 =  0%   |
  4   22ms     3/ 100 =  3%      2/ 100 =  2%  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
                                   0/ 100 =  0%   |
  5   19ms     3/ 100 =  3%      2/ 100 =  2%  z-poznan-gw3.pozman.10Gb.rtr.pionier.gov.pl [212.191.224.18]
                                   0/ 100 =  0%   |
  6   19ms     1/ 100 =  1%      0/ 100 =  0%  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
                                   2/ 100 =  2%   |
  7   18ms     5/ 100 =  5%      2/ 100 =  2%  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
                                   0/ 100 =  0%   |
  8   18ms     3/ 100 =  3%      0/ 100 =  0%  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
                                  97/ 100 = 97%   |
  9  ---     100/ 100 =100%      0/ 100 =  0%  DESKTOP-SSUSOMK [0.0.0.0]
```

- w aplikacji Wireshark:



icmp

No.	Time	Source	Destination	Protocol	Length	Info
22	11.639482	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=1 (no response found!)
23	11.643666	10.202.14.1	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
29	11.695978	10.202.14.1	10.202.14.160	ICMP	70	Destination unreachable (Communication administratively filtered)
106	13.197926	10.202.14.1	10.202.14.160	ICMP	70	Destination unreachable (Communication administratively filtered)
112	14.703722	10.202.14.1	10.202.14.160	ICMP	70	Destination unreachable (Communication administratively filtered)
115	16.211204	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=2 (no response found!)
123	20.176114	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=2 (no response found!)
124	20.181632	10.1.5.1	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
141	24.732814	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=3 (no response found!)
142	24.738822	213.184.0.100	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
145	24.782926	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=4 (no response found!)
146	24.797554	212.191.224.41	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
149	24.867691	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=5 (no response found!)
150	24.882688	212.191.224.18	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
154	25.085672	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=6 (no response found!)
155	25.103294	150.254.163.27	10.202.14.160	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	25.143638	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=7 (no response found!)
159	25.159808	150.254.4.68	10.202.14.160	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
163	25.219589	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=8 (no response found!)
164	25.240173	150.254.6.58	10.202.14.160	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
167	25.281143	10.202.14.160	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=72/18432, ttl=9 (no response found!)
188	28.377492	150.254.6.58	10.202.14.160	ICMP	134	Destination unreachable (Host unreachable)
189	28.419828	10.202.14.160	10.202.14.1	ICMP	106	Echo (ping) request id=0x0001, seq=73/18688, ttl=9 (no response found!)
190	28.425578	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 9 wiadomości typu IMCP.

b) ***Ile wiadomości i jakiego typu komputer otrzymał?***
Komputer otrzymał 13 wiadomości typu ICMP.

c) ***Czy w wysyłanych (odbieranych) pakietach zmieniania jest wartość parametru TTL, jeżeli tak to w jaki sposób?***
Wartość parametru podczas wykonywania polecenia pathping Helios.et.put.poznan.pl w systemie Windows, wartość parametru TTL jest stopniowo zwiększana, zaczynając od 1, aż do momentu, gdy zostanie osiągnięty docelowy adres IP. W każdym kroku pathping wysyła pakiet z określoną wartością TTL i oczekuje na odpowiedź. Jeśli router, przez który przechodzi pakiet, przekroczy maksymalną liczbę skoków określoną przez wartość TTL, pakiet zostanie odrzucony, a pathping otrzyma informację o niepowodzeniu wysłania pakietu. Zmiana wartości parametru TTL będzie się więc zmieniać wraz ze zmianą liczby przeskoków, które pakiet musi przejść, aby dotrzeć do celu.

d) ***Na podstawie przechwyconych pakietów w protokołach ICMP przedstaw zasadę działania polecenia pathping.***
Polecenie pathping w systemie Windows służy do diagnostyki i analizy jakości połączenia z danym adresem IP lub nazwą domenową. Polecenie to działa na zasadzie połączenia funkcjonalności tracert i ping, czyli łączy analizę ścieżki pakietów z pomiarem czasu odpowiedzi hostów. Podczas wykonywania polecenia pathping system Windows wysyła serię pakietów ICMP z coraz większymi wartościami TTL (Time to Live) w celu śledzenia drogi, jaką pakiet musi przebyć, aby dotrzeć do docelowego adresu. Po każdym hopie, na którym zatrzymał się pakiet, otrzymywane są wyniki pomiaru czasu odpowiedzi oraz utworzona zostaje tabela

śledzenia trasy. Wyniki te służą do określenia jakości połączenia z danym adresem IP lub nazwą domenową.

e) ***Narysuj graf przepływu***