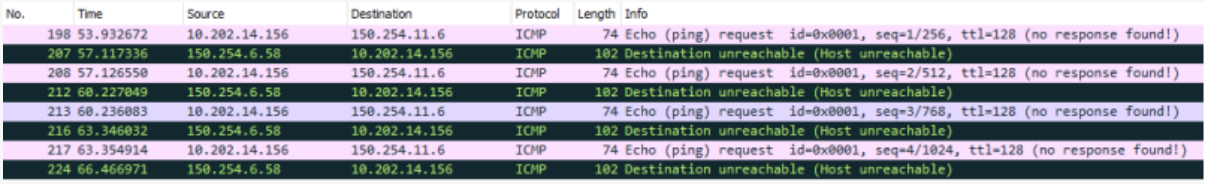
**Wireshark** jest narzędziem do analizy pakietów sieciowych. Pozwala na przechwytywanie i analizowanie ruchu sieciowego przesyłanego przez sieć komputerową. Może być używany do rozwiązywania problemów z siecią, diagnostyki, debugowania protokołów, a także do analizy zabezpieczeń sieciowych.

```
C:\Users\Magda>ping helios.et.put.poznan.pl -i 2

Pinging helios.et.put.poznan.pl [150.254.11.5] with 32 bytes of data:
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.

Ping statistics for 150.254.11.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Magda>
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 198 | 53.932672 | 10.202.14.156 | 150.254.11.6 | ICMP | 74 | Echo (ping) request id=0x0001, seq=1/256, ttl=128 (no response found!) |
| 207 | 57.117336 | 150.254.6.58 | 10.202.14.156 | ICMP | 102 | Destination unreachable (Host unreachable) |
| 208 | 57.126550 | 10.202.14.156 | 150.254.11.6 | ICMP | 74 | Echo (ping) request id=0x0001, seq=2/512, ttl=128 (no response found!) |
| 212 | 60.227049 | 150.254.6.58 | 10.202.14.156 | ICMP | 102 | Destination unreachable (Host unreachable) |
| 213 | 60.236083 | 10.202.14.156 | 150.254.11.6 | ICMP | 74 | Echo (ping) request id=0x0001, seq=3/768, ttl=128 (no response found!) |
| 216 | 63.346032 | 150.254.6.58 | 10.202.14.156 | ICMP | 102 | Destination unreachable (Host unreachable) |
| 217 | 63.354914 | 10.202.14.156 | 150.254.11.6 | ICMP | 74 | Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (no response found!) |
| 224 | 66.466971 | 150.254.6.58 | 10.202.14.156 | ICMP | 102 | Destination unreachable (Host unreachable) |

a) Komputer wysłał wiadomość typu ICMP (Internet Control Message Protocol) Echo Request (żądanie Echa) do wskazanego hosta. Zostały wysłane 4 pakiety.

b) Komputer otrzymał 4 wiadomości typu ICMP.

c) Adres źródłowy i docelowy zależy od konfiguracji sieci i źródła, z którego zostało wykonane polecenie ping. MAC adresy są używane tylko w sieciach lokalnych, więc w przypadku pakietów przesyłanych poza jedną siecią, nie będą one widoczne. Można jednak zobaczyć adresy IP źródłowe i docelowe w nagłówku ICMP.

d) Adres IPv4 jest adresem protokołu warstwy sieciowej, który służy do identyfikacji urządzenia w sieci IP. Adres MAC jest adresem protokołu warstwy łącza danych, który służy do identyfikacji urządzenia w sieci lokalnej.

e) Wartość parametru TTL może być różna w zależności od konfiguracji sieci i tras pakietów. Domyślnie w systemach Windows wartość TTL wynosi 128, ale może być zmieniona przez administratora sieci.

f) TTL (Time To Live) jest ustawiany w pakietach IP i określa maksymalną liczbę skoków, jakie pakiet może wykonać na swojej drodze przez sieć. Wartość TTL jest zwiększana o 1

dla każdego routera, przez który pakiet przechodzi, aż osiągnie swoje maksymalne wartości i zostanie odrzucony. Dzięki temu zapobiega się sytuacji, w której pakiety krążą bez końca w sieci.

g) Podobne pole znajduje się w ramce Ethernetowej, ale nazywa się ono Time To Live (TTL) lub Hop Limit i służy do kontrolowania liczby skoków, jakie ramka może wykonać w sieci.

h)

```
C:\Users\Magda>ping helios.et.put.poznan.pl -i 2

Pinging helios.et.put.poznan.pl [150.254.11.5] with 32 bytes of data:
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.
Reply from 10.100.0.1: TTL expired in transit.

Ping statistics for 150.254.11.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Magda>
```

Przełącznik -i określa interwał czasowy między wysyłanymi pakietami ICMP. W przypadku ustawienia interwału na 2 sekundy, pakiety będą wysyłane co 2 sekundy.

i)diagram przepływu