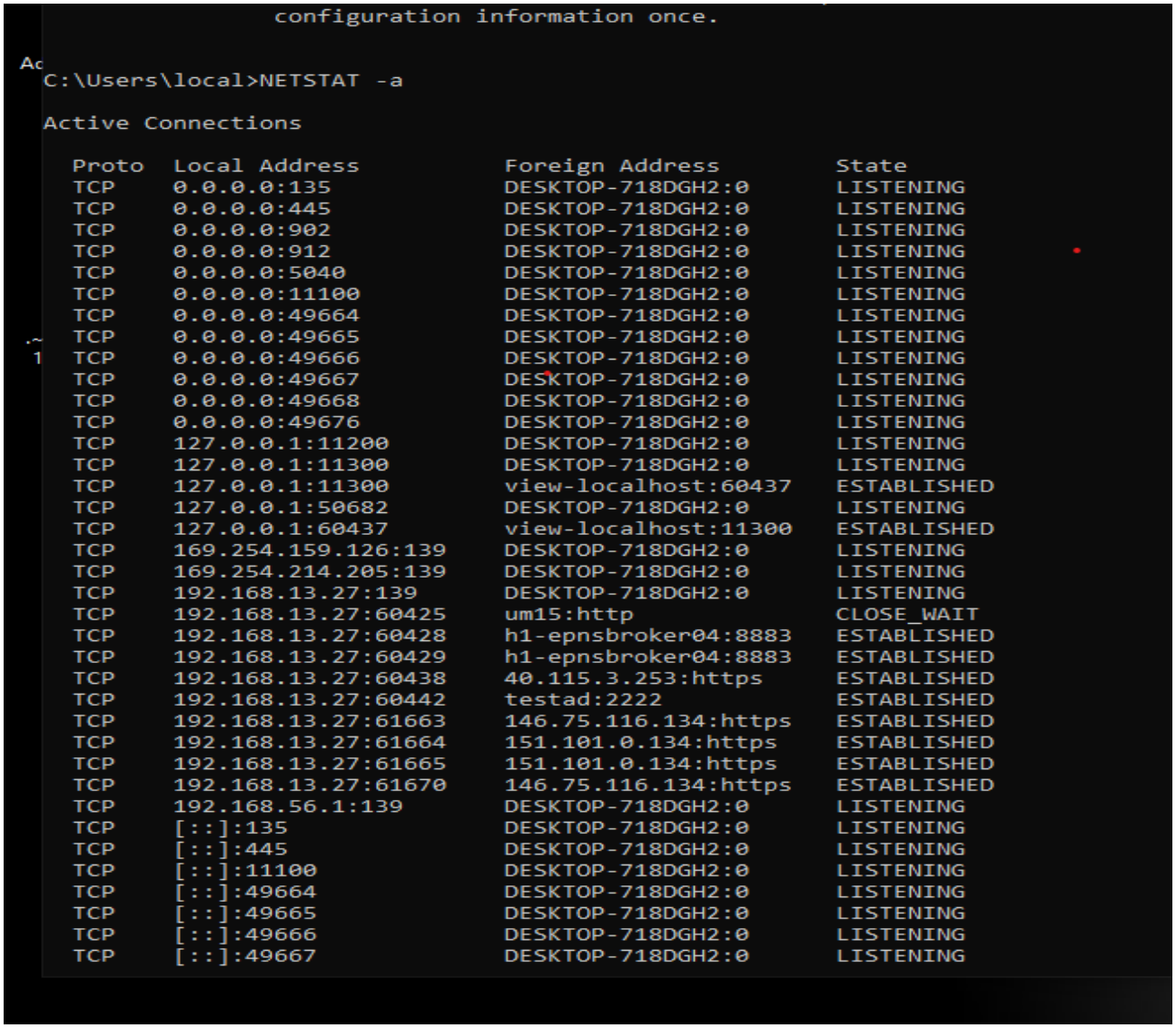
5.NETSTAT

Sprawdzić jakie informacje są możliwe do uzyskania za pomocą polecenia **`netstat`** użytego z wybranymi opcjami (przedstawić uzyskane informacje).

Polecenie -a
Wyświetla wszystkie połączenia i porty oczekujące :



Polecenie -e:
wyświetla statystyki Ethernet-u. Ta opcja może być używana razem z opcją -s :

```
C:\Users\local>NETSTAT -e
Interface Statistics

                           Received            Sent

Bytes                    1134545908      3876498872
Unicast packets             1944342        67538700
Non-unicast packets          112170          134254
Discards                  4012759320               0
Errors                             0               0
Unknown protocols                  0
```

Polecenie -n
wyświetla adresy i porty w postaci liczbowej :

```
C:\Users\local>NETSTAT -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:11300        127.0.0.1:60437        ESTABLISHED
  TCP    127.0.0.1:60437        127.0.0.1:11300        ESTABLISHED
  TCP    192.168.13.27:60425    185.94.157.11:80       CLOSE_WAIT
  TCP    192.168.13.27:60428    91.228.165.147:8883    ESTABLISHED
  TCP    192.168.13.27:60429    91.228.165.147:8883    ESTABLISHED
  TCP    192.168.13.27:60438    40.115.3.253:443       ESTABLISHED
  TCP    192.168.13.27:60442    213.184.0.58:2222      ESTABLISHED
  TCP    192.168.13.27:61663    146.75.116.134:443     ESTABLISHED
  TCP    192.168.13.27:61664    151.101.0.134:443      ESTABLISHED
  TCP    192.168.13.27:61665    151.101.0.134:443      ESTABLISHED
  TCP    192.168.13.27:61670    146.75.116.134:443     ESTABLISHED
```

Polecenie -p
Wyświetla połączenia dla określonego protokołu; może to być protokół TCP lub UDP. Jeżeli ta opcja użyta jest razem z opcją -s, do wyświetlenia wybranego protokołu, protokół może mieć wartość TCP, UDP lub IP.

```
C:\Users\local>NETSTAT -p

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Users\local>
```

Polecenie -r
wyświetla tabelę r outingu.

```
C:\Users\local>NETSTAT -r
===========================================================================
Interface List
 19...0a 00 27 00 00 13 ......VirtualBox Host-Only Ethernet Adapter
 12...bc ae c5 cd 89 10 ......Realtek PCIe GbE Family Controller
 15...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  8...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 14...00 08 a1 5f 37 de ......Realtek RTL8139/810x Family Fast Ethernet NIC
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
1Active Routes:
 Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.13.1    192.168.13.27     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0         On-link   169.254.159.126    291
      169.254.0.0      255.255.0.0         On-link   169.254.214.205    291
  169.254.159.126  255.255.255.255         On-link   169.254.159.126    291
  169.254.214.205  255.255.255.255         On-link   169.254.214.205    291
  169.254.255.255  255.255.255.255         On-link   169.254.159.126    291
  169.254.255.255  255.255.255.255         On-link   169.254.214.205    291
     192.168.13.0    255.255.255.0         On-link     192.168.13.27    281
    192.168.13.27  255.255.255.255         On-link     192.168.13.27    281
   192.168.13.255  255.255.255.255         On-link     192.168.13.27    281
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.13.27    281
        224.0.0.0        240.0.0.0         On-link   169.254.214.205    291
        224.0.0.0        240.0.0.0         On-link   169.254.159.126    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.13.27    281
  255.255.255.255  255.255.255.255         On-link   169.254.214.205    291
  255.255.255.255  255.255.255.255         On-link   169.254.159.126    291
===========================================================================
```

```
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 19    281 fe80::/64                On-link
 12    281 fe80::/64                On-link
  8    291 fe80::/64                On-link
 15    291 fe80::/64                On-link
  8    291 fe80::7e4d:7386:5dc4:ac0/128
                                    On-link
 19    281 fe80::8885:c812:f884:6259/128
                                    On-link
 12    281 fe80::9fec:f446:c2b3:9e85/128
                                    On-link
 15    291 fe80::d1c7:c291:8bc0:1a43/128
                                    On-link
  1    331 ff00::/8                 On-link
 19    281 ff00::/8                 On-link
 12    281 ff00::/8                 On-link
  8    291 ff00::/8                 On-link
 15    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Polecenie -s
wyświetla statystykę wybranego protokołu. Domyślnie jest to statystyka protokołów TCP, UDP i IP;

```
C:\Users\local>NETSTAT -s

IPv4 Statistics

  Packets Received                   = 18793512
  Received Header Errors             = 0
  Received Address Errors            = 2300368
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 77
  Received Packets Discarded         = 143374
  Received Packets Delivered         = 16650136
  Output Requests                    = 10785773
  Routing Discards                   = 0
  Discarded Output Packets           = 8210
  Output Packet No Route             = 2014
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 115157
  Received Header Errors             = 0
  Received Address Errors            = 18015
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 27531
  Received Packets Delivered         = 116157
  Output Requests                    = 42058
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 1
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

```
ICMPv4 Statistics

                            Received    Sent
  Messages                  9832        4393
  Errors                    0           0
  Destination Unreachable   8511        2657
  Time Exceeded             250         0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              1052        8
  Echos                     19          1728
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0

ICMPv6 Statistics

                            Received    Sent
  Messages                  252         977
  Errors                    0           0
  Destination Unreachable   0           5
  Packet Too Big            0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Echos                     4           4
  Echo Replies              4           4
  MLD Queries               0           0
  MLD Reports               0           0
  MLD Dones                 0           0
  Router Solicitations      0           560
  Router Advertisements     0           0
  Neighbor Solicitations    11          203
  Neighbor Advertisements   233         201
  Redirects                 0           0
  Router Renumberings       0           0

TCP Statistics for IPv4

  Active Opens                        = 39720
  Passive Opens                       = 1413
  Failed Connection Attempts          = 11461
  Reset Connections                   = 5589
  Current Connections                 = 8
```

```
TCP Statistics for IPv4

  Active Opens                            = 39720
  Passive Opens                           = 1413
  Failed Connection Attempts              = 11461
  Reset Connections                       = 5589
  Current Connections                     = 8
  Segments Received                       = 12372813
  Segments Sent                           = 4504499
  Segments Retransmitted                  = 14670

TCP Statistics for IPv6

  Active Opens                            = 93
  Passive Opens                           = 13
  Failed Connection Attempts              = 2673
  Reset Connections                       = 26
  Current Connections                     = 0
  Segments Received                       = 3977
  Segments Sent                           = 3809
  Segments Retransmitted                  = 168

UDP Statistics for IPv4

  Datagrams Received    = 4188753
  No Ports              = 20781
  Receive Errors        = 121732
  Datagrams Sent        = 6221432

UDP Statistics for IPv6

  Datagrams Received    = 184335
  No Ports              = 3508
  Receive Errors        = 24023
  Datagrams Sent        = 24140
```

Polecenie odstęp

Wyświetla wybraną statystykę, odczekując zadaną ilość sekund pomiędzy każdym wyświetleniem. Naciśnij CTRL+C, aby przerwać wyświetlanie statystyk. Jeżeli ta zmienna nie zostanie określona, program **netstat** wydrukuje raz informację o konfiguracji.

```
C:\Users\local>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:11300        view-localhost:60437   ESTABLISHED
  TCP    127.0.0.1:60437        view-localhost:11300   ESTABLISHED
  TCP    192.168.13.27:60425    um15:http              CLOSE_WAIT
  TCP    192.168.13.27:60428    h1-epnsbroker04:8883   ESTABLISHED
  TCP    192.168.13.27:60429    h1-epnsbroker04:8883   ESTABLISHED
  TCP    192.168.13.27:60438    40.115.3.253:https     ESTABLISHED
  TCP    192.168.13.27:60442    testad:2222            ESTABLISHED
  TCP    192.168.13.27:61728    waw07s05-in-f10:http   CLOSE_WAIT
  TCP    192.168.13.27:61845    um05:http              TIME_WAIT
```

6.P

6. Polecenie ARP

Zadanie.
Proszę odpowiedzieć na następujące pytania:

a) Do czego służy protokół `arp`?

Protokół ARP (Address Resolution Protocol) umożliwia powiązanie adresu IP z adresem MAC.

b) Jakie informacje można uzyskać za pomocą polecenia `arp`?

W sieciach komputerowych, opartych na protokole IPv4, do uzyskiwania informacji o adresie MAC danego urządzenia służy protokół zwany ARP (ang. Address Resolution Protocol).
ARP to mechanizm pozwalający na odwzorowanie adresu logicznego, czyli IP na adres fizyczny, czyli MAC. Załóżmy, że komputer chcąc przesłać dane do innego urządzenia zna jego adres IP, ale nie zna adresu MAC. Aby ten adres poznać, komputer będący nadawcą danych, zanim te konkretne dane wyśle, tworzy ro-zgłoszeniową ramkę ARP, która rozsyłana jest do wszystkich urządzeń w tej samej sieci. W polu adresu źródłowego takiej ramki zapisywany jest adres komputera, który przygotował taką ramkę, a w polu adresu docelowego, ro zgłoszeniowy adres MAC: FF-FF-FF-FF-FF-FF. Każde z urządzeń, które odbierze ramkę, dekapsuluje ją do postaci pakietu i sprawdza, czy w polu docelowym adres IP jest jego adres. Jeśli w polu docelowy adres IP będzie inny adres niż jego, to zignoruje pakiet, jeśli natomiast to jego adres IP, utworzy nową ramkę, w której zapisany będzie jego adres MAC i przekaże ją do przesłania.
Teraz już komputer, który wysłał ro zgłoszeniową ramkę wie jaki adres fizyczny ma urządzenie, z którym chce się skomunikować i taką komunikację może rozpocząć.
Informacje o odwzorowaniu adresu IP na adres MAC zapisywane są w tablicy ARP każdego urządzenia, tak aby można je było wykorzystać w późniejszym czasie. Domyślnie, w systemach Windows wpis taki utrzymuje się maksymalnie do 10 minut, po tym czasie zostaje usunięty. Aby wyświetlić tablicę ARP, należy w konsoli wykonać polecenie arp -a. Jak widać znajdują się tutaj jakieś wpisy, co oznacza, że w ciągu ostatnich 10 minut odbywała się komunikacja pomiędzy moim komputerem a innym urządzeniem.

c) Jakie opcje są dostępne dla tego polecenia? (proszę podać 3-4).

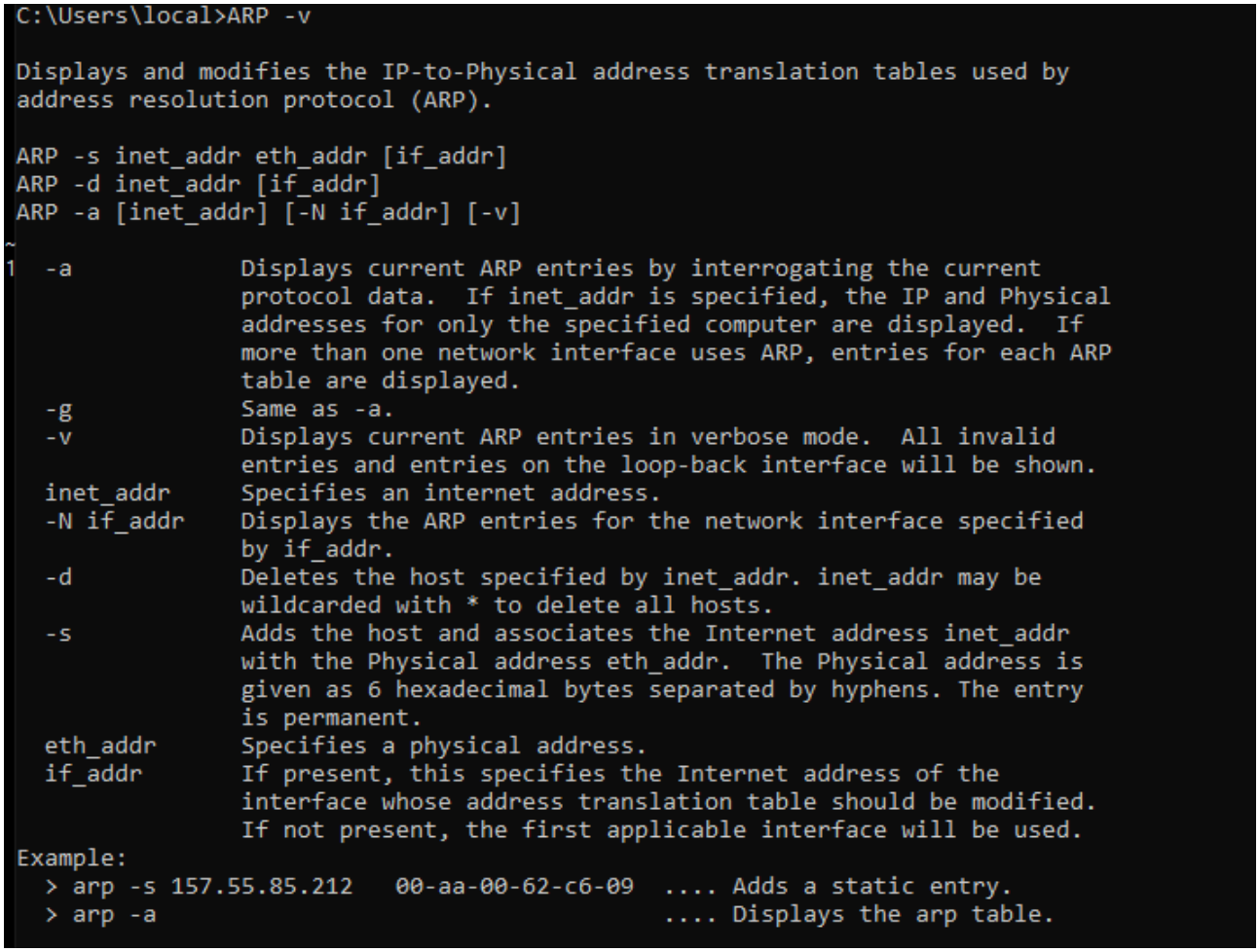
ARP -a:

Wyświetla bieżące wpisy protokołu ARP przez odpytywanie bieżących danych protokołu. Jeżeli **inet_addr** jest określony, to wyświetlany jest adres IP i fizyczny dla określonego komputera. Jeżeli więcej niż jeden interfejs sieciowy korzysta z protokołu ARP, to wyświetlane są wpisy dla każdej tabeli protokołu ARP.

d) Czy informacje uzyskane za pomocą protokołu ARP są zapamiętywane w systemie operacyjnym

ARP -v:

Wyświetla bieżące wpisy protokołu ARP w trybie pełnym. Zostaną pokazane wszystkie nieprawidłowe wpisy oraz wpisy interfejsu pętli zwrotnej.



ARP inet_addr
Określa adres internetowy.
ARP -N if_addr:
Wyświetla wpisy protokołu ARP dla interfejsu sieciowego określonego przez **if_addr.**
ARP-d:
Usuwa hosta określonego przez inet_addr. W inet_addr można użyć symbolu wieloznacznego * do usunięcia wszystkich hostów.
ARP -s:
Dodaje hosta i kojarzy adres internetowy **inet_addr** z fizycznym adresem internetowym **eth_addr**. Adres fizyczny jest reprezentowany przez 6 szesnastkowych bajtów oddzielonych znakami łącznika. Wpis dokonywany jest na stałe.
eth_addr Określa adres fizyczny.

d) Czy informacje uzyskane za pomocą protokołu ARP są zapamiętywane w systemie operacyjnym.
Tak
Informacje o odwzorowaniu adresu IP na adres MAC zapisywane są w tablicy ARP każdego urządzenia, tak aby można je było wykorzystać w późniejszym czasie. Domyślnie, w systemach Windows wpis taki utrzymuje się maksymalnie do 10 minut, po tym czasie zostaje usunięty.

WIRESHARK

4. Przebieg ćwiczenia

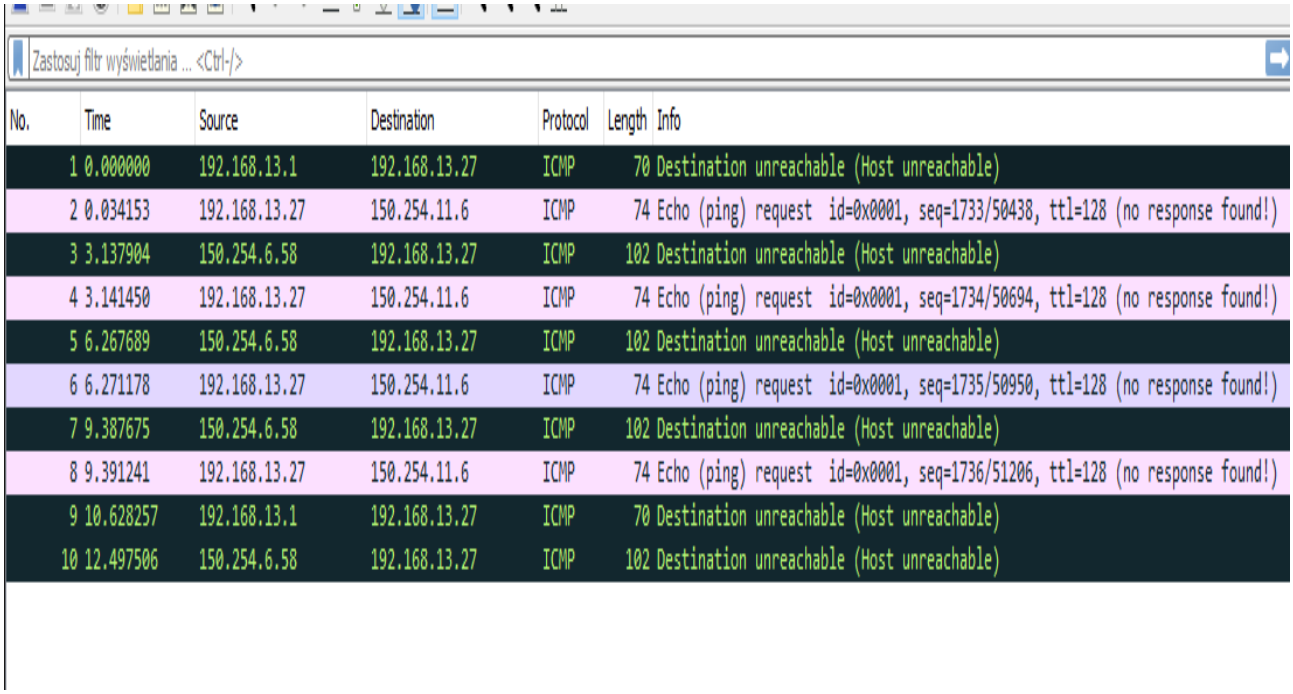
4.1 Analiza działania polecenia `ping`

1. Włączyć wiersz poleceń (cmd).
2. Włączyć program wireshark, wybrać odpowiedni interfejs a następnie włączyć przechwytywanie pakietów.
3. W polu filtra przechwytywania wpisać ICMP.
4. W wierszu poleceń wydać następujące polecenie:

```
ping helios.et.put.poznan.pl
```

5. Po zakończeniu działania polecenia **`ping`** należy wyłączyć przechwytywania pakietów (można zapisać przechwycone pakiety).

```
C:\Users\local>ping helios.et.put.poznan.pl

Pinging helios.et.put.poznan.pl [150.254.11.6] with 32 bytes of data:
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.
Reply from 150.254.6.58: Destination host unreachable.

Ping statistics for 150.254.11.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\local>
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
2	0.034153	192.168.13.27	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=1733/50438, ttl=128 (no response found!)
3	3.137904	150.254.6.58	192.168.13.27	ICMP	102	Destination unreachable (Host unreachable)
4	3.141450	192.168.13.27	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=1734/50694, ttl=128 (no response found!)
5	6.267689	150.254.6.58	192.168.13.27	ICMP	102	Destination unreachable (Host unreachable)
6	6.271178	192.168.13.27	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=1735/50950, ttl=128 (no response found!)
7	9.387675	150.254.6.58	192.168.13.27	ICMP	102	Destination unreachable (Host unreachable)
8	9.391241	192.168.13.27	150.254.11.6	ICMP	74	Echo (ping) request id=0x0001, seq=1736/51206, ttl=128 (no response found!)
9	10.628257	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
10	12.497506	150.254.6.58	192.168.13.27	ICMP	102	Destination unreachable (Host unreachable)

a) Ile wiadomości i jakiego typu wysłał komputer?

-Komputer wysłał 10 wiadomości typu echo.

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

-Komputer otrzymał 10 wiadomości typu echo.

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

- zródło : 192.168.13.1,
- odbiorca: 150.254.6.58,

d) Jakie są różnice pomiędzy adresem IPv4 i MAC?

- adres sieciowy Ipv4 jest zapisany w postaci binarnej, adres Mac jest zapisany w postaci szesnastkowej.

e) **Określić wartość parametru TTL.**

- ttl = 128.

f) Co to jest TTL i dlaczego jest ustawiany w pakietach IP?

- TTl jest to pole w nagłówku pakietu IP, które określa maksymalną liczbę przeskoczeń lub Routerów przez które może przejść pakiet zanim zostanie odrzucony przez sieć. Ustawienie wartości

TTL w pakietach IP umożliwia kontrolowanie, jak daleko i przez ile routerów pakiet może przejść w sieci.

g) Czy pole o podobnym znaczeniu znajduje się w ramce ethernetowej?

Odp: Nie, w ramce Ethernet nie ma pola o podobnym znaczeniu co pole TTL w nagłówku pakietu IP.

Pole TTL jest charakterystyczne tylko dla pakietów protokołu IP.

h) Co się stanie jeżeli polecenie ping zostanie użyte z przełącznikiem –i 2:

```
ping helios.et.put.poznan.pl –i 2
```

i) Narysuj graf przepływu.

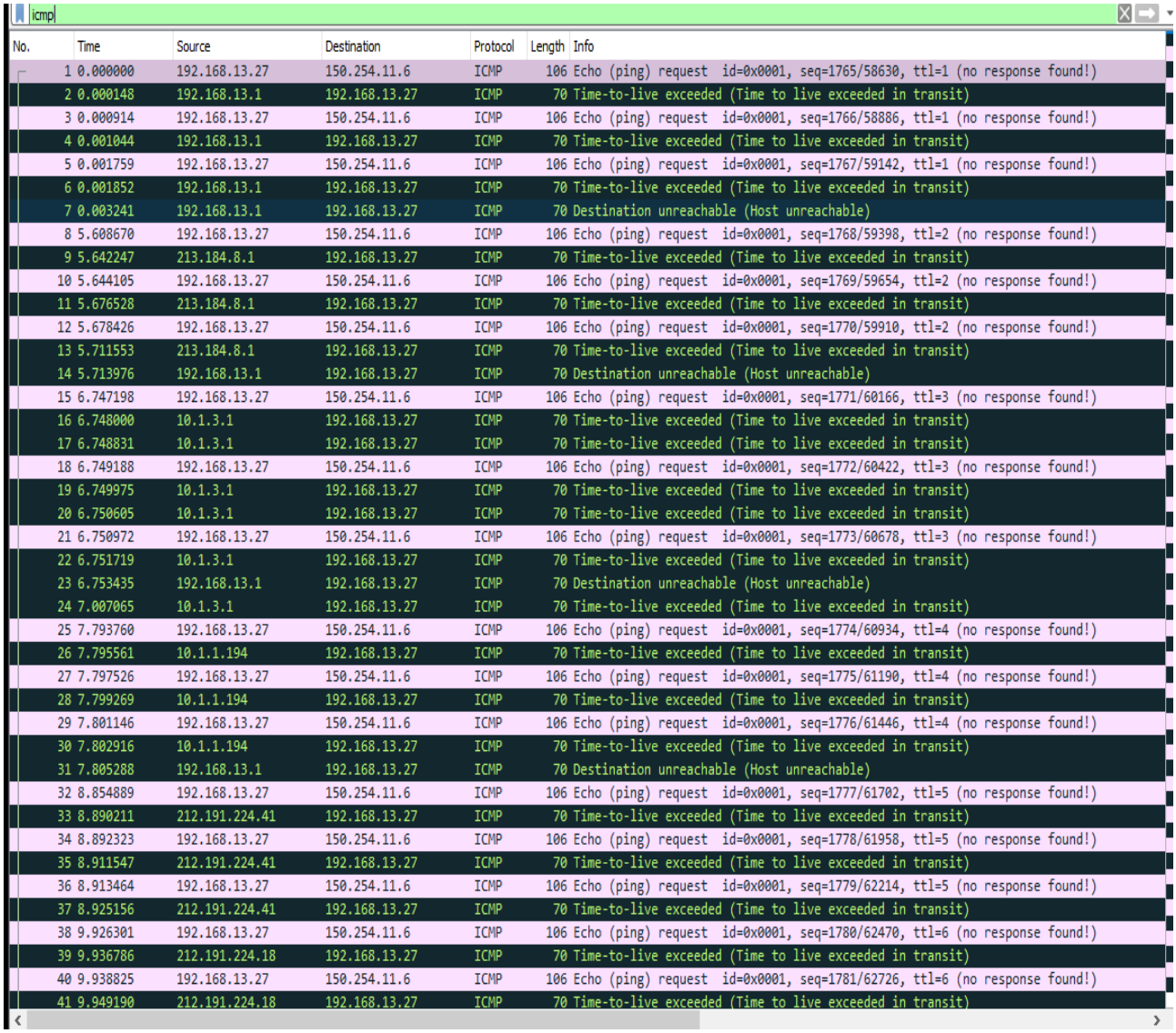
4.2 Analiza działania polecenia `tracert`

1. Włączyć przechwytywanie pakietów.
2. W wierszu poleceń wydać następujące polecenie:

```
tracert helios.et.put.poznan.pl
```

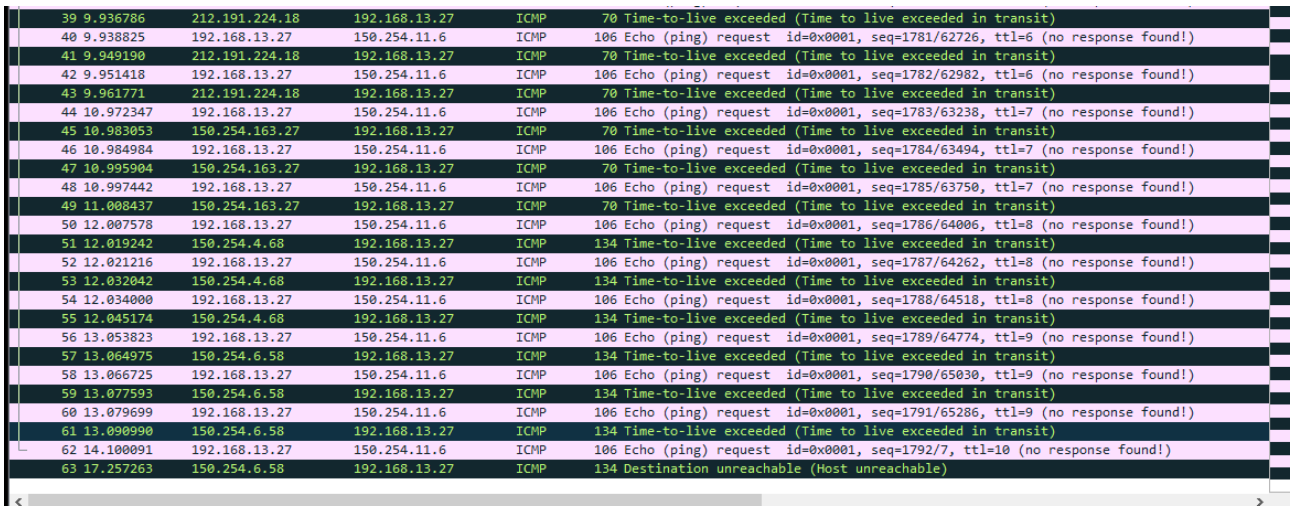
```
C:\Users\local>tracert helios.et.put.poznan.pl

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

  1    <1 ms    <1 ms    <1 ms  192.168.13.1
  2    33 ms    32 ms    33 ms  213.184.8.1
  3     1 ms     1 ms    <1 ms  10.1.3.1
  4     2 ms     2 ms     2 ms  10.1.1.194
  5    35 ms    19 ms    11 ms  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  6    10 ms    10 ms    10 ms  z-poznan-gw3.pozman.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  7    11 ms    11 ms    11 ms  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  8    12 ms    11 ms    11 ms  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  9    11 ms    11 ms    11 ms  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
 10  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]  reports: Destination host unreachable.

Trace complete.
```

3. Po zakończeniu działania polecenia `tracert` należy wyłączyć przechwytywania pakietów a w pole filtru przechwytywania ponownie należy wpisać ICMP.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1765/58630, ttl=1 (no response found!)
2	0.000148	192.168.13.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	0.000914	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1766/58886, ttl=1 (no response found!)
4	0.001044	192.168.13.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.001759	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1767/59142, ttl=1 (no response found!)
6	0.001852	192.168.13.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	0.003241	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
8	5.608670	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1768/59398, ttl=2 (no response found!)
9	5.642247	213.184.8.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	5.644105	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1769/59654, ttl=2 (no response found!)
11	5.676528	213.184.8.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	5.678426	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1770/59910, ttl=2 (no response found!)
13	5.711553	213.184.8.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	5.713976	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
15	6.747198	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1771/60166, ttl=3 (no response found!)
16	6.748000	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
17	6.748831	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.749188	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1772/60422, ttl=3 (no response found!)
19	6.749975	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
20	6.750605	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	6.750972	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1773/60678, ttl=3 (no response found!)
22	6.751719	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	6.753435	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
24	7.007065	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	7.793760	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1774/60934, ttl=4 (no response found!)
26	7.795561	10.1.1.194	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	7.797526	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1775/61190, ttl=4 (no response found!)
28	7.799269	10.1.1.194	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
29	7.801146	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1776/61446, ttl=4 (no response found!)
30	7.802916	10.1.1.194	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31	7.805288	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
32	8.854889	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1777/61702, ttl=5 (no response found!)
33	8.890211	212.191.224.41	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
34	8.892323	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1778/61958, ttl=5 (no response found!)
35	8.911547	212.191.224.41	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
36	8.913464	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1779/62214, ttl=5 (no response found!)
37	8.925156	212.191.224.41	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
38	9.926301	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1780/62470, ttl=6 (no response found!)
39	9.936786	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	9.938825	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1781/62726, ttl=6 (no response found!)
41	9.949190	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)



39	9.936786	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	9.938825	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1781/62726, ttl=6 (no response found!)
41	9.949190	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
42	9.951418	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1782/62982, ttl=6 (no response found!)
43	9.961771	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
44	10.972347	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1783/63238, ttl=7 (no response found!)
45	10.983053	150.254.163.27	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	10.984984	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1784/63494, ttl=7 (no response found!)
47	10.995904	150.254.163.27	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
48	10.997442	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1785/63750, ttl=7 (no response found!)
49	11.008437	150.254.163.27	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	12.007578	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1786/64006, ttl=8 (no response found!)
51	12.019242	150.254.4.68	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
52	12.021216	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1787/64262, ttl=8 (no response found!)
53	12.032042	150.254.4.68	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
54	12.034000	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1788/64518, ttl=8 (no response found!)
55	12.045174	150.254.4.68	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
56	13.053823	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1789/64774, ttl=9 (no response found!)
57	13.064975	150.254.6.58	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
58	13.066725	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1790/65030, ttl=9 (no response found!)
59	13.077593	150.254.6.58	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
60	13.079699	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1791/65286, ttl=9 (no response found!)
61	13.090990	150.254.6.58	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
62	14.100091	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1792/7, ttl=10 (no response found!)
63	17.257263	150.254.6.58	192.168.13.27	ICMP	134	Destination unreachable (Host unreachable)

Odpowiedz na następujące pytania:

a)Ile wiadomości i jakiego typu wysłał komputer?

Odp: Komputer wysłał 63 wiadomości typu echo.

a) Ile wiadomości i jakiego typu odebrał komputer?

Odp: Komputer odebrał wiele wiadomości typu ICMP.

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

Zródło: 192.168.13.27.

Odbiorca: 150.254.6.58.

c) Określić wartość parametru TTL w poszczególnych pakietach.

- Wartości parametrów TTL wynosiły od 1 do 10ttl.

e) Narysuj graf przepływu pakietów (na podstawie grafu wygenerowanego przez wireshark).

5.3 Analiza działania polecenia `pathping`

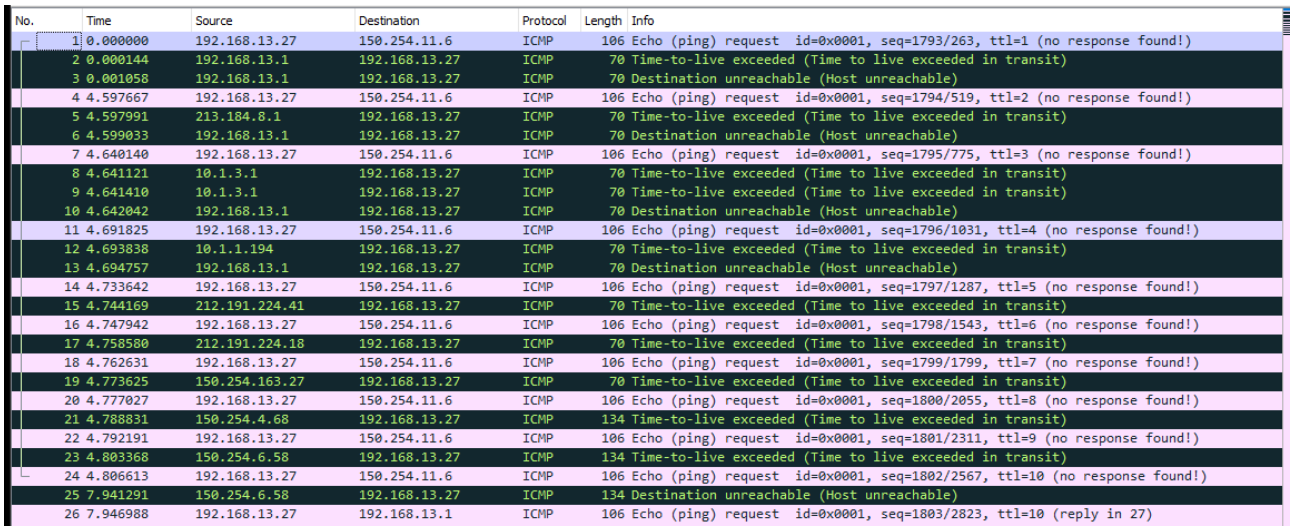
1. Włączyć przechwytywanie pakietów.

2. W wierszu poleceń wydać następujące polecenie:

pathping helios.et.put.poznan.pl

```
C:\Users\local>pathping helios.et.put.poznan.pl

Tracing route to helios.et.put.poznan.pl [150.254.11.6]
over a maximum of 30 hops:
  0  DESKTOP-718DGH2.wmii.local [192.168.13.27]
  1  192.168.13.1
  2  213.184.8.1
  3  10.1.3.1
  4  10.1.1.194
  5  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
  6  z-poznan-gw3.pozman.10Gb.rtr.pionier.gov.pl [212.191.224.18]
  7  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
  8  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
  9  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
 10  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]  reports: Destination host unreachable.

Computing statistics for 250 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-718DGH2.wmii.local [192.168.13.27]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.13.1
                                    0/ 100 =  0%   |
  2    1ms     0/ 100 =  0%     0/ 100 =  0%  213.184.8.1
                                    0/ 100 =  0%   |
  3   ---    100/ 100 =100%   100/ 100 =100%  10.1.3.1
                                    0/ 100 =  0%   |
  4   ---    100/ 100 =100%   100/ 100 =100%  10.1.1.194
                                    0/ 100 =  0%   |
  5   11ms     0/ 100 =  0%     0/ 100 =  0%  z-olsztyna.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.41]
                                    0/ 100 =  0%   |
  6   11ms     0/ 100 =  0%     0/ 100 =  0%  z-poznan-gw3.pozman.10Gb.rtr.pionier.gov.pl [212.191.224.18]
                                    0/ 100 =  0%   |
  7   11ms     0/ 100 =  0%     0/ 100 =  0%  pp-piotrowo-gw.man.poznan.pl [150.254.163.27]
                                    0/ 100 =  0%   |
  8   11ms     0/ 100 =  0%     0/ 100 =  0%  PUTNET-FW-V.put.poznan.pl [150.254.4.68]
                                    0/ 100 =  0%   |
  9   11ms     0/ 100 =  0%     0/ 100 =  0%  PUTNET-X450A-A3-2.put.poznan.pl [150.254.6.58]
                                  100/ 100 =100%   |
 10   ---    100/ 100 =100%     0/ 100 =  0%  DESKTOP-718DGH2 [0.0.0.0]

Trace complete.
```

3. Po zakończeniu działania polecenia pathping należy wyłączyć przechwytywania pakietów a w pole filtru przechwytywania ponownie należy wpisać ICMP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1793/263, ttl=1 (no response found!)
2	0.000144	192.168.13.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3	0.001058	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
4	4.597667	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1794/519, ttl=2 (no response found!)
5	4.597991	213.184.8.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
6	4.599033	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
7	4.640140	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1795/775, ttl=3 (no response found!)
8	4.641121	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	4.641410	10.1.3.1	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	4.642042	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
11	4.691825	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1796/1031, ttl=4 (no response found!)
12	4.693838	10.1.1.194	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	4.694757	192.168.13.1	192.168.13.27	ICMP	70	Destination unreachable (Host unreachable)
14	4.733642	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1797/1287, ttl=5 (no response found!)
15	4.744169	212.191.224.41	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	4.747942	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1798/1543, ttl=6 (no response found!)
17	4.758580	212.191.224.18	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	4.762631	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1799/1799, ttl=7 (no response found!)
19	4.773625	150.254.163.27	192.168.13.27	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
20	4.777027	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1800/2055, ttl=8 (no response found!)
21	4.788831	150.254.4.68	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
22	4.792191	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1801/2311, ttl=9 (no response found!)
23	4.803368	150.254.6.58	192.168.13.27	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
24	4.806613	192.168.13.27	150.254.11.6	ICMP	106	Echo (ping) request id=0x0001, seq=1802/2567, ttl=10 (no response found!)
25	7.941291	150.254.6.58	192.168.13.27	ICMP	134	Destination unreachable (Host unreachable)
26	7.946988	192.168.13.27	192.168.13.1	ICMP	106	Echo (ping) request id=0x0001, seq=1803/2823, ttl=10 (reply in 27)

Odpowiedz na następujące pytania:

a) Ile wiadomości i jakiego typu wysłał komputer?

Komputer wysłał 26 wiadomości typu echo.

b) Ile wiadomości i jakiego typu odebrał komputer?

Komputer odebrał bardzo dużo wiadomości typu echo.

c) Czy w wysyłanych (odbieranych) pakietach zmieniana jest wartość parametru TTL, jeśli tak to w jaki sposób?

Odp: W wysyłanych pakietach jest wartość zmieniana i zawiera się w przedziale od 1 do 10.

d) Na podstawie przechwyconych pakietów w wiadomościami protokołu ICMP przedstaw zasadę działania polecenia `pathping`.

W tym przypadku pathping pozwala na śledzenie trasy pakietów w sieci, podobnie jak tracert, ale również zbiera statystyki przepływu ruchu podobnie jak ping. Pathping działa przez wysyłanie serii pakietów ICMP do każdego routera na trasie miedzy nadawcą a docelowym adresem IP, a następnie monitoruje odpowiedzi na te pakiety ICMP.

e) Narysuj uproszczony graf przepływu.

`5.4` Analiza działania protokołów telnet oraz ssh

1. Włączyć przechwytywanie pakietów (wyczyść filtr przechwytywania).
2. Uruchom program **putty** (rysunek 8) i za pomocą protokołu telent (Connection type Telnet) połącz się z serwerem:
`helios.et.put.poznan.pl`
(w przypadku braku konta na serwerze proszę użyć danych do logowania:
Login: **user**
Password: **qwerty**
3. Niezależnie od tego czy próba logowania zakończyła się sukcesem przerwać przechwytywanie pakietów a w pole filtra wyświetlania wpisać **telnet**.
4. klikając na dowolnym pakiecie związanym z nawiązywaniem połączenia z serwerem za pomocą protokołu telnet prawym klawiszem myszy wybierz opcję **`Follow TCP Stream.`**
Odpowiedz na następujące pytania:
a) Jakie informacje przedstawia program po wyborze opcji **`Follow TCP Stream`**?
b) Co można powiedzieć o protokole **`telnet`**?

c) W jaki sposób przesyłane są login i hasło?
Czynności 1-4 powtórz dla protokołu ssh (program putty, connection type ssh) i odpowiedz na pytania a-c w odniesieniu do protokołu ssh.
Podsumowując tę cześć ćwiczenia odpowiedz na pytanie:
d) Który sposób łączenia się z serwerem jest bardziej bezpieczny?

5.5 Analiza działania protokołu FTP

Wykonać analizę przesyłanych danych niezbędnych do łączenia się z serwerem w przypadku protokołu FTP (ćwiczenie należy wykonać w analogiczny sposób jak
w przypadku protokołów telnet). Również w tym przypadku należy podjąć próbę połączenia z serwerem FTP dostępnym na helios.et.put.poznan.pl
- czy istnieje bezpieczniejszy od FTP sposób przesyłania plików?