Wireshark-Analizator protokołów

zad. 4.1

```
C:\Users\local>ping www.wp.pl
Pinging www.wp.pl [212.77.98.9] with 32 bytes of data:
Reply from 212.77.98.9: bytes=32 time=4ms TTL=56
Ping statistics for 212.77.98.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms
C:\Users\local>ping www.wp.pl
Pinging www.wp.pl [212.77.98.9] with 32 bytes of data:
Reply from 212.77.98.9: bytes=32 time=4ms TTL=56
Reply from 212.77.98.9: bytes=32 time=4ms TTL=56
Reply from 212.77.98.9: bytes=32 time=5ms TTL=56
Reply from 212.77.98.9: bytes=32 time=4ms TTL=56
Ping statistics for 212.77.98.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
C:\Users\local>
```

| No. | Time | Source | Destination | Protocol | Length Info | |
|-----|-------------|---------------|---------------|----------|------------------------|--|
| 7 | 4 2.357121 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request | id=0x0001, seq=9/2304, ttl=128 (reply in 5) |
| + | 5 2.361392 | 212.77.98.9 | 192.168.13.20 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=9/2304, ttl=56 (request in 4) |
| | 8 3.367806 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request | id=0x0001, seq=10/2560, ttl=128 (reply in 9) |
| | 9 3.372198 | 212.77.98.9 | 192.168.13.20 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=10/2560, ttl=56 (request in 8) |
| | 13 4.387699 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request | id=0x0001, seq=11/2816, ttl=128 (reply in 14) |
| | 14 4.392142 | 212.77.98.9 | 192.168.13.20 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=11/2816, ttl=56 (request in 13) |
| | 16 5.407877 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request | id=0x0001, seq=12/3072, ttl=128 (reply in 17) |
| L | 17 5.412144 | 212.77.98.9 | 192.168.13.20 | ICMP | 74 Echo (ping) reply | id=0x0001, seq=12/3072, ttl=56 (request in 16) |

Komputer wysłał cztery wiadomości i otrzymał również cztery odpowiedzi

1 Lokalizacja: IP: 192.168.13.20 MAC: bc:ae:c5:cd:83:06

2 Lokalizacja: IP: 212.77.98.9MAC:fc:f9:38:a3:a1:4f

Wartość parametru TTL jest równy 56

TTL - (ang. Time To Live) to parametr określający maksymalny czas życia pakietów. TTL definiuje jak długo wysłany pakiet danych może krążyć w sieci przechodząc od jednego routera do drugiego.

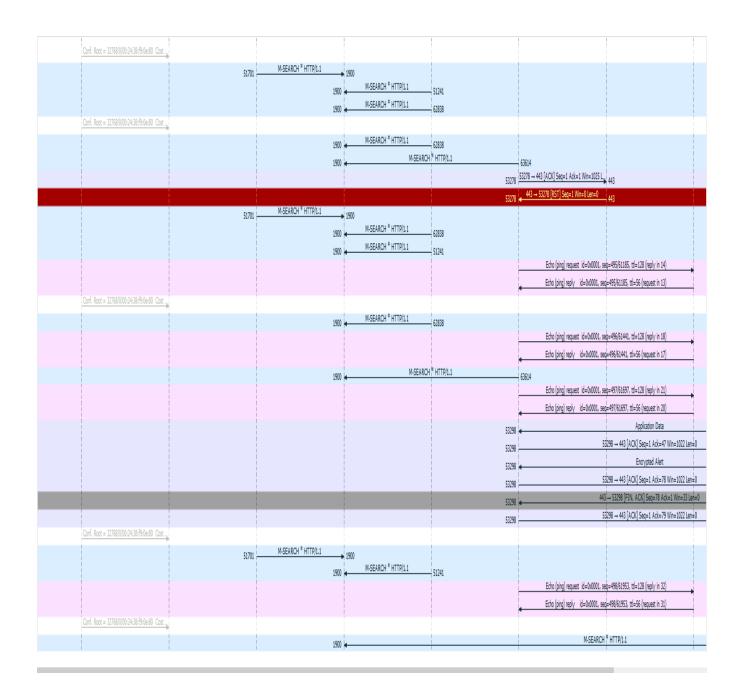
Różnica pomiędzy adresem IPv4 i MAC polega na tym, że adres MAC jednoznacznie identyfikuje urządzenie, które chce wziąć udział w sieci. Z drugiej strony, adres IP w unikalny sposób definiuje połączenie sieci z interfejsem urządzenia. Przeanalizujmy kilka innych różnic między adresem MAC a adresem IP za pomocą tabeli porównawczej pokazanej poniżej.

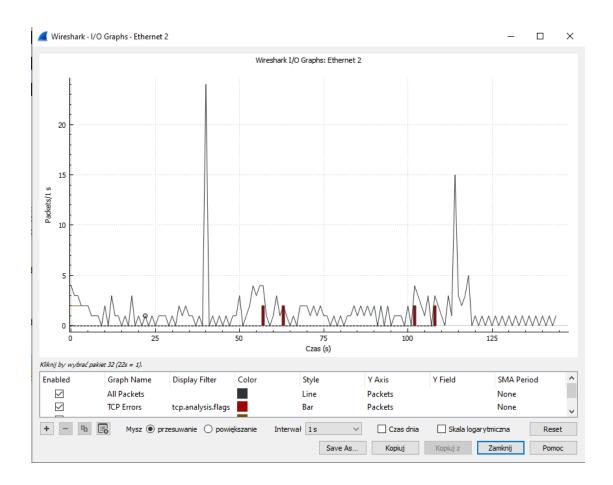
Wykres porównania

| Podstawa do porównania | PROCHOWIEC | IP |
|------------------------|--|---|
| Pełna forma | Adres kontroli dostępu do multimediów. | Adres protokołu internetowego. |
| Cel, powód | Określa adres fizyczny komputera w Internecie. | Określa połączenie komputera w Internecie. |
| Bity | Jest to szesnastkowy adres o długości 48 bitów (6 bajtów). | IPv4 to 32-bitowy (4 bajty) adres, a IPv6 to 128-bitowy (16-bajtowy) adres. |
| Adres | Adres MAC jest przydzielany przez producenta karty NIC. | Adres IP jest przydzielany przez administratora sieci lub dostawcę usług internetowych. |
| Pobierz adres | Protokół ARP może pobrać adres MAC urządzenia. | Protokół RARP może pobrać adres IP urządzenia. |

Przy poleceniu www.wp.pl -i 2 nie uzyskano żadnej odpowiedzi

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|-------------|---------------|---------------|----------|---|
| Γ | 3 0.772911 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request id=0x0001, seq=17/4352, ttl=2 (no response found!) |
| | 4 0.773199 | 213.184.8.1 | 192.168.13.20 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| | 6 1.776989 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request id=0x0001, seq=18/4600, ttl=2 (no response found!) |
| | 7 1.808304 | 213.184.8.1 | 192.168.13.20 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| | 9 2.797090 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request id=0x0001, seq=19/4864, ttl=2 (no response found!) |
| | 10 2.797432 | 213.184.8.1 | 192.168.13.20 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| | 11 3.816933 | 192.168.13.20 | 212.77.98.9 | ICMP | 74 Echo (ping) request id=0x0001, seq=20/5120, ttl=2 (no response found!) |
| | 12 3.823187 | 213.184.8.1 | 192.168.13.20 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |





zad 4.2

Za pomocą polecenia tracert uwm.edu.pl wysłano 21 zapytań i otrzymano 4 odpowiedzi

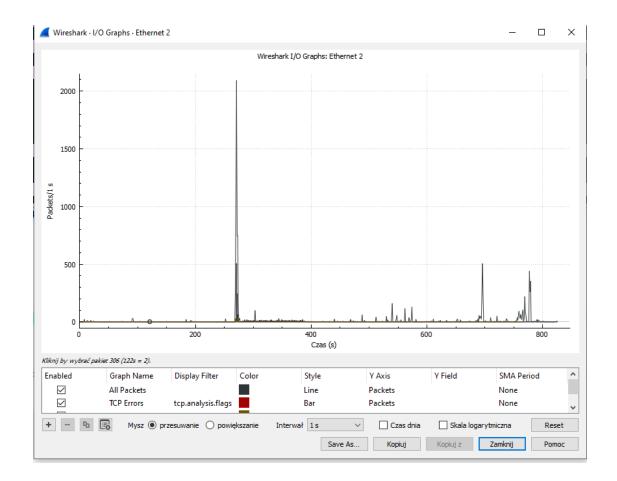
adresy IP oraz Mac źródła i odbiorcy

192.168.13.1 oraz 192.168.13.20

fc:f9:38:a3:a1:4f bc:ae:c5:cd:83:06

TTL=128

| Sandard query 0x59k A www.google.com S3 | |
|---|-------------|
| Sandard query be394: A www.google.com | |
| | |
| Sandard Query Mc32d HTTPS www.google.com | |
| Special Query response 0x632d HTTPS www | |
| SSC3 Protected Phylodic (PRP) PADD (MS, CRYPTO, PADD (MS, C | |
| SSA39 | |
| SSR29 | |
| 53639 A Protected Psychol (NPO) 443 | |
| 2007 | |
| 52629 443 | |
| Protected Psychol (KPO) | |
| SSR35 - """ (White Pay Tour Sept 1997) 443 | |
| 22027 | |
| 53(25 Protected Pay/lead (1909), DCID=#d69519473a2d9ff + 443 | |
| 53629 a Protected Psyload (IAPO) 443 | |
| S1615 Protected Psyload (KPI) | |
| \$5039 Prosecuted Paryland (NOV), DCID=editio3/672e269ff 413 | |
| Conf. Root = 32766()00:2438:R510480 Cost | |
| Conf. Root = 337/60/0002438:f50/e80 Cost | |
| Conf. Root = 32768(000)24/36/9/04/80 Cost | |
| Conf. Root = 32798(900).438/99:0e90 Cost., | |
| | |
| Corf. Roor = 32798(0)002-438/95/se-80 Cost | |
| Corf. Root = 32768(0)00.2438(9)6e:80 Cost | |
| 50637 Standard query (0x0785 A unm edu pl | → 53 |
| 55 Destination unreachable (Hots unreachable) | 4 |
| 50637 Standard query flua?765 A wmm.edu.pl 🛶 53 | |
| Specified Query response Dia 785 A own-setup! 33 | |
| Echo (ping request id=0,0001, seq=499 (52,009, til=1 (po re | sponse fo |
| Time-to-live exceeded (Time to live exceeded in trans) | |
| Echo (ping) risquest: id=0.000001, seep=500(E3455, tink 1 (no n | enonea fo |
| Time-to-live exceeding live from the first account of the first account | aponde 10 |
| | |
| Echo (ping) Repeat id=0x0001, seq=501(82721, ti=1 (no re | sponse to |
| Time-to-live exceeded (Timé to live exceeded in transit) | \vdash |
| | - 53 |
| | |



zad 5.3

Za pomocą polecenia pathping wysłano 762 zapytania i otrzymano 379 odpowiedzi

Wartość TTL jest zmieniana

Parametr TTL zapobiega zapętleniu pakietów w sieci. Żeby pakiet nie krążyły się pomiędzy urządzeniami sieciowymi w nieskończoność, każdy z routerów, przez które przechodzi pakiet, obniża wartość TTL o 1. Jeśli wartość TTL na początku wynosi 64, po przejściu przez pierwszy router będzie miała wartość 63. Pakiet po przejściu przez drugi router będzie miał TTL = 62 itd. Router, który obniży wartość TTL do zera, nie prześle pakietu dalej! Zamiast tego wyśle do nadawcy wiadomość o niemożliwości dalszego przesyłania pakietów. Ponieważ maksymalna wartość TTL to 255 (pole ma rozmiar 8 bitów), pakiet po przejściu przez maksymalnie 255 routerów zostanie zablokowany i nie będzie krążył dłużej w sieci.

