

1. Zapoznaj się z interfejsem i funkcjami programu **Wireshark**. Wyświetl przechwytywane i odfiltrowane wg. dowolnego protokołu pakiety sieciowe.

Welcome to Wireshark

Przechwytywanie

...używając tego filtru:

Wi-Fi
Połączenie lokalne* 9
Połączenie lokalne* 8
Połączenie lokalne* 7
Połączenie lokalne* 10
Połączenie lokalne* 1
Ethernet 2
Adapter for loopback traffic capture
Ethernet

Przechwytywanie

Plik Edytuj Widok Idź Przechwyty Analizuj Statystyki Telefonnia Bezprzewodowe Narzędzia Pomoc

Wzrostaj filtry wyświetlania ... <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
982	10.903589	192.168.1.104	213.184.8.16	TCP	55	[TCP Retransmission] 58970 → 80 [ACK] Seq=0 Ack=1 Win=517 Len=1
983	10.966671	213.184.8.16	192.168.1.104	TCP	54	80 → 58969 [ACK] Seq=1 Ack=1 Win=237 Len=0
984	10.974395	213.184.8.16	192.168.1.104	TCP	54	80 → 58970 [ACK] Seq=1 Ack=1 Win=259 Len=0
985	10.974395	37.157.2.237	192.168.1.104	TCP	54	443 → 58962 [ACK] Seq=1 Ack=2 Win=33 Len=0
986	11.674005	192.168.1.1	192.168.1.255	UDP	329	38934 → 20002 Len=287
987	12.191692	192.168.1.104	20.91.188.53	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 59003 → 5005 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
988	12.469540	192.168.1.104	20.91.188.53	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 58999 → 5005 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
989	12.731345	192.168.1.104	20.91.188.53	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 59000 → 5005 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
990	13.164182	192.168.1.104	51.83.214.237	TCP	55	58949 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
991	13.209732	51.83.214.237	192.168.1.104	TCP	54	443 → 58949 [ACK] Seq=1 Ack=2 Win=501 Len=0
992	13.619563	13.107.3.254	192.168.1.104	TCP	54	443 → 58926 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
993	13.721297	fe80::1e61:b4ff:fe9...ff02::1		ICMPv6	86	Router Advertisement from 1c:61:b4:96:f3:96
994	13.723403	213.184.8.16	192.168.1.104	TCP	54	80 → 58996 [FIN, ACK] Seq=22963 Ack=2799 Win=35328 Len=0
995	13.723458	192.168.1.104	213.184.8.16	TCP	54	58996 → 80 [ACK] Seq=2799 Ack=22964 Win=131328 Len=0
996	14.234021	13.69.239.74	192.168.1.104	TCP	54	443 → 58916 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
997	14.269786	20.193.187.221	192.168.1.104	TCP	54	443 → 58927 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
998	14.440392	13.107.18.254	192.168.1.104	TCP	54	443 → 58925 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
999	14.889260	192.168.1.104	20.91.188.53	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 59002 → 5005 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

> Frame 1: 93 bytes on wire (744 bits) 93 bytes captured (744 bits) on interface \Device\NPF{0F688ADD-2} 0000 30 c9 ah 93 74 hd 1c 61 b4 96 f3 96 08 00 45 00 0...f...aF-

Odfiltrowane pakiety sieciowe

http						
No.	Time	Source	Destination	Protocol	Length	Info
+	179	4.355927	192.168.1.104	213.184.8.16	HTTP	683 GET / HTTP/1.1
+	208	4.462809	213.184.8.16	192.168.1.104	HTTP	1494 [TCP Previous segment not captured] Continuation
+	217	4.465214	213.184.8.16	192.168.1.104	HTTP	164 Continuation
+	226	4.468211	213.184.8.16	192.168.1.104	HTTP	59 Continuation
+	482	6.858522	192.168.1.104	213.184.8.16	HTTP	690 GET /user HTTP/1.1
+	502	7.066484	213.184.8.16	192.168.1.104	HTTP	884 HTTP/1.1 200 OK (text/html)
+	725	8.156989	192.168.1.104	213.184.8.16	HTTP	927 POST /user HTTP/1.1 (application/x-www-form-urlencoded)
+	751	8.467410	213.184.8.16	192.168.1.104	HTTP	912 HTTP/1.1 200 OK (text/html)
+	770	8.627737	192.168.1.104	213.184.8.16	HTTP	714 GET /sites/all/themes/omega/images/misc/message-24-error.png?1382488163 HTTP/1.1
+	781	8.688537	213.184.8.16	192.168.1.104	HTTP	1053 HTTP/1.1 200 OK (PNG)

2. Zapoznaj się z poleceniem **ipconfig**. Porównaj wewnętrzny adres IP z zewnętrznym, który można uzyskać np. na stronie **whatismyip.com**.

```
C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::3450:7c5c:f575:281d%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
Wireless LAN adapter Połączenie lokalne* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Wireless LAN adapter Połączenie lokalne* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
Wireless LAN adapter Wi-Fi:

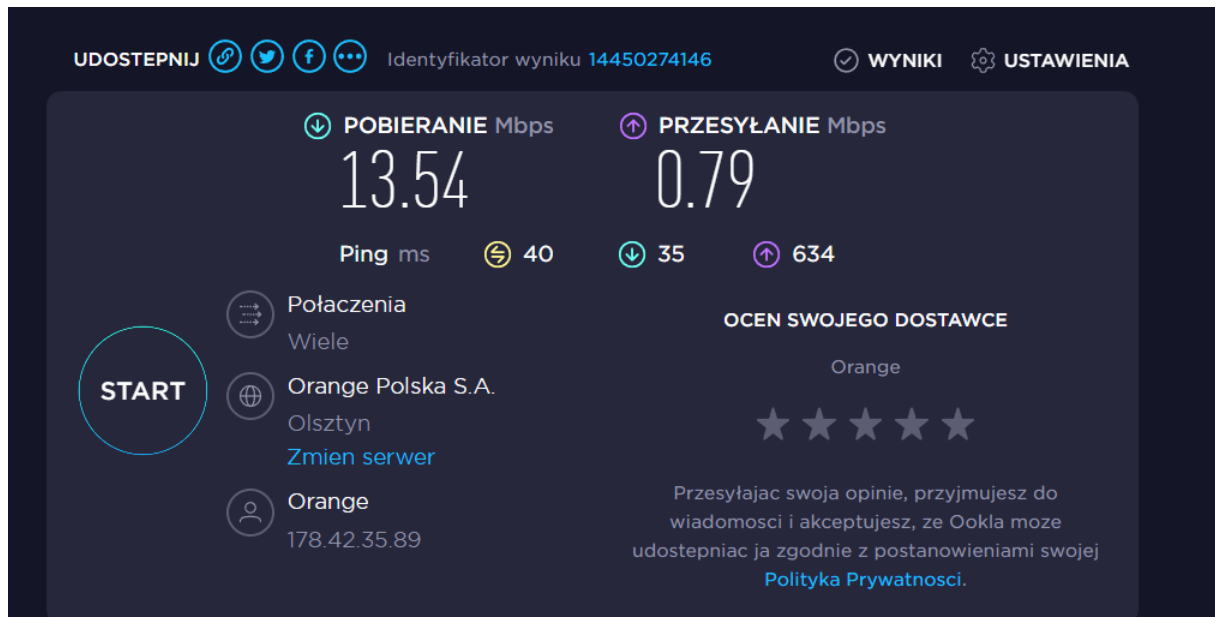
    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::35fc:fd4e:8b05:92dc%5
    IPv4 Address. . . . . : 192.168.1.104
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

Wewnętrzny adres IP: 192.168.1.104

My Public IPv4 is: [178.42.35.89](https://www.speedtest.net/public/178.42.35.89)

Adresy się różnią.

3. Zapoznaj się z możliwościami pomiaru prędkości dostępu do Internetu za pomocą speedtest.net.



4. Zapoznaj się z pracą polecenia ping, wyświetl odpowiedź od dowolnego hosta w Internecie.

```
C:\Users\admin>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=24ms TTL=60
Reply from 212.77.98.9: bytes=32 time=36ms TTL=60
Reply from 212.77.98.9: bytes=32 time=23ms TTL=60
Reply from 212.77.98.9: bytes=32 time=24ms TTL=60

Ping statistics for 212.77.98.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 36ms, Average = 26ms

C:\Users\admin>
```

5. Zapoznaj się z poleceniem tracert, wyświetl trasę do dowolnego hosta w Internecie.

```
C:\Users\admin>tracert www.wp.pl

Tracing route to www.wp.pl [212.77.98.9]
over a maximum of 30 hops:

  1    12 ms    3 ms    3 ms  192.168.1.1
  2    29 ms    22 ms   20 ms  ols-bng2.neo.tpnet.pl [83.1.4.178]
  3    21 ms    21 ms   21 ms  ols-ar2.tpnet.pl [80.50.159.169]
  4    44 ms    24 ms   25 ms  war-ar5.tpnet.pl [213.25.5.30]
  5     *        *        *    Request timed out.
  6    25 ms    23 ms   23 ms  www.wp.pl [212.77.98.9]

Trace complete.

C:\Users\admin>
```

6. Zapoznaj się z narzędziem nslookup, wyszukaj adres IP dowolnego serwera.

```
C:\Users\admin>nslookup www.wp.pl
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.wp.pl
Address: 212.77.98.9

C:\Users\admin>
```

7. Zapoznaj się z poleceniem arp, użyj opcji "arp -a" oraz "arp -d".

```
C:\Users\admin>arp -a

Interface: 192.168.1.104 --- 0x5
Internet Address      Physical Address      Type
192.168.1.1           1c-61-b4-96-f3-96     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xd
Internet Address      Physical Address      Type
192.168.56.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22           01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250      01-00-5e-7f-ff-fa     static

C:\Users\admin>
```

```
C:\Users\admin>arp -d 244.0.0.22
The ARP entry deletion failed: Żądana operacja wymaga podniesienia uprawnień.
```

Nie posiadam uprawnień.

8. Zobacz pliki w folderze C:\Windows\System32\drivers\etc i zapoznaj się z ich przeznaczeniem.

« Windows > System32 > drivers > etc					Przeszukaj: etc
Nazwa	Data modyfikacji	Typ	Rozmiar		
hosts	22.09.2021 16:39	Plik	1 KB		
lmhosts.sam	22.09.2021 16:39	Plik SAM	4 KB		
networks	22.09.2021 16:39	Plik	1 KB		
protocol	22.09.2021 16:39	Plik	2 KB		
services	22.09.2021 16:39	Plik	18 KB		

hosts -> zawiera mapowanie adresów IP z nazwami hostów

```
102.54.94.97      rhino.acme.com      # source server
38.25.63.10      x.acme.com          # x client host
```

lmhosts.sam -> zawiera mapowania adresów IP z nazwami komputerów (NetBIOS).

```
102.54.94.97      rhino      #PRE #DOM:networking #net group's DC
102.54.94.102     "appname  \0x14" #special app server
102.54.94.123     popular      #PRE      #source server
102.54.94.117     localsrv     #PRE      #needed for the include
```

networks -> zawiera mapowanie nazw sieci z numerem sieci dla sieci lokalnych

```
<network name>  <network number>      [aliases...]  [#<comment>]
```

For example:

```
loopback      127
campus        284.122.107
london        284.122.108
```

protocol -> zawiera protokoły internetowe zdefiniowane przez różne RFC

```
# <protocol name>  <assigned number>  [aliases...]  [#<comment>]
```

```
ip      0      IP      # Internet protocol
icmp    1      ICMP    # Internet control message protocol
ggp     3      GGP     # Gateway-gateway protocol
tcp     6      TCP     # Transmission control protocol
egp     8      EGP     # Exterior gateway protocol
pup     12     PUP     # PARC universal packet protocol
udp     17     UDP     # User datagram protocol
hmp     20     HMP     # Host monitoring protocol
```

services -> zawiera numery portów dla dobrze znanych usług zdefiniowanych przez IANA

```
..
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
```

```
echo          7/tcp
echo          7/udp
discard       9/tcp    sink null
discard       9/udp    sink null
sysstat       11/tcp    users          #Active users
sysstat       11/udp    users          #Active users
daytime       13/tcp
daytime       13/udp
qotd          17/tcp    quote          #Quote of the day
qotd          17/udp    quote          #Quote of the day
```