Czym jest Wireshark?

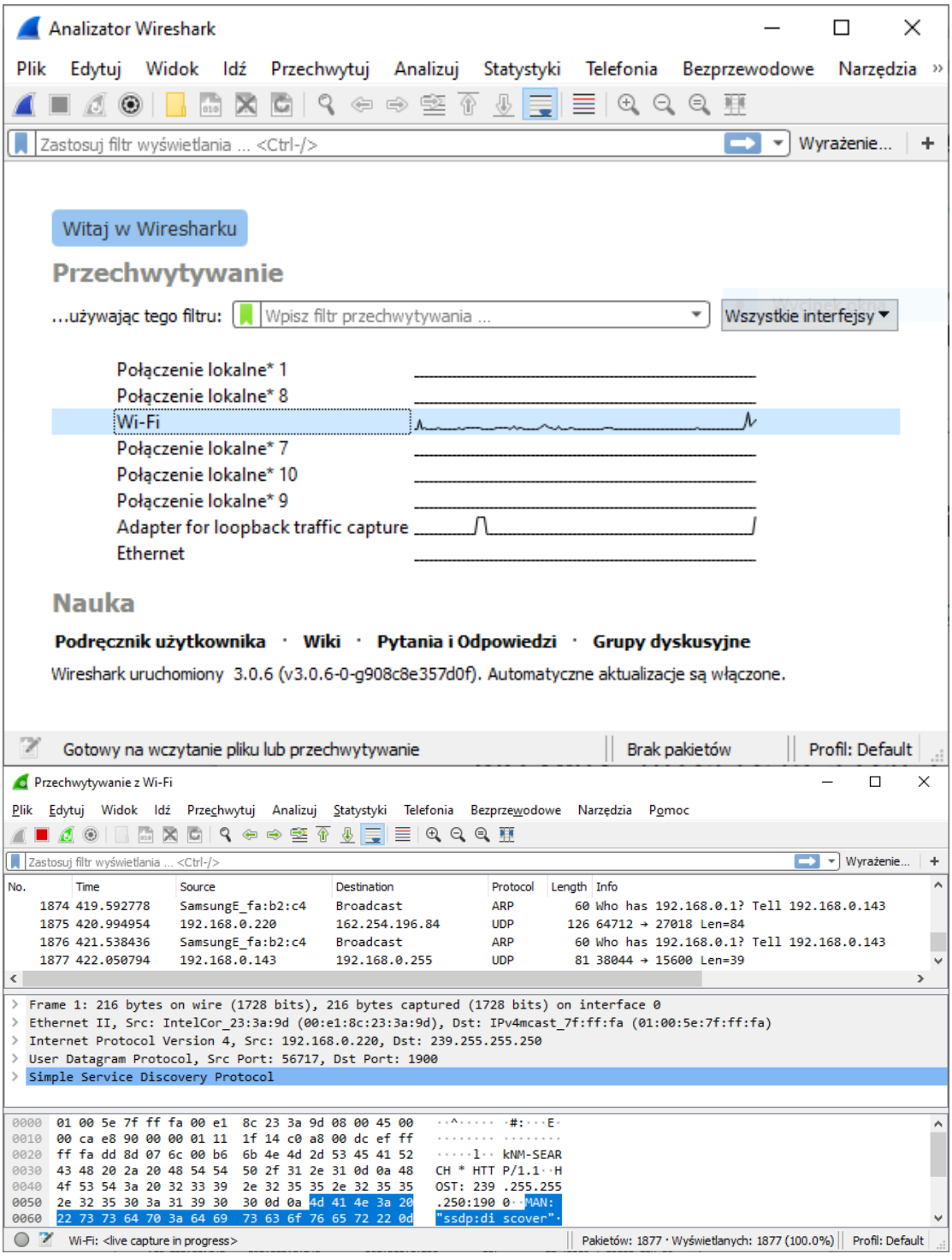
Jest to narzędzie służące do analizy pakietów sieciowych.

Przykłady zastosowania programu Wireshark:

- diagnoza problemów w sieci (trouble-shooting)
- analiza ruchu sieciowego
- budowa nowych protokołów komunikacyjnych

Instalacja oraz używanie programu:

1. Pobranie oraz instalacja programu ze strony:
   https://www.wireshark.org/#download.
2. Uruchom program Wireshark.
3. Wybierz najbardziej aktywny interfejs (ten zazwyczaj będzie głównym interfejsem odpowiedzialnym za sieć).

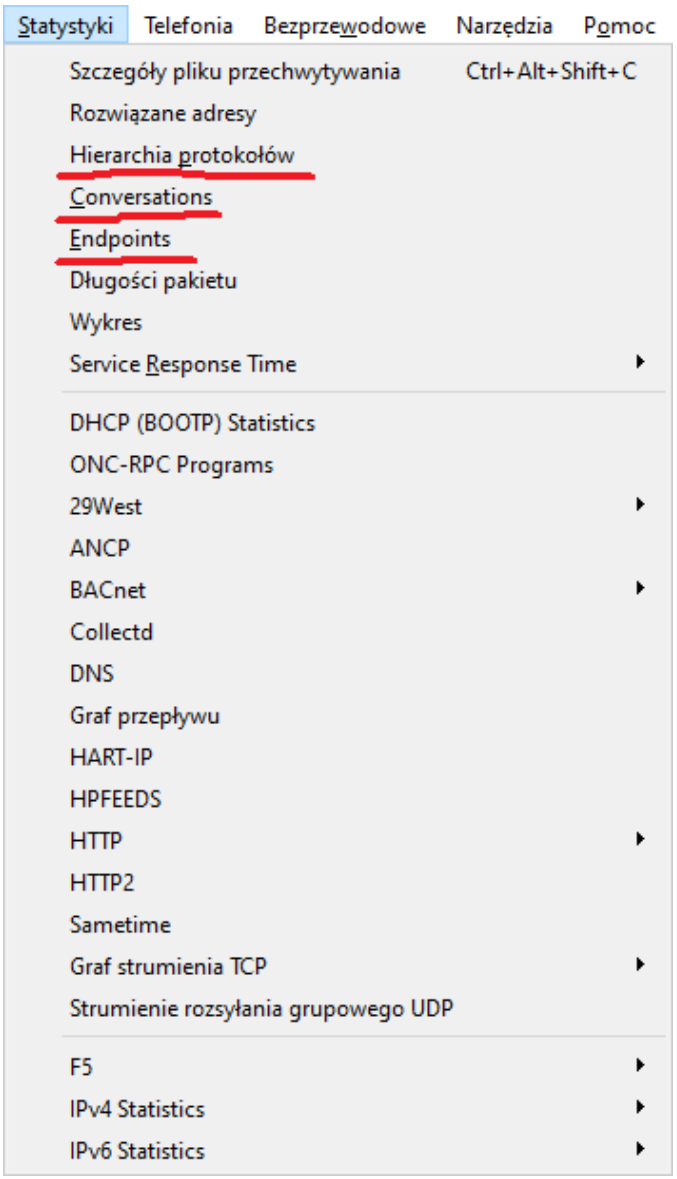

Analizator Wireshark
Plik Edytuj Widok Idź Przechwytuj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia
Zastosuj filtr wyświetlania ... <Ctrl-/>
Wyrażenie...
Witaj w Wiresharku
Przechwytywanie
...używając tego filtru:
Wpisz filtr przechwytywania ...
Wszystkie interfejsy
Połączenie lokalne* 1
Połączenie lokalne* 8
Wi-Fi
Połączenie lokalne* 7
Połączenie lokalne* 10
Połączenie lokalne* 9
Adapter for loopback traffic capture
Ethernet
Nauka
Podręcznik użytkownika · Wiki · Pytania i Odpowiedzi · Grupy dyskusyjne
Wireshark uruchomiony 3.0.6 (v3.0.6-0-g908c8e357d0f). Automatyczne aktualizacje są włączone.
Gotowy na wczytanie pliku lub przechwytywanie
Brak pakietów
Profil: Default
Przechwytywanie z Wi-Fi
Plik Edytuj Widok Idź Przechwytuj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
Zastosuj filtr wyświetlania ... <Ctrl-/>
Wyrażenie...
No. Time Source Destination Protocol Length Info
1874 419.592778 SamsungE_fa:b2:c4 Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.143
1875 420.994954 192.168.0.220 162.254.196.84 UDP 126 64712 → 27018 Len=84
1876 421.538436 SamsungE_fa:b2:c4 Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.143
1877 422.050794 192.168.0.143 192.168.0.255 UDP 81 38044 → 15600 Len=39
Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: IntelCor_23:3a:9d (00:e1:8c:23:3a:9d), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.220, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 56717, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 00 e1 8c 23 3a 9d 08 00 45 00 ··^····· ·#:···E·
0010 00 ca e8 90 00 00 01 11 1f 14 c0 a8 00 dc ef ff ···· ····
0020 ff fa dd 8d 07 6c 00 b6 6b 4e 4d 2d 53 45 41 52 ·····l·· kNM-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1··H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0··MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover"·
Wi-Fi: <live capture in progress>
Pakietów: 1877 · Wyświetlanych: 1877 (100.0%)
Profil: Default

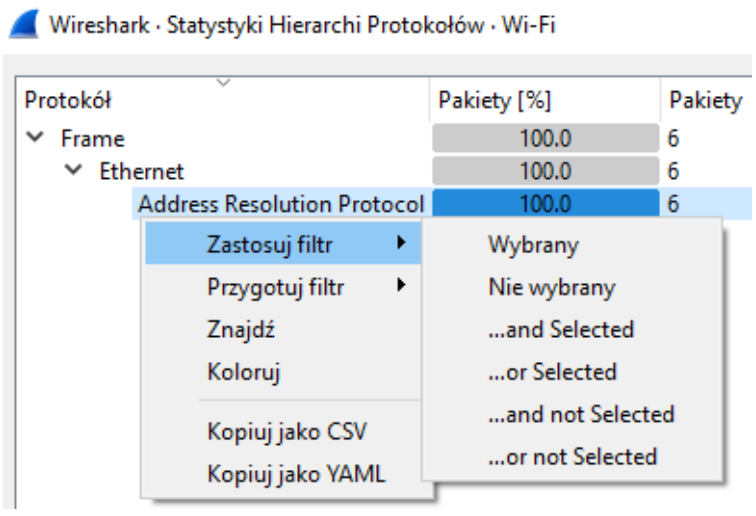
4. Zastosowanie filtrów w celu ograniczenia wyświetlanych pakietów.

Istnieją dwa sposoby na określenie filtru:
- wykorzystanie pola tekstowego
- menu.

❖ wykorzystanie pola tekstowego
- ➢ W polu tekstowym filtra, wpisujemy:
  - ip.addr dla adresu IP
  - ip.src dla adresu źródła
  - ip.dst dla adresu docelowego
  - tcp.port dla portu TCP
  - udp.port dla portu UDP
  - nazwę protokołu
  - == jako porównanie
  - in {[a] [b] [c] [...]} jako przynależność do zbioru (np. tcp.port in {80 25})
  - and, or, not jako i, albo, nie

❖ menu
- ➢ W menu na pasku o nazwie "Statystyki" mamy możliwość ograniczenia pakietów względem protokołu, konwersacji oraz punktów końcowych.





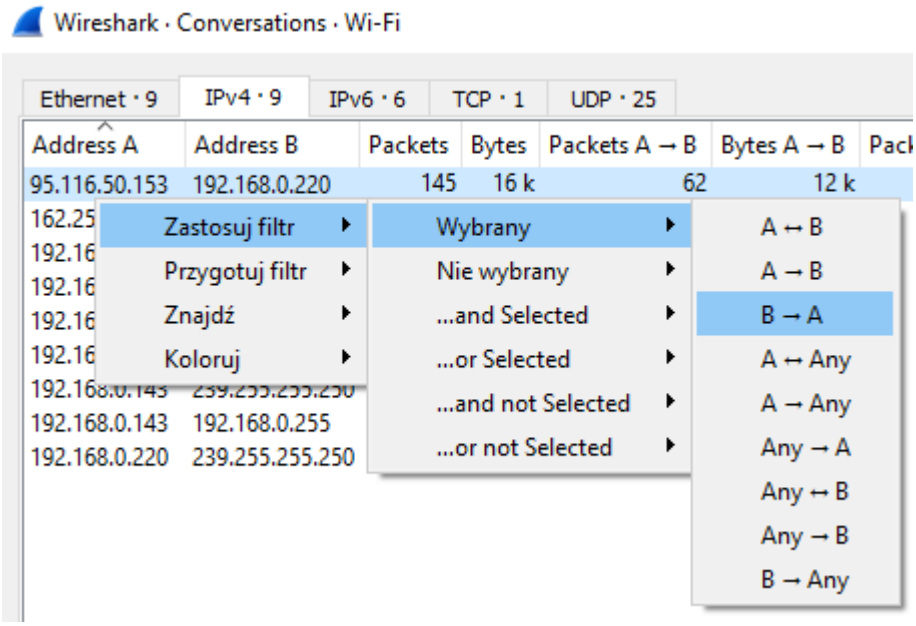
Jeśli potrzebujemy dodać filtr używając tego menu, klikamy na interesujący nas rekord z menu prawym przyciskiem myszy i wybieramy odpowiednią opcję:

Przykładowe zastosowanie Wireshark - przechwytywanie hasła z protokołu Telnet.

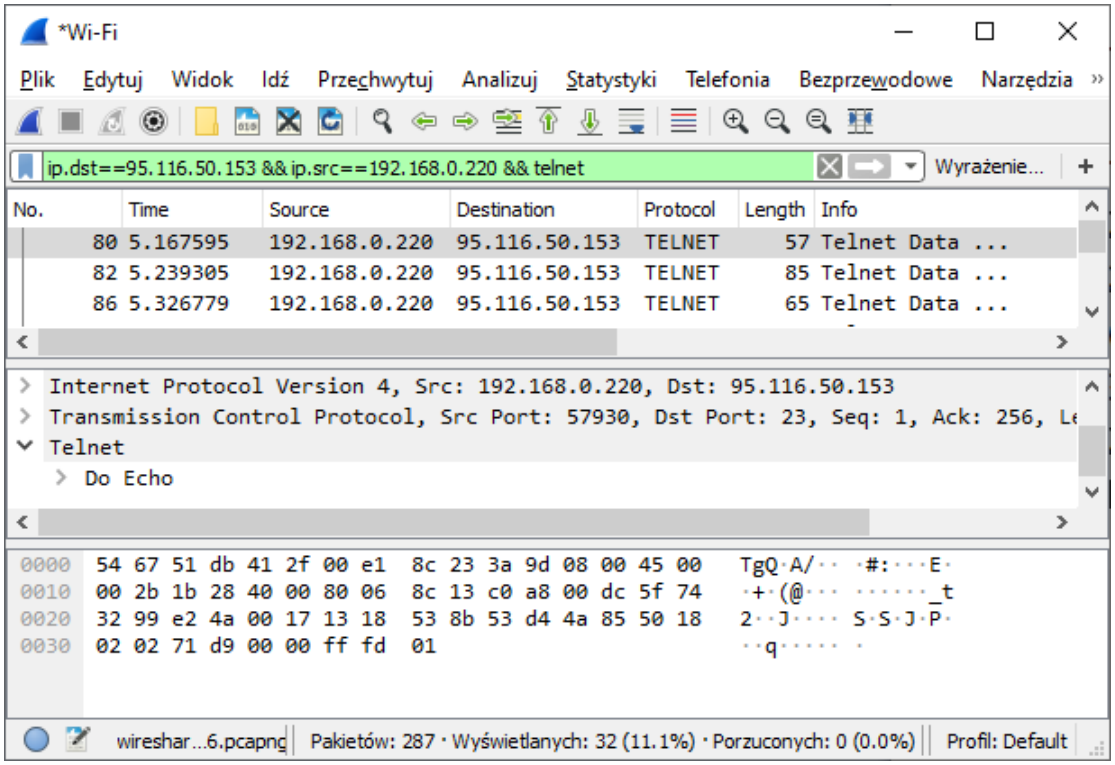
Do eksperymentu potrzebujemy:
- serwer używający usługi Telnet (np. BBS)
- komputer podłączony do Internetu
- klient Telnet (polecam NetRunner)
- Wireshark

1. Rejestrujemy się na danym serwerze (użyłem konta Zsltest z hasłem zaq1@WSX).
2. Włączamy przechwytywanie, po czym następuje login i wylogowanie użytkownika.
3. Analizujemy przechwytywane pakiety.

Zastosowałem filtr konwersacyjny B do A, gdyż ja wysyłam hasło przy logowaniu do serwera:



Dodałem "&& telnet" aby wyfiltrować pakiety tylko te, które mnie interesują:



Szukam pakietów z danymi, które mogą być loginem (znajdują się bezpośrednio po podaniu opcji sesji)...

Telnet Data: Z, Telnet Data: s, Telnet Data: l, Telnet Data: t, Telnet Data: e,
Telnet Data: s, Telnet Data: t;
Telnet Data: \r (nowa linia kończy login);

Telnet Data: z, Telnet Data: a, Telnet Data: q, Telnet Data: 1, Telnet Data: @,
Telnet Data: W, Telnet Data: S, Telnet Data: X;
Telnet Data: \r (nowa linia kończy hasło);

Przygotował: Grzegorz Piekarski
Klasa 3b (2019/2020)