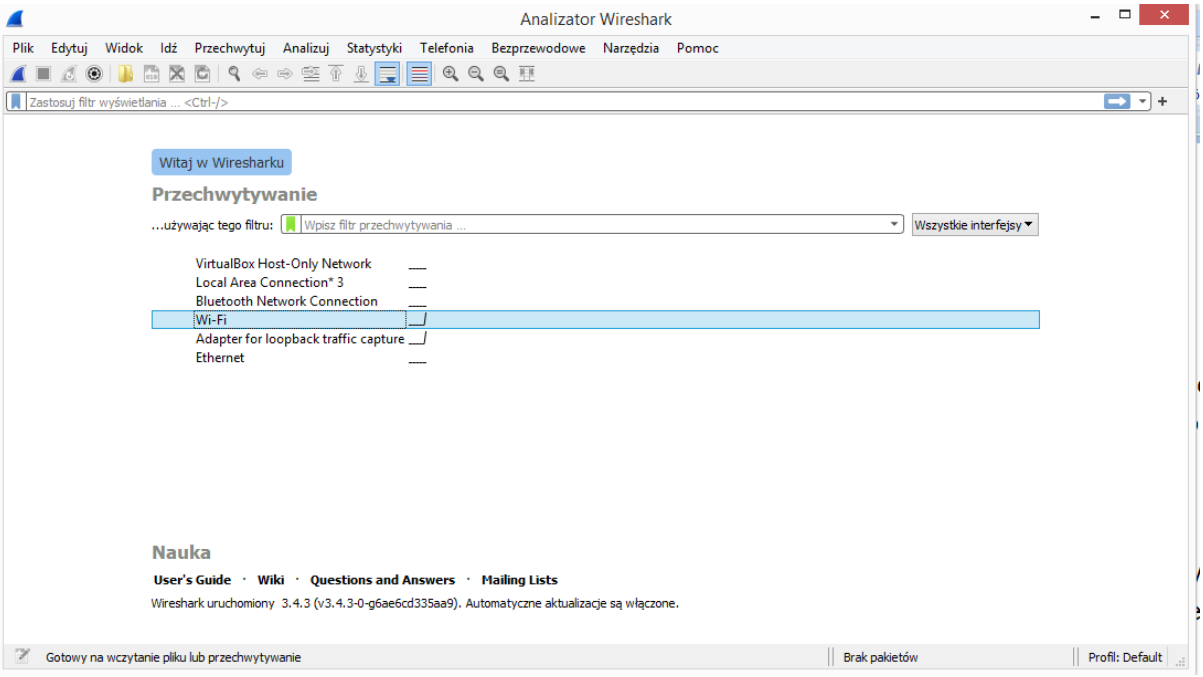
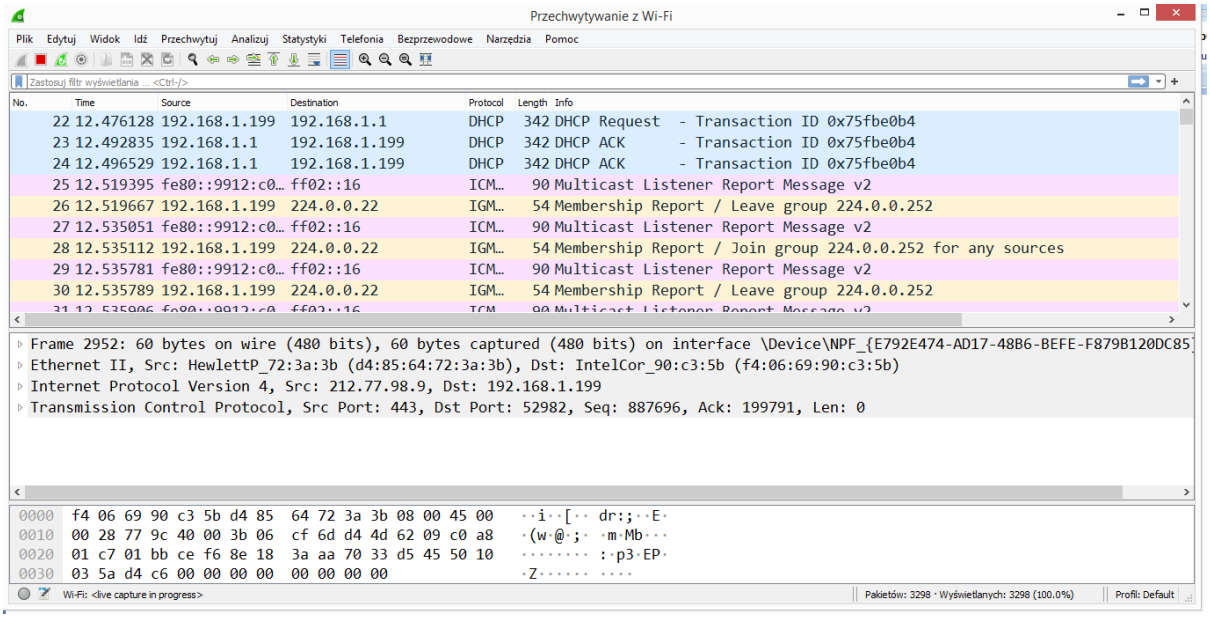
Wireshark

Network Sniffer (ang. program "węszący" sieć) jest to program lub sprzęt komputerowy służący do przechwytywania i zapisywania ruchu sieciowego. Pozwala szczegółowo zapoznać się z zawartością przesyłanych pakietów poprzez ich dekodowanie. Wykorzystywany jest głównie do diagnostyki niezawodności i wydajności sieci. Jednym z najpopularniejszych rozwiązań tego typu jest program Wireshark, rozwijany od 1998 roku na zasadach licencji GNU GPL.

Wireshark umożliwia przechwytywanie pakietów docierających do karty sieciowej. Obsługuje wiele różnych protokołów sieciowych, można również ustawić odpowiednie filtry, które będą wybierać tylko takie pakiety, które pasują do ustalonego wzorca.



Okno startowe programu Wireshark, w pierwszym kroku wybieramy interfejs sieciowy, na którym będziemy nasłuchiwać danych. Można również wybrać więcej niż jeden interfejs sieciowy do monitorowania.

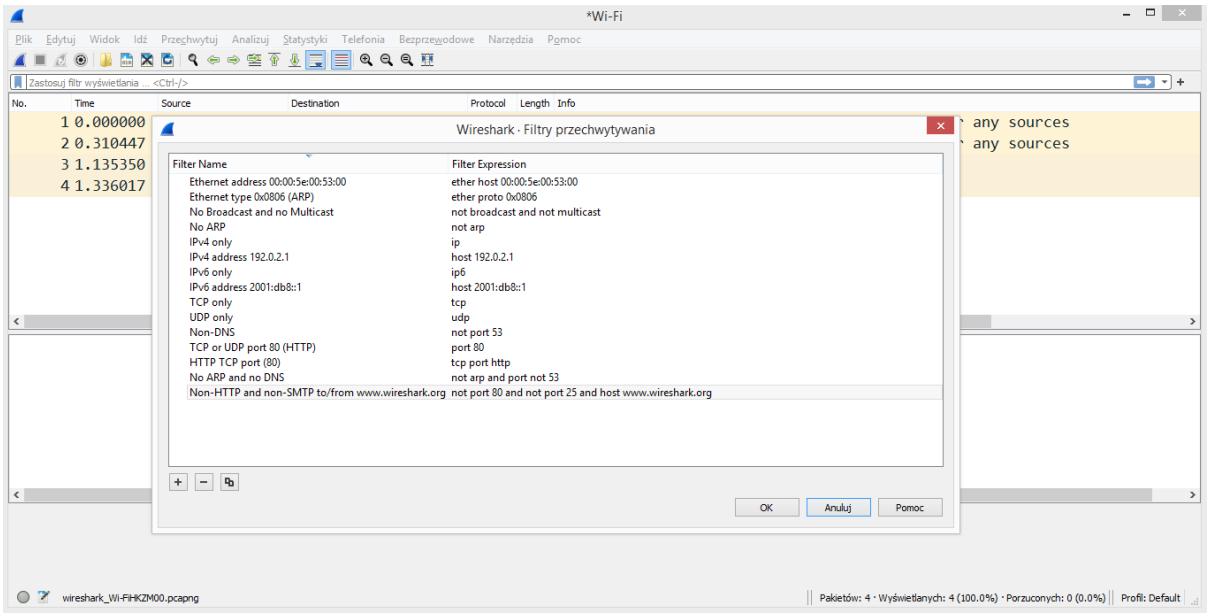


Po włączeniu przechwytywania pakietów, widzimy w kolejnych oknach przechwycone dane.

W górnym oknie znajduje się lista przechwyconych pakietów, w środkowym oknie znajdują się szczegółowe dane wybranego pakietu, w dolnym oknie znajdują się dane z wybranej grupy danych w ramach wybranego pakietu.

Filtry

Ze względu na dużą ilość przechwytywanych pakietów przydatnym narzędziem mogą być filtry. W programie Wireshark istnieją dwa rodzaje filtrów: Capture Filters (filtry przechwytywania) oraz Display Filters (filtry wyświetlania). CaptureFilter służy do definiowania jakie pakiety będą przechwytywane przez program, natomiast Display Filters służą do filtrowania przechwyconych pakietów.



Wygląd okien funkcji filtrowania

Przykładowe filtry

Filtr wyświetlania	Znaczenie
dns	pakiety zawierające protokół DNS
dns.qry.name == www.example.com	pakiety DNS zawierające zapytanie o domenę www.example.com
ip.dst == 1.2.3.4 and tcp	pakiety z adresem odbiorcy 1.2.3.4 zawierających protokół TCP
ip.dst == 1.2.3.4 and http.request.method == GET	pakiety z adresem odbiorcy 1.2.3.4 zawierających żądanie HTTP GET
ip.dst = 1.2.3.4 and icmp.type == 8	pakiety zawierające wiadomość ICMP ECHO Request z adresem odbiorcy 1.2.3.4
ip.src == 1.2.3.4 and icmp.type == 0	pakiety zawierające wiadomość ICMP Echo Reply z adresem nadawcy 1.2.3.4
ftp or ftp-data	pakiety związanych z transmisją opartą o protokół FTP (**`ftp`** to połączenie kontrolne, **`ftp-data`** to transmisja danych)
ftp.request.command == USER	pakiety protokołu FTP z komendą wysyłającą nazwę użytkownika
ftp.request.command == PASS	pakiety protokołu FTP z komendą wysyłającą hasło użytkownika
ftp.request.command == PWD	pakiety protokołu FTP z komendą zwracającą aktualny katalog po stronie serwera
ftp.request.command == MLSD	pakiety protokołu FTP z komendą zwracającą zawartość aktualnego katalogu po stronie serwera

Więcej informacji o filtrach można znaleźć pod adresem:

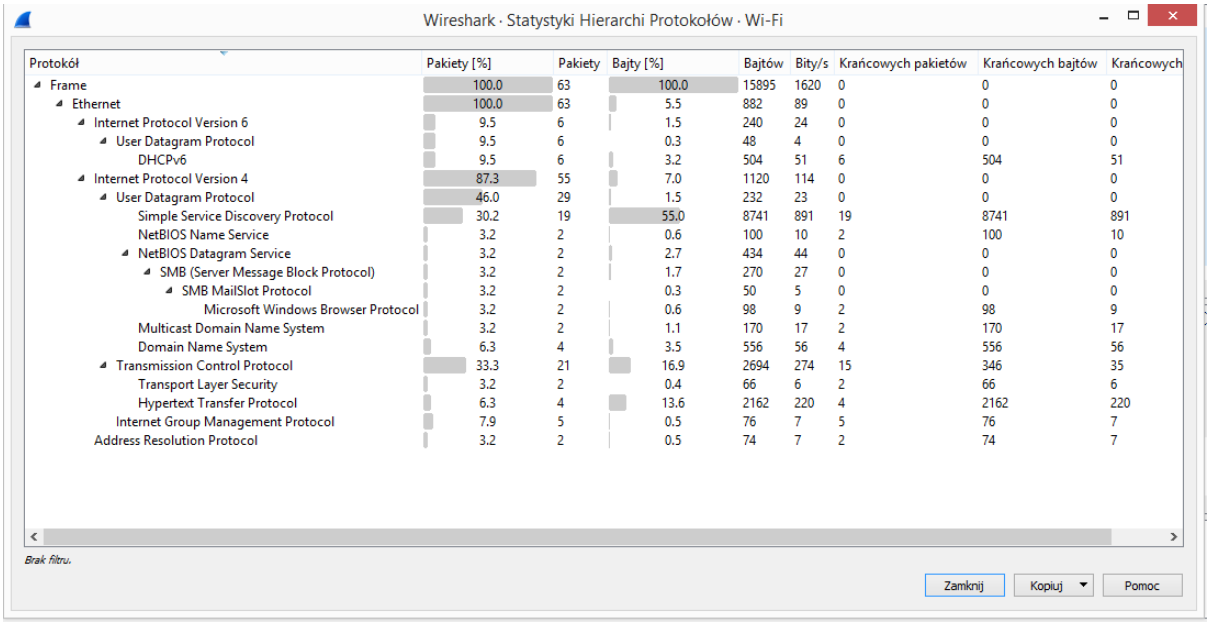
https://wiki.wireshark.org/DisplayFilters
https://wiki.wireshark.org/CaptureFilters#Capture_filter_is_not_a_display_filter

Statystyki

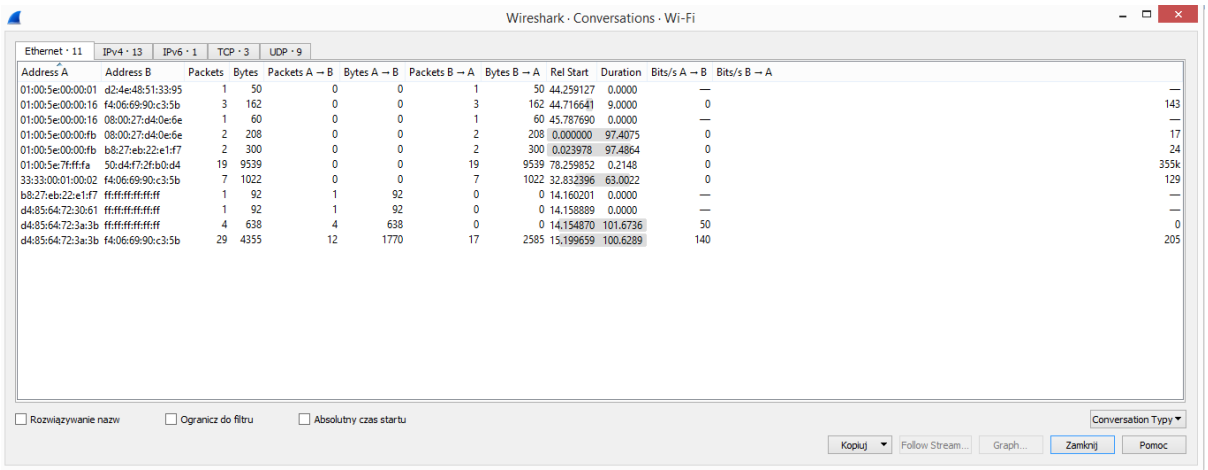
Program Wireshark umożliwia przeprowadzenie analizy statystycznej przechwyconego ruchu. Aby wyświetlić raport należy wybrać rodzaj analizy z menu Statystyki.

Przykładowe analizy to:

Statystyki -> Hierarchia Protokołów: przedstawia procentowy udział protokołów biorących udział w przechwyconym ruchu sieciowym



Statystyki -> Konwersacje: przedstawia ilość danych/pakietów wymienionych między poszczególnymi hostami. Dane są posortowane według protokołów.



Statystyki -> I/O Graph: pozwala wizualnie przedstawić częstotliwość transmisji pakietów. Pozwala tworzyć serie danych wykorzystując pole Display Filters


Wireshark · I/O Graphs · Wi-Fi
Wireshark I/O Graphs: Wi-Fi
10000
7500
5000
2500
Packets/1 min
22:45:00
17.03.21
22:50:00
17.03.21
22:55:00
17.03.21
23:00:00
17.03.21
Czas (s)
Przesuń kursor nad wykresem by zobaczyć szczegóły.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All Packets
Line
Packets
None
TCP Errors
tcp.analysis.flags
Bar
Packets
None
Mysz
przesuwanie
powiększanie
Interwał
1 min
Czas dnia
Skala logarytmiczna
Reset
Save As...
Kopiuj
Kopiuj z
Zamknij
Pomoc