

# PRAKTYCZNA ANALIZA PAKIETÓW

WYKORZYSTANIE NARZĘDZIA WIRESHARK  
DO ROZWIĄZYWANIA PROBLEMÓW Z SIECIĄ

CHRIS SANDERS



Helion



Tytuł oryginału: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-5011-8

Original edition copyright © 2011 by Chris Sanders.  
All rights reserved.

Published by arrangement with No Starch Press, Inc.

Polish edition copyright 2013 by HELION SA.  
All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Wydawnictwo HELION dołożyło wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie bierze jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Wydawnictwo HELION nie ponosi również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo HELION  
ul. Kościuszki 1c, 44-100 GLIWICE  
tel. 32 231 22 19, 32 230 98 63  
e-mail: [helion@helion.pl](mailto:helion@helion.pl)  
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres  
<http://helion.pl/user/opinie/panpak>  
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

# Spis treści

<b>Podziękowania</b>	<b>13</b>
----------------------	-----------

<b>Wprowadzenie</b>	<b>15</b>
---------------------	-----------

Dlaczego właśnie ta książka? .....	15
Koncepcje i podejście .....	16
Jak korzystać z tej książki? .....	18
Przykładowe pliki .....	18
Fundusz The Rural Technology Fund .....	18
Kontakt ze mną .....	19

## I

<b>Podstawy działania sieci i analizy pakietów</b>	<b>21</b>
----------------------------------------------------	-----------

Analiza pakietów i sniffery pakietów .....	22
Ocena aplikacji typu sniffer pakietów .....	22
Jak działa sniffer pakietów? .....	23
W jaki sposób komunikują się komputery? .....	24
Protokoły .....	24
Siedem warstw modelu OSI .....	25
Hermetyzacja danych .....	29
Sprzęt sieciowy .....	31
Klasyfikacje ruchu sieciowego .....	35
Ruch typu broadcast .....	36
Ruch typu multicast .....	37
Ruch typu unicast .....	37
Podsumowanie .....	38

## 2

<b>Dobranie się do sieci</b>	<b>39</b>
------------------------------	-----------

Tryb mieszany .....	40
Przechwytywanie pakietów z koncentratorów .....	41
Przechwytywanie pakietów w środowisku sieci opartej na przełączniku sieciowym .....	43
Kopiowanie ruchu na wskazany port .....	43
Technika hubbing out .....	45

Użycie rozgałęźnika .....	46
Zatrucie bufora ARP .....	49
Przechwytywanie pakietów w środowisku sieci opartej na routerze .....	54
Praktyczne wskazówki dotyczące umieszczania sniffera pakietów .....	55

### 3

<b>Wprowadzenie do narzędzia Wireshark</b> .....	<b>59</b>
Krótką historią narzędzia Wireshark .....	59
Zalety narzędzia Wireshark .....	60
Instalowanie narzędzia Wireshark .....	61
Instalowanie Wireshark w systemie Windows .....	62
Instalowanie narzędzia Wireshark w systemie Linux .....	63
Instalowanie narzędzia Wireshark w systemie Mac OS X .....	64
Podstawy używania narzędzia Wireshark .....	65
Twoje pierwsze przechwycone pakiety .....	65
Okno główne narzędzia Wireshark .....	67
Preferencje narzędzia Wireshark .....	68
Kolorowanie pakietów .....	69

### 4

<b>Praca z przechwyconymi pakietami</b> .....	<b>73</b>
Praca z plikami zawierającymi przechwycone dane .....	73
Zapis i eksport plików zawierających przechwycone dane .....	74
Łączenie plików zawierających przechwycone dane .....	75
Praca z pakietami .....	76
Wyszukiwanie pakietów .....	76
Oznaczanie pakietów .....	77
Wydruk pakietów .....	77
Konfiguracja formatu wyświetlania czasu i odniesień .....	78
Format wyświetlania czasu .....	78
Odniesienie czasu do pakietu .....	79
Konfiguracja opcji przechwytywania danych .....	80
Sekcja Capture .....	81
Sekcja Capture File(s) .....	81
Sekcja Stop Capture .....	82
Sekcja Display Options .....	83
Sekcja Name Resolution .....	83
Używanie filtrów .....	83
Pliki zawierające przechwycone dane .....	84
Filtry wyświetlania .....	90
Zapis filtrów .....	93

## 5

### **Zaawansowane funkcje narzędzia Wireshark 97**

Konwersacje i punkty końcowe sieci .....	97
Przeglądanie punktów końcowych .....	98
Przeglądanie konwersacji sieciowych .....	99
Rozwiązywanie problemów za pomocą okien Endpoints i Conversations .....	100
Okno Protocol Hierarchy Statistics .....	102
Określanie nazw .....	103
Włączenie funkcji określania nazw .....	103
Potencjalne wady określania nazw .....	104
Szczegółowa analiza protokołu .....	104
Zmiana dekodera .....	105
Wyświetlanie kodu źródłowego dekodera .....	107
Funkcja Follow TCP Stream .....	108
Wielkość pakietu .....	109
Grafika .....	110
Wykres operacji wejścia-wyjścia .....	110
Wykres czasu podróży .....	112
Wykres przepływu danych .....	113
Informacje zaawansowane .....	114

## 6

### **Najczęściej używane protokoły niższych warstw 117**

Protokół ARP .....	118
Nagłówek pakietu ARP .....	119
Pakiet 1.: żądanie ARP .....	120
Pakiet 2.: odpowiedź ARP .....	121
Bezpłatny pakiet ARP .....	122
Protokół IP .....	123
Adres IP .....	123
Nagłówek IPv4 .....	125
Wartość Time to Live .....	126
Fragmentacja IP .....	128
Protokół TCP .....	130
Nagłówek TCP .....	131
Porty TCP .....	132
Trzyetapowy proces negocjacji TCP .....	135
Zakończenie komunikacji TCP .....	137
Zerowanie TCP .....	138
Protokół UDP .....	139
Nagłówek UDP .....	140
Protokół ICMP .....	141
Nagłówek ICMP .....	141
Wiadomości i typy ICMP .....	142
Żądania echo i odpowiedzi na nie .....	142
Polecenie traceroute .....	145

## 7

### **Najczęściej używane protokoły wyższych warstw** **149**

Protokół DHCP .....	149
Struktura pakietu DHCP .....	150
Proces odnowy DHCP .....	150
Proces odnowy dzierżawy DHCP .....	156
Opcje DHCP i typy wiadomości .....	156
Protokół DNS .....	156
Struktura pakietu DNS .....	157
Proste zapytanie DNS .....	158
Typy zapytań DNS .....	159
Rekurencja DNS .....	160
Transfer strefy DNS .....	164
Protokół HTTP .....	166
Przeglądanie zasobów za pomocą HTTP .....	166
Przekazywanie danych za pomocą HTTP .....	168
Podsumowanie .....	170

## 8

### **Najczęściej spotykane sytuacje** **171**

Serwisy społecznościowe na poziomie pakietów .....	172
Przechwycenie ruchu sieciowego serwisu Twitter .....	172
Przechwycenie ruchu sieciowego serwisu Facebook .....	176
Porównanie metod stosowanych przez serwisy Twitter i Facebook .....	178
Przechwycenie ruchu sieciowego z ESPN.com .....	179
Użycie okna Conversations .....	179
Używanie okna Protocol Hierarchy Statistics .....	179
Przeglądanie ruchu DNS .....	181
Wyświetlanie żądań HTTP .....	182
Rzeczywiste problemy .....	183
Brak dostępu do internetu: problem związany z konfiguracją .....	183
Brak dostępu do internetu: niechciane przekierowanie .....	187
Brak dostępu do internetu: problemy związane z przekazywaniem danych .....	190
Nieprawidłowo działająca drukarka .....	193
Uwięzieni w oddziale .....	196
Błąd programisty .....	199
Podsumowanie .....	204

## 9

### **Zmagania z wolno działającą siecią** **205**

Funkcje usuwania błędów protokołu TCP .....	206
Ponowna transmisja pakietu TCP .....	206
Duplikaty potwierdzeń TCP i szybka retransmisja .....	209

Kontrola przepływu danych TCP .....	213
Dostosowanie wielkości okna .....	215
Wstrzymanie przepływu danych i powiadomienie o zerowej wielkości okna odbiorcy .....	216
Mechanizm przesuwającego się okna TCP w praktyce .....	217
Wnioski płynące z usuwania błędów protokołu TCP i kontroli przepływu danych .....	220
Lokalizacja źródła opóźnień .....	221
Normalna komunikacja .....	221
Wolna komunikacja — opóźnienie z winy sieci .....	222
Wolna komunikacja — opóźnienie po stronie klienta .....	223
Wolna komunikacja — opóźnienie po stronie serwera .....	224
Struktury pozwalające na wyszukiwanie opóźnień .....	224
Punkt odniesienia dla sieci .....	225
Punkt odniesienia dla miejsca .....	226
Punkt odniesienia dla komputera .....	227
Punkt odniesienia dla aplikacji .....	228
Informacje dodatkowe dotyczące punktów odniesienia .....	229
Podsumowanie .....	229

## **I 0**

<b>Analiza pakietów i zapewnianie bezpieczeństwa</b> .....	<b>231</b>
Rozpoznanie systemu .....	232
Skanowanie TCP SYN .....	232
Wykrywanie systemu operacyjnego .....	237
Włamanie .....	240
Operacja Aurora .....	240
Zatrucie bufora ARP .....	246
Koń trojański umożliwiający zdalny dostęp .....	248
Podsumowanie .....	257

## **I I**

<b>Analiza pakietów w sieci bezprzewodowej</b> .....	<b>259</b>
Względy fizyczne .....	260
Przechwytywanie danych tylko jednego kanału w danej chwili .....	260
Zakłócenia sygnału bezprzewodowego .....	261
Wykrywanie i analizowanie zakłóceń sygnału .....	261
Tryby działania kart sieci bezprzewodowych .....	263
Bezprzewodowe przechwytywanie pakietów w systemie Windows .....	264
Konfiguracja AirPcap .....	264
Przechwytywanie ruchu sieciowego za pomocą urządzenia AirPcap .....	266
Bezprzewodowe przechwytywanie pakietów w systemie Linux .....	268
Struktura pakietu 802.11 .....	269
Dodanie do panelu Packet List kolumn charakterystycznych dla sieci bezprzewodowej .....	271
Filtry przeznaczone dla sieci bezprzewodowej .....	272
Filtrowanie ruchu sieciowego należącego do określonego BSS ID .....	273

Filtrowanie określonych typów pakietów sieci bezprzewodowej .....	273
Odfiltrowanie określonej częstotliwości .....	273
Bezpieczeństwo w sieci bezprzewodowej .....	275
Zakończone powodzeniem uwierzytelnienie WEP .....	275
Nieudane uwierzytelnienie WEP .....	277
Zakończone powodzeniem uwierzytelnienie WPA .....	278
Nieudane uwierzytelnienie WPA .....	279
Podsumowanie .....	281

## **Dodatek.**

<b>Co dalej?</b>	<b>283</b>
Narzędzia analizy pakietów .....	283
tcpdump i Windump .....	284
Cain & Abel .....	284
Scapy .....	284
Netdude .....	284
Colsoft Packet Builder .....	284
CloudShark .....	285
pcapr .....	285
NetworkMiner .....	287
Tcpreplay .....	287
ngrep .....	287
libpcap .....	287
hping .....	287
Domain Dossier .....	288
Perl i Python .....	288
Zasoby dotyczące analizy pakietów .....	288
Witryna domowa narzędzia Wireshark .....	288
Kurs SANS Security Intrusion Detection In-Depth .....	288
Blog Chrisa Sandersa .....	289
Blog Packetstan .....	289
Uniwersytet Wireshark .....	289
IANA .....	289
TCP/IP Illustrated (Addison-Wesley) .....	289
The TCP/IP Guide (No Starch Press) .....	289

## **Skorowidz**

**291**



# 4

## Praca z przechwyconymi pakietami



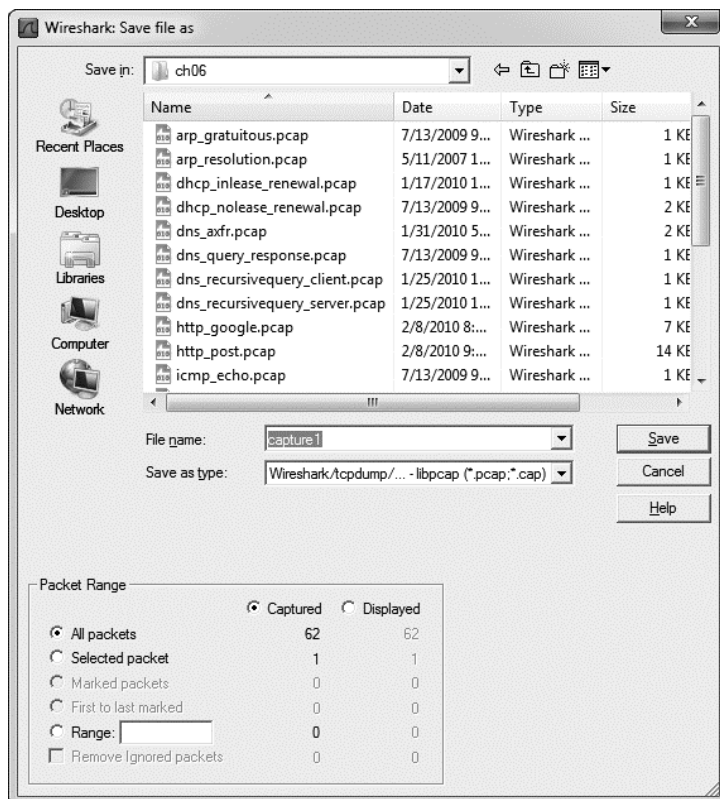
PO KRÓTKIM WPROWADZENIU DO NARZĘDZIA WIRESHARK PRZEDSTAWIONYM W ROZDZIALE 3. JESTEŚ GOTOWY DO ROZPOCZĘCIA PRZECHWYTYWANIA I ANALIZY PAKIETÓW. W TYM ROZDZIALE DOWIESZ SIĘ, JAK PRACOWAĆ Z PLIKAMI ZAWIERAJĄCYMI PRZECHWYCONE DANE, Z PRZECHWYCONYMI PAKIETAMI ORAZ Z FORMATAMI WYŚWIETLANIA CZASU. OMÓWIONE ZOSTANĄ TAKŻE BARDZIEJ ZAAWANSOWANE OPCJE DOTYCZĄCE PRZECHWYTYWANIA PAKIETÓW, A PONADTO ZAGŁĘBIMY SIĘ W ŚWIAT FILTRÓW.

### Praca z plikami zawierającymi przechwycone dane

Podczas przeprowadzania analizy pakietu przekonasz się, że znaczna jej część następuje już po przechwyceniu danych. Najczęściej w różnym czasie przeprowadzasz kilka operacji przechwytywania i zapisywania danych, a następnie analizujesz jednocześnie wszystkie zebrane w ten sposób dane. Narzędzie Wireshark umożliwia zapisywanie plików z przechwyconymi danymi, które będziesz mógł później przeanalizować. Oczywiście masz możliwość łączenia ze sobą wielu takich plików.

## Zapis i eksport plików zawierających przechwycone dane

Aby zapisać przechwycony pakiet, wybierz opcję menu *File/Save As*. Na ekranie powinno wyświetlić się okno dialogowe *Save As* (zob. rysunek 4.1). W oknie tym możesz podać katalog, w którym zostanie zapisany plik, oraz określić format pliku. Jeżeli nie podasz formatu pliku, narzędzie Wireshark użyje domyślnego formatu pliku dla przechwyconych danych — *.pcap*.



Rysunek 4.1. Za pomocą okna dialogowego *Save As* możesz zapisywać przechwycone pakiety

Jedną z najmocniejszych stron okna dialogowego *Save As* jest możliwość zapisu określonego zakresu pakietu. To doskonały sposób na zmniejszenie przerośniętych plików zawierających przechwycone dane pakietu. Możesz więc zapisywać pakiety pochodzące jedynie z podanego zakresu, pakiety oznaczone lub pakiety widoczne po zastosowaniu określonego filtru wyświetlania. (Pakiety oznaczone i filtry zostaną omówione w dalszej części rozdziału).

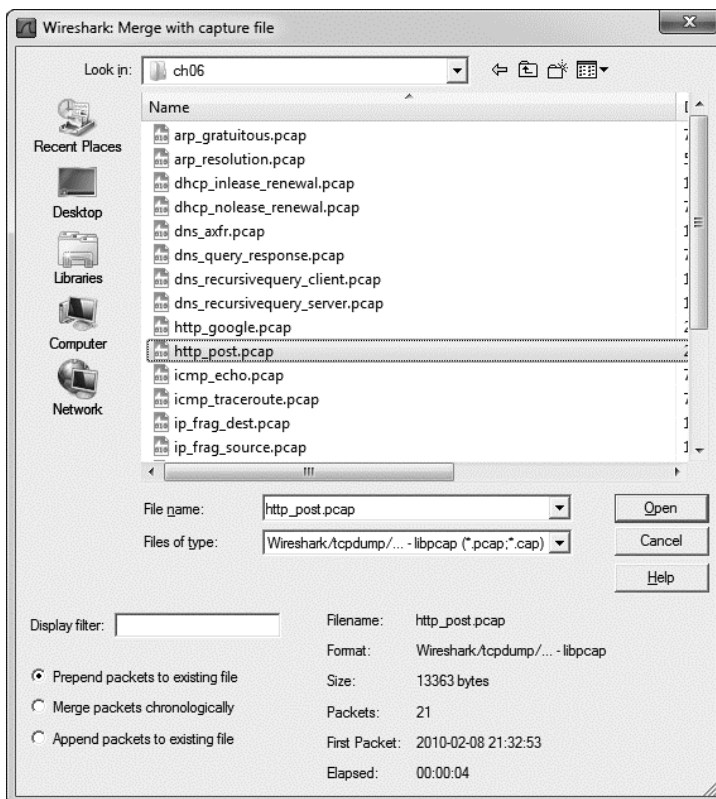
Dane przechwycone przez narzędzie Wireshark możesz eksportować do wielu różnych formatów w celu wyświetlania danych w innych mediach lub przeanalizowania zebranych danych w innych narzędziach. Dostępne formaty to między innymi: zwykły tekst, PostScript, CSV (ang. *Comma Separated Values* — wartości

rozdzielone przecinkami) oraz XML. Aby wyeksportować przechwycone dane pakietu, wybierz opcję menu *File/Export*, a następnie wskaż format pliku, w którym mają zostać zapisane dane. Na ekranie wyświetli się okno dialogowe *Save As* zawierające opcje związane z wybranym formatem.

## **Łączenie plików zawierających przechwycone dane**

Pewne rodzaje analizy wymagają połączenia ze sobą wielu plików zawierających przechwycone dane. Jest to praktyka często stosowana podczas porównywania dwóch strumieni danych lub łączenia strumieni tego samego ruchu sieciowego, które zostały przechwycone oddzielnie.

Aby połączyć ze sobą pliki zawierające przechwycone dane, otwórz jeden z nich, a następnie wybierz opcję menu *File/Merge*. Na ekranie wyświetli się okno dialogowe zatytułowane *Merge with capture file* (zob. rysunek 4.2). W oknie tym wskaż plik, który ma zostać połączony z już otwartym plikiem, a następnie wybierz metodę połączenia plików. Plik wybrany w oknie dialogowym możesz umieścić przed już otworzonym plikiem, dołączyć go na końcu bądź połączyć oba pliki chronologicznie na podstawie ich znaczników czasu.



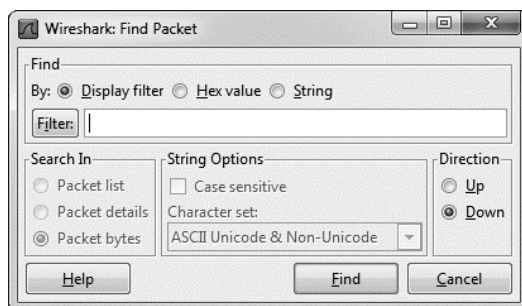
Rysunek 4.2. Okno dialogowe *Merge with capture file* pozwala łączyć dwa pliki zawierające przechwycone dane

# Praca z pakietami

Może się zdarzyć sytuacja, w której wykorzystywana będzie ogromna liczba pakietów. W przypadku wzrostu liczby pakietów do rzędu tysięcy lub nawet milionów musisz mieć możliwość efektywnego poruszania się pomiędzy nimi. Narzędzie Wireshark umożliwia wyszukiwanie i oznaczanie pakietów spełniających określone kryteria. Pakiety można również wydrukować.

## Wyszukiwanie pakietów

Aby wyszukać pakiety spełniające określone kryteria, musisz przejść do okna dialogowego *Find Packet* (zob. rysunek 4.3) poprzez naciśnięcie klawiszy *Ctrl+F*.



Rysunek 4.3. Wyszukiwanie pakietów w narzędziu Wireshark na podstawie określonych kryteriów

Pokazane na rysunku 4.3 okno dialogowe zawiera trzy następujące opcje pozwalające na wyszukiwanie pakietów:

- **Display filter.** W tej opcji możesz podać filtr oparty na wyrażeniu. Dzięki temu filtrowi zostaną wyszukane jedynie pakiety spełniające zdefiniowane tutaj wyrażenie.
- **Hex value.** Ta opcja powoduje wyszukanie pakietów zawierających podaną wartość szesnastkową (bajty powinny być rozdzielone dwukropkami).
- **String.** Ta opcja powoduje wyszukanie pakietów zawierających podany ciąg tekstowy.

Powyższe rodzaje wyszukiwania przedstawiono w tabeli 4.1.

Inne opcje pozwalają na wybór używanego systemu kodowania znaków, określenie kierunku wyszukiwania oraz wskazanie okna, w którym ma zostać przeprowadzona operacja wyszukiwania. Wyszukiwanie z użyciem ciągu tekstowego można rozbudować poprzez podanie używanego systemu kodowania, określenie, czy ma być rozróżniana wielkość znaków, oraz wskazanie panelu, w którym będzie przeprowadzona operacja wyszukiwania.

Po wybraniu odpowiednich opcji w polu tekstowym należy wprowadzić kryteria wyszukiwania, a następnie nacisnąć przycisk *Find* w celu znalezienia pierw-

Tabela 4.1. Dostępne rodzaje operacji wyszukiwania pakietów

Rodzaj wyszukiwania	Przykłady
filtr	not ip ip.addr==192.168.0.1 arp
wartość szesnastkowa	00:ff ff:ff 00:ab:b1:f0
ciąg tekstowy	StacjaRobocza1 UżytkownikB domena

szego pakietu spełniającego zdefiniowane kryteria. Aby znaleźć kolejny pakiet dopasowany do kryteriów, trzeba nacisnąć klawisze *Ctrl+N*, natomiast przejście do poprzedniego znalezionej pakietu następuje po naciśnięciu klawiszy *Ctrl+B*.

## Oznaczanie pakietów

Po znalezieniu pakietów spełniających zdefiniowane kryteria można je oznakować. Przykładowo: pakiety możesz oznakować, aby mieć możliwość ich oddzielnego zapisania lub szybkiego odszukania na podstawie koloru. Oznaczone pakiety wyróżniają się białym tekstem na czarnym tle, jak pokazano na rysunku 4.4. (Podczas zapisywania przechwyconych pakietów możesz zdecydować o zachowaniu jedynie oznaczonych pakietów).

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.16.0.8	157.16.224.25	TCP	3426 > 80 [SYN, Seq=1745901259 Win=8192 Len=0 MSS=1460 WS=2
2	0.024063	157.166.224.25	172.16.0.8	TCP	80 > 3426 [SYN, ACK] Seq=2324576412 Ack=1745901260 Win=5840 Len=0 MSS=1460 WS=7

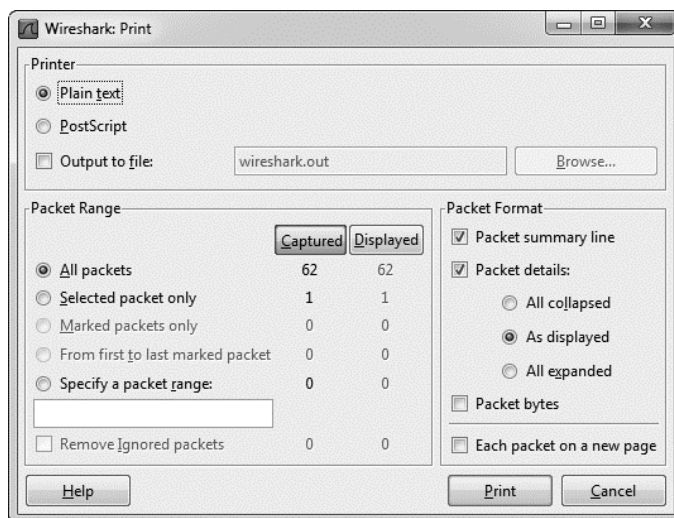
Rysunek 4.4. Oznaczony pakiet jest podświetlony na ekranie. Na rysunku widać, że pakiet pierwszy został oznaczony — ma czarne tło i biały tekst

W celu oznaczenia pakietu kliknij go prawym przyciskiem myszy w panelu *Packet List*, a następnie wybierz opcję *Mark Packet* z rozwijanego menu lub naciśnij klawisze *Ctrl+M*. Natomiast usunięcie zaznaczenia pakietu następuje po ponownym wybraniu wspomnianej opcji lub po ponownym naciśnięciu klawiszy *Ctrl+M*. W przechwyconych danych możesz oznaczyć dowolną liczbę pakietów. Do poruszania się do przodu i do tyłu po oznaczonych pakietach służą klawisze odpowiednio *Shift+Ctrl+N* i *Shift+Ctrl+B*.

## Wydruk pakietów

Wprawdzie większość analizy pakietów przeprowadza się na ekranie komputera, ale zdarzają się sytuacje, gdy trzeba wydrukować przechwycone dane. Sam często drukuję pakiety i umieszczam je na biurku; w ten sposób mogę bardzo szybko sprawdzić ich zawartość podczas przeprowadzania innych analiz. Możliwość zapisu pakietów do pliku w formacie PDF również jest bardzo wygodna, zwłaszcza podczas przygotowywania raportów.

Aby wydrukować przechwycone pakiety, wyświetl okno dialogowe *Print* poprzez wybór opcji menu *File/Print*. Na ekranie pojawi się pokazane na rysunku 4.5 okno dialogowe *Print*.



Rysunek 4.5. Okno dialogowe *Print* umożliwia wydruk wskazanych pakietów

Wskazane dane można wydrukować jako zwykły tekst, PostScript lub do pliku. Podobnie jak w przypadku okna dialogowego *Save As*, także tutaj można wybrać wydruk jedynie określonego zakresu pakietów, pakietów oznaczonych lub wyświetlanych na ekranie jako wynik działania filtru. Ponadto masz możliwość wyboru panelu (jednego z trzech głównych paneli okna Wireshark), z którego będzie wydrukowany pakiet. Po zaznaczeniu wszystkich opcji naciśnij przycisk *Print*.

## Konfiguracja formatu wyświetlania czasu i odniesień

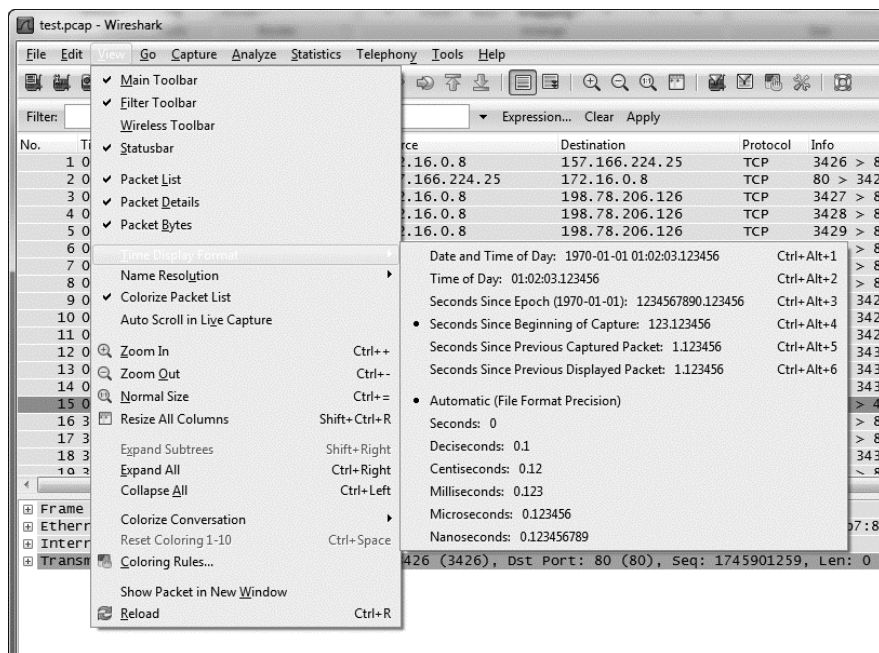
Czas ma istotne znaczenie zwłaszcza podczas przeprowadzania analizy pakietu. Dla wszystkich zdarzeń zachodzących w sieci czas jest ważny, a Twoim zadaniem jest analiza trendów i opóźnień w sieci w niemal każdym pliku zawierającym przechwycone dane. Twórcy narzędzia Wireshark zdają sobie sprawę ze znaczenia czasu, dlatego dostarczyli wiele powiązanych z nim opcji konfiguracyjnych. W tym podrozdziale skoncentrujemy się na formacie wyświetlania czasu oraz na odniesieniach czasu do pakietu.

### **Format wyświetlania czasu**

Każdy pakiet przechwycony przez narzędzie Wireshark ma znacznik czasu, który jest mu przypisany przez system operacyjny. Wireshark ma możliwość wyświetlenia

zarówno bezwzględny znacznik czasu, wskazującego dokładny moment przechwycenia danego pakietu, jak również czasu, który upłynął od ostatniego przechwyconego pakietu, a także od początku i końca operacji przechwytywania.

Opcje związane z wyświetlaniem czasu znajdują się w menu głównym zatytułowanym *View*. Pokazana na rysunku 4.6 grupa *Time Display Format* umożliwia wybór formatu wyświetlania czasu oraz dokładność czasu. Masz możliwość wybrania automatycznego lub ręcznego ustawienia dokładności czasu, na przykład: sekundy, milisekundy, mikrosekundy. Obie opcje będziemy modyfikować w dalszej części książki, więc powinieneś się teraz z nimi zapoznać.



Rysunek 4.6. Dostępnych jest kilka formatów wyświetlania czasu

## Odniesienie czasu do pakietu

Funkcja odniesienia czasu do pakietu pozwala skonfigurować określony pakiet w taki sposób, aby kolejne obliczenia dotyczące czasu były przeprowadzane względem danego pakietu. Ta funkcja jest wyjątkowo użyteczna podczas analizy wielu kolejnych zdarzeń, które są wywoływane gdzieś w środku pliku zawierającego przechwycone dane.

Aby ustawić odniesienie czasu do określonego pakietu, należy w pierwszej kolejności zaznaczyć pakiet w panelu *Packet List*, a następnie wybrać opcję menu *Edit/Set Time Reference*. Usunięcie odniesienia czasu do pakietu następuje po zaznaczeniu pakietu i usunięciu opcji *Edit/Set Time Reference*.

Po włączeniu funkcji odniesienia czasu do określonego pakietu kolumna *Time* w panelu *Packet List* będzie zawierała ciąg tekstowy *\*REF\** (zob. rysunek 4.7).

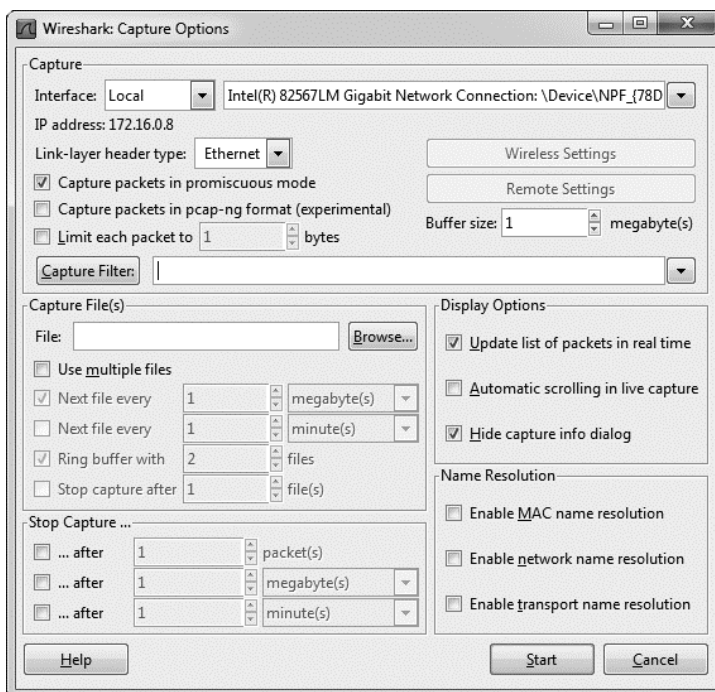
No.	Time	Source	Destination
4	0.118129	172.16.0.8	198.78.206.126
5	*REF*	172.16.0.8	198.78.206.126
6	0.000077	172.16.0.8	198.78.206.126
7	0.000153	172.16.0.8	198.78.206.126

Rysunek 4.7. Pakiet wraz z włączonym odniesieniem czasu względem wskazanego pakietu

Włączenie opcji odniesienia czasu do danego pakietu jest użyteczne tylko wtedy, gdy format wyświetlania czasu przechwyconych danych jest zdefiniowany jako czas wyświetlany względem początku tych danych. Wszelkie inne ustawienia spowodują otrzymanie nieprzewidywalnych wyników oraz utworzenie bardzo mylących znaczników czasu.

## Konfiguracja opcji przechwytywania danych

Wyjątkowo prosty proces przechwytywania danych został przedstawiony w rozdziale 3. W pokazanym na rysunku 4.8 oknie dialogowym *Capture Options* narzędzie Wireshark oferuje znacznie więcej opcji związanych z przechwytywaniem danych. Wyświetlenie tego okna dialogowego następuje po wybraniu opcji *Capture/Interfaces* i kliknięciu przycisku *Options* znajdującego się obok nazwy interfejsu, z którego mają zostać przechwycone pakiety.



Rysunek 4.8. Okno dialogowe *Capture Options*



Okno dialogowe *Capture Options* ma więcej wlotrysków, niż będziesz w stanie wykorzystać, umożliwiających jak największą elastyczność podczas przechwytywania pakietów. Opcje zostały zgrupowane w kilku sekcjach, które teraz omówię.

## Sekcja *Capture*

Rozwijane menu *Interface* w sekcji *Capture* pozwala wybrać konfigurowany interfejs sieciowy. W menu po lewej stronie wybierasz interfejs lokalny bądź zdalny, natomiast menu po prawej stronie pokazuje dostępne interfejsy pozwalające na przechwytywanie danych. Adres IP wybranego interfejsu jest wyświetlany bezpośrednio pod rozwijanym menu.

Trzy pola wyboru umieszczone po lewej stronie sekcji *Capture* służą do włączenia lub wyłączenia trybu mieszanego (domyślnie zawsze jest włączony), przechwytywania pakietów w aktualnie eksperymentalnym formacie pcap-ng oraz do zdefiniowanego w bajtach ograniczenia wielkości każdego przechwyconego pakietu.

Przyciski po prawej stronie sekcji *Capture* pozwalają uzyskać dostęp do ustawień sieci bezprzewodowej lub zdalnej (pod warunkiem, że są dostępne). Poniżej znajduje się opcja konfiguracji wielkości bufora, dostępna jedynie w systemach Microsoft Windows. W tym miejscu możesz określić wielkość przechwyconych danych pakietów, które będą przechowywane w buforze jądra, zanim zostaną zapisane na dysku. (Tej wartości nie powinieneś modyfikować, chyba że zauważysz gubienie dużej liczby pakietów). Opcja *Capture Filter* pozwala zdefiniować filtr przechwytywania danych.

## Sekcja *Capture File(s)*

W sekcji *Capture File(s)* możesz skonfigurować automatyczne przechowywanie przechwyconych pakietów w pliku zamiast najpierw przechwytywania danych, a dopiero później ich zapisywania w pliku. Dostępne tutaj opcje oferują dużą elastyczność w zarządzaniu sposobem zapisu pakietów. Dane mogą być zapisywane w pojedynczym pliku, w zestawie plików, a nawet można użyć bufora wielopierścieniowego (ang. *ring buffer*) do zarządzania liczbą tworzonych plików. Włączenie opcji zapisu danych do pliku (lub plików) wymaga podania pełnej ścieżki dostępu w polu *File*.

Podczas przechwytywania ogromnego ruchu sieciowego lub przeprowadzania długotrwałej operacji przechwytywania danych użyteczne jest utworzenie zestawu plików. Zestaw ten to grupa wielu plików, każdy z nich zawiera dane spełniające określony warunek. Aby wykorzystać zestaw plików, należy użyć opcji *Use Multiple Files*.

Przy zarządzaniu zestawem plików narzędzie Wireshark korzysta z różnych wyzwalaczy opartych na wielkości pliku lub na warunku dotyczącym czasu. Włączenie tych opcji wymaga zaznaczenia pola wyboru znajdującego się obok opcji *Next File Every* (to górne dotyczy wyzwalaczy opartych na wielkości pliku, natomiast dolne — opartych na czasie), a także podania wartości oraz jednostki

powodującej aktywację wyzwalacza. Przykładowo: możesz zdefiniować wyzwalacz tworzący nowy plik po przechwyceniu każdego 1 MB danych lub po upływie minuty przechwytywania danych (zob. rysunek 4.9).

Name	Date modified
Capture_00001_20091115155100	11/15/2011 3:51 PM
Capture_00002_20091115155200	11/15/2011 3:52 PM
Capture_00003_20091115155300	11/15/2011 3:53 PM
Capture_00004_20091115155400	11/15/2011 3:54 PM
Capture_00005_20091115155500	11/15/2011 3:56 PM
Capture_00006_20091115155600	11/15/2011 3:56 PM
Capture_00007_20091115155700	11/15/2011 3:57 PM
Capture_00008_20091115155800	11/15/2011 3:58 PM
Capture_00009_20091115155900	11/15/2011 3:59 PM
Capture_00010_20091115160000	11/15/2011 4:00 PM

Rysunek 4.9. Zestaw plików utworzonych przez narzędzie Wireshark w odstępie jednej minuty

Wymienione opcje można ze sobą łączyć. Przykładowo: po zaznaczeniu obu wyzwalaczy nowy plik zostanie utworzony po przechwyceniu 1 MB danych *lub* po upływie jednej minuty — w zależności od tego, co nastąpi wcześniej.

Opcja *Ring Buffer Width* pozwala na użycie bufora wielopierścieniowego podczas tworzenia zestawu plików. Ta opcja jest wykorzystywana przez narzędzie Wireshark do zastosowania metody FIFO (ang. *First In, First Out* — pierwszy na wejściu, pierwszy na wyjściu) podczas zapisu wielu plików. Pojęcie *bufora wielopierścieniowego* ma wiele znaczeń w informatyce. W narzędziu Wireshark oznacza zestaw plików, gdzie po zapisaniu ostatniego pliku rozpocznie się nadpisywanie pierwszego, kiedy pojawią się kolejne dane konieczne do zachowania. Możesz zaznaczyć tę opcję i zdefiniować maksymalną liczbę plików używanych przez bufor wielopierścieniowy. Przykładowo: możesz zdecydować się na użycie zestawu plików do zapisu przechwytywanych danych i określić tworzenie nowego pliku co godzinę, a maksymalną liczbę plików ustalić na 6. W takim przypadku po utworzeniu ostatniego, szóstego pliku bufor wielopierścieniowy rozpocznie nadpisywanie pierwszego pliku, zamiast utworzyć siódmy. W ten sposób na dysku twardym będzie się znajdowało maksymalnie sześć plików zawierających przechwycone dane (w tym przypadku z sześciu ostatnich godzin) i nadal będzie zachowana możliwość zapisu nowych danych.

Opcja *Stop Capture After* powoduje zatrzymanie przechwytywania danych po utworzeniu wcześniej zdefiniowanej liczby plików.

## Sekcja Stop Capture

Sekcja *Stop Capture* pozwala zatrzymać trwającą operację przechwytywania danych po wystąpieniu określonego wyzwalacza. Podobnie jak w przypadku zestawu plików, także tutaj wyzwalacz może opierać się na wielkości pliku, odstępach czasu, jak również na liczbie pakietów. Te opcje możesz wykorzystywać w połączeniu z omówionymi wcześniej opcjami dotyczącymi zestawu plików.

## Sekcja *Display Options*

Sekcja *Display Options* określa sposób wyświetlania pakietów po ich przechwyceniu. Działanie opcji zatytułowanej *Update List of Packets in Real Time* (uaktualniaj listę pakietów w czasie rzeczywistym) jest oczywiste; ponadto może być ona połączona z opcją *Automatic Scrolling in Live Capture* (automatyczne przewijanie w panelu *Live Capture*). Po włączeniu obu opcji na ekranie wyświetlą się wszystkie przechwycone pakiety, przy czym przechwytywane pakiety będą wyświetlane natychmiast.

**OSTRZEŻENIE** *Połączenie opcji Update List of Packets in Real Time i Automatic Scrolling in Live Capture może spowodować znaczne obciążenie procesora podczas przechwytywania dużych ilości danych. Jeżeli nie masz szczególnego powodu do wyświetlania pakietów w czasie rzeczywistym, najlepiej wyłącz obie opcje.*

Opcja *Hide Capture Info Dialog* wyświetla małe okno pokazujące liczbę oraz wartość procentową pakietów przechwyconych dla danego protokołu.

## Sekcja *Name Resolution*

Opcje w tej sekcji umożliwiają włączenie automatycznego określania nazw MAC (warstwa 2.), sieci (warstwa 3.) i transportu (warstwa 4.) dla przechwytywanych danych. Szczegółowe omówienie określania nazw w narzędziu Wireshark oraz wad tego procesu zostanie przedstawione w rozdziale 5.

# Używanie filtrów

Filtry pozwalają dokładnie wskazać dane, które chcesz przeanalizować. Ujmując rzecz najprościej: filtr to wyrażenie definiujące kryteria dołączania pakietów do przechwyconych danych lub usuwania pakietów z tych danych. Jeżeli dane zawierają nieinteresujące Cię pakiety, możesz utworzyć odpowiedni filtr powodujący pozbycie się tych pakietów. Jeśli natomiast chcesz otrzymywać wyłącznie określone pakiety, wystarczy utworzyć filtr pokazujący jedynie interesujące Cię pakiety.

Narzędzie Wireshark oferuje dwa podstawowe rodzaje filtrów:

- Filtr przechwytywania zostaje zdefiniowany na początku operacji przechwytywania danych i zawiera tylko te pakiety, które wskazano do dołączenia w danym wyrażeniu.
- Filtr wyświetlania zostanie zastosowany względem istniejącego zestawu przechwyconych pakietów w celu ukrycia niepożądanych lub wyświetlenia interesujących Cię pakietów na podstawie określonego wyrażenia.

W pierwszej kolejności zapoznamy się z plikami zawierającymi przechwycone dane.

## **Pliki zawierające przechwycone dane**

*Pliki zawierające przechwycone dane* są używane we faktycznym procesie przechwytywania pakietów. Jednym z podstawowych powodów używania filtra przechwytywania jest zachowanie maksymalnej wydajności działania. Jeżeli wiesz, że nie będziesz analizował określonych form ruchu sieciowego, możesz odfiltrować jego dane za pomocą filtra przechwytywania. W ten sposób zaoszczędzisz nieco mocy procesora, która musiałaby zostać wykorzystana do przechwycenia nieinteresujących Cię pakietów.

Możliwość utworzenia własnych filtrów przechwytywania jest bardzo użyteczna w przypadku obsługi ogromnych ilości danych. Proces analizy można znacznie przyspieszyć poprzez zagwarantowanie, że patrzysz tylko na te pakiety, które mają związek z rozwiązywanym problemem.

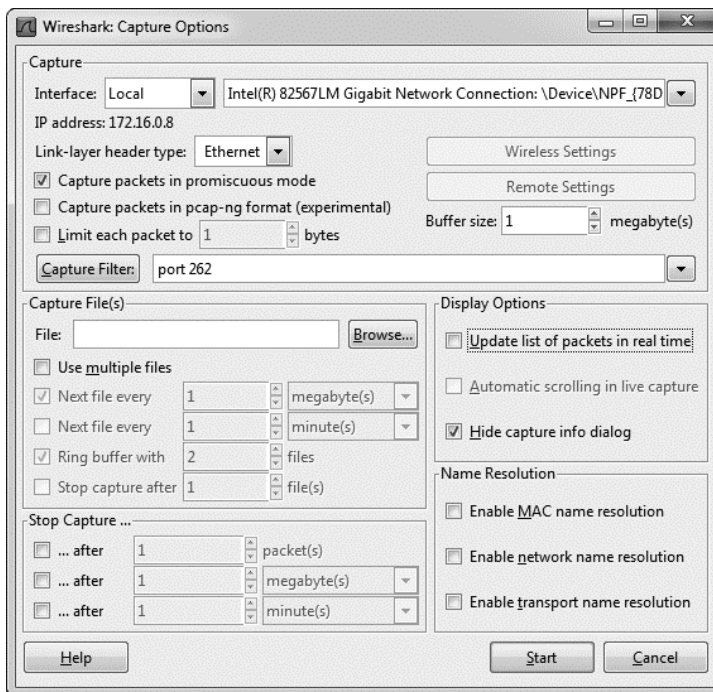
Prosty przykład użycia filtra przechwytywania to sytuacja, w której przechwytyjesz ruch z serwera sieciowego o wielu rolach. Przypuśćmy, że rozwiązujesz problem z usługą udostępnianą na porcie 262. Jeżeli analizowany serwer udostępnia także wiele innych usług na różnych portach, to wyszukanie i przeanalizowanie ruchu przepływającego jedynie przez port 262 będzie samo w sobie już wymagającym zadaniem. Aby przechwycić jedynie ruch przepływający przez port 262, możesz użyć filtra przechwytywania. W tym celu przejdź do omówionego wcześniej okna dialogowego *Capture Options* i wykonaj następujące kroki:

1. Wybierz opcję menu *Capture/Interfaces* i naciśnij przycisk *Options* znajdujący się obok nazwy interfejsu, z którego chcesz przechwycić dane.
2. Wybierz interfejs, z którego będą przechwytywane pakiety, a następnie wskaż filtr przechwytywania.
3. Filtr przechwytywania możesz zastosować poprzez podanie odpowiedniego wyrażenia w polu tekstowym znajdującym się obok przycisku *Capture Filter*. W omawianym przykładzie interesuje nas tylko ruch przepływający przez port 262, zatem w polu tym wpisujemy port 262, jak pokazano na rysunku 4.10. (Wprowadzone tutaj wyrażenie zostanie dokładnie omówione w kolejnej sekcji).
4. Po zdefiniowaniu filtra wystarczy nacisnąć przycisk *Start* rozpoczynający przechwytywanie pakietów.

Po zebraniu odpowiedniej wielkości próbki danych zobaczysz, że próbka zawiera jedynie dane ruchu sieciowego przepływającego przez port 262. Dzięki temu możesz znacznie efektywniej przeprowadzić analizę tych danych.

## **Przechwytywanie i składnia BPF**

Filtry przechwytywania są stosowane przez WinPcap i używają składni BPF (ang. *Berkeley Packet Filter*). Składnia ta jest stosowana w wielu aplikacjach typu sniffer pakietów najczęściej z powodu wykorzystywania przez te aplikacje bibliotek libpcap/WinPcap, które pozwalają na stosowanie składni BPF. Znajomość składni BPF ma więc znacznie krytyczne, jeśli chcesz zagłębić się w sieć na poziomie pakietów.



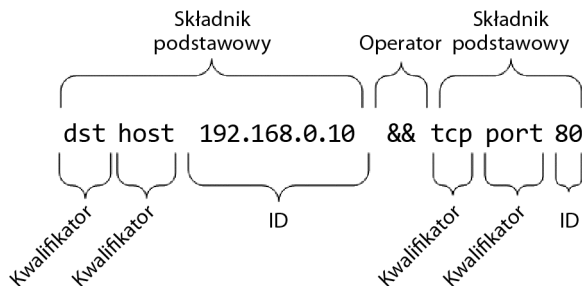
Rysunek 4.10. Zdefiniowanie filtru przechwytywania w oknie dialogowym *Capture Options*

Filtr utworzony z użyciem składni BPF jest nazywany *wyrażeniem*, a każde wyrażenie składa się z co najmniej jednego *składnika podstawowego*. Z kolei składniki składają się z co najmniej jednego *kwalifikatora* (kwalifikatory wymieniono w tabeli 4.2) wraz z identyfikatorem, jak pokazano na rysunku 4.11.

Tabela 4.2. Kwalifikatory składni BPF

Kwalifikator	Opis	Przykłady
typ	określa nazwę lub numer identyfikatora, do którego się odwołuje	host, net, port
kierunek	określa kierunek transmisji do urządzenia o podanej nazwie lub identyfikatorze albo od takiego urządzenia	src, dst
protokół	ogranicza dopasowanie do konkretnego protokołu	ether, ip, tcp, udp, http, ftp

Biorąc pod uwagę komponenty wyrażenia, kwalifikator *src* i identyfikator *192.168.0.10* tworzą postać składnika podstawowego. Taki składnik jest wyrażeniem, które spowoduje przechwycenie ruchu sieciowego pochodzącego jedynie z adresu IP *192.168.0.10*.



Rysunek 4.11. Prosty filtr przechwytywania

W celu łączenia składników i tworzenia bardziej zaawansowanych wyrażeń możesz wykorzystać operatory logiczne. Poniżej wymieniono trzy operatory logiczne dostępne podczas tworzenia wyrażeń:

- operator konkatencji AND (&&);
- operator alternatywy OR (|);
- operator negacji NOT (!).

Przykładowo: poniższe wyrażenie spowoduje przechwycenie ruchu sieciowego pochodzącego z adresu IP 192.168.0.10 oraz z portu 80 lub do tego portu:

```
.....
src 192.168.0.10 && port 80
.....
```

### Filtr nazwy komputera i adresu

Większość tworzonych przez Ciebie filtrów będzie dotyczyła danego urządzenia sieciowego lub grupy urządzeń. W zależności od sytuacji filtrowanie może opierać się na adresie MAC urządzenia, adresie IPv4, IPv6 lub nazwie komputera DNS.

Przykładowo: chcesz się dowiedzieć, jaki ruch sieciowy przepływa przez określony komputer podczas komunikacji z serwerem znajdującym się w danej sieci. Dla serwera możesz więc utworzyć filtr, używając kwalifikatora host. Tak przygotowany filtr będzie przechwytywał cały ruch sieciowy związany z adresem IPv4 interesującego Cię komputera:

```
.....
host 172.16.16.149
.....
```

Jeżeli w sieci używasz protokołu IPv6, to użyty w kwalifikatorze host filtr musi opierać się na adresie IPv6, jak przedstawiono poniżej:

```
.....
host 2001:db8:85a3::8a2e:370:7334
.....
```

W kwalifikatorze host można także użyć filtru opartego na nazwie komputera, na przykład:

```
host serwertestowy2
```

Jeśli masz obawy, że adres IP interesującego Cię komputera może ulec zmianie, możesz przygotować filtr również na podstawie adresu MAC urządzenia, podając kwalifikator ether:

```
ether host 00-1a-a0-52-e2-a0
```

Kwalifikatory kierunku transmisji danych są bardzo często używane w połączeniu z powyższymi przykładami w celu przechwytywania ruchu przychodzącego do określonego komputera lub wychodzącego z niego. Przykładowo: aby przechwycić jedynie ruch przychodzący do danego komputera, można użyć kwalifikatora src:

```
src host 172.16.16.149
```

Aby przechwycić jedynie dane opuszczające serwer o adresie 172.16.16.149 i przeznaczone dla danego komputera, możesz użyć kwalifikatora dst:

```
dst host 172.16.16.149
```

Kiedy nie podajesz kwalifikatora typu (host, net lub port) wraz ze składnikiem podstawowym, domyślnie zakłada się, że został użyty kwalifikator host. Dlatego poniższe wyrażenie jest odpowiednikiem zaprezentowanego w poprzednim przykładzie:

```
dst 172.16.16.149
```

## **Filtry portów**

Oprócz filtrowania na podstawie komputerów można przeprowadzić filtrowanie na podstawie portów używanych w pakietach. Filtrowanie na podstawie portów można wykorzystać do filtrowania na podstawie usług i aplikacji używających standardowych portów. Poniżej przedstawiono prosty filtr przechwytyjący jedynie ruch przepływający przez port 8080:

```
port 8080
```

W celu przechwycenia całego ruchu sieciowego poza przepływającym przez port 8080 można wykorzystać następujące wyrażenie:

```
!port 8080
```

Filtr portu można połączyć z kwalifikatorem kierunku transmisji danych. Przykładowo: aby przechwycić jedynie ruch sieciowy przychodzący do serwera WWW nasłuchującego na standardowym porcie HTTP 80, należy użyć kwalifikatora `dst`:

```
dst port 80
```

## **Filtry protokołów**

Filtry protokołów umożliwiają filtrowanie pakietów na podstawie określonych protokołów. Są wykorzystywane w celu dopasowania protokołów innych niż warstwy aplikacji, przy czym te protokoły nie mogą być zdefiniowane poprzez podanie określonego portu. Dlatego jeżeli chcesz zobaczyć jedynie ruch sieciowy ICMP, możesz użyć następującego filtra:

```
i cmp
```

Aby zobaczyć cały ruch sieciowy poza IPv6, należy użyć filtra:

```
!ip6
```

## **Filtry pola protokołu**

Prawdziwa potęga składni BPF kryje się w możliwości przeanalizowania każdego bajta nagłówka protokołu w celu utworzenia szczegółowych filtrów opartych na tych danych. Omówione w tej sekcji filtry zaawansowane umożliwiają pobieranie określonej liczby bajtów z pakietu rozpoczynającego się we wskazanym położeniu.

Przykładowo: chcesz przeprowadzić filtrowanie na podstawie pola typu nagłówka ICMP. Pole to znajduje się na początku pakietu, czyli jego pozycja wynosi 0. Aby określić konkretne położenie w pakiecie, należy podać konkretną pozycję, używając do tego nawiasu kwadratowego umieszczonego obok kwalifikatora protokołu — w omawianym przykładzie to `i cmp[0]`. Wartością zwrotną będzie jedno-bajtowa liczba całkowita, względem której możemy przeprowadzić operację porównania. Na przykład aby pobrać jedynie pakiety ICMP określające, że pakiet nie dotarł do celu (typ 3), w wyrażeniu filtra należy użyć operatora równości, co przedstawiono poniżej:

```
i cmp[0] == 3
```



W celu przeanalizowania jedynie pakietów ICMP przedstawiających żądania echo (typ 8) lub odpowiedzi na nie (typ 0) należy użyć dwóch składników podstawowych wraz z operatorem OR:

```
icmp[0] == 8 || icmp[0] == 0
```

Przedstawione powyżej filtry działają doskonale, ale przeprowadzają filtrowanie jedynie na podstawie jednobajtowych informacji pochodzących z nagłówka pakietu. Na szczęście można również określić wielkość danych zwracanych przez wyrażenie filtru poprzez jej podanie w nawiasie kwadratowym tuż po wartości określającej pozycję. Obie liczby muszą być rozdzielone dwukropkiem.

Przykładowo: chcemy utworzyć filtr przechwytyjący wszystkie pakiety ICMP, które nie dotarły do celu — są oznaczone jako typ 3 i kod 1. To jednobajtowe pola umieszczone obok siebie w pozycji 0 nagłówka pakietu. Naszym celem jest więc utworzenie filtru sprawdzającego dwa bajty danych znajdujące się na początku nagłówka pakietu (pozycja wynosi 0) i porównanie ich względem wartości szesnastkowej 0301 (typ 3, kod 1). Wyrażenie ma więc następującą postać:

```
icmp[0:2] == 0x0301
```

Bardzo często zdarza się przechwytywanie jedynie pakietów TCP wraz z ustawioną opcją RST. Szczegółowe omówienie protokołu TCP znajdziesz w rozdziale 6. Teraz musisz jedynie wiedzieć, że opcje pakietu TCP są umieszczone w pozycji 13. To interesujące pole, ponieważ jako pole opcji ma wielkość jednego bajta, a poszczególne opcje są identyfikowane za pomocą pojedynczych bitów w tym bajcie. W pakiecie TCP można ustawić jednocześnie wiele opcji, co oznacza brak możliwości efektywnego filtrowania za pomocą prostego wyrażenia tcp[13], ponieważ ten bit RST mógł zostać ustawiony z różnych powodów. Dlatego konieczne jest dokładne wskazanie w bajcie położenia, które ma zostać przeanalizowane. W tym celu do składnika należy dołączyć znak & i podać położenie tego składnika. Opcja RST jest przedstawiana za pomocą bitu o liczbie 4. Gotowy filtr ma następującą postać:

```
tcp[13] & 4 == 4
```

Aby zobaczyć wszystkie pakiety wraz z ustawioną opcją PSH, która w omawianym bajcie jest przedstawiona za pomocą bitu znajdującego się w położeniu 8, filtr powinien mieć postać:

```
tcp[13] & 8 == 8
```

## Przykładowe wyrażenia filtrów przechwytywania danych

Przekonasz się, że sukces lub porażka podczas analizy pakietów bardzo często zależy od Twoich możliwości w dziedzinie tworzenia filtrów odpowiednich do danej sytuacji. W tabeli 4.3 wymieniono kilka przykładowych filtrów przechwytywania danych, których używam najczęściej.

Tabela 4.3. Najczęściej używane filtry przechwytywania danych

Filtr	Opis
<code>tcp[13] &amp; 32 == 32</code>	pakiey TCP wraz z ustawioną opcją URG
<code>tcp[13] &amp; 16 == 16</code>	pakiey TCP wraz z ustawioną opcją ACK
<code>tcp[13] &amp; 8 == 8</code>	pakiey TCP wraz z ustawioną opcją PSH
<code>tcp[13] &amp; 4 == 4</code>	pakiey TCP wraz z ustawioną opcją RST
<code>tcp[13] &amp; 2 == 2</code>	pakiey TCP wraz z ustawioną opcją SYN
<code>tcp[13] &amp; 1 == 1</code>	pakiey TCP wraz z ustawioną opcją FIN
<code>tcp[13] == 18</code>	pakiey TCP SYN-ACK
<code>ether host 00:00:00:00:00:00</code> (adres zastąp swoim adresem MAC)	ruch do podanego adresu MAC oraz z tego adresu
<code>!ether host 00:00:00:00:00:00</code> (adres zastąp swoim adresem MAC)	ruch, który nie przychodzi do podanego adresu MAC oraz nie wychodzi z niego
<code>broadcast</code>	tylko ruch rozgłaszający
<code>icmp</code>	tylko ruch ICMP
<code>icmp[0:2] == 0x0301</code>	urządzenie docelowe ICMP jest niedostępne, komputer jest niedostępny
<code>ip</code>	tylko ruch IPv4
<code>ip6</code>	tylko ruch IPv6
<code>udp</code>	tylko ruch UDP

## Filtry wyświetlania

*Filtr wyświetlania* to ten, który po zastosowaniu względem pliku zawierającego przechwycone dane nakazuje narzędziu Wireshark wyświetlenie jedynie pakietów spełniających kryteria tego filtru. Filtr wyświetlania można zdefiniować w polu *Filter* znajdującym się nad panelem *Packet List*.

Filtry wyświetlania są używane częściej niż filtry przechwytywania danych, ponieważ pozwalają filtrować pakiey bez rzeczywistego pominięcia pozostałych danych zebranych w pliku. W ten sposób, jeśli będziesz musiał powrócić do początkowego zbioru zebranych danych, wystarczy po prostu usunąć wyrażenie filtru.

Filtr wyświetlania możesz wykorzystać do ukrycia nieistotnego w danej chwili ruchu sieciowego zebranego w pliku przechwyconych danych. Przykładowo: możesz ukryć ruch pakietów ARP w panelu *Packet List*, kiedy te pakiey nie mają żadnego związku z aktualnie rozwiązywanym problemem. Jednak ponieważ pakiey ARP mogą być użyteczne później, lepszym rozwiązaniem jest ich tymczasowe ukrycie zamiast trwałego usunięcia.

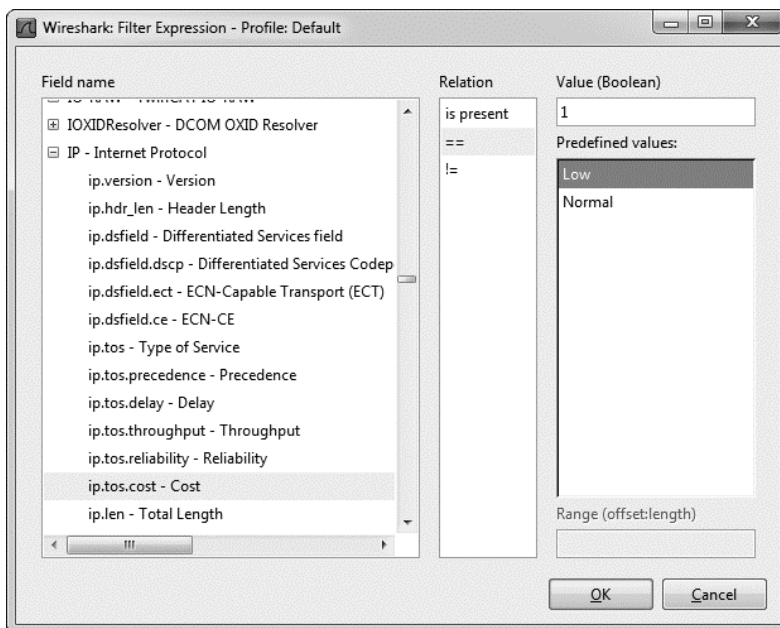
Aby odfiltrować wszystkie pakiety ARP w oknie przechwytywania, po prostu umieść kursor w polu tekstowym *Filter* znajdującym się na górze panelu *Packet List*, a następnie wprowadź wyrażenie `!arp`, które spowoduje ukrycie wszystkich pakietów ARP w panelu *Packet List* (zob. rysunek 4.12). Usunięcie filtru następuje po naciśnięciu przycisku *Clear*.



Rysunek 4.12. Utworzenie filtru wyświetlania za pomocą pola *Filter* znajdującego się nad panelem *Packet List*

## Okno dialogowe *Filter Expression*

Pokazane na rysunku 4.13 okno dialogowe *Filter Expression* znacznie ułatwia początkującym użytkownikom narzędzia Wireshark tworzenie filtrów przechwytywania danych i filtrów wyświetlania. Aby wyświetlić to okno, należy nacisnąć przycisk *Capture Filter* w oknie dialogowym *Capture Options*, a następnie przycisk *Expression*.



Rysunek 4.13. Okno dialogowe *Filter Expression* umożliwia łatwe tworzenie filtrów w narzędziu Wireshark

Po lewej stronie okna dialogowego znajdują się wszystkie dostępne do użycia protokoły. W tych polach można określić wszystkie możliwe kryteria filtru. Aby utworzyć filtr, wykonaj następujące kroki:

1. W celu wyświetlenia kryteriów związanych z danym protokołem rozwiń ten protokół, klikając symbol plusa znajdujący się obok jego nazwy. Po znalezieniu szukanego kryterium, na którym będzie oparty filtr, kliknij je w celu zaznaczenia.
2. Następnie określ, w jaki sposób wybrane kryterium będzie zależało od zdefiniowanej dla niego wartości. Dostępne opcje to: równy, większy niż, mniejszy niż itd.
3. Utwórz wyrażenie filtru poprzez podanie wartości kryterium, która będzie miała związek z wybranym polem. Tę wartość możesz zdefiniować sam lub możesz wybrać jedną z zdefiniowanych w narzędziu Wireshark.
4. Na końcu kliknij przycisk OK i wyświetl tekstową wersję przygotowanego filtru.

Okno dialogowe *Filter Expression* to doskonała pomoc dla początkujących użytkowników. Po nabyciu pewnej wprawy przekonasz się, że ręczne tworzenie wyrażeń filtrów znacznie zwiększa ich efektywność. Składnia wyrażenia filtru wyświetlania jest bardzo prosta i daje ogromne możliwości.

### **Struktura składni wyrażenia filtru (trudniejszy sposób)**

Filtry przechwytywania lub wyświetlania danych najczęściej będziesz wykorzystywał do przeprowadzania filtrowania na podstawie danego protokołu. Załóżmy, że rozwiązujesz problem związany z TCP, więc w pliku zawierającym przechwycone dane chcesz widzieć tylko ruch sieciowy TCP. W takim przypadku prosty filtr `tcp` jest idealnym rozwiązaniem.

Spójrzmy jednak na to z innej strony. Wyobraź sobie, że w trakcie procesu usuwania problemu związanego z TCP bardzo często używasz polecenia `ping`, generując w ten sposób znaczną ilość ruchu sieciowego ICMP. Ruch ICMP możesz ukryć w pliku zawierającym przechwycone dane poprzez użycie wyrażenia filtru o postaci `!icmp`.

Operatory porównania umożliwiają porównywanie wartości. Przykładowo: podczas usuwania problemów w sieciach TCP/IP bardzo często zachodzi potrzeba wyświetlenia wszystkich pakietów odwołujących się do konkretnego adresu IP. Operator porównania (`==`) pozwala na utworzenie filtru wyświetlającego wszystkie pakiety powiązane z adresem IP, na przykład `192.168.0.1`:

```
.....  
ip.addr==192.168.0.1  
.....
```

Załóżmy, że chcesz wyświetlić tylko te pakiety, których wielkość jest mniejsza niż 128 bajtów. W takim przypadku można użyć operatora „mniejszy lub równy” (`<=`) w celu przygotowania następującego wyrażenia filtru:

```
.....  
frame.len <= 128  
.....
```

Operatory porównania wykorzystywane w narzędziu Wireshark zostały wymienione w tabeli 4.4.

Operatory logiczne pozwalają łączyć wiele wyrażeń filtrów w pojedyncze wyrażenie, co znacznie zwiększa efektywność działania filtru. Przykładowo: chcemy wyświetlić pakiety wysyłane tylko do dwóch adresów IP. W tym celu możemy użyć operatora OR do utworzenia pojedynczego wyrażenia filtru, które będzie wyświetlało pakiety zawierające jeden ze zdefiniowanych adresów:

Tabela 4.4. Operatory porównania stosowane w wyrażeniach filtrów narzędzia Wireshark

Operator	Opis
==	równość
!=	nierówność
>	większy niż
<	mniejszy niż
>=	większy lub równy
<=	mniejszy lub równy

ip.addr==192.168.0.1 or ip.addr==192.168.0.2

Operatory logiczne wykorzystywane w narzędziu Wireshark zostały wymienione w tabeli 4.5.

Tabela 4.5. Operatory logiczne stosowane w wyrażeniach filtrów narzędzia Wireshark

Operator	Opis
and	obydwa warunki muszą przyjąć wartość true
or	jeden z warunków musi przyjąć wartość true
xor	jeden i tylko jeden warunek może przyjąć wartość true
not	żaden z warunków nie może przyjąć wartości true

### Przykładowe wyrażenia filtrów wyświetlania

Koncepcje związane z tworzeniem wyrażeń filtrów są całkiem proste, ale czasem podczas rozwiązywania różnych problemów trzeba używać kilku określonych słów kluczowych i operatorów. W tabeli 4.6 wymieniono filtry wyświetlania, z których najczęściej korzystam. Pełną listę filtrów wyświetlania w narzędziu Wireshark znajdziesz w dokumentacji dostępnej na stronie <http://www.wireshark.org/docs/dfref/>.

### Zapis filtrów

Kiedy rozpoczniesz tworzenie ogromnej liczby filtrów przechwytywania i wyświetlania danych, przekonasz się, że pewne z nich są często wykorzystywane. Na

szczęście filtru nie musisz wpisywać za każdym razem, gdy chcesz go użyć, ponieważ narzędzie Wireshark pozwala zapisywać filtry i później je wykorzystywać. Aby zapisać samodzielnie przygotowany filtr przechwytywania danych, wykonaj następujące kroki.

**Tabela 4.6. Najczęściej używane filtry wyświetlania**

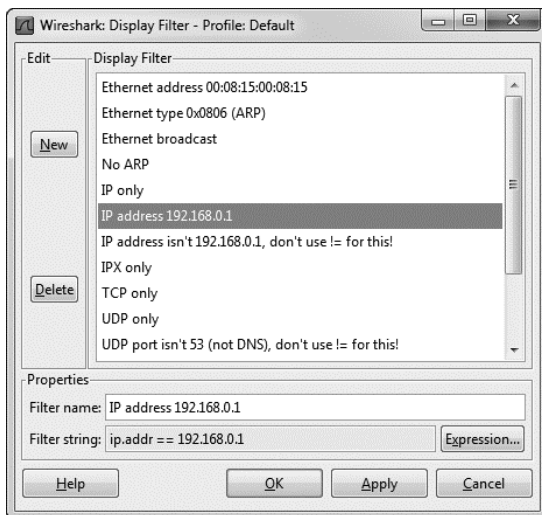
<b>Filtr</b>	<b>Opis</b>
<code>!tcp.port==3389</code>	wyłącznie ruch RDP
<code>tcp.flags.syn==1</code>	pakiety TCP wraz z ustawioną opcją SYN
<code>tcp.flags.rst==1</code>	pakiety TCP wraz z ustawioną opcją RST
<code>!arp</code>	wyłącznie ruch ARP
<code>http</code>	cały ruch HTTP
<code>tcp.port==23    tcp.port 21</code>	ruch administracyjny w postaci zwykłego tekstu (Telnet lub FTP)
<code>smtp    pop    imap</code>	ruch poczty elektronicznej w postaci zwykłego tekstu (SMTP, POP lub IMAP)

1. Wybierz opcję menu *Capture/Capture Filters* w celu wyświetlenia okna dialogowego *Capture Filter*.
2. Utwórz nowy filtr, klikając przycisk *New* znajdujący się po lewej stronie wyświetlonego okna dialogowego.
3. W polu *Filter Name* podaj nazwę filtru.
4. W polu *Filter String* podaj rzeczywiste wyrażenie filtru.
5. Kliknij przycisk *Save* w celu zapisania wyrażenia filtru na liście.

Aby zapisać samodzielnie przygotowany filtr wyświetlania danych, wykonaj następujące kroki.

1. Wybierz opcję *Analyze/Display Filters* albo kliknij przycisk *Filter* znajdujący się nad panelem *Packet List*. W ten sposób na ekranie wyświetli się okno dialogowe *Display Filter* (zob. rysunek 4.14).
2. Utwórz nowy filtr, klikając przycisk *New* znajdujący się po lewej stronie wyświetlonego okna dialogowego.
3. W polu *Filter Name* podaj nazwę filtru.
4. W polu *Filter String* podaj rzeczywiste wyrażenie filtru.
5. Kliknij przycisk *Save* w celu zapisania wyrażenia filtru na liście.

Narzędzie Wireshark zawiera wiele wbudowanych wzorcowych filtrów. Możesz je wykorzystać (wraz z dokumentacją narzędzia Wireshark) podczas tworzenia własnych filtrów. Filtry będziemy stosować w wielu przykładach przedstawionych w tej książce.



Rysunek 4.14. Okno dialogowe Display Filter umożliwia zapis wyrażen filtrów





# Skorowidz

## A

- adres IP, 123
  - adres sieci, 124
  - adres urządzenia, 124
  - alokacja bitów, 124
  - maska sieci, 124
  - skrót CIDR, 125
- adres MAC, 31, 118
- AirPcap, 264
  - konfiguracja, 265
    - Blink Led, 265
    - Capture Type, 265
    - Channel, 265
    - FCS Filter, 266
    - Include 802.11 FCS in Frames, 265
    - Interface, 265
    - WEP Configuration, 266
  - WinPcap, 265
- analiza pakietów, 22
  - błąd programisty, 199
    - przeglądanie komunikacji FTP, 201
  - tworzenie filtru, 200
- brak dostępu do internetu, 183
  - odpowiedź na zapytanie DNS, 191
  - próba określenia nazwy DNS, 184
  - próba ustalenia adresu MAC, 187
  - szukanie bramy domyślnej sieci, 184
  - zapytanie DNS dotyczące rekordu A, 191
- brak dostępu do serwerów aplikacji sieciowych, 196
- ESPN.com, 179
  - okno Conversations, 179
  - okno Protocol Hierarchy Statistics, 179
  - przechwytywanie, 179
  - przeglądanie ruchu DNS, 181

- wyświetlanie żądań HTTP, 182
- Facebook, 172
  - proces logowania, 176
  - przechwytywanie, 176
  - wiadomości prywatne, 177
- hermetyzacja danych, 29
  - przedstawienie graficzne, 30
  - jednostka danych protokołu, 29
  - praktyczny przykład, 29
- koncentrator, 41
  - kolizja, 42
- początkowy proces negocjacji TCP, 221
- protokoły, 24
  - wspólne cechy, 24
- przechwytywanie, 40
  - ESPN.com, 179
  - Facebook, 176
  - koncentrator, 41
  - lokalizacja sniffera, 56
  - przełącznik sieciowy, 43, 57
  - router, 54
  - Twitter, 172
  - Wireshark, 65
  - WLAN, 260
- przełącznik sieciowy, 43
  - okno widoczności, 43
- punkt odniesienia, 225
- sniffer, 22
  - czynniki wyboru, 22
  - OmniPeek, 22
  - proces działania, 23
  - tcpdump, 22
  - Wireshark, 22
  - wybór lokalizacji, 40
- tryb mieszany, 40
- Twitter, 172
  - proces logowania, 172
  - przechwytywanie, 172
  - przekazywanie danych, 174
  - wiadomości bezpośrednie, 175
- Wireshark, 76
  - dekoder protokołu, 104, 114
  - filtry, 83

- format wyświetlania czasu, 78
- funkcja odniesienia czasu, 79
- grafika, 110
- konwersacje sieciowe, 99
- konwersja strumieni TCP, 108
- określanie nazw, 103
- oznaczanie pakietów, 77
- punkty końcowe, 98
- rozkład protokołów w pliku, 102
- szczegółowa analiza protokołu, 104
- wielkość, 109
- wydruk pakietów, 77
- wymuszone dekodowane, 105
- wyszukiwanie pakietów, 76

WLAN, 260

- AIRPcap, 266
- iwconfig, 268
- przechwytywanie, 260
- tryby działania kart, 264

zapewnienie bezpieczeństwa, 231

- foolprinting, 232
- IDS, 231
- skanowanie TCP SYN, 232
- WEP, 275
- włamanie, 240
- WPA, 275
- WPA2, 275

zasoby, 288

analiza protokołu, *Patrz* analiza pakietów

## B

- bezpieczeństwo, 231
  - foolprinting, 232
  - skanowanie TCP SYN, 232
  - wykrywanie systemu operacyjnego, 237
- IDS, 231
- skanowanie TCP SYN, 232

bezpieczeństwo  
skanowanie TCP SYN  
  identyfikacja otwartych  
  i zamkniętych portów, 236  
  możliwe odpowiedzi, 233  
  użycie filtrów, 234  
WEP, 275  
  nieudany proces  
  uwierzytelnienia, 278  
  udany proces  
  uwierzytelnienia, 277  
włamanie, 240  
  koń trojański, 248  
  Operacja Aurora, 240  
  zatrucie bufora ARP, 246  
WPA, 275  
  nieudane uwierzytelnienie, 280  
  proces negocjacji, 279  
  udane uwierzytelnienie, 278  
WPA2, 275  
wykrywanie systemu  
  operacyjnego, 237  
  aktywne, 239  
  pasywne, 238  
broadcast, 35  
  adres rozgłoszeniowy, 36  
  domena rozgłoszeniowa, 36

## C

Cain & Abel, 51, 284  
  aktywowanie sniffiera, 51  
  zatrucie bufora ARP, 53  
CloudShark, 285  
  przeglądanie pliku, 286  
Colasoft Packet Builder, 284

## D

dekoder protokołu, 104  
  informacje zaawansowane, 114  
  Chat, 114, 115  
  Error, 115, 116  
  Note, 114, 116  
  Warning, 115, 116  
Domain Dossier, 288

## E

ESPN.com, 179  
  przechwytywanie pakietów, 179  
  okno Conversations, 179  
  okno Protocol Hierarchy  
  Statistics, 179  
  przeglądanie ruchu DNS, 181  
  wyświetlanie żądań HTTP, 182

## F

Facebook, 172  
  proces logowania, 176  
  przechwytywanie pakietów, 176  
  wiadomości prywatne, 177  
filtry, 83, 272  
  nazwy komputera i adresu, 86  
  poła protokołu, 88  
  portów, 87  
  protokołów, 88  
  przechwytywania, 83  
  najczęściej używane, 90  
  schemat prostego filtra, 86  
  składnia BPF, 84  
  zapis, 94  
WLAN, 272  
  filtrowanie częstotliwości, 275  
  filtrowanie typów pakietów, 274  
  wskazany punkt dostępowy,  
  273  
  wyświetlania, 83, 90  
  najczęściej używane, 94  
  zapis, 94  
fragmentacja pakietu, 128  
  MTU, 128

## H

hermetyzacja danych, 29  
  przedstawienie graficzne, 30  
  jednostka danych protokołu, 29  
  praktyczny przykład, 29  
hping, 287  
hubbing out, 45

## I

iwconfig, 268

## J

jeden do jednego, *Patrz* unicast  
jeden do wielu, *Patrz* multicast  
jeden do wszystkich, *Patrz*  
  broadcast

## K

koncentrator, 31  
  przechwytywanie pakietów, 41  
  przepływ ruchu sieciowego, 32  
kontrola przepływu danych TCP, 213  
  mechanizm przesuwającego się  
  okna, 214  
  bufor TCP, 214  
  dostosowanie wielkości  
  okna, 215

okno odbiorcy, 214  
pakiet keep-alive, 216, 219, 221  
  powiadomienie o zerowej  
  wielkości okna, 216, 219, 221  
konwersacja sieciowa, 98  
koń trojański, 248  
  komunikat ostrzeżenia z systemu  
  IDS, 257  
konwersacje pomiędzy  
  atakującym i ofiarą, 252  
predefiniowane sygnatury  
  ataków, 249  
RAT, 250  
reguła Snort, 251  
usunięcie zbędnych bajtów z  
  pliku JPG, 256  
wykres operacji wejścia-wyjścia,  
  254

## L

LAN, 123  
  adres sieci, 124  
libpcap, 287

## M

mapa sieci, 56  
maska sieci, 124  
  skrót CIDR, 125  
model OSI, 25  
  protokoły, 27  
  hermetyzacja danych, 29  
przepływ danych, 27  
warstwy, 25  
  aplikacji, 25  
  fizyczna, 27  
  graficzny model, 28  
  hierarchia, 26  
  łącza danych, 27  
  prezentacji, 25  
  protokoły, 28  
  sesji, 26  
  sieciowa, 26  
  transportowa, 26  
multicast, 35, 37

## N

narzędzia  
  Cain & Abel, 51, 284  
  CloudShark, 285  
  przeglądanie pliku, 286  
  Colasoft Packet Builder, 284  
  Domain Dossier, 288  
  hping, 287  
  libpcap, 287  
  Netdude, 284  
  modyfikowanie pakietów, 285

- NetworkMiner, 287
- ngrep, 287
- Nmap, 233
- pcapr, 285
  - przeglądanie DHCP, 286
- Scapy, 284
- tcpdump, 284
- Tcpdump, 287
- Wireshark, 59
  - filtry, 83
  - grupa Time Display Format, 79
  - okno Capture Options, 80, 85, 104
  - okno Coloring Rules, 70
  - okno Conversations, 99, 101, 180
  - okno Decode As, 106
  - okno Display Filter, 95
  - okno Edit Color Filter, 70
  - okno Endpoints, 99, 101
  - okno Expert Infos, 115
  - okno Filter Expression, 91
  - okno Find Packet, 76
  - okno Follow TCP Stream, 108
  - okno główne, 67
  - okno IO Graphs, 110
  - okno Merge with capture file, 75
  - okno Packet Lengths, 109
  - okno preferencji, 68
  - okno Print, 78
  - okno Protocol Hierarchy Statistics, 102, 180
  - okno Save As, 74
  - okno Summary, 183
  - pole Filter, 91
  - sekcja Capture, 81
  - sekcja Capture File(s), 81
  - sekcja Display Options, 83
  - sekcja Name Resolution, 83
  - sekcja Stop Capture, 82
- Netdude, 284
  - modyfikowanie pakietów, 285
- NetworkMiner, 287
- ngrep, 287
- Nmap, 233
  - skanowanie SYN, 233

## ●

- określanie nazw, 103
- Operacja Aurora, 240
  - atak spear phishing, 240
  - interakcja z wierszem poleceń ofiary, 244
  - sposób działania luki w zabezpieczeniach, 244

- treść w znaczniku <script>, 242
- żądanie HTTP GET, 241
- opóźnienie, 206
  - duplikaty potwierżeń TCP, 209
  - lokalizacja źródła opóźnień, 221
    - analiza początkowego procesu negocjacji TCP, 221
    - po stronie klienta, 223
    - po stronie serwera, 224
  - punkt odniesienia, 221, 225
    - dla aplikacji, 228
  - punkt odniesienia dla komputera, 227
  - punkt odniesienia dla miejsca, 226
    - struktura poszukiwań, 225
    - z winy sieci, 222
  - mechanizm przesuwającego się okna, 214
  - ponowna transmisja pakietu TCP, 206

## P

- pakiety, 21
  - analiza, 22
    - dekoder protokołu, 104, 114
    - filtry, 83
    - format wyświetlania czasu, 78
    - funkcja odniesienia czasu, 79
    - grafika, 110
    - hermetyzacja danych, 29
    - konwersacje sieciowe, 99
    - konwersja strumieni TCP, 108
    - określanie nazw, 103
    - oznaczanie, 77
    - protokoły, 24
    - punkty końcowe, 98
    - rozkład protokołów w pliku, 102
    - sniffer, 22
    - szczegółowa analiza protokołu, 104
    - Wireshark, 76
    - wydruk, 77
    - wyszukiwanie, 76
    - zapewnienie bezpieczeństwa, 231
    - zasoby, 288
  - jednostka danych protokołu, 29
  - przechwytywanie, 40
    - ESPN.com, 179
    - Facebook, 176
    - koncentrator, 41
    - konfiguracja opcji, 80
    - lokalizacja sniffera, 56
  - przełącznik sieciowy, 43, 57
  - router, 54
    - tryb mieszany, 40
  - Twitter, 172
  - WLAN, 260
  - Wireshark, 65
  - struktura pakietu 802.11, 269
  - transmisja, 24
    - adresy MAC, 118
    - broadcast, 35
    - koncentrator, 31
    - konwersacje sieciowe, 98
    - model OSI, 25
    - multicast, 35
    - przełącznik sieciowy, 32
    - punkty końcowe, 97
    - router, 33
    - routing, 34
    - tabele CAM, 118
    - unicast, 35
    - wielkość, 109
  - pcapr, 285
    - przeglądanie DHCP, 286
  - Perl, 288
  - ping, 142
    - proces działania, 143
  - proces DORA, *Patrz* proces odnowy DHCP
  - proces negocjacji TCP, 135
    - flaga SYN, 135
    - maksymalna wielkość segmentu, 135
    - odpowiedź SYN/ACK, 137
    - pakiet ACK, 136, 137
    - pakiet SYN/ACK, 136
    - początkowy numer sekwencyjny, 135
    - początkowy pakiet SYN, 136
  - proces odnowy DHCP, 150
    - pakiet odkrycia, 151
      - Client identifier, 153
      - DHCP Message type, 153
      - Parameter Request List, 153
      - Requested IP Address, 153
    - pakiet oferty, 153
    - pakiet potwierdzenia, 155
    - pakiet żądania, 154
  - proces odnowy dzierżawy DHCP, 156
  - protokoły, 24
    - ARP, 40, 118
      - bezpłatny pakiet, 122
      - nałówek, 119
      - odpowiedź, 118, 121
      - określanie adresu docelowego, 119
      - przetwarzanie, 50

- protokoły
  - ARP
    - struktura, 120
    - żądanie, 118, 120
  - BOOTP, 149
  - dekoder, 104
    - analiza kodu źródłowego, 107
    - informacje zaawansowane, 114
    - zmiana, 105
  - DHCP, 150
    - opcje, 156
    - pakiet odkrycia, 151
    - pakiet oferty, 153
    - pakiet potwierdzenia, 155
    - pakiet żądania, 154
    - proces odnowy, 150
    - proces odnowy dzierżawy, 156
    - struktura, 150
    - typy wiadomości, 157
  - DNS, 156
    - architektura serwera, 156
    - odpowiedź, 160
    - rekurencja, 160
    - strefa DNS, 164
    - struktura, 157
    - typy rekordów zasobów, 160
    - zapytanie, 159
  - HTTP, 29, 166
    - kody odpowiedzi, 168
    - pakiet HTTP POST, 169
    - przeglądanie zasobów, 166
    - przekazywanie danych, 168
    - żądanie HTTP GET, 167
  - ICMP, 141
    - nagłówek, 141
    - odpowiedzi na żądanie, 144
    - ping, 142
    - traceroute, 145
    - typy, 142
    - żądania echo, 144
  - IP, 29, 123
    - adres IP, 123
    - fragmentacja, 128
    - nagłówek, 125, 127
    - struktura, 126
    - TTL, 127
  - model OSI, 25, 27
    - hermetyzacja danych, 29
  - określanie nazw, 103
  - RFC, 118
  - routing, 34
  - SSL, 105
  - stos, 24
  - TCP, 130
    - bufor TCP, 214
    - duplikat ACK, 209, 212
    - kontrola przepływu danych, 213
  - mechanizm przesuwającego się okna, 214
  - nagłówek, 131
  - ponowna transmisja pakietu, 206
  - porty, 132
  - porty standardowe, 133
  - porty ulotne, 133
  - potwierdzenia selektywne, 213
  - proces negocjacji, 135
  - RTO, 206
  - RTT, 206
  - sekwencje i potwierdzenia, 210
  - usuwanie błędów, 206
  - wykres procesu retransmisji, 207
  - zakończenie komunikacji, 137
  - zerowanie, 138
  - zwłoka retransmisji, 206
- UDP, 139
  - nagłówek, 140
  - wspólne cechy, 24
- przechwytywanie pakietów, 40
  - ESPN.com, 179
    - okno Conversations, 179
    - okno Protocol Hierarchy Statistics, 179
  - Facebook, 176
    - proces logowania, 176
    - wiadomości prywatne, 177
  - koncentrator, 41
    - podłączenie sniffera, 42
  - lokalizacja sniffera, 56
  - przełącznik sieciowy, 43
    - hubbing out, 45
    - kopiowanie ruchu na wskazany port, 43
    - rozgłęźnik sieciowy, 46
  - techniki przechwytywania, 57
  - zatrucie bufora ARP, 49
- router, 54
  - lokalizacja sniffera, 54
- tryb mieszany, 40
- Twitter, 172
  - proces logowania, 172
  - przekazywanie danych, 174
  - wiadomości bezpośrednie, 175
- Wireshark, 66, 80
  - konfiguracja, 80
  - łączenie plików, 75
  - okno Capture Options, 80
  - sekcja Capture, 81
  - sekcja Capture File(s), 81
  - sekcja Display Options, 83
  - sekcja Name Resolution, 83
  - sekcja Stop Capture, 82
  - wybór interfejsu, 66
  - zapis pakietów, 74
- WLAN, 260
  - AirPcap, 266
  - iwconfig, 268
  - tryby działania kart, 264
  - zakłócenia sygnału, 261
- przełącznik sieciowy, 32
  - przechwytywanie pakietów, 43, 57
    - hubbing out, 45
    - kopiowanie ruchu na wskazany port, 43
    - rozgłęźnik sieciowy, 46
    - zatrucie bufora ARP, 49
  - przepływ ruchu sieciowego, 34
  - tabele CAM, 118
  - zarządzany, 33
- punkt końcowy, 97
- punkt odniesienia, 221, 225
  - dla aplikacji, 228
    - szybkość transferu danych, 228
    - uruchamianie i zamykanie, 228
    - używane protokoły, 228
    - związki i zależności, 228
  - dla komputera, 227
    - ruch sieciowy, 227
    - sekwencje uwierzytelnienia, 227
    - uruchamianie i zamykanie, 227
    - używane protokoły, 227
    - związki i zależności, 228
  - dla miejsca, 226
    - rozgłoszeniowy ruch sieciowy, 226
    - sekwencje uwierzytelniania, 226
    - szybkość transferu danych, 226
    - używane protokoły, 226
  - tworzenie, 229
- Python, 288

## R

- RFC, 118
- router, 33
  - przechwytywanie pakietów, 54
    - lokalizacja sniffera, 54
  - przepływ ruchu sieciowego, 36
  - routing, 34
    - zilustrowanie koncepcji, 34
- rozgłęźnik sieciowy, 46
  - agregowany, 47
    - podłączenie, 48
  - nieagregowany, 48
    - podłączenie, 49
  - wybór, 49
- RTT, 112

## S

Scapy, 284  
sieć lokalna, *Patrz* LAN  
składnia BPF, 84  
    kwalifikatory, 85  
    składnik podstawowy, 85  
    wyrażenie, 85  
skrót CIDR, 125  
sniffing pakietów, *Patrz* analiza pakietów  
strefa DNS, 164  
    transfer strefy, 164  
    pełny, 164  
    przyrostowy, 164

## T

tabele CAM, 118  
tcpdump, 284  
    Windump, 284  
Tcpreplay, 287  
traceroute, 145  
    proces działania, 145  
    przykładowe dane wyjściowe, 147  
TTL, 126  
Twitter, 172  
    proces logowania, 172  
    proces uwierzytelnienia, 173  
    zaszyfrowany proces negocjacji, 173  
przechwytywanie pakietów, 172  
    proces logowania, 172  
przekazywanie danych, 174  
wiadomości bezpośrednie, 175

## U

unicast, 35, 37  
usuwanie błędów protokołu TCP, 206  
    duplikaty potwierżeń, 209  
    duplikat ACK, 209, 210, 212, 220  
    sekwencje i potwierżenia, 210  
ponowna transmisja pakietu, 206, 220  
    maksymalna liczba prób retransmisji, 207  
    przykład retransmisji, 208  
    RTO, 206  
    RTT, 206  
    wykres procesu retransmisji, 207  
    złoka retransmisji, 206  
potwierżenia selektywne, 213

## W

WEP, 275  
Wireshark, 59  
    dekodery protokołu, 104  
    analiza kodu źródłowego, 107  
    informacje zaawansowane, 114  
    okno Expert Infos, 115  
    zmiana, 105  
ESPN.com, 180  
    okno Conversations, 180  
    okno Protocol Hierarchy Statistics, 180  
    okno Summary, 183  
filtry, 83  
    nazwy komputera i adresu, 86  
    okno Capture Options, 85  
    okno Display Filter, 95  
    okno Filter Expression, 91  
    operatory, 93  
    operatory porównania, 93  
    pola protokołu, 88  
    pole Filter, 91  
    portów, 87  
    protokołów, 88  
    przechwytywania, 84, 86, 90  
    rodzaje, 83  
    składnia BPF, 84  
    struktura składni wyrażenia, 92  
    tworzenie, 91  
    wyświetlania, 90  
    zapis, 93  
format wyświetlania czasu, 78  
    grupa Time Display Format, 79  
funkcja odniesienia czasu, 79  
grafika, 110  
    okno IO Graphs, 110  
    wykres operacji wejścia-wyjścia, 111, 112  
    wykres przepływu danych, 113  
    wykres RTT, 112  
kolorowanie pakietów, 69  
    okno Coloring Rules, 70  
    okno Edit Color Filter, 70  
konwersacje sieciowe, 99  
    okno Conversations, 99  
konwersja strumieni TCP, 108  
    okno Follow TCP Stream, 108  
koszt, 60  
łączenie plików, 75  
    okno Merge with capture file, 75  
obsługiwane protokoły, 60  
obsługiwane systemy operacyjne, 61  
okno główne, 67  
    Packet Bytes, 68

    Packet Details, 68  
    Packet List, 67  
okno preferencji, 68  
    Capture, 69  
    Name Resolution, 69  
    Printing, 69  
    Protocols, 69  
    Statistics, 69  
    User Interface, 68  
określanie nazw, 103  
    Enable MAC name resolution, 103  
    Enable network name resolution, 103  
    Enable transport name resolution, 103  
okno Capture Options, 104  
    wady, 104  
    włączenie funkcji, 103  
oznaczanie pakietów, 77  
pomoc techniczna, 61  
proces instalacyjny, 61  
    Linux, 63  
    Mac OS X, 64  
    minimalne wymagania systemowe, 61  
    Windows, 62  
przechwytywanie pakietów, 66, 80  
    łączenie plików, 75  
    okno Capture Options, 80  
    sekcja Capture, 81  
    sekcja Capture File(s), 81  
    sekcja Display Options, 83  
    sekcja Name Resolution, 83  
    sekcja Stop Capture, 82  
    wybór interfejsu, 66  
    zapis pakietów, 74  
przyjazność dla użytkownika, 60  
punkty końcowe, 98  
    okno Endpoints, 99  
rozkład protokołów w pliku, 102  
    okno Protocol Hierarchy Statistics, 102  
wielkość pakietów, 109  
    okno Packet Lengths, 109  
WLAN, 272  
    okno Preferences, 272  
wydruk pakietów, 77  
    okno Print, 78  
wymuszone dekodowanie, 105  
    okno Decode As, 106  
wyszukiwanie pakietów, 76  
    Display filter, 76  
    Hex value, 76  
    okno Find Packet, 76  
    rodzaje operacji, 77  
    String, 76

- Wireshark
  - zalety, 60
  - zapisywanie przechwyconych pakietów, 74
  - okno Save As, 74
- WLAN, 260
  - AirPcap, 264
    - narzędzie konfiguracyjne, 266
  - BSS ID, 273
  - filtry, 272
    - filtrowanie częstotliwości, 275
    - filtrowanie typów pakietów, 274
    - wskazany punkt dostępowy, 273
  - iwconfig, 268
  - Kanał, 260

- pakiey 802.11, 269
  - Dane, 270
  - Kontrola, 269
  - nagłówki, 270
  - struktura, 270
  - Zarządzanie, 269
- przechwytywanie pakietów, 260
  - AirPcap, 266
  - iwconfig, 268
  - tryby działania kart, 264
  - zakłócenia sygnału, 261
- tryby działania kart, 263
  - doraźny, 263
  - master, 263
  - monitorowania, 263
  - zarządzany, 263

- zakłócenia sygnału, 261
  - analizator spektrum, 262
- WPA, 275
- WPA2, 275
- wymuszone dekodowanie, 105

## **Z**

- zakończenie komunikacji TCP, 137
  - flagi FIN/ACK, 138
- zatrucie bufora ARP, 49
  - atak MITM, 246, 249
  - Cain & Abel, 53
  - monitorowane punkty końcowe, 247
  - przetwarzanie, 50
  - zasada działania, 50

# PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



- 1. ZAREJESTRUJ SIĘ**
- 2. PREZENTUJ KSIĄŻKI**
- 3. ZBIERAJ PROWIZJĘ**

Zmień swoją stronę WWW  
w działający bankomat!

**Dowiedz się więcej i dołącz już dzisiaj!**

<http://program-partnerski.helion.pl>



## WYJĄTKOWE ŹRÓDŁO INFORMACJI NA TEMAT ANALIZY DANYCH PRZESYŁANYCH W SIECI!

Przechwytywanie pakietów za pomocą najpopularniejszego na świecie sniffera sieciowego, czyli narzędzia Wireshark, jest bardzo łatwe, niezależnie od tego, czy chodzi o pakiety sieci przewodowej, czy bezprzewodowej. W jaki jednak sposób można wykorzystać te pakiety do zrozumienia, co się dzieje w sieci?

*Praktyczna analiza pakietów* to wyjątkowa książka poświęcona temu zaawansowanemu narzędziu. W trakcie lektury dowiesz się, jak przygotować je do pracy oraz jak przeprowadzić proste prace administracyjne z jego wykorzystaniem. Kolejne rozdziały to solidna dawka coraz bardziej zaawansowanej wiedzy. Tworzenie własnych filtrów, monitorowanie sieci w czasie rzeczywistym, analiza statystyczna ruchu i o zadania, które już nigdy więcej nie sprawią Ci problemów. Ponadto będziesz mieć okazję poznać charakterystykę najpopularniejszych protokołów oraz najczęstsze problemy, jakich mogą Ci one przysporzyć. Książka ta jest obowiązkową pozycją na półce każdego administratora sieci komputerowych, jak również każdej zainteresowanej nimi osoby.

Sięgnij po tę książkę i rozwiąż problemy związane z:

- wolno działającą siecią,
- utraconymi pakietami,
- bezpieczeństwem w sieci,
- przydzielaniem adresów IP.

Patron medialny:



niebezpiecznik.pl



**helion.pl**  
księgarnia  
internetowa

Nr katalogowy: 11067



Księgarnia internetowa  
<http://helion.pl>



Zamówienia telefoniczne:

**0 801 339900**



**0 601 339900**



**Helion**

Sprawdź najnowsze promocje:  
• <http://helion.pl/promocje>  
Książki rajchtniej czytane:  
• <http://helion.pl/bestsellery>  
Zamów informacje o nowościach:  
• <http://helion.pl/novosci>

Helion SA  
ul. Kościuszki 1c, 44-100 Gliwice  
tel.: 32 230 91 63  
e-mail: [helion@helion.pl](mailto:helion@helion.pl)  
<http://helion.pl>

sięgnij po **WIECEJ**



KOD KORZYŚCI

ISBN 978-83-245-5011-8



9 788324 650118

Cena: 59,00 zł

Informatyka w najlepszym wydaniu