PRAKTYCZNA ANALIZA PAKIETÓW

WYKORZYSTANIE NARZĘDZIA WIRESHARK DO ROZWIĄZYWANIA PROBLEMÓW Z SIECIĄ

CHRIS SANDERS

no starch press

Helion

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

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-5011-8

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: 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.

Spis treści

4

Praca z przechwyconymi pakietami

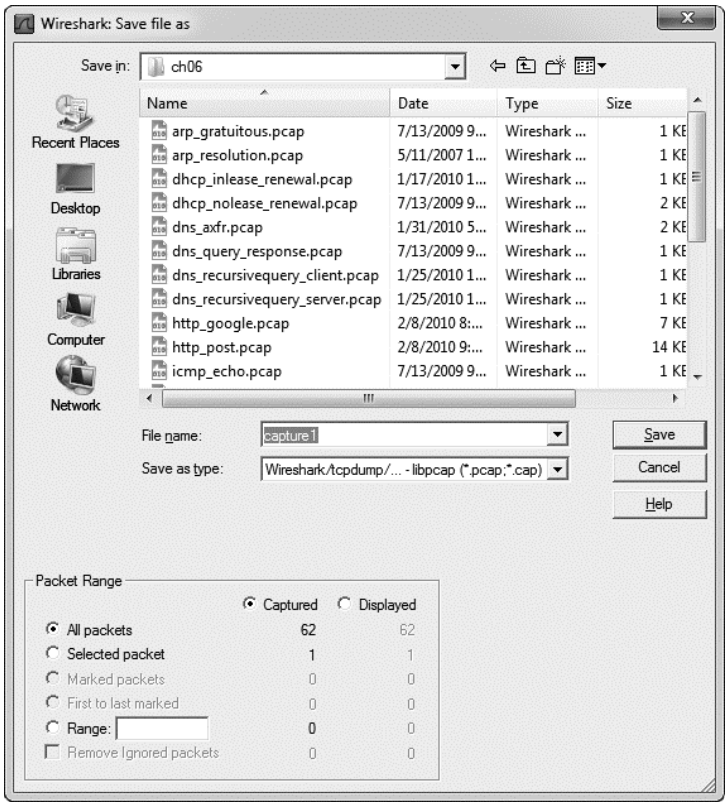
Po krótkim wprowadzeniu do narzędzia Wireshark przedstawionym w rozdziale 3. jesteś gotowy do rozpoczęcia przechwytywania i analizy pakietów. W tym rozdziale dowiesz się, jak pracować z plikami zawierającymi przechwycone dane, z przechwyconymi pakietami oraz z formatami wyświetlania czasu. Omówione zostaną 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).

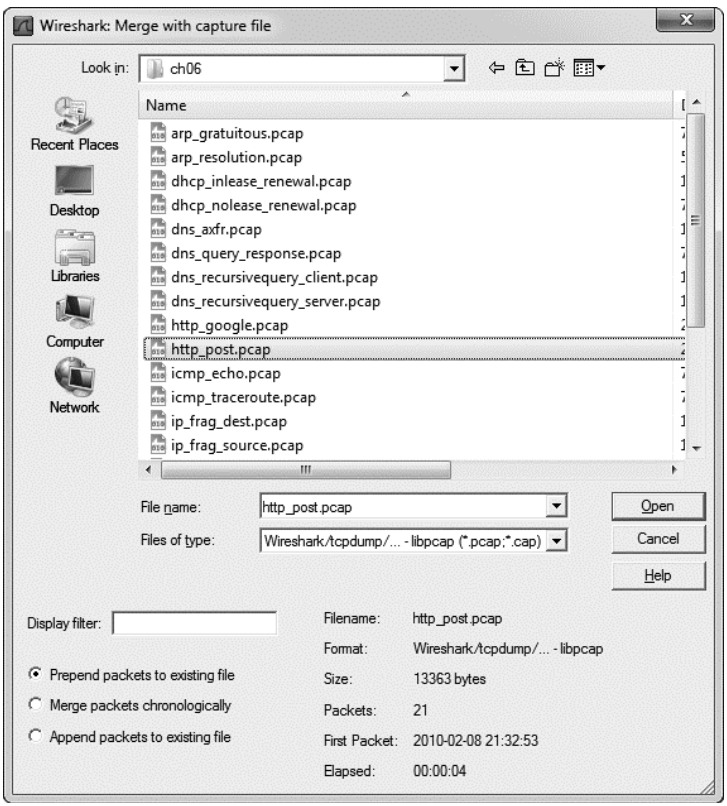
Dane przechwycone przez narzędzie Wireshark możesz eksportować do wielu różnych formatów w celu wyświetlania danych w innych mediach lub przeanalizowania zebranych danych w innych narzędziach. Dostępne formaty to między innymi: zwykły tekst, PostScript, CSV (ang. *Comma Separated Values* — wartości

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`

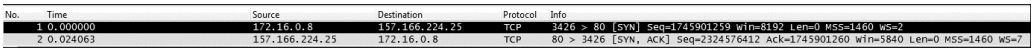
wartość szesnastkowa	`00:ff`
	`ff:ff`
	`00:ab:b1:f0`

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 znalezionego 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).



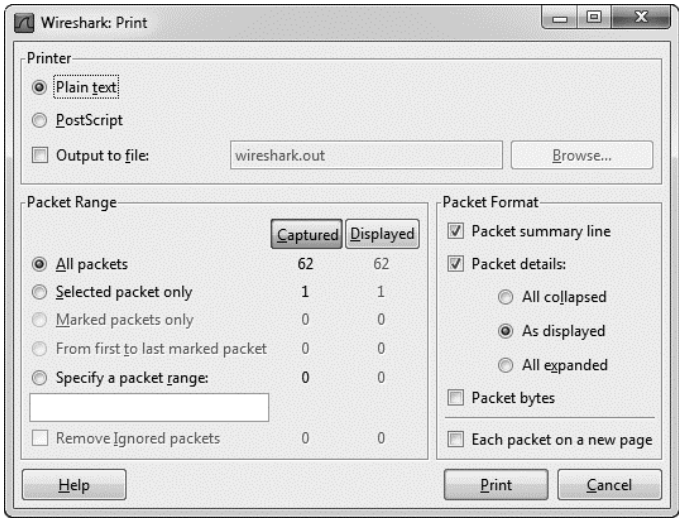
Rysunek 4.4. Oznaczony pakiet jest podświetlony na ekranie. Na rysunku widać, że pakiet pierwszy został oznaczony — ma czarne tło i biały tekst

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

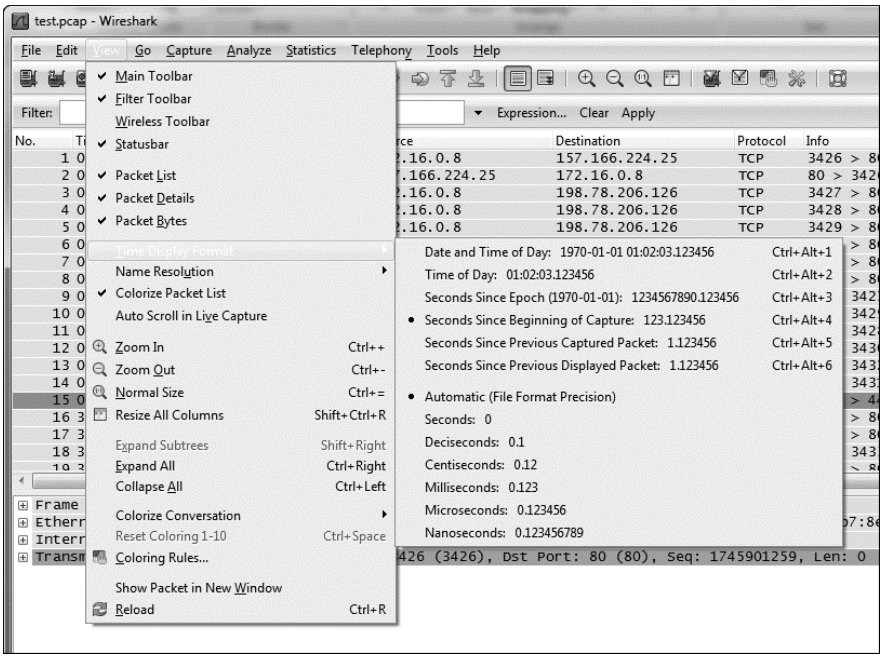
Czas ma istotne znaczenie zwłaszcza podczas przeprowadzania analizy pakietu. Dla wszystkich zdarzeń zachodzących w sieci czas jest ważny, a Twoim zadaniem jest analiza trendów i opóźnień w sieci w niemal każdym pliku zawierającym przechwycone dane. Twórcy narzędzia Wireshark zdają sobie sprawę ze znaczenia 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 bezwzględnego znacznika 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).

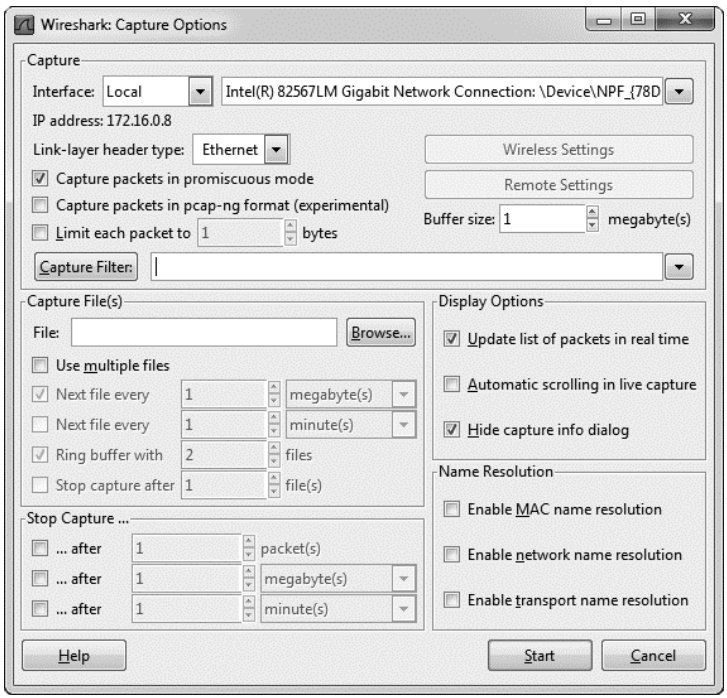
No.	Time	Source	Destination
4	0.118129	172.16.0.8	198.78.206.126
5	*REF*	172.16.0.8	198.78.206.126
6	0.000077	172.16.0.8	198.78.206.126
7	0.000153	172.16.0.8	198.78.206.126

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 wodotrysków, 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.

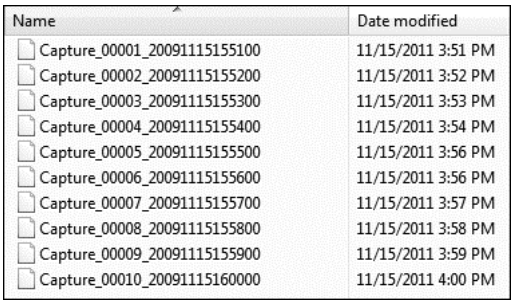
Sekcja Capture File(s)

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 filtru przechwytywania jest zachowanie maksymalnej wydajności działania. Jeżeli wiesz, że nie będziesz analizował określonych form ruchu sieciowego, możesz odfiltrować jego dane za pomocą filtru 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 przyśpieszyć poprzez zagwarantowanie, że patrzysz tylko na te pakiety, które mają związek z rozwiązywanym problemem.

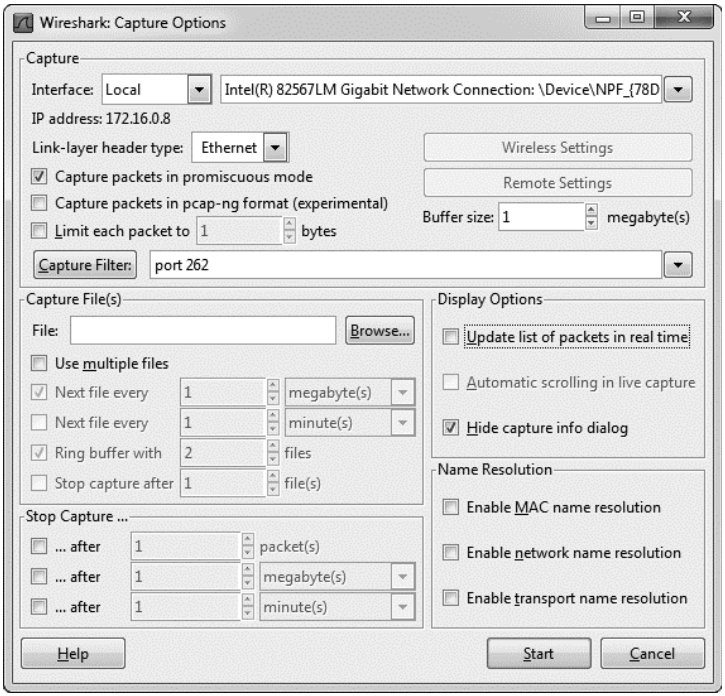
Prosty przykład użycia filtru przechwytywania to sytuacja, w której przechwytujesz ruch z serwera sieciowego o wielu rolach. Przypuśćmy, że rozwiązujesz problem z usługą udostępnianą na porcie 262. Jeżeli analizowany serwer udostępnia także wiele innych usług na różnych portach, to wyszukanie i przeanalizowanie ruchu przepływającego jedynie przez port 262 będzie samo w sobie już wymagającym zadaniem. Aby przechwycić jedynie ruch przepływający przez port 262, możesz użyć filtru 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 filtru 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.



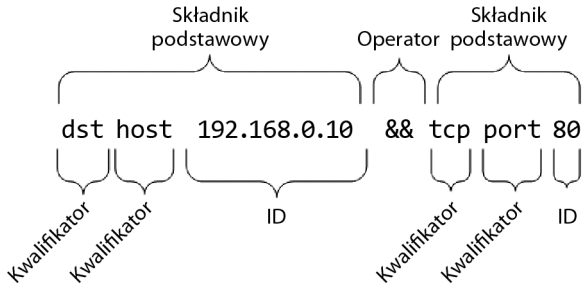
Rysunek 4.10. Zdefiniowanie filtru przechwytywania w oknie dialogowym Capture Options

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 konkatenacji `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 przechwytujący 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 filtru:

```
icmp
```

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

```
!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 `icmp[0]`. Wartością zwrotną będzie jednobajtowa 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 filtru należy użyć operatora równości, co przedstawiono poniżej:

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

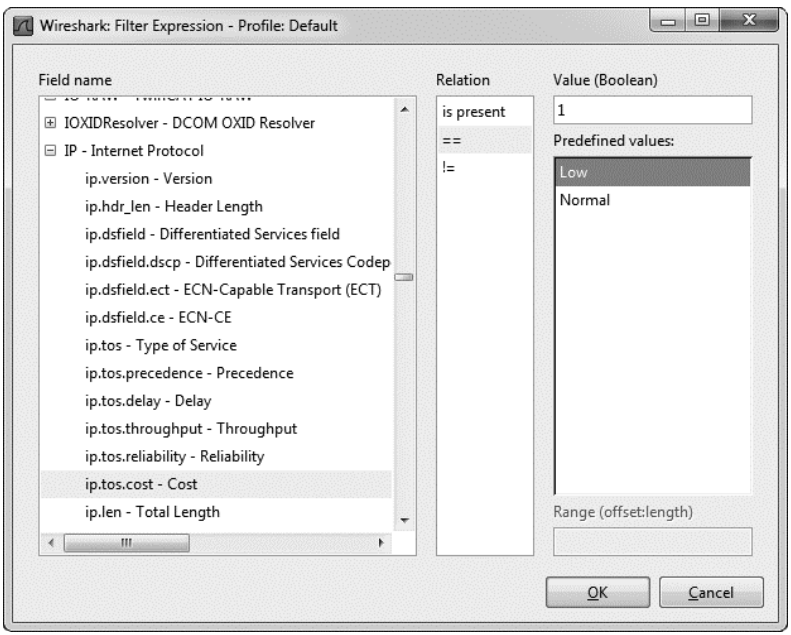
Filtr wyświetlania możesz wykorzystać do ukrycia nieistotnego w danej chwili ruchu sieciowego zebranego w pliku przechwyconych danych. Przykładowo: możesz ukryć ruch pakietów ARP w panelu *Packet List*, kiedy te pakiety nie mają żadnego związku z aktualnie rozwiązywanym problemem. Jednak ponieważ pakiety 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 ze 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

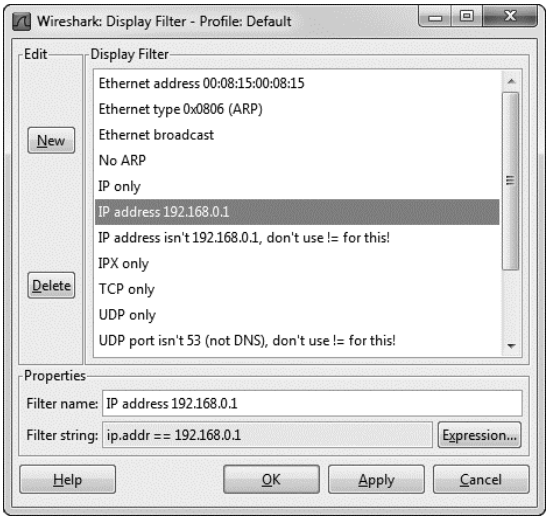
Filtr	Opis
`!tcp.port==3389`	wyłącznie ruch RDP
`tcp.flags.syn==1`	pakiety TCP wraz z ustawioną opcją SYN
`tcp.flags.rst==1`	pakiety TCP wraz z ustawioną opcją RST
`!arp`	wyłącznie ruch ARP
`http`	cały ruch HTTP
`tcp.port==23 || tcp.port 21`	ruch administracyjny w postaci zwykłego tekstu (Telnet lub FTP)
`smtp || pop || imap`	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 wyrażeń filtrów

Skorowidz

C

D

E

F

H

I

J

K

L

M

N

O

P

R

S

T

U

W

Z

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 to 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

sięgnij po WIĘCEJ

KOD KORZYŚCI

no starch press

helion.pl
księgarnia internetowa

Nr katalogowy: 11967

Księgarnia internetowa
http://helion.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

Helion

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

ISBN 978-83-246-5011-8

9 788324 650118

Cena: 59,00 zł