CommView

Network Monitor and Analyzer for MS Windows

Podręcznik użytkownika

Tłumaczenie na język polski Krzysztof Satoła
www.studioinfo.pl

Wstęp

O programie

CommView jest programem do monitorowania aktywności sieciowej zdolnym do przechwytywania i analizowania pakietów danych przepływających przez sieć Ethernet. Zbiera informacje o danych przepływających przez sieć lokalną LAN i dekoduje analizowane dane.

Z pomocą programu CommView można zobaczyć listę połączeń sieciowych, niezbędne statystyki IP, i sprawdzić pojedyncze pakiety. Pakiety IP są deszyfrowane do najniższej warstwy wraz z pełną analizą głównych protokołów IP. Zapewniony jest również pełen dostęp do nieprzetworzonych danych. Przechwycone pakiety mogą być zapisane w plikach logowania w celu poddania ich późniejszej analizie, jak również wyeksportowane do innych formatów. Elastyczny system filtrowania umożliwia odrzucenie niepotrzebnych pakietów, lub przechwytywanie tylko tych pakietów, które są potrzebne i chcesz je przechwycić.

CommView jest pomocnym narzędziem dla administratorów sieci LAN, specjalistów od spraw bezpieczeństwa, programistów piszących oprogramowanie sieciowe, lub dla każdego kto chce mieć pełen obraz ruchu sieciowego przechodzącego przez pojedynczy komputer PC lub segment sieci lokalnej. Ta aplikacja jest zaprojektowana dla małej i średniej wielkości sieci komputerowych i może być uruchomiona na każdym komputerze pracującym pod kontrolą systemu Windows 95/98/Me/NT/2000/XP. Wymaga kart sieciowej Ethernet lub Wireless Ethernet obsługiwanych przez sterowniki zgodne ze standardem NDIS 3.0 lub standardowego interfejsu dial-up (np. modem telefoniczny).

CommView przetwarza następujące protokoły: ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IPsec, IPv4, IPv6, IPX, HSRP, NCP, NDS, NetBIOS, NFS, NLSP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, TCP, TELNET, TFTP, TIME, UDP, VTP, WAP, WDOG, 802.1Q, 802.1X. Obsługa pozostałych protokołów jest tylko kwestią czasu!

Dodatkowo, CommView został wyposażony w możliwość zdalnego przechwytywania pakietów dzięki nowej technologii z każdego komputera z zainstalowanych agentem programu (Remote Agent) niezależnie od jego lokalizacji. Remote Agent wymaga programu CommView i jest jego rozszerzeniem.

Co nowego

Wersja 4.0

- Możliwość ustawiania alarmów związanych z wystąpieniem zdefiniowanych pakietów, adresów MAC i innych zdarzeń.
- Dodano następujące moduły dekodujące: DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q.932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNTP, TIME.
- Wielojęzyczny interfejs.
- Możliwość wykorzystywania dodatkowych modułów dekodujących.
- Nowe parametry pozwalające na automatyczne ładowanie reguł i/lub otwieranie adapterów.
- Okno rekonstrukcji sesji TCP wyposażono w funkcję "Szukaj".
- Szablony pakietów TCP, UDP i ICMP w generatorze pakietów.
- Nowa funkcja "Dekoduj jako" pozwalająca na dekodowanie pakietów przy wykorzystaniu niestandardowych portów.
- Duża ilość nowych opcji konfiguracyjnych.

Wersja 3.4

- Dodano następujące moduły dekodujące: BGP, CDP, EIGRP, IGRP, IPsec, HSRP, NFS, OSPF, RADIUS, RIP, RPC, SNA, VTP, WAP, 802.1Q, 802.1X.
- Możliwość dokonywania podziału oraz łączenia plików CCF.
- Okna rekonstrucji secji TCP pozwalają na przejście do następnej sesji między dwoma hostami.
- Nowe cechy okna statystyk: przełączanie między bitami a bajtami na sekundę, wykorzystanie wskaźnika przepustowości, wykresy związane z protokołem IP wraz z podprotokołami.
- Opcjonalny tryb non-promiscuous.
- Import przechwyconych danych w formatach MS NetMon oraz NAI Sniffer for Windows.
- Podkreślanie składni w oknie zaawansowanej formuły.
- Ulepszone wsparcie dla skór Windows XP.
- Naprawiono ważny błąd w funkcji obsługującej zaawansowane reguły.

Wersja 3.3

- Możliwość tworzenia zaawansowanych filtrów, także z wykorzystaniem arytmetyki Boolean.
- Dodano następujące moduły dekodujące: FTP, TFTP, SOCKS (v. 4,5), TELNET.
- Udoskonalenie szybkości działania.
- Nowe cechy generatora pakietów: wsparcie dla technologii drag-and-drop, duża szybkość generowania pakietów (do 5,000 pakietów/sekundę), możliwość wysyłania wielu różnych pakietów przy pomocy jednego kliknięcia.
- Pliki logów mogą być łączone w jeden duży plik.
- Nowe formaty eksportowania danych: comma-delimited oraz bez danych szesnastkowych.
- Możliwość bezpośredniego zapisu danych (CCF, ENC, itp.) bez potrzeby ładowania ich do przeglądarki logów.
- Tablica hostów LAN może obsłużyć do 1,000 adresów MAC i IP.
- Opcjonalna kolumna "Rozmiar" w liście pakietów.
- Możliwość definiowania adresów IP oraz masek podsieci dla adresów IP, które mają być traktowane jak lokalne.
- Inne mniej ważne usprawnienia.

Wersja 3.2

- Dodano następujące moduły dekodujące: SNMP (v. 1,2,3), IPv6, ICQ, GRE, RDP.
- Pliki otwierane i importowane otwierają się 25 razy szybciej.
- Zmniejszenie wykorzystania jednostki centralnej CPU.
- Rozszerzone statystyki NIC: kolizje i błędy CRC.
- Możliwość aplikowania reguł do danych w przeglądarce logów
- Ulepszone okno wyszukiwania pakietów.

Wersja 3.1

- Dodano następujące moduły dekodujące: DHCP, DNS, HTTP, POP3, RTSP, SMTP.
- Nowa technologia monitoringu.
- Możliwość dodania do 4 różnych protokołów do wykresu podprotokołów IP.
- Możliwość importu plików w formacie Tcpdump (libcap).
- Dodatkowe opcje konfiguracyjne.
- Inne mniej ważne usprawnienia.

Wersja 3.0

- Wspierane protokoły: ARP, BCAST, BMP, DIAG, ICMP, IGMP, IPv4, IPX, NCP, NDS, NetBIOS, NLSP, PPP, PPPoE, RARP, RIPX, RSVP, SAP, SER, SMB, SPX, TCP, UDP, WDOG. Pozostałe już niebawem.
- Wsparcie dla Wireless Ethernet (802.11b).
- Program działa w Windows XP (zgodność z RC1).
- Możliwość wysyłania pakietów przez adapter dial-up w Windows 2000/XP.
- Do generatora pakietów dodano korektor CRC i dekoder protokołów.
- Możliwość uruchomienia kilku instancji programu CommView w celu jednoczesnego monitorowania kilku interfejsów.

- Możliwość dołączenia statystyk IP do raportu.
- Nowa tabela hosty LAN według adresów IP została dodana do statystyk.
- Okno rekonstrukcji sesji TCP pozwala na dołączanie i wyłączanie danych na podstawie kierunku pakietów.
- Możliwość filtrowania pakietów na podstawie flag TCP.
- Program może pracować w "trybie niewidzialnym".
- Możliwość współdzielenia danych programu CommView z inną aplikacją przy pomocy interfejsu TCP/IP.
- Możliwość wyboru wielu pakietów na karcie „Pakiety".

Wersja 2.6

- Do adresów IP można przypisywać aliasy.
- Aktualne reguły mogą być zastosowane w oknie statystyki i w raportach.
- Dekodowanie PPPoE.
- Możliwość otwarcia kilku okien rekonstrukcji sesji TCP.
- Inne mniej ważne usprawnienia.

Wersja 2.5

- Pełne wsparcie dla technologii drag-and-drop.
- W statystykach: wykres rozmiaru dystrybucji pakietów oraz tablica hostów LAN.
- Automatyczne generowanie raportów (HTML, semicolon-delimited).
- Okno rekonstrukcji sesji TCP pozwala na przeglądanie danych jako HTML i EBCDIC oraz ASCII i HEX.

Wersja 2.4

- Odtwarzanie sesji TCP.
- Adresowi MAC można przypisać nazwę (alias) zrozumiałą dla człowieka.
- NIC Vendor Identifier - narzędzie identyfikacji producenta karty na podstawie adresu MAC.
- Więcej kolumn dostępnych na zakładkach "IP Statistics" i "Packets".
- Kolumny na zakładkach "Packets" i "IP Statistics" mogą być ukrywane.
- Dekodowanie pakietów ARP/RARP.
- W regułach odnośnie adresów IP jest możliwe użycie symboli wieloznacznych (np.: *).
- W regułach przechwytywania oprócz opcji "From" (Z) i "To" (Do) dostępna jest opcja "Both" (Obydwa).
- Zakładki z aktywnymi regułami są teraz wyświetlane pogrubioną czcionką.
- Wyświetlanie pakietów może być wstrzymane/wznowione.
- Kilka alternatywnych sposobów wyświetlania statystyk IP.
- Inne mniej ważne usprawnienia.

Wersja 2.3

- Obsługa połączeń dodzwanianych (dial-up) pod Windows 2000.

Wersja 2.2

- Nagłówki MAC, IP, oraz TCP/UDP/ICMP są wyświetlane w różnych kolorach.
- Zawartość zakładki IP Statistics może być zapisana w formacie HTML.
- Dodany Generator Pakietów (Packet Generator) umożliwiający wysyłanie pakietów.
- Konfiguracja reguł użytkownika może zostać zapisana/odczytana.
- W regułach tekstowych rozróżniana jest wielkość liter.
- Poprawione okno dialogowe Find Packet Contents (Znajdź Zawartość Pakietu).
- Usunięcie błędu: problemy z uruchamianiem sterownika na zlokalizowanych wersjach Windows 2000 rozwiązane.

Wersja 2.1

- Podgląd Logu: możesz wczytać i przeglądać pliki logowania tak samo jak dane przechwytywane w czasie rzeczywistym.
- Możliwość importu/eksportu plików logowania z/do formatu programów: NI Observer i NAI Sniffer.
- Numery portów mogą być wyświetlane jako nazwy usług, które z danym numerem portu są skojarzone.
- Nowa funkcja: Jump To (Wykonaj Skok Do): pozwala szybko znaleźć pakiety przychodzące z / wychodzące do podanego adresu IP.
- Kilka usprawnień interfejsu.
- Usunięcie błędu: poprzednie wersje pokazywały niewłaściwą sumę kontrolną UDP.

Wersja 2.01

- Możliwość uruchamiania programu pod Windows 2000.

Wersja 2.0 Final

- Poprawiona wydajność programu pod Windows NT.
- Poprawiono kilka błędów znalezionych w wersji 2.0 Beta.

Wersja 2.0 Beta

- Możliwość uruchamiania programu pod Windows NT.
- Więcej informacji statystycznych.

Wersja 1.0 Final

- Nowe funkcje: Find Packet (Znajdź Pakiet) i Go to Packet Number (Wykonaj Skok Do Pakietu Numer).
- Nowe filtry: przechwytywanie/ignorowanie pakietów w oparciu o adres MAC i kierunek pakietów.
- Statystyki: Wykresy słupkowe Pakiety na sekundę i Bajty na sekundę, wykresy udziału protokołów IP i pod-protokołów.
- Usunięcie błędu: filtr tekstu w wersji 1.0 Beta mógł czasem przechwytywać pakiety niezawierające podanego tekstu.

Umowa licencyjna

Przeczytaj dokładnie następujące warunki i postanowienia przed użyciem tego programu. Użycie tego programu przez Ciebie oznacza, że zgadzasz się z postanowieniami tej umowy licencyjnej. Jeżeli nie zgadzasz się na warunki tej umowy musisz usunąć program ze wszystkich nośników pamięci masowej (tzn. twardego dysku i innych) oraz zaprzestać jego używania.

Prawa autorskie
Ten program jest chroniony prawem autorskim 1999-2003, TamoSoft, Inc. CommView jest znakiem handlowym firmy TamoSoft, Inc. Użycie i prawa autorskie tego programu są regulowane przez międzynarodowe porozumienia o prawach autorskich. TamoSoft, Inc. zachowuje pełen tytuł prawny posiadania i prawa do tego programu i dokumentacji. Przyznanie licencji w żaden sposób nie umniejsza prawa do własności intelektualnej firmie TamoSoft, Inc. Nie wolno rozprowadzać dalej otrzymanych kodów rejestracyjnych, zarówno na papierze, elektronicznie, lub w jakiejkolwiek innej formie.

Wersja próbna
To nie jest bezpłatne oprogramowanie. Jesteś niniejszym upoważniony do używania tego programu w celu poznania jego zalet i zweryfikowania stopnia przydatności, bez opłaty przez okres 30 dni. Używanie tego programu po upływie okresu próbnego jest naruszeniem praw autorskich i może spowodować pociągnięcie do odpowiedzialności cywilnej i karnej – nawet do pełnego wymiaru kary przewidzianego przez prawo.

Wersja zarejestrowana
Jedna zarejestrowana kopia programu może być używana albo przez jedną osobę używającą programu do celów prywatnych na jednym lub kilku komputerach, lub zainstalowana na pojedynczej stacji roboczej używanej niejednocześnie przez większą liczbę użytkowników, ale nie obydwie możliwości razem. Ten program może być zainstalowany na serwerze sieciowym, jednak wymaga to osobnej i odpowiedniej licencji wydanej przez TamoSoft, Inc. dla każdego terminala korzystającego z serwerowej wersji programu.

Zrzeczenie się odpowiedzialności
TEN PROGRAM JEST DOSTARCZONY "TAK JAK JEST" BEZ ŻADNYCH GWARANCJI, ZARÓWNO WYRAŻONYCH WPROST JAK RÓWNIEŻ DOMYŚLNYCH, WŁĄCZAJĄC W TO, ALE NIE OGRANICZAJĄC DO GWARANCJI UŻYWALNOŚCI LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU. W ŻADNYM PRZYPADKU FIRMA TAMOSOFT, INC. NIE JEST ODPOWIEDZIALNA PRZED TOBĄ ZA JAKIEKOLWIEK SZKODY, WŁĄCZAJĄC TO PRZYPADKOWE USZKODZENIA, WYNIKAJĄCE Z UŻYCIA TEGO PROGRAMU, NAWET JEŻELI ZOSTAŁEŚ OSTRZEŻONY O MOŻLIWOŚCI WYSTĄPIENIA TAKICH USZKODZEŃ. POTWIERDZASZ, ŻE PRZECZYTAŁEŚ TĄ UMOWĘ LICENCYJNĄ, ROZUMIESZ JEJ POSTANOWIENIA, I ZGADZASZ SIĘ, BY JEJ POSTANOWIENIA OBOWIĄZYWAŁY CIEBIE.

Nadrzędne prawo
Ta umowa będzie podlegać prawu Republiki Cypru.

Dystrybucja
Ten program może być swobodnie rozprowadzany w postaci niezmodyfikowanej, nie zarejestrowanej wersji instalacyjnej, która powinna zawierać wszystkie oryginalne pliki. Dystrybutorzy nie mogą pobierać pieniędzy za rozprowadzanie programu. Każdy, kto chciałby rozprowadzać ten program za dowolny rodzaj wynagrodzenia musi najpierw skontaktować się z nami w celu uzyskania autoryzacji.

Pozostałe ograniczenia
Nie możesz modyfikować, stosować technik odwrotnej inżynierii oprogramowania, dekompilować lub dzielić na części tego programu w żaden sposób, włączając w to dokonywanie zmian lub usuwanie jakichkolwiek komunikatów czy okienek.

Korzystanie z programu

Przegląd

Interfejs programu składa się z pięciu zakładek, które umożliwiają przeglądanie danych i podjęcie różnych działań na przechwyconych pakietach danych. By rozpocząć przechwytywanie pakietów danych, wybierz interfejs sieciowy z rozwijanej listy na pasku narzędzi, i kliknij na przycisk **Rozpocznij przechwytywanie** lub wybierz polecenie **Plik = > Rozpocznij przechwytywanie** z menu. Jeżeli transmisja pakietów danych odbywa się przez wybrany interfejs sieciowy, CommView zacznie wyświetlać informacje.

Menu Główne

File (Plik)
Start/Stop Capture (Rozpocznij/Zatrzymaj przechwytywanie) – zaczyna/zatrzymuje przechwytywanie pakietów.
Suspend/Resume Packet Output (Zawieś/Wznów wyświetlanie pakietów) – zatrzymuje/wznawia wyświetlanie w czasie rzeczywistym przechwytywanych pakietów na drugiej zakładce.
Remote Monitoring Mode (Tryb zdalnego monitorowania) – ukazuje/ukrywa pasek zdalnego monitoringu.
Save IP Statistics As (Zapisz statystyki IP jako) – pozwala zapisać zawartość zakładki IP Statistics (Statystyki IP) w postaci raportu HTML.
Save Packet Log As (Zapisz log pakietu jako) – pozwala zapisać zawartość zakładki Packets (Pakiety) w różnych formatach. Użyj zakładki Logging (Logowanie) do ustawienia bardziej zaawansowanych opcji zapisywania.
Log Viewer (Przeglądarka logów) – otwiera nowe okno Przeglądarki logów.
Clear IP Statistics (Wyczyść statystyki IP) – czyści tabelę IP Statistics (Statystyki IP) na pierwszej zakładce.
Clear Packet Buffer (Wyczyść bufor pakietów) – czyści zawartość bufora programu i listę pakietów na drugiej zakładce.
Performance Data (Osiągi) – wyświetla statystykę wydajności programu: liczbę pakietów przechwyconych i utraconych przez sterownik urządzenia. To polecenie jest niedostępne pod Windows 95/98/Me.
Exit (Wyjście) – zamyka program.

Search (Szukaj)
Find Packet (Znajdź pakiet) – pokazuje okno dialogowe, które umożliwia odnalezienie pakietów zawierających określony tekst.
Go to Packet Number (Idź do pakietu numer) - pokazuje okno dialogowe, które pozwala na wykonanie skoku do pakietu o podanym numerze.

View (Przeglądaj)
Statistics (Statystyki) – pokazuje okno zawierające statystykę przesyłania danych i udziału protokołów IP i podprotokołów IP.
Port Reference (Informacje o portach) – pokazuje okno zawierające nazwy usług wraz ze skojarzonymi numerami portów.
Log Directory (Katalog logów) – otwiera katalog, w którym domyślnie są zapisywane logi.
IP Statistics Columns (Kolumny statystyk IP) – pokazuje/ukrywa kolumny na zakładce IP Statistics (Statystyka IP).
Packets Columns (Kolumny pakietów) – pokazuje/ukrywa kolumny na zakładce Packets (Pakiety).

Tools (Narzędzia)
Packet Generator (Generator pakietów) – otwiera okno generatora pakietów (niedostępne w Windows 95/98/Me).
Reconstruct TCP Session (Zrekonstruuj sesję TCP) – pozwala na odtworzenie sesji TCP zaczynając od wybranego pakietu; otwiera okno, które wyświetla całą "konwersację" między dwoma komputerami.
NIC Vendor Identifier (Identyfikator dostawcy NIC) – otwiera okno, gdzie można zidentyfikować producenta karty sieciowej używając do tego celu jej adresu MAC.
Scheduler (Harmonogram) – pozwala na zarządzanie zadaniami w czasie.

Settings (Ustawienia)
Fonts (Czcionki) – pokazuje podmenu służące do wybierania czcionki dla elementów interfejsu.
MAC Aliases (Aliasy MAC) – przywołuje okno gdzie możesz przypisać łatwe do zapamiętania aliasy do adresów MAC.
IP Aliases (Aliasy IP) – przywołuje okno gdzie możesz przypisać łatwe do zapamiętania aliasy do adresów IP.
Options (Opcje) – przywołuje okno Options (Opcje), gdzie można dokonać dodatkowej konfiguracji zaawansowanych opcji programu.
Language (Język) – pozwala na zmianę języka interfejsu. Zmiany odnoszą skutek po ponownym uruchomieniu programu.
Install dial-up driver (Zainstaluj sterownik dial-up) – pojawia się, gdy sterownik dial-up nie został zainstalowany podczas instalacji programu.

Rules (Reguły)
Save Current Rules As (Zapisz obecne reguły jako) – pozwala na zapisanie obecnej konfiguracji reguł do pliku.
Load Rules From (Załaduj reguły z) – pozwala na wczytanie wcześniej zapisanej konfiguracji reguł z pliku.
Reset All (Resetuj wszystko) – wymazuje wszystkie istniejące reguły, jeżeli jakiekolwiek są ustawione.

Help (Pomoc)
Contents (Zawartość) – uruchamia pomoc odnośnie składników programu CommView.
Search For Help On ... (Szukaj pomocy w) – umożliwia wyszukiwanie tematu pomocy.
About (O programie) – wyświetla informacje o programie.

Prawie każdy element interfejsu posiada swoje własne kontekstowe menu, które może być przywołane poprzez kliknięcie prawym klawiszem myszki. Wiele poleceń jest dostępnych tylko przez takie kontekstowe menu.

Pierwsza zakładka jest wykorzystywana do wyświetlania szczegółowych informacji o połączeniach sieciowych Twojego komputera (tylko protokoły IP). W celu uzyskania dalszych informacji zajrzyj tutaj – Statystyki IP.

Druga zakładka używana jest do przeglądania przechwyconych pakietów sieciowych i wyświetlania szczegółowych informacji na temat wybranego pakietu. Więcej informacji uzyskasz zaglądając tutaj – Pakiety.

Trzecia zakładka umożliwia zapisanie przechwyconych pakietów do pliku. Więcej informacji znajdziesz tutaj – Logowanie.

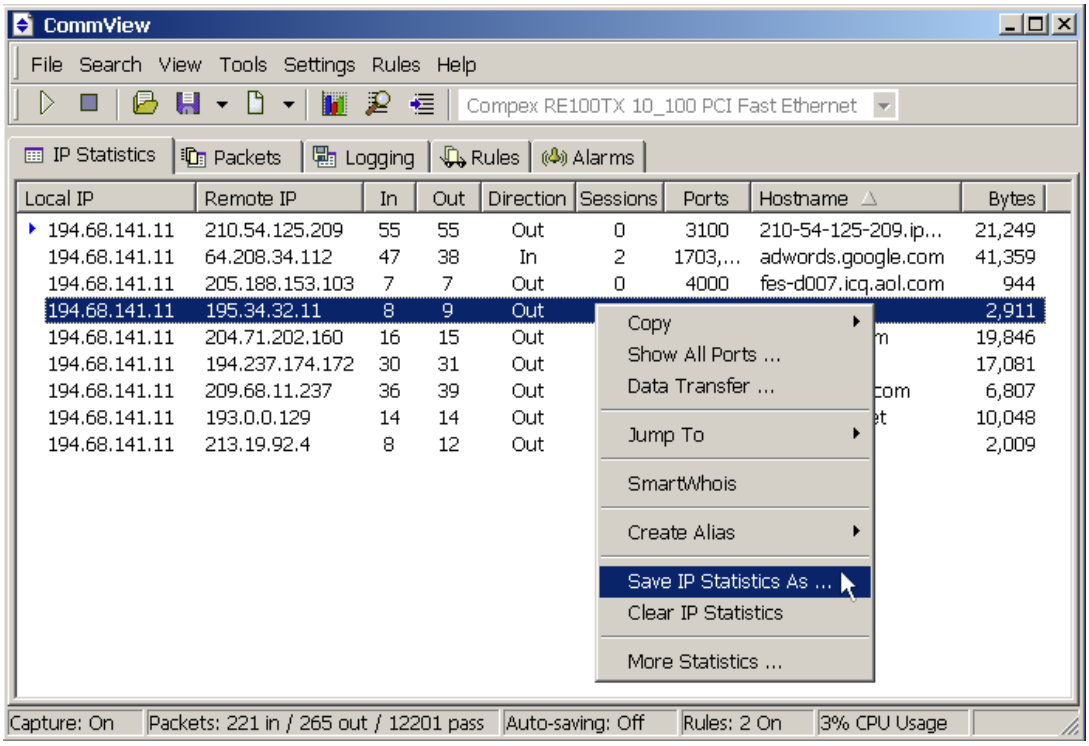
Czwarta zakładka służy do konfiguracji reguł, które umożliwiają przechwycenie/zignorowanie pakietów na podstawie różnych kryteriów, takich jak adres IP czy numer portu. Chcesz uzyskać więcej informacji – przejrzyj temat Reguły.

The fifth tab allows you to create alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, etc. For more information see Alarms.

Możesz zmienić niektóre ustawienia, takie jak czcionki, kolory, i rozmiar bufora wybierając polecenie Settings (Ustawienia) z menu. Chcesz uzyskać więcej informacji – przeczytaj temat Ustawianie opcji.

Statystyki IP

Ta zakładka jest używana do wyświetlania szczegółowych informacji odnośnie połączeń sieciowych Twojego komputera (tylko protokół IP). By rozpocząć przechwytywanie pakietów, wybierz polecenie **File (Plik) = > Start Capturing (Rozpocznij Przechwytywanie)** z menu, lub kliknij na odpowiedni przycisk na pasku narzędzi.



Znaczenie poszczególnych kolumn w tej zakładce jest wyjaśnione poniżej:

Local IP (Lokalny IP) – pokazuje lokalny adres IP. Dla pakietów przychodzących jest to docelowy adres IP, dla pakietów wychodzących i przechodzących jest to źródłowy adres IP.
Remote IP (Zdalny IP) – pokazuje zdalny adres IP. Dla pakietów przychodzących jest to źródłowy adres IP, dla pakietów wychodzących i przechodzących jest to docelowy adres IP.
In (Do) – pokazuje liczbę odebranych pakietów.
Out (Od) – pokazuje liczbę wysłanych pakietów.
Direction (Kierunek) – pokazuje kierunek sesji. Kierunek ten jest określany w oparciu o kierunek pierwszego pakietu otrzymanego lub wysłanego na zdalny adres IP.
Sessions (Sesje) – pokazuje liczbę zestawionych sesji TCP/IP. Jeżeli nie ma żadnych połączeń TCP (połączenia zerwane, albo protokołem jest UDP/IP lub ICMP/IP) ta liczba przyjmuje wartość zero.
Ports (Porty) – wyświetla listę portów zdalnego komputera użytych podczas połączenia TCP/IP lub próby takiego połączenia. Ta lista może być pusta, jeżeli użytym protokołem nie był TCP/IP. Porty mogą być wyświetlane albo jako wartości numeryczne, lub jako nazwy odpowiednich usług sieciowych. By uzyskać więcej informacji zajrzyj tutaj Ustawianie opcji.
Hostname (Nazwa komputera) – pokazuje nazwę zdalnego komputera. Jeżeli niemożliwe jest przetłumaczenie adresu IP na nazwę hosta, ta kolumna będzie pusta.
Bytes (Bajty) – liczba bajtów przesłanych podczas sesji.
Last packet (Ostatni pakiet) – wyświetla czas wysłania/odbioru ostatniego pakietu podczas danej sesji.

Można pokazywać lub ukrywać pojedyncze kolumny, klikając odpowiednią pozycję w menu **View (Widok) => IP Statistics Columns (Kolumny Statystyki IP)**.

Menu Commands (Polecenia menu)

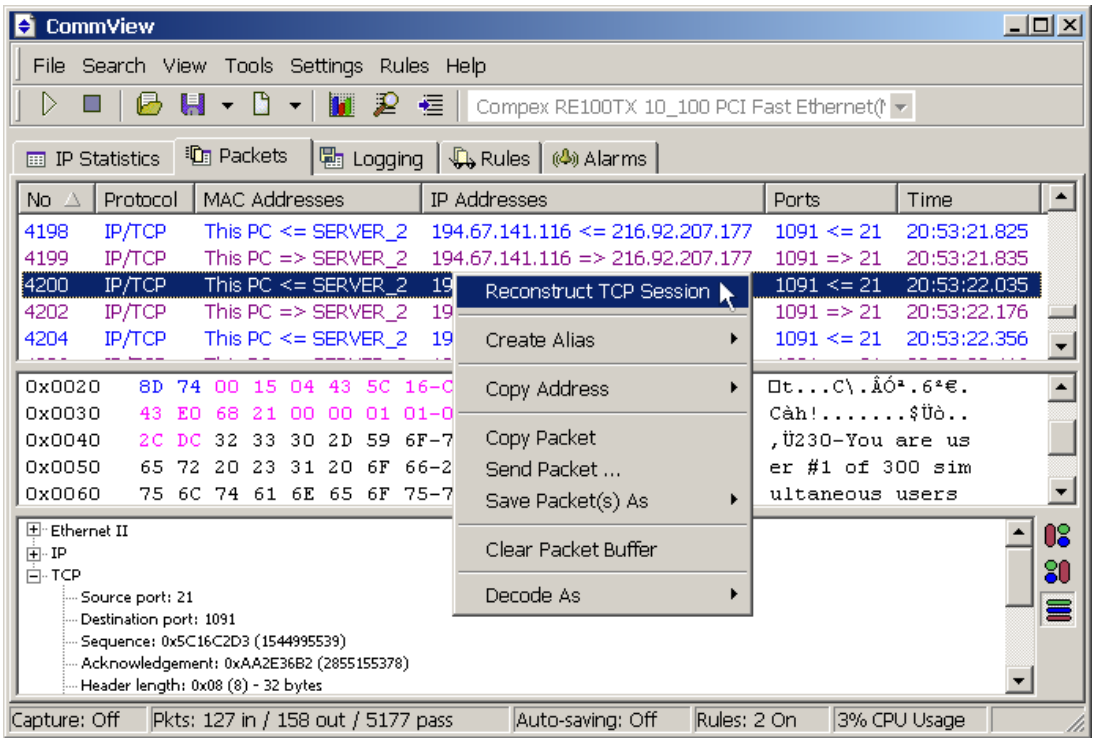
Kliknięcie prawym klawiszem myszki na liście w zakładce IP Statistics (Statystyki IP) wyświetli menu zawierające następujące polecenia:

Copy (Kopiuj) – kopiuje lokalny adres IP, zdalny adres IP, lub nazwę komputera do schowka.
Show All Ports (Pokaż wszystkie porty) – wyświetla okno z kompletną listą portów używanych w komunikacji pomiędzy wybraną parą adresów IP. Jest to przydatne, kiedy użytych było wiele portów i nie mieszczą się one w odpowiedniej kolumnie.
Data Transfer (Transfer danych) – wyświetla okienko zawierające informacje odnośnie wielkości transferu danych pomiędzy wybraną parą adresów IP i czasu wysłania/odbioru ostatniego pakietu.
Jump To (Skocz do) – pozwala na szybki skok do pierwszego/ostatniego pakietu z wybranego, źródłowego/docelowego adresu IP; program wyświetli zakładkę Packets (Pakiety) i ustawi kursor myszki na pakiecie, który pasuje do kryterium.

SmartWhois – wysyła wybrany adres zdalny adres IP do programu SmartWhois, jeżeli jest on zainstalowany na Twoim komputerze. SmartWhois jest samodzielną aplikacją stworzoną i rozwijaną przez naszą firmę, która jest zdolna do uzyskania informacji o dowolnym adresie IP lub komputerze na świecie. Automatycznie podaje informacje związane z adresem IP, takie jak domena, nazwa sieci, kraj, stan lub prowincja, miasto. Program może być pobrany z naszego serwisu WWW.
Create Alias (Utwórz alias) – otwiera okno aliasów umożliwiające przyporządkowanie nazw do adresów IP.
Save IP Statistics As (Zapisz statystyki IP jako) – pozwala na zapisanie zawartości zakładki IP Statistics (Statystyka IP) w posataci raportu HTML.
Clear IP Statistics (Wyczyść statystyki IP) – czyści tabelę.
More Statistics (Więcej statystyk) – pokazuje okno statystyki transferu danych i udziału protokołów sieciowych.

Pakiety

Ta zakładka jest używana do wyświetlania listy wszystkich przechwyconych pakietów sieciowych oraz szczegółowych informacji o wybranym pakiecie.



Górny panel wyświetla listę przechwyconych pakietów. Użyj tej listy, by wybrać pakiet, który chcesz wyświetlić i przeanalizować. Kiedy wybierzesz pakiet klikając na nim, pozostałe panele pokazują informacje odnośnie tego wybranego pakietu.

Znaczenie poszczególnych kolumn w tabeli jest wyjaśnione poniżej:

No (Numer) – unikalny numer pakietu. Jeżeli program CommView filtruje pakiety używając danych z zakładki Rules (Reguły), niektóre z pakietów nie będą przechwycone, ale wciąż będą logowane. Więc, możesz zauważyć, że pakiety nie pojawiają się w porządku sekwencyjnym, tzn. ponumerowane kolejnymi liczbami od najmniejszej do największej.

Protocol (Protokół) – pokazuje nazwę protokołu danego pakietu.

MAC Addresses (Adresy MAC) – pokazuje źródłowy i docelowy adres MAC i kierunek pakietu.

Przykłady:

22:22:22:22:22:22 => 33:33:33:33:33:33 jest pakietem wychodzącym z 22:22:22:22:22:22 do 33:33:33:33:33:33.

22:22:22:22:22:22 <= 33:33:33:33:33:33 jest pakietem przychodzącym z 33:33:33:33:33:33 do 22:22:22:22:22:22.

44:44:44:44:44:44 <=> 55:55:55:55:55:55 jest pakietem przechodzącym z 44:44:44:44:44:44 do 55:55:55:55:55:55.

55:55:55:55:55:55 <=> 44:44:44:44:44:44 jest pakietem przechodzącym 55:55:55:55:55:55 do 44:44:44:44:44:44.

IP Addresses (Adresy IP) – pokazuje źródłowe i docelowe adresy IP (odpowiednio do sytuacji) i kierunek pakietu.
Ports (Porty) – pokazuje źródłowe i docelowe porty (odpowiednio do sytuacji) i kierunek pakietu. Porty mogą być wyświetlane albo jako wartości numeryczne, lub jako odpowiadające numerom portów nazwy usług sieciowych. Po więcej informacji – przejrzyj temat Ustawianie opcji.
Time/Delta (Czas/Czas Delta) – pokazuje czas pakietu – absolutny lub delta. Czas delta jest różnicą pomiędzy czasem absolutnym dwóch ostatnich pakietów. Można przełączać pomiędzy czasem absolutnym i czasem delta poprzez kliknięcie **View (Widok) => Packets Columns (Kolumny pakietów) => Show Time As (Pokaż czas jako)**.
Size (Rozmiar) – pokazuje wielkość pakietów w bajtach. Kolumna nie jest widoczna domyślnie.

Pojedyncze kolumny mogą być pokazane lub ukryte poprzez kliknięcie odpowiedniej pozycji na liście w menu **View (Widok) => Packets Columns (Kolumny pakietów)**. Wyświetlanie przechwyconych pakietów może być wstrzymane poprzez kliknięcie **File (Plik) => Suspend Packet Output (Wstrzymaj wyświetlanie pakietów)**. W trybie wstrzymanego wyświetlania, pakiety są przechwytywane, ale nie są wyświetlane na zakładce Packets (Pakiety). Ten tryb jest przydatny wtedy, gdy jesteś zainteresowany tylko statystyką połączenia zamiast pojedynczymi pakietami. By wznowić wyświetlanie pakietów w czasie rzeczywistym kliknij **File (Plik) => Resume Packet Output (Wznów wyświetlanie pakietów)**.

Środkowy panel wyświetla nieprzetworzoną, surową zawartość pakietów, zarówno w notacji szesnastkowej i jako czysty tekst. W części tekstowej niedrukowalne znaki są zastąpione kropkami.

Dolny panel wyświetla rozszyfrowane informacje o pakiecie, jeżeli jest to pakiet IP. Te informacje zawierają istotne dane, które mogą być wykorzystane przez specjalistów od sieci. Kliknij prawym, aby przywołać menu kontekstowe pozwalające na wykonywanie operacji na węzłach. Można też zmieniać pozycję okna dekodera klikając jeden z trzech przycisków znajdujących się na dole po stronie prawej.

Polecenia menu kontekstowego

Kliknięcie prawym klawiszem myszki na liście pakietów spowoduje pojawienie się menu zawierającego następujące polecenia:

Reconstruct TCP Session (Zrekonstruuj sesję TCP) – pozwala odtworzyć sesję TCP zaczynając od wybranego pakietu; otwiera okno, które wyświetla pełną "konwersację", która miała miejsce pomiędzy dwoma komputerami.
Create Alias (Utwórz alias) – pokazuje okienko przy pomocy, którego możesz przypisać łatwe do zapamiętania aliasy dla wybranego adresu MAC.
Copy Address (Kopiuj adres) – kopiuje źródłowy adres MAC, docelowy adres MAC, źródłowy lub docelowy adres IP do schowka systemowego.
Copy Packet (Kopiuj pakiet) – kopiuje nieobrobione dane wybranego pakietu do schowka systemowego.
Send Packet (Wyślij pakiet(y)) – pokazuje okno generatora pakietów, które pozwala na ponowne wysłanie wybranego pakietu. Istnieje możliwość modyfikacji pakietu przed wysłaniem go.
Save Packet(s) As (Zapisz pakiety jako) – zapisuje zawartość wybranych pakietów do pliku. Pakiet można zapisać albo w pliku binarnym, lub jako sformatowany tekst wraz z informacjami dodatkowymi. Jeżeli wybrana zostanie druga możliwość, plik będzie zawierał informacje wyświetlane na środkowym panelu.
Clear Packet Buffer (Wyczyść bufor pakietów) – czyści bufor programu, usuwa wszystkie zawarte w nim pakiety. Lista pakietów będzie wyzerowana, więc nie będziesz mógł przejrzeć pakietów poprzednio przechwyconych przez program.
Decode As (Dekoduj jako) – dla pakietów TCP i UDP. Opcja pozwala na dekodowanie wspieranych protokołów wykorzystujących porty niestandardowe. Na przykład, gdy twój serwer SOCKS operuje na porcie 333 zamiast na 1080, możesz wybrać pakiet należący do sesji SOCKS i wykorzystać tę opcję do zdekodowania pakietów tak jakby były to pakiety SOCKS 1080, a nie na porcie 333. Takie przekierowanie funkcjonuje do czasu wyjścia z programu. CommView nie pozwoli na dokonywanie podobnych operacji na parze dwóch standardowych portów (np. nie można dekodować pakietów na porcie 80 jako pakietów TELNET).

Można też przeciągać pakiety na pulpit metodą drag-and-drop.

Logowanie

Ta zakładka służy do zapisywania przechwyconych pakietów do pliku na dysku. CommView zapisuje pakiety w swoim własnym formacie CCF (CommView Capture Files). W każdej chwili możesz otworzyć i przeglądać te pliki używając przeglądarki logów, lub po prostu dwukrotnie kliknąć na dowolnym pliku CCF, by wczytać go.

Save Log (Zapisz log)

Użyj tej ramki, by ręcznie zapisać przechwycone pakiety do pliku. Można zapisać wszystkie pakiety obecnie przechowywane w buforze, lub tylko część z nich, z podanego zakresu. Pola To (Do) i From (Od) pozwalają na podanie niezbędnych granic zakresu, w oparciu o numerację pakietów wyświetlaną na zakładce Packets (Pakiety). Kliknij **Save As (Zapisz jako)**, by wybrać nazwę pliku.

Auto-saving (Automatyczne zapisywanie)

Zaznacz tą opcję, by program automatycznie zapisywał przechwycone pakiety zaraz po ich przybyciu. Użyj pola Maximum directory size (Maksymalny rozmiar katalogu), by ograniczyć całkowity rozmiar plików CCF przechowywanych w Log Directory (Katalogu logowania). Jeżeli całkowity rozmiar plików CCF przekracza ustalony limit przestrzeni dyskowej, program automatycznie usuwa najstarsze pliki w katalogu. By zmienić domyślny Log Directory (Katalog logowania), kliknij na opcji Save files to (Zapisuj pliki w) i wybierz inny folder. Pakiety zapisywane są porcjami po 500 pakietów w pliku. Jeśli potrzebujesz mieć wszystkie pakiety w jednym pliku, zaznacz opcję **Concatenate files when capturing is stopped (Połącz logi gdy przechwytywanie zostanie zatrzymane)**. Zaznaczenie tej opcji spowoduje, że program, po zakończeniu przechwytywania, utworzy jeden plik wynikowy.

Plik logu zawierający 500 pakietów ma w przybliżeniu rozmiar 500 kilobajtów.

WAŻNE: Jeżeli chcesz przechowywać pliki logowania przez długi okres czasu, nie trzymaj ich w domyślnym katalogu logowania: istnieje szansa, że będą automatycznie usuwane w momencie zapisywania nowych plików. Przenieś pliki do innego folderu, by je zabezpieczyć przed usunięciem i w ten sposób zachować w stanie nienaruszonym na dłużej.

UWAGA: Program nie zapisuje oddzielnie każdego pakietu natychmiast po nadejściu. Pakiety są zapisywane w partiach, po 500 pakietów każda. To znaczy, że jeżeli przeglądasz plik logowania w czasie rzeczywistym, może on nie zawierać ostatnich 500 pakietów. By spowodować, by program natychmiast zapisał zawartość bufora do pliku logowania, albo kliknij **Stop Capture (Zatrzymaj przechwytywanie)**, lub odznacz opcję **Auto-saving (Automatyczne zapisywanie)**.

Log Management (Zarządzanie logami)

Wykorzystaj tę ramkę do łączenia plików CCF w jeden większy. W tym celu kliknij **Concatenate Logs (Połącz logi)**. Aby podzielić większy plik CCF na mniejsze kliknij **Split Logs (Podziel logi)**. Program poprowadzi cię przez proces odpowiednio łączenia lub dzielenia plików.

Przeglądanie logów

Przeglądarka logów (Log Viewer) jest narzędziem przeznaczonym do przeglądania i przeszukiwania plików logowania, zawierających przechwycone pakiety zapisanych przez program CommView i kilka innych analizatorów pakietów. Posiada taki sam zestaw dostępnych funkcji jak zakładka Packets (Pakiety) z głównego okna programu, lecz w odróżnieniu od niej, Przeglądarka logów wyświetla pakiety wczytane z plików zgromadzonych na dysku zamiast pakietów przechwytywanych w czasie rzeczywistym.

By otworzyć Przeglądarkę logów, kliknij **File (Plik) => Log Viewer (Przeglądarka logów)** w głównym menu programu, lub po prostu podwójnie kliknij na dowolnym pliku logowania, zawierających przechwycone pakiety, które wcześniej zostały zapisane na dysku. Możesz otworzyć tak dużo okien Przeglądarki logów ile tylko chcesz, i dokładnie każde z nich może być użyte do przeszukiwania jednego lub kilku plików logowania.

Przeglądarka logów może być użyta do przeglądania i przeszukiwania plików logowania, zawierających przechwycone pakiety zapisane przez inne analizatory pakietów i osobiste zapory ogniowe. Obecna wersja programu potrafi importować pliki w formatach programów: Network Instruments Observer®, Network Associates Sniffer® for DOS/Windows, Microsoft NetMon i Tcpdump (libcap). Te formaty zapisu są również używane przez pewną liczbę aplikacji firm trzecich. Przeglądarka logów potrafi eksportować dane pakietów, posiadając możliwość zapisywania plików w formacie programów: Network Instruments Observer® i Network Associates Sniffer® for DOS, jak również w swoim własnym formacie zapisu.

Używanie Przeglądarki logów jest podobne do używania zakładki Packets (Pakiety) w głównym oknie; zajrzyj do rozdziału pakiety, jeżeli potrzebujesz szczegółowych informacji.

Menu Przeglądarki logów

File (Plik)
Load CommView Logs (Załaduj logi CommView) – otwiera i odczytuje z dysku jeden lub kilka plików logowania.
Import Logs (Importuj logi) – pozwala na import plików logowania zapisane przez inne analizatory pakietów.
Export Logs (Eksportuj logi) – pozwala na eksport wyświetlonych pakietów do plików logowania w kilku formatach.
Clear Window (Wyczyść okno) – czyści listę pakietów.
Close Window (Zamknij okno) – zamyka okno Przeglądarki logów.

Search (Szukaj)
Find Packet (Znajdź pakiet) – pokazuje okno dialogowe, które pozwala odnaleźć pakiety zawierające pewien tekst.
Go to Packet Number (Idź do pakietu numer) – pokazuje okno dialogowe, które umożliwia wykonanie skoku do pakietu posiadającego podany numer.

Rules (Reguły)
Apply (Zastosuj) – stosuje reguły to pakietów wyświetlanych przez Przeglądarkę logów. Wynikiem tego może być zmazanie pakietów niespełniających wymagań zdefiniowanych przez zdefiniowany zestaw reguł. Plik źródłowy na dysku nie jest modyfikowany.
From File (Z pliku) – działanie podobne jak **Apply (Zastosuj)**, ale zestaw reguł może być załadowany z wcześniej przygotowanego pliku RLS.

Reguły

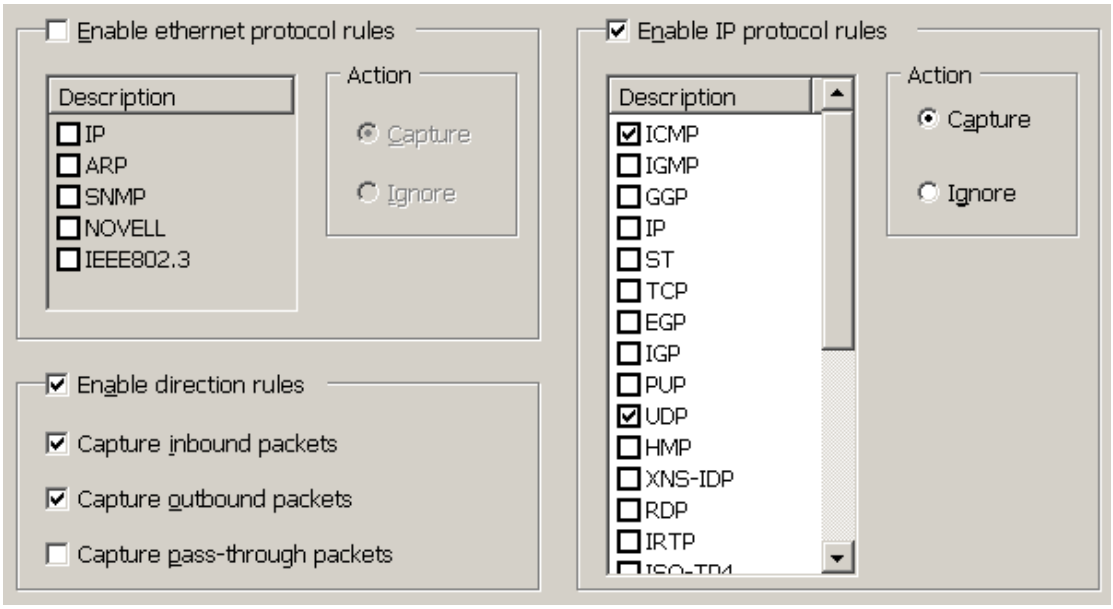
Ta zakładka pozwala na ustalenie reguł, według których będą przechwytywane pakiety. Jeżeli jest zdefiniowana jedna lub więcej reguł, program filtruje pakiety używając tychże reguł i wyświetla tylko te pakiety, które spełniają warunki zdefiniowane w regułach. Uwaga: CommView nie jest firewallem (zaporą ogniową), więc nawet wtedy, kiedy zdefiniowałeś reguły filtrowania pakietów, system operacyjny wciąż przetwarza wszystkie pakiety danych, natomiast nie wszystkie są wyświetlane i zapisywane przez program CommView. Jeżeli zestaw reguł jest aktywny, nazwa odpowiedniej zakładki jest wyświetlana pogrubioną czcionką.

Możesz zapisać konfiguracje swoich reguł filtrowania do pliku i potem wczytać je używając polecenia **Rules (Reguły)** z menu programu.

Ponieważ ruch w sieci LAN potrafi wygenerować dużą liczbę pakietów, zalecane jest użycie reguł w celu odfiltrowania zbędnych pakietów. To może znacznie zmniejszyć ilość zasobów systemowych zajmowanych przez program. Jeżeli chcesz włączyć/wyłączyć regułę, wybierz właściwą zakładkę z lewej strony okna Reguły, na przykład **IP Addresses (Adresy IP)** lub **Ports (Porty)**, i zaznacz lub odznacz opcję opisującą regułę **Enable IP Address rules (Włącz reguły adresów IP)** lub **Enable port rules (Włącz reguły dotyczące portów)**. Jest sześć rodzajów reguł zdefiniowanych oraz reguły zaawansowane (razem siedem rodzajów), które mogą być użyte:

Kierunek protokołów

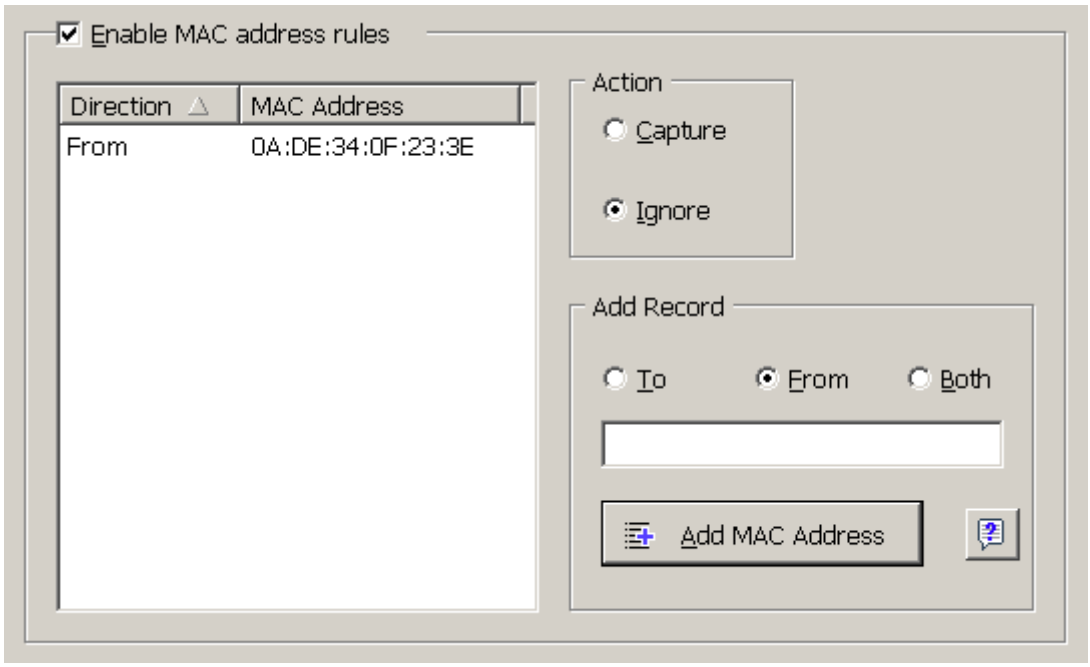
Pozwala na ignorowanie lub przechwytywanie pakietów w oparciu o protokoły: Ethernet (Warstwa 2) i IP (Warstwa 3), jak również na podstawie kierunku pakietu.



Ten przykład pokazuje jak spowodować, by program przechwytywał tylko przychodzące i wychodzące pakiety protokołów ICMP oraz UDP. Wszystkie pakiety pozostałych protokołów z rodziny IP będą ignorowane, wszystkie pakiety przechodzące będą również ignorowane.

Adresy MAC

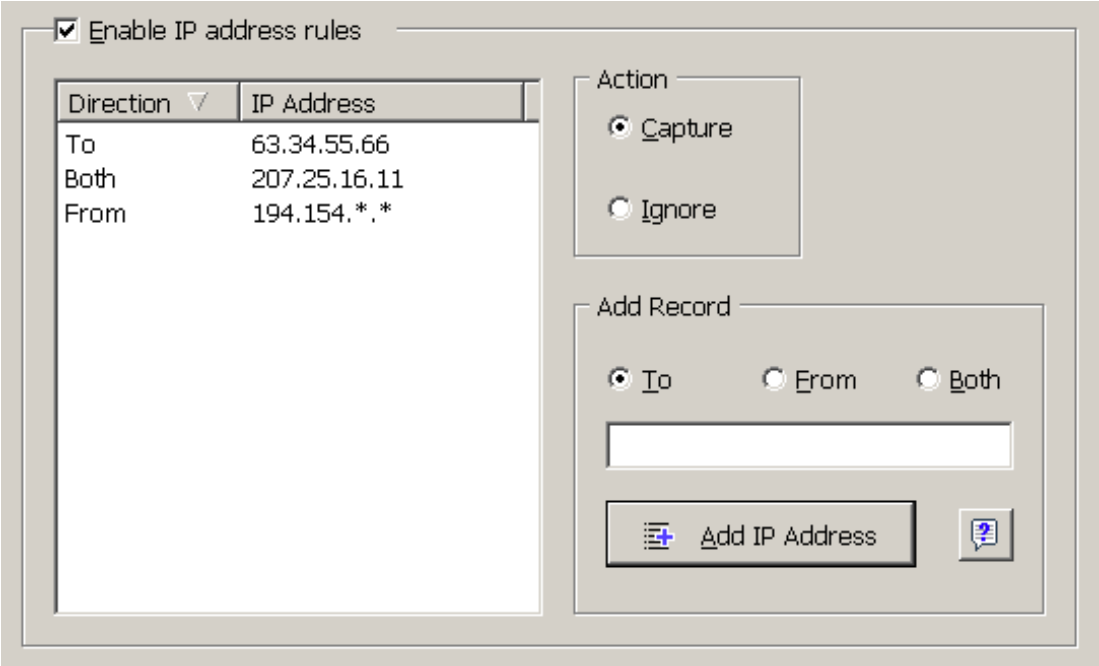
Pozwala na ignorowanie lub przechwytywanie pakietów na podstawie adresu MAC (adresu sprzętowego karty sieciowej). Podaj adres MAC w ramce Add Record (Dodaj Rekord), wybierz kierunek – **From (Przychodzący), To (Wychodzący), lub Both (Oba)**, i kliknij **Add MAC Address (Dodaj Adres MAC)**. Nowa reguła zostanie wyświetlona. Teraz możesz wybrać akcję, jaka zostanie podjęta podczas przetwarzania nowego pakietu: pakiet może być przechwycony lub zignorowany. Możesz też kliknąć MAC Aliases (Aliasy MAC), aby zobaczyć listę zdefiniowanych aliasów (taki przycisk z dymkiem i pytajnikiem obok dużego przycisku Dodaj adres MAC).



Ten przykład pokazuje jak spowodować, by program ignorował pakiety, które pochodzą z adresu: 0A:DE:34:0F:23:3E. Wszystkie pakiety, które pochodzą z innych adresów MAC będą przechwytywane.

Adresy IP

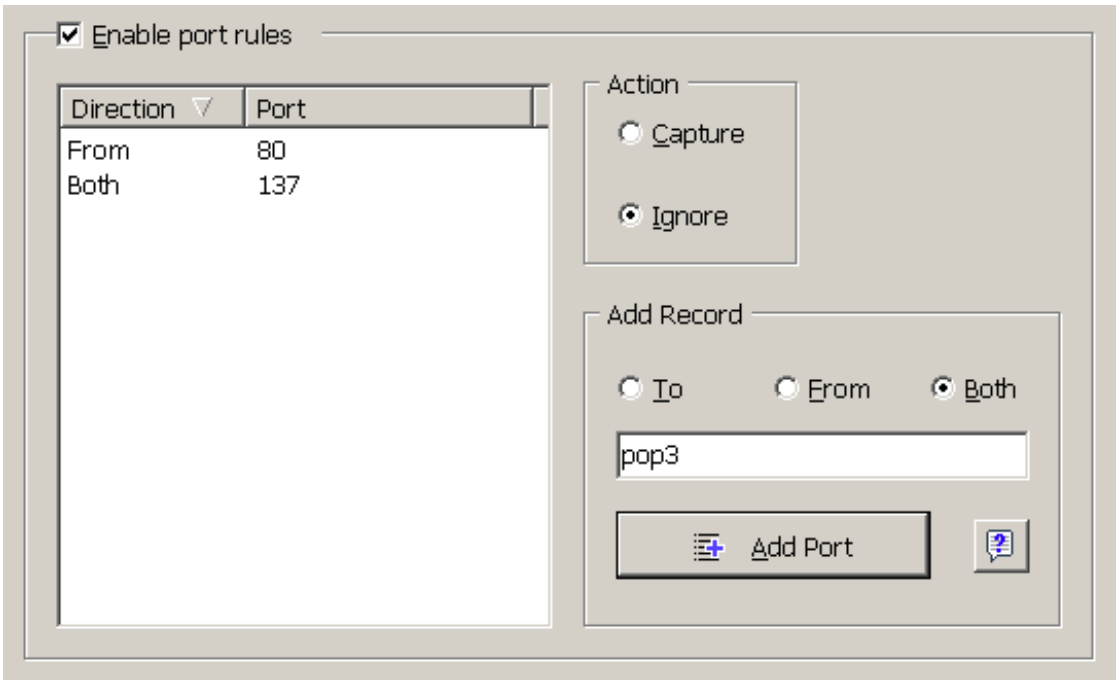
Pozwala na ignorowanie lub przechwytywanie pakietów w oparciu o adresy IP. Podaj adres IP w ramce **Add Record (Dodaj rekord)**, wybierz kierunek **From (Przychodzący), To (Wychodzący),** lub **Both (Oba)**, i kliknij **Add IP Address (Dodaj adres IP)**. Możesz użyć symboli wieloznacznych w celu określenia zakresu adresów IP. Nowa reguła zostanie wyświetlona. Teraz możesz wybrać akcję, jaka zostanie podjęta podczas przetwarzania nowego pakietu: pakiet może być przechwycony lub zignorowany. Możesz też wykorzystać listę aliasów (klikając mały przycisk obok dużego przycisku Dodaj adres IP) w celu wprowadzenia nowego adresu IP.



Ten przykład pokazuje jak spowodować, by program przechwytywał pakiety, które podążają na adres 63.34.55.66, przychodzą i wychodzą z adresu 207.25.16.11 i przychodzą ze wszystkich adresów z zakresu od 194.154.0.0 do 194.154.255.255. Wszystkie pakiety, które pochodzą z innych adresów lub są przeznaczone dla innych adresów będą ignorowane. Ponieważ adresy IP są używane w protokole IP, taka konfiguracja automatycznie spowoduje ignorowanie przez program wszystkich pakietów nie będących pakietami protokołu IP.

Porty

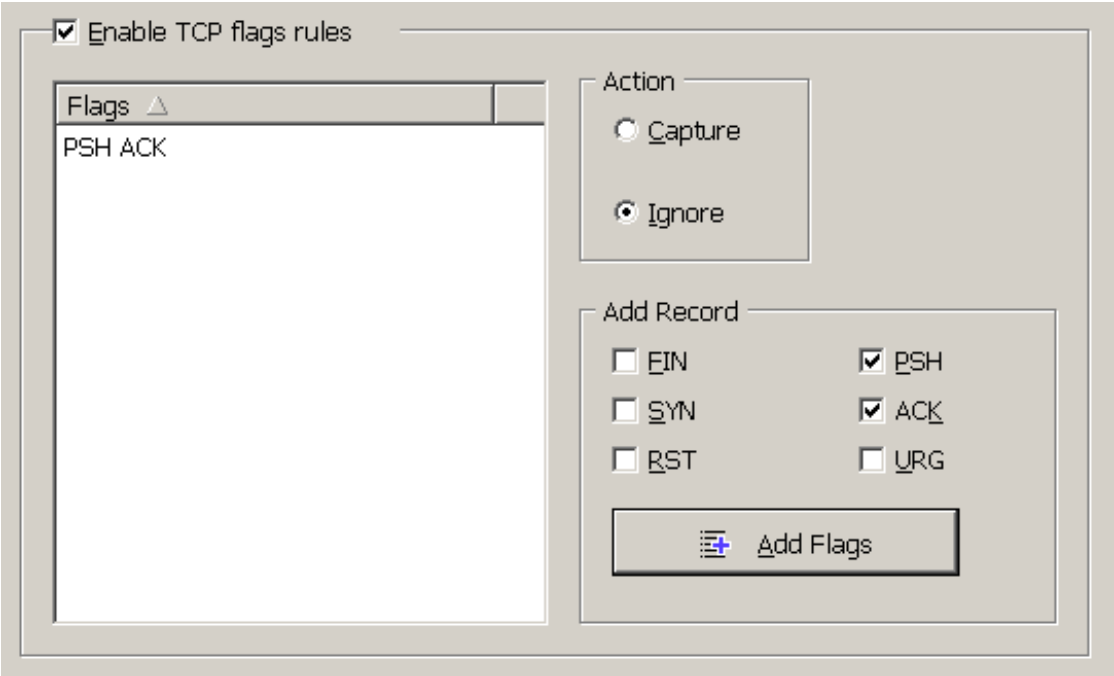
Pozwala określić przechwytywanie lub ignorowanie pakietów w oparciu o porty. Podaj numer portu w ramce **Add Record (Dodaj rekord)**, wybierz kierunek **From (Przychodzący), To (Wychodzący),** lub **Both (Oba)**, i kliknij **Add Port (Dodaj port)**. Nowa reguła zostanie wyświetlona. Teraz możesz wybrać akcję, która będzie podjęta w trakcie przetwarzania nowego pakietu: może on być albo przechwycony bądź zignorowany. Możesz również nacisnąć przycisk Port Reference (Lista portów), by zobaczyć listę wszystkich znanych portów, dwukrotnie kliknij na numerze portu, który chciałbyś dodać i ten numer pojawi się w odpowiednim polu. Porty można podawać jako tekst, na przykład możesz wpisać nazwę usługi: *http* lub *pop3*, a program zamieni ją na numer portu skojarzony z tą usługą sieciową.



Ten przykład pokazuje jak spowodować, by program ignorował pakiety przychodzące z portu 80, przychodzące oraz wychodzące z portu 137. Taka reguła zapobiegnie wyświetlaniu przychodzącego ruchu HTTP, jak również przychodzącego i wychodzącego ruchu Netbios Name Service. Wszystkie pakiety przychodzące i wychodzące z innych portów będą przechwytywane.

Flagi TCP

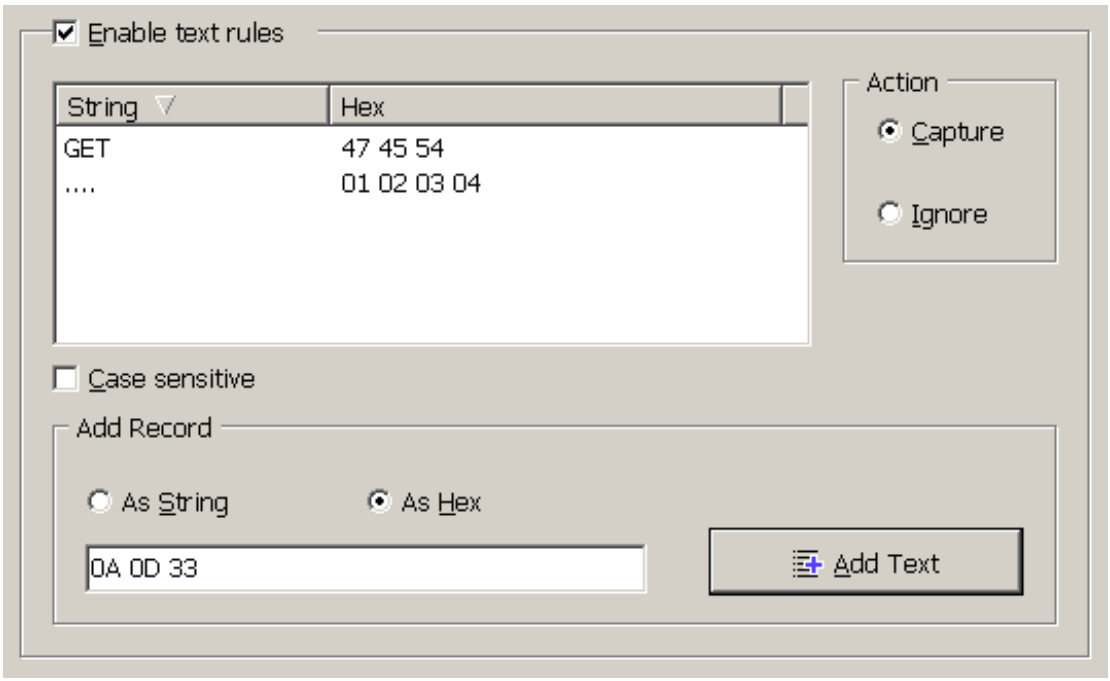
Pozwala na przechwytywaniu lub ignorowaniu pakietów w oparciu o flagi TCP. Zaznacz flagę lub flagi w ramce **Add Record (Dodaj rekord)**, i kliknij **Add Flags (Dodaj flagi)**. Zostanie wyświetlona nowa reguła. Teraz można wybrać rodzaj akcji: pakiety będą przechwytywane lub ignorowane.



Ten przykład pokazuje jak spowodować, by program ignorował pakiety TCP z ustawioną (bit flagi = 1) flagą PSH ACK. Wszystkie pakiety z innymi flagami będą przechwycone.

Tekst

Pozwala przechwytywać pakiety, które zawierają pewien tekst. Wpisz tekst w ramce **Add Record (Dodaj rekord)**, wybierz rodzaj wpisanych informacji – **As String (Jako ciąg)** lub **As Hex (Szesnastkowo)**, i kliknij **Add Text (Dodaj tekst)**. Ciąg oznacza dowolny tekst. Nowa reguła zostanie wyświetlona. Możesz podać tekst w postaci ciągu, lub jako wartość szesnastkową. Druga metoda powinna być używana wtedy, kiedy chcesz wpisać niedrukowalne znaki: po prostu wpisz wartości szesnastkowe znaków oddzielone spacjami, tak jak pokazane poniżej. Teraz możesz wybrać akcję, która będzie podjęta podczas przetwarzania nowego pakietu: może on być przechwycony lub zignorowany.



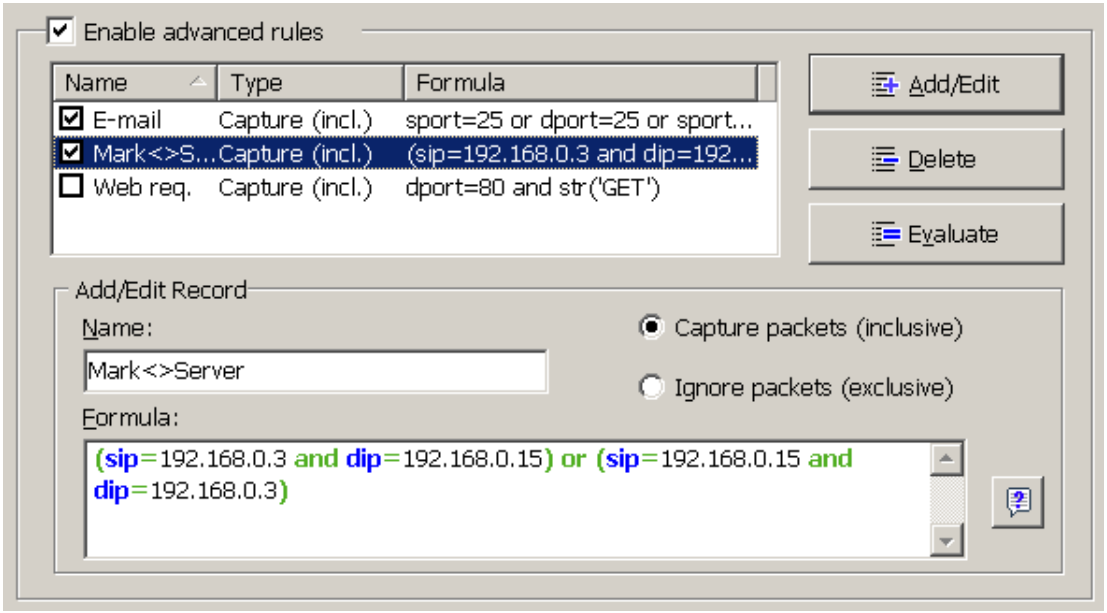
Ten przykład pokazuje jak spowodować, by program przechwytywał tylko pakiety, które zawierają albo ciąg "GET" lub ciąg danych szesnastkowych: 01 02 03 04. Zaznacz opcję **Case sensitive (Rozróżniaj wielkość liter)**, jeżeli chcesz, by rozróżniana była wielkość liter w warunkach reguł. Wszystkie inne pakiety, które nie zawierają tekstu wyżej wspomnianego będą ignorowane.

Zaawansowane

Reguły zaawansowane pozwalają na jeszcze bardziej dokładne ustalanie reguł rządzących przechwytywaniem pakietów. Dzięki nim można tworzyć złożone filtry wykorzystującą logikę Boolean. Szczegóły związane z regułami zaawansowanymi dostępne są w rozdziale Reguły zaawansowane.

Zaawansowane reguły

Reguły zaawansowane pozwalają na jeszcze bardziej dokładne ustalanie reguł rządzących przechwytywaniem pakietów. Dzięki nim można tworzyć złożone filtry wykorzystującą logikę Boolean. Korzystanie z zaawansowanych reguł wymaga zrozumienia podstawowych zasad matematyki oraz logiki, ale składnia reguł jest raczej nieskomplikowana.



Opis ogólny

Aby dodać nową regułę należy podać jej nazwę w polu **Name (Nazwa)**, wybrać opcję **Capture/Ignore (Przechwytuj/Ignoruj zaznaczone pakiety)**, wprowadzić formułę w okienku **Formula (Formuła)** posługując się składnią opisaną niżej, a potem kliknąć przycisk **Add/Edit (Dodaj/Edytuj)**. Nowa reguła ukaże się na liście i od razu będzie aktywna. Możesz dodać dowolną liczbę reguł, ale aktywne będą tylko te, które mają zaznaczone pole obok swojej nazwy. Możesz uruchamiać i zatrzymywać wykorzystywanie reguł klikając na pole obok nazwy reguły. Możesz też usunąć regułę korzystając z przycisku **Delete (Usuń)**. Jeśli aktywnych jest więcej niż jedna reguła, możesz dokonać ich wzajemnej oceny klikając przycisk **Evaluate (Oceń)**. Jeśli zdefiniowałeś kilka reguł, będą one połączone ze sobą operatorem OR, na przykład mając trzy reguły: RULE1, RULE2 i RULE3, wynikową regułą będzie RULE1 OR RULE2 OR RULE3.

Możesz łączyć reguły podstawowe i zaawansowane, jednak jeśli znasz logikę Boolean wystarczy ci stosowanie tylko zaawansowanych reguł. Reguły zaawansowane dają więcej możliwości. Reguły podstawowe i zaawansowane łączone są za pomocą operatora logicznego AND.

Składnia

dir – Kierunek pakietu. Możliwe wartości: *in* (*przychodzący*), *out* (*wychodzący*) i *pass* (*przechodzący*).

etherproto – Protokół Ethernetowy, 13 i 14 bajt pakietu. Akceptowanymi wartościami są numery (np. *etherproto=0x0800* dla IP) lub ogólnie stosowane aliasy (n.p. *etherproto=ARP*, co może być też zapisane jako *0x0806*).

ipproto – Protokół IP. Akceptowanymi wartościami są numery (n.p. *ipproto!=0x06* dla TCP) lub ogólnie stosowane aliasy (np. *ipproto=UDP*, co może być też zapisane jako *0x11*).

smac – Źródłowy adres MAC. Akceptowanymi wartościami są adresy MAC w notacji szesnastkowej (np. *smac=00:00:21:0A:13:0F*) lub aliasy adresów MAC zdefiniowane przez użytkownika.

dmac – Docelowy adres MAC.

sip – Źródłowy adres IP. Akceptowanymi wartościami są adresy IP w notacji kropkowo-dziesiętnej (np. *sip=192.168.0.1*), adresy IP ze znakami wieloznacznymi (wildcards) (np. *sip!=*.*.*.255*), adresy sieci wraz z maskami podsieci (np. *sip=192.168.0.4/255.255.255.240* or *sip=192.168.0.5/28*), zakresy IP (np. *sip from 192.168.0.15 to 192.168.0.18* lub *sip in 192.168.0.15 .. 192.168.0.18*), lub aliasy zdefiniowane przez użytkownika.

dip - Docelowy adres IP.

sport – Źródłowy port pakietów TCP i UDP. Akceptowanymi wartościami są numery (np. *sport=80* dla HTTP), zakresy (np. *sport from 20 to 50* lub *sport in 20..50* dla każdego portu między 20 i 50) lub aliasy zdefiniowane w systemie operacyjnym (np. *sport=ftp*, co odpowiada wartości 21). Aby uzyskać listę aliasów wspieranych przez system operacyjny należy wybrać z menu głównego programu **View (Przeglądaj) => Port Reference (Informacje o portach)**.

dport – Docelowy port pakietów TCP i UDP.

flag – flaga TCP. Akceptowanymi wartościami są numery (np. *0x18* dla PSH ACK) lub jeden z następujących znaków: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), and *U* (URG), oraz słowo kluczowe *has*, oznaczające, że pakiet posiada ustawiony bit danej flagi (bit flagi = 1). Przykłady: *flag=0x18*, *flag=SA*, *flag has F*.

size – Rozmiar pakietu. Akceptowanymi wartościami są numery (np. *size=1514*) lub zakresy (np. *size from 64 to 84* lub *size in 64..84* dla każdego rozmiaru między 64 a 84).

str – Zawartość pakietu. Sprawdza zawartość pakietu pod kątem występowania zdefiniowanego ciągu znaków. Funkcja ta ma trzy argumenty: string (ciąg znaków), position (pozycja) i case sensitivity (rozróżnianie wielkości liter). Przykładem pierwszego argumentu jest na przykład ciąg *'GET'*. Drugi argument wskazuje na pozycję ciągu znaków w pakiecie (offset). Pierwszy bajt w pakiecie ma wartość *0,* drugi *1,* trzeci *2*, itd. Gdy offset nie ma znaczenia, użyj wartości *–1*. Trzeci argument przyjmuje dwie wartości *false* (wielkość liter w ciągu nie jest rozróżnialna) lub *true* (wielkość liter w ciągu jest rozróżnialna). Argumenty drugi i trzeci są nieobowiązkowe, gdy nie zostaną wprowadzone program automatycznie przypisuje im wartości odpowiednio *–1* i *false*. Przykłady: *str('GET',-1,false)*, *str('GET',-1)*, *str ('GET')*.

hex – Zawartość pakietu. Wykorzystaj tę funkcję, aby przechwycić pakiety zawierające wzorzec podany w postaci szesnastkowej. Funkcja ma dwa argumenty: hex pattern (wzorzec) i position (pozycję). Pierwszy argument jest wartością wyrażoną w kodzie szesnastkowym, np. *0x4500*. Drugi argument wskazuje na pozycję wzorca w pakiecie (offset). Pierwszy bajt w pakiecie ma wartość *0,* drugi *1,* trzeci *2*, itd. Gdy offset nie ma znaczenia, użyj wartości *–1*. Drugi argument nie jest wymagany; jeśli zostanie pominięty, program automatycznie nada mu wartość *–1*. Przykłady: *hex(0x04500, 14)*, *hex(0x4500, 0x0E)*, *hex (0x010101)*.

Słowa kluczowe opisane wyżej mogą być wykorzystywane z następującymi operatorami:

and – iloczyn logiczny (Boolean conjunction).
or – syma logiczna (Boolean disjunction).
not – zaprzeczenie (Boolean negation).
= – jednoznaczność (Arithmetic equality).
!= – wykluczenie (Arithmetic inequality).
<> – tak jak wyżej.
> – więcej niż.
< – mniej niż.
( ) – nawiasy pomagają w określaniu zakresów i kolejności działań.

Wszystkie liczby mogą być zapisywane w notacji dziesiętnej lub szesnastkowej. W drugim przypadku, liczba musi być poprzedzona przedrostkiem *0x*, na przykład *15* oznacza to samo co *0x0F*.

Przykłady

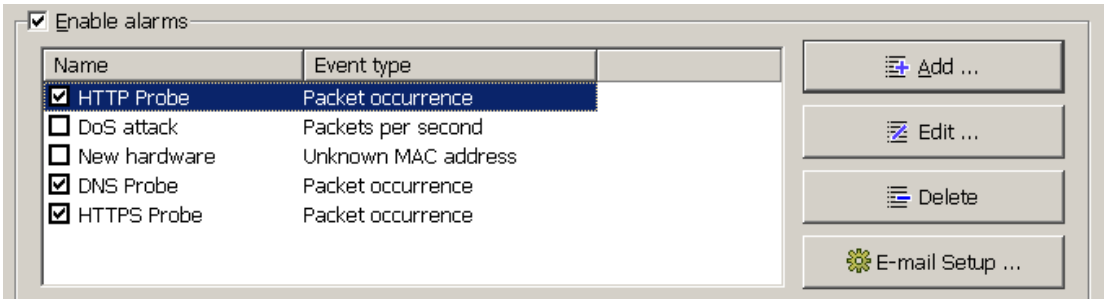
Poniżej znajduje się kilka przykładów obrazujących wykorzystanie składni reguł zaawansowanych wraz z opisami. Treści reguł podane są na czerwono. Komentarze występują po dwóch znakach ukośnika.

- dir!=pass // Przechwytuje tylko pakiety przychodzące i wychodzące. Pakiety przechodzące (pzesyłane pomiedzy innymi hostami w sieci LAN) nie są brane pod uwagę.
- (smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp // Przechwytuje pakiety ARP przesyłane przez komputery o adresach MAC 00:00:21:0A:13:0E oraz 00:00:21:0A:13:0F.
- ipproto=udp and dport=137 // Przechwytuje pakiety UDP/IP wysyłane na port 137.
- dport=25 and str('RCPT TO:', -1, true) // Przechwytuje pakiety TCP/IP lub UDP/IP zawierające 'RCPT TO:' oraz gdzie port przeznaczenia ma numer 25.
- not (sport>110) // Przechwytuje wszystkie pakiety z wyjątkiem tych, których numery portów źródłowych są większe niż 110.
- (sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3) // Przechwytuje pakiety IP przesyłane tylko między dwoma hostami: 192.168.0.3 oraz 192.168.0.15. Wszystkie inne pakiety są ignorowane.
- ((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600) // Przechwytuje pakiety TCP, których rozmiar mieści się między 200 i 600 bajtami oraz pochodzące z zakresu adresów IP 192.168.0.3 - 192.168.0.7, gdzie adres docelowy IP pochodzi z segmentu 192.168.1.0/255.255.255.240 oraz flaga TCP ma wartość PSH ACK.
- Hex(0x0203, 89) and (dir<>in) // Przechwytuje pakiety zawierające 0x0203 na pozycji 89, gdzie kierunek pakietu nie jest przychodzący.

Alarmy

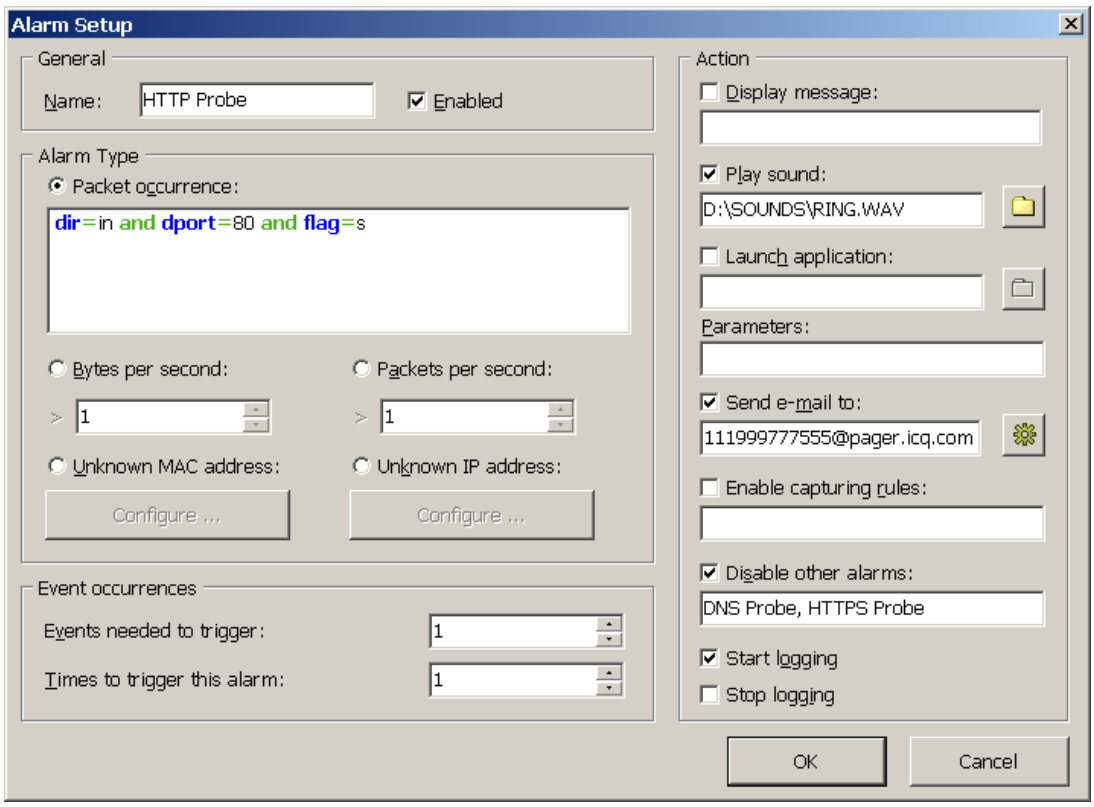
To narzędzie pozwala na generowanie alarmów mających miejsce, gdy zdarzy się coś ważnego, zostanie przechwycony podejrzany pakiet, próg wykorzystania łącza przekroczy zdefiniowaną wartość, pojawi się nieznany adres IP, itp. Alarmy są niezwykle przydatne, gdy monitorujesz sieć pod kątem wystąpienia podejrzanych zdarzeń, na przykład ruchu pakietów zawierających zdefiniowane wzorce, skanowania portów, niespodziewanych połączeń w sieci między urządzeniami.

Zarządzanie alarmami odbywa się za pomocą listy alarmów pokazanej poniżej:



Każda linia reprezentuje pojedynczy alarm, obok jego nazwy **Name (Nazwa)** znajduje się pole, które można zaznaczyć. Alarmy z zaznaczonymi kwadracikami są aktywne. Gdy nastąpi zdarzenie wywołujące alarm, zaznaczenie wpisu obok nazwy zostaje odhaczone. Aby ponownie aktywować alarm należy ręcznie zaznaczyć odpowiedni wpis. Aby wyłączyć wszystkie alarmy, odznacz opcję **Enable alarms (Dostępne alarmy)**. Aby dodać nowy, dokonać edycji istniejącego lub usunąć alarm wykorzystaj przyciski znajdujące się po prawej stronie. Przycisk **E-mail Setup (Konfiguracja e-mail)** pozwala na wprowadzenie informacji dotyczących twojego serwera SMTP związanego z wysyłaniem informacji poprzez e-mail.

Okno konfiguracji alarmu:



Pole **Name (Nazwa)** służy do opisu zastosowania alarmu. Zaznacz **Enabled (Włączony)**, aby aktywować alarm zaraz po zakończeniu konfiguracji. Aktywowanie alarmu można też przeprowadzić na karcie Alarms (Alarmy) na liście Dostępne alarmy. Ramka **Alarm Type (Typ alarmu)** pozwala na wprowadzenie jednego z czterech typów alarmów:

- **Packet occurrence (Wystąpienie pakietu)**: Gdy CommView przechwyci pakiet zgodny z podaną formułą zostanie uruchomiony alarm. Składnia formuły jest identyczna jak dla reguł zaawansowanych i jest opisana w rozdziale Zaawansowane reguły.
- **Bytes per second (Bajtów na sekundę)**: Alarm zostanie uruchomiony, gdy rozmiar transferu danych przekroczy 1 MB na sekundę. Wartość wprowadzona powinna być w bajtach, a więc dla granicy 1 MB należy wprowadzić 1000000.

- **Packets per second (Pakietów na sekundę)**: Alarm zostanie uruchomiony, gdy liczba pakietów na sekundę przekroczy zdefiniowaną wartość.

- **Unknown MAC address (Nieznany adres MAC)**: Alarm zostanie uruchomiony, gdy CommView przechwyci pakiet o nieznanym docelowym adresie MAC. Kliknij przycisk **Configure (Konfiguruj)** w celu wprowadzenia listy autoryzowanych adresów MAC. Ten rodzaj alarmu jest bardzo przydatny do wykrywania nieautoryzowanego sprzętu działającego w sieci LAN.

- **Unknown IP address (Niezany adres IP)**: Alarm zostanie uruchomiony, gdy CommView przechwyci pakiet o nieznanym docelowym adresie IP. Kliknij przycisk **Configure (Konfiguruj)** w celu wprowadzenia listy autoryzowanych adresów IP. Ten rodzaj alarmu jest bardzo przydatny do wykrywania nieautoryzowanych połączeń poza zaporą ogniową.

Pole **Events needed to trigger (Zdarzeń wymaganych do rozpoczęcia)** pozwala na zdefiniowanie ilość wystąpień poszczególnych zdarzeń zanim alarm zostanie uruchomiony. Na przykład dla wartości 3, alarm zostanie uruchomiony dopiero po trzecim wystąpieniu zdarzenia. Jeśli właściwości alarmu zostaną poddane edycji, pole to zostanie zmienione na 1.

Pole **Times to trigger this alarm (Ilość wystąpień)** pozwala na zdefiniowanie ilość wystąpień poszczególnych zdarzeń zanim alarm zostanie deaktywowany. Domyślnie wartością tego pola jest 1, a więc po pierwszym uruchomieniu alarmu zostanie od deaktywowany. Zwiększanie tej wartości spowoduje, że CommView będzie alarmował odpowiednio większą ilość razy. Jeśli właściwości alarmu zostaną poddane edycji, pole to zostanie zmienione na 1.

Ramka **Action (Akcja)** pozwala na zdefiniowanie czynności, jakie ma wykonać program, gdy alarm zostanie uruchomiony. Możliwe są następujące działania:

- **Display message (Wyświetl informację)**: Wyświetla okienko w trybie niemodalnym zawierające informację o zdarzeniu.

- **Play sound (Odtwórz dźwięk)**: Odtwarza plik WAV.

- **Launch application (Uruchom aplikację)**: Uruchamia plik EXE lub COM. W polu **Parameters (Parametry)** można wprowadzić dodatkowe parametry dla uruchamianego programu.

- **Send e-mail to (Wyślij e-mail do)**: Wysyła wiadomość e-mail pod wskazany adres. Aby ta opcja działała, należy skonfigurować CommView do korzystania z sewera SMTP. W tym celu należy kliknąć przycisk **E-mail Setup (Konfiguracja e-mail)**, który znajduje się obok pola adresu e-mail oraz sprawdzić poprawność wpisanych danych wysyłając wiadomość testową. Zwykle wiadomości e-mail mogą być też wysyłane na pager, telefon komórkowy oraz do oprogramowania komunikacyjnego. Na przykład wysłanie informacji do użytkwnika ICQ polega na wpisaniu adresu e-mail w następujący sposób: ICQ_USER_UIN@pager.icq.com, gdzie ICQ_USER_UIN jest numerem identyfikacyjnym ICQ. Dokładne informacje na ten temat powinny być dostępne w dokumentacji telefonu komórkowego, pagera lub programu komunikacyjnego.

- **Enable capturing rules (Włącz przechwytywanie reguł)**: Pozwala na przechwytywanie zaawansowanych reguł; należy wprowadzić jedną lub więcej nazw reguł. Jeśli wprowadzasz więcej nazw, powinieneś oddzielić je przecinkami lub średnikami.

- **Disable other alarms (Wyłącz inne alarmy)**: Wyłącza inne alarmy; należy wprowadzić jedną lub więcej nazw alarmów. Jeśli wprowadzasz więcej nazw, powinieneś oddzielić je przecinkami lub średnikami.

- **Start logging (Rozpocznij zbieranie logów)**: Włącza automatyczne zapisywanie (zobacz rozdział Logging); CommView rozpocznie zapisywanie pakietów na twardym dysku.

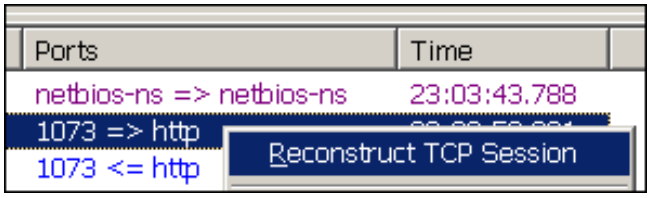
- **Stop logging (Zakończ zbieranie logów)**: Wyłącza automatyczne zapisywanie.

Kliknij **OK** w celu zapisania konfiguracji alarmu oraz wyjścia z okna konfiguracji.

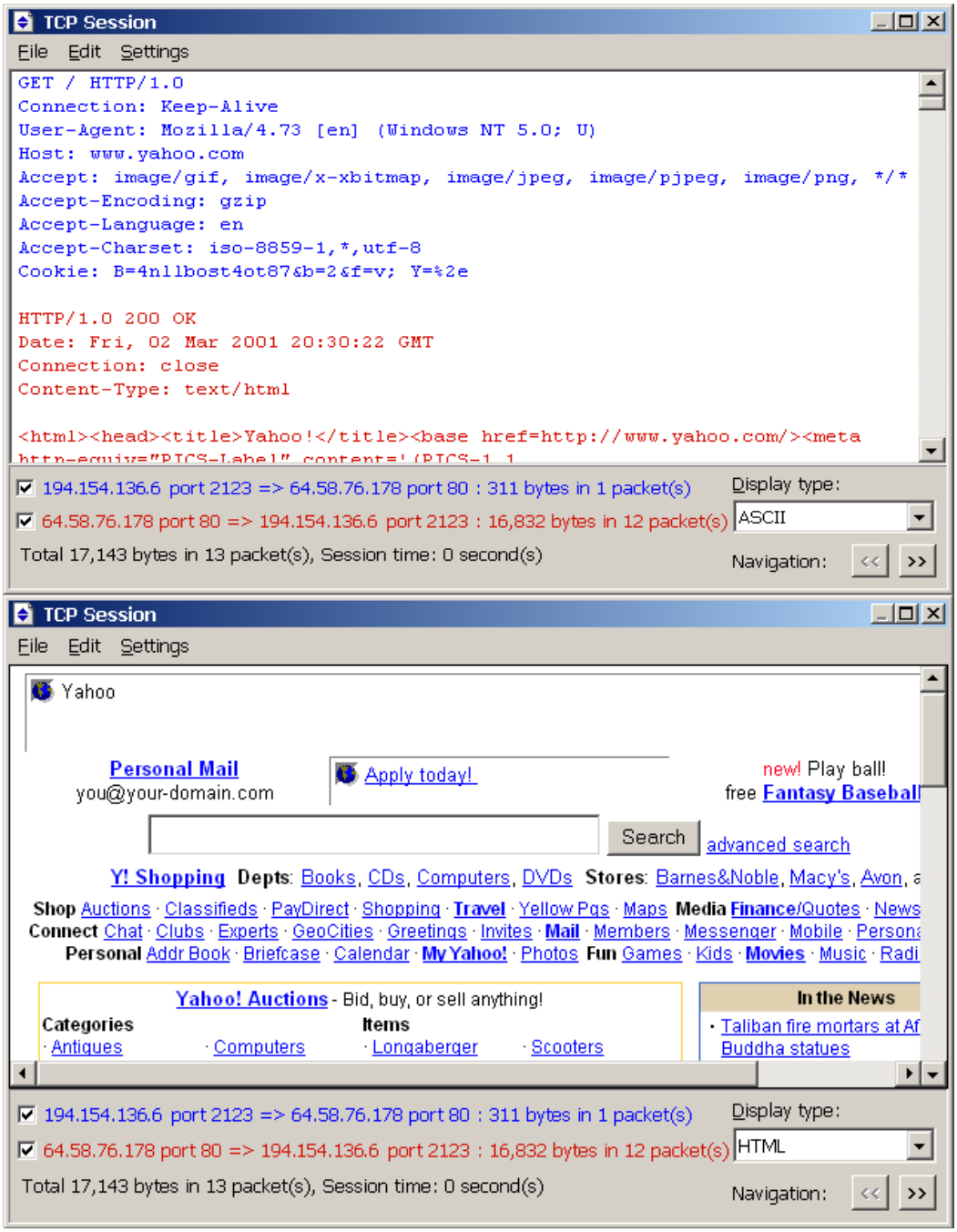
Wszystkie zdarzenia związane z alarmami zostaną wyświetlone w okienku **Event Log (Zapis zdarzeń)** znajdującym się poniżej listy alarmów.

Odtwarzanie sesji TCP

To narzędzie pozwala na przejrzenie "konwersacji" TCP, jaka miała miejsce pomiędzy dwoma komputerami. W celu rekonstrukcji sesji TCP na początek powinieneś wybrać pakiet TCP z zakładki **Packets (Pakiety)**. Jeżeli chcesz odtworzyć całą sesję, zalecany jest wybór pierwszego pakietu tej sesji; w innym przypadku odtwarzanie sesji może rozpocząć się od środka "konwersacji". Po odnalezieniu i wybraniu pakietu, kliknij na nim prawym klawiszem myszki i wybierz polecenie **Reconstruct TCP Session (Zrekonstruuj Sesję TCP)** z kontekstowego menu tak jak jest to pokazane poniżej:



Rekonstrukcja sesji działa najlepiej w przypadku protokołów tekstowych, takich jak POP3, Telnet, czy HTTP. Oczywiście możesz odtworzyć sesję ściągania dużego skompresowanego pliku ZIP, lecz może to zabrać programowi CommView dużo czasu na odtworzenie kilku MB danych, a otrzymane informacje mogą być bezużyteczne w większości przypadków. Próbka sesji protokołu HTTP została pokazana poniżej:



Odznaczając jeden z wyborów dostępnych w dolnej części okienka TCP Session (Sesja TCP) możesz przeglądać dane biegnące tylko w jednym kierunku. Przychodzące i wychodzące dane są oznaczane innymi kolorami dla Twojej wygody i komfortu. Jeżeli chcesz zmienić jeden z kolorów, kliknij Settings (Ustawienia) => Colors (Kolory) i wybierz inny kolor. Możesz też włączyć lub wyłączyć zawijanie słów w menu **Settings (Ustawienia) => Word Wrap (Zawijanie słów)**.

Rozwijana lista **Display type (Rodzaj wyświetlania)** pozwala na przeglądanie danych w formatach: **ASCII** (tekst), **HEX** (szesnastkowo), **HTML** (strona www), oraz **EBCDIC** (kodowanie dla IBM mainframe). Wyświetlanie danych w formacie HTML może być nieco zubożone (np. grafiki normalnie istniejące w dokumencie HTML mogą być niedostępne), jednak to, co będzie wyświetlone powinno wystarczyć.

Przyciski **Navigation (Nawigacja)** pozwalają na przechodzenie do następnej i poprzedniej sesji nawiązanej między dwoma hostami. Jeśli przeglądasz kilka sesji, powinieneć rozpocząć ich przeglądanie od pierwszej przechwyconej, ponieważ przycisk (**<<**) nie może przeskoczyć do sesji wcześniejszej niż wybrana do rekonstrukcji jako pierwsza.

Uzyskane dane można zapisać w postaci bianrnej, tekstowej, lub w formacie RTF (Rich Text File) poprzez kliknięcie **File (Plik) => Save As (Zapisz Jako)**. Możesz też wyszukiwać pakiety zawierające określony ciąg znaków klikając **Edit (Edytuj) => Find (Znajdź)**.

Statystyki i raporty

Okienko **View (Widok) => Statistics (Statystyka)** wyświetla niezbędną statystykę sieciową Twojego komputera lub segmentu sieci LAN, zawierającą następujące wskaźniki: ilość pakietów na sekundę, ilość bajtów na sekundę, i wykresy pokazujące procentową obecność pakietów protokołów i podprotokołów (subprotokołów) IP. Możesz skopiować dowolny z wykresów do Schowka podwójnie klikając na wykresie. Wykresy protokołów i podprotokołów IP mogą być obracane przy użyciu małych przycisków znajdujących się w prawym dolnym rogu, co pozwala lepiej widzieć poszczególne fragmenty wykresu.

Dane wyświetlane na każdej zakładce okna Statystyka mogą być zapisane jako bitmapy lub do pliku tekstowego, gdzie wartości oddzielane są średnikami (semicolon-delimited text). Zakładka **Report (Raport)** pozwala na automatyczne generowanie raportów w formacie HTML lub pliku tekstowego, gdzie wartości oddzielane są średnikami.

Statystyki sieciowe mogą być zbierane na podstawie wszystkich danych napływających do hosta lokalnego lub aktualnie zdefiniowanych reguł. Jeśli chcesz, aby CommView brał pod uwagę tylko pakiety zgodne z regułami, zaznacz **Apply current rules (Zastosuj obecne reguły)**.

General (Główne)
Wyświetla ilość pakietów na sekundę, aktualne wykorzystanie sieci (ruch na sekundę podzielony przez prędkość interfejsu sieciowego) oraz ogólne liczniki pakietów i bajtów.

IP Protocols (Prot. IP)
Wyświetla rozkład procentowy na główne protokoły IP: TCP, UDP oraz ICMP. Wykorzystaj listę rozwijaną **Chart by (Wykres)**, aby wybrać jeden z wykresów procentowo wg: liczby pakietów lub liczby bajtów.

IP Sub-protocols (Sub-prot. IP)
Wyświetla rozkład procentowy na główne podprotokoły (subprotokoły) warstwy aplikacyjnej protokołu IP: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, oraz DNS. Aby dodać kolejne podprotokoły kliknij **Customize (Dostosuj)**. Pojawi się okienko pozwalające na zdefiniowanie 8 dodatkowych protokołów. Należy podać nazwę, typ protokołu IP (TCP/UDP) oraz numer portu. Wykorzystaj listę rozwijaną **Chart by (Wykres)**, aby wybrać jeden z wykresów procentowo wg: liczby pakietów lub liczby bajtów.

Sizes (Rozmiary)
Wyświetla rozkład procentowy rozmiarów pakietów.

LAN Hosts (MAC) (Hosty LAN (MAC))
Wyświetla listę hostów LAN wg adresów MAC i wyświetla statystyki dotyczące transferu danych. Do adresów MAC można przypisać aliasy.

LAN Hosts (IP) (Hosty LAN (IP))
Wyświetla listę hostów LAN wg adresów IP i wyświetla statystyki dotyczące transferu danych. Ponieważ pakiety przechwycone mogą pochodzić od wielu hostów (nie tylko z sieci LAN), domyślnie zakładka ta nie wyświetla statystyk. Aby uruchomić wyświetlanie, należy ustawić zakres adresów IP, które będą monitorowane, klikając **Add/Set Ranges (Dodaj/Ustaw zakresy)**. Zwykle powinny to być adresy IP należące do sieci LAN. Możesz wprowadzić dowolną liczbę zakresów, ale ilość wszystkich adresów IP nie może przekroczyć 1000. Aby usunąć zakres, kliknij prawym przyciskiem myszy na zakresie i wybierz odpowiednią opcję z menu kontekstowego. Do adresów IP można przypisać aliasy.

Errors (Błędy)
Wyświetla informacje o błędach Ethernet otrzymanych od adaptera sieciowego:

Rx CRS Errors
Liczba ramek z błędami circular redundancy check CRC lub frame check sequence FCS.
Rx Alignment Errors
Liczba ramek z błędami dopasowania.
Rx Overrun
Liczba ramek nieotrzymanych z powodu błędu Overrun.
Tx One Collision
Liczba ramek przesłanych po jednym błędzie kolizji.
Tx More Collisions
Liczba ramek przesłanych po więcej niż jednym błędzie kolizji.
Tx Deferred
Liczba ramek przesłanych po przynajmniej jednym wstrzymianiu przez NIC.
Tx Max Collisions
Liczba ramek nieprzesłanych w wyniku błędów kolizji.
Tx Underrun
Liczba ramek nieprzesłanych w wyniku błędów Underrun.
Tx Heartbeat Failure
Liczba ramek przesłanych bez nasłuchiwania sygnału transmisji.
Tx Times CRS Lost
Liczba przypadków utraty sygnału transmisji.
Tx Late Collisions
Liczba kolizji wykrytych po normalnym oknie.
Rx Frames w/Errors
Liczba ramek otrzymanych i nierozpoznanych.
Rx Frames w/o Errors

Liczba ramek otrzymanych i rozpoznanych.
Tx Frames w/Errors
Liczba ramek nieprzetransmitowanych.
Tx Frames w/o Errors
Liczba ramek przetransmitowanych bez błędów.

Zwróć uwagę, że:

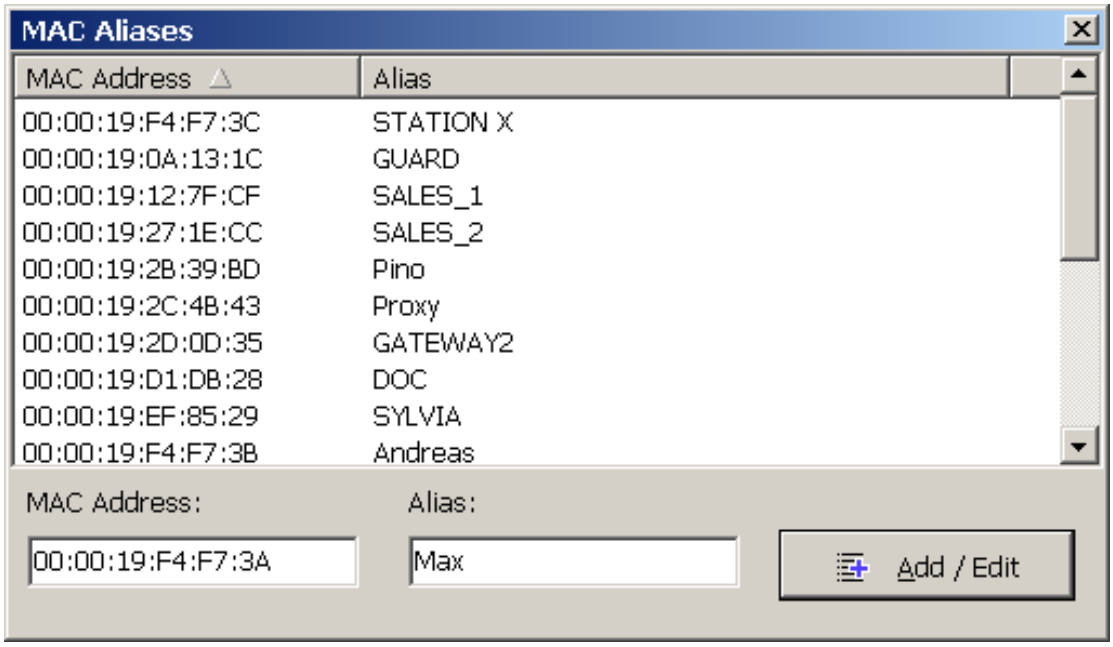
- Adaptery dial-up nie są wspierane, tylko karty Ethernet.
- Nie wszystkie karty sieciowe dostarczają wszystkich informacji.
- Przycisk **Errors** nie powoduje wyzerowania statystyki błędów. Licznik jest inicjalizowany za każdym razem, gdy komputer jest włączany.
- Zakładka błędy nie jest wyświetlana w Windows 95.

Report (Raport)
Pozwala na automatyczne generowanie raportów w formacie HTML lub pliku tekstowego, gdzie wartości oddzielane są średnikami.

Używnie aliasów

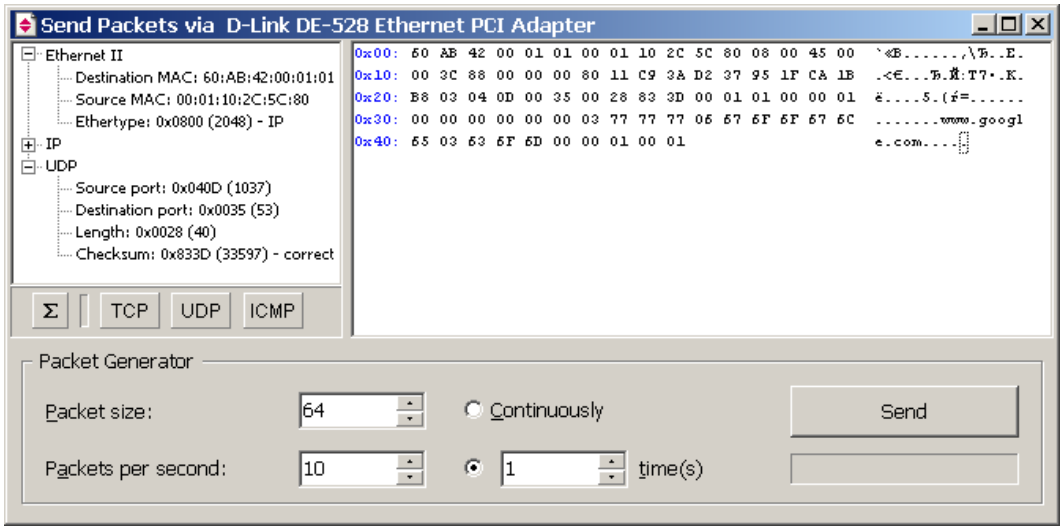
Aliasy są to łatwe do zapamiętania czytelne nazwy, którymi CommView zastąpi adresy MAC podczas wyświetlania pakietów na zakładkach **Packets (Pakiety)** i **Statistics (Statystyki)**. To może ułatwić identyfikację i analizę pakietów. Np.: zamiast adresu 00:00:19:2D:0D:35 pojawi się nazwa GATEWAY2, a zamiast ns1.earthlink.com – MyDNS.

By dodać alias kliknij prawym klawiszem myszki na pakiecie i wybierz polecenie **Create Alias (Twórz Alias) => Using Source MAC (Używając Źródłowego Adresu MAC)** lub **Using Destination MAC (Używając Docelowego Adresu MAC)** z menu kontekstowego. Pojawi się okienko, w którym pole MAC adress (adres MAC) będzie wypełnione, więc trzeba będzie tylko wpisać alias. Alternatywnie możesz kliknąć **Settings (Ustawienia) => MAC Aliases (Aliasy MAC)** i ręcznie wpisać adres MAC i alias w odpowiednie pola. By usunąć alias lub pozbyć się wszystkich aliasów z listy kliknij prawym klawiszem myszki na okienku Aliases (Aliasy) i wybierz **Delete Record (Usuń Rekord)** lub **Clear All (Wyczyść Wszystko)**. W taki sam sposób można zarządzać aliasami IP. Gdy tworzony jest nowy alias IP poprzez kliknięcie prawym przyciskiem myszy pakietu, pole aliasu może być wypełnione nazwą hosta i może być edytowane przez użytkownika.



Generator pakietów

To narzędzie pozwala na edycję i wysyłanie pakietów przez kartę sieciową. Dostępne jest tylko pod Windows NT/2000/XP. By uruchomić Generator Pakietów, kliknij **Tools (Narzędzia) => Packet Generator (Generator Pakietów)**, lub wybierz pakiet z zakładki **Packets (Pakiety)**, kliknij na nim prawym klawiszem myszki, i wybierz polecenie **Send Packet (Wyślij Pakiet(y))**.



Generator pakietów pozwala na dekodowanie i dokonywanie zmian w zawartości pakietu. Umożliwia też tworzenie dowolnych pakietów IP, TCP, UDP, oraz ICMP. Przycisk **Sigma** pozwala na automatyczne poprawianie sum kontrolnych pakietów.

Możesz też wykorzystać przyciski **TCP**, **UDP**, oraz **ICMP** w celu załadowania pustych wzorów pakietów w tych protokołach. Jeśli jednak masz szczególne wymagania w tym względzie, możesz stworzyć dowolny pakiet od podstaw. Własne szablony można tworzyć w postaci plików CCF i umieszczać je w katalogu aplikacji. Nazwy plików powinny być następujące: "template_tcp.ccf", "template_udp.ccf", oraz "template_icmp.ccf". Gdy CommView znajdzie któryś z tych plików w katalogu aplikacji, załaduje je, gdy użytkownik kliknie na jeden z przycisków **TCP**, **UDP**, lub **ICMP**. Pliki te powinny zawierać tylko jeden pakiet, jeśli będzie ich więcej, program załaduje pierwszy.

Po dokonaniu edycji pakietu, użyj kontrolek znajdujących się poniżej okna głównego generatora:

Packet Size (Rozmiar pakietu) – modyfikuje rozmiar pakietu.
Packets Per Second (Pakietów na sekundę) – kontroluje prędkość, z jaką pakiety będą wysłane. Nie wysyłaj pakietów zbyt szybko, jeśli dysponujesz wolnym łączem. Na przykład wysłanie pakietu o rozmiarze 1KB z częstotliwością 5000 na sekundę spowoduje zablokowanie karty 10 Mbit (lub odrzucenie nadmiaru pakietów).
Continuously (Ciągłe wysyłanie) – wybierz tę opcję, jeżeli chcesz by Generator Pakietów wysyłał pakiety nieprzerwanie aż do naciśnięcia przycisku Stop.
Time(s) (raz(y)) – wybierz tę opcję, jeżeli chcesz by Generator Pakietów wysłał pakiet podaną ilość razy.
Send/Stop (Wyślij/Zatrzymaj) – kliknij ten przycisk, jeżeli jesteś gotowy do wysłania pakietów lub do wstrzymania ich wysyłania.

Praca z wieloma pakietami

Generator pakietów pozwala na wysyłanie więcej niż jednego pakietu. Można to zrobić zaznaczając więcej niż jeden pakiet oraz wybranie z menu kontekstowego opcji Wyślij pakiet(y) lub przeciągając wybrane pakiety do otwartego okna generatora pakietów. W takim przypadku edytor i dekoder pakietu będą niedostępne.

Zapisywanie edytowanych pakietów

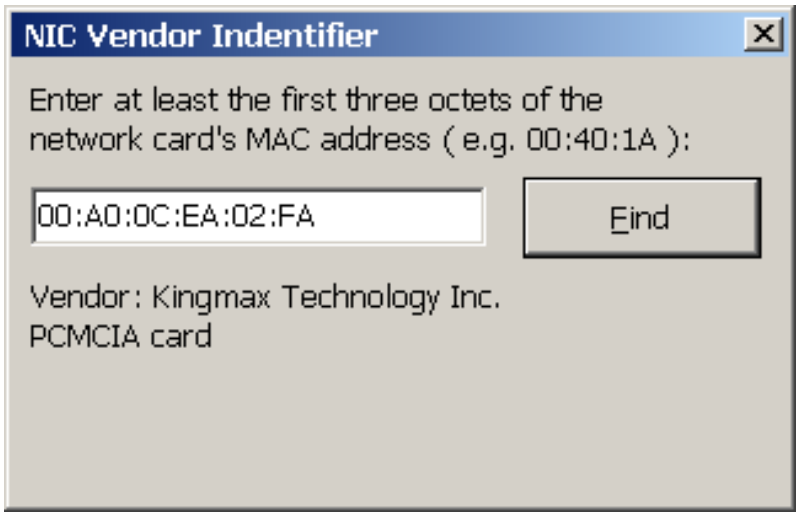
If you edit a packet and would like to save it, just drag the decoder tree to the desktop or any folder, and a new file in CCF format containing the packet will be created. The file name is always PACKET.CCF.

WARNING (Ostrzeżenie):

1. Nie używaj Generatora Pakietów chyba, że wiesz dokładnie, jaki efekt chcesz osiągnąć. Wysyłanie pakietów może wywołać nieprzewidywalne rezultaty i w związku z tym zalecamy powstrzymanie się od używania tego narzędzia chyba, że jesteś doświadczonym administratorem sieci.
2. W momencie, gdy będziesz używał Generatora Pakietów w sieci LAN powinien pracować przynajmniej jeden komputer poza Twoim własnym, gdyż inaczej doświadczysz dotkliwych opóźnień w przesyłaniu pakietów.
3. To narzędzie nie może być użyte do wysyłania pakietów przez interfejs RAS w Windows NT.

Identyfikator dostawcy NIC

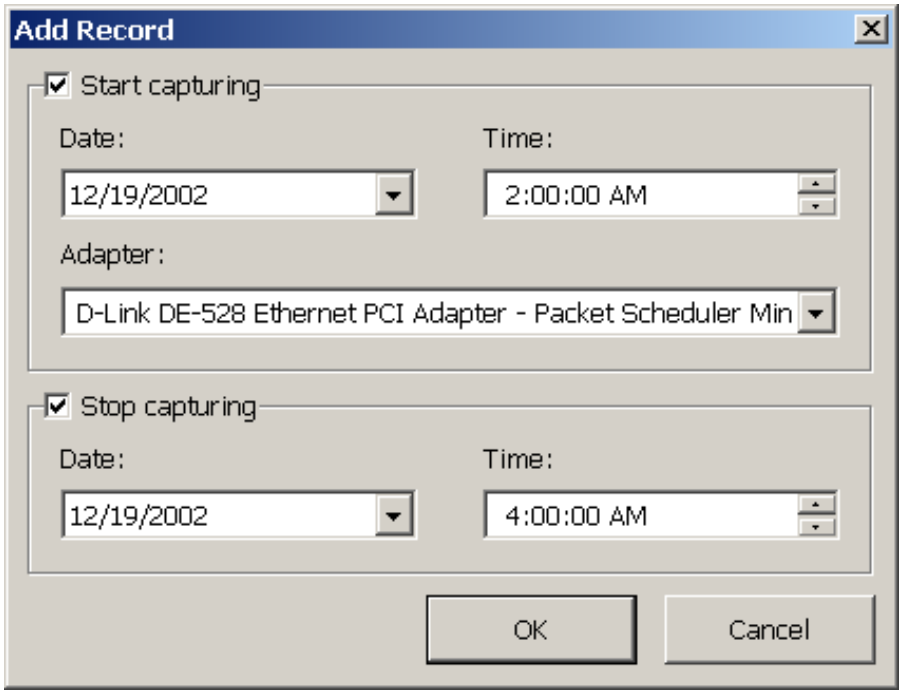
Pierwsze 24 bity adresu MAC karty sieciowej jednoznacznie identyfikują producenta karty sieciowej. Ta 24-bitowa liczba jest zwana skrótowo OUI ("Organizationally Unique Identifier"), czyli ("Organizacyjnie Unikalny Identyfikator"). NIC Vendor Identifier (Identyfikacja Producenta Karty Sieciowej) jest narzędziem, które pozwala zidentyfikować producenta karty po jej unikalnym adresie MAC. By skorzystać z tego narzędzia kliknij **Tools (Narzędzia) => NIC Vendor Identifier (Identyfikacja dostawcy NIC)**, podaj adres MAC, i kliknij **Find (Znajdź)**. Nazwa procenta zostanie wyświetlona.



Lista producentów jest zawarta w pliku MACS.TXT, który znajduje się w folderze programu CommView. Można go ręcznie modyfikować w celu do/zmiany zawartych w nim informacji.

Harmonogram

Narzędzie to pozwala na automatyczne uruchamianie i zatrzymywanie działania programu CommView we wcześniej zdefiniowanych momentach, na przykład w nocy lub w weekend. Aby dodać nowy wpis do harmonogramu, należy kliknąć **Tools (Narzędzia)** => **Scheduler (Harmonogram)**, a następnie kliknąć przycisk **Add (Dodaj)**.



Ramka **Start capturing (Rozpocznij przechwytywanie)** pozwala na zdefiniowanie daty i czasu uruchomienia przechwytywania pakietów oraz na wybór z listy rozwijanej **Adapter** adaptera sieciowego, który ma być wykorzystywane w zdefiniowanym zadaniu. Ramka **Stop capturing (Zakończ przechwytywanie)** pozwala na zdefiniowanie daty i czasu zakończenia przechwytywania pakietów. Nie musisz korzystać z obu ramek na raz. Jeśli wybierzesz tylko górną z nich **Start capturing**, przechwytywanie pakietów będzie kontynuowane dopóki nie nastąpi jego ręczne wyłączenie. Jeśli wybierzesz tylko dolną ramkę **Stop capturing**, musisz wcześniej ręcznie uruchomić przechwytywanie. Wtedy program zakończy je w określonym w harmonogramie momencie.

Jeśli w trakcie przechwytywania pakietów zaplanujesz nowe przechwytywanie z wykorzystaniem innego adaptera niż obecnie wykorzystywany, CommView zatrzyma przechwytywanie, przełączy adaptery i ponownie wznowi przechwytywanie pakietów.

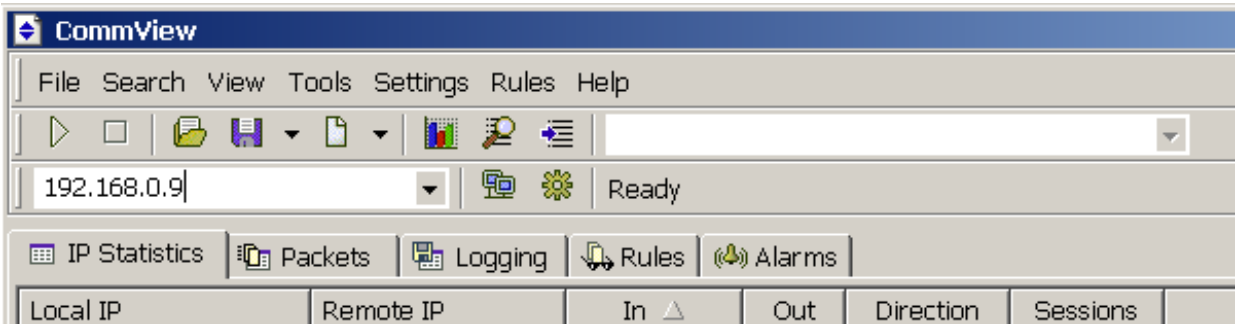
Należy pamiętać o tym, że funkcje harmonogramu są aktywne jedynie wtedy, gdy CommView jest uruchomiony.

Wykorzystywanie zdalnych agentów

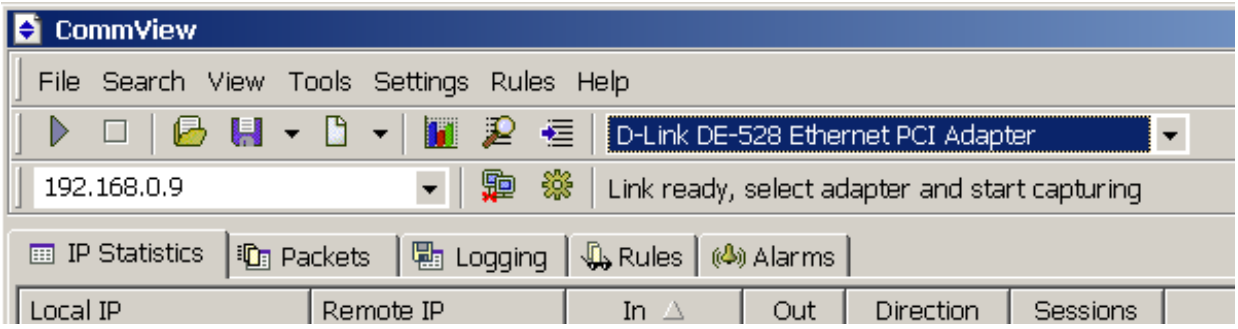
CommView Remote Agent jest dodatkowym oprogramowaniem pozwalającym użytkownikom CommView na przechwytywanie pakietów ze zdalnego hosta. Wszystko, co trzeba zrobić, to zainstalowanie programu Remote Agent na zdalnym komputerze i połączenie się z nim przy pomocy CommView. Gdy oba programy uzyskają ze sobą połączenie i nastąpi pomyślne uwierzytelnienie, możesz przechwytywać pakiety ze zdalnego hosta tak samo jakbyś pracował na nim lokalnie.

Ważne: Informacje zgromadzone w tym rozdziale dotyczą jedynie podłączania zdalnego agenta do CommView oraz zdalnego przechwytywania pakietów. Bardziej dokładne informacje związane z programem Remote Agent znajdują się w pliku pomocy do tego programu. Zaleca się zapoznanie się z tą dokumentacją zanim Remote Agent będzie wykorzystywany. Dokumentacja dostępna jest na naszej stronie.

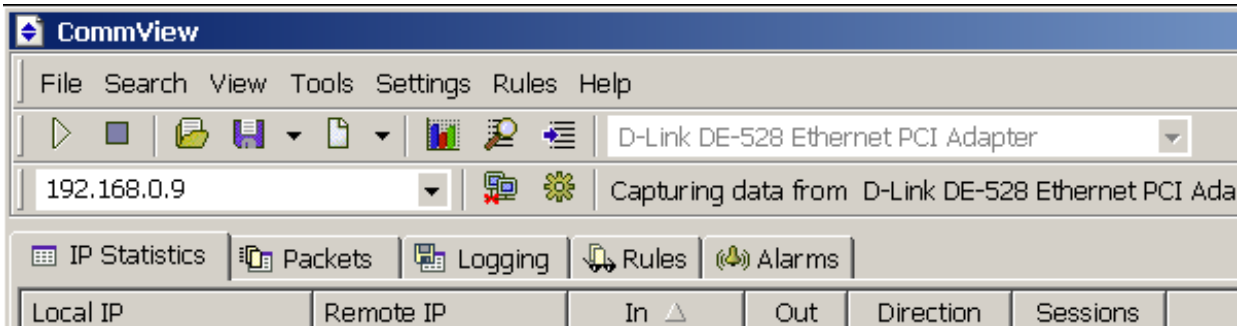
Aby uruchomić CommView w trybie zdalnym, należy z menu głównego wybrać **File (Plik)** => **Remote Monitoring Mode (Tryb zdalnego monitorowania)**. Po zaznaczeniu tej opcji pojawi się pasek zdalnego dostępu w oknie programu. Wprowadź adres IP komputera, na którym zainstalowano zdalnego agenta i kliknij **Connect (Połącz)**. Jeśli komunikacja odbywa się poprzez zaporę sieciową lub zdalny agent korzysta z niestandardowego portu, skorzystaj z przycisku **Network Settings (Zaawansowane ustawienia sieciowe)**.



Pojawi się okno z prośbą o wprowadzenie hasła. Wprowadź hasło do programu Remote Agent. Pojawi się wtedy informacja o gotowości połączenia oraz rozwijana lista adapterów sieciowych zdalnego hosta.



Teraz można ustalić reguły przechwytywania wykorzystując zakładkę **Rules (Reguły)**. Poprawna konfiguracja reguł ma w tym przypadku ogromne znaczenie, ze względu na ruch pakietów między CommView i Remote Agent. Przechwytywanie zbyt wielu pakietów na hoście zdalnym może bardzo obniżyć wydajność lub nawet zapchać łącze. Gdy wszystkie ustawienia zostaną skonfigurowane, można przystąpić do przechwytywania pakietów klikając przycisk **Start Capture (Rozpocznij przechwytywanie)**.



CommView rozpocznie przechwytywanie pakietów w taki sposób, jakby czynność ta odbywała się lokalnie; z punktu widzenia użytkownika nie stanowi to żadnej różnicy. Gdy przechwytywanie ma być zakończone, kliknij przycisk **Stop Capture (Zatrzymaj przechwytywanie)**. Można wtedy zmienić adapter na zdalnym hoście lub rozłączyć się z nim klikając przycisk **Disconnect (Rozłącz)**. Aby powrócić do trybu standardowego, kliknij **File (Plik)** => **Remote Monitoring Mode (Tryb zdalnego monitorowania)**, pasek dostępu zdalnego zostanie ukryty.

Ustawianie opcji

Możesz tutaj skonfigurować niektóre opcje programu wybierając polecenie Settings (Ustawienia) z menu.

Fonts (Czcionki)

Użyj tego menu, by wybrać czcionkę, jaka będzie użyta do wyświetlania tekstu interfejsu programu oraz poszczególnych pakietów. W celu zmiany koloru tekstu, jakim będą wyświetlane pakiety, użyj menu Options (Opcje), którego opis znajdziesz poniżej.

Options (Opcje)

General (Ogólne)

Auto-start capturing (Auto-start przechwytywania) – zaznacz tą opcję, jeżeli chcesz, aby CommView zaczynał przechwytywanie pakietów natychmiast po uruchomieniu programu. Dla systemów posiadających więcej jak jeden interfejs sieciowy, powinieneś również wybrać z listy rozwijanej ten, który będzie używany w procesie przechwytywania pakietów danych w sieci.

Network (Sieć)

Disable DNS resolving (Wyłącz rozwiązywanie nazw DNS) – zaznacz tą opcję, jeżeli nie chcesz, by CommView wykonywał odwrotne zapytania do serwera DNS odnośnie adresów IP, innymi słowy: zamieniał adres IP na nazwę domenową. Jeżeli zaznaczysz tą opcję, kolumna Hostname (Nazwa komputera) na zakładce IP Statistics (Statystyki IP) pozostanie pusta.

Convert numeric port values to service names (Konwertuj numery portów na nazwy usług) – zaznacz tą opcję, jeżeli chcesz by CommView wyświetlał nazwy usług skojarzonych z danym numerem portu zamiast tychże numerów. Na przykład, jeżeli ta opcja jest zaznaczona, port **21** zamiast liczby 21 jest określany jako **ftp**, port **23,** jako **telnet**, port **22** zaś jako **ssh** (secure shell – bezpieczna wersja usługi telnet). Program zamienia numeryczne wartości na nazwy poszczególnych usług posługując się plikiem SERVICES instalowanym przez system Windows. W zależności od wersji Windows, plik SERVICES znajduje się w innym folderze: w Windows 95/98/Me znajdziesz go w folderze \Windows, a w Windows NT/2000/XP znajdziesz go w folderze \Winnt\system32\drivers\etc. Możesz ręcznie zmodyfikować zawartość pliku SERVICES dopisując do niego więcej portów i związanych z nimi usług sieciowych.

Convert MAC addresses to aliases (Konwertuj adresy MAC na aliasy) – podmienia adresy MAC na aliasy na zakładce **Packets (Pakiety)**. Aliasy mogą zostać przypisane do adresów MAC poprzez użycie polecenia z menu **Settings (Ustawienia) => MAC Aliases (Aliasy MAC)**.

Convert IP addresses to aliases (Konwertuj adresy IP na aliasy) – podmienia adresy IP na aliasy na zakładce **Packets (Pakiety)**. Aliasy mogą zostać przypisane do adresów IP poprzez użycie polecenia z menu **Settings (Ustawienia) => IP Aliases (Aliasy IP)**.

Convert IP addresses to hostnames in the "Packets" tab (Konwertuj adresy IP na nazwy w kolumnie "Pakiety") – zaznacz tę opcję jeśli chcesz, żeby CommView pokazywał nazwy hostów, a nie ich adresy IP w zakładce **Packets (Pakiety)**. Jeśli opcja ta jest aktywna, CommView postara się znaleźć aliasy dla adresów IP. Jeśli żaden alias nie zostanie odnaleziony lub opcja **Convert IP addresses to aliases** jest nieaktywna, CommView wyśle zapytanie do wewnętrzej pamięci DNS z prośbą o zwrócenie nazwy. W przypadku, gdy nie można rozwiązać adresu IP na nazwę, program wyświetla adres IP.

Use non-promiscuous mode (Użyj trybu non-promiscuous) – domyślnie, CommView przełącza adapter sieciowy w tryb promiscuous, co oznacza, że przechwytuje on wszystkie pakiety przesyłane w lokalnym segmencie sieci LAN. Aktywacja tej opcji wyłącza ten tryb pracy. Wtedy adapter przechwytuje tylko pakiety przychodzące i wychodzące do niego. To ustawienie może mieć istotne znaczenie w środowiskach, gdzie obowiązujące zasady wykorzystywania zasobów sieciowych nie powalają administratorom na podsłuchiwanie dowolnego ruchu sieciowego.

Memory Usage (Wykorzystanie pamięci)

Display (Wyświetlanie)

Maximum packets in buffer (Maksymalna liczba pakietów w buforze) – ustawia maksymalną liczbę pakietów, jakie program przechowuje w pamięci i może wyświetlić na liście pakietów (druga zakładka). Na przykład, jeżeli ustawisz tą wartość na 3000, tylko ostatnie 3000 pakietów będzie przechowywanych w pamięci i na liście pakietów. Im wyższa jest ta wartość, tym więcej zasobów komputera program zajmuje.

Jeżeli chcesz mieć dostęp do dużej ilości pakietów, zaleca się użycie możliwości automatycznego zapisywania (zajrzyj do temat Logowanie by uzyskać więcej informacji na ten temat): pozwala na zrzut wszystkich pakietów do pliku logowania na twardym dysku.

Maximum IP statistics lines (Maksymalna liczba linii statystyk IP) - ustawia liczbę linijek tekstu, jakie program wyświetla na zakładce IP Statistics (Statystyki IP). W momencie, gdy liczba połączeń sieciowych przekracza określony przez

użytkownika limit, połączenia, które najdłużej były bezczynne (np. po otwarciu połączenia nie odbywała się wymiana pakietów danych) są usuwane z listy.

Driver Buffer (Windows NT/2000/XP only) (Bufor sterownika) - ustawia rozmiar bufora dla sterownika. To ustawienie wpływa w znaczący sposób na wydajność programu: im więcej pamięci jest zajmowanej na potrzeby bufora sterownika programu, tym mniej pakietów program gubi. W przypadku sieci LAN o małym obciążeniu i połączeń dodzwanianych (dial-up) rozmiar bufora nie jest ustawieniem krytycznym – nie ma aż tak wielkiego znaczenia jak np. w przypadku bardziej obciążonych lokalnych sieci komputerowych. W przypadku sieci LAN o dużym obciążeniu możesz chcieć zwiększyć rozmiar bufora zwłaszcza, jeżeli zauważysz, że w trakcie przechwytywania program gubi niektóre pakiety. By sprawdzić jak duża jest ilość traconych przez program pakietów, użyj polecenia z menu **File (Plik) => Performance Data (Osiągi),** podczas gdy przechwytywanie pakietów danych jest włączone.

IP Statistics (Statystyki IP)

Display Logic (Rodzaj wyświetlania) – pozwala wybrać sposób wyświetlania statystyki IP, który najlepiej pasuje do Twoich potrzeb. Wybranie pozycji z rozwijanej listy wyświetli opis wybranego sposobu. W większości przypadków zalecane jest użycie domyślnego sposobu wyświetlania – schematu **Smart**.

Define Local IP Addresses (Definiuj lokalne adresy IP) – powinieneś wykorzystać tę opcję, gdy monitorujesz hosty o adresach IP wewnętrznych LAN i zewnętrznych oraz, gdy duży procent ruchu stanowią pakiety przechodzące. Opcja ta ułatwia odpowiednie przypisanie do kolumn w widoku pakietów przez program adresów IP zewnętrznych i wewnętrznych. Opcja ta będzie działała tylko dla schematu **Smart**.

Colors (Kolory)

Packet color (Kolor pakietu) – ustawia kolor służący do wyświetlania pakietów na zakładce Packets (Pakiety) w oparciu o kierunek pakietu (przychodzący, wychodzący, przechodzący). By zmienić kolor, wybierz kierunek pakietu z rozwijanej listy i kliknij kolorowy prostokąt.

Colorize Packet Headers (Koloruj nagłówki pakietów) – zaznacz tą opcję, jeżeli chcesz, by CommView wyświetlał zawartość pakietów używając kilku kolorów. Jeżeli ta opcja jest zaznaczona, program wyświetla nagłówki MAC, IP, oraz TCP/UDP/ICMP używając różnych kolorów. By zmienić kolor, wybierz rodzaj nagłówka, dla którego chcesz zmienić kolor i kliknij na kolorowym prostokącie.

Formula syntax highlighting (Formuła podkreślania składni) – ustawia zasady podkreślania składni w formułach, zobacz Zaawansowane reguły.

Selected byte sequence color (Wybierz kolor sekwencji bajtów) – ustawia kolor wyświetlania sekwencji bajtów zaznaczonych w oknie dekodera pakietu. By zmienić kolor, wybierz kierunek pakietu z rozwijanej listy i kliknij kolorowy prostokąt.

Decoding (Dekodowanie)

Always fully expand all nodes in the decoder window (Zawsze całkowicie rozwijaj wszystkie węzły w oknie dekodera) – steruje rozwijaniem węzłów w oknie dekodera.

Decode up to the first level only in ASCII export (Dekoduj do pierwszego poziomu tylko przy eksporcie ASCII) – opcja ma wpływ na format dekodowania, gdy eksportujesz log pakietu lub pakiet do pliku ASCII. Gdy jest zaznaczona, tylko najwyższe poziomy dekodowania zostaną zapisane. Na przykład, gdy zapisujesz pakiet TCP/IP i opcja jest wyłączona, wszystkie węzły typu usługi są zapisane. Gdy opcja jest aktywna, węzły usług nie zostają zapisane. Opcja umożliwia generowanie plików ASCII wypełnionych mniejszą ilością informacji.

Ignore incorrect checksums when reconstructing TCP sessions (Ignoruj niepoprawne sumy kontrolne podczas rekonstruowania sesji TCP) – opcja dotyczy uszkodzonych pakietów przechwyconych przez CommView. Domyślnie jest aktywna i dlatego program nie odrzuca pakietów z błędami w sumach kontrolnych podczas rekonstruowania sesji TCP. Jeśli opcja zostanie wyłączona, pakiety z błędnymi sumami kontrolnymi zostaną odrzucone. Użytkownicy kart gigabajtowych powinni mieć na uwadze, że wszystkie wychodzące pakiety będą miały niepoprawne sumy kontrolne, gdy funkcja "checksum offload" będzie dostępna. Dlatego szczególnie ci użytkownicy nie powinni wyłączać tej opcji.

Miscellaneous (Różne)

Hide from the taskbar on minimization (Ukryj z paska gdy zminimalizowany) – zaznacz tą opcję jeżeli nie chcesz widzieć przycisku programu na pasku zadań po minimalizacji okna programu. Jeżeli ta opcja jest zaznaczona, użyj ikony programu znajdującej się w zasobniku systemowym w celu przywrócenia go po zminimalizowaniu.

Allow multiple application instances (Zezwalaj na uruchamianie kilku kopii programu w tym samym czasie) – opcja niedostępna w Windows 95, pozwala n przechwytywanie pakietów jednocześnie z większej ilości adapterów sieciowych.

Prompt for confirmation when exiting the application (Poproś o potwierdzenie podczas zamykania aplikacji) – przed zamknięciem program zapyta o potwierdzenie.

Auto-scroll packet data window (Automatycznie przewijaj okno zawierające dane pakietu) – jeżeli ta opcja jest zaznaczona, program automatycznie przewija tekst pakietów, gdy wybierzesz nowy pakiet z listy (ale tylko wtedy, gdy tekst nie mieści się w oknie). Jest to użyteczne wtedy, kiedy chcesz widzieć treść dużego pakietu bez ręcznego przewijania zawartości okna.

Auto-scroll packet list to the last packet (Automatycznie przewijaj listę do ostatniego pakietu) – program automatycznie przesunie listę pakietów w zakładce **Packets (Pakiety)** tak, aby wskazywać na ostatni przechwycony pakiet.

Auto-sort new records in IP statistics (Sortuj automatycznie nowe rekordy w statystyce IP) – jeżeli ta opcja jest zaznaczona , program automatycznie sortuje nowe rekordy na zakładce IP Statistics (Statystyki IP) w oparciu o zdefiniowane przez użytkownika kryterium (np.: zdalne adresy IP w porządku rosnącym).

Smart CPU utilization control (Kontrola wykorzystania procesora Smart CPU) – program zmniejsza częstotliwość odświeżania ekranu zwiększając wydajność przechwytywania pakietów (opcja istotna, gdy ruch pakietów jest wzmożony).

Run on Windows startup (Uruchom podczas uruchamiania systemu) – jeżeli ta opcja jest zaznaczona, program jest automatycznie uruchamiany za każdym razem kiedy jest uruchamiany system operacyjny Windows.

Run minimized (Uruchom i zminimalizuj) - jeżeli ta opcja jest zaznaczona, program jest uruchamiany jako zminimalizowany, główne okno nie jest wyświetlane aż do momentu, kiedy klikniesz na ikonie programu znajdującej się w zasobniku systemowym (prawy dolny róg ekranu) lub na przycisk na pasku zadań.

Znajdź pakiet

Okno dialogowe **Search (Szukaj) => Find Packet (Znajdź pakiet)** pozwala znaleźć pakiety pasujące do podanego wzorca. Wpisz poszukiwany ciąg znaków, wybierz typ podanej informacji (**String – Ciąg znaków**, **Hex – Szesnastkowo** lub **IP Address – adres IP**), i kliknij **Find Next (Znajdź następny)**. Program zacznie poszukiwanie pakietów, które pasują do kryterium wyszukiwania i wyświetli je na zakładce **Packets (Pakiety)**.

Możesz wprowadzić tekst albo jako ciąg znaków (dowolny tekst), adres IP lub jako wartość szesnastkową. Trzecia metoda powinna być użyta w momencie, gdy chciałbyś wpisać jakieś znaki niedrukowalne: po prostu wpisz wartości szesnastkowe tych znaków oddzielone spacjami, np.: AD 0A 02 78 04.

Zaznacz **Match Case (Rodzaj zgodności)**, jeżeli chcesz, by w trakcie przeszukiwania była rozróżniana wielkość liter. Zaznacz **At offset (W ofsecie (hex))** by szukać ciągu, który zaczyna się od określonego miejsca. Pamiętaj, że wskaźnik przesunięcia jest liczbą szesnastkową

Zestawienie portów

To okno wyświetla tabelę zawierającą numery portów i odpowiadające im nazwy usług sieciowych. To zestawienie jest pobierane z pliku SERVICES instalowanego przez system Windows. Zależnie od wersji systemu Windows, plik SERVICES znajduje się w innym folderze: w Windows 95/98/Me można go znaleźć w folderze \Windows, a w Windows NT/2000/XP znajduje się on w folderze \Winnt\system32\drivers\etc. Możesz dokonywać ręcznej edycji tego pliku, jeżeli chcesz dopisać jakiś port i nazwę usługi. CommView czyta ten plik w trakcie uruchamiania, więc Twoje zmiany dokonane w nim zostaną wyświetlone dopiero po kolejnym uruchomieniu programu.

Porady & rozwiązywanie problemów

Najczęściej zadawane pytania

W tym rozdziale znajdziesz odpowiedzi na niektóre z najczęściej zadawanych pytań. Najnowsza wersja FAQ (Frequently Asked Questions) jest zawsze dostępna pod adresem http://www.tamos.com/products/commview/faq.php

Q. Czy CommView może być użyty do przechwytywania pakietów z interfejsu dial-up (RAS)?
A. Tak, pod Windows 95/98/Me/NT/2000/XP.

Q. Co właściwie CommView "widzi", kiedy jest zainstalowany na PeCecie podłączonym do sieci LAN?
A. CommView przełącza kartę sieciową w tzw. tryb promiscuous, który umożliwia przechwytywanie całego ruchu sieciowego w obrębie danego segmentu sieci LAN. Innymi słowy, przechwytuje i analizuje pakiety adresowane do pozostałych komputerów znajdujących się w danym segmencie sieci, nie tylko te przeznaczone dla komputera, na którym jest uruchomiony program. Dla kart bezprzewodowych (Wireless Ethernet) istnieje możliwość monitorowania tylko ruchu bezpośrednio związanego z hostem. Istnieje też problem sieci przełączanych (patrz poniżej).

Q. Jestem podłączony do sieci LAN za pośrednictwem przełącznika i kiedy uruchamiam CommView przechwytuje on tylko packiety wysyłane do i z mojego komputera, nie widzę ruchu sieciowego generowanego przez inne komputery w sieci. Dlaczego tak się dzieje?
A. W odróżnieniu od koncentratorów, przełączniki zapobiegają tzw. bezładnemu węszeniu (przechwytywaniu wszystkich pakietów w danym segmencie sieci LAN). W sieciach przełączanych (switched network environment), CommView (oraz każdy inny analizator pakietów sieciowych) ma ograniczenia w postaci nasłuchiwania tylko ruchu typu broadcast, multicast oraz wysyłanego do i z hosta, na którym uruchomiono CommView. Większość współczesnych przełączników wspiera tzw. "port mirroring", czyli funkcję umożliwiającą przesyłanie wszystkich pakietów z określonych portów urządzenia do określonego portu. Dzięki tej opcji możliwe jest monitorowanie ruchu w całym segmencie sieci LAN. Szczegóły konfiguracyjne znajdują się w dokumentacji przełączników. Różni producenci stosują różne nazwy określające tę przydatną cechę.

Producent	**Nazwa związana z „port mirroring”**	**Modele wspierające “port mirroring”**
Cisco	Port spanning	Cisco Catalyst 1900 Series Switches Cisco Catalyst 6000 Family Switches
3COM	Roving analysis port (RAP)	3Com SuperStack 3 Switch 4400
Intel	Port mirroring	Intel Express 460T Intel Express 480T

Q. Ok, jestem podłączony do sieci LAN za pomocą koncentratora, ale nadal nie mogę przechwytywać pakietów, podobnie jak poprzez przełącznik. Dlaczego tak się dzieje?
A. Są dwie możliwości: albo masz przełącznik, który przez producenta został nazwany koncentratorem (np. Linksys), albo masz koncentrator współpracujący z kartami o różnej przepustowości (np. jeśli masz kartę 10 Mbit nie możesz podglądać ruchu generowanego przez karty 100 Mbit).

Q. Czy CommView może przechwytywać pakiety z adaptera, który nie ma adresu IP?
A. Tak. Jest to bardzo wygodne zwłaszcza podczas testowania sieci. Nie musisz wtedy znać zakresów adresów IP w niej wykorzystywanych. Po prostu podłączasz komputer do sieci i rozpoczynasz przechwytywanie pakietów. Musisz jednak wyłączyć powiązanie adaptera sieciowego ze stosem protokołów TCP/IP. W Windows 2000/XP otwórz Control Panel (Panel Sterowania) => Network Connections (Połączenia sieciowe), kliknij prawym przyciskiem myszy na ikonie adaptera, wybierz Properties (Właściwości), odznacz wszystkie wpisy, które nie mają być wykorzystywane przez adapter. W Windows 9x Control Panel (Panel Sterowania) => Network (Sieć), wybierz TCP/IP => ikona karty sieciowej, kliknij Remove (Usuń), i uruchom ponownie komputer.

Q. Uruchomiłem program i kliknąłem "Start Capture", ale żadne pakiety nie są wyświetlane. Dlaczego?
A. Dwie możliwe przyczyny: albo wybrałeś nieużywany interfejs sieciowy, lub popełniłeś błąd podczas konfiguracji reguł przechwytywania. Spróbuj wyłączyć reguły i zobacz, co się stanie. W każdej sytuacji, nawet wtedy, kiedy reguły przechwytywania są aktywne, program na pasku statusu powinien wyświetlać liczbę wszystkich pakietów, więc zanim zaczniesz wpadać w panikę spójrz właśnie tam.

Q. Zauważyłem, że sumy kontrolne pakietów wychodzących IP/TCP/UDP są niepoprawne. Dlaczego?
A. Nowe gigabajtowe karty sieciowe posiadające sprzętowy mechanizm tworzenia sum kontrolnych. Pozwala to częściowo odciążyć procesor komputera. Ponieważ CommView przejmuje pakiety jeszcze przed interfejsem karty sieciowej, pojawiają się błędy. Jest to normalna sytuacja. Należy jedynie zapoznać się z rozdziałem Ustawianie opcji, w celu sprawdzenia, czy opcja Ignoruj niepoprawne sumy kontrolne podczas rekonstruowania sesji TCP jest aktywna.

Q. Czy CommView potrafi używać nie-Ethernetowych kart sieciowych, takich jak TokenRing?
A. Obecnie nie, przykro nam.

Q. Czy CommView działa na komputerach wieloprocesorowych?
A. Tak.

Q. Łączę się z siecią na pomocą modemu kablowego xDSL. Czy CommView będzie mógł monitorować ruch sieciowy?
A. Tak, jeśli twój modem ma interfejs dual USB/Ethernet i jest podłączony do karty ethernetowej. Jeśli modem połączony jest z komputerem za pomocą USB – musisz spróbować (może będzie działał).

Q. Mój firewall ostrzega mnie, że CommView "attempting to access the Internet." (próbuje uzyskać dostęp do sieci Internet). Wiem, że istnieją programy monitorujące poczynania użytkowników w sieci. Czemu CommView próbuje uzyskać dostęp do Internetu?
A. CommView próbuje uzyskać nazwy hostów należące do adresów IP i w tym celu kontaktuje się z serwerem DNS. Istnieje możliwość wyłączenia tej cechy (Settings => Options => Disable DNS resolving), ale wtedy adresy IP nie będą rozwiązywane na nazwy hostów. Zapytania DNS to jedyny typ połączeń programu CommView z Internetem. CommView nie wykonuje żadnych ukrytych zadań. Nie sprzedajemy programów typu spyware.

Q. W Windows 2000/XP jestem często zalogowany jako użytkownik bez praw administracyjnych. Czy aby korzystać z CommView muszę się zalogować jako administrator?
A. Nie, możesz otworzyć folder programu, trzymając SHIFT kliknąć prawym przyciskiem myszy plik CV.exe i wybrać "Run As" (Uruchom jako). Potem należy wpisać login i hasło konta z prawami administracyjnymi. Program zostanie uruchomiony.

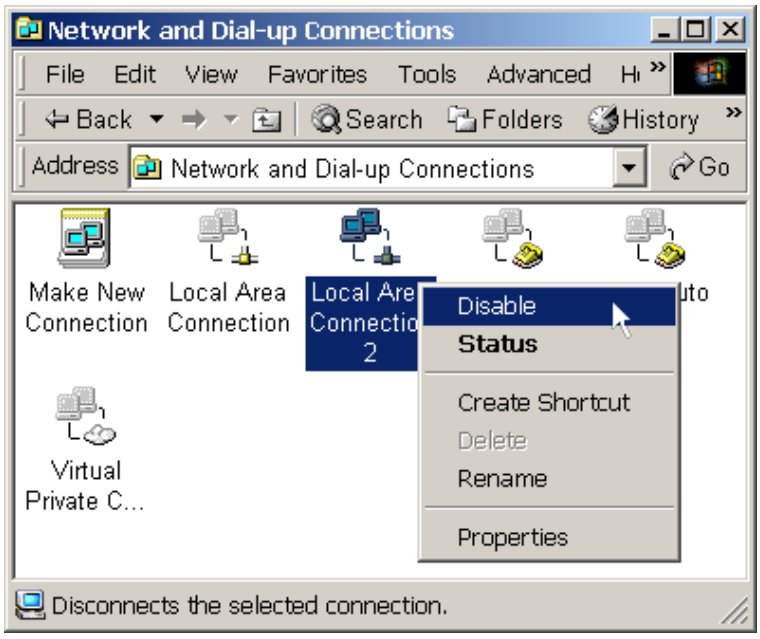
Q. Mam Windows NT, i widzę kilka wpisów "Remote Access Service WAN Wrapper" na liście adapterów sieciowych. Który powinienem wybrać, by CommView zaczął przechwytywać pakiety RAS?
A. To zależy od Twojego systemu. Najłatwiej jest wypróbować jeden po drugim, i w większości przypadków któryś z nich zadziała. W przypadku jednego interfejsu Remote Access Service WAN Wrapper możesz spotkać się z pewnym niepożądanym efektem: CommView przechwytuje i wyświetla pakiety, lecz pakiety nie są dostarczane programom sieciowym (np.: limit czasu połączenia minął itd.). Jeżeli masz ten problem, po prostu zakończ przechwytywanie i wybierz inny interfejs RAS WAN Wrapper z listy.

Q. Mam Windows 95 i połączenie dodzwaniane (dial-up). Kiedykolwiek kliknę na "Stop Capture" mój modem zrywa połączenie. Mogę coś z tym zrobić?
A. Tak, powinieneś ściągnąć i zainstalować uaktualnienia zarówno interfejsu Winsock jak i programu Dial-Up Networking dla Windows 95 przygotowane przez firmę Microsoft, to rozwiąże ten problem. Weź pod uwagę, że kolejność instalacji jest istotna, najpierw Windows Socket 2 Update a potem Dial Up Networking 1.4 Performance & Security Update.

Windows Socket 2 Update

Dial Up Networking 1.4 Performance & Security Update

Q. Używam Windows 2000, kiedy próbuję odinstalować program widzę komunikat: "CommView will now uninstall the drivers. Click "OK" to continue. This can take between 10 and 60 seconds." (CommView odinstaluje teraz sterowniki. Kliknij OK. by zacząć. To może potrwać 10 – 60 sekund.) Ale nic się potem nie dzieje!
A. Może się tak zdarzyć, jeżeli połączenia sieciowe są aktywne w trakcie deinstalacji programu. Powinieneś tymczasowo zablokować wszystkie aktywne połączenia tak jak jest pokazane poniżej:



Zaraz po zablokowaniu aktywnych połączeń sieciowych, CommView wznowi proces deinstalacji, po zakończeniu którego możesz ponownie odblokować połączenia sieciowe.

Q. Korzystam z Windows 2000 Terminal Server i mam problem z uruchomieniem CommView poprzez klienta usług terminalowych.
A. Rozwiązanie zależy od wersji CommView:

CommView 3.0 i nowszy: zrestartuj serwer po zainstalowaniu programu CommView.

CommView 2.4 – 2.6: kliknij tutaj, aby pobrać uaktualnioną wersję pliku CV2K.DLL, nadpisz stary plik (w folderze aplikacji),

rozpocznij i zacznij przechwytywanie jako użytkownik lokalny a następnie zrestartuj komputer. Po ponownym uruchomieniu systemu upewnij się, że możesz przechwytywać pakiety jako użytkownik lokalny. Nie powinieneś mieć więcej problemów z korzystaniem z CommView.

Jedynym ograniczeniem jest fakt, że tylko jeden adapter może być otwarty przez jednego użytkownika. Oznacza to, że na przykład dwóch użytkowników (lokalny i zdalny) nie może używać tego samego adaptera w tym samym czasie do przechwytywania pakietów.

Q. Kiedy monitoruję połączenie Dial-up, nie widzę pakietów PPP podczas ustanawiania sesji (CHAP, LCP, etc). Czy to jest normalne?
A. Niestety, pakiety PPP można przechwytywać tylko w Windows 95/98/NT/ME, CommView nie robi tego w Windows 2000/XP.

Q. Czy mogę zmieniać karty PC w moim notebooku, podczas gdy CommView jest uruchomiony?
A. Nie, bezpieczniej jest zamknąć program CommView, potem zmienić lub podłączyć/odłączyć kartę, i ponownie uruchomić program. Lista kart sieciowych zostanie automatycznie uaktualniona.

Q. Jestem podłączony do sieci LAN generującej wysoki ruch sieciowy, zauważyłem, że CommView zwiększa obciążenie procesora i/lub staję się mniej stabilny. Co mogę z tym zrobić?
A. Najlepszym sposobem optymalizacji wydajności programu jest użycie reguły w celu odfiltrowania pakietów, których nie potrzebujesz śledzić. Np.: przesłanie pliku o rozmiarze 50 MB pomiędzy dwoma komputerami w Twojej sieci LAN potrafi wygenerować w przybliżeniu 40,000 pakietów NetBIOS i przy założeniu, że prędkość transmisji wynosi 1 MB na sekundę, może to być naprawdę duże obciążenie dla programu. Lecz normalnie nie potrzebujesz przeglądać każdego przesyłanego pakietu NetBIOS, więc możesz tak skonfigurować program CommView, by przechwytywał tylko pakiety IP. CommView posiada elastyczny system filtrowania, więc możesz dokładnie dostroić aplikację, by wyświetlała tylko te pakiety, których naprawdę potrzebujesz. Jeśli interesują cię tylko informacje statystyczne (wykresy, diagramy) wykorzystaj polecenie menu "Suspend packet output" pozwalające na przechwytywanie danych bez wyświetlania ich w trybie rzeczywistym. Zobacz też rozdział Przechwytywanie dużego ruchu sieciowego.

Q. Czy są znane jakieś konflikty z innym oprogramowaniem?
Obecnie znane nam są konflikty z następującymi programami:

- SoftIce by Numega: Możliwe zawieszenie systemu.
- PGPNet 7.0 by NAI: Gdy PGP jest powiązany z adapterem dial-up – możliwe jest ukazanie się "niebieskiego ekranu śmierci".
- Sygate Personal Firewall: Problem ze sterownikiem adapter dial-up a w Windows 2000/XP – możliwe jest ukazanie się "niebieskiego ekranu śmierci" podczas próby monitoringu (CommView 3.3 lub starszy). Problemy nie występują podczas monitoringu przy wykorzystaniu interfejsu ethernetowego. Problem poprawiony w CommView 3.4.
- Kerio Personal Firewall version 2.x: Niezgodność ze sterownikiem KPF w Windows XP– możliwe jest ukazanie się "niebieskiego ekranu śmierci", gdy monitorujesz ruch poprzez adapter dial-up i zainstalowałeś CommView po zainstalowaniu KPF. Problemy nie występują podczas monitorowania przy wykorzystaniu interfejsu ethernetowego. Problem poprawiony w KPF 3.0.

Jeśli odkryłeś jakiekolwiek nieprawidłowości w funkcjonowaniu programu, będziemy wdzięczni za informacje.

Q. Czy muszę być profesjonalistą by używać tego programu?
A. Nie. Mamy nadzieję, że nawet niedoświadczeni użytkownicy znajdą w nim coś, co im się przyda, co uznają za przydatne. Nie musisz używać wszystkich funkcji programu. Np.: nawet początkujący użytkownicy komputera mogą być zainteresowani, by mieć pełen obraz sytuacji w zakresie połączeń sieciowych, w których biorą udział ich komputery, lub mogą chcieć dowiedzieć się, czy zainstalowany wczoraj program tak naprawdę nie jest koniem trojańskim, który wysyła ich hasła dial-up pod określony adres e-mail.

Q. Gdzie mogę znaleźć dobry FAQ związany z przechwytywaniem i analizą pakietów sieciowych?
A. Zobacz tutaj:

Sniffing (network wiretap, sniffer) FAQ

Protocols.com

Przechwytywanie dużego ruchu sieciowego

Podczas przechwytywania ruchu sieciowego o dużym natężeniu, możliwe jest wystąpienie przeciążenia procesora (CPU), które może prowadzić do spowolnień działania aplikacji. W takim przypadku powinno się stosować reguły filtrujące z całego ruchu tylko te potrzebne pakiety. Na przykład wysłanie pliku o wielkości 50 MB do drugiej maszyny w sieci LAN zajmie w przybliżeniu 40,000 pakietów NetBIOS przy transferze danych 1MB na sekundę, co może być dużym obciążeniem dla aplikacji. Zwykle jednak nie ma potrzeby monitorować każdego pakietu NetBIOS, więc wystarczy skonfigurować CommView do przechwytywania tylko pakietów IP. CommView został wyposażony w wszechstronny system filtrów pozwalający na praktycznie dowolne dopasowanie ustawień aplikacji w zależności od potrzeb związanych z monitorowaniem ruchu w sieci. Jeśli potrzebne są tylko statystyki związane z ruchem (diagramy, wykresy i tabelki), można skorzystać z opcji "Suspend packet output" (Zawieś wyświetlanie pakietów) z menu Plik (opcja dostępna podczas przechwytywania), która powala na zbieranie danych statystycznych bez wyświetlania przechwyconych pakietów w czasie rzeczywistym.

Czynniki wpływające na wydajną pracę programu:

- Szybki procesor CPU (przynajmniej Pentium III)
- Rozmiar pamięci RAM (128 lub więcej)
- System operacyjny zbudowany na technologii NT (najlepiej Windows 2000/XP)
- Wykorzystanie reguł do filtrowania przechwytywanych pakietów
- Wykorzystywanie trybu "Suspend packet output" (Zawieś wyświetlanie pakietów)

Czynniki wpływające na spadek wydajności programu:

- Zbyt wolny procesor lub niewystarczająca ilość pamięci RAM
- Wykorzystywanie dużej ilości aliasów MAC i IP
- Wykorzystywanie konwersji port number (numer portu) => port name (nazwa usługi działającej na porcie)

Praca z kilkoma programami na raz

CommView może przechwytywać pakiety z kilku adapterów sieciowych na raz (opcja niedostępna w Windows 95). W menu **Settings (Ustawienia) => Options (Opcje) => Miscellaneous (Różne)** zaznaczenie opcji **Allow Multiple Application Instances (Zezwalaj na uruchamianie kilku kopii programu w tym samym czasie)** pozwala na uruchomienie kilku kopii programu. Każda z kopii uruchomionej może monitorować ruch tylko jednego adaptera. Podobne ograniczenie występuje też, gdy program uruchomiony jest poprzez usługę Terminal Server: dwaj użytkownicy (lokalny i zdalny) nie mogą przechwytywać pakietów wykorzystując ten sam adapter sieciowy na tym samym serwerze.

Uruchamianie CV w trybie ukrytym

Aby uruchomić CommView w trybie ukrytym:

1. Uruchom CommView korzystając z przełącznika "hidden" (ukryty):

   CV.EXE hidden

2. Gdy CommView został już uruchomiony, w celu ukrycia programu zastosuj kombinację klawiszy: ALT+SHIFT+h. Aby "odkryć" program naciśnij: ALT+SHIFT+u.

Pamiętaj, że w Windows nie można całkowicie ukryć aplikacji. Aplikacje (procesy) uruchomione w systemie można zobaczyć w oknie Menedżera zadań systemu, które dostępne jest poprzez naciśnięcie w Windows NT/2000/XP: ALT+CTRL+DEL. W Windows 95/98/ME, trzeba wykorzystać dodatkowe oprogramowanie.

Parametry linii komend

Program umożliwia stosowanie komend wydawanych w trybie tekstowym::

- Aby załadować i aktywować zestaw reguł, użyj przełącznika "/ruleset":

  CV.EXE /ruleset "C:\Program Files\CommView\Rules\POP3Rules.rls"

  Jeśli w nazwie lub w ścieżce dostępu znajdują się odstępy, należy zawrzeć ją między znakami (" ").

- Aby otworzyć i uruchomić wybrany adapter sieciowy, użyj przełącznika "/adapter":

  CV.EXE /adapter "Intel(R) PRO/1000 T Desktop Adapter"

  Nazwa adaptera musi być zawarta między znakami (" "). Dobrym pomysłem jest skopiowanie nazwy adaptera z okna ustawień sieciowych systemu przy pomocy Ctrl-C (kopiowanie do schowka).

Oba parametry mogą być wykorzystywane jednocześnie.

Wymiana danych z innymi aplikacjami

Od wersji 3.0, CommView udostępnia prosty interfejs TCP/IP pozwalający na przetwarzanie pakietów przechwyconych przez inne aplikacje w trybie rzeczywistym.

Jak to działa
Powinieneś uruchomić CommView z przełącznikiem "mirror" adresem IP i numerem portu.

Przykłady:
CV.EXE mirror:127.0.0.1:5555 // dubluje pakiety do pętli zwrotnej lokalnego komputera na port TCP 5555
CV.EXE mirror:192.169.0.2:10200 // dubluje pakiety na adres IP na port TCP 10200

Gdy CommView zostanie uruchomiony z przełącznikiem "mirror" próbuje ustanowić sesję TCP łącząc się z podanym adresem IP i usługą działającą na podanym porcie. Oznacza to, że jeszcze wcześniej należy uruchomić drugą aplikację. Gdy nawiązanie połączenia nie powiedzie się, CommView będzie ponawiał próby co 15 sekund. Gdy połączenie zostanie nawiązane, CommView rozpoczyna przesyłanie przechwyconych przez siebie pakietów w czasie rzeczywistym.

Format danych
Aby odczytać strumieniowo przesyłane dane, aplikacja nasłuchująca musi umieć je zdekodować. CommView wykorzystuje proste nagłówki pozwalające na podział strumienia danych na poszczególne pakiety. Każdy pakiet jest poprzedzony 3 bajtowym nagłówkiem. Pierwsze dwa bajty to długość pakietu (bez nagłówka CommView). Zwróć uwagę, że stosowany jest tutaj zapis odwrotny (little-endian byte order). Na przykład 0x0200 wynosi 2, a 0x0002 to 512. Trzeci bajt definiuje kierunek przechwyconego pakietu:

0x00 – przechodzący (pass-through)
0x01 – przychodzący (inbound)
0x02 – wychodzący (outbound)

Przykłady:

0xE80000 – pakiet przechodzący (pass-through), długość 232 bajty
0xB10102 - pakiet wychodzący (outbound), długość 433 bajty

Znając te informacje, możesz łatwo stworzyć parser pakietów przesyłanych przez CommView.

Przykładowe projekty
Dwie proste aplikacje demonstrujące nasłuchiwanie, dekodowanie pakietów ze strumienia danych oraz wyświetlanie surowych danych.

- http://www.tamos.com/products/commview/samp_mirr_c.zip. Projekt Visual Studio z kodem w C++
- http://www.tamos.com/products/commview/samp_mirr_d.zip. Projekt Delphi z kodem w Pascalu. Do kompilacji wymagane są komponenty ICS przygotowane przez François Piette dostępne: http://overbyte.delphicenter.com/frame_index.html

Przepustowość
Połączenie wykorzystywane przez CommView oraz inną aplikację, do której przesyłane są przechwycone pakiety musi mieć odpowiednią przepustowość. Jeśli CommView przechwytuje z prędkością 500 Kbit/sek., a połączenie może obsłużyć tylko 50 Kbit/sek., mogą wystąpić różnorakie problemy. Jeśli potrzebujesz bardziej wszechstronne rozwiązanie, które można optymalizować, zainteresuj się programem CommView Remote Agent.

Niestandardowe dekodowanie

Od wersji 4.0, CommView pozwala na wykorzystywanie niestandardowego dekodera dostarczonego przez użytkownika. Jeśli zostanie on zaimplementowany, informacje od niego będą wyświetlane w dodatkowym polu zakładki **Packets (Pakiety)**. Dekoder musi być postaci 32-bitowej biblioteki dynamicznej DLL o nazwie "Custom.dll", która eksportuje jedyną procedurę o nazwie "Decode". Poniżej znajdują się jej prototypy w językach C i Pascal:

```
extern "C" {
  void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);
}
```

```
procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

Biblioteka DLL musi znajdować się w folderze aplikacji CommView. Podczas uruchamiania CommView szuka pliku "Custom.dll" w swoim katalogu i jeśli go znajdzie, ładuje go do pamięci. Gdy znajdzie wpis o nazwie "Decode" dodaje nową kolumnę o nazwie "Custom" do widoku listy pakietów.

Gdy zostanie przechwycony pakiet, który powinien zostać wyświetlony, CommView wywołuje procedurę "Decode" przekazując zawartość pakietu do biblioteki DLL. Procedura "Decode" musi przetworzyć dane i zwrócić je do bufora. Pierwszy argument to wskaźnik do danych, drugi to rozmiar pakietu, trzeci jest wskaźnikiem do bufora wynikowego, a czwarty jest rozmiarem bufora wynikowego (obecnie zawsze 1024 bajtów). Bufor jest alokowany i zwalniany przez CommView, co zwalnia programistę od dodatkowych czynności. Zawartość bufora wynikowego wyświetlana jest w kolumnie "Custom".

Twoja procedura musi być wystarczająco szybka, aby poradzić sobie z tysiącami pakietów na sekundę, w przeciwnym razie może doprowadzić do znacznego spowolnienia aplikacji. Nie zapomnij wykorzystać STDCALL.

Przykładowe projekty

Dwie biblioteki DLL są dostępne jako demonstracja prostej operacji: wyjściem funkcji "Decode" jest kod szesnastkowy ostatniego bajtu pakietu. Oczywiście dekoder może też wykonywać bardziej wymyślne operacje.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Projekt Visual Studio z kodem w C++
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Projekt Delphi z kodem w Pascalu

Informacje

Jak nabyć CommView

Program dostępny jest jako 30-dniowa wersja próbna. Poniżej znajduje się zestawienie opłat licencyjnych za użytkowanie programu. Dzięki temu będzie można korzystać z w pełni funkcjonalnej, legalnej i pozbawionej ograniczeń wersji programu:

Rodzaj licencji	**Cena, US$**
CommView Home License 1 user (dla prywatnego, niekomercyjnego użytku)	129.00
CommView Enterprise License 1 user (dla profesjonalnego, komercyjnego użytku)	249.00

- Tańszy typ licencji **Home License** pozwala na wykorzystywanie programu do niekomercyjnych zastosowań. CommView może być wykorzystywany do monitorowania maksymalnie 5 hostów w sieci domowej.

- Droższy typ licencji **Enterprise License** pozwala na wykorzystywanie programu wszędzie do zastosowań komercyjych i niekomercyjnych bez ograniczeń w ilości monitorowanych hostów.

Jedna kopia programu CommView może być wykorzystywana przez jedną i tą samą osobę na jednym lub więcej komputerach lub może być zainstalowana na jednym komputerze i używana niejednocześnie przez więcej niż jedną osobę. Informacje związane z opłatami za licencje wieloużytkownikowe dostępne są na naszej stronie.

Jako zarejestrowany użytkownik masz prawo do:

- W pełni funkcjonalnej i nieograniczonej kopii programu
- Bezpłatnych uaktualnień przez rok od daty zakupu licencji
- Informacji dotyczących uaktualnień oraz nowych produktów
- Bezpłatnego wsparcia technicznego

Akceptujemy zamówienia realizowane za pomocą kart kredytowych, zamówienia telefoniczne i przez faks, czeki, przelewy. Zastrzegamy sobie także prawo do zmiany warunków licencji oraz cen bez powiadomienia. Najbardziej aktualne informacje dotyczące cen naszych produktów dostępne są na stronie:

http://www.tamos.com/order/

Kontakt

Web

http://www.tamos.com

E-mail

sales@tamos.com (pytania dotyczące oferty handlowej)
support@tamos.com (pozostałe pytania)

Adres i faks

Mailing address:

PO Box 1385
Christchurch 8015
New Zealand

Fax: +64 3 359 0392 (New Zealand)
Fax: +1 503 213-7764 (USA)

Inne produkty TamoSoft

SmartWhois

SmartWhois jest wygodnym narzędziem dostarczającym informacje na temat adresu IP, nazwy hosta lub domeny. Program dostarcza informacje niezależnie od tego, w której z licznych baz są one przechowywane. Umożliwia, w ciągu kilku sekund, otrzymanie informacji: domeny, nazwy sieciowej, kraju, stanu lub prowincji, oraz miasta. Nawet, gdy rozwiązanie adresu IP na nazwę się nie powiedzie, SmartWhois dostarczy inne informacje!

Informacje szczegółowe

Essential NetTools

Essential NetTools jest zbiorem programów przydatnych do diagnozowania i monitorowania połączeń sieciowych komputera. Zawiera wszystkie potrzebne narzędzia sieciowe przydatne w codziennej pracy. Program zawiera narzędzie NetStat wyświetlające otwarte porty, nawiązane sesje między komputerem lokalnym a zdalnymi wiążąc te informacje z nazwami aplikacji z nich korzystających. Zawiera też szybki skaner NetBIOS, NetBIOS Auditing Tool do testowania bezpieczeństwa sieci LAN, monitor udostępnianych przez komputer zasobów, umożliwia też monitorowanie uruchomionych procesów, usług i programów uruchomionych na lokalnym komputerze. Nie są to wszystkie narzędzia. W skład Essential NetTools wchodzą też: Ping, TraceRoute i NSLookup. Program umożliwia tworzenie raportów w formatach: HTML, tekstowym i innych. Zestaw jest bardzo prosty w obsłudze i znakomicie zastępuje narzędzia systemowe, takie jak: nbtstat, netstat oraz NetWatcher, oferując jednocześnie wiele funkcji nie dostępnych dla tych i innych narzędzi systemowych.

Informacje szczegółowe

DigiSecret

DigiSecret jest łatwym w użyciu programem wykorzystywanym do zabezpieczania danych oraz bezpiecznego ich udostępniania. Wykorzystuje ogólnie uznane algorytmy szyfrujące, potrafi generować samorozpakowujące się archiwa oraz współdzielone pliki zabezpieczone przed nieautoryzowanym dostępem. DigiSecret zawiera też narzędzie do kompresji eliminujące potrzebę posiadania programu kompresującego w formacie ZIP. Program integruje się z systemem operacyjnym a jego funkcji dostępne od prawym przyciskiem myszy. Wspiera też mechanizm drag-and-drop (przeciągnij i upuść).

Informacje szczegółowe