



CommView®

Netzwerk Monitor und Analyzer für Microsoft Windows

Hilfe-Dokumentation
Version 7.0

Inhalt

Inhalt	2
Einführung	4
Über CommView	4
Was ist neu?	5
Programmbenutzung.....	8
Überblick	8
Hauptmenü.....	8
Netzwerkschnittstelle zur Paketerfassung auswählen.....	11
Aktuelle IP Verbindungen.....	13
Pakete.....	16
Protokollierung.....	19
Logbetrachter	21
Regeln	23
Erweiterte Regeln.....	28
Alarmer	31
Rekonstruktion von TCP-Sitzungen	35
Pakete Suchen	40
Statistiken und Berichte	41
Die Verwendung von Kennnamen.....	45
Paketgenerator.....	46
Optischer Paketersteller.....	48
NIC Vendor (Hersteller) Identifier (Identifiziertool)	50
Scheduler.....	51
Der Einsatz des Remote Agent	52
RPCAP anwenden	54
Entschlüsselten SSL-Datenverkehr erfassen	55
Loopback Datentransfer erfassen	57
Port Referenz.....	58
Einstellungen	59
Häufig gestellte Fragen.....	65
VoIP-Analyse.....	69
Einleitung.....	69
Arbeiten mit dem VoIP-Analyser	70

SIP- und H.323-Sitzungen	72
RTP-Ströme.....	74
Registrierungen	76
Endpunkte	77
Fehler.....	78
Anrufprotokoll	79
Berichte	80
Anrufwiedergabe	81
VoIP-Protokollbetrachter	84
Arbeiten mit Auflistungen im VoIP-Analyser.....	85
NVF-Dateien	87
Weiterführende Themen.....	88
Erfassung von intensivem Verkehr.....	88
Arbeiten mit mehreren Instanzen.....	89
CommView im nicht sichtbaren Modus	90
Kommandozeilen Parameter.....	91
Datenaustausch mit Ihrer Anwendung	93
Maßgeschneidertes Decoding.....	95
CommView Logdateien Format.....	97
Einkauf und Support.....	99

Einführung

Über CommView

CommView ist ein Programm zur Überwachung des Internet- und Local Area Network-Verkehrs (LAN), das in der Lage ist Netzwerkpakete zu empfangen und zu analysieren. Das Programm sammelt Informationen über die Daten von Wählverbindungen oder Ethernet-Karten und decodiert die zu analysierenden Daten.

CommView erstellt eine Liste der Netzwerkverbindungen sowie eine IP-Statistik und erlaubt einzelne Datenpakete individuell zu untersuchen. Pakete werden bis zur untersten Ebene mit einer Vollanalyse der wichtigsten Protokolle decodiert. Auch ist ein Vollzugriff auf Rohdaten möglich. Die empfangenen Pakete können in Logdateien für weitere Analysen abgespeichert werden. Ein flexibles Filtersystem macht es möglich, nicht zu nutzende Packet zu verwerfen oder nur die Pakete zu erfassen, die Sie wünschen. Durch konfigurierbare Alarmmeldungen kann der Anwender über wichtige Ereignisse, wie verdächtige Pakete, hohe Bandbreitenausnutzung oder unbekannte Adressen informiert werden.

CommView beinhaltet ein VoIP-Modul für detaillierte Analysen, Aufnahme und Wiedergabe von SIP- und H 323-Sprachkommunikationen.

CommView ist ein sehr hilfreiches Werkzeug für LAN-Administratoren, Sicherheitsbeauftragte, Netzwerkprogrammierer und jeden, der einen ausführlichen Überblick über den Netzwerkverkehr an seinem Rechner oder LAN-Abschnitt erhalten möchte. Diese Applikation erfordert eine Ethernet- oder Wi-Fi-Netzkarte, oder einen Standard-Modem-Adapter. CommView verfügt über einen erweiterten Protokoll-Decoder, der Tausende der weit verbreiteten Netzwerk-Protokolle parsen kann.

Zusätzlich erlaubt die neue Fernüberwachungstechnologie den CommView-Benutzern das Aufzeichnen des Datenverkehrs von jedem Computer, auf welchem der sogenannte Remote Agent aktiv ist, ungeachtet des physikalischen Standortes des Computers. Um diese einzigartige Fähigkeit nutzen zu können, ist der Remote Agent als Zusatz für CommView erforderlich.

Was ist neu?

Version 7.0

- Sie können jetzt entschlüsselten SSL-Verkehr zum / vom Computer erfassen, auf dem CommView ausgeführt wird.

Version 6.5

- Ein komplett überarbeiteter Protokoll-Decoder: mehr unterstützte Protokolle und eine Daten-Zusammenfassung für jedes Paket.

Version 6.4

- Neue Betriebssysteme werden unterstützt: Windows Server 2008 32-bit und 64-bit Editionen.
- Verringerte RAM-Auslastung durch das VoIP-Analysemodul. Die neue Version kann bei geringerer RAM-Benutzung mehr simultane Anrufe handhaben.
- Einstellbarer Jitter-Puffer für eine realistischere Simulation der realen VoIP-Telefonsoundqualität.
- Verbesserter "Suche-Dialog": Suchrichtung und Unicode-Suche (UTF-8, UTF-16) werden jetzt unterstützt.
- Mehr flexible Decoder-Baumoptionen: Sie können jetzt die Anzahl der aufzuklappenden Knoten bestimmen.
- Viele andere Verbesserungen und Fehlerbehebungen.

Version 6.0

- VoIP-Modul für eine gründliche erweiterte Analyse, Aufnahme und Wiedergabe von SIP- und H 323-Sprachnachrichten.
- Visual TCP-Sitzungen mit graphischer Darstellung von Sitzungsdiagrammen.
- Optischer Paketersteller, der die Paketkonstruktion im Paketgenerator erleichtert.

Version 5.5

- Volle IPv6-Unterstützung durch die Applikation (Dekodierung, Filterung, Suche, Alarme).
- UTF-8-Unterstützung bei der TCP-Sitzungsrekonstruktion.
- Optionaler Wiederaufbau fragmentierter IP-Pakete.
- Ein neuer Alarmtyp: Die Applikation kann Nachrichtentexte unter Benutzung der Windows Text-to-speech engine verkünden.
- Einige Verbesserungen und konfigurierbare Optionen bezüglich der Dekodierung und Sitzungsrekonstruktion.
- Ein Ressourcen-Leck unter Windows Vista wurde behoben, wenn der DPI-Wert auf 120 oder höher gesetzt wurde und ein möglicher Systemabsturz ist bei einer überwachten Modemverbindung möglich.

Version 5.4

- Windows Vista-Unterstützung.

Version 5.3

- IP-Landeszuordnung für IP-Adressen erstellt Echtzeit-Ortsangaben für alle durch die Applikation angezeigten IP-Adressen.

- Im Register "Pakete" und im "Logbetrachter" bringen die Spalten im neuen Design mehr Bequemlichkeit. Die Spaltenreihenfolge in allen Registern des Hauptfensters sind jetzt anpassbar.
- Die Fähigkeit eine beliebige Menge von Schnappschüssen des aktuellen Paketpuffers zu erstellen, macht es leichter mit Paketen unter einer schweren Netzwerkbelastung zu arbeiten. Sie können den Puffer jetzt in separaten Fenstern untersuchen, ohne das Risiko alte Pakete zu verlieren und um Pakete anzusehen, die aus dem Fenster herausgescrollt sind.
- Verbesserte Alarme erlauben jetzt anpassbare E-Mail-Benachrichtigungen zu verschicken.
- Größenänderbares Statistikfenster.
- Verbesserter Finden-Dialog.
- Optionale Rasterlinien für eine bessere Paketübersicht.
- Ein paar andere Verbesserungen.

Version 5.1

- Quick-Filter ermöglichen Ihnen neue Ansichten ähnlicher Pakete einfach auf der Grundlage von MAC- bzw. IP-Adressen oder Ports erzeugen zu können.
- Filterung nach Prozessnamen ist jetzt möglich.
- Aktualisierte MAC-Herstellerliste.
- Automatische Anwendungs-Updates.
- Viele weitere Verbesserungen und Fehlerbehebungen.

Version 5.0

- Datenpakete können der Applikation welche diese versendet oder empfangen hat zugeordnet werden. Diese Funktion steht nur unter Windows 2000/XP/2003 zur Verfügung.
- Hochauflösender Zeitstempeldienst (bisher zu Mikrosekunden) ist Verfügbar unter Windows NT/2000/XP/2003).
- Ein neues, kompaktes, offenes Logformat.
- Host-Kommunikation wird nun über grafische Matritzen dargestellt.
- Neue Entschlüsselungsmodule wurden hinzugefügt: MS SQL, LDAP und YMSG. Die Entschlüsselung von SMB und ICQ wurde verbessert.
- Support für Windows XP 64-bit Edition auf AMD Opteron und Athlon64 Prozessoren.
- Mehrere gleichzeitige Remote Agent-Verbindungen werden nun unterstützt.
- Verbesserter Paketgenerator durch Bereitstellung von Vorlagen.
- HTML-Berichte können nun auch grafische Darstellungen enthalten.
- Neue Alarmarten.
- Geringere Anforderungen an die CPU.

Version 4.1

- Jetzt ist es möglich den Datenverkehr von sog. Loopback-Verbindungen zu erfassen, also Pakete welche an oder von einer lokalen IP-Adresse (z. B. 127.0.0.1) gesandt werden. Diese Funktion steht unter Windows NT/2000/XP/2003 zu Verfügung.
- Das Programm kann nun auch die besuchten URL's aufzeichnen.

- Neue Module zur Protokollentschlüsselung wurden hinzugefügt: IMAP, NNTP, SSH, TLS.
- Das offene Plugin-Interface erlaubt Ihnen Ihre eigenen Protokollschlüssel zu implementieren.
- Die TCP-Sitzungsrekonstruktionfenster können nun auch GZIP'd-kompimierten Webinhalt dekomprimieren, ja sogar auch Bilder, die über HTTP-Sessions angezeigt werden. Sitzungsrekonstruktionfenster können nun auch GZIP'd-kompimierten Webinhalt dekomprimieren, ja sogar auch Bilder, die über HTTP-Sessions angezeigt werden.
- Die TCP-Sitzungsrekonstruktionfenster erlauben nun zwischen zwei beliebigen Hosts zur nächsten TCP-Sitzung zu springen. In den bisherigen Versionen konnte nur zwischen den beiden ursprünglich ausgewählten Hosts hin- und hergesprungen werden.
- Das Programm benachrichtigt Sie über Änderungen in der Liste der vorhandenen Netzwerkadapter.
- Die Paketerfassung wird, nach der Rückkehr aus dem Windows-Ruhezustand oder nach einer vorübergehenden Unterbrechung von Windows, automatisch wieder gestartet.
- Token Ring-Adapter werden unterstützt. Diese Funktion steht unter Windows NT/2000/XP/2003 zur Verfügung.
- Jumbo Frames werden unterstützt.
- Das Programm kann neben Echtzeitauswertungen auch vorher abgegriffene Daten statistisch auswerten.
- Die verbesserte Alarmfunktion kann jetzt auch Variablen an bereits laufende Anwendungen oder Alarmmeldungen senden.
- Viele kleinere Verbesserungen.

Version 4.0

- Alarme: Das Programm kann Sie bei entsprechender Konfiguration über bestimmte Paketarten, unbekannte MAC-Adressen, etc. informieren.
- Neue Decoder für folgende Protokolle: DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q.932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNMP, TIME.
- Mehrsprachige Benutzeroberfläche.
- Ein kundenspezifisches Decodermodul kann mit der Applikation verwendet werden.
- Neue Kommandozeilen-Parameter, welche das automatische Laden von Regeln und/oder das Öffnen von Netzwerkadaptern erlauben.
- Das Register TCP-Sitzungsrekonstruktion hat neu eine Finde-Funktion.
- Paketgenerator: Vorlagen für TCP-, UDP- und ICMP-Pakete.
- Eine neue Decodiere als-Funktion erlaubt das Decodieren von unterstützten Protokollen die keine Standard-Ports verwenden.
- Das Programm wurde um eine Reihe von Optionen erweitert.

Programmbenutzung

Überblick

Das Programminterface besteht aus fünf Bereichen, die es Ihnen ermöglichen sich die Daten anzusehen bzw. verschiedene Aktionen mit den empfangenen Paketen durchzuführen. Um die Paketerfassung zu starten, wählen Sie eine Netzwerkkarte aus der Drop-Down-Liste in der Werkzeugleiste und klicken Sie auf **Paketerfassung starten** oder **Datei = > Paketerfassung starten**. Wenn der gewählte Netzwerkadapter Paketverkehr verarbeitet, wird CommView diesen erfassen und anzeigen.

Hauptmenü

Datei

Erfassung starten – startet/stoppt das Empfangen von Paketen.

Paketausgabe unterbrechen – stoppt/nimmt den Echtzeit Paket-Output des zweiten Registers wieder auf.

Fernüberwachungsmodus – ein-/ausblenden der [Fernüberwachungsleiste](#).

Aktuelle IP-Verbindungen speichern unter – erlaubt das Speichern der aktuellen IP-Verbindungen als HTML- oder komma-getrennter CSV-Bericht.

Paketlog speichern unter ... – erlaubt das Abspeichern der Inhalte des Paketregisters in verschiedene Formate.

Log Betrachter – öffnet ein neues [Log Viewer](#)-Fenster.

VoIP-Logbetrachter – öffnet ein neues [VoIP-Logbetrachterfenster](#).

Aktuelle IP-Verbindungen löschen – löscht den Inhalt des Registers Aktuelle IP-Verbindungen (Erstes Register).

Paketpuffer löschen – löscht den Inhalt des Programmpuffers und die Paketliste (Zweites Register).

VoIP-Daten leeren – Entleert den Inhalt des VoIP-Registers.

Durchsatzdaten ... – Zeigt die Performance-Statistik des Programms an: die Zahl der empfangenen und durch den Gerätetreiber ausgeschiedenen Pakete.

Beenden – Beendet das Programm.

Suchen

Finde Paket ... – Mit diesem Dialog [finden Sie Pakete](#), die einen bestimmten Text enthalten.

Gehe zu Paket Nummer ... – Mit diesem Dialog springen Sie zu einer definierten Paketnummer.

Ansicht

Statistiken – Zeigt ein Fenster mit [Datentransfer- und Protokollverteilungsstatistiken](#).

Port Referenz – Zeigt ein Fenster mit der [Portreferenzinformation](#).

Log Verzeichnis – Öffnet das Verzeichnis in dem standardmäßig die Logs abgespeichert werden.

Aktuelle IP Verbindungsspalten – Zeigt/Verbirgt einzelne Spalten im Register Aktuelle IP Verbindungen.

Paketspalten – Zeigt/Verbirgt einzelne Spalten im Paketregister.

Werkzeuge

Paketgenerator – Öffnet das Fenster zur [Paketgenerierung](#).

Rekonstruiere TCP Sitzung – Ermöglicht Ihnen die [Rekonstruktion einer TCP-Sitzung](#) ausgehend vom gewählten Paket. Dabei öffnet sich ein Fenster, das die ganze Kommunikation zwischen zwei Hosts darstellt.

NIC-Herstelleridentifikation – Öffnet ein Fenster, mit dem Sie über die MAC-Adresse den [Netzwerkadapterhersteller identifizieren](#) können.

Paketerfassungplaner – Ermöglicht es [geplante Erfassungsaufgaben](#) hinzuzufügen oder zu löschen.

Einstellungen

Schrift – Zeigt das Untermenü für die Einstellungen der Interface-Fonts.

MAC-Kennname – Öffnet ein Fenster, in dem Sie MAC-Adressen leicht zu merkende [Kennnamen](#) zuordnen können.

IP-Kennname – Öffnet ein Fenster, in dem Sie IP-Adressen leicht zu merkende [Kennnamen](#) zuordnen können.

Optionen – Öffnet das Optionsfenster, in dem Ihnen weitere Einstellmöglichkeiten zur Verfügung stehen.

Sprache – Erlaubt die Auswahl der Interface-Sprache.

Modemtreiber installieren – Installiert einen Treiber für die Paketerfassung über ein Modem. Dieser Menüpunkt nicht sichtbar falls der Treiber bereits installiert ist.

Token Ring-Treiber installieren – Installiert einen Treiber für die Paketerfassung über Token Ring-Adapter. Dieser Menüpunkt nicht sichtbar falls der Treiber bereits installiert ist.

Regeln

Aktive Regeln speichern als – Ermöglicht die Speicherung der aktuellen Regeln als Datei.

Regeln laden von – Erlaubt das Laden von vorher abgespeicherten Regelkonfigurationen aus einer Datei.

Alles Rücksetzen – Löscht alle vorhandenen Regeln, sofern vorhanden.

Hilfe

Inhalt – Startet die CommView-Hilfe.

Suche nach Hilfe über ... – Zeigt den Hilfeindex von CommView.

Online-Anleitung – Öffnet die CommView- in einem Webbrowser-Fenster.

Im Web nach Updates suchen – Öffnet den Update-Assistent. Bitte folgen Sie der Anleitung auf dem Bildschirm um das neueste Upgrade von CommView von der TamoSoft-Website herunterzuladen und zu installieren.

Aktivierung - Ermöglicht Ihnen, Ihre Softwarelizenz freizuschalten oder den gegenwärtigen Aktivierungsstatus einzusehen.

Info – Zeigt Informationen über das Programm.

Fast jedes Element des Interfaces hat ein kontextsensitives Menü, das Sie über die rechte Maustaste aufrufen können und viele Befehle stehen Ihnen über diese Menüs zur Verfügung.

Das erste Register dient zur Darstellung detaillierter Informationen über die Computer-Netzwerkverbindungen (nur IP-Protokolle). Weitere Informationen finden sie unter [Aktuelle IP-Verbindungen](#).

Das zweite Register dient zur Betrachtung der empfangenen Netzwerkpakete und der Darstellung detaillierter Informationen über ein ausgewähltes Paket. Weitere Informationen finden sie unter [Pakete](#).

Das dritte Register dient zum Abspeichern der empfangenen Pakete in eine Datei. Weitere Informationen finden sie unter [Protokollierung](#).

Das vierte Register dient zur Regelkonfiguration zum Empfangen/Ignorieren von Paketen auf der Basis verschiedener Kriterien, wie der IP-Adresse oder Portnummer. Weitere Informationen finden sie unter [Regeln](#).

Das fünfte Register ermöglicht es Alarme zu erzeugen, die Sie über bestimmte Ereignisse informieren, wie verdächtige Pakete, starke Bandbreitennutzung, unbekannte Adressen usw. Solche Alarme sind sehr nützlich, wenn Sie das Netzwerk auf bestimmte verdächtige Ereignisse überwachen, wie auffällige Bytemuster in den empfangenen Paketen, Portscans oder unerwartete Hardwareverbindungen. Weitere Informationen finden sie unter [Alarme](#).

Das sechste Register ermöglicht Ihnen mit dem [VoIP-Analysemodule](#) zu arbeiten. Beachten Sie bitte, dass dieses Modul nur verfügbar ist für VoIP-Lizenzinhaber oder für Anwender der Testversion mit gewähltem VoIP-Testmodus.

Einige der Einstellungen, wie Fonts, Farben und Puffergröße können über den Menüpunkt Einstellungen verändert werden. Weitere Informationen finden sie unter [Einstellungen](#).

Netzwerkschnittstelle zur Paketerfassung auswählen

Um eine Netzwerkverbindung zu überwachen muss zuerst der zugehörige Netzwerkadapter ausgewählt werden, dessen Netzwerkverkehr überwacht werden soll. Die Auswahl des richtigen Netzwerkadapters ist entscheidend um das gewünschte Aufzeichnungsergebnis zu erhalten. Wir haben versucht dies so benutzerfreundlich wie möglich zu machen. Alles was Sie vor dem Start der Paketerfassung machen müssen ist aus der Drop-Down-Liste der lokalen Netzwerkadapter den richtigen Netzwerkadapter auszuwählen. Danach klicken Sie auf den Button **[Paketerfassung starten]**.

Da sich die Netzwerktechnologie ständig weiterentwickelt nimmt die Zahl der verfügbaren Netzwerkadapter auf dem Markt ständig zu. WiFi-Adapter, xDSL, was auch immer Sie wollen. CommView unterstützt eine Vielzahl dieser Adapter, jedoch hat jeder Typ von Verbindung seine Eigenheiten, die Sie kennen müssen um das beste Aufzeichnungsergebnis zu erreichen.

Lassen Sie uns eine Liste der gängigsten Netzwerkadapter betrachten um aufzuzeigen wie CommView mit ihnen arbeitet und konfiguriert werden muss.

Während der Installation erkennt CommView alle in Ihrem System verfügbaren Netzwerkadapter. An einem bestimmten Punkt werden Sie gefragt ob Sie die Treiber für das Modem installieren möchten. Klicken Sie **[Ja]**, wenn Sie die Verbindungen über das Modem oder Ihr xDSL-Modem oder PPPoE/VPN-Verbindungen überwachen möchten. Wenn Sie auf **[Nein]** klicken können Sie die Treiber zu einem späteren Zeitpunkt unter **Einstellungen => Modemtreiber installieren** installieren. Während der Modemreiberinstallation werden alle Netzwerkverbindungen für einen Moment unterbrochen.

Wenn die Installation beendet ist, klicken Sie auf die Drop-Down-Liste in der Werkzeugleiste. Sie sehen dann den Loopback-Adapter, den lokalen Netzwerkadapter (vorausgesetzt es ist einer vorhanden) und den Einwahladapter falls Sie bei der Aufforderung den Einwahltreiber zu installieren **[Ja]** angeklickt haben.

Diese Einträge korrespondieren wie folgt zu der im System vorhandenen Hardware und den Netzwerkverbindungstypen.

Wenn Sie mittels eines einfachen **Ethernet-Adapters** mit dem Netzwerk verbunden sind, wählen Sie ihn einfach aus der Drop-Down-Liste und starten die Paketerfassung. CommView unterstützt praktisch jeden auf dem Markt verfügbaren 10-, 100- oder 1000Mbit-Ethernet-Adapter.

Wenn Sie sich via **Modem** in das Netzwerk einwählen, dann wählen Sie das Modem aus der Drop-Down-Liste aus. Nehmen Sie zur Kenntnis, das Sie nur ein- und ausgehenden aber keinen durchgehenden Paketverkehr sehen werden. Dies ist keine Einschränkung von CommView. Es liegt in der Natur jeder Punkt-zu-Punkt-Verbindung; nur zwei Hosts, der lokale und der entfernte Host beteiligen sich an der Verbindung. Wenn Sie ICS benutzen, können Sie alle Pakete von und zu den ICS-Clients empfangen.

Wenn Sie mit CommView drahtlose 802.11 a-, b-, g-, n- oder ac-Netzwerke überwachen wollen, wählen Sie den Wi-Fi-Adapter aus der Drop-Down-Liste aus. Der Standarttreiber für Wi-Fi-Adapter kann diese nicht in den sogenannten Gemischten-Modus versetzen. Das heißt CommView erfasst eingehende, ausgehende sowie Multicast- und Broadcast-Pakete. Die 802.11-Paket-Header werden nicht angezeigt. Wenn Sie ein Überwachungstool mit dem vermischten Modus für drahtlose Netzwerke suchen, sollten Sie den Einsatz von [CommView for WiFi](#) in Betracht ziehen, das den drahtlosen Paketverkehr zwischen anderen drahtlosen LAN-Teilnehmern und AP's erfassen kann. CommView for WiFi kann von der TamoSoft-Webseite [heruntergeladen](#) werden.

Wenn Sie sich via **xDSL-Modem** mit **USB-Schnittstelle** in das Netzwerk einwählen, kann es sein, dass Sie den Netzwerkverkehr mit CommView erfassen können. Offiziell unterstützt CommView keine Adapter mit USB-Schnittstellen. Am besten Sie probieren es einfach aus. In vielen Fällen wird die Netzwerkverbindung via PPPoE-Link erstellt. In diesen Fällen wählen Sie den Dial-In-Adapter aus der Drop-Down-Liste und starten die Paketerfassung.

Wenn Sie ein **xDSL-Modem** mit **Ethernet-Schnittstelle** haben, die eigentliche Verbindung jedoch via PPPoE-Link erstellt wird, müssen Sie das Modem aus der Drop-Down-Liste auswählen. Wenn Sie den Ethernetadapter auswählen kann es sein, dass Sie zwar den Datenverkehr auf dem LAN-Segment erfassen können, die Pakete jedoch in das PPPoE-Protokoll eingepackt und somit verschlüsselt sind.

Wenn Sie via sicheren **VPN-Link** mit dem Netzwerk verbunden sind, werden Sie auf dem Ethernetadapter nur verschlüsselte Pakete erfassen können. In diesem Fall müssen Sie den Datenverkehr auf dem Modem erfassen um die tatsächlich übertragenen Daten zu sehen.

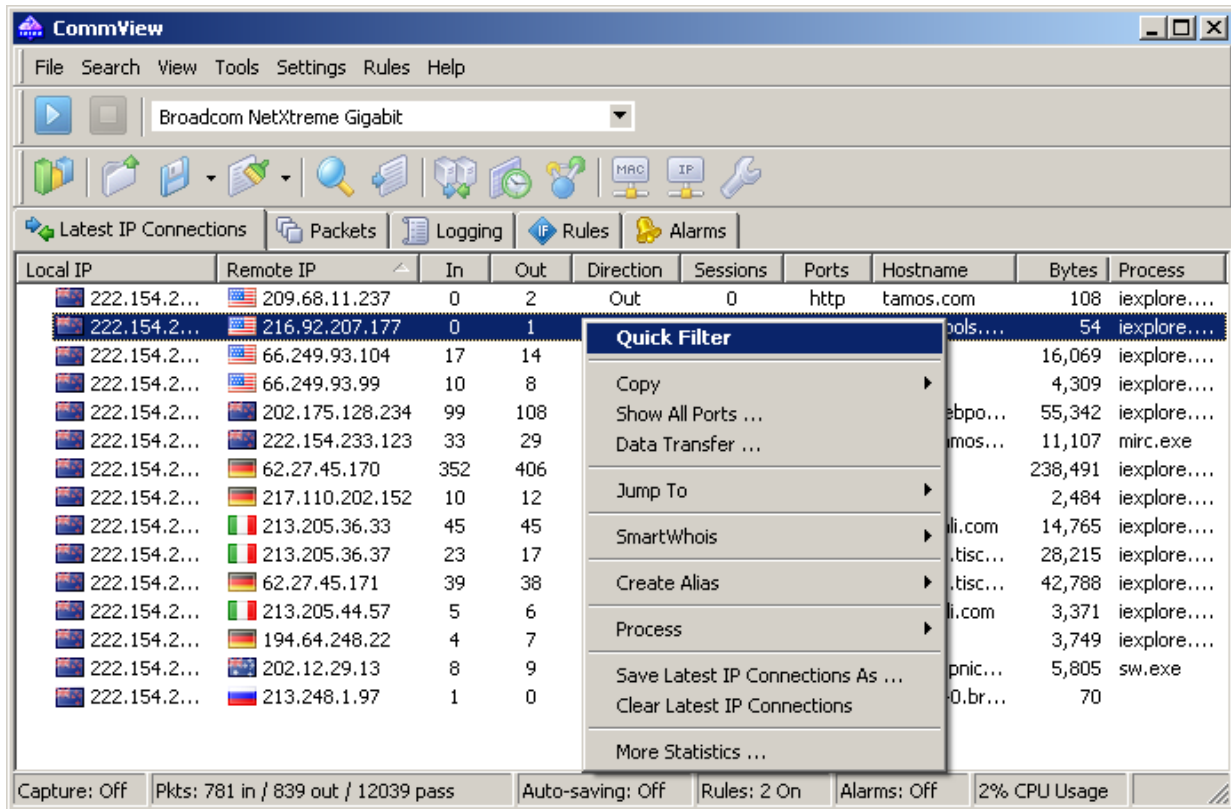
Wenn Sie in Ihrem Computer zwei oder mehr Netzwerkadapter haben die **Gebrückt** sind, so werden Sie beim Erfassen des Datenverkehrs auf der Brücke den Datenverkehr von und zu jedem Adapter in der Brücke, Broadcast- und Multicast-Pakete und die Pakete die zu einem anderen Adapter in der Brücke umgeleitet werden, sehen.

Die Paketerfassung auf dem **Loopback-Adapter** zeigt den Datenverkehr, welcher von Programmen auf Ihrem PC über TCP/IP lokal gesendet oder empfangen wird. Wenn keine der laufenden Programme auf Ihrem PC lokal Daten austauschen, werden Sie auf dem Loopback-Adapter keinen Verkehr sehen. Nehmen Sie zur Kenntnis, dass der Paketgenerator nicht mit dem Loopback-Adapter funktioniert. Weitere Informationen finden sie im Kapitel [Loopback-Verkehr erfassen](#).

Neben physischen und virtuellen Netzwerkadaptern ermöglicht die neueste CommView-Version die Auswahl eines virtuellen Adapters zur Erfassung des **entschlüsselten SSL-Verkehrs**. Diese virtuellen SSL-Adapter werden im Kapitel [Entschlüsselten SSL-Datenverkehr erfassen](#) beschrieben.

Aktuelle IP Verbindungen

Dieses Register wird zur Anzeige detaillierter Informationen Ihrer Computernetzwerkverbindungen (nur IP- und IPv6-Protokolle) benutzt. Zum Start der Paketüberwachung wählen Sie im Menü **Datei => Erfassung starten** oder klicken Sie auf den zugehörigen Button in der Werkzeugleiste.



Die Bedeutung der einzelnen Register-spalten ist im Folgenden erklärt:

Lokale IP – zeigt die lokale IP-Adresse. Bei ankommenden Paketen ist es die IP-Zieladresse, bei aus- und durchgehenden Paketen ist es die IP-Quellenadresse.

Remote IP – zeigt die entfernte IP-Adresse. Bei ankommenden Paketen ist es die IP-Quellenadresse, bei aus- und durchgehenden Paketen ist es die IP-Zieladresse.

Das Programm bestimmt automatisch den Standort jeder IP-Adresse, und je nach Ihren Landeseinstellungen, kann der Landesname oder die Landesflagge der IP-Adresse angezeigt werden. Weitere Informationen finden sie unter [Einstellungen](#).

Eingehend – Zeigt die Anzahl der eingegangenen Pakete.

Ausgehend – Zeigt die Anzahl der ausgehenden Pakete.

Richtung – Sitzungsrichtung. Die Sitzungsrichtung wird bestimmt aufgrund der Richtung des ersten von der entfernten IP-Adresse empfangenen oder zu dieser geschickten Paketes.

Sitzungen – Zeigt die Anzahl der vorhandenen TCP/IP-Sitzungen. Wenn keine TCP-Verbindungen vorhanden sind ist dieser Wert Null (Verbindungen kamen nicht zustande oder das Protokoll ist UDP/IP bzw. ICMP/IP).

Ports – Zeigt die Ports des Quellcomputers (Sender), die für die TCP/IP-Verbindung genutzt werden bzw. für den Versuch des Verbindungsaufbaus. Diese Liste kann durchaus leer sein, wenn das verwendete Protokoll nicht TCP/IP

ist. Ports können entweder als Zahlenwerte dargestellt werden oder als korrespondierender Servicename. Weitere Informationen finden sie unter [Einstellungen](#).

Hostname – Zeigt den Hostnamen des Sendecomputers. Wenn dieser nicht aufgelöst werden kann, wird nichts angezeigt.

Bytes – Zeigt die während der Sitzung übertragene Bytemenge an.

Letztes Paket – Zeigt die Uhrzeit des während der Session zuletzt gesendeten/empfangenen Paketes an.

Prozess – zeigt den Prozess auf dem lokalen PC an, welcher in dieser Sitzung Pakete empfängt oder sendet. Die Zuordnung eines Prozesses zu Paketen funktioniert nur lokal für ein- und ausgehende Pakete, da CommView nicht auf die Netzwerktätigkeit von Prozessen auf anderen PC's schliessen kann. Im Falle wenn mehrere Prozesse mit demselben entfernten PC Daten austauschen, zeigt CommView im Register **Aktuelle IP-Verbindungen** den letzten Prozess, der Daten mit einem bestimmten entfernten PC ausgetauscht hat. Die Zuordnung eines Prozesses (mit dem gesamten Pfad) zu einem bestimmten Paket kann in der Baumansicht des decodierten Paktes im Register **Pakete** eingesehen werden. Das der gesamte Pfad angezeigt wird, kann unter **Einstellungen => Optionen => Allgemein => Prozesspfad in voller Länge anzeigen** aktiviert werden. Wenn Sie durch Remote Agents im ferngesteuerten Überwachungsmodus arbeiten, zeigt diese Spalte die IP-Adresse oder den Hostnamen des paketempfangenden Remote Agents an; Prozessbezeichnungen sind nicht verfügbar. Bitte beachten Sie, dass diese Spalte auf einigen Betriebssystemen nur Prozessbezeichnungen auflistet, wenn ein Computer-Reset nach der CommView-Installation durchgeführt wird.

Einzelne Spalten können durch Rechtsklicken auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Letzte IP-Verbindungen-Spaltenmenü**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden.

Menübefehle

Ein Rechtsklick auf das Register Aktuelle IP-Verbindungen öffnet ein Kontextmenü mit den folgenden Befehlen:

Schnellfiltern – Findet die zwischen den ausgewählten IP-Adressen versendeten Pakete und zeigt die Pakete in einem neuen Fenster an. Dies geschieht auch, wenn Sie einen Doppelklick auf das Fenster ausführen.

Kopieren – Kopiert die lokale und die verbundene IP-Adresse bzw. den Hostnamen in die Zwischenablage.

Alle Ports anzeigen – Zeigt eine Liste aller Ports, die für die Kommunikation zwischen dem ausgewählten IP-Adressenpaar verwendet wurden. Dies ist nützlich, wenn viele Ports verwendet wurden und diese nicht in die entsprechende Spalte hineinpassen.

Datentransfer – Zeigt die Information über das Datentransfervolumen zwischen dem ausgewählten IP-Adressenpaar bzw. über die Uhrzeit des letzten Paketes.

Gehe zu – Hiermit springen Sie schnell zum ersten/letzten Paket der ausgewählten Quell-/Ziel-IP-Adresse. Das Programm zeigt dabei den Paketbereich und setzt den Cursor auf das Paket, welches dem Kriterium entspricht.

SmartWhois – sendet die ausgewählte Ausgangs-/Ziel-IP-Adresse zu SmartWhois, sofern dies auf Ihrem System installiert ist. SmartWhois ist eine selbstständige Anwendung, die von Tamosoft entwickelt wurde. SmartWhois ist in der Lage Informationen über jede IP-Adresse bzw. jeden Hostnamen auf der Welt zu erlangen. Die Anwendung zeigt dabei automatisch die zu einer IP-Adresse gehörenden Informationen, wie die Domäne, den Netzwerknamen, das Land, den Bundesstaat bzw. den Bezirk und die Stadt. Dieses Programm kann von der Tamosoft-Webseite [heruntergeladen](#) werden.

Kenntname anlegen – Öffnet ein Fenster, in welchem Sie leicht zu merkende [Kennnamen](#) für die ausgewählten IP-Adressen bestimmen können.

Prozess – ermöglicht Ihnen zusätzliche Informationen, über Leistungsaktionen beim Ablauf des Sendens und Empfangens der ausgewählten Sitzung, zu erhalten. Sie können einen Arbeitsablauf **Abbrechen**, den Dialog **Dateieigenschaften** einsehen oder lassen das Programm den **Gesamtpfad anzeigen** zur Verarbeitung von Exec-Dateien.

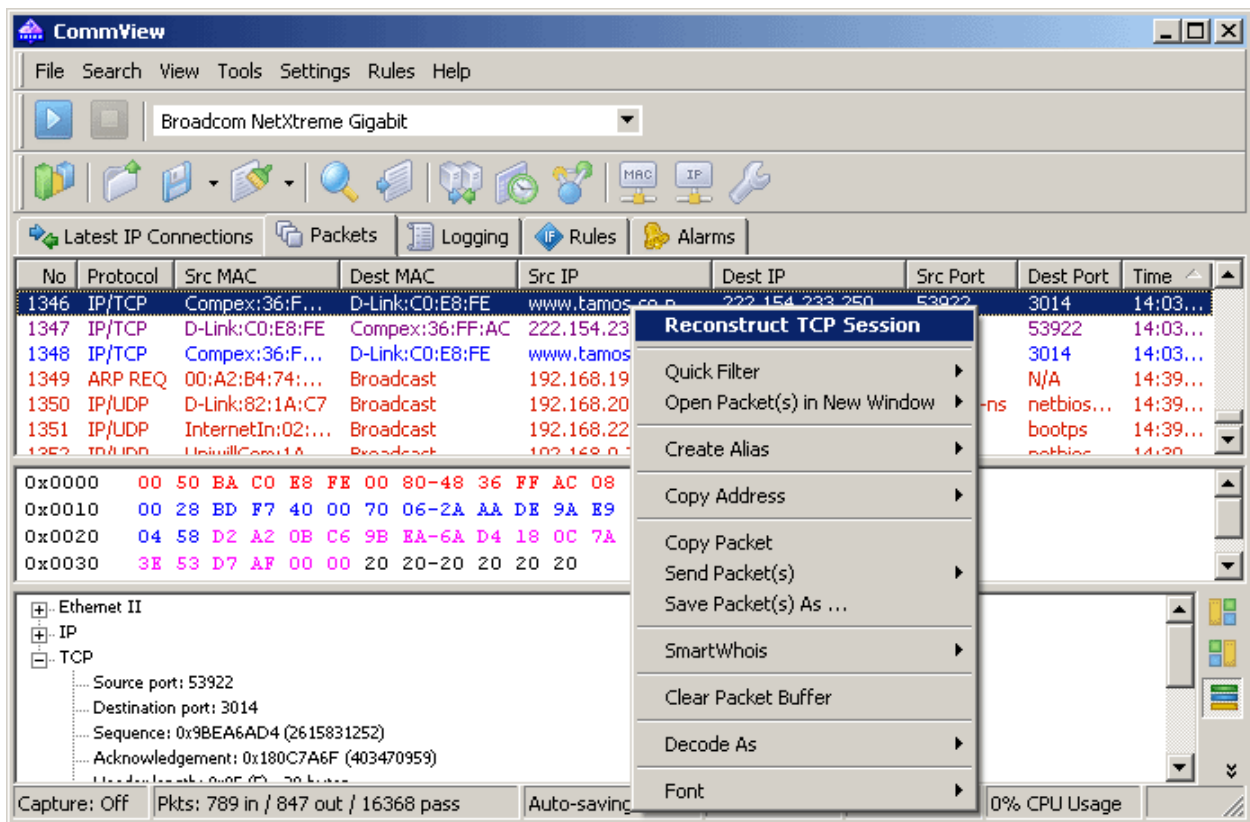
Aktuelle IP-Verbindungen speichern unter – Erlaubt das Speichern der aktuellen IP-Verbindungen als HTML- oder komma-getrennter CSV-Bericht.

Letzte IP Verbindungen löschen – Löscht den Inhalt des Registers.

Weitere Statistiken – Zeigt ein Fenster mit den [Datentransfer- und Protokollverteilungsstatistiken](#).

Pakete

Dieses Register dient zur Auflistung aller empfangenen Netzwerkpakete und zeigt detaillierte Informationen über das ausgewählte Paket.



Der **obere Bereich** zeigt eine Liste der empfangenen Pakete. Verwenden Sie diese Liste um ein Paket auszuwählen, dass Sie angezeigt und analysiert haben möchten. Wenn Sie ein Paket durch anklicken auswählen, zeigen die anderen Bereiche Informationen über dieses Paket.

Die Bedeutung der einzelnen Register-spalten ist im Folgenden erklärt:

Nr. – Eine eindeutige Paketnummer.

Protokoll – Zeigt das Paketprotokoll.

Src MAC, Dest MAC – zeigt die Quell- und Ziel-MAC-Adressen.

Src IP, Dest IP – zeigt die Quell- und Ziel-IP-Adresse (wo zutreffend).

Src Port, Dest Port – Zeigt die Quell- und Ziel-Ports (wo zutreffend). Ports können entweder als Zahlenwerte dargestellt werden oder als korrespondierender Servicenamen. Weitere Informationen finden sie unter [Einstellungen](#).

Zeit / Delta – Zeigt die absolute oder Deltzeit des Pakets. Die Deltzeit ist dabei der Unterschied zwischen den absoluten Zeitangaben der letzten zwei Pakete. Der Wechsel zwischen beiden Zeitarten geschieht durch **Ansicht => Paketspalten => Zeit anzeigen als**.

Größe – Zeigt die Paketgröße in Bytes.

Mehr Details – Zeigt die Zusammenfassung für jedes Paket.

Einzelne Spalten können durch Rechtsklicken auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Pakete-Spaltenmenü**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden.

Die kontinuierliche Paketanzeige kann mit **Datei => Paketausgabe unterbrechen** unterbrochen werden. In diesem Modus werden Pakete zwar empfangen, aber nicht im Register **Paket** analysiert. Dies ist nützlich, wenn Sie eher an den allgemeinen Statistiken als an einzelnen Paketen interessiert sind. Um die Echtzeitanzeige der Pakete wieder zu aktivieren klicken Sie auf **Datei => Erfassung starten**.

Der **mittlere Ausschnitt** des Registers zeigt den Grobinhalt des Paketes, sowohl in Hexadezimaldarstellung als auch im Klartext. Im Klartext werden nichtdruckbare Zeichen durch Punkte ersetzt. Wenn im **oberen Ausschnitt** Pakete ausgewählt wurden, zeigt der **mittlere Ausschnitt** die Gesamtanzahl der ausgewählten Pakete an, ferner deren Gesamtgröße und den zeitlichen Abstand zwischen dem ersten und dem letzten Paket.

Der **untere Ausschnitt** des Registers zeigt die entschlüsselten Paketdaten für das ausgewählte Paket. Dies enthält wichtige Informationen für Netzwerkexperten. Mit einem Rechtsklick auf den Bereich rufen Sie ein kontextsensitives Menü auf, das es Ihnen ermöglicht die Knoten auf- oder zuzuklappen bzw. den ausgewählten Knoten oder alle zu kopieren.

Das Register **Pakete** beinhaltet ferner eine kleine Werkzeugleiste, wie unten gezeigt:



Sie können die Position des Dekoderfensters verändern, indem Sie auf einen der drei Button dieser Werkzeugleiste klicken (das Dekoderfenster kann unten, links- oder rechtsbündig ausgerichtet werden). Der vierte Button führt ein automatisches Scrollen in der Paketliste zum zuletzt empfangenen Paket durch. Der fünfte Button läßt das ausgewählte Paket weiterhin sichtbar bleiben (z. B. wenn neue Pakete ankommen). Der sechste Button ermöglicht Ihnen den Inhalt des aktuellen Paket-Buffers in einem neuen Fenster zu öffnen. Diese Funktionalität ist äußerst brauchbar bei schwerer Netzwerkbelastung, gerade wenn die Paketliste rasch scrollt und es schwierig ist, Pakete zu untersuchen, bevor Sie den sichtbaren Bereich wieder verlassen. Klicken auf diesen Button erzeugt einen Schnappschuss des Puffers, sodass Sie den Puffer in einem separaten Fenster untersuchen können. Sie können so viele Schnappschüsse erzeugen wie Sie möchten.

Menübefehle

Ein Rechtsklick auf das Register **Paket** öffnet ein Kontextmenü mit den folgenden Befehlen:

Rekonstruiere TCP Sitzung – Ermöglicht Ihnen die [Rekonstruktion einer TCP-Sitzung](#) ausgehend vom gewählten Paket. Dabei öffnet sich ein Fenster, das die ganze Kommunikation zwischen zwei Hosts darstellt. Dies geschieht auch, wenn Sie einen Doppelklick auf das Fenster ausführen.

Schnellfilter – Findet die zwischen zwei ausgewählten MAC- bzw. IP-Adressen oder Ports gesendeten Pakete und zeigt diese in einem neuen Fenster an.

Paket(e) in neuem Fenster öffnen – Ermöglicht Ihnen ein oder mehrere Pakete, für eine komfortable Untersuchung, in einem neuen Fenster zu öffnen.

Kenntname anlegen – Öffnet ein Fenster in dem Sie leicht zu merkende [Kennnamen](#) den MAC- bzw. IP-Adressen zuordnen können.

Adresse kopieren – Kopiert die Quell-MAC-Adresse, Ziel-MAC-Adresse, Quell-IP-Adresse, oder die Ziel-IP-Adresse in die Zwischenablage.

Paket kopieren – Kopiert die Rohdaten des ausgewählten Paketes in die Zwischenablage.

Paket(e) senden – Zeigt den [Packetgenerator](#), welcher das Senden des ausgewählten Paketes oder einer Gruppe von Paketen erlaubt.

Paket(e) speichern unter – Speichert die Inhalte der ausgewählten Pakete in eine Datei.

SmartWhois – sendet die ausgewählte Quell-/Ziel-IP-Adresse zu SmartWhois, sofern dies auf Ihrem System installiert ist. SmartWhois ist eine selbstständige Anwendung, die von Tamosoft entwickelt wurde. SmartWhois ist in der Lage Informationen über jede IP-Adresse bzw. jeden Hostnamen auf der Welt zu erlangen. Die Anwendung zeigt dabei automatisch die zu einer IP-Adresse gehörenden Informationen, wie die Domäne, den Netzwerknamen, das Land, den Bundesstaat bzw. den Bezirk und die Stadt. Dieses Programm kann von der Tamosoft-Webseite [heruntergeladen](#) werden.

Packetpuffer leeren – Löscht die Inhalte des Programmspeichers. Der Inhalt des Registers Pakete wird auch gelöscht, so dass Sie nicht mehr die bisher erhaltenen Pakete ansehen können.

Decodieren als – Für TCP- und UDP-Pakete. Dies ermöglicht es, unterstützte Protokolle, welche nicht standardisierte Ports verwenden zu decodieren. Wenn z. B. Ihr SOCKS-Server auf Port 333 statt 1080 läuft, so können Sie ein Paket der SOCKS-Session wählen und dann über dieses Menü veranlassen, dass CommView alle Pakete auf Port 333 als SOCKS-Pakete erkennt. Solche Protokollumbenennungen sind jedoch nicht permanent und nur aktiv bis das Programm beendet wird. Beachten Sie bitte, dass Sie Standardprotokollpaare nicht umdefinieren können. So kann CommView Pakete auf Port 80 nicht als TELNET Pakete erkennen.

Schrift – erlaubt Ihnen die Schriftgröße für Paketanzeige zu verkleinern oder zu vergrößern, dies hat keine Auswirkung auf alle anderen Elemente der Bedienoberfläche.

Ausgewählte Pakete können über Drag&Drop auf den Desktop gezogen werden.

Protokollierung

Dieses Register dient zum Speichern empfangener Pakete in eine Datei auf die Festplatte. CommView speichert dabei die Pakete in einem eigenen Format mit der Endung NCF. Das ältere CCF-Format wird aus Abwärtskompatibilitätsgründen auch unterstützt. Die gesammelten Pakete können jedoch nicht länger abgespeichert werden. Sie können diese Dateien jederzeit mit dem Logbetrachter anschauen bzw. einfach auf die NCF- oder CCF-Datei Doppelklicken um sie vom [Logbetrachter](#) öffnen zu lassen.

NCF ist ein offenes Format. Mehr dazu unter [CommView-Logdateiformat](#).

Speichern und verwalten

Mit diesem Bereich können Sie die empfangenen Pakete manuell abspeichern und abgespeicherte Dateien verbinden bzw. splitten.

Alle im Speicher befindlichen Pakete oder ein ausgewählter Bereich können abgespeichert werden. Die Grenzen innerhalb der Paketnummern werden durch die Felder **Von/Bis** gesetzt. Klicken Sie auf **Speichern unter...** um einen Dateinamen auszuwählen.

Um manuell mehrere NCF-Dateien in eine große Datei zu verbinden klicken Sie auf **[Logs zusammenfügen]**. Um zu groß geratene NCF-Dateien zu splitten klicken Sie auf **[Logs splitten]**. Das Programm wird Sie dann so führen, dass Sie die Dateien in der gewünschten Größe erhalten.

Autospeicherung

Wählen Sie diese Checkbox, damit das Programm die empfangenen Pakete automatisch bei der Ankunft abspeichert. Mittels des Feldes **Maximale Verzeichnisgröße** legen Sie die Größe der im **Logverzeichnis** gespeicherten Informationen fest. Wenn diese Größe überschritten wird werden zuerst die ältesten Daten überschrieben. Mit dem Feld **Durchschnittliche Logdateigröße** geben Sie die ungefähre Größe einer Logdatei vor. Wenn die Logdatei diese vorgegebene Größe erreicht, wird automatisch eine neue Logdatei erzeugt. Um das standardmässige **Logverzeichnis** zu ändern, wählen Sie mittels **Log Speichern** unter: einen neuen Pfad.

WICHTIG. Wenn Sie ein wichtiges empfangenes Datenpaket lange aufbewahren wollen, sollten Sie es nicht im Standardlogpfad ablegen, denn es könnte durch neuere Daten überschrieben werden. Verschieben Sie die Datei zur Aufbewahrung in ein anderes Verzeichnis.

Bedenken Sie, dass das Programm nicht automatisch jedes Paket nach dessen Empfang abspeichert. Dies bedeutet, wenn Sie die Logdateien in Echtzeit ansehen, die letzten Pakete fehlen können. Um den Puffer in die Logdateien zu schreiben, klicken Sie entweder **[Erfassung stoppen]** oder deaktivieren Sie die Checkbox **Autospeicherung**.

WWW-Zugriff-Protokollierung

Aktivieren Sie diese Checkbox um das Logging von HTTP-Sitzungen zu starten. Mittels des Feldes **Maximale Dateigröße** begrenzen Sie die Größe der Logdatei. Wenn diese Grenze überschritten wird, werden zuerst die ältesten Logdateien überschrieben. Um den Standardlogdateinamen bzw. -pfad zu ändern, klicken Sie auf die Funktion **Logdateien speichern unter** und wählen Sie dann einen neuen Namen. Logdateien können im **HTML-** oder **TXT-Format** erzeugt werden. Mittels eines Klicks auf **Konfiguration** können Sie die Standard-Logging-Optionen ändern. Sie können die Portnummer für den HTTP-Zugang ändern (der Standardwert von 80 funktioniert vielleicht nicht bei Ihnen, da Sie hinter einem Proxy sind) und bestimmte Datentypen ausschliessen (normalerweise sollte etwas anderes als HTML-Seiten nicht gelogged werden, aber es ist eine gute Idee die URL's von Bildern aus der Logdatei auszuschliessen).

Logbetrachter

Der Logbetrachter ist ein Werkzeug zum Betrachten und Erforschen von Dateien, die von CommView oder anderen Paket-Analysern gesammelt wurden. Es hat die Funktionalität des Registers **Pakete** im Hauptfenster, im Unterschied zum Register **Pakete**, zeigt der Logbetrachter geladene Pakete von auf der Festplatte befindlichen Dateien eher an als die in Echtzeitanzeige erfassten Pakete.

Um den Logbetrachter zu öffnen klicken Sie im Hauptfenster auf **Datei => Logbetrachter** oder doppelklicken Sie auf eine CommView Erfassungsdatei, die Sie bereits abgespeichert haben. Sie können beliebig viele Logbetrachterfenster öffnen, und jedes davon kann zur Analyse eines oder mehrerer Dateien heranziehen.

Der Logbetrachter kann auch zur Analyse von Dateien auch anderer Paket-Analyser und Personal Firewalls benutzt werden. In der aktuellen Version können Dateien aus Network Instruments Observer®-Network General Sniffer® für DOS/Windows-, Microsoft® NetMon-, WildPackets EtherPeek™- und AiroPeek™-, Wireshark/Tcpdump- und Wireshark/pcapng-Formate importiert werden. Diese Formate werden auch oft in Drittherstellerprodukten verwendet. Der Protokollbetrachter besitzt die Fähigkeit Paketdaten durch Dateierzeugung in Network Instruments Observer®, Network General Sniffer® für DOS/Windows-, Microsoft® NetMon-, WildPackets EtherPeek™- und AiroPeek™-, Wireshark/Tcpdump und Wireshark/pcapng-Formate zu erzeugen, aber auch im eigenen CommView-Format.

Die Verwendung des Logbetrachters ist analog zum Register **Pakete** im Hauptfenster. Mehr dazu im Kapitel [Pakete](#).

Logbetrachtermenü

Datei

Lade CommView Logs – Öffnet eine oder mehrere CommView-Erfassungsdateien.

Logs importieren – Importiert Dateien aus anderen Paket-Analysern.

Logs exportieren – Exportiert die angezeigten Pakete in andere Formate.

Fenster leeren – Löscht den Inhalt der Paketliste.

Statistiken generieren – Lässt CommView-Statistiken über die im Logbetrachter befindlichen Pakete erzeugen. Ferner können auch die im **Statistikfenster** angezeigten Daten gelöscht werden. Diese Funktion zeigt keine Zeitreihenanalyse. Sie zeigt nur Summen, Protokollkarten und LAN-Host-Tabellen.

An VoIP-Analyser senden – Sendet alle Pakete vom aktuellen Protokollanzeigefenster zu einem neuen [VoIP-Protokollanzeigefenster](#) für eine VoIP-spezifische Analyse.

Fenster schliessen – Schließt das Fenster.

Suchen

Finde Paket... – Mit diesem Dialog [finden Sie Pakete](#), die einen bestimmten Text enthalten.

Gehe zu Paket Nummer... – Mit diesem Dialog springen Sie zu einer definierten Paketnummer.

Regeln

Anwenden – Wendet die aktuellen Regeln auf die im Logbetrachter gezeigten Pakete an. Als Folge werden die nicht mehr passenden Pakete gelöscht. Dies ändert jedoch nicht die gespeicherte Datei.

von Datei ... – Analog zu Anwenden, allerdings verwenden Sie hier ein bereits gespeichertes Regelset (RLS-Datei) anstatt der aktuellen Regeln.

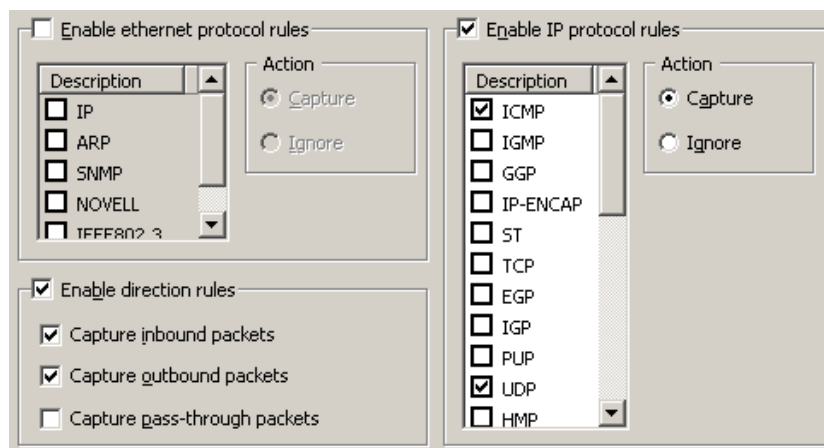
Regeln

Dieses Register erlaubt die Definition von Regeln zur Erfassung der Datenpakete. Sind hier Regeln gesetzt worden, filtert das Programm die Pakete danach und zeigt dann nur die regelkonformen Pakete an. Nehmen Sie zur Kenntnis, dass CommView keine Firewall ist und daher durch das Betriebssystem auch Pakete verarbeitet werden, die nicht den Regeln entsprechen. Die Wirkung der Regeln beschränkt die Anzeige der Pakete in CommView. Wenn eine Regel definiert wird, wird die zugehörige Registerbezeichnung in Fettschrift angezeigt.

Sie können mittels der **Regeln** im Programmmenü Ihre Regeleinstellungen in einer Datei speichern und später wieder laden.

Da LAN-Verkehr oft eine große Zahl von Datenpaketen erzeugt, empfehlen wir die Verwendung von Regeln, um nicht benötigte Pakete auszuschließen. Dadurch werden die benötigten Systemressourcen gesenkt. Wenn Sie eine Regel aktivieren bzw. deaktivieren wollen, wählen Sie den entsprechenden Teil im linken Teil des Fensters (z. B. **IP-Adressen** oder **Ports**) und deaktivieren Sie die Checkbox, die zur Regel gehört (z. B. **Aktiviere IP Adressenregeln** bzw. **Aktiviere Portregeln**). Es gibt acht Regeltypen:

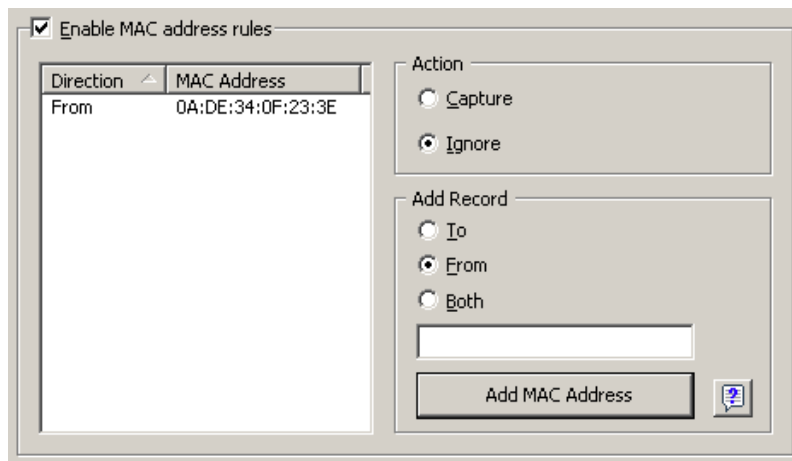
Protokolle & Richtung



Dieses Beispiel zeigt, wie man nur ein- und ausgehende ICMP- und UDP-Pakete empfängt. Alle anderen Pakete der IP-Familie werden ignoriert. Auch alle durchgehenden Pakete werden ignoriert.

MAC-Adressen

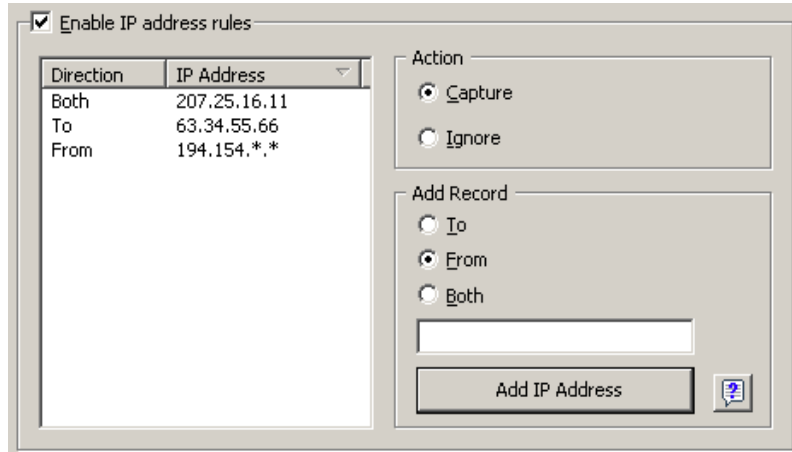
Der Dialog ermöglicht das Empfangen/Ignorieren von Paketen basierend auf MAC-Adressen (Hardware). Fügen Sie eine MAC-Adresse in das Eingabefeld **Datensatz hinzufügen** ein, wählen die Richtung (**Nach**, **Von** oder **Beides**) und klicken auf **[MAC-Adresse hinzufügen]**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein Paket ankommt. Das Paket kann ignoriert oder erfasst werden. Sie können auch auf den Button MAC-Kennname klicken, um eine Liste der Kennnamen zu erhalten. Doppelklicken Sie auf einen Kennnamen, den Sie hinzufügen wollen. Die MAC-Adresse wird der Eingabeliste hinzugefügt.



Dieses Beispiel zeigt, wie man das Programm Pakete ignorieren läßt, die von 0A:DE:34:0F:23:03E kommen. Alle Pakete von anderen MAC-Adressen werden empfangen.

IP-Adressen

Mit diesem Dialog können Pakete basierend auf IP-Adressen ignoriert oder empfangen werden. Geben Sie einfach eine IP- oder IPv6-Adresse im Bereich **Datensatz hinzufügen** ein, wählen die Richtung (**Nach, Von** oder **Beides**) und klicken dann auf **[IP-Adresse hinzufügen]**. Sie können dabei für IP-Blöcke sogenannte Wildcards (Platzhalter) verwenden. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein Paket ankommt. Das Paket kann ignoriert oder erfasst werden. Über den Button IP-Kennname können sie eine Liste von Kennnamen erhalten. Doppelklicken Sie auf den Kennnamen, den Sie hinzufügen wollen und die entsprechende IP-Adresse wird der Eingabeliste hinzugefügt.

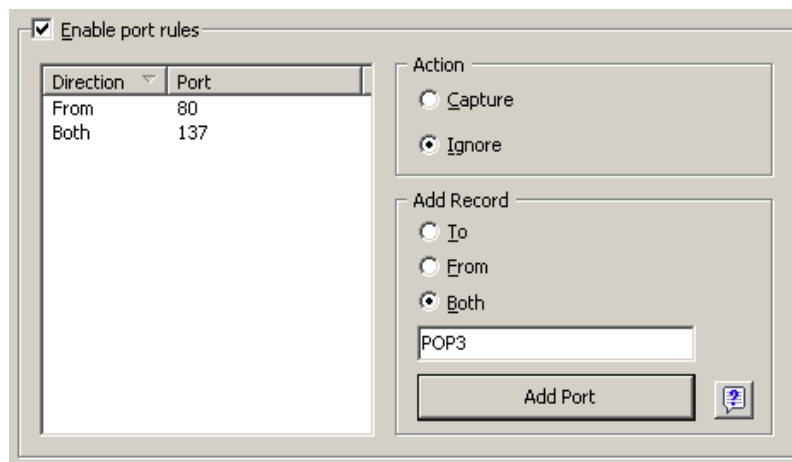


In diesem Beispiel zeigen wir wie Sie die Pakete definieren können, die an 63.34.55.66 gehen bzw. von 207.25.16.11 und von allen Adressen im Bereich 194.154.0.0 und 194.154.255.255 kommen. Alle Pakete, die von anderen Adressen kommen, werden ignoriert. Da im IP-Protokoll IP-Adressen verwendet werden, würde eine solche Konfiguration alle Nicht-IP-Pakete automatisch ignorieren. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

Ports

Der Dialog ermöglicht das Ignorieren oder Empfangen von Paketen über Ports. Fügen Sie einfach eine Portnummer im Bereich **Datensatz hinzufügen** ein, wählen dann die Richtung (**Nach, Von** oder **Beides**) und klicken **[Port hinzufügen]** an. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein Paket ankommt.

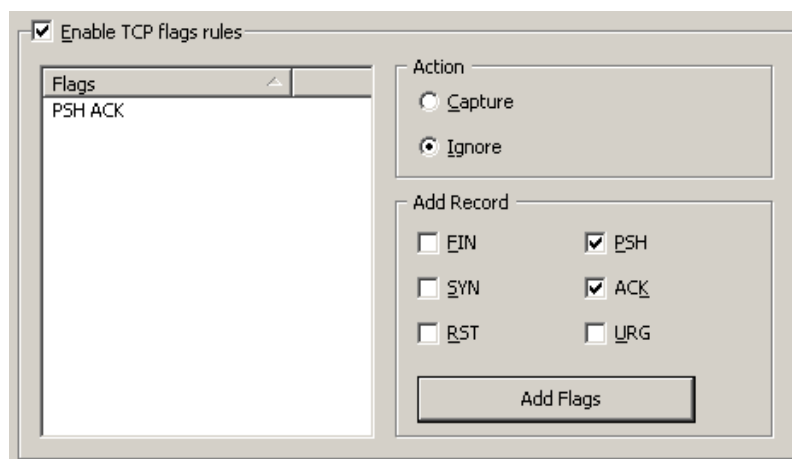
Das Paket kann ignoriert oder erfasst werden. Betätigen Sie den Button [Port Referenz] um eine Liste aller bekannten Ports zu erhalten. Doppelklicken Sie auf den Port, den Sie hinzufügen wollen und seine Portnummer wird der Eingabeliste hinzugefügt. Ports können als Text eingegeben werden, z. B. http oder pop3. Das Programm wird dann den Portnamen in einen numerischen Wert umwandeln.



In diesem Beispiel sehen Sie, wie Sie das Programm dazu bringen Pakete von Port 80 kommend bzw. zu Port 137 gehend zu ignorieren. Diese Regel verhindert, dass CommView eingehenden HTTP-Verkehr bzw. ein- und ausgehenden NETBIOS NAME Service-Verkehr anzeigt. Alle von oder zu anderen Ports gehende Pakete werden aber angezeigt.

TCP-Flags

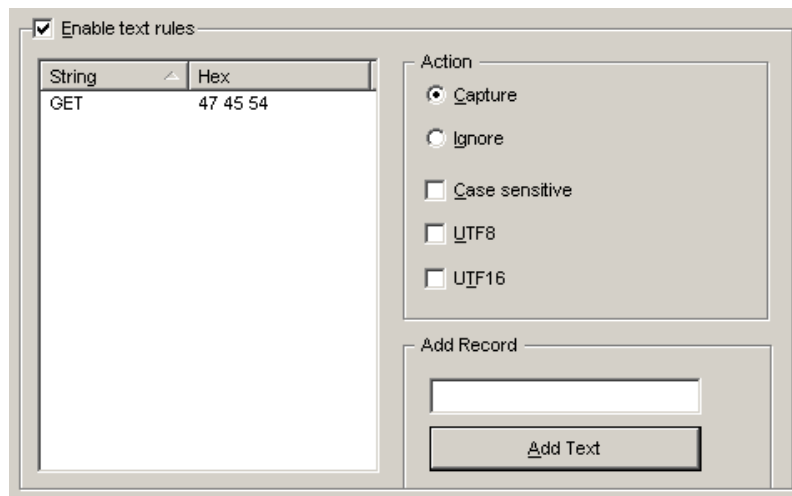
Der Dialog ermöglicht das Ignorieren oder Empfangen von Paketen basierend auf TCP-Flags. Wählen Sie eine oder mehrere Checkboxes im Bereich **Datensatz hinzufügen** und klicken Sie dann auf **[Flags hinzufügen]**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket mit vorgegebenen TCP-Flags ankommt: Das Paket kann ignoriert oder erfasst werden.



In diesem Beispiel sehen Sie, wie das Programm TCP-Pakete mit dem PSH ACK-Flag ignoriert. Alle Pakete mit anderen TCP-Flags werden empfangen.

Text

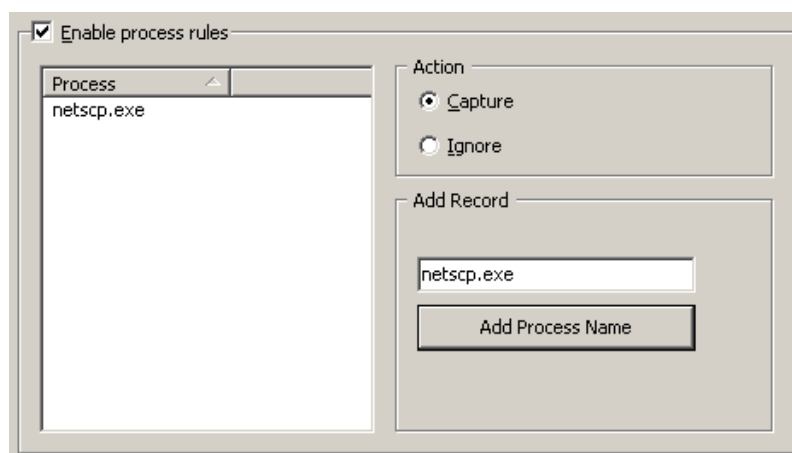
Der Dialog ermöglicht den Empfang von Paketen, die einen bestimmten Text enthalten. Fügen Sie den Text-String im Bereich **Datensatz hinzufügen** ein und klicken Sie dann auf **[Text hinzufügen]**. Wählen Sie die durchzuführende Aktion, wenn ein Paket ankommt: Das Paket kann ignoriert oder erfasst werden.



In diesem Beispiel sehen Sie, wie man das Programm dazu bringt, nur Pakete zu empfangen, die "GET" enthalten. Wählen Sie die Checkbox **Gross-/Kleinschreibung unterscheiden**, wenn die Groß- und Kleinschreibung beachtet werden soll. Wählen Sie die Checkbox **UTF8** oder **UTF16**, wenn Sie möchten, dass die Regel mit der jeweiligen Kodierung Ihres Textes übereinstimmt. Alle Pakete, die nicht den genannten Text enthalten, werden nun ignoriert. Wenn Sie eine Regel erstellen möchten, die auf hexadezimalen Bytesequenzen basiert, wenn der Text nicht druckfähig ist (z.B. 0x010203), sehen Sie im Kapitel [Erweiterte Regeln](#) nach.

Prozess

Ermöglicht Ihnen die Erfassung der Pakete über den Prozessnamen. Geben Sie im Bereich **Datensatz hinzufügen** den Prozessnamen ein und klicken Sie auf **[Prozessname hinzufügen]**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket verarbeitet wird: Das Paket kann ignoriert oder erfasst werden. Es können ganze Prozessnamen oder Teile von Prozessnamen, d.h. *netscp* oder *net*, eingegeben werden. Alle Prozesse die den Teil eines Prozessnamens enthalten erfüllen die Regel. Gross- bzw. Kleinschreibung wird bei den Prozessnamen nicht unterschieden.



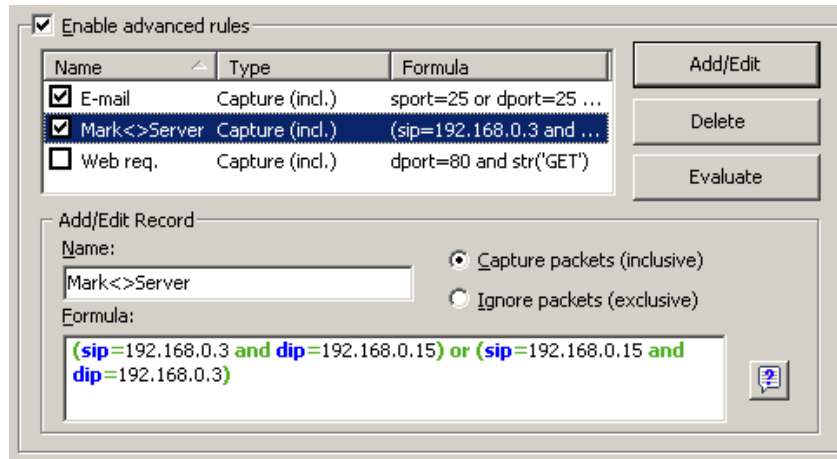
Das obige Beispiel zeigt eine Regel, die nur die Erfassung von Paketen erlaubt, welche von einem Prozess namens netscp.exe gesandt oder empfangen wurden. Alle Pakete die von anderen Prozessen gesandt werden, werden ignoriert.

Für Fortgeschrittene

Erweiterte Regeln sind die mächtigsten und flexibelsten Regeln. Sie ermöglichen Ihnen komplexe Filter basierend auf Bool'scher Logik zu implementieren. Eine detaillierte Hilfe zu der erweiterten Regeln finden Sie im Kapitel [Erweiterte Regeln](#).

Erweiterte Regeln

Erweiterte Regeln sind die mächtigsten und flexibelsten Regeln. Sie ermöglichen Ihnen komplexe Filter basierend auf Bool'scher Logik zu implementieren. Um diese zu nutzen brauchen Sie grundlegende Kenntnisse in Mathematik und Logik. Die Regelsyntax ist aber leichtverständlich.



Übersicht

Um eine neue Regel hinzuzufügen müssen Sie einen beliebigen Namen im Eingabefeld **Name** eingeben, wählen Sie dann die Aktion **Pakete erfassen/ignorieren**. Geben Sie eine Formel nach der weiter unten erklärten Syntax ein und klicken anschließend auf **[Hinzufügen/Editieren]**. Die neue Regel wird hinzugefügt und ist augenblicklich aktiv. Es können beliebig viele Regeln hinzugefügt werden. Es sind jedoch nur die Regeln aktiv, die eine aktivierte Checkbox neben ihrem Namen haben. Die Regeln können über die entsprechenden Checkboxes aktiviert/deaktiviert werden. Zum endgültigen Löschen von Regeln verwenden Sie den Button **[Löschen]**. Wenn mehrere Regeln aktiv sind, können Sie das Ergebnis abschätzen, indem Sie **[Auswerten]** anklicken. Mehrere aktive Regeln werden über den logischen ODER-Operator gekoppelt, wenn Sie also drei aktive Regeln haben, nennen wir sie REGEL1, REGEL2, REGEL3, ist das Ergebnis gültig, sobald mindestens eine der drei Regeln zutrifft.

Sie können Erweiterte Regeln in Verbindung mit konventionellen Regeln des vorherigen Kapitels verwenden. Wenn Sie mit boolscher Logik vertraut sind ist es empfehlenswert nur die erweiterten Regeln zu verwenden da diese eine mehrfache Flexibilität offerieren. Die Grundregeln werden über einen logischen UND-Operator mit den Fortgeschrittenenregeln verknüpft.

Syntax Beschreibung

dir – Paketrichtung. Mögliche Werte sind *in* (inbound), *out* (outbound), und *pass* (pass-through).

etherproto – Ethernet Protokoll, das 13. und 14. Byte des Paketes. Erlaubte Werte sind Zahlen (wie *etherproto!=0x0800* für IP) oder allgemeine Kennnamen (wie *etherproto=ARPM* was gleichwertig zu 0x0806 ist).

ipproto – IP Protokoll. Erlaubt sind Zahlen (wie *ipproto=0x06* für TCP) oder allgemeine Kennnamen (wie *ipproto=UDP*, was gleichwertig zu 0x11 ist).

smac – Source MAC Adresse. Erlaubt sind hier MAC-Adressen in Hexnotation (wie *smac=00:00:21:0A:13:00F*) oder benutzerdefinierte Kennnamen.

dmac – Destination MAC Adresse (Ziel-MAC-Adresse).

sip – Source IP oder IPv6-Adresse. Erlaubt sind IP-Adressen in Punktnotation (wie *sip=192.168.0.1* oder *sip=fe80::02c0:26ff:fe2d:edb5*), IP-Adressen mit Wildcards (wie *sip!=*.*.*.255* mit Ausnahme von IPv6 addresses), Netzwerkadressen mit Subnet-Masken (wie *sip=192.168.0.4/255.255.255.240* oder *sip=192.168.0.5/28*), IP-Bereiche (wie *sip from 192.168.0.15 to 192.168.0.18* oder *sip in 192.168.0.15 .. 192.168.0.18*) oder benutzerdefinierte Kennnamen. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

dip – Ziel-IP- oder IPv6-address.

sport – Source Port (Ausgangs-Port) für TCP- und UDP-Pakete. Erlaubt sind Zahlen (wie *sport=80* für HTTP), Bereiche (wie *sport von 20 bis 50* oder *sport in 20..50* für alle Portnummer zwischen 20 und 50) oder die vom Betriebssystem definierten Kennnamen (wie *sport=ftp*, was gleichwertig zu 21 ist). Um die Liste aller Betriebssystemkennnamen zu erhalten klicken Sie bitte auf **Ansicht => Portreferenz**.

dpport – Ziel-Port (Ziel-Port) für TCP- und UDP-Pakete.

flag – TCP flag. Erlaubt sind Zahlen (wie *0x18* für PSH ACK) oder ein bzw. mehrere der folgenden Zeichen: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), und *U* (URG) oder das Schlüsselwort *has* (ist). Dies bedeutet, dass das Flag einen bestimmten Wert enthält. Beispiele: *flag=0x18*, *flag=SA*, *flag has F*.

size – Packet size (Paketgröße). Erlaubt sind Zahlen (wie *size=1514*) oder Bereiche (wie *size from 64 to 84* oder *size in 64..84* für jede Größe zwischen 64 und 84).

str – Paketinhalt. Wählen Sie dieses Argument, wenn das Paket einen bestimmten String enthalten muß. Es gibt drei Argumente: string, position und case sensitivity (Groß-/Kleinschreibung beachten). Das erste Argument ist ein String, wie *'GET'*. Das zweite Argument ist eine Zahl, welche die Stringposition (Offset) im Paket festlegt. Das Offset ist nullbasierend, d.h. wenn Sie das erste Byte des Paketes suchen, muss der Offsetwert *0* sein. Wenn das Offset ohne Bedeutung ist, wählen sie *-1*. Das dritte Argument legt die Bedeutung der Groß-/Kleinschreibung fest. Es ist entweder *false* (case-insensitive) oder *true* (case-sensitive). Das zweite und dritte Argument sind optional. Wenn hier nichts eingetragen wird ist der Standardwert *-1* und die case-sensitivity Einstellung ist *false*. Beispiele: *str('GET',-1,false)*, *str('GET',-1)*, *str('GET')*.

hex – Paketinhalt. Verwenden Sie diese Funktion, wenn das Paket bestimmte Hexadezimalwerte enthalten muß. Diese Funktion hat zwei Argumente: Hexmuster und Position. Das erste Argument ist ein Hexwert, wie *0x4500*. Das zweite Argument ist eine Zahl, welche die Musterposition (Offset) im Paket definiert. Das Offset ist nullbasierend, d. h. wenn Sie das erste Byte des Paketes suchen, muss der Offsetwert *0* sein. Wenn das Offset ohne Bedeutung ist, wählen sie *-1*. Das zweite Argument ist optional, wenn es weggelassen wird, ist die Standardeinstellung *-1*. Beispiele: *hex(0x04500, 14)*, *hex(0x4500, 0x0E)*, *hex (0x010101)*.

bit – Paketinhalt. Mit dieser Funktion ermitteln Sie, ob ein bestimmtes Bit eines definierten Offsets auf 1 gesetzt ist, so dass die Funktion *true* ausgegeben wird. Sollte das definierte Bit 0 sein oder außerhalb der Paketgrenzen liegen, so ergibt die Funktion *false*. Diese Funktion hat zwei Argumente: Bit-Index und Byte-Position. Das erste Argument ist der Bit-Index im Byte. Die erlaubten Werte sind hier im Bereich 0-7. Der Index ist nullbasierend, d. h. wenn Sie das 8. Bit suchen ist der Indexwert 7. Das zweite Argument ist die Zahl, die die Byte-Position (Offset) im Paket definiert. Auch dies ist nullbasierend, d. h. das 1. Bit hat den Wert *0*. Beide Argumente sind zwingend notwendig. Beispiele: *bit(0, 14)* , *bit(5, 1)*.

Die oben genannten Schlüsselwörter können mit den folgenden Operatoren verwendet werden:

and – Bool'sche Verknüpfung.

or – Bool'sche Unterscheidung.

not – Bool'sche Verneinung.

= – Arithmetisch gleich.

!= – Arithmetisch ungleich.

<> – Arithmetisch ungleich.

> – Arithmetisch größer als.

< – Arithmetisch kleiner als.

() – Runde Klammer, Operatorenvorrangsregel.

Zahlen entweder in Dezimal- oder Hexadezimalschreibweise. In der Hexnotation muß 0x vor jeder Zahl stehen, z. B. 15 oder 0x0F.

Beispiele

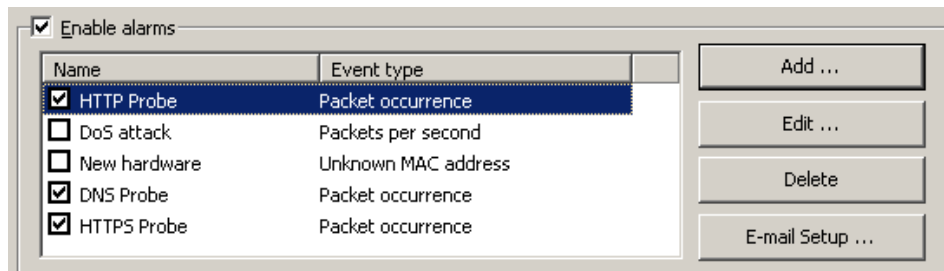
Folgende Beispiele zeigen die Regelsyntax. Jede Regel besitzt einen Kommentar zur Regelerklärung. Die Kommentare folgen nach zwei Schrägstrichen. Die Kommentare folgen nach zwei Schrägstrichen.

- **dir!=pass** // Erfasst nur ankommende und ausgehende Pakete. Durchgehende Pakete von anderen LAN Teilnehmern werden ignoriert.
- **(smac=00:00:21:0A:13:00E or smac=00:00:21:0A:13:00F) and etherproto=arp** // Empfängt die ARP-Pakete, die von den zwei Computern 00:00:21:0A:13:00E und 00:00:21:0A:13:00F gesendet werden.
- **ipproto=udp and dport=137** // Empfängt die UDP-/IP-Pakete die an Port 137 gesendet werden.
- **dport=25 and str('RCPT TO:', -1, true)** // Empfängt die TCP/IP- oder UDP/IP-Pakete, welche "'RCPT TO:" enthalten und die den Zielport 25 haben.
- **not (sport>110)** // Empfängt alle Pakete, außer denen, deren Quellport größer als 110 ist.
- **(sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3)** // Empfängt nur die IP-Pakete, die zwischen den Maschinen 192.168.0.3 und 192.168.0.15 ausgetauscht werden. Alle anderen Pakete werden ignoriert.
- **((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)** // Empfängt die TCP-Pakete, deren Größe zwischen 200 und 600 Bytes ist und die aus dem IP-Bereich 192.168.0.3 - 192.168.0.7 kommen, deren IP-Zieladresse im Bereich 192.168.1.0/255.255.255.240 liegt und deren TCP-Flag PSH ACK ist.
- **Hex(0x0203, 89) and (dir<>in)** // Empfängt die Pakete, die 0x0203 im Offset 89 enthalten und deren Paketrichtung nicht inbound ist.

Alarme

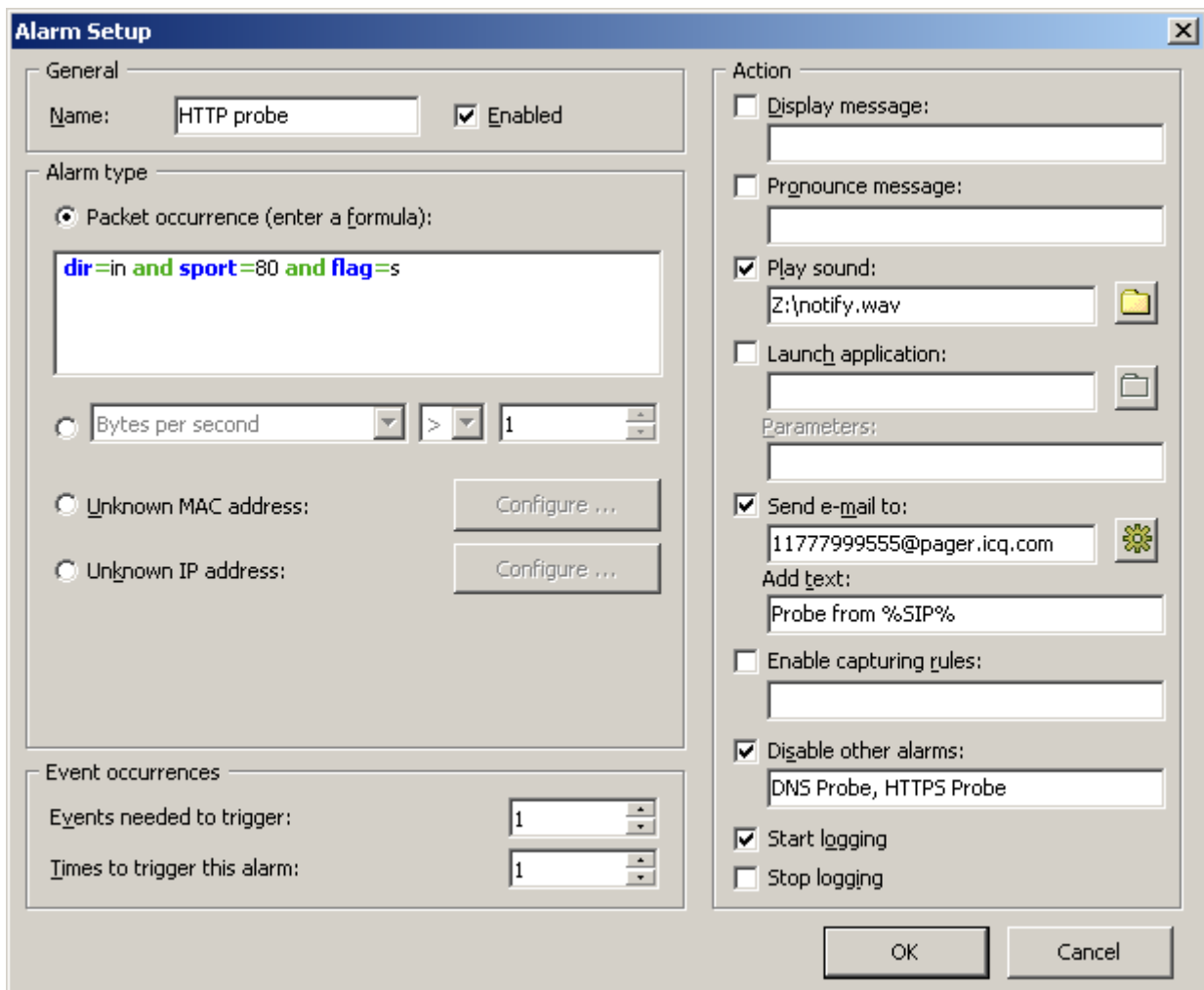
Dieses Register ermöglicht es Alarme zu erzeugen, die Sie über bestimmte Ereignisse informieren, wie verdächtige Pakete, starke Bandbreitennutzung, unbekannte Adressen usw. Solche Alarme sind sehr nützlich, wenn Sie das Netzwerk auf bestimmte verdächtige Ereignisse überwachen, wie auffällige Bytemuster in den empfangenen Paketen, Portscans oder unerwartete Hardwareverbindungen.

Alarme werden über die folgende Liste verwaltet:



Jede Zeile entspricht einem separaten Alarm und die Checkbox daneben zeigt, ob der Alarm gegenwärtig aktiv ist. Wenn ein Alarm ausgelöst wird verschwindet die Checkbox. Um einen deaktivierten Alarm wieder zu aktivieren markieren Sie erneut die Checkbox neben dem Alarmnamen. Um alle Alarme zu deaktivieren, leeren Sie die Liste **Alarme aktivieren**. Um einen neuen Alarm zu editieren oder zu löschen verwenden Sie bitte die gleichnamigen Buttons im rechten Teil des Dialogs. Mittels des Button **[E-Mail-Setup]** können Informationen zu Ihrem SMTP-Server eingegeben werden, wenn Sie E-Mail-Benachrichtigung wünschen (s. u.).

Das Alarmeinstellungsfenster wird unten gezeigt:



Das Feld **Name** sollte für die Beschreibung der Alarmfunktion genutzt werden. Aktivieren Sie die Checkbox **Aktiviert** wenn der Alarm nach dem Hinzufügen/Editieren bei Beendigung des Setup aktiviert werden soll. Diese Checkbox entspricht der in der Alarmliste. Mit dem Auswahlbereich **Alarm Typ** wählen Sie einen von sieben Alarmen aus:

- **Paket-Ereignis:** CommView löst den Alarm aus, wenn es ein Paket empfängt, das einer bestimmten Formel entspricht. Die Formelsyntax entspricht der Syntax für die Fortgeschrittenenregeln. Mehr dazu unter [Erweiterte Regeln](#).
- **Bytes/Sekunde:** Der Alarm wird ausgelöst, wenn die Byteanzahl/Sekunde einen Grenzwert über- bzw. unterschreitet. Bitte beachten Sie, dass der Wert in Bytes eingegeben werden muss, so dass bei einem gewünschten Alarm ab 1 Mbyte/Sekunde ein Wert von 1000000 eingegeben werden muss.
- **Pakete/Sekunde:** Der Alarm wird ausgelöst, wenn die Anzahl der Pakete/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Broadcasts/Sekunde:** Der Alarm wird ausgelöst, wenn die Anzahl der Broadcast-Pakete/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Multicasts/Sekunde:** Der Alarm wird ausgelöst, wenn die Anzahl der Multicast-Pakete/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Unbekannte MAC-Adr.:** Der Alarm wird ausgelöst, wenn CommView ein Paket von einer unbekanntem Quell- oder zu einer unbekanntem Ziel-MAC-Adresse empfängt. Mittels des Buttons **[Konfigurieren]** können

Sie eine bekannte MAC-Adresse eingeben. Dieser Alarm ist nützlich, um neue unautorisierte Geräte zu erkennen, die mit Ihrem LAN verbunden sind.

- **Unbekannte IP-Adresse:** Der Alarm wird ausgelöst, wenn CommView ein Paket mit einer unbekanntem Quell- oder Ziel-IP-Adresse oder IPv6-Adresse empfängt. Mittels des Buttons **[Konfigurieren]** können Sie eine bekannte IP-Adresse eingeben. Dieser Alarm ist nützlich, um unautorisierte IP-Verbindungen hinter einer Firmen-Firewall zu entdecken. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

Das Eingabefeld **Erford. Anzahl Ereignisse für Alarm:** ermöglicht Ihnen den Schwellenwert für die Ereignisanzahl festzulegen, um einen Alarm auslösen zu lassen. Wenn Sie z. B. einen Wert von 3 wählen, wird ein Alarm erst ausgelöst, wenn das entsprechende Ereignis dreimal auftaucht. Wenn Sie einen bereits existierenden Alarm editieren, wird der Zähler auf Null zurückgesetzt.

Das Eingabefeld **Max. Anzahl Auslösungen des Alarms:** ermöglicht es Ihnen die Anzahl der Alarme festzulegen, bevor diese deaktiviert werden. Standardeinstellung ist hier 1, so dass nach dem ersten Alarm dieser deaktiviert wird. Wenn Sie diesen Wert erhöhen, wird CommView ihn mehrmals auslösen. Wenn Sie einen Alarm editieren, wird der Zähler auf Null zurückgesetzt.

Im Bereich **Aktion** wählen sie die mit dem Alarm auszulösenden Ereignisse. Folgende Aktionen stehen zur Wahl:

- **Nachrichten anzeigen** – Zeigt eine non-modale Meldungbox mit dem definierten Text. Mit dieser Aktion können Sie Variablen verwenden, die im Alarmfall durch die entsprechenden Parameter des Paketes, das den Alarm hervorrief, ersetzt werden. Diese Variablen sind:

%SMAC% -- Quell-MAC-Adresse.

%DMAC% -- Ziel-MAC-Adresse.

%SIP% -- Quell-IP-Adresse.

%DIP% -- Ziel-IP-Adresse.

%SPORT% -- Quell-Port.

%DPORT% -- Ziel-Port.

%ETHERPROTO% -- Ethernet-Protokoll.

%IPPROTO% -- IP-Protokoll.

%SIZE% -- Paketgröße.

%FILE% -- Pfad zu einer temporären Datei, die das empfangene Paket enthält.

So wird z. B. in Ihrer Nachricht in der Meldung "SYN Paket von %SIP%," im aktuellen Popup Windowtext %SIP% ersetzt werden durch die Quell-IP-Adresse des alarmauslösenden Paketes. Wenn Sie die %FILE%-Variable verwenden, wird eine NCF-Datei in einem temporären Verzeichnis erzeugt. Es liegt in Ihrer Verantwortung diese Datei nach der Bearbeitung zu löschen. Sie sollten keine Variablen verwenden, wenn der Alarm ausgelöst wurde von **Bytes/Sekunde** - oder **Pakete/Sekunde-Werten**, da diese Alarme nicht von individuellen Paketen ausgelöst werden.

- **Nachricht sprechen** – Lässt Windows, unter Benutzung der Text-to-speech engine, die Nachricht sprechen. Diese Checkbox ist abgeschaltet, wenn Ihre Windows-Version keine Text-to-speech engine besitzt. Standardmäßig kommt Windows nur mit englischen Computerstimmen, sodass Windows nicht in der Lage ist, Nachrichtentext in anderen Sprachen als englisch korrekt auszusprechen. Sie können die in der Sektion **Nachrichten anzeigen** beschriebenen Variablen im Nachrichtentext benutzen.
- **Akustisches Signal** – Spielt die gewählte WAV-Datei ab.

- **Applikation starten** – Startet die ausgewählte EXE- oder COM-Datei. Mit dem optionalen Feld **Parameter:** können in der Befehlszeile Parameter eingegeben werden. Die Variablen, die in der Sektion **Nachrichten anzeigen:** beschrieben wurden können als Befehlszeilenparameter eingegeben werden, sofern Sie möchten, dass die Anwendung Informationen über das alarmauslösende Paket empfängt und bearbeitet.
- **E-Mail senden an** – Sendet eine E-mail an eine definierte Adresse. CommView MUSS konfiguriert werden, um Ihren SMPT-Server vor dem Senden der E-Mail nutzen zu können. Mittels des Buttons **E-Mail-Einstellungen** neben der Alarmliste können Sie Ihre SMPT-Server-Einstellungen eingeben und eine Test-E-Mail absenden. Man kann E-Mail-Benachrichtigungen auch an Instant Messenger-Anwendungen, Handy oder Pager senden. Um z. B. eine Nachricht an einen ICQ-User zu senden, geben Sie die E-Mail-Adresse als ICQ_USER_UIN@pager.icq.com ein, wobei ICQ_USER_UIN die eindeutige ICQ-Identifikationsnummer ist. Dazu müssen die EmailExpress Messages in den ICQ-Optionen aktiviert sein. Mehr dazu in Ihrem Instant Messenger- oder Handy-Handbuch. Das Feld Text hinzufügen kann zum Hinzufügen einer beliebigen Nachricht zur E-Mailbenachrichtigung genutzt werden. Sie können die in der Sektion Nachrichten anzeigen beschriebenen Variablen im Nachrichtentext benutzen.
- **Erfassungsregeln aktivieren** – Aktiviert [Erweiterte Regeln](#); Sie müssen den Regelname eingeben. Mehrere Regeln werden komma- bzw. semikolongetrennt eingegeben.
- **Andere Alarmer deaktivieren** – Deaktiviert andere Alarmer. Sie sollten dabei den Alarmnamen eingeben. Mehrere Regeln werden komma- bzw. semikolongetrennt eingegeben.
- **Logging starten** – Startet die Autospeicherung (s. Kapitel [Protokollierung](#)). CommView beginnt dann Pakete auf der Festplatte abzulegen.
- **Logging stoppen** – beendet die Autospeicherung.

Klicken Sie auf **[OK]** um die Einstellungen abzuspeichern und das Alarmdialogfenster zu schliessen.

Alle Ereignisse und Aktionen, die mit den Alarmen zu tun haben, finden Sie im Bereich **Ereignislog** unterhalb der Alarmliste.

Rekonstruktion von TCP-Sitzungen

Mit diesem Dialog können Sie sich die TCP-Kommunikation zwischen zwei Host's ansehen. Um eine TCP-Sitzung zu rekonstruieren, wählen Sie als erstes ein TCP-Paket im Register **Pakete**. Abhängig von den Einstellungen (Checkbox: **Suche den Sitzungstart wenn TCP-Sitzungsrekonstruktion startet** in **Einstellungen => Optionen => Dekodierung**), wird die Sitzung von dem ausgewählten Paket ausgehend (kann ein Paket aus der Sitzungsmitte oder vom Sitzungsstart sein) rekonstruiert. Nach dem Sie das Paket gefunden und ausgewählt haben, führen Sie einen Rechtsklick darauf aus und wählen **TCP-Sitzung rekonstruieren** wie unten gezeigt:

Dest IP	Src Port	Dest Port	Time
62.27.45.170 (DE)	3098	http	14:01.
62.27.45.170 (DE)	3100	http	14:01.
222.154.233.			
222.154.233.			
adswb.tiscali			

Reconstruct TCP Session

Quick Filter

Rekonstruktionssitzungen funktionieren am besten mit textbasierten Protokollen, wie POP3, Telnet oder HTTP. Natürlich können Sie den Download einer großen Zip-Datei rekonstruieren, aber es kann sein, dass CommView für die Rekonstruktion von mehreren Megabytes sehr lange braucht, und meist ist dann auch die erhaltene Information sinnlos. Das Register **Inhalt** zeigt die aktuellen Sitzungsdaten an, während das Register **Sitzungsanalyse** den Fluss der rekonstruierten TCP-Sitzungen graphisch darstellt.

Eine Beispiel-HTTP-Session mit HTML-Daten, die im ASCII- und HTML-Modus angezeigt werden, ist im Folgenden dargestellt:

The screenshot shows the 'TCP Session' window in CommView. The window title is 'TCP Session' and it has a menu bar with 'File', 'Edit', and 'Settings'. Below the menu bar are two tabs: 'Contents' and 'Session Analysis'. The main area displays the following text:

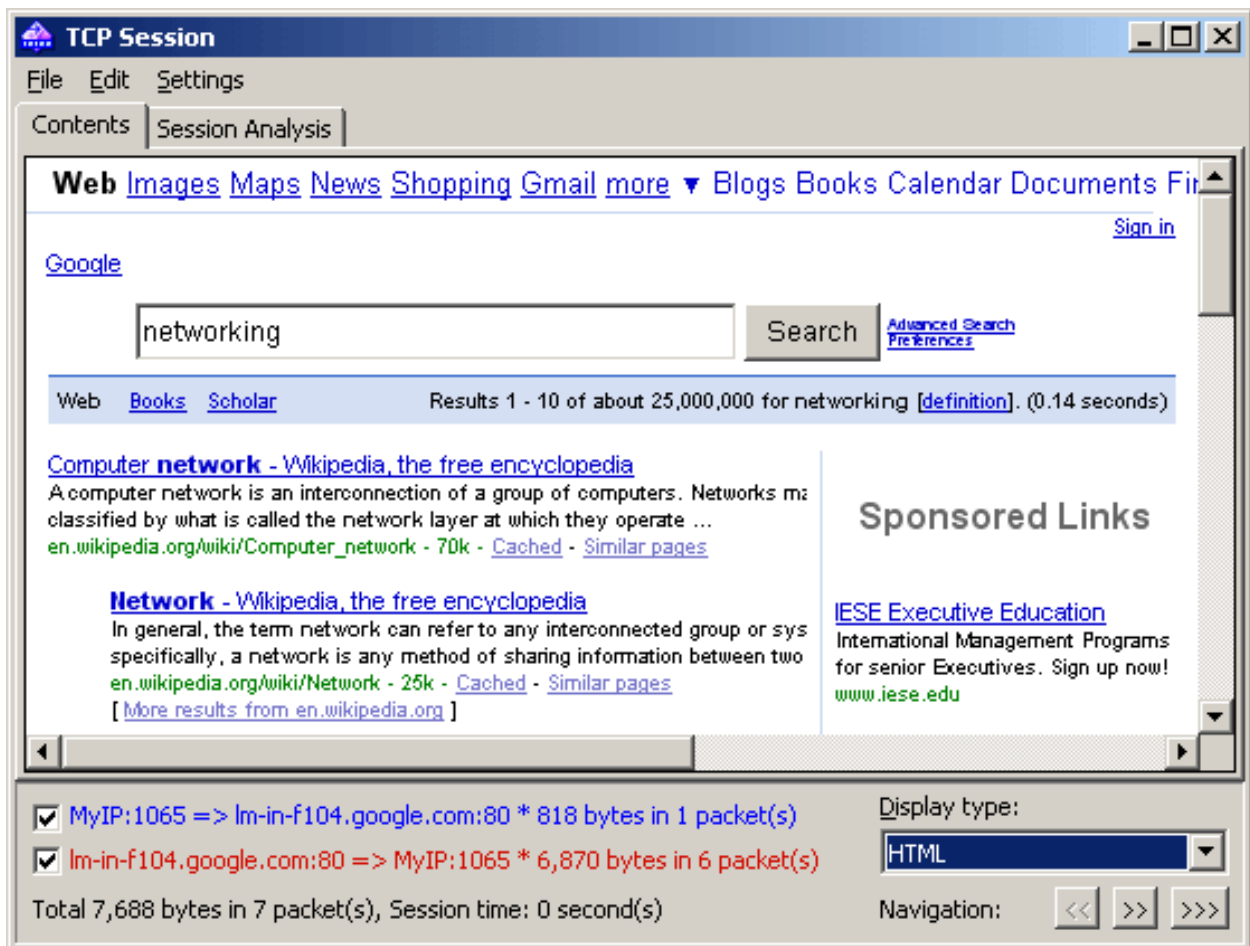
```
GET /wiki/Computer_network HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword,
application/x-silverlight, */*
Referer:
http://www.google.com/search?sourceid=navclient&ie=UTF-8&rlz=1T4GFRC_enRU220
RU225&q=networking
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
2.0.50727; .NET CLR 1.1.4322)
Host: en.wikipedia.org
Connection: Keep-Alive

HTTP/1.0 200 OK
Date: Mon, 17 Dec 2007 09:50:04 GMT
```

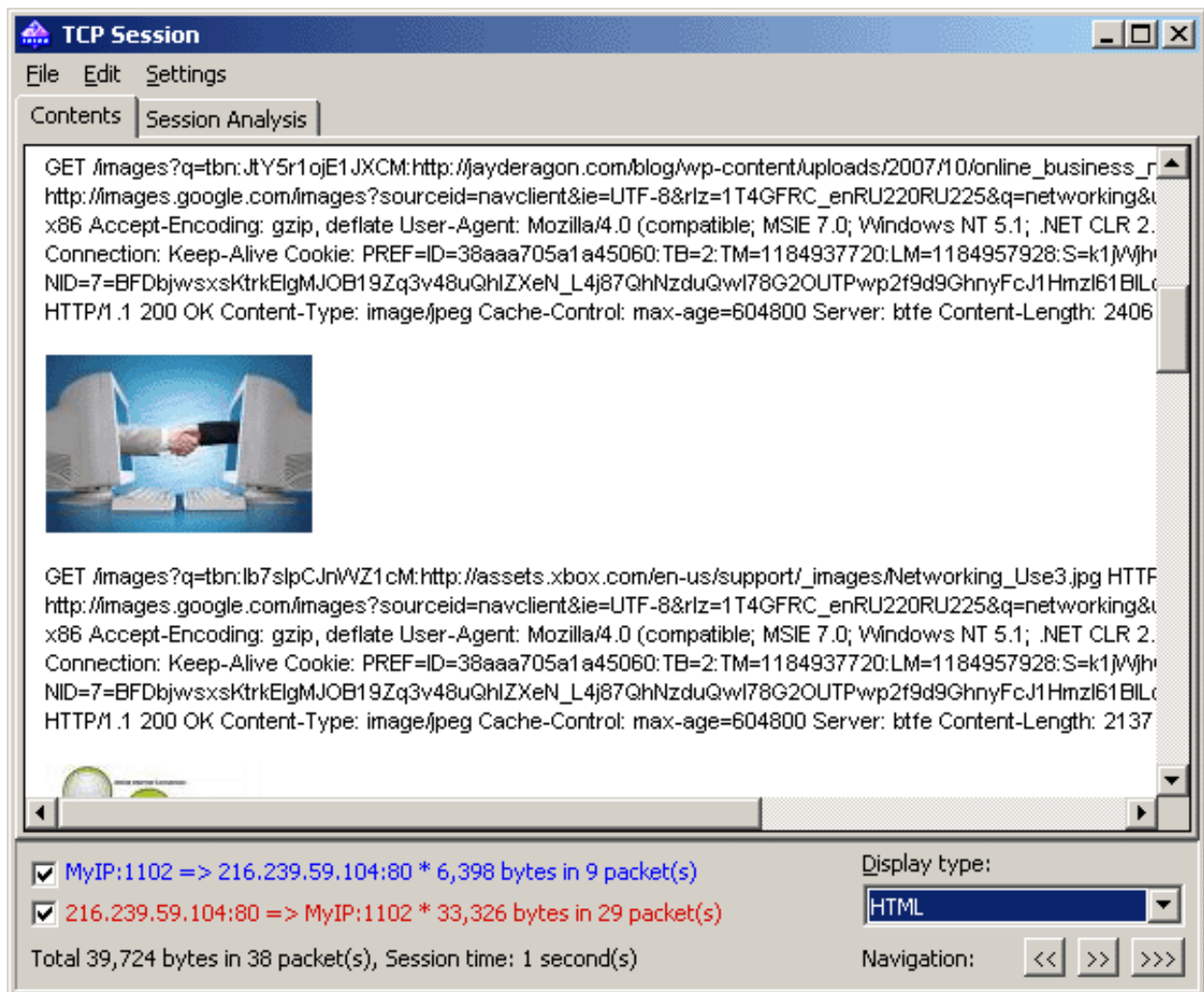
At the bottom of the window, there are two checked checkboxes:

- MyIP:1068 => rr.pmtpa.wikimedia.org:80 * 1,472 bytes in 4 packet(s)
- rr.pmtpa.wikimedia.org:80 => MyIP:1068 * 24,372 bytes in 19 packet(s)

Below these is the text: 'Total 25,844 bytes in 23 packet(s), Session time: 3 second(s)'. To the right, there is a 'Display type:' dropdown menu set to 'ASCII' and 'Navigation:' buttons: '<<', '>>', and '>>>'.



Im HTML-Anzeigemodus werden in den HTML-Seiten niemals Bilder angezeigt, da im HTTP-Protokoll Bilder separiert vom Text übertragen werden. Um diese Bilder zu sehen, müssen Sie zur nächsten TCP-Sitzung navigieren. Im Folgenden finden Sie ein Beispiel für eine HTTP-Sitzung, die Bilder enthält und im HTML-Modus angezeigt wird:



Standardmässig versucht CommView GZIP-ten Webinhalt zu dekomprimieren und Bilder aus dem Binärstrom zu rekonstruieren. Diese Funktion kann im Dialog **Einstellungen** mittels des Bereichs **Decodierung** abgeschaltet werden.

Wenn Sie im unteren Bereich eine der Checkboxes deaktivieren, können Sie Daten, die aus einer bestimmten Richtung kommen ausfiltern. Ein- und ausgehende Daten haben, um markanter zu sein, verschiedene Farben. Diese Farben können Sie mittels **Einstellungen => Farben** ändern. Wort-Wrapping kann mittels **Einstellungen => Word Wrap** aktiviert/deaktiviert werden.

Mittels der Dropdown-Liste **Anzeigetyp** können Sie die Daten in folgenden Formaten ansehen: **ASCII-** (Klartext), **HEX-** (hexadezimal), **HTML-** (Webseiten und Bilder), **EBCDIC-Format** (IBM mainframes' data encoding) und **UTF-8** (Unicode-Daten). Bitte beachten Sie, dass die Ansicht der Daten im HTML- Format nicht automatisch dieselben Ergebnisse bringt, wie mit dem Webbrowser (Sie sehen dann keine Inlinegrafik), dennoch erhalten Sie eine ungefähre Vorstellung, wie die Seite im Original aussah.

Im Dialog **Einstellungen** können Sie unter **Decodierung** festlegen, wie der Standardanzeigetyp für die Rekonstruktion von TCP-Sitzungen aussieht.

Mit den **Navigation**-Buttons können Sie den Puffer nach der nächsten oder letzten TCP-Sitzung absuchen. Der erste Vorwärts-Button [**>>**] sucht nach der nächsten Sitzung zwischen den beiden Hosts, die an der ersten Rekonstruktionssitzung beteiligt waren. Der zweite Vorwärts-Button [**>>>**] sucht nach der nächsten Sitzung zwischen zwei beliebigen Hosts. Wenn Sie mehrere TCP-Sitzungen zwischen den zwei Hosts im Puffer haben und

alle nacheinander ansehen wollen, empfehlen wir mit der Rekonstruktion der ersten Sitzung anzufangen, da der Rückwärtsbutton [**<<**] nicht weiter zurück als bis zur zuerstrekonstruierten TCP-Sitzung gehen kann.

Die so erhaltenen Daten können als Binärdaten, HTML-, Text- oder Rich-Textdatei durch Klicken auf **Datei => Speichern unter...** gesichert werden. Wenn Sie in ein Textformat speichern, ist die Ergebnisdatei eine Unicode UTF-16-Datei. Wird ins HTML-Format gespeichert, ist die Verschlüsselung der Ergebnisdatei vom aktuell gewählten **Anzeigetyp** abhängig. Wenn HTML aktuell gewählt ist, wird die Ergebnisdatei eine ANSI-Textdatei, für alle anderen Anzeigetypen ist die Ergebnisdatei eine Unicode UTF-16-Datei. Beachten Sie, wenn Sie eine HTTP-Sitzung mit Bildern speichern, werden die Bilder in das temporäre Verzeichnis auf Ihrer Festplatte gespeichert, falls Sie die Bilder behalten möchten, öffnen Sie die gespeicherte Datei in Ihrem Browser und speichern die Datei in einem Format, das Bilder beinhaltet, z.B. MHT, bevor Sie CommView schließen.

Sie können durch Klicken auf **Bearbeiten => Finden...** nach einer Zeichenkette in der Sitzung suchen.

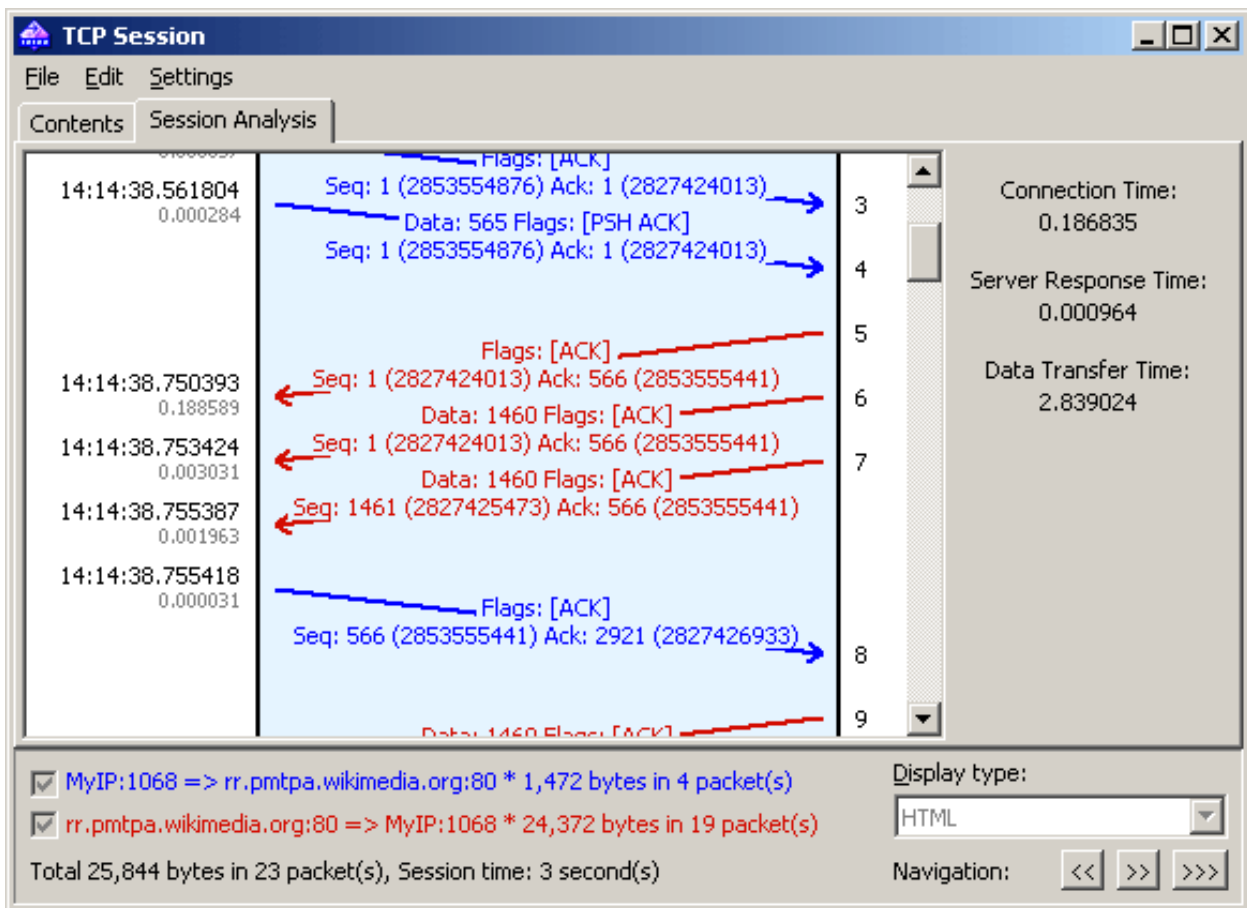
Sitzungsanalyse

Das Register Sitzungsanalyse des TCP-Sitzungsfensters stellt rekonstruierte TCP-Sitzungen grafisch dar. Sie können den Sitzungsdatenfluss, Fehler, Verzögerungen und verlorene erneut übertragene Daten sehen.

Die folgenden Daten werden für jedes Sitzungspaket angezeigt:

- TCP-Flags.
- Absolute und relative SEQ- und ACK-Werte.
- Paketankunftszeit.
- Zeitdifferenz zwischen dem aktuellen und dem vorhergehenden Paket.
- Paketnummer in der rekonstruierten Sitzung.

Wenn ein Paket Fehler beinhaltet, wird die Eigenschaft des Fehlers erklärt. Es erscheint ein Beschreibungstext am rechten Rand des Diagramms. Wenn Sie die Maus über ein Paket mit Dateninhalt bewegen, wird der Dateninhalt in einem Hinweisfenster angezeigt. Beachten Sie, dass das Feld **Anzeigetyp** bestimmt, wie die Daten im Anzeigefenster decodiert werden. Ein Beispiel für ein Sitzungsanalysefenster wird unten gezeigt:



Der rechte Ausschnitt zeigt einige Basisstatistiken für die vorgegebene Sitzung:

Verbindungszeit – Die benötigte Zeit zur Herstellung der TCP-Verbindung. In anderen Worten, es ist die Dreiweg-TCP-Handshake-Zeit (SYN => SYN ACK => ACK).

Server-Antwortzeit – Die verstrichene Zeit zwischen der Klientenanfangsanfrage und der ersten Datenantwort des Servers.

Datenübertragungszeit – Die Zeit zwischen der ersten und der letzten Datenantwort des Server's (0 bei nur einer Server-Antwort).

Sie können das grafische Schaubild der rekonstruierten TCP-Sitzung als BMP-, GIF- oder PNG-Datei durch Rechtsklick auf das Schaubild und Auswahl des Kontextmenüpunktes **Bild speichern als...** speichern. Sitzungen mit einer großen Paketanzahl werden in mehrere Dateien aufgeteilt. UDP-Ströme rekonstruieren

Dieses Werkzeug ist dem im vorhergehenden Kapitel beschriebenen Werkzeug [TCP-Sitzungen rekonstruieren](#) sehr ähnlich; schauen Sie bitte für weitergehende Informationen in diese Kapitel. Allerdings ist UDP, nicht wie TCP, ein verbindungsloses Protokoll, die folgenden Unterschiede bestehen zwischen TCP-Sitzungsrekonstruktion und UDP-Stream-Rekonstruktion:

- Es gibt kein Register Sitzungsanalyse, weil es keine Sitzungen, SEQs oder ACKs in UDP gibt.
- Weil es keine SYNs oder FINs in UDP gibt, gelten alle zwischen den IP-Adresspaaren und Ports gesendeten Pakete, als zu demselben Stream gehörend.

Pakete Suchen

Um die Pakete aufzufinden, die einen bestimmten Text oder eine bestimmte Adresse enthalten, öffnen Sie den **Finde Paketinhalt** Dialog (**Suchen => Finde Paket**). Geben Sie einen Such-String ein, wählen Sie die Art der eingegebenen Information (**String** oder **Hex**) und klicken Sie auf [**Finde nächstes**]. Das Programm sucht dann nach Paketen, die dem Suchkriterium entsprechen und zeigt diese dann im Register **Pakete** an.

Sie können den Text als String, hexadezimal Wert, MAC- oder IP-Adresse eingeben. Die Zeichenkettensuche wird in ASCII- und Unicode-Formaten (UTF-8 und UTF-16) ausgeführt. Einen Hex-String sollte benutzt werden wenn Sie nichtdruckbare Zeichen eingeben wollen: Geben Sie die hexadezimalen Werte folgendermaßen ein, z. B. AD0A027804. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

Aktivieren Sie **Gross-/Kleinschr.** für eine Suche unter Berücksichtigung der Gross- und Kleinschreibung. Aktivieren Sie **Bei Offset** (hex.): um einen String zu suchen, der zu einem bestimmten Offset beginnt. Beachten Sie bitte, dass der Offset-Indikator hexadezimal und nullbasierend ist (wenn Sie z. B. nach dem ersten Byte in dem Paket suchen, ist das Offset 0). Sie können ebenso eine Suchrichtung auswählen, **Aufwärts** oder **Abwärts**.

Statistiken und Berichte

Dieser Dialog (**Ansicht => Statistiken**) zeigt wichtige Netzwerkstatistiken für Ihr LAN-Segment, wie Paketanzahl/Sekunde, Bytes/Sekunde, Ethernet-Protokolle, IP-Protokolle, Sub-Protokolle und die Verteilungsgrafiken zu den Sub-Protokollen. Jede grafische Darstellung kann durch Doppelklicken in die Zwischenablage kopiert werden. Die Kuchengrafiken der Ethernet-Protokolle, IP-Protokolle und der Sub-Protokolle können, mittels der kleinen Buttons im unteren rechten Eck, zur besseren Sichtbarkeit der Bereiche rotiert werden.

Die auf jeder Seite angezeigten Daten können als Bitmap oder kommaseparierte Textdatei über das Kontextmenü bzw. durch Drag&Drop gespeichert werden. Mit der Seite **Bericht** kann CommView automatisch individualisierte Berichte im HTML- bzw. kommaseparierten Textformat erstellen.

Netzwerkstatistiken können aus allen über ihr Netzwerkadapter laufenden Daten oder durch die Regeldefinitionen erzeugt werden. Wenn sie wollen, dass die Statistikzähler nur die Daten der Pakete erfassen, die dem aktuellen Regelsatz entsprechen (und keine anderen), sollten Sie die Checkbox **Aktuelle Regeln anwenden** aktivieren.

Allgemein

Dies zeigt die Pakete/Sekunde bzw. Bytes/Secunde oder Bits/Sekunde als Histogramm an, ferner den Bandbreitenverbrauch (Verkehr/Sekunde dividiert durch die Geschwindigkeit des WLAN-Adapters), ferner den Gesamtpaket- und -bytezähler. Ein Doppelklick auf die Anzeige öffnet ein Dialogfenster, in dem Sie die Adaptergeschwindigkeit manuell konfigurieren können, damit diese für die Bandbreitennutzungsberechnungen verwendet werden kann.

Protokolle

Zeigt die Verteilung der Ethernet-Protokolle, wie ARP, IP, SNAP, SPX, etc. Mittels der Dropdown-Liste Diagramm von: können Sie eine von zwei möglichen Berechnungsmethoden verwenden: Nach der Anzahl der Pakete oder nach der Byteanzahl. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl.

IP-Protokolle

Zeigt die Verteilung der IP-Protokolle TCP, UDP, und ICMP. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl.

IP-Unterprotokolle

Zeigt die Verteilung der wichtigsten IP-Anwendungslevel-Unterprotokolle: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, und DNS. Um weitere Protokolle hinzuzufügen verwenden Sie den Button **[Einstellungen]**. Mit diesem Dialog können Sie bis zu 8 selbstdefinierte Protokolle hinzufügen. Geben Sie dazu den Protokollnamen ein, wählen Sie den Protokolltyp (TCP/UDP) und die Portnummer. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl.

Größe

Zeigt die Verteilung (Grafik) nach Paketgröße.

Hosts nach MAC

Listet die aktiven LAN-Hosts geordnet nach MAC-Adresse auf und zeigt die Datentransferstatistik. Sie können den MAC-Adressen Kennnamen zuordnen. Wenn Sie zu viel Multicast-Pakete in Ihrem Netzwerk haben, so dass die Hosts nach MAC-Tabelle überfüllt ist, können Sie die Multicast-Adressen zusammenfassen (GroupedMulticast). Diese Funktion aktivieren Sie mittels Aktivierung der Checkbox **Multicast-Adressen gruppieren**. Beachten Sie, dass nur Pakete, die nach der Aktivierung dieser Funktion ankommen, entsprechend gruppiert werden, vorher empfangene Pakete werden nicht berücksichtigt.

Hosts nach IP

Listet die aktiven LAN-Hosts nach IP-Adresse auf und zeigt die Datentransferstatistik. Da empfangene IP-Pakete von beliebig vielen IP-Adressen stammen können (innerhalb bzw. außerhalb Ihres LANs), zeigt diese Tabelle standardmässig keine Statistik. Zur Anzeige der Statistik müssen Sie erst den zu überwachenden IP-Adressraum durch klicken auf **Bereich hinzufügen/setzen** festlegen. Normalerweise sollte dieser Bereich zu Ihrem LAN gehören. Durch die Konfiguration eines solchen Bereiches von IP-Adressen erhalten Sie die Nutzungsstatistik. Sie können jeden Bereich definieren, solange der Gesamt-IP-Adressbereich nicht mehr als 1.000 IP-Adressen umfaßt. Um einen Bereich zu löschen rechtsklicken Sie auf die Liste des Bereiches und wählen dann den entsprechenden Menübefehl. Sie können den IP-Adressen Kennnamen zuordnen. Ferner können Sie die Checkbox **Alle** wählen, um alle IP-Adressen aufzulisten. Diese Funktion wird jedoch nicht empfohlen für die Nutzungserfassung von RAM und CPU.

Matrix nach MAC

Diese Seite zeigt eine grafische Matrix zwischen Hosts und deren MAC-Adressen. Die durch die MAC-Adressen repräsentierten Hosts sind innerhalb des Kreises und die Sessions werden als Verbindungen zwischen diesen angezeigt. Wenn Sie den Mauszeiger über einen Host führen werden alle Verbindungen von diesem Host zu anderen Hosts hervorgehoben. Die Anzahl der aktivsten Hostpaare können Sie mittels des Wertes im Feld **Aktivste Hostpaare** ändern. Wenn Sie die Anzahl der zuletzt untersuchten Paare ändern wollen, verändern Sie bitte den Wert im Feld **Letzte Pakete einbeziehen**. Wenn die Matrix zu voll ist, da Ihr Netzwerk zu viele Broadcast- bzw. Multicastpakete hat, aktivieren Sie die Checkboxen **Broadcasts ignorieren** und **Multicasts ignorieren**.

Matrix nach IP

Diese Seite zeigt grafisch den Zusammenhang zwischen Hosts und deren IP-Adressen. Die durch die IP-Adressen repräsentierten Hosts sind innerhalb des Kreises, und die Sitzungen werden als Verbindungen zwischen diesen angezeigt. Wenn Sie den Mauszeiger über einen Host führen werden alle Verbindungen von diesem Host zu anderen Hosts hervorgehoben. Die Anzahl der aktivsten Hostpaare können Sie mittels des Wertes im Feld **Aktivste Hostpaare** ändern. Wenn Sie die Anzahl der zuletzt untersuchten Paare ändern wollen, verändern Sie den Wert im Feld **Letzte Pakete einbeziehen**. Wenn die Matrix zu voll ist, da Ihr Netzwerk zu viele Broadcast- bzw. Multicastpakete hat, aktivieren Sie die Checkboxen **Broadcasts ignorieren** und **Multicasts ignorieren**.

Fehler

Fehlerinformationen der Ethernet-Adapter können statistisch erfasst werden. Folgend eine Liste der Fehlertypen mit Erläuterungen:

CRS-Fehler

Anzahl der empfangenen Frames mit einem CRC-Fehler oder FCS-Fehler.

Rx Alignment-Fehler

Anzahl der empfangenen Frames mit einem Alignment- Fehler.

Rx Overrun

Anzahl der nicht empfangenen Frames, verursacht aufgrund eines Overrun-Fehlers der NIC.

Tx One Collision

Anzahl der, nach genau einer Kollision, erfolgreich übertragenen Frames.

Tx More Collisions

Anzahl der, nach mehr als einer Kollision, erfolgreich übertragenen Frames.

Tx Deferred

Anzahl der erfolgreich übertragenen Frames nachdem die NIC die Übertragung mindestens einmal verschoben hat.

Tx Max Collisions

Anzahl der, aufgrund zu vieler Kollisionen, nicht erfolgreich übertragenen Frames.

Tx Underrun

Anzahl der nicht übertragenen Frames, verursacht aufgrund eines Underrun-Fehlers der NIC.

Tx Heartbeat Failure

Anzahl der erfolgreich übertragenen Frames ohne dass eine Heartbeat-Kollision festgestellt wurde.

Tx Times CRS Lost

Anzahl der verlorenen CRS-Signale während der Paketübertragung.

Tx Late Collisions

Anzahl der Kollisionen die nach dem normalen Fenster festgestellt wurden.

Rx Frames w/Errors

Anzahl der Frames die empfangen wurden, die jedoch aufgrund eines Fehlers nicht einem aktivierten Protokoll zugeordnet werden können.

Rx Frames w/o Errors

Anzahl der Frames die fehlerfrei empfangen wurden und die einem aktivierten Protokoll zugeordnet werden können.

Tx Frames w/Errors

Anzahl der von der NIC nicht übertragenen Frames.

Tx Frames w/o Errors

Anzahl der fehlerlos übertragenen Frames.

Bitte nehmen Sie zur Kenntnis:

- Modems werden nicht unterstützt, sondern nur Ethernet-Karten.
- Ihre Ethernet Karte unterstützt bzw. meldet möglicherweise nicht alle der oben erwähnten Fehler. Das ist Hersteller- bzw. NIC abhängig.
- Im Gegensatz zu anderen Daten im Statistikfenster, können die Daten im Register **Fehler** nicht durch Klicken auf den Button **[Reset]** zurückgesetzt werden. Die Initialisierung dieses Zählers erfolgt beim Hochfahren ihres PC's.

Bericht

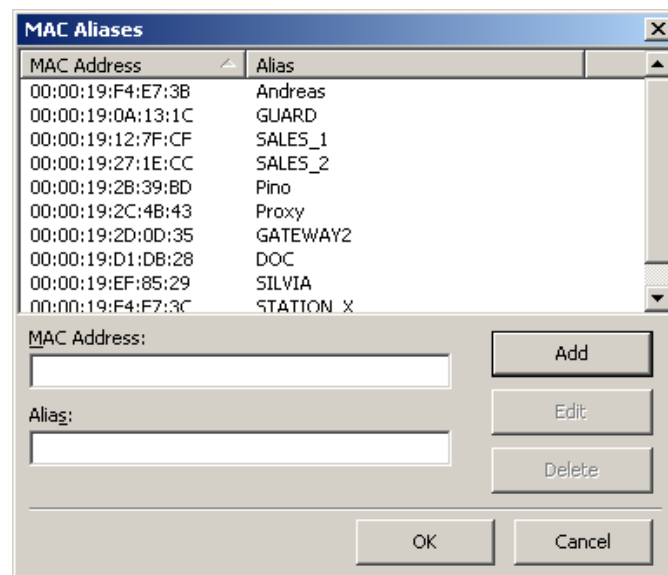
Mit diesem Dialog erzeugt CommView automatisch Berichte im HTML- (einschl. Bildern von Tabellen und Graphen) oder kommaseparierten Textformat.

Neben den Echtzeitstatistiken kann das Programm auch Statistiken aus bereits gesammelten Daten erstellen. Dazu laden Sie eine Datei in den [Logbetrachter](#) und klicken dann **Datei => Statistik generieren**. Vorher im Statistikfenster gesammelte Daten können, wenn gewünscht, gelöscht werden. Diese Funktion zeigt keine Zeitreihenanalyse. Sie zeigt nur Summen, Protokollkarten und LAN-Host-Tabellen.

Die Verwendung von Kennnamen

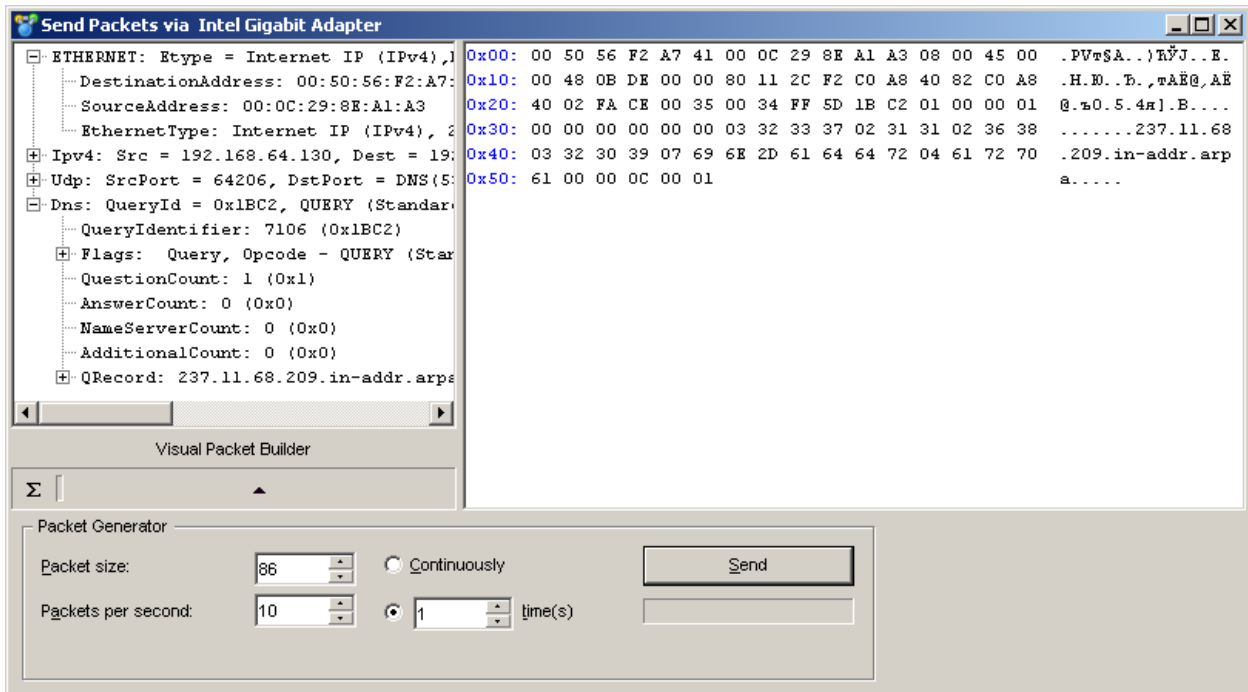
Kennnamen sind leicht zu merkende, für Menschen besser lesbare Namen, die CommView anstelle von MAC- bzw. IP-Adressen einsetzt, wenn Pakete in den Registern **Pakete** und **Statistiken** angezeigt werden. Die Pakete können so leichter erkannt und analysiert werden. Es wird z. B. 00:00:19:2D:0D:35 in GATEWAY2 und ns1.earthlink.com wird zu MyDNS gewandelt.

Um einen MAC-Kennnamen zu erzeugen, rechtsklicken Sie auf das Paket und wählen dann im Popup-Menü **Quell-MAC verwenden** oder **Ziel-MAC verwenden**. Es erscheint ein Popup-Fenster, in dem das MAC-Adressenfeld schon ausgefüllt ist und Sie nur noch einen Kennnamen eingeben müssen. Sie können aber auch auf **Einstellungen => MAC Kennname ...** klicken und das Feld mit der MAC-Adresse und dem Kennnamen manuell ausfüllen. Um einen Kennnamen zu löschen bzw. die ganze Kennnamenliste zu löschen, rechtsklicken sie auf die Kennnamenliste und wählen dann **Datensatz löschen** bzw. **Alles löschen**. Die Erzeugung von IP-Kennnamen ist analog. Wenn durch einen Rechtsklick auf das Paket ein neuer IP-Kennname gewählt wird, ist das Kennnamenfeld mit dem entsprechenden Hostnamen vorausgefüllt (sofern vorhanden). Dieser kann dann vom Benutzer editiert werden.



Paketgenerator

Mit diesem Dialog können Sie Pakete über ihr Netzwerkadapter versenden bzw editieren. Um den Paketgenerator zu starten, klicken sie auf **Werkzeuge => Paketgenerator** oder wählen Sie ein Paket im **Register Pakete**, rechtsklicken Sie darauf und wählen dann den Befehl **Sende Paket(e)**.



Beachten Sie, dass der Paketgenerator sogenannte Application-layer-TCP-Streams nicht versenden kann und soll. Das bedeutet, er kann nicht zunehmende SEQ- oder ACK-Werte automatisch verarbeiten, die Checksummen oder Paketgrößen anpassen, usw. Wenn Sie einen TCP-Stream versenden wollen, benötigen Sie eine speziell für diesen Zweck entwickelte winsock-basierende Anwendung. Der Paketgenerator ist ein Tool zum Wiederabspielen von gesammelten Daten, zum Testen von Firewalls und Intrusion Detection-Systemen und für andere Aufgaben die manuelle Paketerzeugung benötigen.

Der Paketgenerator ermöglicht es die Paketinhalte zu ändern und das decodierte Paket im linken Fenster beim Editieren anzuzeigen. Sie können damit beliebige Pakete erzeugen und haben volle Kontrolle über die Paketinhalte. Bei IP-, TCP-, UDP- und ICMP-Paketen können Sie die Checksumme automatisch mit dem Button Sigma korrigieren. Um Sie bei der Paketbearbeitung zu unterstützen, ist zusätzlich das Werkzeug [Optischer Paketersteller](#) vorhanden. Klicken Sie auf den entsprechenden Button, um ihn aufzurufen.

Sie können auch auf den Pfeilbutton klicken um die Liste der erhältlichen Paketvorlagen zu sehen. Das Programm hat bereits **TCP-, UDP- und ICMP-Paketvorlagen**. Mit diesen Vorlagen sind Sie meist schneller als beim Eintippen von Hexcodes in das Editorfenster. Diese Vorlagen enthalten typische TCP-, UDP- und ICMP-Pakete. Sie können statt der vorgegebenen, auch eigene Vorlagen verwenden um einzelne Paketfelder selbst zu editieren bzw. Werte einzugeben die Ihren Ansprüchen genügen, wie MAC- und IP-Adressen, Portnummern, SEQ- und ACK-Nummern usw. Sie können ein Paket aus dem CommView-Paketbereich durch Drag&Drop in die Vorlagensektion des Paketgenerators ziehen. Wenn Sie mehrere Pakete in die Vorlagensektion einfügen wird nur das erste als Vorlage verwendet. In der Vorlagenliste wird nun der Eingangsname "Neue Vorlage" vorgegeben. Durch Rechtsklick auf eine neue Vorlage in der Liste können Sie diese mit **Umbenennen** neu benennen. Wenn Sie eine Vorlage löschen wollen, rechtsklicken Sie darauf und wählen dann **Löschen** im Kontextmenü. Die Auswahl einer Vorlage in der Liste öffnet sie im Editorfenster, wo sie vor dem Absenden verändert werden kann.

NCF-Dateien können mit den Vorlagen Ihrer Wahl im Anwendungsverzeichnis im Unterordner TEMPLATES abgelegt werden. Wenn CommView mindestens eine NCF-Datei im Unterverzeichnis Templates findet, wird die Vorlage in einer Dropdown-Liste zusammen mit den anderen Vorlagen angezeigt. Diese NCF-Dateien sollten nur ein Paket pro Datei enthalten, wenn Sie aber eine Datei mit mehreren Paketen öffnen, wird CommView nur das erste anzeigen.

Nach dem Editieren des Paketes können Sie mit den folgenden Befehlen die Pakete versenden:

Paketgröße – Ändert die Paketgröße.

Pakete/Sekunde – Beeinflusst die Paketsendegeschwindigkeit. Stellen Sie sicher, dass Sie nicht zu schnell Pakete versenden, wenn Sie eine langsame Verbindung haben. Wenn Sie z.B. ein 1000 Byte Paket 5000 mal pro Sekunde senden ist das mehr als eine 10MBit NIC handhaben kann.

Kontinuierlich – Hier sendet der Paketgenerator kontinuierlich Pakete, bis Sie Stop klicken.

Zeiten – Zur Vorgabe von Versendezeiten durch den Paketgenerator.

Senden/Stop – Betätigen Sie den Button, wenn Sie Pakete versenden bzw. den Versand stoppen wollen.

Arbeiten mit mehreren Paketen

Mit dem Paketgenerator können Sie mehrere Pakete auf einmal senden. Dazu wählen Sie die zu versendenden Pakete in der Liste, aktivieren den Paketgenerator durch das Kontextmenü oder ziehen mittels Drag&Drop die ausgewählten Pakete in das Paketgeneratorfenster. Sie können aber auch die gesammelten Dateien mit Drag&Drop in allen unterstützten Formaten in das Paketgeneratorfenster hineinziehen. Wenn mehrere Pakete versandt werden, werden der Packer-Editor und der Dekoder-Baum sichtbar.

Editierte Pakete speichern

Wenn Sie ein Paket bearbeiten und dann abspeichern möchten, ziehen Sie den Dekoder-Baum auf den Desktop oder auf ein beliebiges Verzeichnis. Es wird eine neue Datei im NCF-Format mit dem Paket erzeugt. Die Datei heißt stets PACKET.NCF. Sie können auch das Paket in das Vorlagenfenster ziehen. Wenn Sie mehrere Pakete bearbeiten wollen, sollten Sie diese nacheinander bearbeiten. Ziehen Sie jedes Mal dabei ein Paket auf den Desktop und benennen die Datei dann um. Danach öffnen Sie einen neuen Logbetrachter und verschieben (Drag&Drop) die bearbeiteten Pakete vom Desktop in den Logbetrachter. Anschliessend wählen Sie die Pakete mit der Taste [Shift] aus und rufen mittels Kontextmenü den Paketgenerator auf.

WARNUNG

1. Sie sollten den Paketgenerator nicht verwenden, bis Sie genau wissen, welchen Effekt Sie erreichen wollen. Das Senden von Paketen kann unvorhersehbare Ergebnisse mit sich bringen. Wir empfehlen daher dringend, dass Sie dieses Tool nur benutzen, wenn Sie ein erfahrener Netzwerkadministrator sind.
2. Wenn Sie dieses Tool einsetzen, sollte neben Ihrem eigenen PC noch mindestens ein weiterer, funktionierender PC an Ihrem LAN angeschlossen sein. Anderenfalls kann das Senden von Paketen Probleme verursachen.

Optischer Paketersteller

Der Optische Paketersteller ist ein Werkzeug zur leichteren Paketbearbeitung und –erstellung im [Paketgenerator](#). Dieses Werkzeug ermöglicht Ihnen, neue Pakete schnell und korrekt zu erstellen oder bestehende Pakete mit vorgefertigten Vorlagen zu modifizieren. Einmal erstellt oder bearbeitet, kann ein Paket mit dem [Paketgenerator](#) im Netzwerk in Umlauf gebracht werden.

The screenshot shows the 'Visual Packet Builder' application window. The 'Packet Type' is set to 'ICMP'. The 'Ethernet II' section shows source and destination MAC addresses as 00:50:00:BB:BB:BB and 00:50:00:AA:AA:AA. The 'IP' section is configured with source address 1.1.1.1, destination address 2.2.2.2, total length 92, and identification 0x1111. The 'ICMP [Echo Request]' section is set with type 8, code 0, ID 768, and sequence 256. The 'ICMP Data' section has a size of 64 bytes. The interface includes various dropdown menus, text boxes, and checkboxes for configuring different layers of the packet.

Standard TCP- UDP-, ICMP- (auf der 4. und 6. Version des IP-Protokolls basierend) und ARP-Paketgenerierung wird unterstützt. Zur Erstellung eines Paketes, wählen Sie den Typ aus dem Ausklappenü **Pakettyp**. Die Standardwerte der Paketfelder werden automatisch ausgefüllt, sie können aber nachträglich geändert werden.

ICMP-, TCP-, UDP- und ARP-Pakete beinhalten verschiedene verkapselte Ebenen und das Interface des Optischen Paketerstellers ist entsprechend aufgebaut. Optionen die zu einer entsprechenden Ebene gehören werden in einem separaten Feld angezeigt. Zum Beispiel, ein TCP-Paket beinhaltet 4 Ebenen, **QuellMAC-** und **ZielMAC-Adressfelder** angeordnet im **Ethernet II-Feld** (Datenverbindungsebene) und **Src Port-** und **Dst Port-Werte** werden im TCP-Feld (Transportebene) angezeigt. Falls Sie ein Feld ausblenden möchten, klicken Sie auf den in der rechten Ecke des Feldkopfes angeordneten Button **Aus-/Einklappen**.

Beachten Sie, dass einige „Parental“ Ebenenwerte die Pakete auf tiefere Ebenen bewegen; daher kann die Modifizierung höherer Ebenen zur Erneuerung von unteren Ebenen eines Paketes führen. Deshalb führt eine Änderung des **Protkolltyps** im **Ethernet II-Feld** (Datenverbindungsebene) zur Erneuerung des gesamten Paketes. Eine andere Besonderheit die Sie beachten sollten, ist, dass die Werte einiger Felder abhängig vom Inhalt anderer Felder sind, ebenso wie der Dateninhalt tieferer Ebenen. Solche Felder sind: Checksummen und Kopflängen und/oder Daten der unteren Ebenen. Der Optische Paketersteller kalkuliert solche Werte automatisch. Immer wenn Sie ein nichtstandardisiertes Paket erstellen, können Sie verschiedene Werte manuell bestimmen, indem Sie die Checkbox **Standardwerte überschreiben** aktivieren und die gewünschten Werte festlegen.

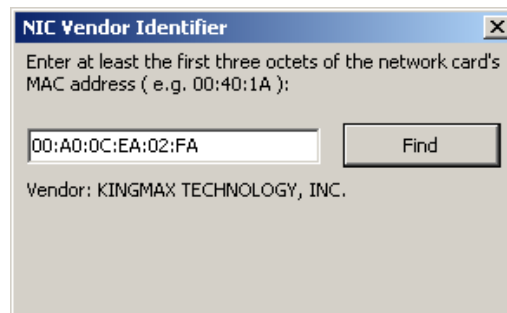
Hinweis. Der Optische Ersteller hilft Ihnen die Korrektheit der erstellten Pakete, durch eine rote Hervorhebung der Köpfe und Felder, mit unkorrekten oder nichtstandardisierten Werten zu kontrollieren.

Trotz der Tatsache, dass der Optische Paketersteller nur interne Unterstützung für die TCP-, UDP-, ICMP- und ARP-Protokolle besitzt, können Sie doch Pakete damit bearbeiten, die andere Protokolle benutzen. Für solche Pakete können Sie den Hex-Editor zur Bearbeitung nutzen.

Ist ein Paket einmal erstellt, kann es gespeichert und anschließend wieder in den Optischen Paketersteller geladen werden. Benutzen Sie die jeweiligen Befehle aus dem Menü **Datei** des Optischen Paketerstellers zum Laden/Speichern der erfassten Dateien. Sie können jede mit CommView erfasste Datei (NCF) laden; immer wenn die Datei mehr als ein Paket enthält, wird nur das erste Paket geladen.

NIC Vendor (Hersteller) Identifier (Identifiziertool)

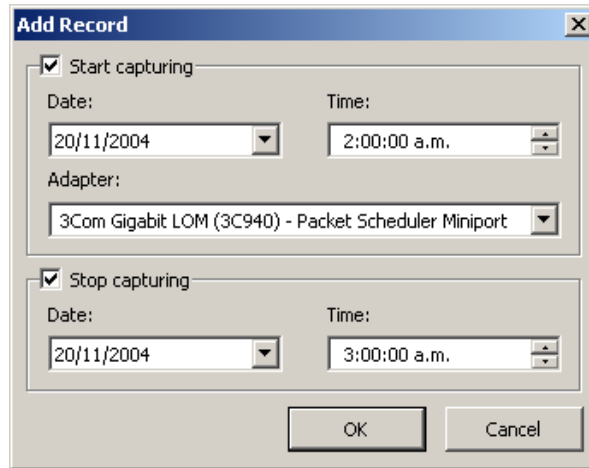
Die ersten 24 Bit der MAC-Adresse einer Netzwerkkarte identifizieren klar den Hersteller. Diese 24-Bit-Nummer wird OUI (Organizationally Unique Identifier) genannt. Der NIC-Hersteller-Identifier ist ein Werkzeug, das Ihnen ermöglicht, den Hersteller über die MAC-Adresse zu ermitteln. Um einen Hersteller zu finden, klicken Sie auf **Werkzeuge => NIC-Herstelleridentifikation**. Geben Sie eine MAC-Adresse ein und klicken Sie auf **[Finde]**. Sie sehen dann den Namen des Herstellers. Standardmässig ersetzt CommView die ersten drei Oktets der MAC-Adresse durch den Herstellernamen der Netzwerkkarte im Register **Pakete**. Dieses Verhalten kann unter **Einstellungen => Allgemein** durch deaktivieren der Checkbox **Herstellernamen in MAC-Adressen anzeigen** geändert werden.



Die Herstellerliste ist in der Datei MACS.TXT im CommView-Anwendungsverzeichnis enthalten und kann manuell verändert werden. Sie können diese Liste manuell bearbeiten um Informationen hinzuzufügen oder zu modifizieren.

Scheduler

Mit diesem Dialog können Sie zeitgesteuerte Aufgaben erzeugen und editieren. Dies ist sinnvoll, wenn CommView den Empfang selbstständig zu einem bestimmten Zeitpunkt aktivieren bzw. deaktivieren soll, z. B. nachts oder am Wochenende. Eine neue Aufgabe fügen Sie mittels klicken auf **Werkzeuge => Paketerfassungsplaner** hinzu, dann klicken Sie auf den Button **[Hinzufügen]**.



Im Bereich **Paketerfassung starten** können Sie das Datum und die Uhrzeit festlegen, wann CommView den Empfang starten soll. Mit der Dropdown-Liste **Adapter** wählen Sie den zu benutzenden Adapter. Im Bereich **Paketerfassung stoppen** kann festgelegt werden, wann CommView den Empfang beendet. Die Checkboxen **Paketerfassung starten** und **Paketerfassung stoppen** müssen nicht gleichzeitig aktiviert sein. Wenn nur die erste Checkbox aktiv ist, findet der Empfang bis zum manuellen Abbruch statt. Sie müssen zwar manuell starten, wenn nur die zweite Box aktiv ist, CommView stoppt dann aber automatisch zum angegebenen Zeitpunkt.

Wenn CommView schon Pakete empfängt und gleichzeitig ein anderer Adapter programmiert ist, bricht CommView den Empfang ab, wechselt zum neuen Adapter und beginnt den Empfang erneut.

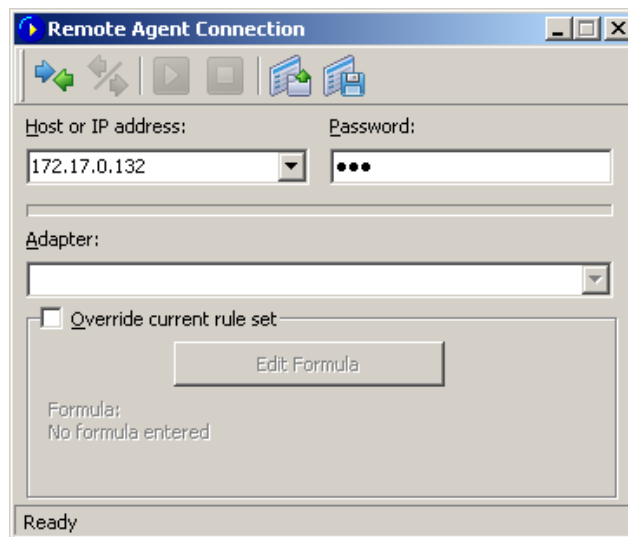
Achtung: Zeitgesteuerte Aufgaben können nur durchgeführt werden, wenn CommView aktiv ist.

Der Einsatz des Remote Agent

CommView Remote Agent ist ein Begleitprodukt, das es erlaubt Netzwerkverkehr "aus der Ferne" zu erfassen. Zu diesem Zweck müssen Sie den Remote Agent auf dem Zielcomputer installieren und anschliessend von Ihrem lokalen Computer eine Verbindung zum Remote Agent des Zielcomputer herstellen. Wenn Sie die Verbindung hergestellt und sich authentifiziert haben, können Sie den Paketverkehr auf dem Zielcomputer erfassen als ob die Erfassung auf Ihrem lokalen Computer stattfinden würde.

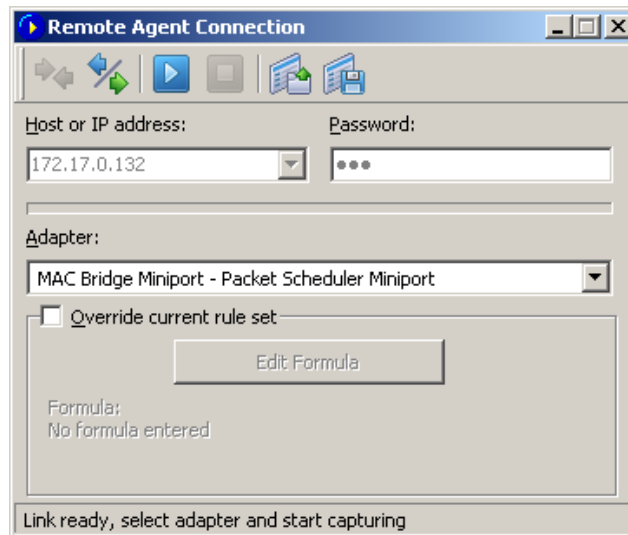
WICHTIG. Dieses Kapitel beschreibt, wie man mit CommView unter Verwendung des Remote Agent Pakete von einem Zielcomputer erfassen kann. Für detaillierte Informationen über die Installation und Konfiguration des Remote Agent, konsultieren Sie bitte die Benutzeranleitung des Remote Agent. Wir empfehlen Ihnen die Benutzeranleitung des Remote Agent sorgfältig zu studieren, bevor Sie diesen benutzen. Der CommView Remote Agent kann von unserer [Webseite](#) heruntergeladen werden.

Um auf den Remote-Erfassungs-Modus umzuschalten klicken Sie auf **Datei => Remote Monitoring Modus**. Eine weitere Werkzeugleiste im Hauptfenster wird eingeblendet. Wenn Sie sich hinter einer Firewall oder einem Proxy-Server befinden oder einen nicht üblichen Remote Agent-Port verwenden, klicken Sie auf den Button **[Erweiterte Netzwerkeinstellungen]** und passen Sie die Portnummer und/oder die SOCKS5 Proxy-Server-Einstellungen an.

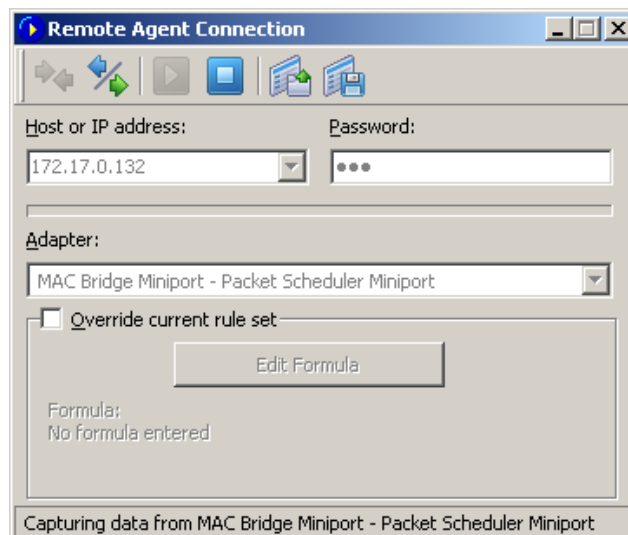


Klicken Sie auf den Button **[Neue Remote Agent Verbindung]** um eine neue Verbindung zu definieren oder klicken Sie auf den Button **[Remote Agent Profil laden]** um ein bereits vorhandenes Verbindungsprofil zu verwenden. Ein bestehendes Verbindungsprofil kann auch aus dem Dialog Neue Remote Agent Verbindung geladen werden.

Geben Sie in das eingeblendete Verbindungsfenster Remote Agent die IP-Adresse des Computers auf welchem der Remote Agent läuft und das entsprechende Passwort ein. Klicken Sie anschließend auf **[Verbinden]**. Ist das Passwort korrekt wird eine Verbindung hergestellt. Sie werden dann eine Link Ready-Nachricht sehen und die Netzwerkadapterliste wird alle Adapter des Zielcomputers enthalten.



Es ist nun der beste Moment um die Regeln im Dialog **Regeln** festzulegen. Es ist sehr wichtig Regeln korrekt zu definieren, sodass das Verkehrsvolumen zwischen CommView und dem Remote Agent, das Bandbreitenlimit auf beiden Seiten der Verbindung nicht überschreitet, da sonst grössere Verzögerungen auftreten können. Seien Sie sicher, überflüssige Pakete auszufiltern (lesen Sie mehr weiter unten über diese Thematik). Sie können ebenso ein Set von Erfassungsregeln auf diese Verbindung übernehmen und die in CommView definierten Regeln überschreiben. Aktivieren Sie dazu die Checkbox **Aktuelle Regeln überschreiben**, klicken auf den Button **[Formel editieren]** und geben die Formel im nachfolgenden Feld ein. Wenn Sie zur Paketerfassung bereit sind, klicken Sie auf **[Paketerfassung starten]**. Die Syntax der Regeln ist dieselbe wie bei den [Erweiterten Regeln](#). Wenn Sie zur Erfassung bereit sind, wählen Sie den Netzwerkadapter aus der Liste und klicken Sie auf den Button **[Paketerfassung starten]**. CommView erlaubt Ihnen die Remote Agent-Verbindungseinstellungen für einen späteren leichten und schnellen Zugriff als Profil zu speichern. Klicken Sie auf den Button [Remote Agent-Profil speichern] im Dialog **Neues Remote Agent-Verbindung** und geben Sie eine Bezeichnung für die Datei ein.



CommView wird die Paketdaten des Zielcomputers erfassen als ob die Erfassung auf Ihrem Computer lokal stattfinden würde. Für den Benutzer erscheint kein Unterschied zwischen der lokalen und der remote Paketerfassung. Wenn Sie die Erfassung stoppen möchten klicken Sie auf **[Paketerfassung stoppen]**. Dann können Sie entweder einen anderen Adapter wählen oder die Verbindung zum Remote Agent durch Klicken auf **[Unterbrechen]** stoppen. Um zum Modus für die lokale Paketerfassung zurück zu kehren, klicken Sie auf **Datei => Remote Monitoring Modus**. Die zusätzliche Remote Agent-Werkzeugleiste wird ausgeblendet.

Beachten Sie, dass CommView mit mehreren Remote Agents in verschiedenen Netzwerksegmenten gleichzeitig arbeiten kann. Jede der Remote Agent-Verbindungen kann innerhalb einer CommView-Instanz ihr eigenes Verbindungsprofil und damit ihre eigenen Regeln und Einstellungen haben.

RPCAP anwenden

Wichtig. Dieses Kapitel beschreibt eine experimentelle Funktionalität, die wie erwartet funktionieren kann oder auch nicht; dies hängt von der konkreten Implementierung in die Soft- und Hardware von Drittherstellern ab. Für diese Funktionalität wird keine Unterstützung angeboten.

Zusätzlich zur Funktionalität der Daten-Fernerfassung, die [CommView Remote Agent](#) anbietet, kann CommView mithilfe des RPCAP auch den Netzwerkverkehr entfernter Computer erfassen. Dieses Protokoll wird von Hardware (z.B. Aerohive Access Points) und Software (z.B. WinPcap) unterstützt.

Um den Fernbeobachtungsmodus einzuschalten, wählen Sie **Datei => Fernbeobachtungsmodus**. Es erscheint eine zusätzliche Werkzeugleiste neben der Hauptwerkzeugleiste im Hauptfenster von CommView. Klicken Sie auf **[Neue RPCAP-Verbindung]**, um ein Fenster für die neue Verbindung zu öffnen.

Um sich mit einem Ferngerät zu vernetzen, geben Sie dessen **Hostnamen oder IP-Adresse** ein, bestimmen Sie die **Port-Nummer** (standardmäßig verwendet RPCAP Port 2002), aktivieren Sie die Checkbox „**Benutzer-Authentifikation**“, geben Sie **Benutzer-ID** und **Passwort** ein, falls eine Authentifikation erforderlich ist, dann aktivieren Sie die Checkbox „**Vermischter Modus**“, falls dies der Erfassungsmodus ist, den Sie benutzen möchten. Klicken Sie auf **[Verbinden]**, um die Verbindung aufzubauen. Wenn die Verbindung aufgebaut ist, zeigt die Dropdown-Liste **Adapter** die optionalen Schnittstellen. Um die Datenerfassung zu starten, klicken Sie auf **[Paketerfassung starten]**.

Entschlüsselten SSL-Datenverkehr erfassen

Neben physischen und virtuellen Netzwerkadaptern können Sie in CommView einen der "**Entschlüsselten SSL**"-Adapter zum Erfassen und Entschlüsseln des lokalen SSL-Verkehrs auswählen. Dies sind keine echten Adapter. Vielmehr werden sie der Einfachheit halber emuliert und als "Adapter" bezeichnet. Wenn Sie entschlüsselten lokalen SSL-Verkehr von diesen Adaptern erfassen, emuliert CommView TCP-Pakete mithilfe abgefangener SSL-Sitzungen. Infolgedessen können Sie mit diesen Paketen genauso arbeiten, wie Sie es normalerweise mit anderen Paketen von echten Adaptern tun würden.

Beachten Sie beim Arbeiten mit entschlüsseltem SSL-Verkehr Folgendes:

- **Nur lokaler SSL-Verkehr** kann entschlüsselt werden. Mit anderen Worten, CommView (oder eine andere Software) kann den verschlüsselten Datenverkehr anderer Computer nicht entschlüsseln. Wenn dies möglich wäre, hätten wir wahrscheinlich eine Auszeichnung in Höhe von mehreren Millionen Dollar für den größten Durchbruch in der Kryptografie erhalten.
- Es wird dringend empfohlen, dass Sie **Ihre Browser schließen**, bevor Sie mit der Erfassung des SSL-Datenverkehrs beginnen, **und diese öffnen, nachdem Sie mit der Erfassung begonnen haben**. Dies ist erforderlich, um sicherzustellen, dass die Browser ihre Liste vertrauenswürdiger Zertifikate aktualisieren können. CommView fügt sein Zertifikat dem vertrauenswürdigen Speicher hinzu und ermöglicht damit das Abfangen und Entschlüsseln von SSL-Verkehr.
- Wir können nicht garantieren, dass CommView jede SSL-Sitzung entschlüsseln kann, die von Ihrem Computer stammt. Einige Anwendungen verwenden stark angepasste Komponenten für die SSL-Verschlüsselung. Wir haben jedoch sichergestellt, dass **alle modernen gängigen Browser unterstützt werden**.
- Sobald Sie mit der Erfassung begonnen haben, beschwerten sich einige Anwendungen möglicherweise über ein "**unbekanntes**" oder "**nicht vertrauenswürdiges**" **SSL-Zertifikat**. Dies ist normal, da CommView als Vermittler zwischen der auf Ihrem Computer ausgeführten Software und dem Server fungiert, mit dem es verbunden ist. Dies beinhaltet das vorübergehende Ersetzen des Serverzertifikats durch das CommView-eigene Zertifikat (nur wenn CommView Daten erfasst). Wenn eine solche Meldung "Unbekanntes Zertifikat" angezeigt wird, starten Sie die betreffende Anwendung einfach neu. Dies sollte das Problem in den meisten Fällen lösen. Wenn dies nicht hilft, können Sie das CommView-Zertifikat zum vertrauenswürdigen Zertifikatspeicher der Anwendung hinzufügen, falls vorhanden. Das Zertifikat finden Sie unter *C:\Programme (x86)\CommView\certs\SSL\CommView CA 2.cer* (für 64-Bit-Windows) oder *C:\Programme\CommView\certs\SSL\CommView CA 2.cer* (für 32-Bit-Windows). Wenn dies auch nicht hilft, können wir leider nichts tun.
- Die TCP-/IP-Pakete, die Sie in diesem Erfassungsmodus sehen, werden emuliert. Dies bedeutet, dass sie über **künstliche Ethernet-, IP- und TCP-Header** verfügen. Solche Pakete haben spezifische Quell- und Ziel-MAC-Adressen: 00: 00: 00: 00: 10 und 00: 00: 00: 00: 20 für eingehende Pakete und umgekehrt für ausgehende Pakete. Sie haben auch emulierte SEQ- und ACK-Werte.
- Da Pakete emuliert werden, **zeigen sie möglicherweise nicht vollständig die Struktur der realen SSL-Sitzung**. Beispielsweise kann eine an Ihren Browser gesendete SSL-verschlüsselte Webseite mit einer Länge von 10.000 Byte in der Realität mit 7 oder 8 verschlüsselten TCP-Paketen übertragen werden. In CommView wird die gesamte Seite jedoch möglicherweise als ein einziges TCP- Paket mit einer Länge von 10.000 Byte dargestellt, das entschlüsselte Daten enthält. Ebenso werden SSL-Sitzungshandshakes nicht angezeigt, da sie keine nutzbare Nutzlast enthalten.

Es stehen drei Arten von entschlüsselten SSL-emulierten Adaptern zur Auswahl:

1. **Local SSL (Decrypted)**
2. **Local SSL (Decrypted) + HTTP**
3. **Local SSL (Decrypted) + TCP**

Die erste Art erfasst nur SSL-Sitzungen. Die zweite Art erfasst SSL-Sitzungen und HTTP-Sitzungen (unverschlüsselt). Die dritte Art erfasst SSL-Sitzungen und alle anderen TCP-Sitzungen. Bitte beachten Sie, dass in allen drei Modi emulierte TCP-Sitzungen mit den oben beschriebenen Besonderheiten vorhanden sind. Wenn Sie ursprüngliche, unveränderte Pakete sehen möchten, die von Ihrem Netzwerkadapter gesendet / empfangen wurden, wählen Sie diesen Adapter anstelle einen der emulierten Adapter in CommView aus.

Loopback Datentransfer erfassen

CommView erlaubt die Datentransfererfassung von sog. Loopback-Verbindungen. Zum Start der Überwachung des Loopback-Interfaces, wählen Sie dieses aus der Drop-down-Liste in der Werkzeugleiste.

Loopback Pakete werden vom selben Computer gesandt und empfangen, wie z.B. an sich selbst adressierte Pakete. Auf einem PC im Normalbetrieb bestehen in der Regel keine Loopback-Verbindungen. Es ist jedoch unter Entwicklern üblich Loopback-Verbindungen zum Testen von Netzwerkanwendungen zu verwenden. Daher sind Entwickler die primäre Zielgruppe für die Erfassung von Loopback-Datenpaketen.

Pakete die von einer Loopback-Verbindung erfasst werden, sehen genau gleich aus wie jene die von irgendeinem anderen Host gesandt werden. Ein Unterschied besteht darin, dass die Checksumme nicht verarbeitet wird. Bitte beachten Sie folgende Punkte, wenn Sie Pakete von Loopback-Verbindungen erfassen:

- CommView erfasst Loopback-Verkehr von allen lokalen IP-Adressen. Dies schließt immer die Adressen 127.0.0.1/255.0.0.0 ein, sowie die IP-Adressen der lokalen Ethernet-Adapter, z.B. 192.168.0.1.
- ICMP-Pakete können nicht erfasst werden. Andere Protokolle (TCP, UDP, usw.) sind möglich.
- Nur erfolgreich gesendete/empfangene Pakete werden erfasst. Wenn z.B. ein Verbindungsversuch scheitert, werden Sie keine SYN-/RST-Pakete sehen.
- Sitzungen werden still geschlossen, d.h. es werden keine FIN-Pakete erfasst.

Port Referenz

Dieses Fenster zeigt eine Port-Nummertabelle und die zugehörigen Servicenamen. Dieser Bezug wird aus der Datei SERVICES erhalten, die von Windows installiert wurde. Sie finden die Datei im Verzeichnis \system32\drivers\etc. Sie können diese Datei manuell editieren, wenn sie mehr Portnummern/Services hinzufügen möchten. CommView liest diese Datei beim Programmstart, so dass Ihre Änderungen erst nach einem Neustart des Programms aktiv werden.

Einstellungen

Sie können einige Programmeinstellungen im Menü **Einstellungen** konfigurieren.

Allgemein

Autostart-Paketerfassung – Aktivieren Sie diese Checkbox, wenn CommView sofort nach dem Programmstart mit dem Empfang von Paketen beginnen soll. Wenn Sie mehrere Netzwerkadapter in Ihrem Computer haben, sollten Sie aus der Drop-Down-Liste einen entsprechenden Adapter auswählen.

Netzwerk

Keine DNS/Auflösung – Mit dieser Checkbox verhindern Sie, dass CommView "reverse DNS lookups" der IP-Adressen durchführt. Wenn die Checkbox aktiviert ist bleibt die Spalte **Hostname** im Register **Letzte IP Verbindungen** leer.

Portnummern in Servicenamen konvertieren – Aktivieren Sie diese Checkbox, wenn CommView Servicenamen statt Nummern anzeigen soll. Wenn die Checkbox aktiviert ist, wird z. B. Port **21** als **ftp** und Port **23** als **telnet** angezeigt. Über die von Windows installierte SERVICES-Datei wandelt das Programm die numerischen Werte in Servicenamen um. Sie finden die Datei im Verzeichnis `\system32\drivers\etc`. Sie können diese Datei manuell editieren, wenn sie mehr Portnummern/Services hinzufügen möchten.

MAC-Adressen in Kennnamen konvertieren – Wandelt im Register **Pakete** MAC/Adressen in Kennnamen um. [Kennnamen](#) können über das Menü **Einstellungen => MAC Kennnamen** MAC-Adressen zugeordnet werden.

IP-Adressen in Kennnamen konvertieren – Wandelt in den Registern **Pakete** und **Statistiken** IP-Adressen in Kennnamen um. [Kennnamen](#) können über das Menü **Einstellungen => IP Kennname** IP-Adressen zugeordnet werden.

IP-Adressen im Register Pakete in Hostnamen konvertieren – Wählen Sie diese Checkbox, wenn CommView aufgelöste Hostnamen statt IP-Adressen im Register Pakete anzeigen soll. Wenn diese Checkbox aktiv ist, versucht CommView zuerst einen Kennnamen für die genannte IP-Adresse zu finden. Wenn kein Kennname gefunden wird oder die vorhergehende Checkbox **IP-Adressen in Kennnamen konvertieren** nicht aktiviert wurde, wird CommView den internen DNS-Cache nach einem Hostnamen absuchen. Wenn kein Hostname gefunden wird, wird die IP-Adresse in numerischer Form dargestellt.

Herstellernamen in MAC-Adressen anzeigen – CommView ersetzt standardmäßig im Register Pakete die ersten drei Oktets der MAC-Adresse durch den Adapterherstellernamen. Wenn Sie dies nicht wünschen müssen Sie die Checkbox deaktivieren.

Kein Promiscuous Modus – grundsätzlich versetzt CommView die Netzwerkkarte in den sogenannten Promiscuous-Modus, was zur Folge hat, dass der gesamte Paketverkehr des lokalen LAN-Segmentes von der Netzwerkkarte erfasst wird. Durch das Setzen diese Checkbox wird das Umschalten in den Promiscuous-Modus unterlassen, wodurch die Netzwerkkarte in ihrem normalen Betriebsmodus belassen wird. Dies kann z. B. von Nutzen sein, wenn die IT-Vorschriften der Firma den Einsatz von Netzwerkmonitoren im Promiscuous-Modus nicht erlauben, Sie die CPU-Ressourcen nicht zu stark belasten wollen oder Sie nur am ein- und ausgehenden Paketverkehr Ihres PC's interessiert sind und nicht den durchgehenden Paketverkehr herausfiltern wollen.

Benachrichtigen bei Veränderung der Adapterliste – verändert sich die Liste der aktiven Adapter, wird bei gesetzter Checkbox im Systemleistenbereich eine Nachricht eingeblendet.

Prozesspfad in voller Länge anzeigen – Aktivieren Sie diese Checkbox wenn der Pfad des lokalen Prozesses der die Pakete der im Register **Letzte IP-Verbindungen** gezeigten Verbindung sendet/empfängt in voller Länge angezeigt werden soll. Dies gilt auch für die Baumansicht der decodierten Pakete im **Register** Pakete (z.B. C:\Files\Program.exe ist der Pfad in voller Länge, wogegen Program.exe nur die ausführbare Datei benennt).

Freundliche Adapternamen anzeigen – aktivieren Sie diese Checkbox wenn für die Anzeige der Adapter in der Drop-Down-Liste die Namen aus der Windows-Seite der Netzwerkverbindungen verwendet werden sollen.

Rasterlinien einblenden – Blendet in allen Paketlisten Rasterlinien ein.

Speicherauslastung

Anzeige

Maximale Anzahl Pakete im Puffer – Definiert die maximale Anzahl von Paketen, die das Programm im Speicher haben kann und zeigt die Paketliste (Zweites Register). Sie können z. B. den Wert auf 3000 setzen. Dann werden nur die letzten 3000 Pakete im Speicher bzw. in der Paketliste berücksichtigt. Je höher dieser Wert ist, desto mehr Computerressourcen benötigt das Programm.

Beachten Sie, wenn Sie Zugang zu sehr vielen Paketen benötigen, dass Sie die Autospeicherungsfunktion nutzen (mehr dazu unter [Protokollierung](#)). Damit können Sie alle Pakete in einer Logdatei auf der Festplatte ablegen.

Maximale Anzahl Zeilen der aktuellen IP-Verbindungen – Legt die Anzahl der Zeilen zur Anzeige der aktuellen IP-Verbindungen fest. Wenn die Anzahl der Verbindungen den Schwellenwert überschreitet, werden die Verbindungen die am längsten nicht aktiv waren aus der Liste entfernt.

Treiber-Puffer – definiert die Treiberpuffergröße. Diese Einstellung beeinflusst die Performance des Programms. Je mehr Speicher für den Treiberpuffer reserviert ist, desto weniger Pakete verliert das Programm. Für LAN's mit geringem Verkehr und Wählverbindungen ist die Puffergröße nicht wichtig. Für LAN's mit hohem Verkehr sollten Sie jedoch die Puffergröße erhöhen, wenn das Programm zu viele Pakete verliert. Die Anzahl der verlorenen Pakete ermitteln Sie mittels **Datei => Durchsatzdaten** wenn die Paketerfassung aktiviert ist.

Aktuelle IP-Verbindungen

Logik anzeigen – Ermöglicht die Auswahl des Layouts der aktuellen IP-Verbindungen an Ihre Bedürfnisse anzupassen. Mit der Auswahl eines Objektes aus der Dropdown-Liste wird die ausgewählte Logik angezeigt. Meistens empfiehlt sich die Verwendung der standardmäßigen Smart-Logik.

Lokale IP-Adressen definieren – Dieses Tool sollten Sie verwenden, wenn Sie LAN-Verkehr beobachten, der viele Pass-through-Pakete und eine Mischung aus internen und externen IP-Adressen enthält. In solch einer Situation weiß CommView nicht, welche IP-Adressen als lokale Adressen definiert werden sollen und könnte dann die IP-Adressen in den Lokal- und Remote- IP-Spalten vertauschen. Mit diesem Werkzeug definieren Sie die lokalen Netzwerkadressen und Subnet-Masken, um sicher zu sein, dass die aktuellen IP-Verbindungen richtig angezeigt werden. Dies funktioniert jedoch nur mit der standardmäßigen **Smart-Logik**.

Prozessnamen um PID-Nummer erweitern – aktivieren Sie diese Checkbox, wenn in der Prozessspalte die sogenannte Prozess-ID direkt neben dem Prozessnamen angezeigt werden soll.

Farben

Paketfarbe – definiert die Farbe der Pakete im Register Pakete in Abhängigkeit ihrer Richtung (ausgehend, ankommend oder durchgehen). Um die Farbe zu ändern wählen Sie eine Richtung aus der Drop-Down-Liste und klicken Sie auf die Farbe Ihrer Wahl.

Paket-Header einfärben – Aktivieren Sie diese Checkbox, wenn CommView Paketinhalte einfärben soll. Wenn diese Checkbox aktiv ist, zeigt das Programm die ersten acht Paketschichten mit verschiedenen Farben an. Zum Ändern einer Farbe wählen Sie die zu ändernde Header-Art und klicken dann auf das farbige Rechteck.

Formelsyntax hervorheben – Definiert die Farben zum Hervorheben der Schlüsselwörter in den Formeln für die [Erweiterte Regeln](#).

Ausgewählte Bytesequenzfarbe – Definiert den Font und die Hintergrundfarbe für die Darstellung der Bytesequenz, die im Decoderbaum gewählt wurde. Wählen Sie z. B. den TCP-Baumknoten, werden die entsprechenden Teile des Pakets mit diesen Farben hervorgehoben.

Decodierung

Inhalt aller Knoten im Decoderfenster anzeigen – Aktivieren sie diese Checkbox, um alle Knoten im Decoderfenster automatisch geöffnet darzustellen, wenn Sie ein neues Paket in der Paketliste wählen.

Letzten Knoten ausklappen – Aktivieren Sie diese Checkbox, wenn Sie möchten, dass der letzte Knoten im Dekoderfenster automatisch ausgeklappt wird, wenn Sie ein Paket in der Paketliste auswählen. Standardmäßig wird der erste Knoten ausgeklappt. Diese Einstellung ist wirkungslos, wenn die Checkbox **Immer alle Knoten ausklappen** im Dekoderfenster aktiviert ist.

Ebene ausklappen – Bestimmen Sie die Anzahl der Ebenen, die Sie ausklappen möchten.

Für ASCII-Export nur bis zur ersten Ebene decodieren – Diese Option beeinflusst das Decodierformat für den Export eines Paketlogs bzw. eines individuellen Paketes als ASCII-Datei mit Decodierung. Wenn diese Checkbox aktiv ist, werden nur die Toplevel-Knoten abgespeichert. Wenn Sie z. B. ein TCP/IP-Paket speichern möchten, während diese Funktion deaktiviert ist, werden alle *Arten von Service-Sub-Knoten* auch gespeichert. Wenn die Option aktiv ist, werden die Sub-Knoten nicht mitgespeichert. Damit wird die Ausgabe der ASCII-Dateien weniger detailliert und kompakter.

Falsche Prüfsummen für die TCP-Sitzungsrekonstruktion ignorieren – Hiermit beeinflussen Sie, wie CommView mit schadhafte TCP/IP-Paketen umgeht, wenn das Programm TCP-Sitzungen rekonstruiert. Diese Option ist per Default aktiviert d.h. auch Pakete mit falscher Prüfsumme werden in der Rekonstruktion berücksichtigt und angezeigt. Schalten Sie die Option aus wenn Sie wollen das Pakete mit falscher Prüfsumme in der Rekonstruktion nicht berücksichtigt werden. Achtung Gigabit Kartenbenutzer: Alle ausgehenden Pakete haben eine falsche Prüfsumme, wenn die Option Checksum Offload aktiv ist! Sie sehen dann in der Rekonstruktion nur einen Teil der beteiligten Pakete. Das gilt auch für die Rekonstruktion von Loopback-Verbindungen, da Loopback-Pakete Null-Checksummen haben.

Paketnummern einbinden bei TCP-Sitzungsrekonstruktion – Aktivieren Sie diese Checkbox, wenn Sie möchten, dass die Dateneinheiten im TCP-Sitzungsrekonstruktionsfenster mit zugehörigen, vorangestellten Paketnummern dargestellt werden.

Bei TCP-Sitzungsrekonstruktion nach dem Sitzungsstart suchen – Wenn diese Checkbox angekreuzt ist, wird das Programm versuchen, den Beginn der TCP-Sitzung zu finden, wenn Sie die Sitzung rekonstruieren. Ist die Checkbox nicht aktiviert, wird die Sitzung von dem gewählten Paket ausgehend rekonstruiert, d.h. früher Pakete werden verworfen.

GZIP-Inhalt entpacken – Aktivieren Sie diese Checkbox damit CommView GZIP-komprimierten HTTP-Inhalt in lesbaren Text innerhalb des TCP-Sitzungsrekonstruktionsfenster darstellt. GZIP-Inhalt wird nur dekomprimiert, wenn der Anzeigetyp im Fenster auf ASCII gesetzt ist.

Bilder rekonstruieren – Aktivieren Sie diese Checkbox, wenn CommView binäre HTTP-Streams, die Bilder darstellen, in betrachtungsfähige JPG-, BMP-, PNG- und GIF-Bilder im TCP-Sitzungsrekonstruktionsfenster verwandeln soll. Bilder werden nur angezeigt, wenn der Anzeigetyp im Fenster auf HTML gesetzt ist. Bilder werden nie innerhalb der HTML-Seite angezeigt zu der sie gehören, sie werden durch den Server über eine separate HTTP-Sitzung transportiert.

IPv4-Formendungen in IPv6-Adressen verwenden – Wenn diese Checkbox nicht angekreuzt ist, werden IPv6-Adressen nur in hexadezimaler Schreibweise dargestellt, z.B. fe80::02c0:26ff:fe2d:edb5. Ist die Checkbox angekreuzt, werden die letzten 4 Byte der IPv6-Adressen in der IPv4-Darstellungsart angezeigt, z.B. fe80::02c0:26ff:254.45.237.181.

Fragmentierte IP-Paket wieder zusammensetzen – Kreuzen Sie diese Checkbox an, wenn das Programm fragmentierte IP-Pakets wieder zusammensetzen soll. Standardmäßig werden fragmentierte IP-Pakete angezeigt, wie Sie empfangen wurden, in ihrer Originalform. Ist diese Option eingeschaltet, wird das Programm einen internen Fragmentpuffer erhalten und versuchen, die Fragmente zusammenzufügen. Dabei werden nur erfolgreich zusammengesetzte Fragmente als Ergebnis angezeigt.

Versuche eingehende UDP-Pakete Arbeitsabläufen zuzuordnen – Standardmäßig versucht das Paket-zu-Applikation-Zuordnungssystem des Programms keine eingehenden UPD-Pakete in einem eigenen Arbeitsablauf zuzuordnen, infolge der wahrscheinlichkeitstheoretischen Beschaffenheit solcher Zuordnungen. Kreuzen Sie die Checkbox an, wenn Sie möchten, dass das Programm versucht diese Pakete zuzuordnen.

Standard Anzeigetyp – Wählen Sie aus der Dropdown-Liste den Anzeigetyp, den Sie als Standard für die TCP-Sitzungsrekonstruktion setzen wollen. Erlaubte Werte sind ASCII, HEX, HTML und EBCDIC.

HINWEIS: Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

VoIP-Analyse deaktivieren – Deaktivierung der Erfassung und Analyse von VoIP-Daten. Aktivieren Sie diese Checkbox wenn Sie nicht mit VoIP arbeiten und wenn Sie die Benutzung der Computerressourcen durch die Applikation minimieren möchten.

Maximale Aufzeichnungen in der Liste – Begrenzt die Anzahl der angezeigten und verarbeiteten VoIP-Vorgänge. Wenn die Anzahl der Aufzeichnungen die festgelegte Begrenzung übersteigt, werden ältere Aufzeichnungen aus der Liste gelöscht.

Verwaiste RTP-Ströme ignorieren – Wenn diese Checkbox aktiviert ist, ignoriert der VoIP-Analyser RTP-Datenströme die keine Ausgangssignalsitzung haben. Verwaiste RTP-Ströme entstehen typischerweise wenn die Paketerfassung in der Mitte eines Telefonates gestartet wird oder das Signalprotokoll der Applikation unbekannt ist (z.B. kein SIP oder H.323) oder das Signalprotokoll wurde in einer nichtstandardisierten Art und Weise gesendet (z.B. verschlüsselt oder als Teil einiger anderer Sitzungen). Solche Ströme sind immer noch zur Analyse verfügbar und manchmal zur Wiedergabe. Schauen Sie bitte in das Kapitel [Telefonate wiedergeben](#) um detaillierte Informationen über die Wiedergabe von Telefonaten zu erhalten. Deaktivieren Sie diese Option, wenn Sie kein Interesse an solchen verwaisten Strömen haben und Computerressourcen sparen möchten. Beachten Sie, wenn verwaiste Ströme nicht ignoriert werden kann der VoIP-Analyser über das UDP-Protokoll übertragene Ströme irrtümlicherweise als RTP-Ströme identifizieren. Allgemein ist dies kein Fehler, weil RTP-Pakete keine standardisierte einheitliche Signatur besitzen, deshalb sind solche "Falschpositiven Ergebnisse" in Ordnung.

Geo-Standort

Geo-Standort ist die Länderzuordnung für IP-Adressen. Wenn diese Funktionalität aktiviert ist, überprüft CommView die interne Datenbank um die zugehörigen Länderinformationen für jede IP-Adresse. Sie können das Programm so konfigurieren, dass es den **ISO-Ländercode**, den **Landesnamen** oder die **Landesflagge** für jede IP-Adresse anzeigt. Sie können Geo-Standort auch deaktivieren. Für einige reservierte IP-Adressen (z. B. 192.168.*.* oder 10.*.*.*) kann keine Länderinformation zugeteilt werden. In solchen Fällen wird der Landesname nicht angezeigt, oder falls Sie die Option **Landesflagge** benutzen, wird eine Flagge mit einem Fragezeichen angezeigt. In solchen Fällen wird der Landesname nicht angezeigt, oder falls Sie die Option **Landesflagge** benutzen, wird eine Flagge mit einem Fragezeichen angezeigt.

Wenn die IP-Zuweisung ständig wechselt, ist es wichtig, dass Sie immer eine aktuelle Version von CommView benutzen. Eine frische aktuelle Datenbank ist in jeder Ausgabe von CommView. Eine frische Datenbank hat eine 98%ige Treffgenauigkeit. Ohne Updates fällt die Treffgenauigkeit jedes Jahr prozentual um ca. 15%.

Verschiedenes

Bei minimierter Darstellung nicht in der Taskleiste anzeigen – Aktivieren Sie diese Checkbox, wenn beim Minimieren des Fensters der Button nicht in der Taskleiste angezeigt werden soll. Wenn diese Checkbox aktiv ist wird das Programm nach der Minimierung über ein System Tray-Icon erneut geöffnet.

Mehrere Instanzen dieser Applikation zulassen – Wenn diese Checkbox aktiviert ist, dann können Sie mehrere Instanzen von CommView auf demselben PC laufen lassen. Sie können dann den Paketverkehr von mehreren Netzwerkadaptern gleichzeitig erfassen. Diese Option steht Ihnen unter Windows 95 nicht zur Verfügung.

Verlassen der Applikation bestätigen – Aktivieren Sie diese Checkbox, wenn Sie die Programmbeendigung bestätigen möchten.

Auto-Scrollen im Register Pakete – Wenn diese Checkbox aktiv ist, scrollt das Programm den Text im Register Pakete automatisch, wenn Sie ein neues Paket aus der Paketliste auswählen (nur wenn der Text nicht in das Fenster passt). Dies ist nützlich, wenn sie bei einem großen Paket die Inhalte ansehen wollen ohne manuell scrollen zu müssen.

Auto-Scrollen zum letzten Paket in Paketliste – Wenn diese Checkbox aktiv ist, scrollt das Programm automatisch im Register Pakete die Paketliste durch bis zum letzten erhaltenen Paket.

Sortieren neuester Datensätze der aktuellen IP-Verbindungen – Wenn diese Checkbox aktiv ist, sortiert das Programm automatisch die neuen Einträge im Register Aktuelle IP-Verbindungen nach einem benutzerdefinierten Kriterium (z. B. aufsteigende Reihenfolge der Remote-IP-Adressen).

Smart CPU-Control verwenden – Wenn diese Checkbox aktiv ist versucht das Programm durch Senkung der Qualität und Frequenz der Bildschirm-Updates die CPU-Last beim Empfangen von sehr starkem Verkehr zu senken.

Mit Windows starten – Wenn diese Checkbox aktiv ist, startet das Programm jedesmal automatisch, wenn Windows gestartet wird. Unter Windows Vista und höher, ist diese Checkbox wirkungslos, wenn UAC aktiviert ist. Dies ist eine Einschränkung von Vista und den letzten Windows-Versionen, die verhindern, dass Applikationen mit höheren Rechten beim Windowsstart geladen werden. Wenn diese Funktionalität wichtig ist, deaktivieren Sie UAC.

Minimiert starten – Wenn diese Checkbox aktiv ist, wird das Programm minimiert gestartet und das Hauptfenster nicht angezeigt bis Sie das System Tray-Icon oder den Taskleisten-Button gedrückt haben.

Automatische Applikations-Updates aktivieren – Mit dieser Checkbox lassen Sie das Programm sich regelmäßig mit der TamoSoft-Website verbinden und nach Updates suchen. Mit dem Eingabefeld **Intervall zwischen den Checks** definieren Sie in welchen Abständen diese Überprüfung durchgeführt werden soll.

Plug-Ins

Dieser Bereich wird für Plug-Ins von Drittherstellern benötigt um Konfigurationsaufgaben zu ermöglichen. Mehr dazu unter [Maßgeschneidertes Decoding](#).

Häufig gestellte Fragen

In diesem Kapitel finden Sie die Antworten auf einige der am häufigsten gestellten Fragen (so genannte FAQ's). Die aktuellsten FAQ's finden Sie unter <http://www.tamos.com/products/commview/faq.php>.

F. Kann CommView den Paketverkehr eines Modems (RAS Adapter) erfassen?

A. Ja.

F. Was genau sieht CommView auf einem PC der mit einem LAN verbunden ist?

A. CommView aktiviert den vermischten Modus für die Netzwerkkarte und kann dann den gesamten Paketverkehr auf diesem LAN Segment erfassen. Es werden also die Pakete die an irgendeinen PC im LAN-Segment adressiert sind erfasst und analysiert. Im Falle von Wireless Ethernet (es können nur ankommende und ausgehende Pakete erfasst werden) und Netzwerken mit Switches gibt es gewisse Limitierungen (siehe Frage zum Thema Switches in diesen FAQ).

F. Ich bin via eines Switch mit einem LAN verbunden. Wenn ich CommView starte werden nur Pakete erfasst, die zu oder von meinem Computer gesendet wurden. Der Datenverkehr anderer LAN-Teilnehmer wird nicht erfasst. Warum ist das so?

A. Im Gegensatz zu Hubs verhindern Switches das Sniffing mit Netzwerkadaptern im Promiscuous-Modus. In einem LAN mit Switches ist CommView (und jeder andere Packetanalyzer) nur in der Lage Broadcast- und Multicast-Pakete, sowie die ankommenden und ausgehenden Pakete des PC's auf welchem CommView installiert ist, zu erfassen. Moderne Switches unterstützen jedoch das sog. Port Mirroring, welches ermöglicht, Teile des Paketverkehrs oder den gesamten Paketverkehr auf dem Switch auf einen bestimmten Monitoring-Port umzuleiten. Dies erlaubt Ihnen den gesamten LAN-Verkehr dieses Segmentes einzusehen. Wir haben das Informationsdokument [Vermischte Erfassung in Ethernet- und Wi-Fi-Netzwerken](#) zusammengestellt, welches dieses Thema im Detail behandelt.

F. OK, ich bin durch einen Hub mit einem LAN verbunden aber ich kann den Datenverkehr der anderen LAN-Teilnehmer nicht sehen, als ob es ein Switch wäre. Warum ist das so?

A. Dafür gibt es zwei mögliche Gründe. Entweder der Hub ist nur als Hub ausgewiesen, es ist aber ein Switch (z. B. Hersteller wie Linksys) oder der Hub ist ein sogenannter Multi-Speed-Hub. In diesem Fall kann der Paketverkehr von Netzwerkadaptern, die mit einer anderen Geschwindigkeit arbeiten als Ihr Netzwerkadapter, nicht angezeigt werden. Wenn Sie also z. B. einen 10MBit/s Netzwerkadapter haben, können Sie den erzeugten Paketverkehr von 100MBit/s Netzwerkadaptern, nicht sehen.

F. Ich habe zu Hause ein LAN und bin via Breitband-Router mit dem Internet verbunden und ich kann nur meinen eigenen Datenverkehr sehen. Ist es auch möglich den Datenverkehr anderer Teilnehmer meines LAN's zu sehen?

A. Kurz gesagt: Ja. Es gibt mehrere Möglichkeiten dieses Problem zu lösen. Konsultieren Sie für weitere Informationen und Beispiele der Netzwerkanordnungen das Informationsdokument [Vermischte Erfassung in Ethernet- und Wi-Fi-Netzwerken](#).

F. Kann CommView Daten eines Netzwerkadapters erfassen das keine IP-Adresse hat?

A. Ja, der Netzwerkadapter muss nicht an TCP/IP oder ein anderes Protokoll gebunden sein. Besonders bei der Fehlersuche kann es vorkommen, dass Sie den Computer auf dem CommView läuft mit irgendeinen freien Port eines Hub's verbinden müssen. In einer solchen Situation müssen Sie sich nicht um Ihre IP-Adresse im LAN-Segment kümmern. Sie brauchen nur die Bindung des Netzwerkadapters mit dem TCP/IP-Protokoll zu unterbrechen und dann können Sie mit der Paketerfassung beginnen. Öffnen Sie die Systemsteuerung => Netzwerkverbindungen, rechts klicken Sie auf das Icon der Verbindung, wählen Sie Eigenschaften und deaktivieren Sie die entsprechende Checkbox welche das Protokoll an den Netzwerkadapter (NIC) bindet.

F. Ich bin in einem LAN mit hohem Verkehrsvolumen und es ist schwer einzelne Pakete zu untersuchen, weil die alten Pakete schnell aus der Pufferanzeige entfernt werden, wenn die Applikation hunderte oder tausende von Paketen pro Sekunde empfängt. Kann ich etwas dagegen tun?

A. Ja, Sie können den Button **[Aktuellen Puffer in neuem Fenster öffnen]** auf der kleinen Werkzeugleiste des Registers **Pakete** benutzen. Das ermöglicht Ihnen bei jedem Intervall, so viele Schnappschüsse des aktuellen Puffers zu erstellen, wie Sie möchten. Sie werden dann in der Lage sein, die Pakete in den neuen Fenstern in Ihrer arbeitsfreien Zeit zu untersuchen.

F. Ich startete das Programm und klickte auf Paketerfassung starten aber es werden keine Pakete angezeigt. Warum?

A. Es gibt zwei mögliche Gründe: Entweder Sie haben einen unbenutzten Netzwerkadapter gewählt oder es ist bei der Definition der Paketerfassungsregeln ein Fehler unterlaufen. Schalten Sie alle Regeln aus und schauen Sie was passiert. Die Statusleiste des Programms sollte in jedem Fall die Gesamtzahl der erfassten Pakete anzeigen.

F. Ich habe festgestellt, dass die Prüfsumme der ausgehenden IP-/TCP-/UDP-Pakete nicht korrekt ist. Warum ist das so?

A. Neue Gigabit-Netzwerkadapter haben eine Checksum Offload-Option, welche ermöglicht, dass der Netzwerkadapter selbst die CRC bestimmt. Dies dient der Entlastung der CPU. Da CommView die ausgehenden Pakete abfängt, bevor Sie beim Netzwerkadapter ankommen, erscheint die CRC nicht korrekt, da sie vom Netzwerkadapter noch nicht bestimmt wurde. Das ist grundsätzlich korrekt und betrifft allenfalls die Rekonstruktion einer TCP-Sitzung, sofern Sie die Grundeinstellungen der Option Falsche Prüfsummen für die TCP Sitzungsrekonstruktion ignorieren geändert haben (siehe [Einstellungen](#) für weitere Informationen).

F. Arbeitet CommView auch auf Multiprozessor-Computer?

A. Ja.

F. Es scheint unmöglich zu sein, mehr als 5000 Pakete vom Paketpuffer zu speichern. Gibt es eine Abhilfe?

A. Aktuell existiert keine solche Begrenzung. Die Applikation benutzt einen Umlaufpuffer zur Speicherung erfasster Pakete. Standardmäßig kann der Puffer die letzten 5000 Pakete aufnehmen, aber dieser Wert kann über die **Einstellungen** angepasst werden. Die maximale Puffergröße beträgt 20000 Pakete (der Puffer kann aus einem nahe liegenden Grund nicht unbegrenzt sein: Ihr Computer-RAM ist nicht unbegrenzt). Sie können den Pufferinhalt unter Benutzung des Registers **Protokolle** in eine Datei speichern. Diese Begrenzung der Puffergröße schränkt die Fähigkeit zur Speicherung einer Anzahl von Paketen keineswegs ein. Sie brauchen nur die automatische **Protokollierung** im Register Protokollierung aktivieren. Eine solche automatische Protokollierung veranlasst die Applikation zur kontinuierlichen Ausgabe der erfassten Pakete in Dateien und Sie können eine Begrenzung der Gesamtgröße der erfassten Daten festlegen.

F. Ich habe eine Netzwerkverbindung via Kabel/xDSL Modem. Ist CommView in der Lage diesen Paketverkehr zu erfassen?

A. Wenn Ihr Modem eine Dual-USB/Ethernet-Schnittstelle hat und Sie das Modem mit einer Ethernet-Karte verbinden können wird CommView den Paketverkehr erfassen. Wenn das Modem nur eine USB-Schnittstelle hat, versuchen Sie es am besten einfach.

F. Meine Firewall-Software warnt mich, dass CommView versucht sich mit dem Internet zu verbinden. Ich weiß, dass manche Webseiten die Besucher tracken können, indem Sie die Information sammeln, die durch das Programm über das Internet geschickt wird. Warum versucht CommView sich mit dem Internet zu verbinden?

A. Drei Dinge können Ihre Firewall alarmiert haben. Erstens: Es kann ein Versuch sein IP-Adressen in Hostnamen aufzulösen. Da CommView Kontakt zu Ihrem DNS-Server hat um DNS-Anfragen durchzuführen, kann so unausweichlich ein Alarm ausgelöst werden. Sie können diese Funktion ausschalten (unter Einstellungen => Optionen => Keine DNS Auflösung). Im Register Letzte IP-Verbindungen werden dann keine Hostnamen mehr angezeigt. Zweitens: Sie haben das Programm so konfiguriert, dass es nach Updates bzw. neueren Versionen sucht. Dabei verbindet sich CommView mit www.tamos.com. Dies können Sie unter Einstellungen => Optionen => Versch. => Automatische Applikations-Updates aktivieren deaktivieren. Drittens: Wenn Sie das Programm kaufen, müssen Sie es aktivieren, CommView muss sich dazu mit www.tamos.com verbinden. Sie können dies umgehen, wenn Sie die manuelle Aktivierung auswählen. Dies sind die einzigen Gründe warum CommView allenfalls eine Verbindung ins Internet herstellt. Es gibt keine versteckten Aktivitäten. Wir verkaufen keine Spyware.

F. Ich bin oft als Benutzer und ohne administrative Rechte angemeldet. Muss ich mich um CommView zu starten abmelden und als Administrator wieder anmelden?

A. Nein. Sie können das CommView-Verzeichnis öffnen, rechtsklicken Sie dann auf CA.exe während Sie Shift gedrückt halten und wählen Sie dann **Ausführen als...** aus dem Kontextmenü. Geben Sie den administrativen Login und das Passwort ein und klicken Sie dann auf **[OK]** um das Programm zu starten. Unter Windows Vista und höher startet CommView automatisch mit erhöhten Rechten.

F. Kann CommView den Datenverkehr auf einem Netzwerkadapter erfassen wenn es unter Microsoft Virtual PC läuft?

A. Ja. Die einzige Beschränkung ist der Vermischte-Modus, er ist für virtuelle Adapter nicht verfügbar. D.h. Sie können nur Ihren eigenen Datenverkehr und Broadcast-Pakete erfassen.

F. Wenn ich den Paketverkehr meiner Einwahlverbindung untersuche kann ich während des Sitzungsaufbaus (CHAP, LCP, etc.) keine PPP-Pakete finden. Ist das normal?

A. Leider können PPP-Handshaking-Pakete nicht erfasst werden. Nehmen Sie zur Kenntnis, dass alle anderen PPP-Pakete, welche dem einleitenden Handshake-Vorgang folgen, erfasst werden.

F. Ich benutze WireShark und ich bemerke, dass ich nach der CommView-Installation keine Pakete mehr erfassen kann.

A. Da existiert ein bekannter Konflikt zwischen WinPcap, dem Treiber von WireShark und einigen anderen ähnlichen Produkten, und dem von CommView benutzten Treiber. Einfache Abhilfe: Starten Sie die Erfassung mit WireShark bevor Sie die Paketerfassung mit Commview starten. In diesem Fall werden beide Produkte in der Lage sein, Daten simultan zu erfassen. Falls Sie die Erfassung mit CommView zuerst starten, wird WinPcap aus einem uns unbekanntem Grund keine Pakete erfassen.

F. Bei der Rekonstruktion von TCP-Sitzungen die japanische oder chinesische HTML-Seiten beinhalten kann ich den Originaltext nicht sehen.

A. Zur Anzeige ostasiatischer Sprachen sollten Sie ostasiatische Fonts installieren. Öffnen Sie Systemsteuerung => Ländereinstellungen, wählen Sie das Register "Sprachen" und aktivieren Sie die Checkbox "Dateien für ostasiatische Sprachen installieren".

F. Kann ich Ton vom VoIP-Analyser in eine Standard-.wav- oder .mp3-Datei speichern?

A. Nicht direkt, aber es gibt eine Menge Hilfsmittel auf dem Markt, die ein "virtuelles Audiokabel" anbieten, welches alles in eine Datei speichert, was Ihre Soundkarte abspielt. Versuchen Sie zum Beispiel, [Xilisoft Sound Recorder](#) (benutzen Sie den Modus "Was Sie hören").

VoIP-Analyse

Einleitung

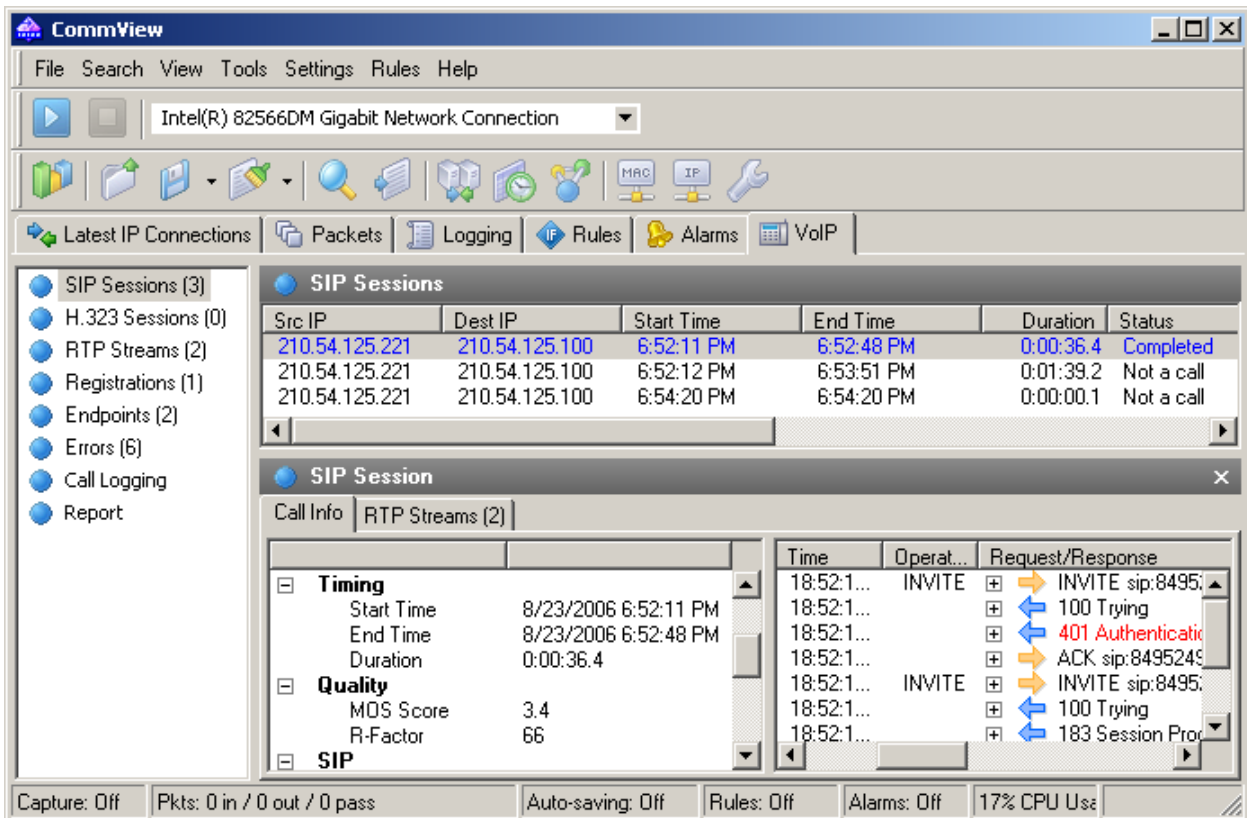
HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser ist ein eingebautes CommView-Modul, das für die Echtzeiterfassung und Analyse von Internettelefonie (VoIP) geeignet ist, darunter fallen Anrufabläufe, Nachrichtenübermittlungen, Registrierungen, Medienströme, Fehler usw. Dieses Hilfsmittel hilft, durch die Sichtbarmachung dieser Daten und Beurteilung der Sprachqualität, Ihre Produktivität bei der Austestung von Netzwerken, Software und Hardware zu steigern. CommView's VoIP-Analyser unterstützt **SIP 2.0**- und **H.323**-Nachrichtenprotokolle und **RTP 2.0**-Medienströme und viele weitverbreitete Codecs. Zusätzlich zur Echtzeitanalyse, kann der Analyser für den nachträglichen Import der erfassten Daten und zur Analyse von Erfassungsprotokollen in einer Vielzahl von Formaten (z.B. Tcpdump, EtherPeek, usw.) genutzt werden.

Arbeiten mit dem VoIP-Analyser

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser wird über das Register VoIP des Hauptfensters erreicht, in dem die Echtzeitanalyse erfasster Pakete aufgeführt wird oder durch das [VoIP-Protokoll-Betrachterfenster](#), das benutzt werden sollte, wenn Sie eine nachträgliche Analyse von Protokolldateien ausführen möchten. Der VoIP-Analyser arbeitet korrekt mit der Paketerfassung und zeigt die Ergebnisse in Echtzeit an:



Die Informationen im VoIP-Analyser-Fenster werden in verschiedenen Kategorien gegliedert. Die Kategorienuflistung wird im Fensterausschnitt angeordnet und ermöglicht die Auswahl und Ansicht detaillierter Analysedaten, welche im rechten Teil des Fensters dargestellt werden. Die folgenden Kategorien sind verfügbar:

SIP-Sitzungen – Auflistung erfasster SIP 2.0-Sitzungen.

H.323-Sitzungen – Auflistung erfasster H.323-Sitzungen.

RTP-Ströme – Auflistung erfasster RTP-Ströme.

Registrierungen – Auflistung der am Registrations-Server registrierten Klienten und der Klienten-Registrierungsverlauf.

Endpunkte – Auflistung der am VoIP-Datenaustausch beteiligten Arbeitsplätze.

Fehler – Auflistung der während des VoIP-Datenaustausches registrierten Fehler.

Anrufprotokoll – Protokollkonfiguration für erfasste VoIP-Daten.

Bericht – Konfiguration der Berichtserstellung, inklusive des Automatikmodus.

Für detaillierte Informationen, über die Datenanordnung im VoIP-Analyser, verweisen wir auf das Kapitel [Arbeiten mit Auflistungen im VoIP-Analyser](#).

SIP- und H.323-Sitzungen

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser unterstützt aktuell zwei Typen von VoIP-Signalprotokollen, SIP und H.323. SIP- und H.323-Sitzungen werden als zwei separate Elemente im linken Fensterausschnitt dargestellt. Durch Auswahl eines der Elemente werden die zugehörigen, durch die Applikation erfassten Nachrichtensitzungen und detaillierte Informationen zu jeder Sitzung dargestellt:

The screenshot shows the 'VoIP Log Viewer [G.723 including SIP.ncf]' application. The left sidebar contains a tree view with categories: SIP Sessions (3), H.323 Sessions (0), RTP Streams (2), Registrations (1), Endpoints (2), and Errors (6). The main window is divided into two panes. The top pane, titled 'SIP Sessions', displays a table with columns: Src IP, Dest IP, Start Time, End Time, Duration, Status, and Sr. The table contains three rows of session data. The bottom pane, titled 'SIP Session', shows detailed information for a selected session, including 'Call Info' and 'RTP Streams (2)'. The 'Call Info' section is expanded to show 'Transport Information', 'Timing', 'Quality', and 'SIP' details. The 'Request/Response' section shows a sequence of SIP messages: an INVITE at 18:52:11.965000, a 100 Trying response at 18:52:12.021000, a 401 Authentication required response at 18:52:12.021000, and an ACK at 18:52:12.034000. The 401 response header is highlighted in green and includes fields like Via, From, To, CallID, CSeq, WWW-Authenticate, Server, and Content-Length.

Src IP	Dest IP	Start Time	End Time	Duration	Status	Sr
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed	
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call	
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call	

Transport Information

Src IP	210.54.125.221
Src Port	3068
Dest IP	210.54.125.100
Dest Port	5060
Protocol	UDP

Timing

Start Time	8/23/2006 6:52...
End Time	8/23/2006 6:52...
Duration	0:00:36.4

Quality

MOS Score	3.4
R-Factor	66

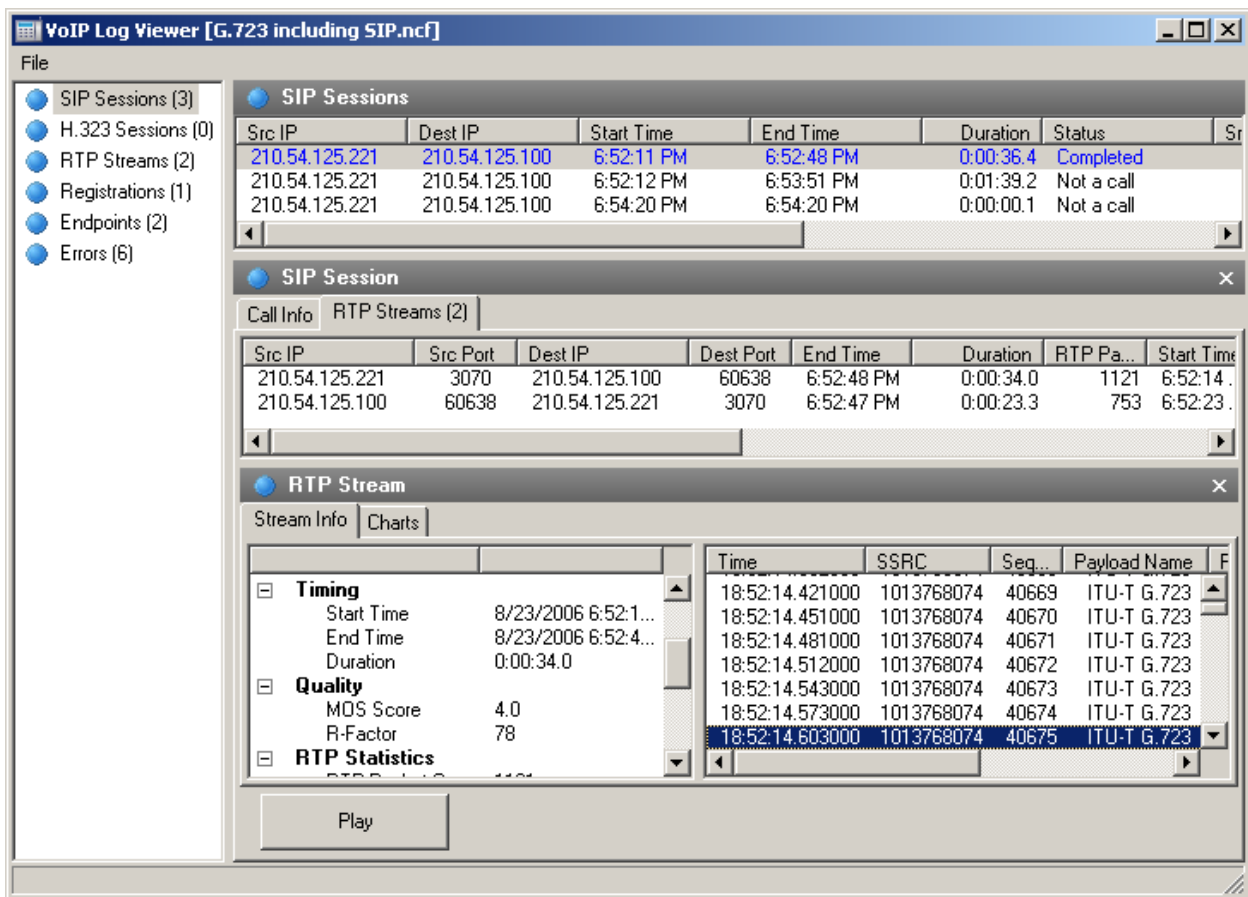
SIP

Call ID	29002@192.16...
Calling Party	
Src Display ...	
Src SIP Ad...	2326845@tamo...
Src Tag	16403
Src User Ag...	PortSIP softpho...

Request/Response

Time	Request/Response
18:52:11.965000	INVITE sip:12345678901@tamos....
18:52:12.021000	100 Trying
18:52:12.021000	401 Authentication required
18:52:12.034000	ACK sip:12345678901@tamos.cor...
18:52:12.046000	INVITE sip:12345678901@tamos...

Der obere Fensterausschnitt zeigt eine komplette Auflistung der erfassten SIP- oder H.323-Sitzungen. Wenn Sie eine SIP-/H.323-Sitzung aus der Liste auswählen, werden detaillierte Informationen der ausgewählten Sitzung im unteren Fensterausschnitt eingeblendet, inklusive eines detaillierten Sitzungsprotokolls, summierte und statistische Daten, sowie die RTP-Ströme bezogen auf die ausgewählte Sitzung.



Falls RTP-Ströme für die gewählte Nachrichtensitzung verfügbar sind, ist es möglich einen Anruf durch klicken auf **[Wiedergabe]** wiederzugeben.

Siehe auch:

[Arbeiten mit Auflistungen im VoIP-Analyser](#)

[Anrufswiedergabe](#)

[NVF-Dateien](#)

RTP-Ströme

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Das Echtzeittransportprotokoll (RTP oder Real-time Transport Protocol) definiert ein standardisiertes Paketformat zum in Umlauf bringen von Audio und Video über das Internet. Während Protokolle wie SIP oder H.323 zur Kontrolle des Anrufs benutzt werden (z.B. zur Verbindungseinstellung, zum Wählen, zur Verbindungstrennung, usw.), wird RTP zur sicheren Übertragung von Datenpaketen und zur Erhaltung der Dienstqualität benutzt. In anderen Worten, RTP-Ströme befördern die aktuelle Sprachladung unter Benutzung eines Codecs aus einer Anzahl von Codecs und die Analyse der RTP-Daten stellt unschätzbare Informationen zur Beurteilung der Anrufqualität und zur Fehlersuche in VoIP-Netzwerken bereit.

Zur Anzeige von durch die Applikation erfassten RTP-Strömen, wählen Sie **RTP-Ströme** im linken Fensterausschnitt des VoIP-Analyser-Fensters:

The screenshot shows the VoIP Log Viewer interface. The main window title is "VoIP Log Viewer [G.723 including SIP.ncf]". On the left, there is a navigation pane with the following items: SIP Sessions (3), H.323 Sessions (0), RTP Streams (2), Registrations (1), Endpoints (2), and Errors (6). The "RTP Streams" section is selected, displaying a table with the following data:

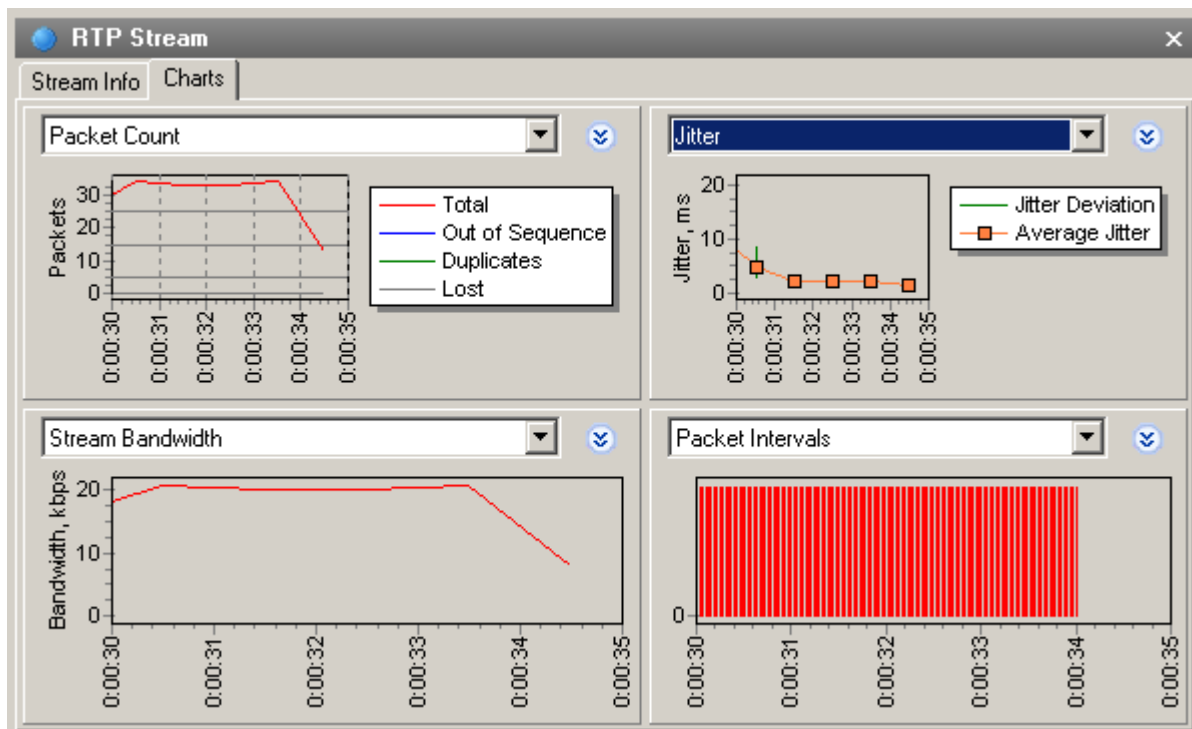
Src IP	Dest IP	Start Time	Duration	RTP ...	Avera...	Lost Packets	Max Jitte...	MOS
210.54.125.100	210.54.125.221	6:52:23 PM	0:00:23.3	753	19.63	27 (3.5%)	56.26	
210.54.125.221	210.54.125.100	6:52:14 PM	0:00:34.0	1121	20.07	0	19.16	

Below this table, a detailed view of an RTP Stream is shown. The "RTP Stream" window has tabs for "Stream Info" and "Charts". The "Stream Info" tab is active, showing the following details:

- Transport Infor...**
 - Src IP: 210.54.125.100
 - Src Port: 60638
 - Dest IP: 210.54.125.221
 - Dest Port: 3070
 - Protocol: UDP
- Timing**
 - Start Time: 8/23/2006 6:...
 - End Time: 8/23/2006 6:...
 - Duration: 0:00:23.3
- Quality**
 - MOS Score: 3.4
 - R-Factor: 66
- RTP Statistics**
 - RTP Packet Co...: 753
 - Lost Packets: 27 (3.5%)
 - Duplicate Pack...: 0
 - Sequence Errors: 0
- Network Utilizat...**
 - Total Traffic (byt...): 58,734
 - Network Tra: 31.626 (53.8%)

The "Charts" tab is also visible, showing a list of RTP packets with columns for Time, SSRC, Payload Na..., Jitter..., and RTI. The list contains 20 entries, each representing a packet received at a specific time with a unique SSRC and a payload of ITU-T G.723.

Der obere Teil zeigt eine komplette Auflistung aller RTP-Ströme. Wenn Sie einen RTP-Strom aus der Liste auswählen, werden detaillierte Informationen des ausgewählten Stroms im unteren Fensterausschnitt eingeblendet, inklusive der vollständigen RTP-Paketliste, summierte und statistische Daten, sowie die Diagramme:



Bis zu vier verschiedene Diagramme können für den ausgewählten Strom simultan, mit einem Fensterintervall von 5 bis 60 Sekunden, angezeigt werden. Beachten Sie bitte, dass durch Rechtsklicken und Ziehen das Schaubild nach links blättert oder entsprechend nach rechts. Die folgenden Diagrammtypen sind verfügbar:

Paketanzahl – Anzahl der RTP-Pakete/Sekunde inklusive Duplikate, verloraener und defekter Pakete.

Stombandbreite – Geschwindigkeit des Stroms in Kilobits/Sekunde.

Paketgröße – Durchschnittliche Größe, der durch das Netzwerk, die RTP-Köpfe und die RTP-Ladung getrennte, RTP-Pakete.

Jitter – Strom-Jitter.

R-Factor, MOS Score – Stromqualitätsbeurteilung.

Paketintervalle – Zeitliche Zuordnung von RTP-Paketen zu einem Strom.

Die RTP-Stromauflistung beinhaltet alle erfassten RTP-Ströme, zugehörig zu SIP- oder H.323-Nachrichtensitzungen und solche für nicht identifizierte Nachrichtensitzungen (s.g. Verwaiste Ströme, die z.B. zu keiner Hauptsitzung gehören). Für detaillierte Informationen, zum Ausschluss von RTP-Strömen, ohne zugehörige Nachrichtensitzungen, verweisen wir auf das Kapitel [Einstellungen](#).

Siehe auch:

[Arbeiten mit Auflistungen im VoIP-Analyser](#)

[Anrufswiedergabe](#)

[NVF-Dateien](#)

Registrierungen

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Zur Anzeige des mit dem Registrierungs-Server registrierten VoIP-Klienten, wählen Sie das Element **Registrierung** im linken Fensterausschnitt des VoIP-Analyser-Fensters:

The screenshot shows the 'VoIP Log Viewer [G.723 including SIP.ncf]' application. On the left is a navigation pane with categories: SIP Sessions (3), H.323 Sessions (0), RTP Streams (2), Registrations (1), Endpoints (2), and Errors (6). The main window is divided into two panes. The top pane, titled 'Registrations', contains a table with columns: Last Activity, User IP, User, Domain, Location, and Registrar IP. The bottom pane, titled 'Registration Trace : 2326845@tamos.com', contains a table with columns: Src IP, Dest IP, Date, Time, and Request/Response. The 'Request/Response' column shows a sequence of REGISTER, 401 Authentication required, and 200 OK messages. A detailed view of a 401 Authentication required response is shown in a highlighted box, including SIP headers and content.

Last Activity	User IP	User	Domain	Location	Registrar IP
6:54:20 PM	210.54.125.221	2326845@tamo...	tamos.com	2326845@192.168.13...	210.54.125.100

Src IP	Dest IP	Date	Time	Request/Response
210.54.125.221	210.54.125.100	8/23/2006	18:52:12.049000	REGISTER sip:tamos.com:5060
210.54.125.100	210.54.125.221	8/23/2006	18:52:12.126000	401 Authentication required
210.54.125.221	210.54.125.100	8/23/2006	18:52:12.130000	REGISTER sip:tamos.com:5060
210.54.125.100	210.54.125.221	8/23/2006	18:52:12.186000	200 OK
210.54.125.221	210.54.125.100	8/23/2006	18:52:30.317000	REGISTER sip:tamos.com:5060
210.54.125.100	210.54.125.221	8/23/2006	18:52:30.568000	401 Authentication required
210.54.125.221	210.54.125.100	8/23/2006	18:52:30.580000	REGISTER sip:tamos.com:5060
210.54.125.100	210.54.125.221	8/23/2006	18:52:30.762000	200 OK
210.54.125.221	210.54.125.100	8/23/2006	18:53:09.819000	REGISTER sip:tamos.com:5060

Header
SIP/2.0 401 Authentication re
Via: SIP/2.0/UDP 192.168.131.70:
Path: <sip:81.140.116.2.3068.nat.c
From: <sip:2326845@tamos.com:50
To: <sip:2326845@tamos.com:506
Call-ID: 2896@192.168.131.70
CSeq: 17 REGISTER
WWW-Authenticate: Digest realm=
Server: CommuniGatePro/5.0.10
Content-Length: 0

Content
(none)

Der obere Teil des rechten Ausschnittfensters zeigt eine Auflistung aller Registrierungen, inklusive des aktuellen Registrierungsstatus der VoIP-Klienten. Wenn Sie einen registrierten Datensatz auswählen, wird das Registrierungsprotokoll des VoIP-Klienten mit den gesendeten/emfangenen Mitteilungen des Registrierungs-Servers eingeblendet.

Endpunkte

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Dieser Fensterausschnitt zeigt eine Auflistung aller am VoIP-Datenaustausch beteiligten Arbeitsplätze, inklusiver statistischer Daten und eine Liste der Hauptanrufer.

The screenshot shows the 'VoIP Log Viewer [G.723 including SIP.ncf]' application window. On the left is a sidebar with a tree view containing: SIP Sessions (3), H.323 Sessions (0), RTP Streams (2), Registrations (1), Endpoints (2), and Errors (6). The main area is divided into three sections:

- Endpoints:** A table with columns: Last Activity, IP Address, MAC Address, Description, Placed..., Received..., and Successf...

Last Activity	IP Address	MAC Address	Description	Placed...	Received...	Successf...
6:54:20 PM	210.54.125.221	00:00:01:00:00:00	PortSIP softphone 2.0	1	0	
6:54:20 PM	210.54.125.100	80:AB:20:00:01:00	CommuniGatePro/5.0.10	0	1	
- Endpoint : 210.54.125.221 - PortSIP softphone 2.0:** A sub-section with tabs for SIP Sessions (3) and H.323 Sessions (0). It contains a table:

Src IP	Dest IP	End Time	Duration	Start Time	Status
210.54.125.221	210.54.125.100	6:52:48 PM	0:00:36.4	6:52:11 PM	Comp
210.54.125.221	210.54.125.100	6:53:51 PM	0:01:39.2	6:52:12 PM	Not a
210.54.125.221	210.54.125.100	6:54:20 PM	0:00:00.1	6:54:20 PM	Not a
- SIP Session:** A sub-section with tabs for Call Info and RTP Streams (2). It contains a table:

Src IP	Src Port	Dest IP	Dest Port	End Time	Duration	RTP Pa...	Start Tir
210.54.125.221	3070	210.54.125.100	60638	6:52:48 PM	0:00:34.0	1121	6:52:14
210.54.125.100	60638	210.54.125.221	3070	6:52:47 PM	0:00:23.3	753	6:52:23

At the bottom of the window, there is a 'Play' button.

Die vollständige Liste der Arbeitsplätze wird im oberen Teil des Fensterausschnittes angezeigt. Wenn Sie einen Endpunkt auswählen, zeigt der untere Teil des Fensterausschnittes die eingeleiteten oder empfangenen Anrufe des ausgewählten Computers.

Fehler

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Dieser Fensterausschnitt zeigt die Auflistung der letzten, während des Datenaustausches zwischen den VoIP-Clients und Server, registrierten Fehler:

The screenshot shows the 'VoIP Log Viewer [G.723 including SIP.ncf]' application. The left sidebar lists various session types: SIP Sessions (3), H.323 Sessions (0), RTP Streams (2), Registrations (1), Endpoints (2), and Errors (6). The main window is divided into two sections. The top section, titled 'Errors', displays a table of the most recent errors. The bottom section, titled 'SIP Session', provides a detailed view of a selected session, including call information, transport details, timing, quality, and SIP message exchanges.

Time	IP Address	Call ID	Error Class	Error Description
18:52:12.021000	210.54.125.100	29002@192.16...	Authorization	401 Authentication required
18:52:12.126000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:52:30.568000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:53:09.861000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:53:51.184000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:54:20.174000	210.54.125.100	8956@192.168...	Authorization	401 Authentication required

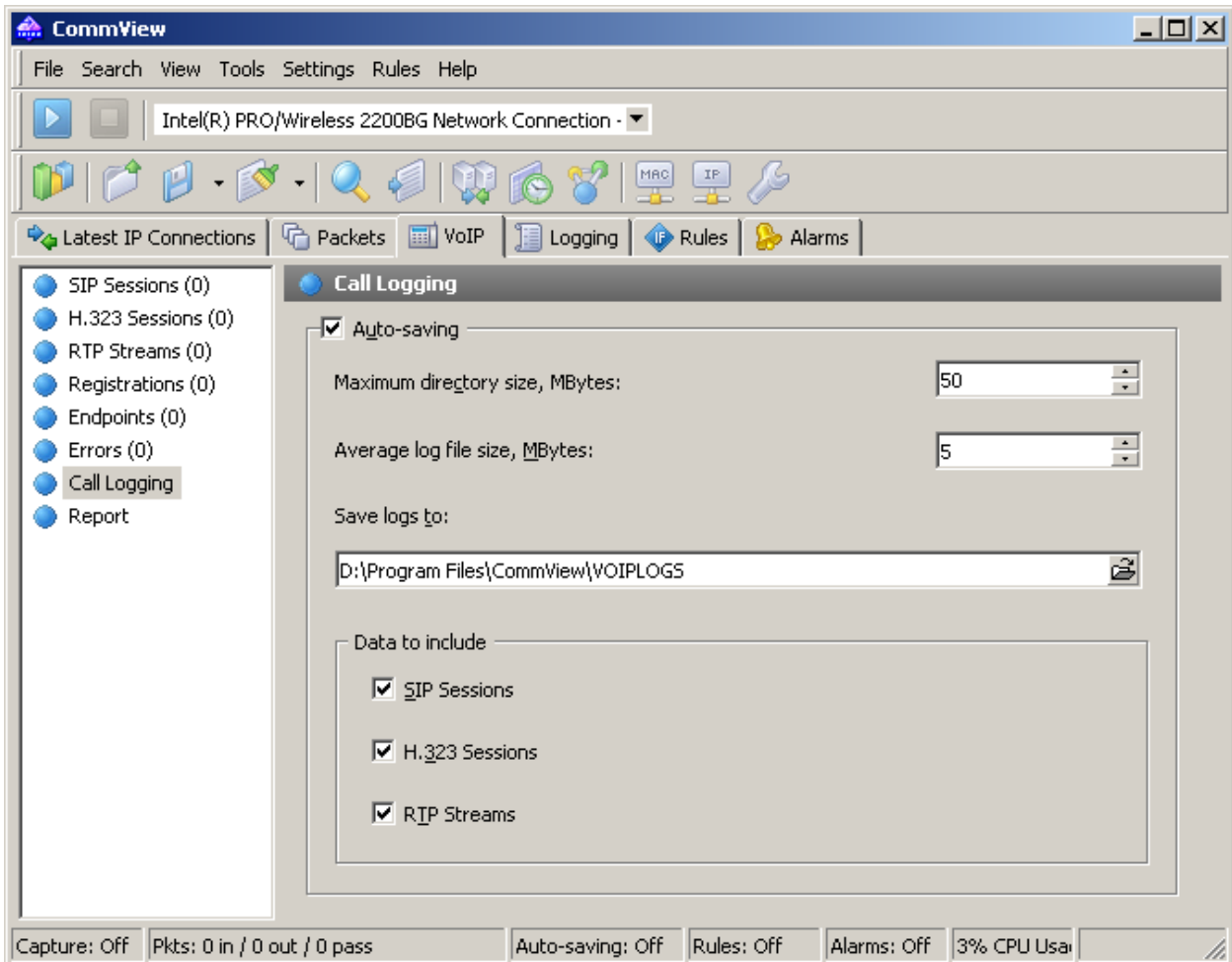
Time	Request/Response
18:52:12.049000	REGISTER sip:amos.com:5060
18:52:12.126000	401 Authentication required
18:52:12.130000	REGISTER sip:amos.com:5060
18:52:12.186000	200 OK
18:52:30.317000	REGISTER sip:amos.com:5060
18:52:30.568000	401 Authentication required
18:52:30.580000	REGISTER sip:amos.com:5060
18:52:30.762000	200 OK
18:53:09.819000	REGISTER sip:amos.com:5060
18:53:09.861000	401 Authentication required
18:53:09.866000	REGISTER sip:amos.com:5060
18:53:09.937000	200 OK
18:53:51.143000	REGISTER sip:amos.com:5060
18:53:51.184000	401 Authentication required
18:53:51.190000	REGISTER sip:amos.com:5060
18:53:51.252000	200 OK

Die Auflistung der letzten Fehler wird im oberen Teil des Fensterausschnittes angezeigt. Wenn Sie einen Datensatz auswählen, werden die zugehörigen Anrufinformationen im unteren Teil des Ausschnittfensters eingeblendet.

Anrufprotokoll

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Das Anrufprotokoll ermöglicht Ihnen automatisch alle VoIP-bezogenen Pakete als CommView-Erfassungsdatei zu speichern:

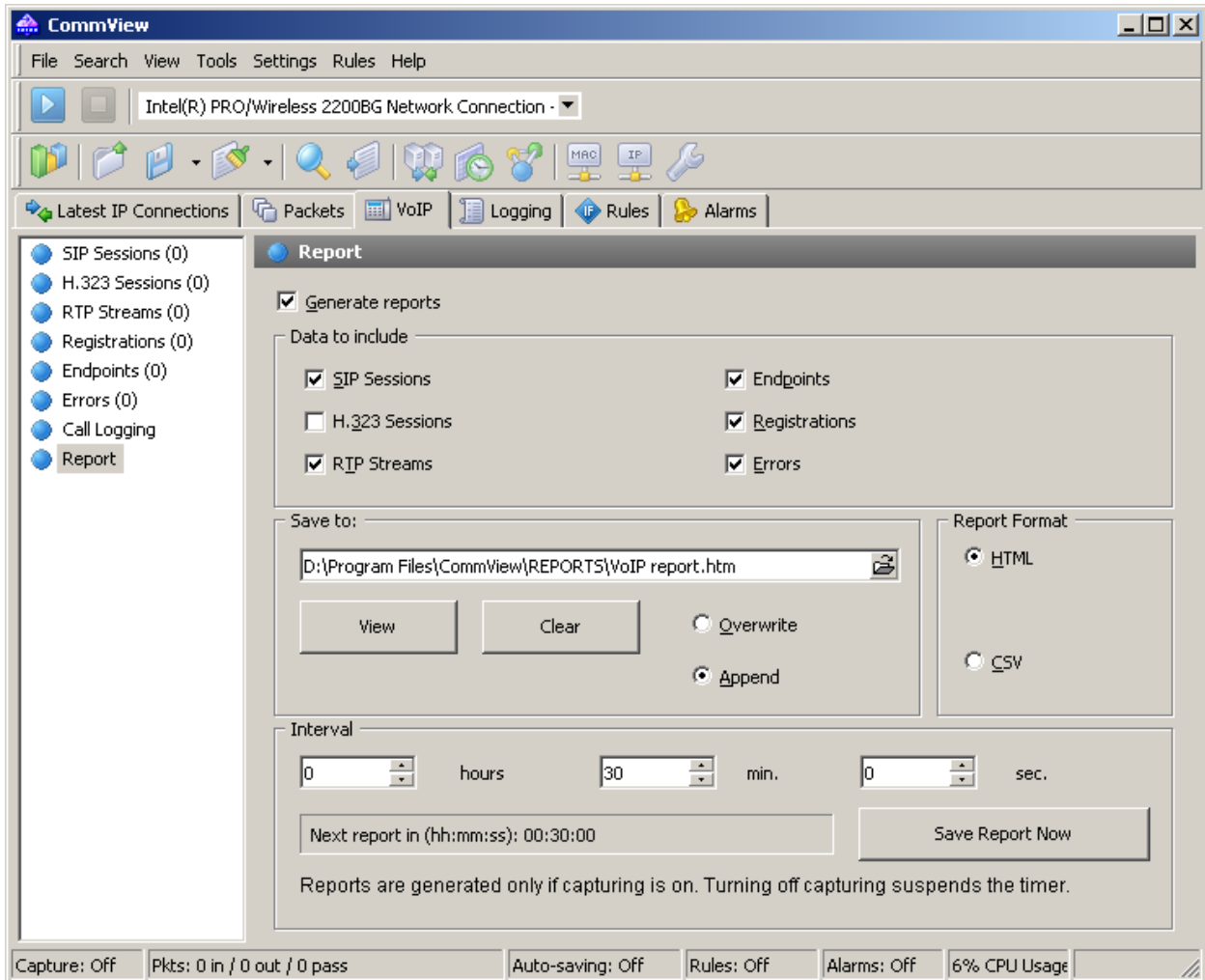


Aktivieren Sie die Funktion **Automatische Speicherung** und wählen Sie die zu erfassenden Ausgabedaten die in eine Protokolldatei gespeichert werden sollen. Die Festlegung der Daten im Bereich **Einzubindende Daten**, lässt Sie die spezifischen Pakete konfigurieren, welche die Applikation protokollieren soll.

Berichte

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Das Ausschnittfenster **Berichte** ist für die automatische Erstellung von VoIP-Berichten vorgesehen:

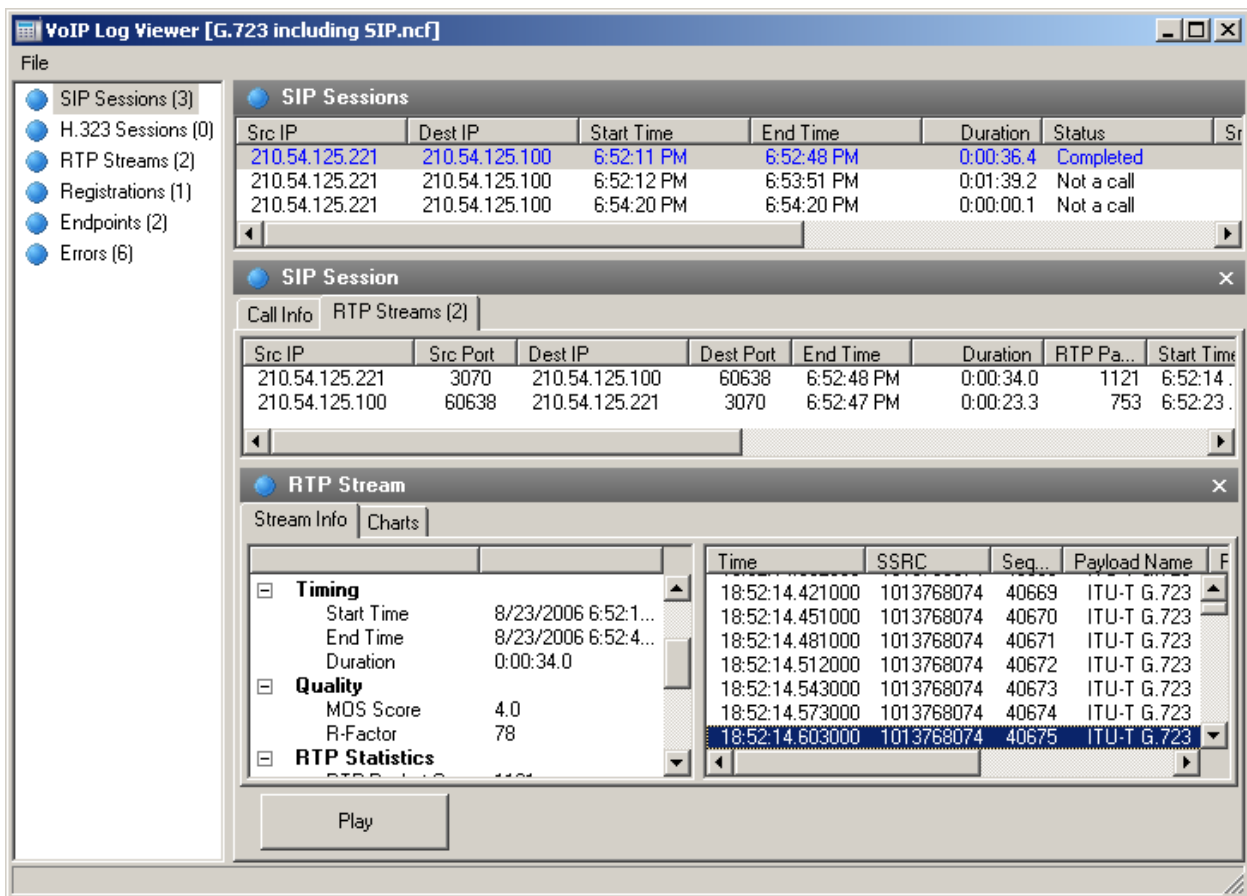


Ankreuzen der Checkbox **Berichte generieren** aktiviert die Berichtserzeugung. Der Bereich **Einzubindenden Daten**, lässt Sie die spezifischen Informationen konfigurieren, welche Sie in die Berichte einbinden möchten. Sie können ebenso das Berichtsformat (CSV oder HTML) einstellen, sowie die Zeitintervalle in denen die Berichte erstellt werden sollen. Neuere Berichte können entweder ältere ersetzen oder angehängt werden.

Anrufwiedergabe

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

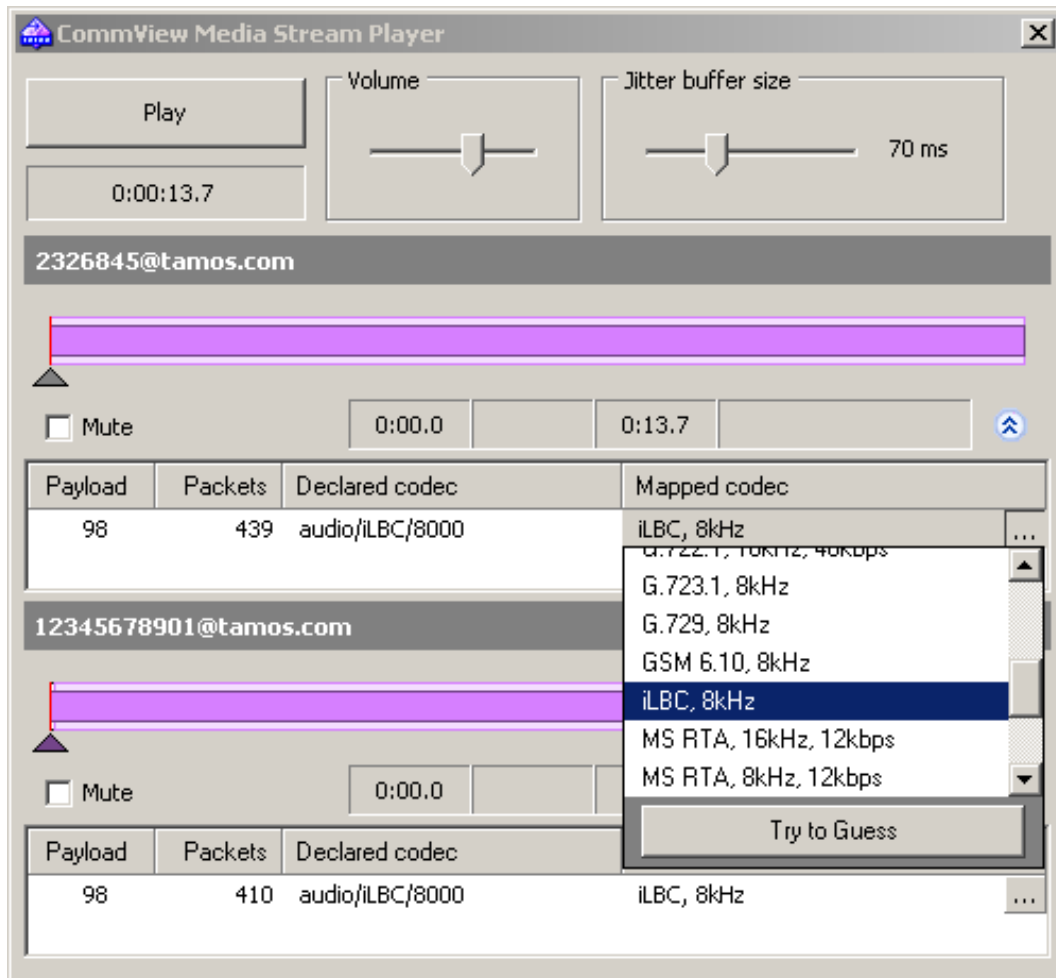
Die Funktionalität der Anrufwiedergabe kann erfahrungsgemäß zur Beurteilung der Audioqualität, die an einem VoIP-Anruf teilnehmenden Parteien genutzt werden. In den meisten Fällen, ermöglicht Ihnen der VoIP-Analyser erfasste Anrufe wiederzugeben (dies ist von der Unterstützung des bei dem vorgegebenen VoIP-Anruf verwendeten Codec's abhängig). Zur Wiedergabe eines Anrufs, wählen Sie die gewünschte Aufzeichnung im VoIP-Analyser-Fenster, wählen das Register **RTP-Ströme** und klicken auf den Button **[Wiedergabe]**:



Alternativ können Sie ein beliebiges Element aus der Auflistung der RTP-Ströme (z.B. die [RTP-Stromkategorie](#)) im rechten Fensterausschnitt auswählen, wählen Sie ein oder mehrere Ströme, führen Sie einen Rechtsklick darauf aus und wählen Sie den Menüpunkt **Auswahl wiedergeben**. Auf diesem Weg ist es möglich Ströme mit fehlenden oder nichtunterstützten Signalsitzungen (z.B. das Protokoll ist kein SIP oder H.323) zu verbinden und wiederzugeben.

HINWEIS. Simultane Wiedergabe von RTP-Strömen, die zu **unterschiedlichen Anrufen** gehören und die zu verschiedenen Zeiten ausgeführt wurden, ist nicht durchführbar. Das Hauptproblem ist die erhebliche Zeitdifferenz zwischen den Strömen, die zu unterschiedlichen VoIP-Anrufen gehören, abgesehen davon, macht es keinen Sinn, sich Audiosignale anzuhören, welche ein Teil von bezugslosen Anrufen sind. Die Funktionalität, zur Auswahl freiwählbarer RTP-Ströme für eine nachfolgende Wiedergabe, ist einzig und allein für die manuelle Wiederherstellung eines Anrufs aus mehreren Strömen vorgesehen, für den Fall, dass keine SIP- oder H.323-Stammsitzungen verfügbar sind.

Nach Betätigung des Buttons **[Wiedergabe]** wird das Medienstrom-Player-Fenster geöffnet:



Zur Anzeige weiterer detaillierter Informationen über die Audioströme und zum Aufruf der manuellen Codec-Zuordnung, klicken Sie auf den Button mit dem Doppelpfeil. Für jeden RTP-Strom können Sie:

- Manuell einen Strom über die Zeit synchronisieren, z.B. einstellen der Startzeit für die Wiedergabe in Bezug zu anderen Strömen. Zur Durchführung, bewegen Sie das kleine Dreieck nach links oder rechts.
- Wählen Sie den korrekten Sound-Codec für jeden Ladungstyp der RTP-Ströme. In den meisten Fällen, wählt der Medienstrom-Player den richtigen Codec automatisch. Allerdings, wenn Sie mit verwaisten RTP-Strömen arbeiten denen die SIP- oder H.323-Stammsitzungen fehlen, dann werden Informationen über den richtigen Codec benötigt, den Sie dann manuell aus der Ausklappliste auswählen müssen. Wenn Sie es

schwierig finden, den richtigen Codec auszuwählen, klicken Sie auf den Button **[Versuchen zu erraten]** und der Medienstrom-Player wird selbst versuchen den Codec auszuwählen.

Hinweis: Es ist manchmal nicht möglich, den Ton von RTP-Strömen wiederzugeben, weil diese Ströme verschlüsselt sind, geschützte Codecs benutzen oder die Codecs von CommView nicht unterstützt werden.

Der **Lautstärkeregler** ermöglicht Ihnen die Einstellung der Lautstärke. Der Regler Jitter-Puffergröße erlaubt Ihnen einen Jitter-Puffer in VoIP-Endknoten zu simulieren, wie er in der realen Welt genutzt wird. Eine typische Jitter-Puffergröße ist 30 ms bis 50 ms. Eine Anhebung des Jitter-Puffers verbessert die Sprachqualität, erhöht aber auch die Wartezeit.

VoIP-Protokollbetrachter

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Protokollbetrachter ist ein Werkzeug zur Anzeige und Auswertung durch CommView und einigen Netzwerkanalysern von Drittherstellern erzeugter und erfasster Dateien. Er hat eine ähnliche Funktionalität wie der VoIP-Analyser, der Bestandteil des Programmhauptfensters ist; seine Zweckbestimmung ist die Analyse nach der Erfassung, z.B. lieber arbeiten mit Dateien als Pakete in Echtzeit erfassen. Für detaillierte Informationen, wie Sie mit diesem Werkzeug arbeiten, verweisen wir auf das Kapitel [Arbeiten mit dem VoIP-Analyser](#).

Klicken Sie auf **Datei => VoIP-Protokollbetrachter** um den VoIP-Protokollbetrachter zu öffnen. Sie können so viele VoIP-Protokollbetrachterfenster öffnen wie Sie möchten und jedes Fenster kann für die Analyse einer oder mehrerer erfasster Dateien benutzt werden.

Der VoIP-Protokollbetrachter kann durch CommView erfasste Dateien im NCF-Format laden, sowie andere durch Netzwerk-Analysen von Drittherstellern erzeugte Formate. Zusätzlich ist es möglich, [CommView-VoIP-Dateien \(NFV\)](#) in den VoIP-Protokollbetrachter zu laden.

VoIP-Protokollbetrachtermenü

CommView-Protokolle laden – Öffnet eine oder mehrere CommView-Erfassungsdateien.

Protokolle importieren – Ermöglicht Ihnen von anderen Paketanalysern erzeugte Erfassungsdateien zu importieren.

Bericht erzeugen – Generiert einen Übersichtsbericht der in den VoIP-Protokollbetrachter geladenen Daten und speichert diesen auf Ihre Festplatte. Wenn Sie einen Bericht generieren, werden die Einstellungen des [Berichtsbedienfeldes](#) im Hauptfenster des VoIP-Analyser benutzt.

VoIP-Daten leeren – Leert das aktuelle Fenster.

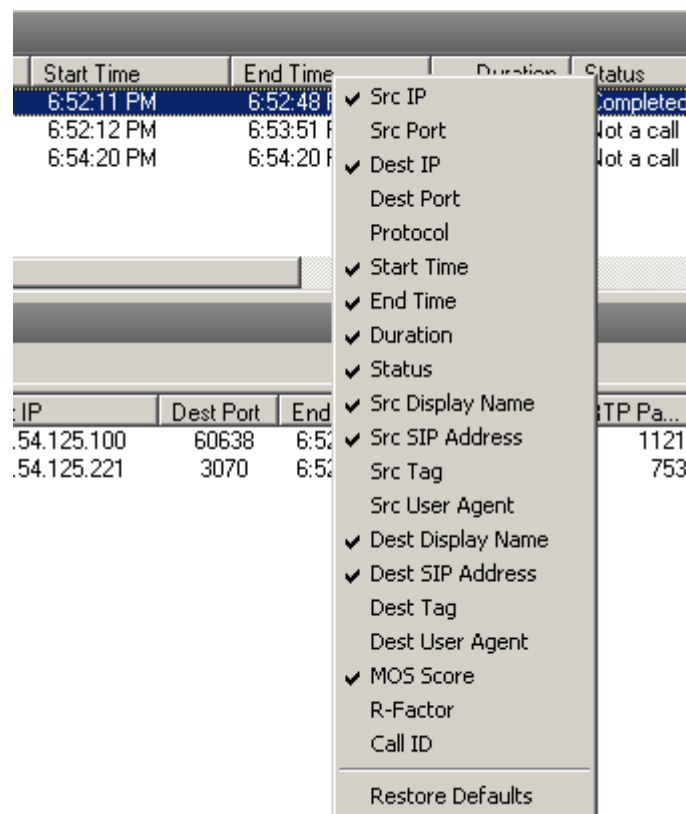
Fenster schliessen – Schließt das Fenster.

Arbeiten mit Auflistungen im VoIP-Analyser

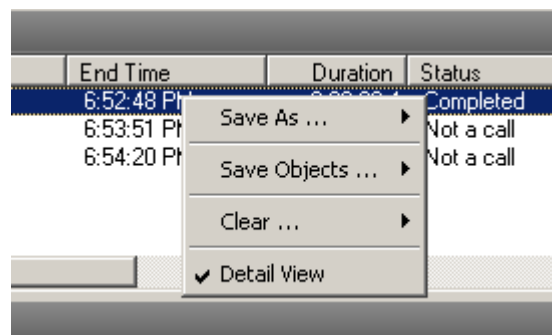
HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Weil die im VoIP-Analyser gezeigten Informationsauflistungen Daten verschiedener Arten beinhalten, wird der gemeinsame Stil und das gemeinsame Datenpresentationsprinzip dieser Listen unten erklärt.

Standardmäßig beinhaltet die Auflistung nur die meistgenutzten Datenfelder, während alle anderen Felder ausgeblendet werden. Zur Auswahl der Felder, die Sie angezeigt bekommen möchten, rechtsklicken Sie auf den Listenkopf und aktivieren/deaktivieren die zugehörigen Optionen. Es ist ebenso möglich, die Spaltenweite und die Reihenfolge der darzustellenden Datenfelder durch Ziehen mit der Maus einzustellen.



Rechtsklicken auf eine Liste öffnet ein Kontextmenü mit den folgenden Elementen:



Speichern als... – Exportiert alle oder ausgewählte Aufzeichnungen in eine Textdatei.

Objekt speichern... – Speichert alle oder ausgewählte Objekte in eine NVF-Datei. Für detaillierte Informationen über das NVF-Format, verweisen wir auf das Kapitel [NVF-Dateien](#).

Leeren... – Entfernt alle oder ausgewählte Objekte/Listen. Das Löschen von Stammobjekten führt auch zur Löschung der untergeordneten Objekte; z.B. bei der Löschung eines SIP-Anrufs, wird der zugehörige RTP-Strom des Anrufs ebenfalls von der **RTP-Stromauflistung** gelöscht.

Detailansicht – Wenn Sie mit einer Masterliste arbeiten, d.h. wenn mehr zugehörige Details des ausgewählten Objekts vorhanden sind, wird das Ein/Ausschalten dieser Option, das Programm veranlassen, die zugehörigen Details des Objekts Ein- bzw. Auszublenden. Z.B., die Auswahl **Detailansicht** in der **SIP-Sitzungsauflistung**, veranlasst das Programm detaillierte Informationen der ausgewählten SIP-Sitzung, wie die Anrufinformationsübersicht und zugehörige RTP-Ströme, ein- bzw. auszublenden.

NVF-Dateien

HINWEIS. Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser ermöglicht Ihnen ein oder mehrere VoIP-Datenobjekte in eine Containerdatei im NVF-Format zu speichern. Anders als gemeinsam erfasste Dateien, beinhaltet NVF keine erfassten Datenpakete. Stattdessen ist dies ein, in einer Einzeldatei gespeicherter Satz von VoIP-Objekten. NVF-Dateien sind hilfreich, wenn Sie einen VoIP-Anruf für eine spätere Analyse speichern möchten.

VoIP-Objekte, die in eine NVF-Datei gespeichert werden können, sind:

- **SIP-Sitzungen**
- **H.323-Sitzungen**
- **RTP-Ströme**

Um ein Objekt in eine NVF-Datei zu speichern, wählen Sie bitte ein oder mehrere Objekte in der VoIP-Analyserliste aus, führen einen Rechtsklick zur Öffnung des Kontextmenüs aus und wählen das Menüelement **Objekte speichern als...**

SIP- oder H.323-Sitzungen und zugehörige RTP-Ströme (wenn überhaupt) werden in eine Datei gespeichert. Wenn Sie jedoch nur den RTP-Strom zur Speicherung auswählen, wird die zugehörige SIP- oder H.323-Stammsitzung nicht mitgespeichert.

Sie können die gespeicherte NVF-Datei in das [VoIP-Protokollbetrachterfenster](#) laden.

Weiterführende Themen

Erfassung von intensivem Verkehr

Wenn Sie Daten aus einem grossen und stark benutzten Netzwerksegment erhalten, sollten Sie berücksichtigen, dass die Verarbeitung von tausenden Paketen/Sekunde durchaus die CPU-Auslastung erhöhen und das Programm träger reagieren kann. Zur Erhöhung der Programmpformance sollten Sie Regeln benutzen, um nichtbenötigte Pakete auszufiltern. Das Senden einer 50 MB grossen Datei zwischen zwei Maschinen innerhalb Ihres LANs erzeugt ungefähr 40.000 NetBIOS Pakete mit einem Datentransfervolumen von 10 MB/Sekunde, was doch eine starke Belastung für das Programm darstellen kann. Normalerweise brauchen Sie aber nicht jedes NETBIOS-Paket überwachen, so dass Sie CommView so konfigurieren könnten, dass es nur IP-Pakete erfasst. CommView bietet ein flexibles Filtersystem, mit dem Sie die Anwendung so feintunen können, dass sie nur die wirklich benötigten Pakete anzeigt. Wenn Sie nur statistische Funktionen brauchen (Histogramme, Kuchengrafiken, Hosttabellen) können Sie mittels des Menüs Paketausgabe unterbrechen die statistischen Informationen gewinnen, ohne eine Echtzeitanzeige zu benötigen.

Die Programmpformance wird verbessert durch:

- Eine schnelle CPU (Intel Core i7 wird empfohlen)
- RAM Größe (8 GB und mehr wird empfohlen)
- Die Verwendung von Filtern, zur Ausfilterung von unnötigem Verkehr.

Arbeiten mit mehreren Instanzen

Wenn mehrere Instanzen von CommView auf demselben Computer laufen, kann der Paketverkehr von mehreren Netzwerkadaptern gleichzeitig erfasst werden. Sie können diese Option aktivieren, durch Setzen der Checkbox **Mehrere Instanzen dieser Applikation zulassen**, unter **Einstellungen => Optionen => Verschiedenes**. Nehmen Sie zur Kenntnis, dass Sie mit zwei Instanzen von CommView nicht den Paketverkehr desselben Netzwerkadapters erfassen können. Der gleichen Limitierung unterliegen auch Terminal Server: Zwei Benutzer (ob lokal oder entfernt) können nicht den Paketverkehr desselben Netzwerkadapters erfassen, indem Sie zwei Instanzen von CommView auf demselben Server laufen lassen.

CommView im nichtsichtbaren Modus

Es gibt zwei Möglichkeiten CommView als versteckten Prozess laufen zu lassen:

1. Starten Sie CommView mit dem Switch hidden (verborgen), z.B.:

CV.EXE hidden

2. Wenn CommView bereits läuft können Sie mit es ein-/ausblenden, indem Sie einen Hotkey verwenden. Zum Ausblenden drücken Sie bitte die Tastenkombination **[ALT]+[SHIFT]+[h]**. Zum Einblenden hingegen **[ALT]+[SHIFT]+[u]**.

Vergessen Sie nicht, dass Sie Windows-Applikationen nicht vollständig verstecken können. Im unsichtbaren Modus kann man den CommView-Prozess immer noch im Task-Manager sehen.

Kommandozeilen Parameter

Bei laufendem Programm können Sie mit folgenden Kommandozeilenparameter bestimmte Aktionen starten lassen:

- Lade und aktiviere ein Regelset aus einer Datei. Verwenden Sie den Schalter /ruleset mit nachfolgendem Dateinamen und dem vollen Pfad, z.B.:

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

Wenn ein Dateiname oder dessen Pfad Leerzeichen enthält, muß dieser in Anführungszeichen (" ") gesetzt werden.

- Öffnen Sie ein Adapter und Starten die Paketerfassung. Verwenden Sie den Schalter /adapter gefolgt vom Namen des zu verwendenden Adapters, z.B.:

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

Der Adaptername muss in Anführungszeichen gesetzt werden. Da diese Namen tendenziell eher lang sind, können Sie diese aus der Adapterauswahlliste von CommView auswählen. Zum Kopieren des Adaternamens, wählen Sie diesen in der Adapterauswahlliste und kopieren ihn mit [Strg]+[C] über die Zwischenablage.

- Wählen Sie das ausgesuchte Verzeichnis für die Logdateispeicherung. Verwenden Sie den Schalter /logdir gefolgt vom vollen Pfad zur Datei, z.B.:

```
CV.EXE /logdir "C:\Program Files\CommView\Logs"
```

- Verbinden Sie zu einem oder mehreren Remote Agents. Benutzen Sie den Schalter "/ra" mit nachfolgender IP-Adresse oder Hostnamen des Remote Agents zu dem Sie sich verbinden möchten, gefolgt vom Passwort in Anführungszeichen und der zuüberwachenden Adapternummer (der Adapter-Index ist 1-basierend, z.B. wenn Sie das erste Adapter überwachen müssen, benutzen Sie die "1"), z.B.:

```
CV.exe /ra 192.168.0.5 "MeinPasswort" 1
```

Zur Verbindung zu mehreren Remote Agents aus derselben CommView-Instanz, stellen Sie bitte zunächst in den Optionen sicher, dass das mehrfache Starten von CommView nicht erlaubt wird und benutzen Sie dann eine Stapelverarbeitungsdatei ähnlich der folgenden:

```
START "CV" "C:\Program Files\CommView\CV.exe" /noprompt
PING 1.1.1.1 -n 1 -w 5000 >NUL
START "CV" "C:\Program Files\CommView\CV.exe" /ra 192.168.0.1 "pwd1" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START "CV" "C:\Program Files\CommView\CV.exe" /ra 192.168.0.2 "pwd2" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START "CV" "C:\Program Files\CommView\CV.exe" /ra 192.168.0.3 "pwd3" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
```

Dieses Script startet CommView, wartet 5 Sekunden um sichzustellen, dass die Applikation geladen wurde (wir benutzen das Kommando PING zum pausieren, da es keine Möglichkeit gibt, in einer BAT-Datei eine

Pause zu programmieren), dann übergeben wir der Applikation die IP-Adresse, Passwörter und Adapternummern von 3 Remote Agents (mit 1-Sekunden-Pausen).

Sie können alle diese Parameter gleichzeitig anwenden, ausgenommen den letzten Parameter.

Datenaustausch mit Ihrer Anwendung

CommView bietet ein einfaches TCP/IP-Interface, das es Ihnen ermöglicht von CommView empfangene Pakete zu verarbeiten, während Sie gleichzeitig Ihre eigene Applikation in Echtzeit verwenden. Ab Version 5.0 können Sie mit diesem Interface auch Pakete senden (analog zur Paketgeneratorfunktion in CommView).

Nehmen Sie zur Kenntnis, dass sich das Datenformat im Vergleich zu älteren CommView-Versionen wesentlich verändert hat. Der TS-Schalter wurde aufgehoben da alle Paketinformationen inklusive dem Zeitstempel nun im Header enthalten sind.

So geht das

CommView sollte mit dem speziellen Kommandozeilenargument MIRROR gestartet werden. Dieses fordert das Programm auf empfangene Pakete an eine bestimmte IP-Adresse und einen TCP-Port Ihrer Wahl zu spiegeln.

Beispiele:

```
CV.EXE mirror:127.0.0.1:5555 // spiegelt die Pakete in die Loopbackadresse, TCP Port 5555
```

```
CV.EXE mirror:192.169.0.2:10200 // spiegelt die Pakete nach 192.169.0.2, TCP Port 10200
```

Wenn CommView mit einem solchen Schalter gestartet wurde, versucht es eine TCP-Session durch Verbinden zu der definierten IP- Adresse bzw. Portnummer zu generieren. Das bedeutet, dass Sie bereits die Anwendung laufen lassen und einen bestimmten Port abhören lassen. Wenn CommView keine Verbindung erzeugen kann, versucht das Programm alle 15 Sekunden eine Neuverbindung herzustellen. Dies geschieht auch bei einem Verbindungsabbruch. Auch hier versucht CommView alle 15 Sekunden eine Neuverbindung herzustellen. Wenn diese Verbindung erfolgreich hergestellt wurde sendet CommView die gesammelten Pakete in Echtzeit zu dieser definierten IP-Adresse.

Daten Format

Die Daten werden im NCF-Format übertragen. Mehr dazu unter [CommView Logdateiformat](#).

Senden von Paketen

Pakete können von Ihrer Anwendung nicht nur empfangen, sondern auch mittels des Paketgenerators gesendet werden. Dabei sendet CommView die Daten über dieselbe TCP-Verbindung, über die Sie auch die Daten erhalten. Das Datenformat ist einfach. Sie sollten die Paketlänge (2 Byte lange unsigned Integer in little-endian Standardreihenfolge) und danach das Paket selbst senden. Wenn der Adapter nicht geöffnet wurde oder keine Paketinjection erlaubt, wird das Paket ohne Hinweis verworfen.

Beispielprojekte

Zwei einfache Demoanwendungen, die auf eingehende Verbindungen hören extrahieren Pakete aus dem Stream und zeigen sofern vorhanden die Rohdaten.

http://www.tamos.com/products/commview/samp_mirr_c5.zip. Dies ist ein Visual Studio Projekt mit C++ Quellcode.

http://www.tamos.com/products/commview/samp_mirr_d5.zip. Dies ist ein Delphi-Projekt mit Pascal Sourcecode. Wenn Sie das Projekt kompilieren wollen benötigen Sie die bekannten ICS-Komponentensuite von Francois Piette, erhältlich unter <http://www.overbyte.be>.

Bandbreite

Wenn Sie Daten auf einem entfernten Computer spiegeln, sollten Sie sicherstellen, dass der Link zwischen CommView und dem Ziel der Spiegelung schnell genug ist, um die empfangenen Daten zu transportieren. Wenn CommView 500 KBytes/sec empfängt und Ihr Link nur 50 KBytes/sec versenden kann, werden Sie zwangsläufig einen Datenstau bekommen, der verschiedene Probleme erzeugen kann. Z. B. könnte Winsock bei einigen Windowsversionen aufhören Daten zu senden. Wenn Sie in diesem Zusammenhang eine flexiblere Lösung suchen, die Smart Buffering und Remote Control unterstützt, sollten Sie die Verwendung des [CommView Remote Agent](#) in Betracht ziehen.

Maßgeschneidertes Decoding

CommView ermöglicht die Verwendung von zwei selbstdefinierten Decoder-Arten:

Einfacher Decoder

Wenn Sie diesen Decodertyp wählen wird die Decoder-Ausgabe in einer Extraspalte im Register **Pakete** angezeigt. Der Decoder sollte dabei eine 32-bit DLL-Datei namens "Custom.dll" sein, die nur eine Prozedur namens "Decode" exportiert. Der Grundtyp dieser Prozedur wird im folgenden für C und Pascal gezeigt:

```
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;
```

Die DLL muß sich dabei im CommView Installationsverzeichnis befinden. Beim Start von CommView sucht es nach der Custom.dll im Installationsverzeichnis und lädt diese in den Speicher. Wenn der Eingangspunkt für Decode gefunden wurde, fügt CommView eine neue Spalte namens Custom (Selbstdefiniert) der Paketliste hinzu.

Wird ein neues Paket empfangen und angezeigt, ruft CommView die Decode-Prozedur auf und gibt die Paketinhalte an die DLL weiter. Die Decode-Prozedur muß nun die Paketinformation verarbeiten und kopiert dann das Ergebnis in den Puffer. Das erste Argument ist der Paket-Pointer zu den Paketdaten, das zweite Argument die Datenlänge und das dritte Argument der Pointer zum Puffer, in den die Ergebnisse des Decodings kopiert werden sollen. Das vierte Argument ist die Puffergröße (derzeit stets 1024 Bytes). Der gesamte Puffer ist für CommView zugeteilt und freigegeben. Sie sollten nicht versuchen diese Zuteilung zu ändern. Das in den Speicher kopierte Ergebnis wird dann als String in der Spalte Custom angezeigt.

Ihre Prozedur sollte schnell genug sein um tausende von Paketen/Sekunde zu verarbeiten. Sonst wird die Anwendung unnötig langsam. Bitte halten Sie sich auch an die Konvention STDCALL.

Zwei Demo-DLL's sind verfügbar. Sie zeigen eine einfache Operation. Die Ausgabe der Decode-Funktion ist der Hexcode der letzten Byte des Paketes. Ihr eigener Decoder kann natürlich beliebig komplex sein:

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Dies ist ein Visual Studio Projekt mit C++ Quellcode.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Dies ist ein Delphi-Project mit Pascal Sourcecode.

Komplexer Decoder

Bei der Verwendung dieses Decodertypes wird die Decoderausgabe als zusätzliche Objekte im Paketdecoderbaum angezeigt. Mehr zur Implementation dieses Decoders erhalten Sie durch das Herunterladen folgender Datei:

http://www.tamos.com/products/commview/complex_decoder_c7.zip

Diese Decoderart kann nur in Microsoft Visual C++ geschrieben werden, da es mit C++ erzeugte Klassen benutzt.

Technischer Support

Technischen Support für maßgeschneiderte Decoder gibt es auf der Basis von "Besten Ergebnissen". Wir sind leider nicht in der Lage auf Ihre Programmierfragen einzugehen.

CommView Logdateien Format

CommView und CommView for WiFi verwenden das unten beschriebene Datenformat um empfangene Pakete als NCF-Datei abspeichern zu können. Dies ist ein offenes Datenformat, das Sie zur Verarbeitung von Logdateien verwenden können, aber auch für den direkten Datenaustausch mit Ihrer Applikation. Dies ist in der Hilfedatei beschrieben.

Die Pakete werden nacheinander aufgenommen. Ein 24-Byte-Header, der unten beschrieben wird, geht jedem Paket voran. Alle Header-Felder, die länger als 1 Byte sind, verwenden sogenannte Little-endian-Bytefolgen.

Feldname	Länge (Bytes)	Beschreibung															
Datenlänge	2	Die Länge des Paketkörpers nach dem Header															
Ausgangsdatenlänge	2	Originallänge des Paketkörpers nach dem Header (ohne Kompression). Wenn keine Kompression benutzt wurde, ist der Wert identisch mit dem aus dem vorherigen Feld.															
Version	1	Paketformat Version (0 für die aktuelle Implementation)															
Jahr	2	Paketdatum (Jahr)															
Monat	1	Paketdatum (Monat)															
Tag	1	Paketdatum (Tag)															
Stunden	1	Paketzeit (Stunden)															
Minuten	1	Paketzeit (Minuten)															
Sekunden	1	Paketzeit (Sekunden)															
Microsekunden	4	Paketzeit (Microsekunden)															
Flags	1	Bitflags: <table border="1" data-bbox="571 1473 1401 2011"> <tbody> <tr> <td>Medium</td> <td>0...3</td> <td>Mediumtyp für das Paket (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td> </tr> <tr> <td>Entschlüsselt</td> <td>4</td> <td>Das Paket wurde entschlüsselt (nur für WiFi Pakete anwendbar)</td> </tr> <tr> <td>beschädigt</td> <td>5</td> <td>Das Paket ist beschädigt, z.B. ein falscher CRC-Wert (nur für WiFi-Pakete)</td> </tr> <tr> <td>Komprimiert</td> <td>6</td> <td>Das Paket wurde komprimiert abgespeichert</td> </tr> <tr> <td>Reserviert</td> <td>7</td> <td>Reserviert</td> </tr> </tbody> </table>	Medium	0...3	Mediumtyp für das Paket (0 - Ethernet, 1 - WiFi, 2 - Token Ring)	Entschlüsselt	4	Das Paket wurde entschlüsselt (nur für WiFi Pakete anwendbar)	beschädigt	5	Das Paket ist beschädigt, z.B. ein falscher CRC-Wert (nur für WiFi-Pakete)	Komprimiert	6	Das Paket wurde komprimiert abgespeichert	Reserviert	7	Reserviert
Medium	0...3	Mediumtyp für das Paket (0 - Ethernet, 1 - WiFi, 2 - Token Ring)															
Entschlüsselt	4	Das Paket wurde entschlüsselt (nur für WiFi Pakete anwendbar)															
beschädigt	5	Das Paket ist beschädigt, z.B. ein falscher CRC-Wert (nur für WiFi-Pakete)															
Komprimiert	6	Das Paket wurde komprimiert abgespeichert															
Reserviert	7	Reserviert															

Signallevel	1	Signallevel in Prozent (nur für WiFi Pakete anwendbar)
Übertragungsrate	1	Datenübertragungsrate in Mbps mal 2 (nur für WiFi Pakete anwendbar)
Band	1	Übertragungsbandbreite. 0x01 für 802.11a, 0x02 für 802.11b, 0x04 für 802.11g, 0x08 für 802.11a-turbo, 0x10 für 802.11 SuperG, 0x20 für 4.9 GHz Public Safety, 0x40 für 5 GHz 802.11n, 0x80 für 2.4 GHz 802.11n (nur für WiFi-Pakete anwendbar)
Kanal	1	Kanalnummer (nur für WiFi Pakete anwendbar)
Richtung	1	Paketrichtung. 0x00 bei Pass-through, 0x01 bei Inbound, 0x02 bei Outbound (nicht für WiFi-Pakete anwendbar)
Reserviert	2	Reserviert
Signalstärke (dBm)	1	Signalstärke in dBm (nur für WiFi-Pakete anwendbar)
Geräuschstärke (dBm)	1	Geräuschstärke in dBm (nur für WiFi-Pakete anwendbar)
Daten	...	Paketkörper (unmodifiziert, so wie es über das Medium übertragen wurde). Wenn das Kompressionsflag gesetzt wurde, werden die Daten mittels der öffentlich zugänglichen Zlib 1.1.4 Library komprimiert. Die Länge dieses Feldes wird unter "Datenlänge" aufgezeichnet.

Die Headergesamtlänge ist 24 Byte.

Wenn Pakete komprimiert gespeichert werden enthält das Feld Datenlänge die Länge nach der Kompression, während die Ausgangslänge die Originallänge beschreibt. Bei unkomprimierten Paketen sind die Werte identisch.

Einkauf und Support

Das Programm ist eine 30-Tage-Probeversion. Sie können eine vollfunktionierende, nicht eingeschränkte Version des Programms über unsere Webseite kaufen. Zwei Lizenztypen sind gegenwärtig für CommView verfügbar: **Standard** und **VoIP**. Die teure **VoIP**-Lizenz aktiviert alle Applikationsfunktionen, inklusive des VoIP-Analysers; indem die **Standard**-Lizenz hat keinen VoIP-Analyser.

Überprüfen Sie unsere [Webseite](#) für die Einzel-Anwender- und Mehrfachanwenderlizenpreise. Eine lizenzierte Kopie von CommView kann von einer Einzelperson, auf einem Computer persönlich genutzt werden. Eine zweite Kopie kann auf einem zusätzlichen mobilen Computer installiert werden. Schauen Sie bitte für detaillierte Beschreibungen unserer Lizenzrichtlinien in das Endanwenderlizenzenabkommen, welches während der Installation eingeblendet wird.

Als registrierter Benutzer erhalten Sie:

- Eine vollfunktionale, unbeschränkte Ausgabe der Software
- Kostenlose Updates innerhalb eines Jahres nach Kaufdatum
- Informationen über Updates und neue Produkte
- Kostenlosen technischen Support

Wir akzeptieren Bestellungen über Kreditkarte, telefonische und Faxbestellungen, Schecks und Überweisung. Preise, Definitionen und Konditionen können sich ändern, überprüfen Sie daher unsere Webseite auf die neuesten Produktangebote und Preise.

<http://www.tamosoft.de/order/>

Für technischen Support, besuchen Sie bitte <http://www.tamosoft.de/support/>