CommView Remote Agent

User Manual

Copyright © 2001-2002 TamoSoft, Inc.

Einleitung

Über den CommView Remote Agent

Der CommView Remote Agent ist eine Applikation die es CommView Benutzern erlaubt, den Netzwerkverkehr "aus der Ferne" (engl. Remote) zu betrachten bzw. zu erfassen. Dies ist möglich unabhängig vom physikalischen Standort des PC's des CommView Benutzers und des PC's der mit dem Remote Agent ausgerüstet ist. Diese neue und einzigartige Technologie erweitert Ihren Horizont: Sie sind nicht mehr länger durch die Grenzen Ihres LAN Segmentes oder Ihres PC's limitiert. Wenn Sie in Tokyo sind können Sie ohne weiteres eine Software Installation in Amsterdam untersuchen. Wenn Sie den Remote Agent auf dem Zielsystem installiert haben, können Sie in Ihrer gewohnten Arbeitsumgebung den TCP/IP Verkehr des Zielsystems erfassen, also ob sie vor Ort wären!

Nach der Installation und einer einfachen Konfiguration ist der Remote Agent bereit um eine Verbindung von CommView zu akzeptieren. Wenn Sie die Verbindung hergestellt und sich authentifiziert haben, ist der Remote Agent bereit Pakete vom Ziel-Netzwerksegment zu erfassen und sie zum CommView PC zu senden. Die übermittelten Datenpakete sind komprimiert um die Netzwerkbandbreite nicht zu stark zu belasten und sie sind verschlüsselt um eine sichere Übertragung durch unbekannte Kanäle zu gewährleisten. CommView hat ein flexibles Filtersystem, dass das Herausfiltern aller nicht interessierenden Pakete erlaubt und so ebenfalls zur Reduktion der Belastung der Netzwerkbandbreite zwischen CommView und dem Remote Agent beiträgt.

Der CommView Remote Agent ist für Netzwerk-, Software- und Sicherheitsprofis ein unentbehrliches Werkzeug, dass zur Lösung eines grossen Bereiches von Problemen wie dem Analysieren von Multisegment LAN's oder der Fehlerbehebung bei Netzwerksoftware beitragen kann.

Der CommView Remote Agent kann auf Systemen mit Windows 95/98/ME/NT/2000/XP installiert werden. Voraussetzung ist eine Ethernet oder Wireless Ethernet Karte, welche den NIS 3.0 Standard unterstützt oder ein Standart Modem.

Was ist neu

Version 1.1

- Dies ist ein Wartungsrelease zur Behebung bekannter Probleme aus dem vorgangigen Release und zur Verbesserung der .NET Kompatibilitat. Des weiteren wird mit diesem Release der Treiber aktualisiert um die Kompatibilitat mit CommView und weiteren Produkten zu gewahrleisten.

Lizenzübereinkommen

Bitte lesen sie das folgende Lizenzübereinkommen genau durch bevor sie diese Software verwenden. Die Verwendung dieser Software bedeutet, dass sie das Lizenzübereinkommen akzeptieren. Wenn Sie mit diesem Lizenzübereinkommen nicht einverstanden sind müssen Sie diese Software von Ihrem System entfernen und die Verwendung dieser Software unterlassen.

Copyright (Kopierrecht)
Diese Software ist kopierrechtlich geschützt durch 1999-2001 TamoSoft Inc. CommView ist ein Warenzeichen von TamoSoft Inc. Der Gebrauch und der Kopierschutz dieser Software ist durch internationale Kopierrechte geregelt. TamoSoft behält den Titel und die vollen Rechte an dieser Software und der zugehörigen Dokumentation. Die Benutzerlizenz gibt kein Anrecht auf das geistige Eigentum von TamoSoft Inc. Sie sind nicht berechtigt den Registriercode weiterzugeben, weder auf Papier noch elektronisch noch in irgend einer anderen Form.

Evaluationsversion (Evaluation Version)
Diese Software ist nicht Freeware. Sie werden hiermit berechtigt diese Software zu Evaluationszwecken für eine Zeitdauer von 30 Tagen kostenlos zu verwenden. Diese Software nach Ablauf der Evaluationszeit von 30 Tagen zu verwenden ist eine Verletzung der Kopierrechte und kann strafrechtliche Folgen nach sich ziehen.

Registrierte bzw. lizenzierte Version (Registered Version)
Eine registrierte Kopie dieser Software berechtigt Sie zur Installation und Verwendung eben dieser auf einem Computer. Wenn sie dieses Programm auf mehreren Computern installieren und Verwenden wollen, müssen sie eine Lizenz für mindestens diese Anzahl von Computern bestellen.

Disclaimer (Ablehnungshinweis)

DIESE SOFTWARE WIRD OHNE IRGEND EINE ART VON GARANTIE FÜR IRGEND EINEN BESTIMMTEN ZWECK (OB EXPLIZIT ERWÄHNT ODER IMPLIZIT ENTHAHLTEN) AUSGELIEFERT. IN KEINEM FALL WIRD TAMOSOFT INC. FÜR IRGEND EINE ART VON SCHADEN HAFTEN, DER DURCH DEN GEBRAUCH DIESER SOFTWARE VERURSACHT WURDE, SELBST WENN DIE MÖGLICHKEIT DAFÜR ERWÄHNT WURDE. SIE BESTÄTIGEN MIT DEM GEBRAUCH DER SOFTWARE, DASS SIE DIESES LIZENZÜBEREINKOMMEN GELESEN UND VERSTANDEN HABEN UND SEINEN INHALT ALS VERBINDLICH AKZEPTIEREN.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL TAMOSOFT, INC. BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS.

Rechtliche Grundlage (Governing Law)
Dieses Übereinkommen basiert auf den Rechtsgrundlagen der Republik von Zypern.

Verteilung (Distribution)
Diese Software darf nur in ihrer originalen, nicht veränderten und nicht registrierten Form frei vertrieben werden. Die Distribution muss alle Files der original Distribution enthalten. Distributoren (Vertreiber) dürfen keine Gebühr für diese Weiterverteilung verlangen. Jedermann der diese Software weiter vertreiben will, muss uns um ausdrückliche Erlaubnis bitten.

Einschränkungen (Other Restrictions)
Das Modifizieren, Reversen, Dekompilieren oder Disassemblieren dieser Software auf irgend eine Art und Weise, inklusive dem Verändern oder Entfernen von Fenstern oder Nachrichten ist nicht erlaubt.

Windows ist ein registriertes Warenzeichen der Microsoft Corporation. Alle anderen Warenzeichen sind Eigentum der betreffenden Besitzer dieser Warenzeichen.

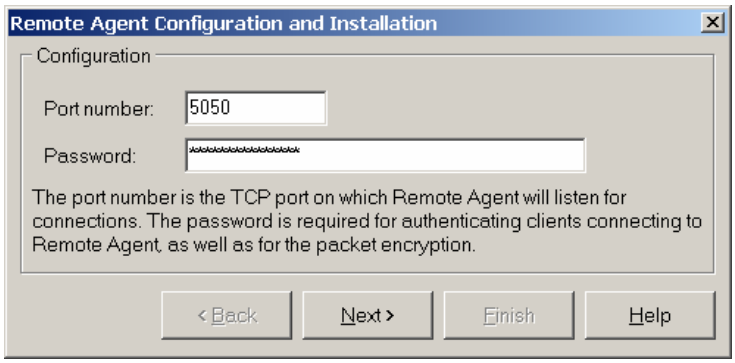
Die Benutzung von CommView Remote Agent

Installation und Konfiguration

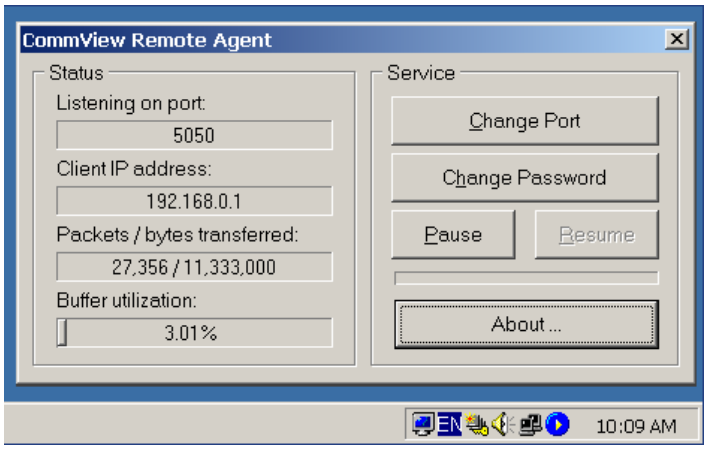
Der CommView Remote Agent muss auf dem Ziel-PC installiert werden, dessen Pakete Sie "aus der Ferne" (remote) erfassen möchten. Wie CommView kann der Remote Agent den gesamten Netzwerkverkehr der durch seine Netzwerkkarte (engl. network interface card, kurz NIC) oder durch sein Modem (engl. dial-up adapter) geht erfassen. Der Remote Agent kann auf einem LAN Teilnehmer PC oder auf einem Stand-Alone PC installiert werden. Unter Windows NT/2000/XP müssen Sie in jedem Fall Administrator Rechte besitzen damit Sie den Remote Agent installieren können, auch wenn diese nach der erfolgreichen Installation und Konfiguration nicht mehr erforderlich sind. Sie sollten CommView und den Remote Agent NICHT auf dem selben PC installieren, da dies absolut keinen Sinn macht.

Konfiguration des Programms

Um das Programm zu installieren, starten sie SETUP.EXE und folgen Sie den Instruktionen. Nachdem die Files in das Zielverzeichnis auf Ihrem PC kopiert worden sind, erscheint ein Fenster zur Definition von Grundangaben. Sie müssen eine TCP Port Nummer (Default 5050) und ein Passwort wählen. Über die Port Nummer wird die Kommunikation mit CommView laufen. Das Passwort wird zur Authentifikation bei der Verbindungsaufnahme mit dem CommView Remote Agent und für die Ver- und Entschlüsselung der übertragenen Datenpakete verwendet. Wählen Sie ein langes und sicheres Passwort, verwenden Sie Gross-/Kleinschreibung. Sollte jemand Ihr Passwort herausfinden, ermöglicht dies den Zugriff auf den PC auf welchem der CommView Remote Agent installiert ist und damit Zugriff auf Ihr Netzwerkverkehr!



Klicken Sie auf **Next** um fortzufahren bzw. um die notwendigen Treiber zu installieren und anschliessend den CommView Remote Agent zum ersten Mal zu starten. Das Programm Icon sollte im System Tray unten rechts erscheinen. Klicken Sie auf das Icon um das Hauptfenster der Applikation sichtbar zu machen:



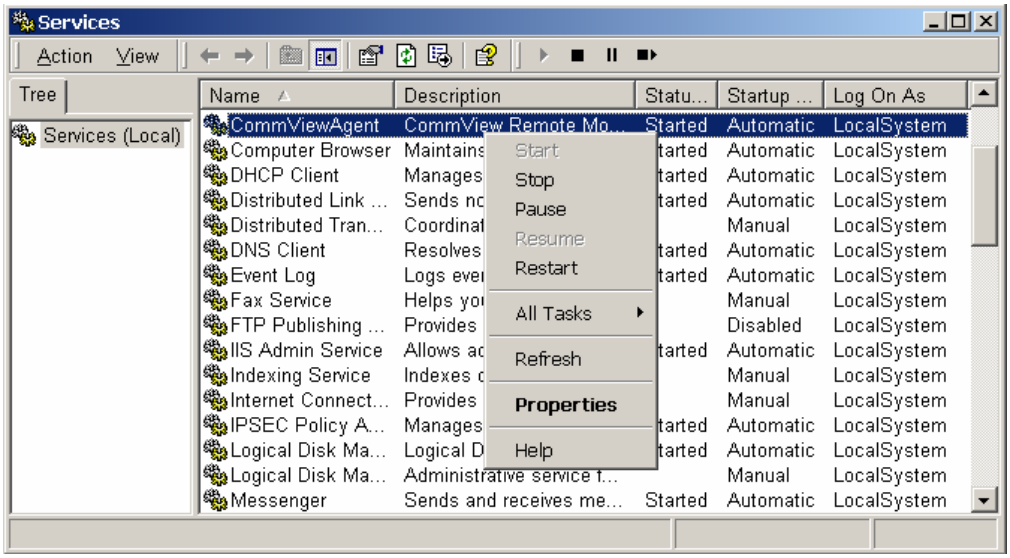
Der **Status** Bereich zeigt den aktuellen Zustand des Programmes: Die Port Nummer auf welcher der CommView Remote Agent eine Verbindungsaufnahme von CommView Clients erwartet, die IP Nummer eines CommView Clients der Verbunden ist, die Paketübertragungsstatistik, die Buffer Ausnutzung. Der **Service** Bereich hat mehre Knöpfe zur Programmkonfiguration. Klicken Sie auf **Change Port** um die Port Nummer für die Kommunikation mit den CommView Clients zu ändern. Klicken Sie auf **Change Password** um das Passwort zu wechseln. Sie können die Remote Agent Aktivität temporär stoppen (**Pause**) oder wieder aufnehmen (**Resume**). Allgemeine Programminformationen werden durch Klicken auf den **About** Knopf angezeigt.

Nehmen Sie zur Kenntnis, dass der CommView Remote Agent nur die Verbindung zu einem CommView Client gleichzeitig akzeptiert.

Kontrolle des Programms

Der CommView Remote Agent ist eine **NT Service Application** . Das bedeutet dass er nach dem Booten des Computers automatisch gestartet wird, auch wenn kein Benutzer in das System eingeloggt ist. Wie jede andere Service Applikation kann der

CommView Remote Agent via Control Panel => Administrative Tools => Services konfiguriert werden. Sie können dort auch den sog. Start-Up Mode (automatic/manual) ändern sowie den CommView Remote Agent stoppen etc. (stop/start/pause/resume).



Unter Windows 95/98/ME simuliert der CommView Remote Agent eine Service Applikation bzw. verhält sich wie eine NT Service Applikation. Das bedeutet im Wesentlichen, dass er unabhängig von Benutzern die sich ein- und ausloggen nach dem Booten des PC's gestartet wird und bereit ist.

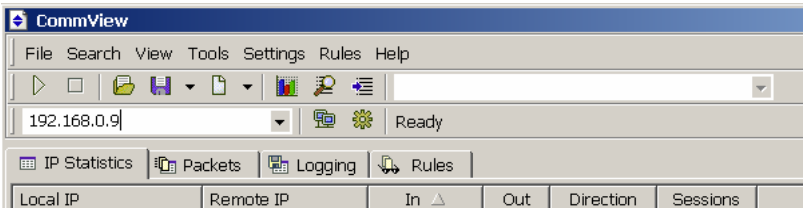
Zur einfacheren Handhabung des Services haben wir ein Tool zum Starten etc. (stop/start/pause/resume) integriert. Dieser sog. Service Indicator ist in der CommView Remote Agent Programm Gruppe unter Start => Programs => CommView Remote Agent => Service Indicator zu finden.

Datenverkehr erfassen

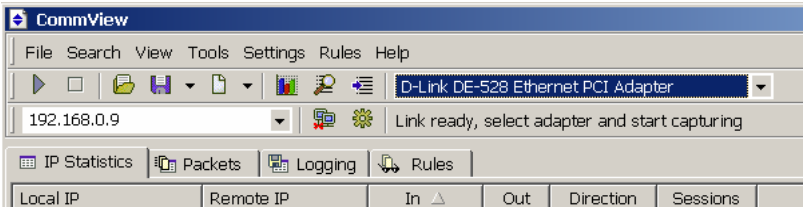
Dieses Kapitel beschreibt wie Sie CommView mit dem CommView Remote Agent verbinden um den Datenverkehr eines LAN's "aus der Ferne" zu analysieren. Um den Datenverkehr dieses entfernten LAN's zu erfassen müssen Sie auf einem Host an diesem LAN den CommView Remote Agent installiert und aktiviert haben und Sie müssen auf Ihrem Computer CommView gestartet haben. Wir setzen voraus, dass der CommView Remote Agent auf dem Host installiert wurde und läuft (Sie finden zu diesem Thema im vorherigen Kapitel detaillierte Informationen) und dass Sie im Umgang mit CommView gute Kenntnisse haben. Wenn Sie mit CommView keine Erfahrung haben, laden Sie es bitte herunter und eignen Sie sich gute CommView Kenntnisse an, bevor Sie sich mit dem CommView Remote Agent auseinander setzen.

CommView mit dem CommView Remote Agent verbinden

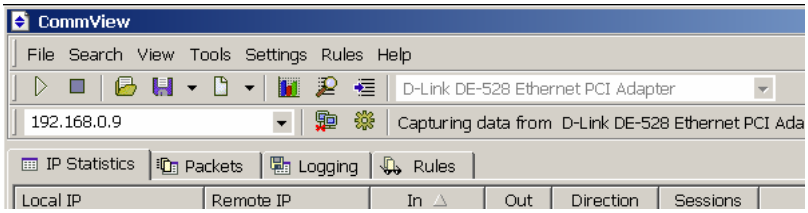
CommView kennt zwei Betriebszustände (engl. Mode) bezüglich der Paketerfassung: Die lokale und die remote (Remote Agent) Paketerfassung. Um auf den "remote Erfassungs" Mode umzuschalten klicken Sie auf **File => Remote Monitoring Mode**. Eine weitere Toolbar im Hauptfenster wird erscheinen. Geben Sie die IP Adresse des Computers, auf welchem der Remote Agent läuft, in das entsprechenden Eingabefeld ein und klicken Sie auf **Connect**. Wenn Sie sich hinter einer Firewall oder einem Proxy Server befinden oder einen nicht üblichen Remote Agent Port verwenden, müssen Sie unter **Network Settings** die Port Nummer und die SOCKS5 Proxy Server Einstellungen anpassen.



Nach dem Drücken von **Connect** wird ein Passwort Eingabefenster erscheinen. Geben Sie das Remote Agent Passwort ein und die Verbindung wird hergestellt. Sie werden dann eine *Link Ready* Nachricht sehen und die Netzwerkadapter Liste wird alle Adapter des Zielcomputers enthalten.



Es ist nun der beste Moment um die Regeln (im **Rules** Fenster) festzulegen. Es ist sehr wichtig Regeln zur Reduktion des Datenverkehrs zwischen CommView und dem Remote Agent zu definieren, um die Bandbreite der Verbindung nicht zu überschreiten, da sonst grössere Verzögerungen in der Anzeige auftreten können. Versuchen Sie alle nicht interessierenden Pakete heraus zu Filtern (mehr dazu folgt in diesem Kapitel). Wenn Sie für die Paketerfassung bereit sind, klicken Sie auf **Start Capture**.



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 **Stop Capture**. Dann können Sie entweder einen anderen Adapter wählen oder die Verbindung zum Remote Agent durch Klicken auf **Disconnect** stoppen. Um zum Mode für die lokale Paketerfassung zurück zu kehren, klicken Sie wieder auf **File => Remote Monitoring Mode**. Die zusätzliche Remote Agent Toolbar wird verschwinden.

Der effiziente Einsatz des CommView Remote Agent

Wir möchten Sie darauf hinweisen, den Erfassungsregeln (capturing rules) auf der **Rules** Seite im Hauptfenster besondere Beachtung zu schenken. Die Bandbreite der Netzwerkverbindung zwischen CommView und dem CommView Remote Agent hat Grenzen, besonders wenn der CommView Remote Agent auf einem Host bzw. LAN arbeitet, welches bereits stark belastet ist. Es kann dann passieren, dass die verbleibende Bandbreite durch den CommView Remote Agent aufgebraucht wird, weil dieser versucht alle erfassten Pakete an CommView zu senden. Es ist daher ausserordentlich wichtig, dass Sie die Filterregeln sorgfältig bestimmen, damit das zu untersuchende Netzwerk bzw. der Kanal der CommView mit dem CommView Remote Agent verbindet nicht überlastet wird. Wenn Sie CommView zum Beispiel via einem T1 oder T3 Kanal (das entspricht 1.5 bzw. 4.5 MB/s) mit dem CommView Remote Agent verbinden und der remote Computer (mit dem CommView Remote Agent) an einem stark belasteten

100MB/s LAN angeschlossen ist, beträgt die Bandbreite des Verbindungskanals einen Bruchteil der Remote Agent LAN Bandbreite, was es verunmöglicht alle vom CommView Remote Agent erfassten Pakete zum CommView PC zu senden.

Wenn der CommView Remote Agent mehr Pakete erfasst als er zu CommView senden kann, wird ein interner Buffer zur Zwischenspeicherung der Pakete verwendet, welche nicht unmittelbar zu CommView gesandt werden können. Die Buffergrösse beträgt 5Mbytes. Die **Buffer utilization** (Buffer Ausnutzung) Anzeige des CommView Remote Agent gibt die jeweils aktuelle Ausnutzung dieses Buffers an. Wenn also 2.5Mbytes Pakete zwischen gespeichert werden, wird die **Buffer utilization** 50% anzeigen. Wenn die Buffer Ausnutzung 100% erreicht, werden keine weiteren Pakete mehr zwischen gespeichert, bis wieder Bufferspeicher frei wird. Diese Pakete die nicht zwischen gespeichert werden können, gehen verloren. Um diesen Fall zu verhindern, sollten Sie die Erfassungsregeln (capturing rules) auf der **Rules** Seite im Hauptfenster von CommView besonders sorgfältige bestimmen.

Security (Sicherheit)

Sicherheit war bei der Entwicklung des CommView Remote Agent ein wichtiges Kriterium. Der Zugriff ist nur über ein Passwort möglich, das nie als reiner Text übertragen wird, sondern das mit einem "challenge-response" Protokoll und einer Hash Funktion gesichert wird. Wenn die Authentifizierung erfolgreich war, wird der gesamte Datenverkehr komprimiert und dann mit diesem Passwort verschlüsselt. Bitte treffen Sie Vorkehrungen um das Passwort geheim zu halten. Eine nicht autorisierte Person wäre mit diesem Passwort in der Lage Ihr Netzwerk via CommView Remote Agent im grossen Umfang zu studieren und Daten zu entwenden!

Informationen

Bestellen von CommView Remote Agent

Dieses Programm ist ein Evaluationsversion mit einer Laufzeit von 30 Tagen. Folgend sehen Sie die Preise für eine voll funktionsfähige Version ohne Restriktionen:

Lizenz	**Preis, US$**
1 Computer	149
5 Computer	499
10 Computer	799

Bitte nehmen Sie zur Kenntnis, dass der CommView Remote Agent **per Computer und nicht per Benutzer** lizenziert wird. Eine Einzellizenz berechtigt Sie den CommView Remote Agent auf einem Computer zu installieren und einzusetzen. Wenn Sie das Programm auf mehreren Computern installieren bzw. einsetzen möchten, müssen Sie eine Lizenz für mehrere Computer bestellen. Sie benötigen des weiteren mindestens eine lizenzierte CommView Kopie, damit sie ein Verbindung zu einem CommView Remote Agent erstellen können.

Als registrierter Benutzer erhalten Sie:

- Voll funktionsfähige Kopie dieser Software ohne Restriktionen.
- Updates die innerhalb eines Jahres vom Bestelldatum an erscheinen kostenlos.
- Informationen über Updates und neue Produkte.
- Kostenloser technischer Support

Wir akzeptieren Bestellungen mit Kreditkarte, Bestellungen via Telephon und FAX. Bezahlung mit Checks, Bezahlung auf Rechnung oder via Banktransfer ist möglich. Preise und Bedingungen können jederzeit ohne Benachrichtigung ändern. Bitte besuchen Sie unsere Webseite für die aktuellen Produkte, Preise und Bedingungen.

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

Kontaktieren Sie uns

Web

http://www.tamos.com (US Server)

http://www.tamosoft.com (UK Server)

E-mail

sales@tamos.com (Verkaufsfragen)
support@tamos.com (Alle anderen Fragen)

Adresse und Fax

Adresse:

PO Box 1385
Christchurch 8015
New Zealand

Fax: +643 359 0392 (New Zealand)
Fax: +1 503 213-7764 (USA)

Weiter Produkte von TamoSoft

CommView

CommView ist ein Programm zur Aufzeichnung von Local Area Network (LAN) Aktivitäten. CommView ist in der Lage Datenpakete welche durch eine Einwahlverbindung via Modem oder Ethernet Karte gehen zu erfassen und diese zu analysieren bzw. decodieren. CommView erstellt ein Liste der Netzwerkverbindungen sowie eine IP Statistik und erlaubt einzelne Datenpakete individuell zu untersuchen. Die erfassten Datenpakete können bis auf tiefste Ebene dekodiert und mit den gebräuchlichsten Protokollen analysiert werden: TCP, UDP und ICMP. Auch direkter Zugriff auf die erfassten Datenpakete ist möglich. CommView ist ein hilfreiches Werkzeug für LAN Administratoren, Sicherheitsbeauftragte, Netzwerkprogrammierer bzw. Jedermann der gerne Übersicht haben möchte, welche Datenpakete durch seinen PC oder sein LAN Segment gehen.

Mehr Informationen

SmartWhois

SmartWhois ist ein Werkzeug das Ihnen hilft Informationen über irgend eine IP Adresse, einen Hostnamen oder eine Domäne zu erhalten. Im Gegensatz zu standart Whois Werkzeugen liefert Ihnen SmartWhois automatisch alle wichtigen Informationen über eine IP Adresse/eine Domäne/einen User unabhängig von der geographischen Registrierung : Domäne, Netzwerkname, Land, Staat oder Provinz und Ort. Sogar wenn die IP Adresse nicht in einen Hostnamen konvertiert werden kann. SmartWhois wird nicht versagen!

Mehr Informationen

Essential NetTools

Essential NetTools ist ein Set von Netzwerk Tools die beim Untersuchen und Anzeigen der Netzwerkverbindungen von grossem Nutzen sein können. Es ist das Schweizer Offiziersmesser für jeden der ein Netzwerktool für den täglichen Gebrauch sucht. Dieses Programm enthält ein NetStat Tool, dass die Netzwerkverbindungen und offenen Ports Ihres Computers anzeigt und sie den entsprechenden Applikationen zuordnet. Es beinhaltet auch einen NetBIOS Scanner, ein NetBIOS Auditor Tool zur Prüfung der LAN Sicherheit und ein Monitor zur Anzeige der externen Verbindungen zu Ihren freigegebenen (shared) Ressourcen wie auch ein Monitor zur Anzeige aller Prozesse resp. Services die auf Ihrem System laufen. Des weiteren sind nützliche Tools wie ein Ping, TraceRoute und NSLookup enthalten. Es erlaubt auch die Generierung eines Reports im HTML Format, Text Format, Semicolon-getrenntem Text Format sowie in benutzerspezifischen Formaten. Es ist ein einfach zu bedienendes und mächtiges Programm als Ersatz für Windows Tools wie nbstat, netstat und NetWatcher. Es vereinigt viele Optionen, welche die Standard Tools nicht bieten können.

Mehr Informationen

DigiSecret

DigiSecret ist eine einfach zu bedienende, sichere und mächtige Applikation für die File Verschlüsselung und Freigabe (Sharing). Es werde starke und bewährte Verschlüsselungsalgorithmen für die Erstellung von Archiven (self-extracting EXE Files) und freigegebene (shared) Files verwendet. Des weiteren ist eine intelligente Filekompression integriert, welche die Verwendung von .zip Archiven überflüssig macht. Das Programm ist in die Windows Umgebung integriert, so dass Sie alle Operationen nach dem Klicken auf die rechte Maustaste ausführen können. Das Programm unterstützt auch Drag-and-Drop.

Mehr Informationen