Essential NetTools™

Bedienungshandbuch

Einführung

Über Essential NetTools

Essential NetTools ist ein Satz von Netzwerkwerkzeugen, die sehr nützlich zur Netzwerkdiagnose und Netzwerkverbindungsüberwachung Ihres Computers sind. Das Programm ist ein Schweizer Taschenmesser für jeden, der machtvolle Werkzeuge für den Alltagseinsatz sucht. Es beinhaltet:

- **NetStat:** Zur Anzeige der ein- und ausgehenden Netzwerkverbindungen, inkl. der Informationen über offene TCP- und UDP-Ports, IP-Adressen und der Verbindungszustände. Was es von anderen NetStat-Hilfsmitteln unterscheidet, ist die Zuordnungsmöglichkeit offener Ports zu eigenen Applikationen. Konfigurierbare Warnsignale für ein- und ausgehende Verbindungen sind ebenso verfügbar.
- **ProcMon:** Zeigt die Auflistung der laufenden Prozesse mit allen Informationen über den Programmstandort, Hersteller, Prozess-ID und die geladenen Module. Mit diesem Tool können Sie CPU-Auslastungsstatistiken einsehen, versteckte Applikationen identifizieren, laufende Prozesse abbrechen und die Benutzung Ihrer PC-Ressourcen effektiver verwalten.
- **TraceRoute** und **Ping:** Diese vertrauten Funktionen besitzen anpassbare Optionen und eine zweckmäßige Ergebnisausgabe ermöglicht eine Untersuchung und Fehlersuche bei Internet- und Anschlussproblemen.
- **PortScan:** Ein erweiterter TCP-Port-Scanner, der es Ihnen ermöglicht, ihr Netzwerk auf aktive Ports zu untersuchen. Dieses Hilfsmittel unterstützt beide Scan-Modi: konventioneller (vollverbundener) und verdeckter (halboffener) Modus.
- **HostAlive:** Ein Netzwerküberwachungshilfsmittel, dass periodisch einen Host auf Aktivierung und laufende Netzwerkdienste überprüft, wie HTTP- oder FTP-Server.
- **EmailVerify:** Überprüft, die Gültigkeit einer E-Mail-Adresse bei der Kommunikation mit dem zugehörigen Mail-Server über SMTP.
- **NSLookup:** Ermöglicht eine Konvertierung von IP-Adressen zu Hostnamen und umgekehrt, Kennnamen zu erhalten und die Ausführung von DNS-Abfragen, wie MX oder CNAME.
- **IPBlackList:** Überprüft, ob eine IP-Adresse in verschiedenen IP-Adress-Schwarzlisten vorhanden ist: SPAM-Datenbanken, offene Proxy-Server und Mailausgaberelais usw. Dieses Tool hilft Ihnen herauszufinden, warum eine bestimmte IP-Adresse von einigen Netzwerkressourcen, wie Mail-Server, verweigert wird.
- **NBScan:** Ist ein schneller und leistungsfähiger NetBIOS-Scanner. NBScan kann ein Netzwerk innerhalb eines vorgebenen Bereiches von IP-Adressen abtasten und listet gefundene NetBIOS-Ressource Sharing-Dienste auf, ebenso wie deren Namens- und MAC-Adresslisten. Im Gegensatz zu dem mit Windows gelieferten Standard-NETSTAT Utility, ist dieses Werkzeug mit einer graphischen Benutzeroberfläche und einer einfachen Verwaltung für LMHost-Dateien ausgestattet und zeichnet sich durch sein Parallel-Scannen aus, dass die Überprüfung eines Klasse-C-Netzwerkes in weniger als einer Minute ermöglicht. NBScan kann häufig auftretende Routineaufgaben von Systemintegratoren, Administartoren oder Analytikern erleichtern.
- **RawSocket:** Unterstützt Sie mit der Fähigkeit, systemnahe TCP- und UDP-Verbindungen einzurichten, um verschiedene Netzwerkdienste zu testen und auf Fehler zu untersuchen. Die mehrfarbige Ausgabe und eine komfortable Bedienoberfläche machen es zu einem großartigen Werkzeug für jeden Netzwerkadministrator oder Programmierer.
- **WiFiMan**: Ist ein Werkzeug, dass die installierten drahtlosen Adapter Ihres Computers anzeigt, verfügbare drahtlose Netzwerke auflistet und Ihnen ermöglicht Verbindungsprofile zu verwalten.
- **Shares:** Überwacht und protokolliert externe Verbindungen zu den gemeinsam genutzten Ressourcen Ihres Computers, listet lokale Verteilungen auf und stellt ebenso auf schnelle und einfache Art und Weise die Verbindungen zu ferngesteuerten Ressourcen her.
- **NetAudit** (NetBIOS Auditing Tool): Ermöglicht Ihnen die Ausführung verschiedener Sicherheitsüberprüfungen in Ihrem Netzwerk und/oder Einzelcomputer bieten den NetBIOS File Sharing-Dienst an. Dieses Tool kann Ihnen helfen potentielle Sicherheitslücken zu identifizieren.
- **SNMPAudit:** Erweiterter SNMP-Gerätescanner. Er ermöglicht Ihnen schnell SNMP-Geräte im ausgewählten Netzwerksegment zu lokalisieren und anpassbare Datenabfragen von jedem der Geräte zu empfangen. Sie können den SNMP-Browser zur detaillierten Untersuchung eines Gerätes benutzen.
- **SysFiles:** Ein komfortabler Editor für die fünf wichtigsten Systemdateien: Dienste, Protokolle, Netzwerke, Hosts und LMHosts.

Andere Funktionen beinhalten die Berichtserstellung in HTML, Text und kommagetrennten Formaten; schneller gemeinsamer IP-Adressenzugriff verschiedener Werkzeuge; Geostandortbestimmung von IP-Adressen; ein umfangreiches Systemübersichtsfenster und eine anpassbare Bedienoberfläche.

Was ist neu?

Version 4.3

- WiFiMan: Ein neues Tool zur Arbeit mit drahtlosen Netzwerken. Scannen nach verfügbaren Netzwerken, Profilverwaltung, Überwachungssignalstärke usw.
- Unterstützung von Windows 7.
- Verbesserte NetStat- und ProcMon-Berichtsgenerierung.
- Aktualisierte IP-Zuweisungsübersicht.
- Einige andere Verbesserungen

Version 4.2

- Neue Netzwerk-Tools wurden hinzugefügt: HostAlive zur Dienstverfügbarkeitsüberwachung; EmailVerify zur Gültigkeitsüberprüfung einer E-Mail-Adresse bei der Kommunikation mit dem zugehörigen Mail-Server; IPBlackList zur Überprüfung, ob eine IP-Adresse in verschiedenen IP-Adress-Schwarzlisten vorhanden ist.
- Alle Werkzeuge beinhalten jetzt eine Geo-Standortbestimmung, d.h. alle IP-Adressen werden ihrem Land zugeordnet, sowie der Landesname nebst Flagge neben jeder IP-Adresse eingeblendet.
- Einige Programmfehler wurden behoben.

Version 4.1

- Windows Vista-Unterstützung.

Version 4.0

- SNMPAudit – Ein neues Werkzeug zur Untersuchung SNMP-aktiver Geräte. Ein SNMP-Browser wurde zur detallierten Untersuchung SNMP-aktiver Gerätezustände hinzugefügt.
- Vollüberarbeitetes NetAuditTool. Gesteigerte Gesamtleistung und verbesserte Kompatibilität mit modernen Netzwerkstandards. Die Bedienoberfläche wurde hinsichtlich der Benutzerfreundlichkeit und der einfacheren Benutzung verändert.
- Erweitertes und verbessertes NetStat. Für eingehende und ausgehende Verbindungen wurde ein neues einstellbares Alarmsystem hinzugefügt, sowie Icon-darstellende Prozesse in der aktuellen Verbindungsliste. Verschiedene Verbindungstypen werden koloriert dargestellt, einschließlich der geschlossenen Verbindungen.
- Das ProcMon-Modul zeigt jetzt die CPU-Zeitzuordnungsstatistik pro Vorgang an.
- Ein automatisches Update-System ermöglicht Ihnen schnell die TamoSoft-Webseite auf neue Updates zu überprüfen.
- Verbesserungen der Bedienoberfläche die, einstellbare Buttons in der Seitenleiste und die Fähigkeit das Windows-Standard-System-Utility zu starten, und andere Verbesserungen beinhalten.
- RawSocket ermöglicht jetzt, beliebige Daten inklusive nichtdruckbarer Zeichen, wie 0x00, zu senden.
- TraceRoute führt jetzt die DNS-Auflösung im Hintergrund durch, was die Modulleistung maßgeblich verbessert.
- Einige Programmfehler der vorherigen Version wurden behoben.

Version 3.2

- Ein neues Sytemauswertungsfenster stellt Ihnen sehr detaillierte Informationen auf Ihrem Computer bereit.
- Eine verbesserte Protokollierung ermöglicht Ihnen jetzt nur neue Verbindungen zu protokollieren oder diese in NetStat und ProcMon zu verarbeiten.
- Ping besitzt jetzt die Fähigkeit einen IP-Adressbereich anzupingen.
- Neue Schnellstart- und Windows-Werkzeugmenüelemente können, zum Start Ihrer bevorzugten Applikationen und zum Zugriff auf viele üblich genutzter Windows-Tools, von einem zentralen Platz aus, benutzt werden.
- Raw UDP-Verbindungen werden jetzt neben TCP unterstützt.
- Neue Verbindungen werden in NetStat hervorgehoben.
- Lokal gemeinsam genutzte Ressourcen werden jetzt in Anteile aufgelistet.
- SysFiles – Ein neues Werkzeug, dass Ihnen eine leichte Bearbeitung der fünf wichtigsten Systemdateien ermöglicht: Dienste, Protokolle, Netzwerke, Hosts und LMHosts.
- Mehrsprachiges Interface.

Version 3.1

- PortScan – Ein neues Werkzeug zur TCP-Port-Abtastung.
- Benutzerdefinierbare Filter in NetStat.
- Sie können TCP-Verbindungen beenden, die durch andere Applikationen eingerichtet wurden.
- Das Programm kann automatisch NetStat- und ProcMon-Protokolle erstellen.
- Ein paar andere Verbesserungen.

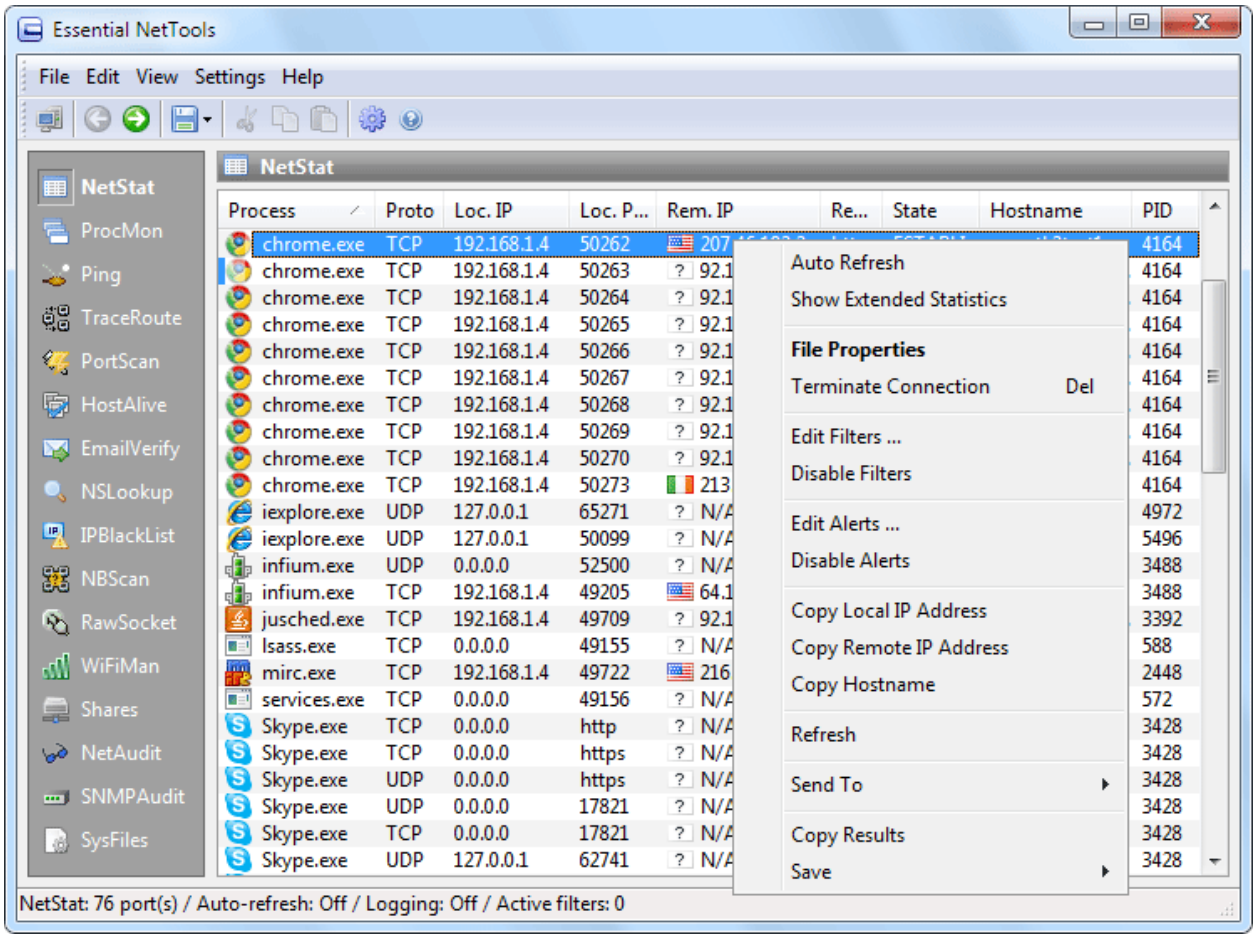
Version 3.0

- Eine neue, verbesserte Bedienoberfläche.
- Betriebsbereit für Windows XP.
- NetStat ordnet jetzt offene Ports und Verbindungen der zugehörigen Applikation zu (nur Windows NT/2000/XP).
- Neue Werkzeuge: TraceRoute, Ping, NSLookup und Ablaufmonitor.

Programmbenutzung

Bedienoberflächenübersicht

Das Programmhauptfenster besteht aus einer größenänderbaren Leiste auf der linken Seite, aus welcher Sie ihr benötigtes Tool auswählen können, und dem Hauptausschnitt, in dem das ausgewählte Tool eingeblendet wird. In der Statusleiste, am unteren Rand des Hauptfensters, wird der Status des aktiven Tools (z.B. Working oder Idle) angezeigt. Detaillierte Informationen zu jedem Werkzeug, finden Sie in den entsprechenden Kapiteln dieser Bedienungsanleitung.



Hauptmenü

Datei
Systemzusammenfassung – Blendet einen Dialog mit detaillierten Informationen zu Ihrem Computer ein.
Windows-Systemprogramme – Gibt Ihnen einen schnellen Zugang zu vielen gängigen Windows-Systemtools und -Hilfsmitteln.
Schnellstart – startet andere netzwerkabhängige Tools von TamoSoft, wenn Sie auf Ihrem System installiert sind, ebenso können Sie das Programm konfigurieren, dass es Ihre bevorzugten Anwendungen startet.
Ausführen – öffnet den Windows-Standarddialog **Ausführen**.
Bericht speichern – speichert die Ausgabe des aktiven Werkzeugs als Datei.
Protololllierung – öffnet den Dialog Protokoll.
Beenden – schließt das Programm.

Bearbeiten
Ausschneiden, Kopieren, Einfügen – führt jeweils das Standard-Textkommando aus.

Ansicht
Werkzeugleiste – blendet die Werkzeugleiste ein/aus.
Statusleiste – blendet die Statusleiste ein/aus.
Seitenleiste – ein-/ausblenden der Seitenleiste.
Seitenleiste einstellen – ermöglicht Ihnen, die Buttons der Seitenleiste zu konfigurieren.
Lokale IP-Adresse(n) – zeigt Ihnen ihre Computer-IP-Adresse.
Vorheriges Tool, Nächstes Tool – ermöglicht die Schaltung zum nächsten/vorherigen Tool.
NetStat, NBScan, usw. – ermöglicht Ihnen, dass Tool zu wählen mit dem Sie arbeiten möchten.

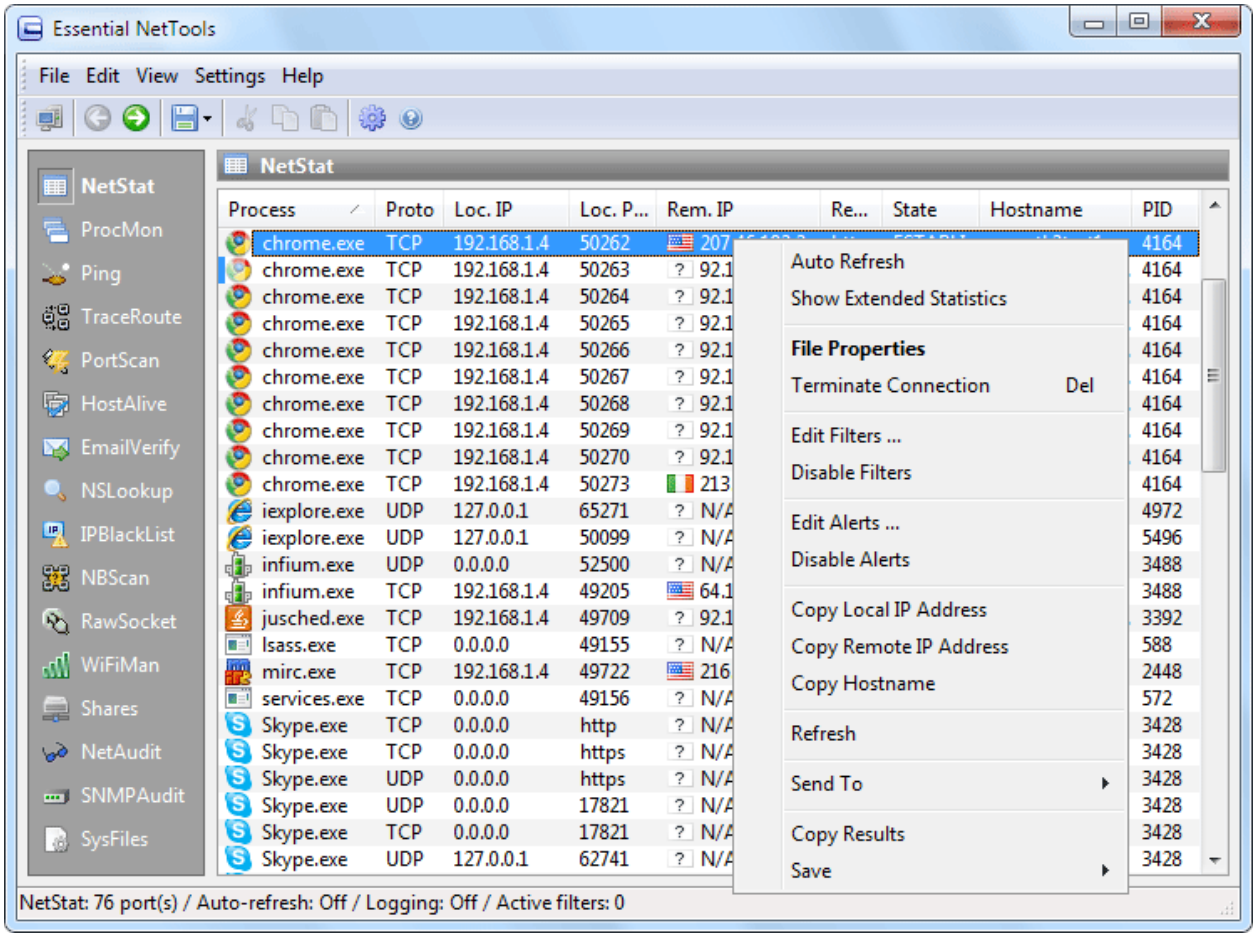
Einstellungen
Fonts – ermöglicht Ihnen, einen Interface-Font und einen Font mit festgelegter Schriftbreite auszuwählen (dieser Font wird in manchen Programmfenstern wie NetAudit oder NSLookup benutzt).
Optionen – blendet den Dialog Optionen ein.
Sprache – benutzen Sie diesen Befehl, um die Interface-Sprache auszuwählen.

Hilfe
Inhalt – Öffnet die Hilfedatei.
Nach Hilfe suchen über – Öffnet den Essential NetTools-Hilfeindex.
Im Web nach Updates suchen – Öffnet den Dialog Download. Bitte folgen Sie den Anweisungen auf dem Bildschirm und installieren Sie das aktuellste Upgrade für Essential NetTools von der TamoSoft-Webseite.

Info – Blendet das Programminfomationsfenster ein.

NetStat

Diese Tools ersetzt das Windows Standard-Kommandozeilenprogramm netstat. Das Programm zeigt alle ein- und ausgehenden Verbindungen, sowie alle offenen Ports Ihres Computers an. Zusätzlich ordnet NetStat offene Ports und bestehende Verbindungen den entsprechenden Applikationen zu.



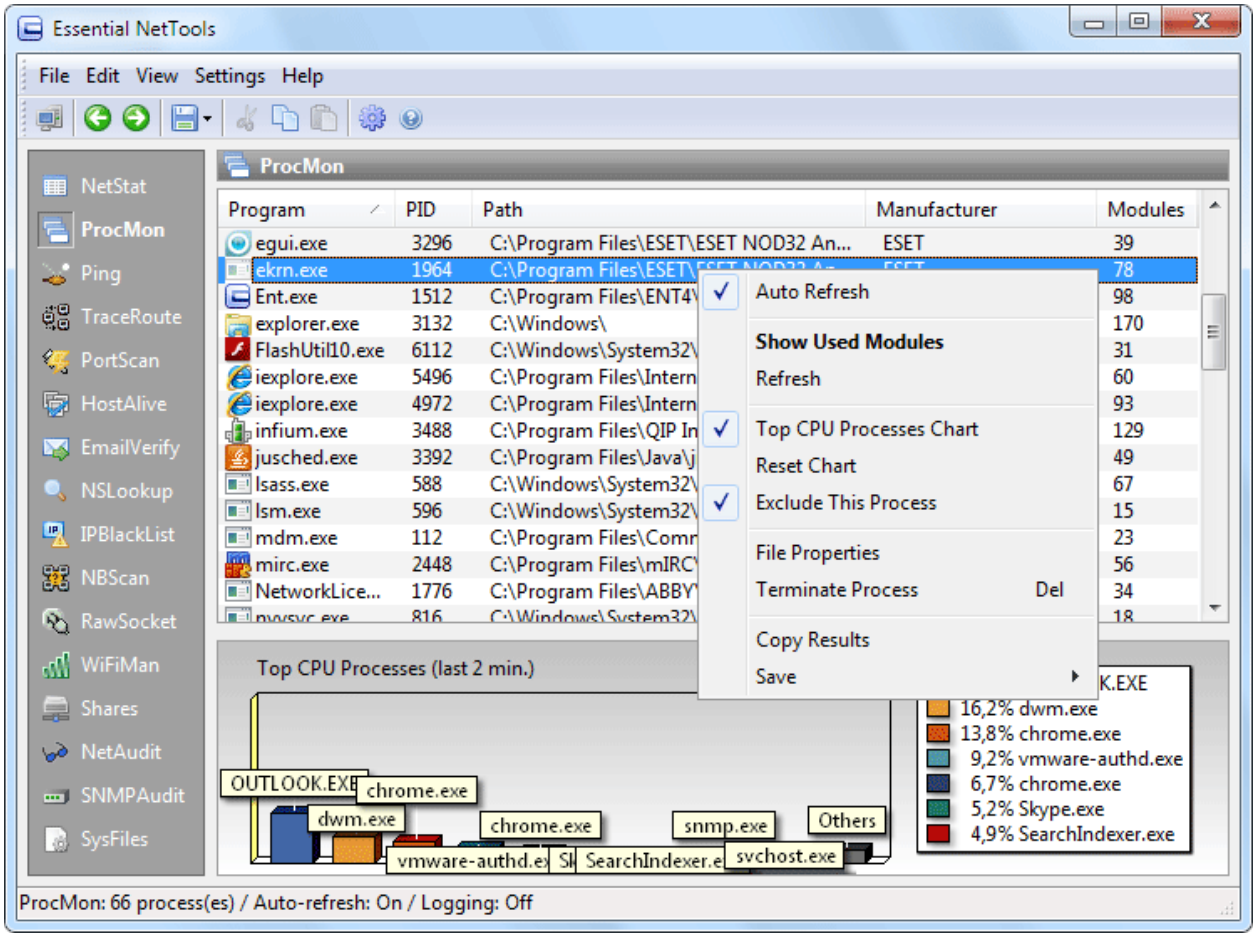
Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Automatisches Aktualisieren – ein-/ausschalten des Aktualisierungsprozesses der Auflistung. Der Aktualisierungsintervall ist einstellbar (siehe Optionen).
Erweiterte Statistik anzeigen – blendet ein zusätzliche Fenster mit erweiterten Statistiken pro Protokoll.
Dateieigenschaften – öffnet den Dialog Dateieigenschaften für den zugehörigen Verbindungsprozess.
Verbindung schließen – schließt die ausgewählte TCP-Verbindung.
Filter bearbeiten – öffnet den Dialog Filter.
Filter deaktivieren – aktiviert/deaktiviert alle aktuell konfigurierten Filter.
Warnsignale bearbeiten – öffnet den Dialog Warnsignale.
Warnsignale deaktivieren – aktiviert/deaktiviert alle aktuell konfigurierten Warnsignale.
Lokale IP-Adresse kopieren – kopiert die lokale IP-Adresse in die Zwischenablage.
Remote IP-Adresse kopieren – kopiert eine entferntgelegene IP-Adresse in die Zwischenablage.
Hostnamen kopieren – kopiert den entfernten Hostnamen in die Zwischenablage.
Aktualisieren – aktualisiert die gegenwärtig angezeigte Auflistung.
Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die NetStat-Tabelle in die Zwischenablage.
Speichern – speichert die NetStat-Tabelle in eine Datei.

Das Programm kann so konfiguriert werden, dass nicht alle Verbindungen eingeblendet werden, dass Portnummern in Servicenamen konvertiert werden, dass IP-Adressen in Hostnamen aufgelöst werden usw. Neue und geschlossene Verbindungen werden für fünf Sekunden hervorgehoben. Für weiterführende Information schauen Sie bitte in das Kapitel Optionen.

ProcMon

ProcMon ist ein Tool, dass eine Liste aller gegenwärtig auf Ihrem Computer laufenden Prozesse (Applikationen und Dienste) anzeigt. Die Spalte **Programm** zeigt den Programmnamen, die Spalte **PID** die einzigartige Prozess-ID, die Spalte **Pfad** den gesamten Pfad zur Programmstartdatei, die Spalte **Hersteller** den Hersteller der Startdatei und die Spalte **Module** die Anzahl der von diesem Prozess benutzten Module. ProcMon ist ein praktisches Tool zur Identifizierung versteckter Applikationen, zum Stoppen laufender Prozesse und um die Benutzung Ihrer PC-Ressourcen effektiv zu verwalten.



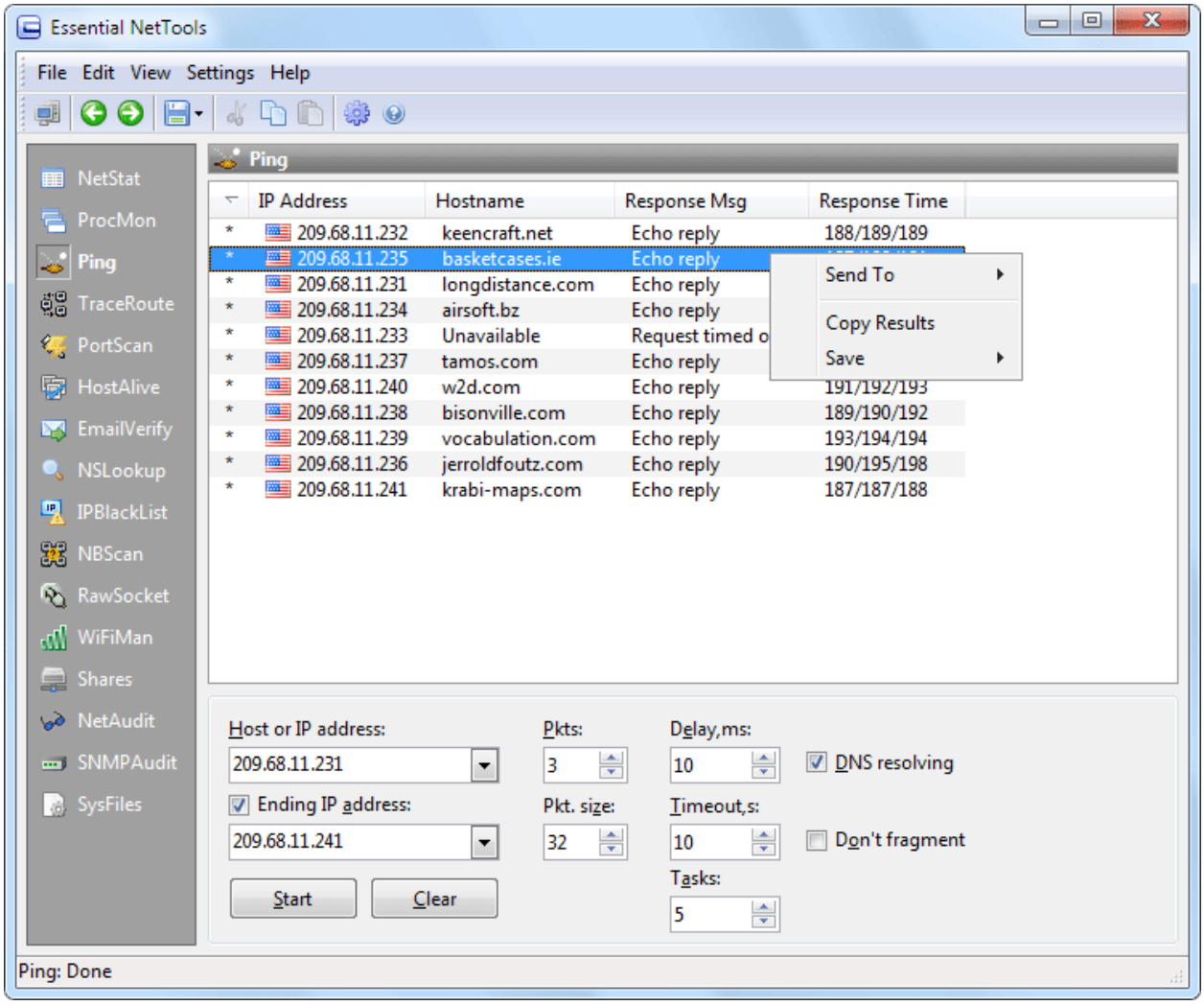
Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Automatisches Aktualisieren – ein-/ausschalten des Aktualisierungsprozesses der Auflistung. Der Aktualisierungsintervall ist einstellbar (siehe Optionen).
Genutzte Module anzeigen – blendet eine Auflistung aller vom ausgewählten Prozess benutzten Module (DLL-Dateien) ein.
Aktualisieren – aktualisiert die gegenwärtig angezeigte Auflistung.
Spitzen-CPU-Prozessdiagramm – ein-/ausblenden der 10 CPU-Prozesse mit dem höchsten Ressourcenkonsum als Diagramm.
Diagramm zurücksetzen – Zurückstellung aller angesammelter Statistiken und erneutes starten der Datenansammlung.
Prozess ausschließen – ausschließen des ausgewählten Prozesses aus der Statistik.
Dateieigenschaften – öffnet den Dialog Dateieigenschaften für den ausgewählten Prozess.
Prozess schließen – schließt den ausgewählten Prozess (mit Vorsicht benutzen).
Ergebnisse kopieren – kopiert die ProcMon-Tabelle in die Zwischenablage.
Speichern – speichert die ProcMon-Tabelle in eine Datei.

Das CPU-Auslastungsdiagramm zeigt die CPU-Ressourcenverteilung zwischen den Prozessen während der letzten Minuten an. Die 10 CPU-Prozesse mit dem höchsten Ressourcenkonsum, einschließlich der abgeschlossenen Prozesse, werden eingeblendet. Der Aktualisierungsintervall für das CPU-Auslastungsdiagramm ist konfigurierbar (siehe Optionen).

Ping

Ping ist ein Tool, dass Ihnen ermöglicht, die Existenz einer bestimmte IP-Adresse zu überprüfen und Anfragen entgegenzunehmen, wobei eine Internet Control Message Protocol (ICMP) *Echo Request*-Nachricht geschickt wird. Ping wird diagnostisch zur Sicherstellung eingesetzt, dass der Hostcomputer den Sie zu erreichen versuchen, aktiv ist. Wenn Sie z.B., einen Host nicht per Ping erreichen, sind Sie nicht in der Lage das File Transfer Protocol (FTP) zu benutzen, um Dateien zu diesem Host zu senden. Ping kann ebenso benutzt werden, um zu sehen, wie lange es dauert, eine Antwort von einem aktiven Host zu erhalten. Ist ein Host-Computer aktiv, antwortet er normalerweise mit einer *Echo Reply*-Nachricht.



Dieses Tool kann in zwei verschiedenen Modi arbeiten. Wenn Sie die Checkbox **End-IP-Adresse** nicht aktivieren, wird lediglich eine IP-Adresse angepingt und jedes Ping wird in einer separaten Zeile angezeigt. Wenn Sie die Checkbox **End-IP-Adresse** aktivieren, wird ein IP-Adressbereich angepingt und jede Adresse wird in einer separaten Zeile angezeigt. In diesem Modus zeigt die Spalte **Reaktionszeit** die Minimal-, Durchschnitts- und Maximalzeit getrennt durch Schrägstriche an.

Zur Benutzung dieses Tools, geben Sie eine IP-Adresse oder Hostnamen ein und klicken auf **[Starten]**. Die folgenden Optionen stehen zur Verfügung:

Pakete – definiert die Anzahl der Pakete, die zum entfernten Host gesandt werden.
Verzögerung – legt die Zeitintervalle (in Millisekunden) zwischen den Pings fest.
Paketgröße – legt die Größe (in Bytes) der Datenmenge des ICMP-Paketes fest.
Zeitüberschreitung – legt die maximale Zeit (in Sekunden) fest, die Ping auf die Reaktion eines Hosts wartet.
DNS-Auflösung – aktivieren Sie diese Checkbox wenn TraceRoute die IP-Adressen zu Hostnamen auflösen soll.
Nicht fragmentieren – setzt im Paket das Flag *Nicht fragmentieren*.
Tasks – legt die Anzahl der gleichzeitigen Aufgaben fest, wenn ein IP-Adressbereich angepingt wird. Es wird empfohlen, eine kleine Anzahl zu wählen, wenn Ihr PC nicht über ausreichend RAM verfügt, eine hohe Anzahl von Aufgaben kann Ihre Systemressourcen ausschöpfen.
Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

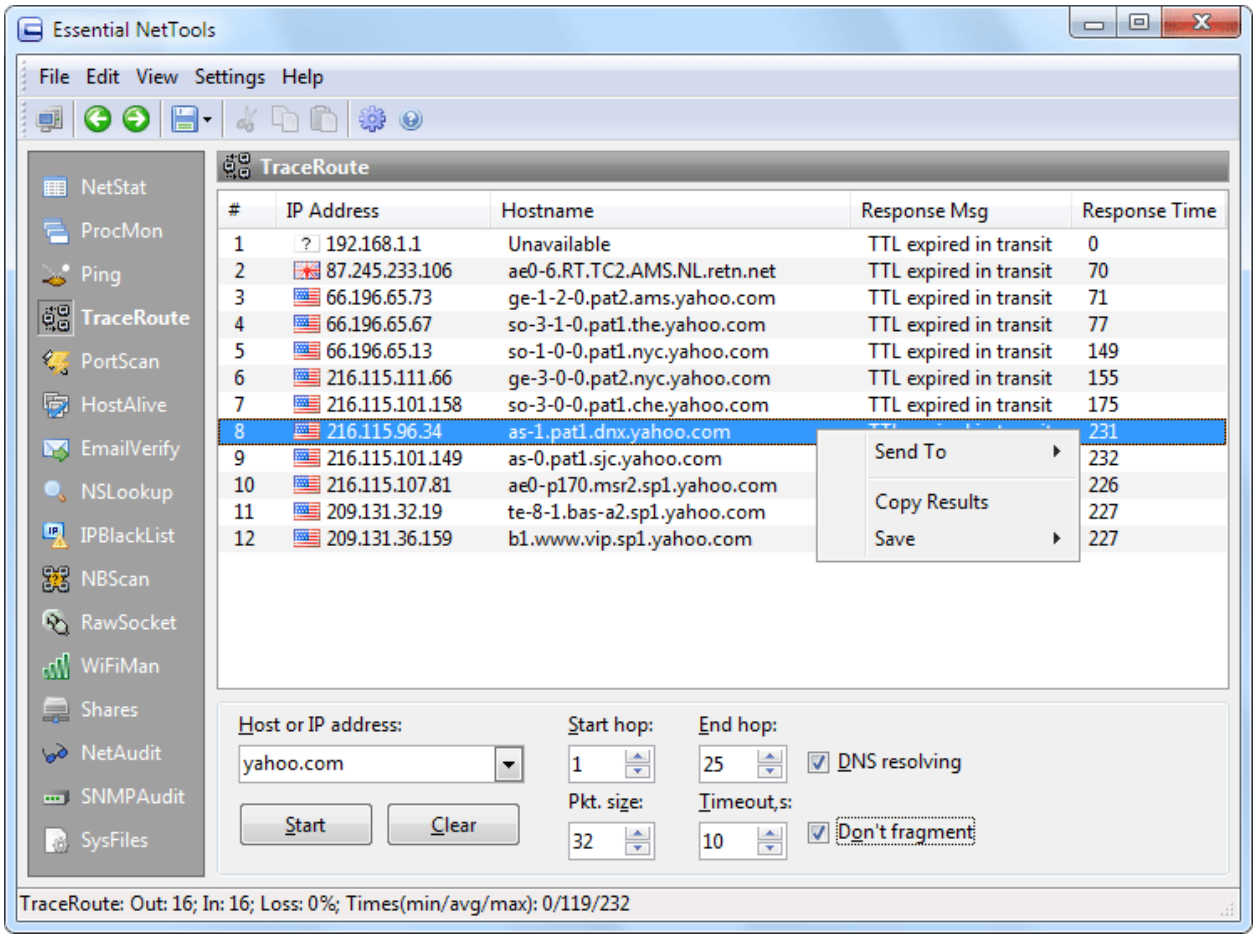
Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die Ping-Tabelle in die Zwischenablage.
Speichern – speichert die Ping-Tabelle in eine Datei.

TraceRoute

TraceRoute ist ein Tool, dass die Route (spezifische Gateway-Computer bei jedem Sprung) von einem Client-Computer zum Zielhost verfolgt, in dem alle Router-IP-Adressen die dazwischenliegen zurückgemeldet werden. Es berechnet und zeigt die Zeitmenge für jeden Sprung. TraceRoute ist ein praktisches Tool, das Ihnen hilft, Internetprobleme sowie die Funktionsweise des Internets, detailliert zu verstehen.

TraceRoute veranlasst jeden Router innerhalb des Netzwerkpfades ein Internet Control Message Protocol (ICMP)-Fehlermeldung zurückzusenden. Ein IP-Paket beinhaltet einen Time-To-Live-Bereich (TTL), der festlegt wie lange die Suche nach dem Ziel dauern darf, bis die Suche verworfen wird. Jedesmal, wenn ein Paket einen Router passiert, wird der TTL-Wert um 1 verringert; wenn er Null erreicht, wird das Paket verworfen und eine ICMP *TTL expired in transit-Fehlermeldung* an den Sender zurückgesandt.

Das TraceRoute-Programm verschickt die erste Gruppe von Paketen mit einem TTL-Wert von 1. Der erste Router innerhalb des Pfades, wird deshalb das Paket verwerfen (sein TTL wird auf 0 verringert) und den *TTL expired in transit-Fehler* zurücksenden. Damit haben wir den ersten Router auf dem Pfad gefunden. Jetzt werden Pakete mit einem TTL von zwei, dann drei usw. verschickt, sodass TraceRoute von jedem Router auf dem Pfad einen Fehler zurückgemeldet bekommt und diesen Router identifizieren kann. Einige Router verwerfen stillschweigend Pakete mit abgelaufenem TTL; für solche Sprünge erhalten Sie dann einen *Request timed out-Fehler*. Schließlich wird entweder das Ziel oder der Maximalwert erreicht und TraceRoute beendet. Am Ziel sendet TraceRoute ein ICMP Echo Request Packet (ping) und wenn der Computer erreichbar ist, meldet TraceRoute in der Spalte Antwort *Echo reply*.



Zur Benutzung dieses Tools, geben Sie eine IP-Adresse oder Hostnamen ein und klicken auf **[Starten]**. Die folgenden Optionen stehen zur Verfügung:

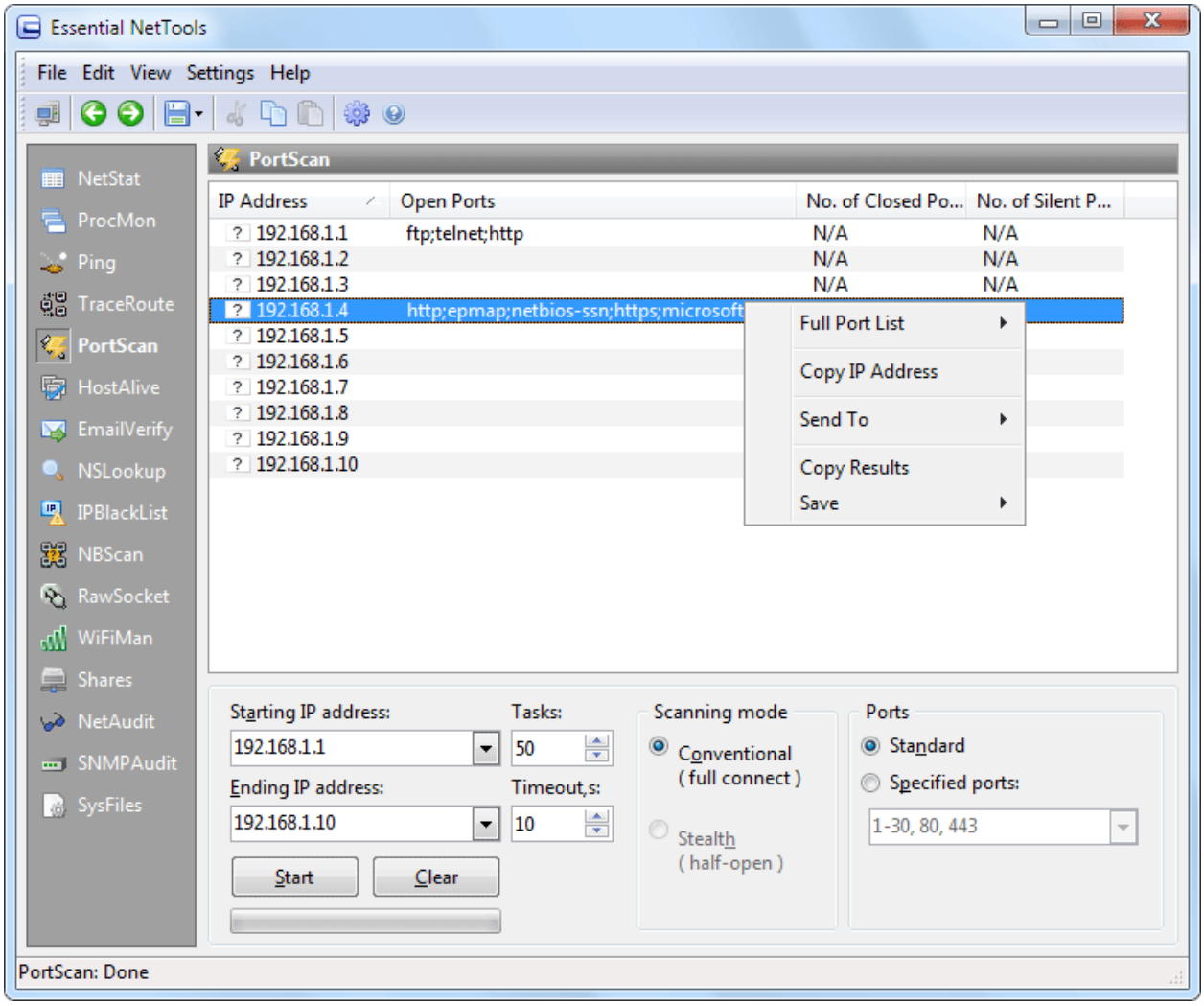
Sprungstart – ermöglicht Ihnen den Startpunkt für das TraceRoute festzulegen. Meistens ist es sinnvoll, einen höheren Wert als 1 einzugeben, wenn die ersten Sprünge auf der Route immer gleich sind; durch die Eingabe eines höheren Wertes können Sie Zeit einsparen.
Sprungende – ermöglicht Ihnen die Anzahl der Sprünge, die verfolgt werden sollen zu begrenzen.
Paketgröße – legt die Größe (in Bytes) der Datenmenge des ICMP-Paketes fest.
Zeitüberschreitung – legt die maximale Zeit (in Sekunden) fest, die TraceRoute auf die Reaktion eines Routers wartet.
DNS-Auflösung – aktivieren Sie diese Checkbox wenn TraceRoute die IP-Adressen zu Hostnamen auflösen soll.
Nicht fragmentieren – setzt im Paket das Flag *Nicht fragmentieren*.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die TraceRoute-Tabelle in die Zwischenablage.
Speichern – speichert die TraceRoute-Tabelle in eine Datei.

PortScan

PortScan ist ein TCP-Scanner, ein Tool das erkennt, ob sichere TCP-Ports geöffnet sind und ob diese Verbindungen annehmen. TCP-Scanner werden normalerweise zur Überprüfung von entfernten Computern benutzt, ob dort Dienste laufen (z.B. Telnet oder FTP) und zur Sicherheitsanalyse. Ein Portscan beinhaltet die Sendung von Daten an anwenderspezifizierte Ports und die Auswertung der empfangenen Antwort, ob der Port offen ist.



Information für Windows XP SP2- und Vista-Anwender.

Windows XP Service Pack 2 und neuere Windowsversionen begrenzen die Anzahl der gleichzeitigen unvollständig ausgehenden TCP-Verbindungen auf 10 pro Applikation. Bei Erreichen dieser Begrenzung, werden nachfolgende Verbindungsversuche in eine Warteschlange platziert bis das Problem der fixierten Anzahl behoben ist. Dies kann eine Applikation maßgeblich verlangsamen, die eine große Anzahl von Verbindungsversuchen durchführt. Ein Beispiel einer solchen Applikation ist Essential NetTools im Port-Scan-Modus (das Port Scan-Tool).
Zur Zeit sind keine offiziellen Zwischenlösungen für dieses Problem verfügbar. Es gibt allerdings ein inoffizielles Patch, welches die Systemdateien modifiziert und die Begrenzung entfernt. Wenn Sie Windows XP Service Pack 2 benutzen und sind mit der Port Scan-Geschwindigkeit oder mit der Qualität der Ergebnisse (z.B. viele Ports bleiben unerkannt) unzufrieden, können sie versuchen einen der inoffiziellen, unter http://www.lvllord.de/ verfügbaren Patches zu installieren. Warnung: Dieser Patch kann nur mit Windows XP Service Pack 2 angewendet werden. Dieses Patch wird nicht durch Microsoft unterstützt.
.
Zusätzlich: Windows XP Service Pack 2 und neuere Windowsversionen entfernen die Unterstützung für Raw Sockets und machen den Verdeckten-Scan-Modus im Port Scan-Tool unmöglich. Zur Zeit sind keine inoffiziellen Patches bekannt.

Bevor Sie den Scan starten, sollten Sie eine **Start-IP-Adresse** und eine **End-IP-Adresse** wie oben gezeigt und die Anzahl gleichzeitiger Verbindungen und die Verbindungszeitüberschreitungen in die Aufgaben- und Zeitüberschreitungsfelder eingeben.
Dann sollten Sie den Scanner-Modus wählen: **Normal** oder **Verdeckt**. Im Normalmodus wird eine TCP-Verbindung zwischen Ihrem Computer und dem zu scannenden Computer eingerichtet. Im Verdeckten-Modus wird die Verbindung zwar initiiert aber nicht erstellt. Diese Scan-Technik ist bekannt als *halb-offen*- oder *SYN-Scanning*: Das Programm sendet ein SYN-Paket (als wenn eine Verbindung geöffnet werden soll) an den Zielhost, und der Zielhost antwortet mit einem SYN ACK- (dies zeigt an, dass der Port hört) oder RST ACK-Paket (dies zeigt an, das der Port nicht hört). Verdeckte Scans auf TCP-Ebene können vom Zielhost nicht protokolliert werden, obwohl sie durch auf der Paketebene arbeitende Intrusions Detection Systeme (IDS –

Eindringerkennungssysteme) protokolliert werden können. Dieser Modus kann zum Test der Konfiguration und der Effizienz Ihres eigenen LAN-IDS nützlich sein.Der verdeckte Modus ist **nur unter Windows 2000/XP** verfügbar, erfordert Administratorrechte und kann zum Scannen der eigenen IP-Adresse benutzt werden (zum Finden der eigenen IP-Adresse, benutzen Sie den Normalmodus oder benutzen Sie das NetStat-Tool zur Ansicht der offenen Ports). Beachten Sie bitte, dass laufende Firewall-Software (inklusive der windowseigenen Firewall) auf Ihrem Computer Auswirkung auf das Scanergebnis des Verdeckten Modus haben; deshalb empfehlen wir, für diesen Scanvorgang die Firewall-Software temporär auszuschalten.

Schließlich sollten Sie zur Untersuchen von Ports eine Liste auswählen. Die Standardliste beinhaltet die folgenden Ports: 7, 9, 11, 13, 17, 19, 21, 23, 25, 43, 53, 70, 79, 80, 88, 110, 111, 113, 119, 135, 139, 143, 389, 443, 445, 512, 513, 1080, 1512, 3128, 6667 und 8080. Wenn Sie eine eigene Liste bevorzugen, wählen Sie die Liste **Spez. Ports** und geben Sie Ihre eigenen Ports ein. Die Syntax zur Porteingabe ist einfach: Sie können Einzelports oder Portbereiche kommagetrennt eingeben. Nachfolgend finden Sie einige Beispiele an gültigen Portlisten:

1-1024
1-30, 80, 443
21, 22, 25, 80-88, 1000-1024, 6666

Wenn alle Optionen eingegeben sind, klicken Sie auf **[Starten]**. Die Scangeschwindigkeit kann im Programmmenü unter **Einstellungen => Optionen** verändert werden (für weiterführende Informationen schauen Sie bitte in das Kapitel Optionen).

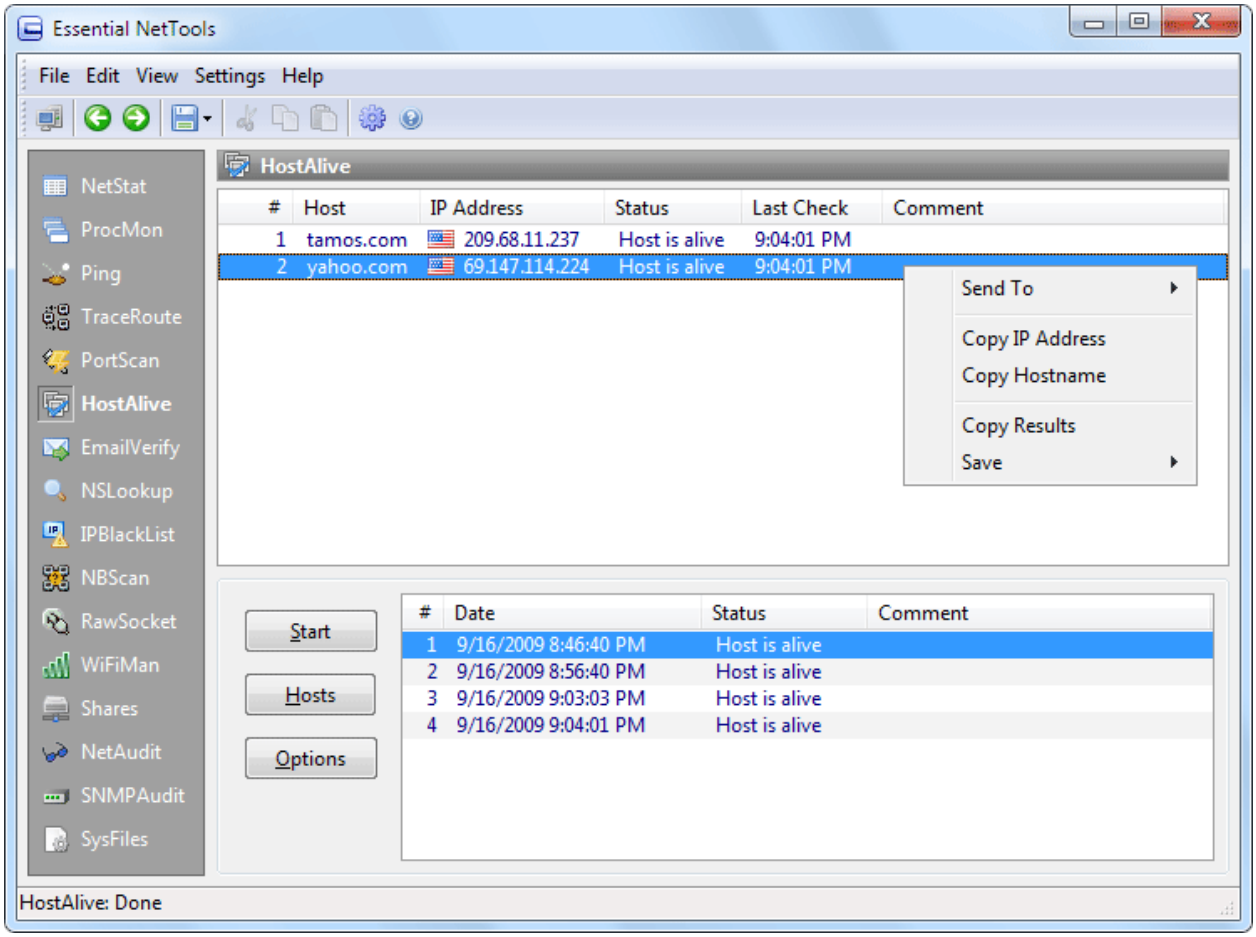
Während des Scanvorgangs werden die Portinformationen fortlaufend der Liste hinzugefügt. Die Spalte **Offene Ports** zeigt die TCP-Ports, die eine Verbindung annehmen. Die Spalte **Anz. geschl. Ports** zeigt die Ports, die Verbindungen ablehnen, während die Spalte **Anz. inaktiver Ports**, die Ports anzeigt, welche Verbindungsversuche ignorieren. Im Normalmodus, können die beiden letzten Spalte diese Anzahl nicht anzeigen, da dieser Modus nur offene Ports entdecken, aber nicht zwischen geschlossenen und inaktiven Ports unterscheiden kann. Mit anderen Worten, im Normalmodus werden alle nicht offenen Ports als geschlossen angesehen. Im Verdeckten Modus werden Ports, die mit einem RST ACK antworten als geschlossen betrachtet, während Ports, die ein SYN-Paket komplett ignorieren als inaktiv angesehen werden, was anzeigt, das sie durch eine Firewall geschützt sind.

Rechtsklicken auf einen gelisteten Computer öffnet ein Menü mit folgenden Befehlen:

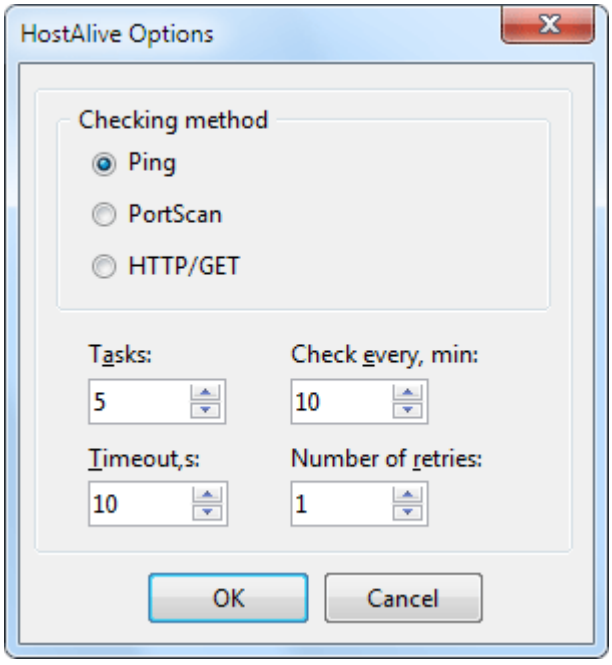
Portliste – blendet die komplette Portliste mit offenen, geschlossenen und stillen Ports ein. Die Portliste ist normalerweise sehr lang, daher ist dieser Befehl brauchbar zur Anzeige solch langer Listen.
IP-Adresse kopieren – kopiert die ausgewählte Computer-IP-Adresse in die Zwischenablage.
Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die PortScan-Tabelle in die Zwischenablage.
Speichern – speichert die PortScan-Tabelle in eine Datei.

HostAlive

HostAlive ist ein Tool, dass periodisch einen entfernten Host oder eine Gruppe von Hosts, auf Aktivität überprüft. HostAlive basiert auf einem einfachen Prinzip: Es sendet ein Netzwerkpaket an den Zielhost und wartet auf eine Antwort. Zum Beispiel, kann es die Aktivität des HTTP-Dienstes auf dem entfernten Computer überprüfen. Der Überprüfungstyp und –intervall ist einstellbar.



Zur Erstellung einer Hostliste, die überprüft werden sollen, klicken Sie auf den Button **[Hosts]**. Geben Sie die Namen oder IP-Adressen der zu überprüfenden Hosts ein. Zum Einstellen des Überprüfungstyps, klicken Sie auf den Button **[Optionen]** und konfigurieren den gewünschten Typ:



Drei Überprüfungsmethoden stehen zur Verfügung:

- **Ping:** Eine Standardüberprüfung unter Benutzung von ICMP-Ping-Paketen. Dies ist eine allgemeine Überprüfung, die Ihnen die Information bringt, ob der Host mit dem Netzwerk verbunden und das Operationssystem aktiv ist. Sie erhalten aber keine Information, ob ein bestimmter Netzwerkdienst, wie HTTP oder POP3 läuft. Beachten Sie bitte, dass Hosts hinter Firewalls kein Pingpaket beantworten können.
- **PortScan:** Eine Überprüfung, basierend auf der Fähigkeit des Hosts, eine TCP-Verbindung anzunehmen. Zum Beispiel, können sie so einen POP3-Dienst auf Aktivität überprüfen, wenn Sie den TCP-Port 110 scannen.
- **HTTP/GET:** Eine Überprüfung für Webserver, die vergleicht, ob ein entfernter Host Verbindungen auf dem HTTP-Standardport annimmt und eine korrekte HTTP-Antwort zurücksendet. Der Standard-HTTP-Port ist 80, Sie können aber auch einen eigenen Bereich eingeben.

Die folgenden Optionen sind ebenso verfügbar:

Aufgaben – konfiguriert die Anzahl der Jobs, die das Tool gleichzeitig starten kann.
Prüfen, alle (Min) – legt den Zeitintervall zwischen den Überprüfungen fest.
Zeitüberschreitungen (s) – konfiguriert, wieviele Sekunden das Tool auf die Antwort des Hosts warten soll.
Anz. der Versuche – legt die Anzahl der Versuche fest, die ausgeführt werden sollen.

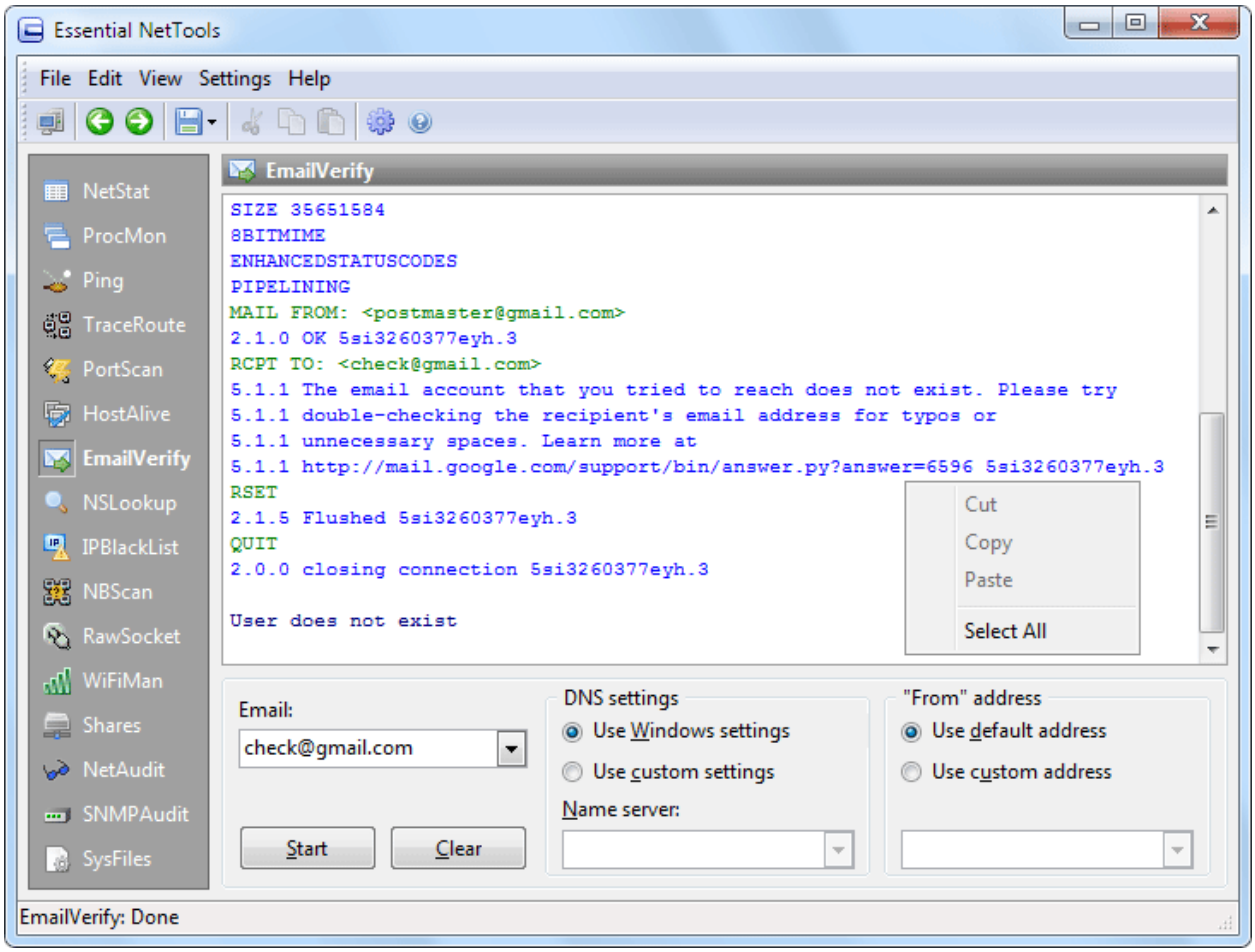
Sobald Sie die Liste der zu überprüfenden Hosts eingegeben und Sie die Optionen konfiguriert haben, klicken Sie auf **[Starten]** um den Vorgang zu initiieren. Das Tool wird die Überprüfung solange fortführen, bis Sie auf **[Stoppen]** klicken oder die Applikation beenden.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
IP-Adresse kopieren – kopiert die ausgewählte Computer-IP-Adresse in die Zwischenablage.
Hostnamen kopieren – kopiert den ausgewählten Hostnamen in die Zwischenablage.
Ergebnisse kopieren – kopiert die HostAlive-Tabelle in die Zwischenablage.
Speichern – speichert die HostAlive-Tabelle in eine Datei.

EmailVerify

EmailVerify ist ein Tool, das es Ihnen ermöglicht eine E-Mailadresse auf deren Existenz zu überprüfen und ob diese Mail annimmt. Dieses Tool sieht nach MX Records für die E-Mailadresse (mit anderen Worten, es findet heraus welcher Mailserver E-Mails für die vorgegebene Adresse bearbeitet) und versucht sich mit dem Mailserver zu verbinden und liefert eine E-Mail. Es wird keine reale E-Mail während der Überprüfung versendet.



Zur Überprüfung einer E-Mailadresse geben Sie diese im entsprechenden Fenster ein und klicken auf **[Starten]**. Das Protokoll der Überprüfung wird im Hauptfenster eingeblendet.

Um den Mailserver zu finden muss EmailVerify einige DNS-Abfragen durchführen. Standardmäßig benutzt das Tool DNS-Server, die von Windows benutzt werden. Bei einigen nichtstandardisierten Fällen müssen Sie diese Einstellungen außer Kraft setzen, aktivieren Sie dazu die Checkbox **Eigene Einstellungen benutzen** und geben Ihre eigenen Serveradressen ein.

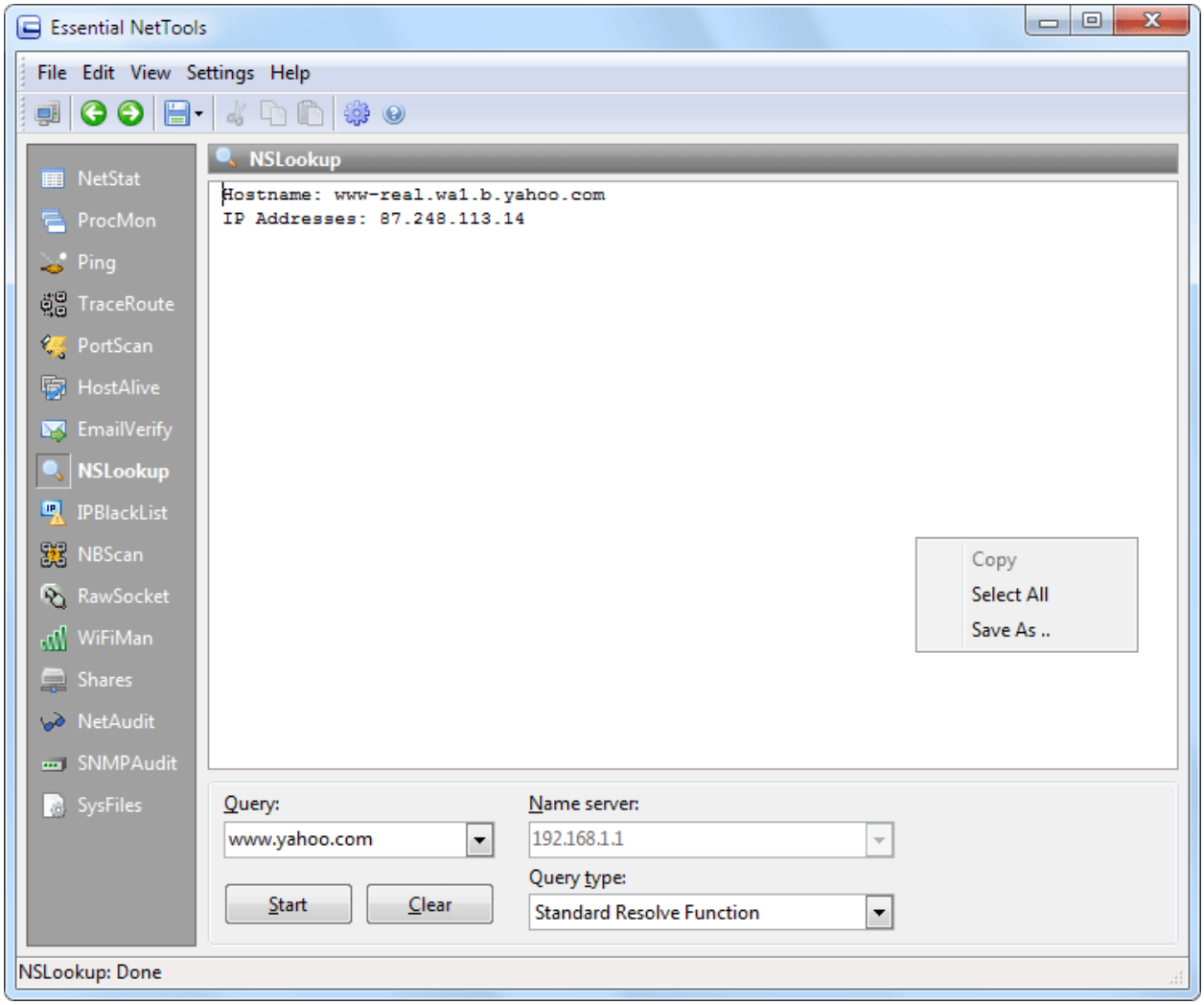
Während des E-Mailüberprüfungsvorganges muss EmailVerify die Senderadresse bereitstellen. Standardmäßig benutzt das Tool die *postmaster@domain-Adresse*, wobei domain der Domänenteil der E-Mailadresse ist. Zum Beispiel, Sie überprüfen *user1@gmail.com*, dann benutzt EmailVerify *postmaster@domain* als "Von-Adresse". Sie können dies durch Aktivierung der Option **Eigene Mailadressen benutzen** ändern und spezifizieren dann eigene Adressen.

Es ist wichtig, sich zu erinnern, dass das Ergebnis dieses Testes von der IP-Adresse abhängig ist, von der aus Sie die Verbindung herstellen, sowie von der benutzten "Von-Adresse". Der Mailserver kann Mail von bestimmten IP-Adressen oder von allen dynamischen IP-Adressen ablehnen. Er kann auch Mail von bestimmten Domänen und spezifischen Konten ablehnen.

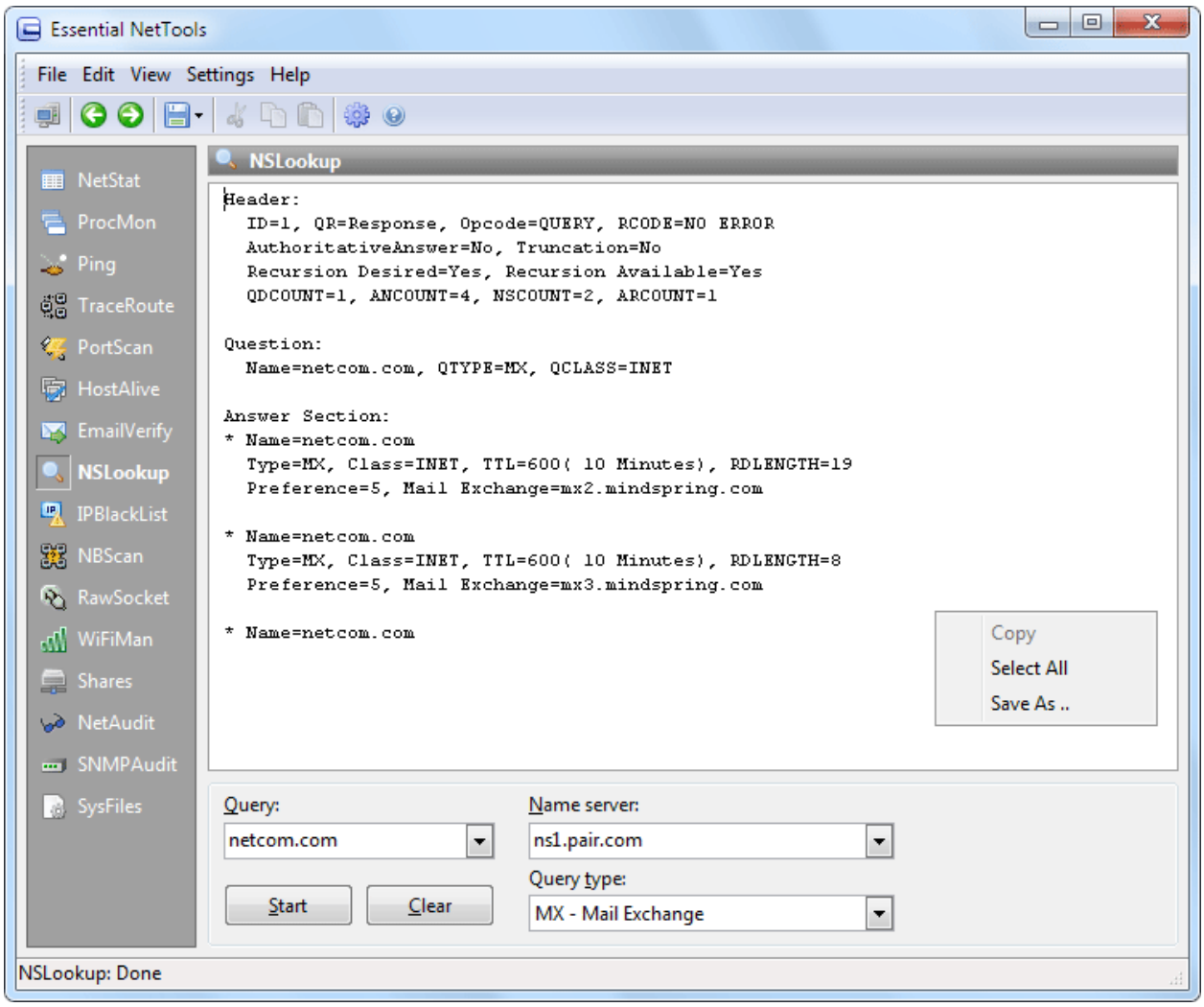
NSLookup

NSLookup ist ein Tool, dass Sie einen Hostnamen eingeben lässt (z.B. www.yahoo.com) und die zugehörige IP-Adresse herausfindet. Es kann auch rückwärts suchen und findet den Hostnamen einer von Ihnen spezifizierten IP-Adresse. Solch eine Umwandlung von Hostnamen in IP-Adressen und umgekehrt ist die Hauptfunktion von NSLookup; trotzdem können fortgeschrittene Anwender es zur Durchführung von spezifizierten Abfragen benutzen, z.B. Abfragen für Mail Exchange-Datensätzen (MX). NSLookup arbeite durch senden einer DNS-Abfrage (Domain Name System) an Ihren Standard-DNS-Server (im Rahmen einer Standard-Auflösungsfunktion) oder an jeden von Ihnen spezifizierten DNS-Server (im Rahmen aller anderen Abfragetypen).

Zur Durchführung einer Standardabfrage, wählen Sie **Standardauflösungsfunktion** aus der Auflistung **Abfragetyp**, geben eine IP-Adresse oder einen Hostnamen in das Feld **Abfrage** ein und klicken auf **[Starten]**. Das Programm wird das Abfrageergebnis in wenigen Sekunden einblenden. Für Standardabfragen wird sich das Programm immer mit Ihrem Standard-DNS-Server verbinden, sodass das Feld **Namenserver** deaktiviert ist.



Zur Ausführung von nicht-standardisierten Abfragen, wählen Sie den Aufzeichnungstyp aus der Liste **Abfragetyp**, geben Ihre Abfrage in das Feld **Abfrage** und eine DNS-Serveradresse im Feld **Namenserver** ein. Wenn Sie das Programm zum erstenmal starten, beinhaltet die Drop-Down-Liste **Namenserver** eine Auflistung Ihrer Standard-DNS-Server; Sie können einen Server aus der Liste auswählen oder geben Sie einen beliebigen Server ein, z.B. ns1.pair.com.



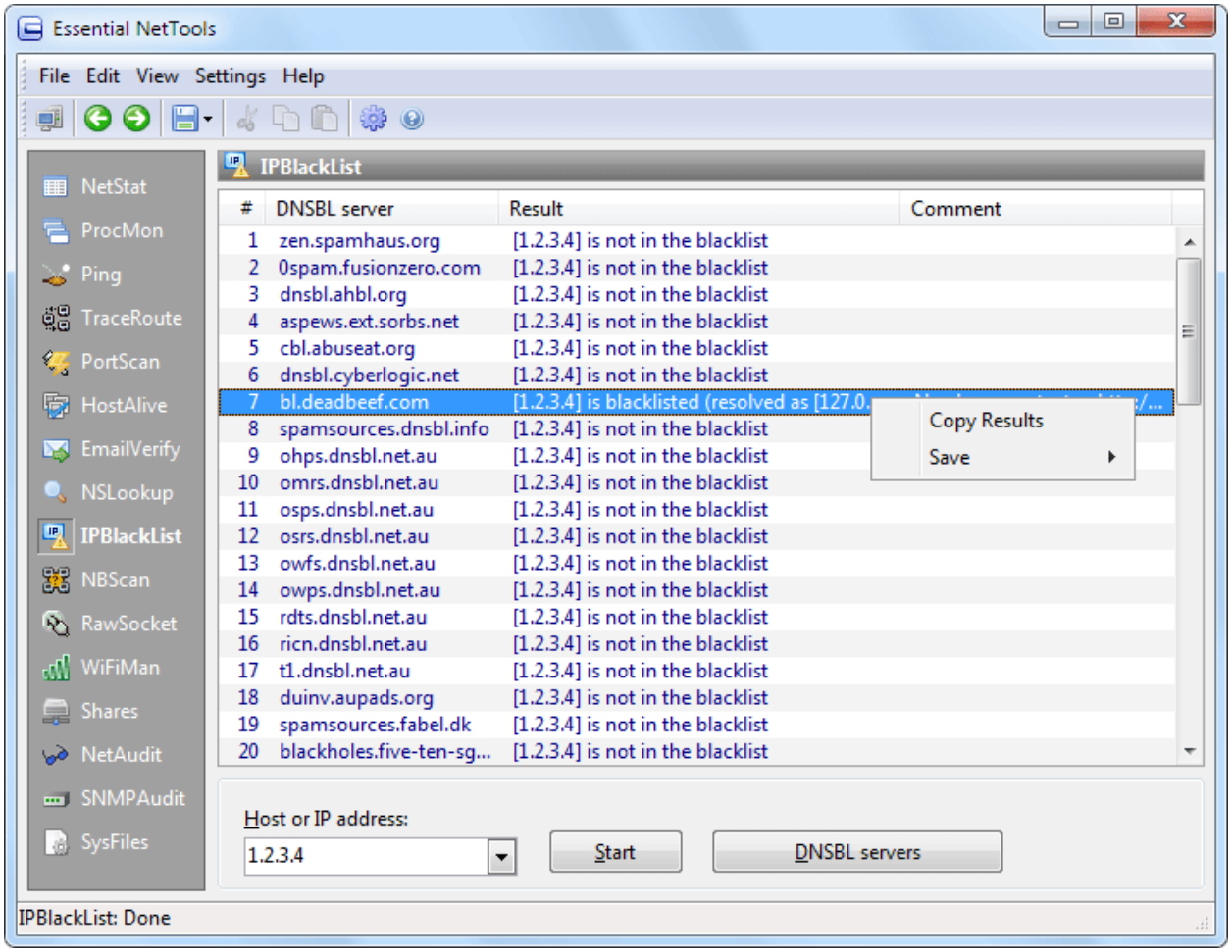
NSLookup stellt eine Menge Abfragetypen bereit, aus denen Sie auswählen können und Sie benötigen einige Internetkenntnisse um Abfragen auszuführen, anders als mit der **Standard-Auflösungsfunktion**. Wenn Sie ein Beginner sind und möchten mehr über die verschiedenen Abfragetypen erfahren, schlagen wir vor, die Dokumente RFC 1034 und RFC 1035 zu lesen oder im Internet nach Abfragetypen zu suchen.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Kopieren – kopiert den ausgewählten Text in die Zwischenablage.
Alles markieren – Markiert den gesamten Text im Fenster.
Speichern – speichert das Protokoll in eine Datei.

IPBlackList

IPBlackList ist ein Tool zur Überprüfung, ob eine IP-Adresse in verschiedenen Black-Listen vorhanden ist, wie SPAM-Datenbanken, verbotene IP-Adressen, offene Proxies oder Mail-Ausgabegeräte usw.. Dieses Tool ist hilfreich um herauszufinden warum eine bestimmte IP-Adresse durch einige Netzwerkressourcen, wie Mail-Server, abgewiesen wird.



IPBlackList überprüft die eingegebene IP-Adresse gegen die durch DNSBL-Server gewartete Datenbanken (für mehr Information über diese Technik, klicken Sie bitte hier). In Kürze, dieses Tool arbeitet wie folgt: Für den Fall, Sie wollen die IP-Adresse 1.2.3.4 überprüfen, ob diese sich auf einer Blacklist befindet, die vom Server *antispam.somedomain.com* gewartet wird. IPBlackLIst sendet eine DNS-Abfrage, wie *4.3.2.1.antispam.somedomain.com* an den Standard-DNS-Server. Wenn solch ein DNS-Datensatz existiert, z.B. die angegebene Hostadresse ist in eine IP-Adresse aufgelöst (entsprechend den DNSBL-Spezifikationen, muss eine IP-Adresse zu einem Bereich von lokalen IP-Adressen gehören, wie 127.x.x.x), dann befindet sich die überprüfte IP-Adresse 1.2.3.4 auf einer Blacklist.

Beachten Sie bitte, dass wir keine dieser Listen pflegen, deshalb können wir Sie auch nicht von einer der Listen entfernen.

IPBlackList ermöglicht Ihnen gleichzeitig eine IP-Adresse gegen mehrere DNSBL-Server zu prüfen. Essential NetTools beinhaltet eine Auflistung populärer DNSBL-Server, durch Klicken auf den Button **[DNSBL-Server]** können Sie aber Ihre eigene Liste benutzen.

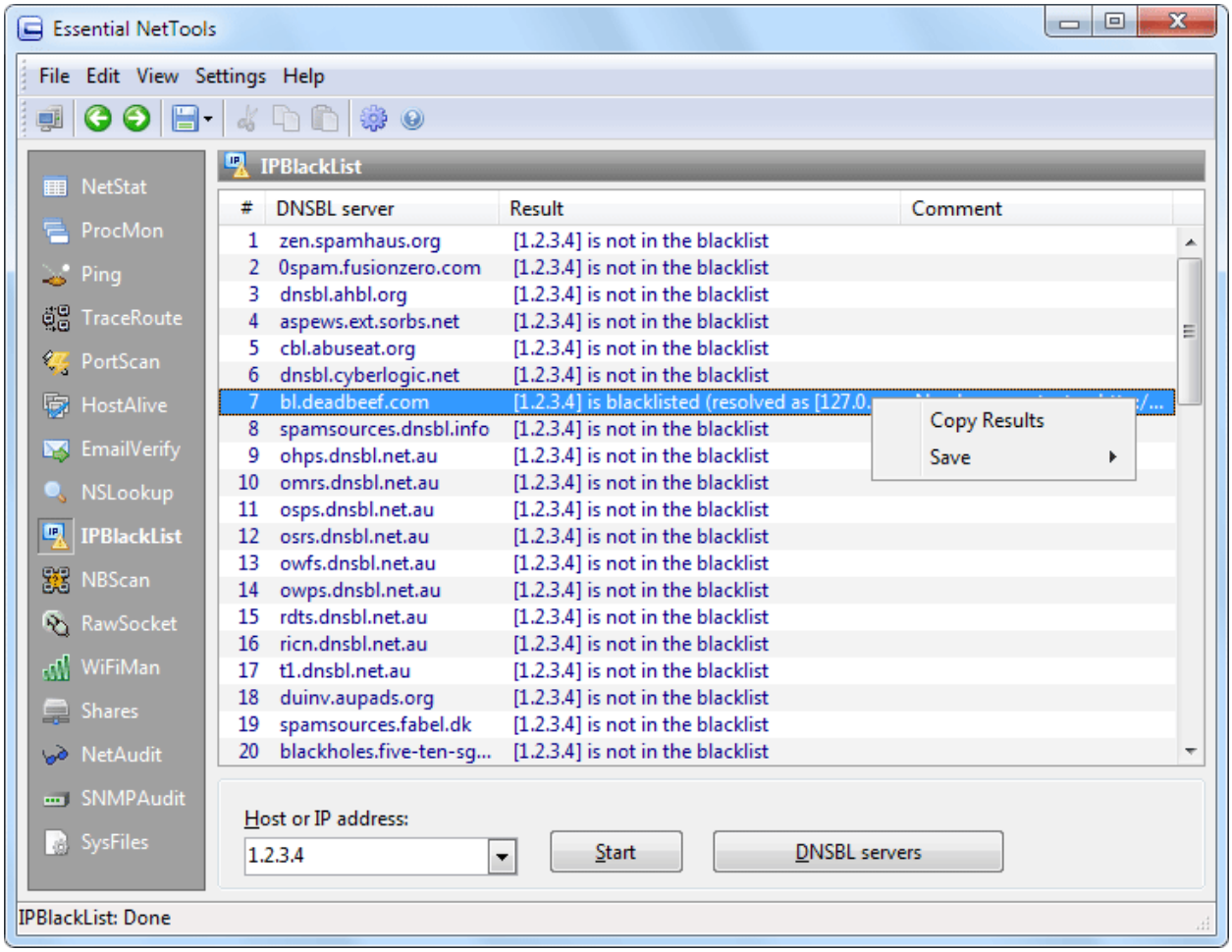
Eine aktuelle Auflistung funktionierender DNSBL-Server steht unter http://www.declude.com/Articles.asp?ID=97 zur Verfügung.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Ergebnisse kopieren – kopiert die IPBlackList-Tabelle in die Zwischenablage.
Speichern – speichert die IPBlackList-Tabelle in eine Datei.

NBScan

NBScan ist ein NetBIOS-Scanner, ein leistungsstarkes und schnelles Tool zur Erforschung von Netzwerken. NBScan kann Netzwerke innerhalb eines vorgegebenen IP-Adressenbereichs abtasten und listet Computer mit NetBIOS-Ressource Sharing-Dienst sowie deren Namenslisten. Anders als das mit Windows mitgelieferte nbtstat-Utility bietet dieses Tool eine freundliche, grafische Bedienoberfläche und eine leichte Verwaltung der LMHost-Dateien und ist mit Parallelabtastung ausgestattet, was ein Class C-Netzwerk in weniger als 1 Minute überprüft. Beide, Class C- und B-Netzwerke, können abgetastet werden. NBScan kann oft ausgeführte Routineaufgaben von Systemintegratoren, Administartoren und Analysten erleichtern.



Bevor Sie mit der Abtastung beginnen, sollten Sie eine **Start-IP**-Adresse und eine **End-IP**-Adresse wie oben gezeigt und die Anzahl gleichzeitiger Verbindungen und die Verbindungszeitüberschreitung in die Aufgaben- und Zeitüberschreitungsfelder eingeben. Sie können auch den **Erweiterten Modus aktivieren** (siehe Beschreibung weiter unten). Klicken Sie zum Scannen auf **[Starten]**.
Wenn NBScan innerhalb des vorgegebenen Bereichs einen Computer mit NetBIOS-Ressource Sharing entdeckt, wird die Information über den Computer aufgelistet. Die Spalten **Name**, **Arbeitsgruppe**, **IP-Adresse** und **MAC-Adresse** sind selbsterklärend. Die Spalte **RS** oder **Ressourcenteilung** wird benutzt, wenn der Computer Ressourcenteilung anbietet: Einige Computer können nicht konfiguriert werden Ressourcen zu teilen, sie antworten auf NetBIOS-Abfragen und werden gelistet.

Linksklicken auf einen gelisteten Computer zeigt dessen Namensliste im unteren Fenster. Wenn Sie Probleme mit der Interpretation der Namensliste haben, schauen Sie bitte in das Dokument NetBIOS Table reference innerhalb der Hilfedatei.

Rechtsklicken auf einen gelisteten Computer öffnet ein Menü mit folgenden Befehlen:

Computer öffnen – versucht einen ausgewählten Computer zu öffnen. Wenn der Computer erreichbar ist, wird ein neues Windows Explorer-Fenster mit Fernsteuerressourcen eingeblendet.
Zu LMHosts hinzufügen – fügt, im entsprechenden Format einen dem Computer zugehörigen Datensatz, der LMHost-Datei hinzu.
Alle Elemente den LMHosts hinzufügen – fügt, im entsprechenden Format alle den Computern zugehörigen Datensätze, der LMHost-Datei hinzu (Computer ohne Ressourcenteilung werden nicht hinzugefügt).
IP-Adresse kopieren – kopiert die IP-Adresse des ausgewählten Computer's in die Zwischenablage.
MAC-Adresse kopieren – kopiert die MAC-Adresse des ausgewählten Computer's in die Zwischenablage.
Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die NBScan-Tabelle in die Zwischenablage.
Speichern – speichert die NBScan-Tabelle in eine Datei.

Erweiterter Modus

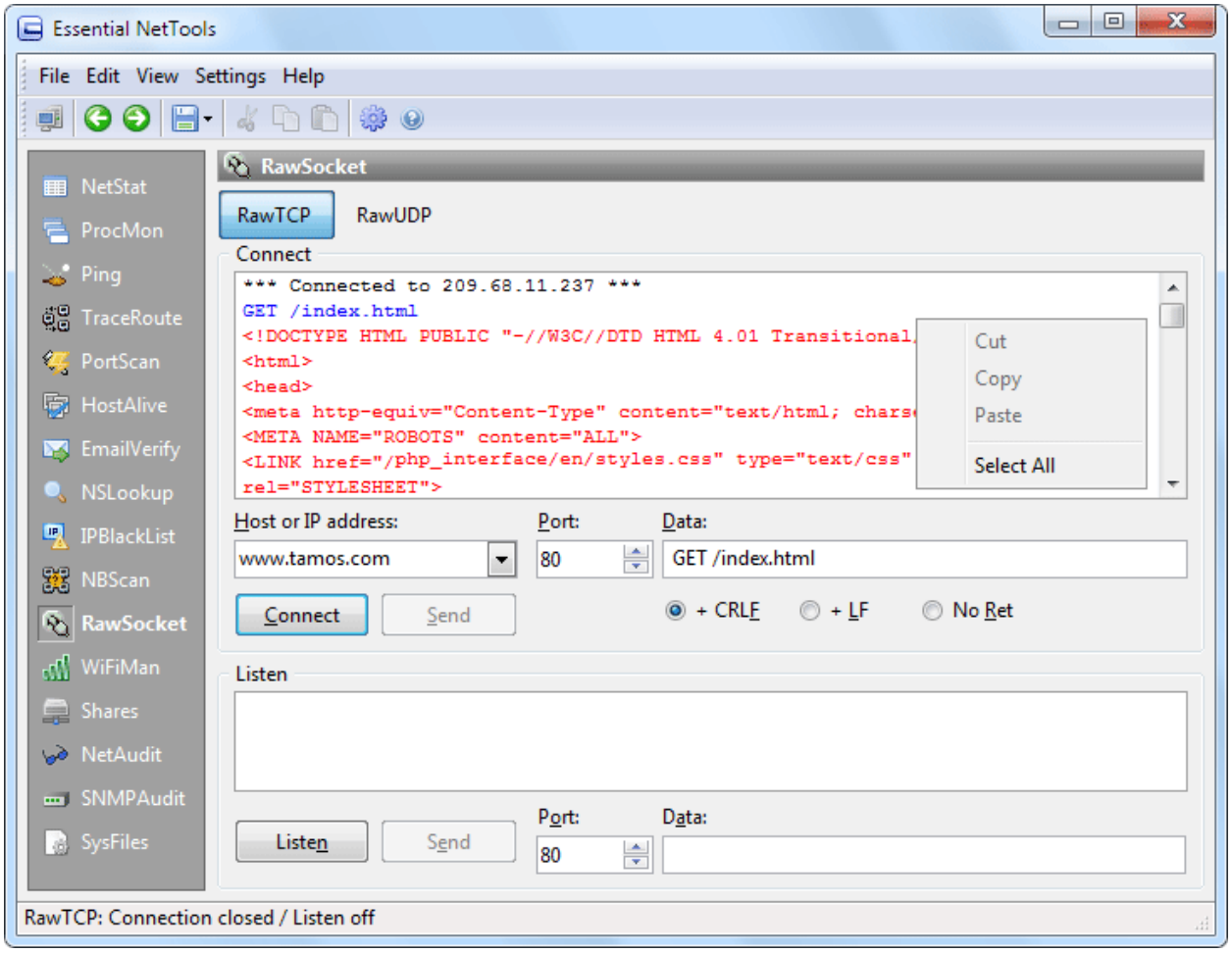
Aufgrund einiger lokaler Besonderheiten in der Behandlung von NetBIOS-Verbindungen, kann ein kleiner prozentualer Anteil von Computern auf Abfragen Rückantworten nur auf Port 137 senden, unabhängig davon von welchem Port die Abfrage gesandt wurde. Der erweiterte Modus ermöglicht Ihnen zu wählen, falls Sie möchten, dass das Programm Rückantworten auf Port 137 empfangen soll. Um in den erweiterten Modus zu schalten, aktivieren Sie die Checkbox **Erweiterter Modus (binden an Local Port 137)**. Der erweiterte Modus ist nicht verfügbar, wenn der Computer an einem Netzwerk angemeldet ist. Wenn der Computer schon angemeldet ist, ist dieses Menüelement deaktiviert. Wenn Sie diesen Modus benutzen möchten, sollten Sie ihn einschalten, bevor Sie sich im Netzwerk anmelden. Falls Sie zum Beispiel, eine Modemverbindung zum Internet benutzen, starten Sie zuerst das Programm und aktivieren die Checkbox **Erweiterter Modus (binden an Local Port 137)** und wählen sich dann ins Internet ein.

Wichtig: Die Benutzung des erweiterten Modus kann den Betrieb einiger Windows Netzwerkdienste, die den Port 137 benutzen, beeinflussen, z.B. sind Sie nicht in der Lage nbstat zu benutzen oder sich mit entfernten Computern zu verbinden. Um den Normalbetrieb solcher Dienste wieder herzustellen, sollten Sie den erweiterten Modus wieder abschalten, sich vom Netzwerk abmelden und sich erneut anmelden.

Der Grund für diese Begrenzung ist einfach: Es existiert nur ein Port 137 auf jedem System und dieser ist dem Prozess zugeordnet, der ihn zuerst beansprucht. Wenn Essential NetTools zuerst mit diesem Port verbunden war kann das Programm den erweiterten Modus betreiben, aber das OS ist nicht in der Lage ihn zu benutzen. Wenn das OS mit ihm zuerst verbunden ist, dann kann Essential NetTools diesen Port nicht benutzen. Bitte nehmen Sie zur Kenntnis, dass dieser Modus eine fortgeschrittene Fähigkeit ist und Sie müssen diese nicht nutzen. Eigentlich ist es durchaus glaubhaft, dass Sie keinen Unterschied zwischen den Ergebnissen bemerken, ob diese mit aktiviertem oder deaktiviertem erweiterten Modus beschafft wurden.

RawSocket

Mit **RawSocket** steht Ihnen ein Tool zur Verfügung, dass es Ihnen ermöglicht Raw-Daten an eine IP-Adresse zu senden oder von dort zu empfangen, ebenso können Sie eingehende TCP- oder UDP-Verbindungen auf jedem lokalen Port abhören. Es ist brauchbar bei der Fehlersuche in verschiedenen Netzwerkdiensten und zum Verstehen der Programmebenenprotokolle, wie POP, SMTP oder DAYTIME. Der Beispiel-Screenshot zeigt eine HTTP-Sitzung die mit dem Tool hergestellt wurde:



Verbinden
Zur Verbindung mit einem entfernten Host, geben Sie eine IP-Adresse oder Hostnamen ein, wählen einen Zielport und klicken auf **[Verbinden]**. Sobald die Verbindung eingerichtet ist, können Sie im Eingabefeld **Daten** Ihre Eingaben durchführen und klicken auf den Button **[Senden]** um die Daten zum entfernten Host zu senden. Wenn Sie Daten übertragen können Sie die Zeichen umschalten, welche als Zeichenkettenbegrenzer benutzt werden: Line Feed (0x0A), Carriage Return + Line Feed (0x0D0A), oder keine Begrenzer. Benutzen Sie die Struktur [xx] zur Versendung beliebiger Zeichen (inklusive der nichtdruckbaren Zeichen), wobei xx der Hexadezimalcode des übertragenen Zeichens ist. Beispielsweise wird die Struktur [48]ELLO als HELLO übersetzt, wobei der ASCII-Code des Zeichens 'H' 0x48 ist. Die gesendeten Daten werden in blau angezeigt; die empfangenen Daten werden in rot angezeigt.

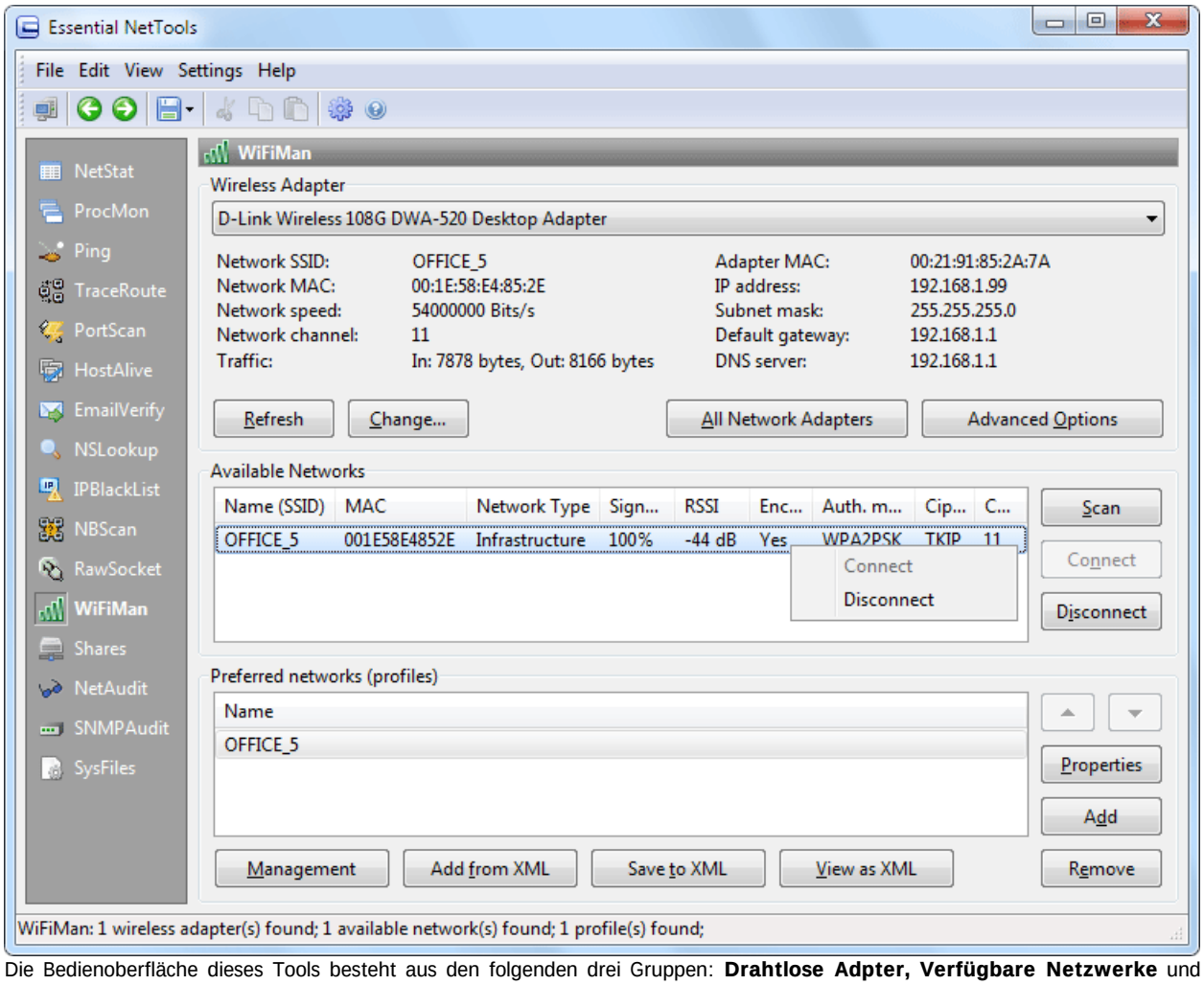
Horchen
Um eingehende Verbindungen zu empfangen, wählen Sie einen lokalen Port und klicken auf **[Lauschen]**. Wenn ein entfernter Host sich mit Ihrem PC verbindet, wird die Information dieser Verbindung auf dem Bildschirm eingeblendet. Wenn der entfernte Host die Datenübertragung zum offenen Port startet, werden die gesendeten Daten in rot angezeigt. Sie können Daten an den entfernten Host, wie oben beschrieben wurde, übertragen. Ihre Daten werden in blau angezeigt. Zum Schließen des lokalen Ports klicken Sie auf den Button **[Trennen]**.

Die obigen Informationen treffen auf **RawTCP** und **RawUDP** zu, mit der einzigen Ausnahme: Da UDP ein zustands- und verbindungsloses Protokoll ist, existiert kein Button **[Verbinden]** mehr unter RawUDP. Zur Übertragung von UDP-Daten müssen Sie keine Verbindung mehr einrichten. Sie müssen die Daten eigentlich nur verschicken.

WiFiMan

WiFiMan ist ein Tools, dass die drahtlosen, auf Ihrem Computer installierten Adapter anzeigt, listet verfügbare drahtlose Netzwerke auf und ermöglicht Ihnen, Verbindungsprofile zu verwalten.

Hinweis: Dieses Modul erfordert Windows XP SP2 oder ein aktuelleres Operationssystem.



Die Bedienoberfläche dieses Tools besteht aus den folgenden drei Gruppen: **Drahtlose Adpter, Verfügbare Netzwerke** und **Netzwerkprofile**.

Die Gruppe **Drahtlose Adapter** zeigt Informationen über das gewählte Netzwerkadapter. Falls Sie mehr als ein Adapter installiert haben, wählen Sie das gewünschte Adapter aus der Auflistung. Für jedes Adapter können Sie die Basisparameter einsehen, inklusive der Details des verbundenen drahtlosen Netzwerkes. Die folgenden Befehle sind für diese Gruppe verfügbar:

- **Aktualisieren** – Aktualisiert die Informationen über das drahtlose Netzwerk.
- **Ändern...** – Blendet einen Dialog ein, in dem Sie die Parameter des gewählten drahtlosen Adapters ändern können: **IP-Adresse**, **Subnet-Maske**, **Standard-Gateway**, **DNS-Server** und **MAC-Adresse**.
- **Alle Netzwerkadapter** – Blendet einen Dialog mit der Auflistung aller Netzwerkadapter und deren Informationen ein. Benutzen Sie die zugehörigen Button zur Aktivierung, Deaktivierung oder zum Neustart des Adapters.

- **Erweiterte Optionen** – Erlaubt Ihnen eine Anzahl von Einstellungen zu konfigurieren; Sie können den Netzwerktyp auswählen, angeben, ob Windows zur Verwaltung der Adapter benutzt werden soll und wählen den Modus, welcher zur Verbindung mit einem Netzwerk benutzt werden soll. Die folgen Optionen sind für diesen Dialog verfügbar:

    - **Netzwerkzugriff** – Konfiguriert das Verhalten der drahtlosen Netzwerksuche. Diese Option ist nsur in Windows Vista oder neueren Operationssystemen wirksam.

    - **Windows zur Einstellungskonfiguration benutzen** – Diese Option ist nur in Windows XP wirksam.

    - **Automatisch verbinden mit nichtbevorzugten Netzwerken** – Diese Option ist nur in Windows XP wirksam.

Die Gruppe **Verfügbare Netzwerke** listet alle verfügbaren drahtlosen Netzwerke zusammen mit deren Details auf. Die folgenden Befehle ind für diese Gruppe verfügbar:

- **Scan** – Tastet die Luft nach verfügbaren drahtlosen Netzwerken ab.
- **Verbinden** – Verbindet zum ausgewählten Netzwerk.
- **Trennen** – Trennt die Verbindung zum ausgewählten Netzwerk.

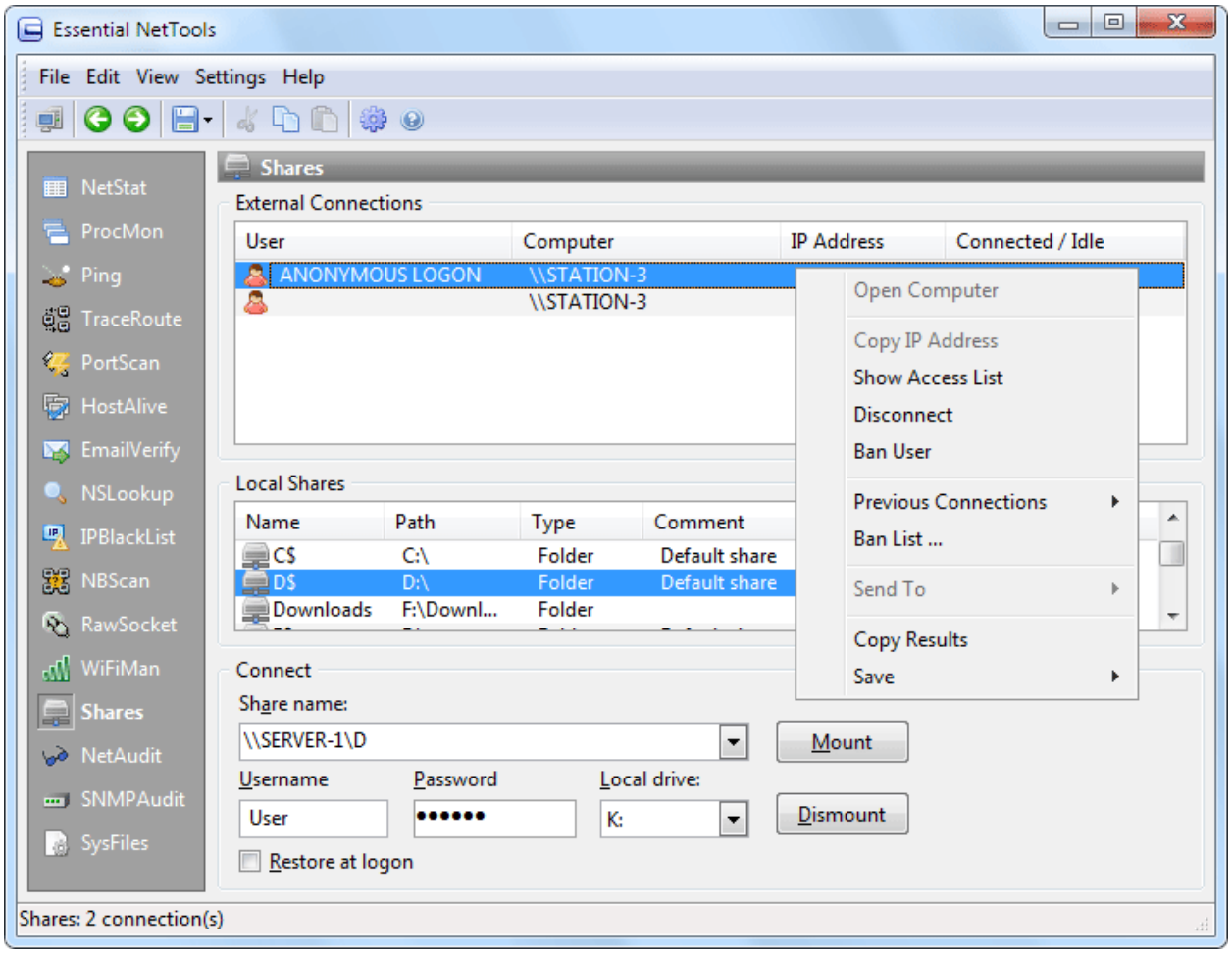
Rechtsklicken auf einen Datensatz blendet das Kontextmenü mit den Befehlen **[Verbinden]** und **[Trennen]** ein.
Die Gruppe **Bevorzugte Netzwerke (Profile)** listet voreingestellte Profile zur Verbindung mit drahtlosen Netzwerken auf. Sie können Profile erstellen, bearbeiten und löschen. Profilex- und -import im XML-Format ist nutzvoll, wenn Sie schnell Einstellungen von einem Computer auf einen anderen transferieren müssen oder wenn Sie Einstellungen über eine Gruppe von Anwendern verteilen möchten. Die folgenden Befehle stehen zur Verfügung:

- **Verwaltung** – Öffnet den Standarddialog zur Verwaltung drahtloser Netzwerke. Diese Option ist nur in Windows Vista oder neueren Operationssystemen wirksam. Nicht in Windows XP.
- **Von XML hinzufügen** – Fügt ein Netzwerkprofil aus einer XML-Datei hinzu.
- **In XML speichern** – Speichert ein Netzwerkprofil in eine XML-Datei.
- **als XML anzeigen** – Ermöglicht Ihnen, dass ausgewählte Netzwerkprofil als XML-Datei anzuzeigen.
- **Eigenschaften** – Bei Klick auf diesen Button (oder Doppelklick auf den ausgewählten Datensatz) wird der Profilkonfigurationsdialog eingeblendet. Die Authentifikation, die Datenverschlüsselung und andere Einstellungen können in diesem Dialog konfiguriert werden.
- **Hinzufügen** – Fügt ein neues Netzwerkprofil ein und ermöglicht Ihnen die Einstellungen zu konfigurieren.
- **Entfernen** – Löscht das ausgewählte Profil von der bevorzugten Netzwerkliste.

Falls Sie die Reihenfolge der bevorzugten Netzwerkprofile ändern möchten, benutzen Sie bitte die Button **[Auf]** und **[Ab]**, die rechts in der Liste **Bevorzugte Netzwerke (Profile)** angeordnet sind.

Shares

Das Tool **Shares** ermöglicht Ihnen, drei Aufgaben auszuführen: Überwachung der Verbindungen zu Ihren Ressourcen, lokale offene Ports anzeigen und das Verbinden zu entfernten Ressourcen über das Netzwerk.



Externe Verbindungen

Wenn das Programm eine externe Verbindung zu Ihrem Computer entdeckt, blendet es Ihnen die Informationen über den Benutzer ein, wie es oben gezeigt wird. Eine neue Verbindung wird auch durch einen Warnton und durch die veränderte Farbe des Systemablageicons angezeigt: das Icon wird rot.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Computer öffnen – versucht einen ausgewählten Computer zu öffnen. Wenn der Computer erreichbar ist, wird ein neues Windows Explorer-Fenster mit den Fernsteuerressourcen eingeblendet. Zur Nutzung dieser Funktion, müssen Sie den Client für Microsoft Netzwerke installiert haben.
IP-Adresse kopieren – kopiert die IP-Adresse des ausgewählten Computer's in die Zwischenablage.
Zugriffsliste anzeigen – öffnet ein Fenster mit der Auflistung lokaler Dateien, auf die durch den Benutzer zugegriffen wird.
Trennen – trennt die Verbindungen der ausgewählten Computer.
Benutzer sperren – fügt den ausgewählten Computername der Sperrliste hinzu. Wenn ein gesperrter Benutzer versucht sich mit Ihrem Computer zu verbinden, wird er oder sie automatisch getrennt.
Vorherige Verbindungen – zeigt das Protokoll mit früheren Verbindungen und ermöglicht Ihnen diese zu löschen.
Sperrliste – ermöglicht Ihnen die Sperrliste zu bearbeiten.
Senden an – sendet die ausgewählte IP-Adresse an andere Tools oder an SmartWhois.
Ergebnisse kopieren – kopiert die Verbindungstabelle in die Zwischenablage.
Speichern – speichert die Verbindungstabelle in eine Datei.

Wichtig: Das Unterbrechen bzw. Sperren von Benutzern darf nicht als ernsthafte Sicherheitsmaßname betrachtet werden. Bei der Unterbrechung eines Benutzers, weisen Sie das Betriebssystem nur an die aktuelle Verbindung zu unterbrechen, dies hindert den gesperrten Benutzer nicht daran in einigen Sekunden wieder eine Verbindung herzustellen. Dies kann solche Verbindungen verlangsamen. Wenn Sie einen unberechtigten Zugriff bemerken, wird empfohlen, dass Sie die Zugriffsrechte auf die freigegebenen Ressourcen durch Passwörter schützen.

Lokale Freigaben

Diese Auflistung zeigt die freigegebenen Ressourcen auf Ihrem Computer an.

Verbinden

Sie können dieses Tool benutzen, um sich über das Netzwerk mit entfernten Ressourcen zu verbinden. Für die Zuordnung (Mapping) einer entfernten Ressource zu Ihren lokalen freien Laufwerken, sollten Sie einen gültigen Freigabenamen in das Feld **Freigabenamen** eingeben. Ein gültiger Freigabenamen ist der Computername mit zwei vorangestellten Backslashes und einem folgenden Backslash und ein Ressourcenamen. Zum Beispiel, um das Verzeichnis "COMMON" auf dem Computer "STATION1" zuzuordnen, geben Sie ein:

\\STATION1\COMMON

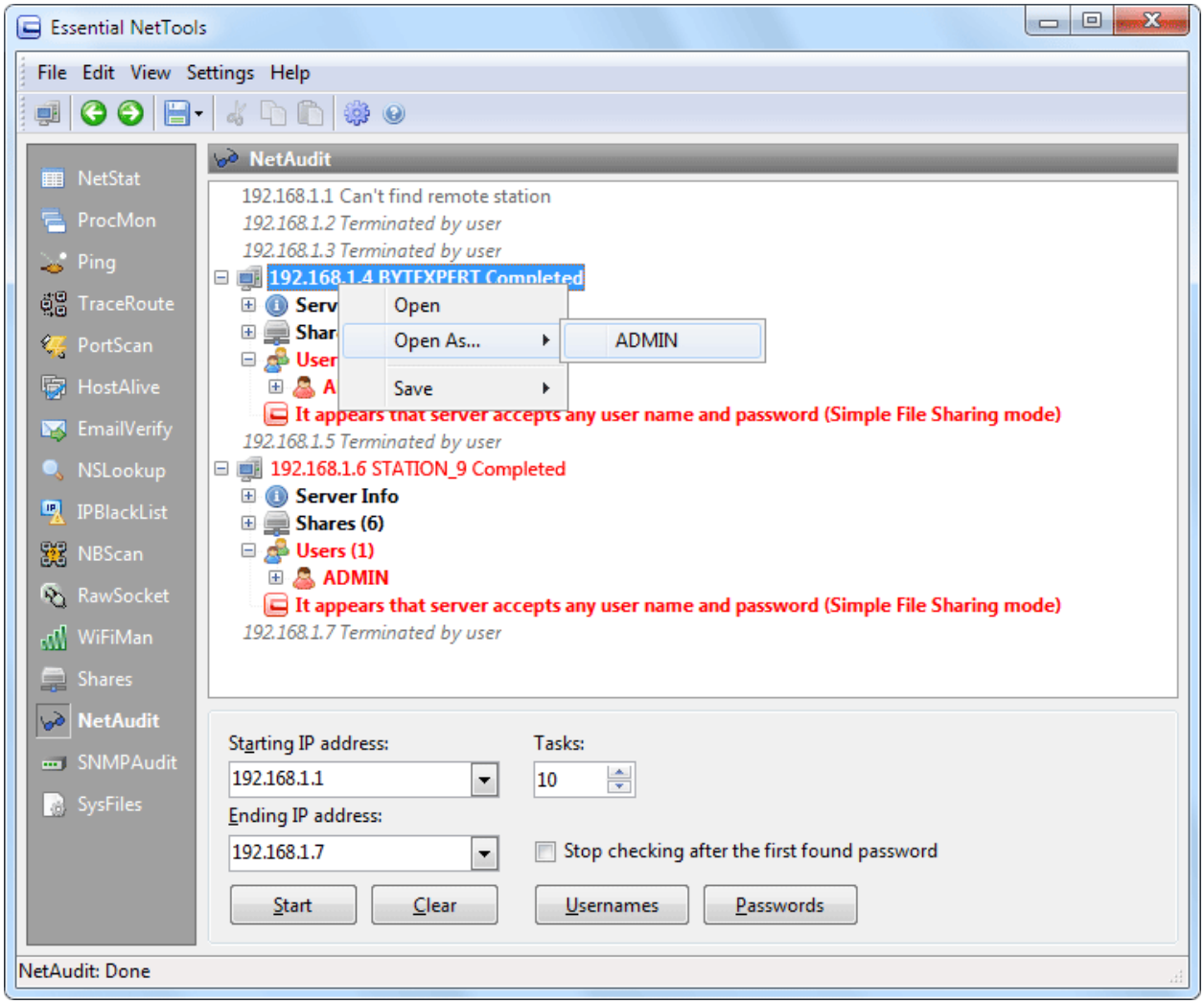
Geben Sie einen Benutzernamen und ein Passwort in den zugehörigen Feldern ein und wählen Sie einen freien Laufwerksbuchstaben aus der Drop-Down-Liste **Lokale Laufwerke**. Beachten Sie bitte, dass Ihr Computer in der Lage ist den entfernten Computernamen aufzulösen, den Sie einer zugehörenden IP-Adresse zugewiesen haben. Dies bedeutet, dass das Datenpaar IP-Adresse - Computername normalerweise in Ihrer LMHost-Datei vorhanden sein sollte. (Sie können dieses Paar der LMHost-Datei unter Benutzung des Tools SysFiles hinzufügen).

Klicken Sie schließlich auf **[Aufbauen]** um eine Freigabe einem lokalen Laufwerk zuzuordnen. Aktivieren Sie die Checkbox **Beim nächsten Logon wiederherstellen**, wenn Sie möchten, dass der Computer beim nächsten Logon diese Verbindung wieder herstellt. Zum Lösen dieser Verbindung klicken Sie auf den Button **[Abbauen]**. Beachten Sie, dass der Befehl **Abbauen** versuchen wird die Verbindung zum, im Feld **Lokales Laufwerk** spezifizierten Laufwerk, zu trennen; sollten mehrere Ressourcen verbunden sein, wählen Sie den zugehörigen Laufwerksbuchstaben.

NetAudit

NetAudit (NetBIOS Auditing Tool) ist ein Tool zur Prüfung von Netzwerken und Einzelplatzrechnern mit laufendem NetBIOS-File Sharing-Dienst. Dieses Tool wurde vor einigen Jahren als GNU-Kommandozeilen-Utility geschrieben und war sehr populär. Unser Tool wurde von Grund auf neu geschrieben, ist aber inspiriert von diesem populären Utility.

Trotzdem, dass sehr leistungsstarke und teuere Lösungen existieren um Hunderte von Schlupflöchern in Netzwerken zu überprüfen, stammen die meisten Probleme von der unkorrekten Konfiguration des NetBIOS-Resource Sharing-Dienstes. Mit NetAudit können Sie leicht Ihr Netzwerk und/oder Ihren Einzelplatzrechner überprüfen. Denken Sie daran, dass Sie Administratorrechte benötigen, bevor Sie das Netzwerk überprüfen.



Bevor Sie die Überprüfung beginnen, sollten Sie die Start-IP- und die End-IP-Adresse in die Felder **Start-IP** und **End-IP** eingeben, wie oben gezeigt. Beachten Sie bitte, dass die ersten 3 Zeichen der Start- und End-IP-Adresse gleich sein müssen. Sie können den Benutzernamen und das Passwort konfigurieren, wenn Sie auf die zugehörigen Button **[Benutzernamen]** und **[Passwörter]** klicken. Diese Listen werden zur Überprüfung möglicher, potentieller Eindringversuche genutzt, und Sie können diese basierend auf der durch NBScan beschafften Namensliste individuell anpassen. Ein Null-Passwort wird immer automatisch als erstes Passwort der Liste hinzugefügt, weil es nicht druckbar ist; trotzdem ist es ein gutes Passwort und immer einen Versuch wert. Alle Passwörter können mit allen Benutzernamen verwendet werden. Falls Sie vorher die Listen modifiziert haben, können Sie durch klicken auf den Button **[Standardwerte]**, diese auf die Standardwerte zurücksetzen.

Sie können die Anzahl der gleichzeitig zu überprüfenden Adressen in der Spinbox einstellen. Sie können auch die Überprüfung einzelner Hosts auf das erste erfolgreich empfangene Passwort begrenzen, indem Sie die Checkbox **Überprüfung nach Empfand des ersten Passwortes stoppen** aktivieren. Dies ermöglicht Ihnen, die Suche nach weiteren Passwörtern zu stoppen und direkt mit der nächsten Adresse fortzufahren.

Zum Start der Überprüfung klicken Sie auf den Button **[Starten]**. Der Prozess kann jederzeit durch klicken auf den Button **[Stoppen]** gestoppt werden. Bedenken Sie, dass die Überprüfung eines Computers ein langdauernder Prozess ist und von vielen Faktoren abhängt; Sie sollten sich auf eine längere Wartezeit einrichten, besonders wenn Sie einen großen Bereich von IP-Adressen eingegeben haben. Wenn NetAudit während der Prüfung eine Sicherheitslücke entdeckt, wird ein Warnton abgespielt und das Systemablage-Icon beginnt zu blinken.

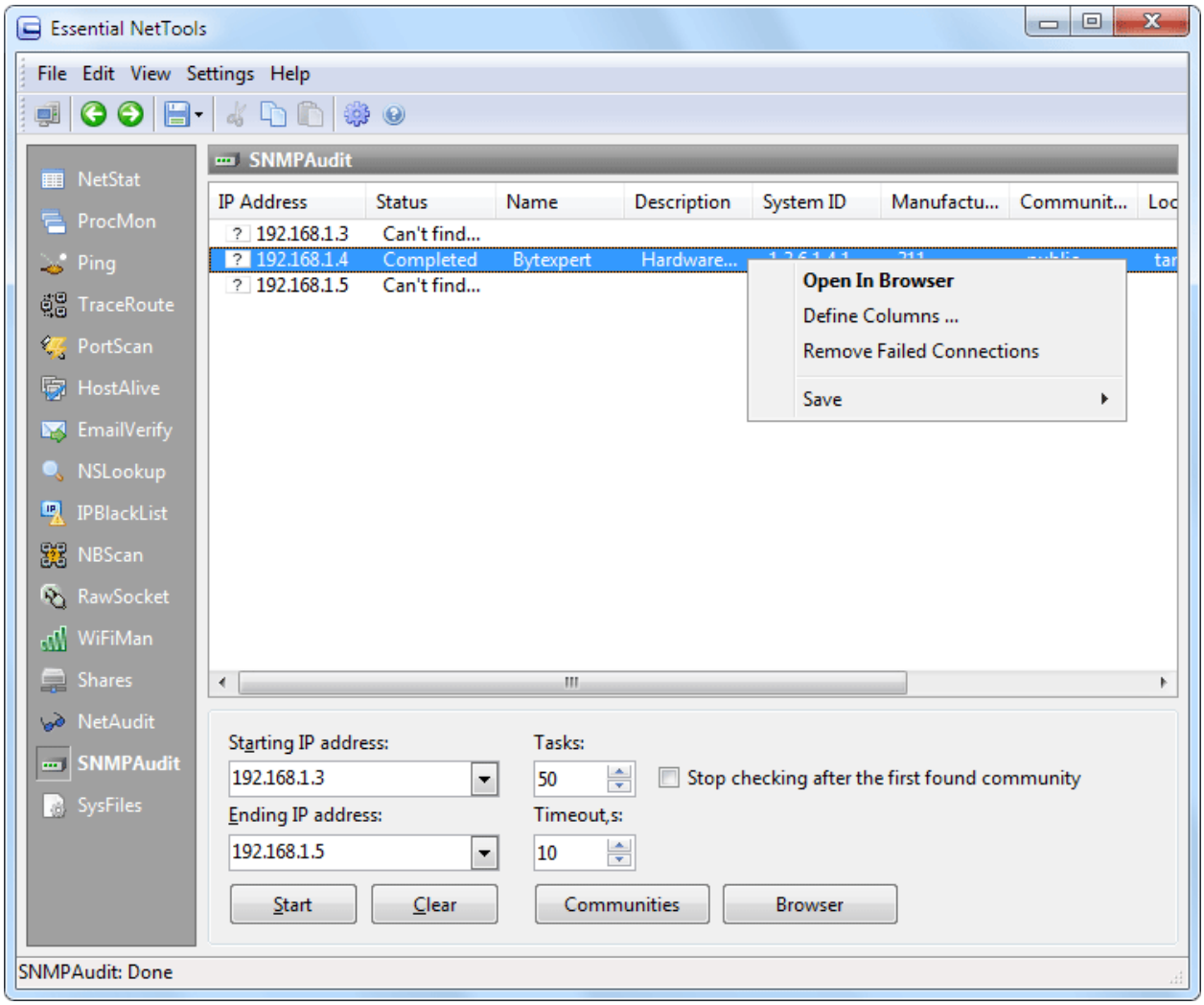
Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Kopieren – kopiert den ausgewählten Text in die Zwischenablage.
Alles markieren – Markiert den gesamten Text im Fenster.
Speichern – speichert das Protokoll in eine Datei.

SNMPAudit

SNMPAudit ist ein Tool zur schnellen Ermittlung und Informationsansammlung von SNMP-aktiven Geräten. Dieses Tool kann zur Abfrage der Geräte genutzt werden, die im spezifizierten Adressbereich präsent sind. Das SNMP-Protokoll (Simple Network Management Protocol) wird zur Verwaltung verschiedener Netzwerkgeräte benutzt, wie Server, Router, Switche usw. Bei einem SNMP-aktiviertem Gerät ist es möglich eine große Datenmenge, über den Status und die Funktionen des Gerätes, anzusammeln.

Das SNMP-Protokoll benutzt einen Gemeinschaftsausdruck zur Anzeige der Zugehörigkeit einiger Modelle eines SNMP-Gerätes, bezüglich der Gerätefunktionalität und Verwendungzweck. Ein SNMP-Gerät kann so konfiguriert werden, dass es zu mehreren Gemeinschaften gehört. Bei Verbindung zu einem SNMP-Gerät, zeigt die Bedienoberfläche (z.B. Essential NetTools), die Gemeinschaft an, an der die Abfrage adressiert ist. Es ist wichtig, zu wissen, wem das Gerät gehört. Wenn die Gemeinschaft unkorrekt spezifiziert ist, wird das Gerät diese Abfrage einfach ignorieren. Die Gemeinschaft kann ebenso ein Authorisierungselement (ähnlich wie ein Passwort) benutzen, welches erforderlich ist, um Zugriff auf das SNMP-aktive Gerät und Daten von Ihm zu erhalten.



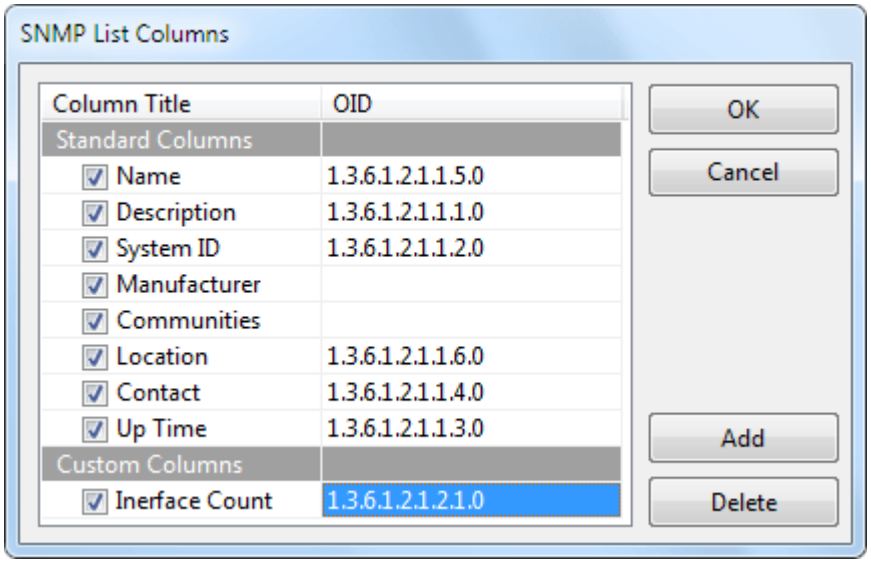
Der üblich benutzte Gemeinschaftsnamen ist '**public**'. Sie können Ihre Gemeinschaft zur Liste der abgefragten Gemeinschaften durch klicken auf den Button **[Gemeinschaft]** hinzufügen. Beachten Sie bitte, dass SNMPAudit immer auf die Verfügbarkeit der Gemeinschaft **public** prüft, auch wenn Sie nicht in der Gemeinschaftsliste ist. Essential NetTools wird jedes Element (z.B. Community) von der Gemeinschaftsliste, für jede Adresse des spezifizierten Bereichs, versuchen. Wenn Sie mit gerade einer entdeckten Gemeinschaft pro Host zufrieden sind, dann aktivieren Sie die Checkbox **Überprüfung nach der ersten gefundenen Gemeinschaft stoppen**. In diesem Fall wird SNMPAudit nach der ersten gefundenen Gemeinschaft stoppen und die noch übrigen Gemeinschaften der Auflistung nicht überprüfen. Das Programm wird dann mit der Abfrage anderer Adressen des spezifizierten Bereichs fortfahren.

Bevor Sie mit der Abtastung starten, sollten Sie die Start- und End-IP-Adresse in die Felder **Start-IP** und **End-IP** eingeben, wie es oben gezeigt wird. Stellen Sie die Anzahl der gleichzeitigen Verbindungen und Verbindungszeitüberschreitungen in den vorgesehenen Feldern ein. Klicken Sie auf den Button **[Start]** um den Abtastvorgang zu starten. Die IP-Adressen, der Status der abgefragten Hosts und andere Informationen werden im Fenster **SNMPAudit** während der Abtastung eingeblendet. Falls ein Host kein aktiviertes SNMP-Gerät ist, werden Sie Meldungen in der Spalte Status sehen wie, "Kann die ferngesteuerte Station nicht finden" oder "Verbindung abgelehnt" (Mit dem Kontextbefehl **Fehlgeschlagene Verbindungen entfernen** können Sie die fehlgeschlagenen Verbindungen aus der Auflistung entfernen). Wenn Sie das Abtasten abbrechen möchten, klicken Sie auf den Button **[Stop].** Klicken auf den Button **[Leeren]** entleert die Auflistung im Hauptfenster; Ihre aktuellen Einstellungen wie Start-

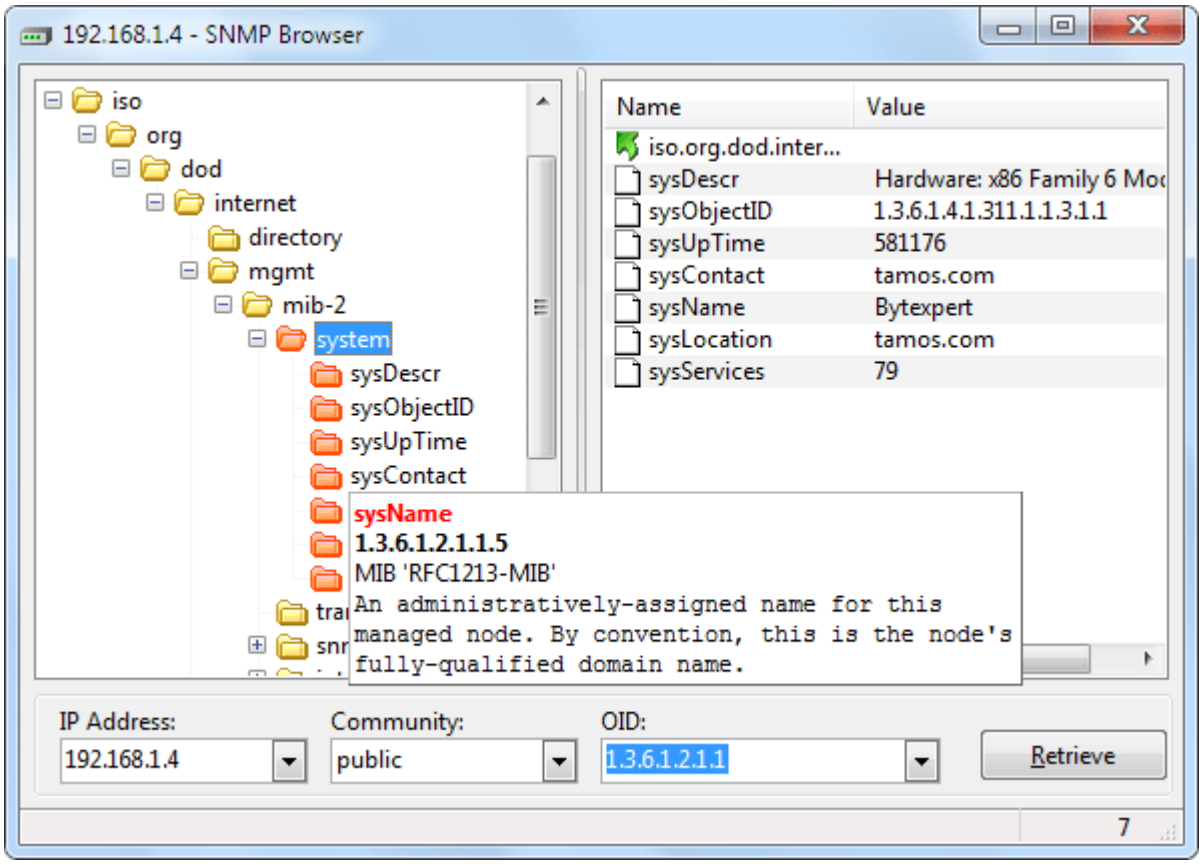
und End-IP-Adressen, Einstellungen der Anzahl der gleichzeitigen Verbindungen und Verbindungszeitüberschreitungen bleiben erhalten.

Nach der Entdeckung eines Gerätes, das zu einer Gemeinschaft aus der Auflistung gehört, führt SNMPAudit eine Abfrage für die Primärdatencharaterisierung des Gerätes durch und zeigt die gesammelten Daten in der Auflistung an. Sie können die folgenden Datenspalten zur Anzeige im Hauptfenster des SNMPAudit-Tools auswählen: Gerätename, Gerätebeschreibung, Gerätestandort, Gerätehersteller, System-ID, Admin-Kontaktinfo und die Betriebszeit. Rechtsklicken Sie auf das Hauptfenster und wählen Sie aus dem Ausklappmenü **Spalten definieren**. Sie können dann die Spalten aktivieren und selbstdefinierte Datenspalten hinzufügen, die Sie angezeigt bekommen möchten.

Sie können die Einstellungen der Standardspalten nicht modifizieren oder löschen. Wenn Sie selbsteingestellte Spalten hinzufügen müssen Sie den korrekten Pfad zu den SNMP-Daten in die Spalte **OID** eintragen. Sie können die Aufklappliste benutzen oder nach OID in der MIB-Datenbank suchen. Wenn Sie die Spalte löschen möchten, wählen Sie diese aus und klicken auf den Button **[Löschen]**.



Wenn Sie ein besonderes SNMP-aktives Gerät von der Geräteliste überprüfen möchten, doppelklicken Sie darauf oder wählen es aus und klicken auf den Button **[Durchsuchen].** Ein SNMP-Browser-Fenster wird geöffnet.



SNMP Browser ermöglicht Ihnen alle empfangenen verfügbaren Daten der vorgegebenen Gemeinschaft vom SNMP-Gerät zu durchsuchen. Wenn die dazugehörende Beschreibung in der MIB-Datenbank existiert, sind Sie auch in der Lage die Beschreibung der empfangenen Daten zu lesen.

Geben Sie die IP-Adresse des Gerätes ein, community und starten Sie OID im SNMP Browser-Fenster. Klicken Sie auf **[Empfangen]** oder drücken Sie auf **[ENTER]**. Das Programm wird alle zugrunde liegenden Datenebenen abfragen beginnend mit der spezifizierten OID. Die abgefragte Datenstruktur wird im linken Fensterausschnitt eingeblendet. Wenn Sie nicht sicher sind, mit welcher OID Sie starten sollen, wählen Sie den Startwert aus dem Baum von der linken Seite. In diesem Fall wird das Feld **OID** mit dem Pfad zum ausgewählten Baumelement automatisch gefüllt. Normalerweise gehören alle Daten zu iso.org oder 1.3-Abzweigen – bitte wählen Sie OID **1** oder **1.3** für die Abfrage aller verfügbarer Daten des ausgewählten Gerätes.

Die aktuell vom Gerät abgefragten Daten werden im rechten Fensterausschnitt eingeblendet. Vom Gerät abgefragte Datenfelder werden im linken Fensterausschnitt eingeblendet und mit einem hervorgehobenen Icon markiert.

Standardmäßig zeigt der rechte Bildausschnitt die zum ausgewählten Baumelement (Windows Explorer-Stil) gehörenden Daten. Wenn Sie alle Daten der nachfolgenden Ebenen anzeigen möchten, Rechtsklicken Sie auf die Auflistung und wählen **Alle Werte wählen** aus dem Ausklappmenü.

Sie können so viele SNMP Browser-Fenster öffnen wie Sie möchten.

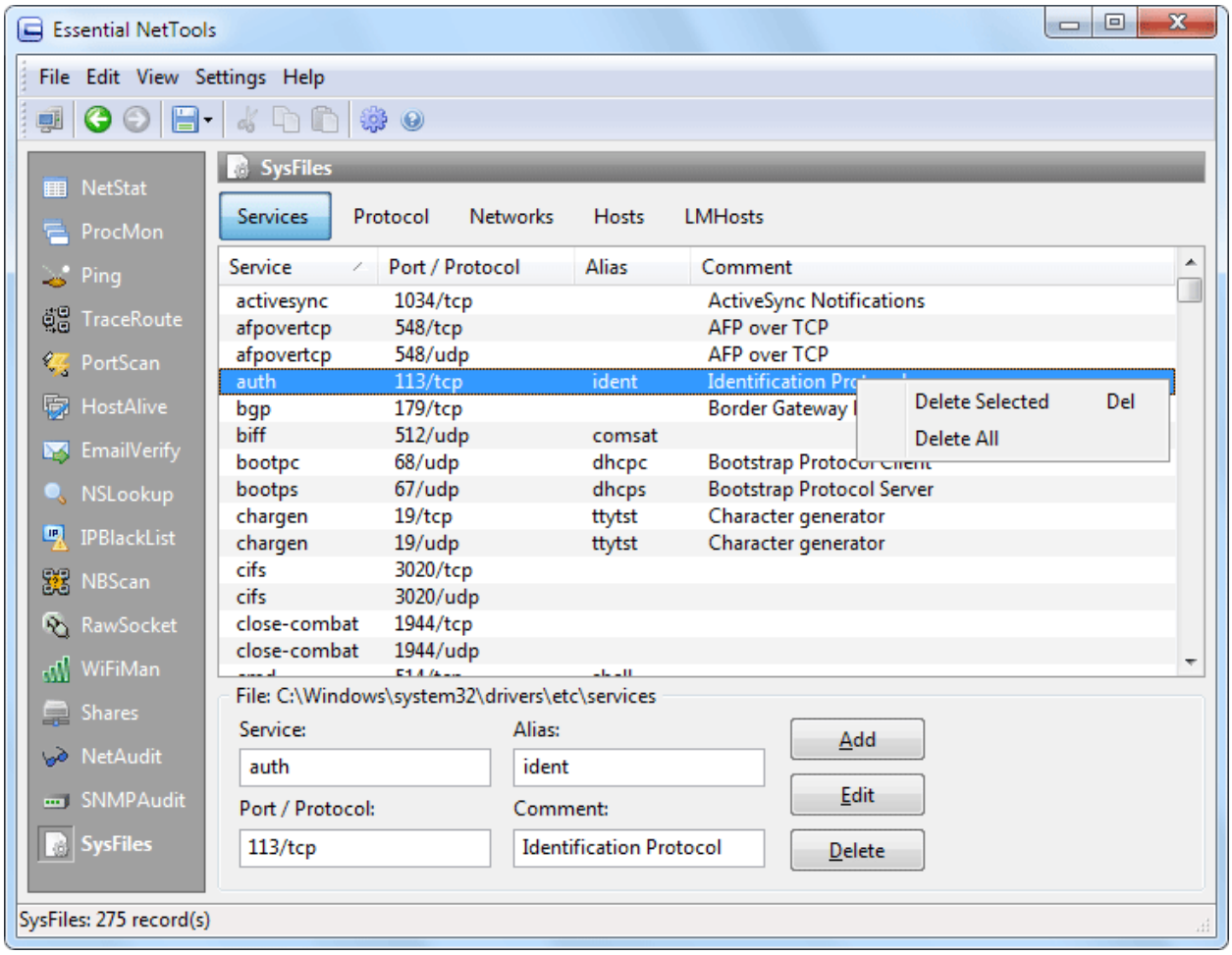
MIB-Datenbanken

Mit dem ersten Browser-Start, wird Essential NetTools MIB-Datenbanken vom Programmverzeichnis (standardmäßig C:\Programme\EssNetTools3\SNMP\MIB) laden und zeigt diese als Baumansicht. MIB steht für Management Information Base und OID steht für Object ID. MIB-Datenbanken beinhalten den Zugangspfad zu verschiedenen Daten (OID) des SNMP-aktiven Gerätes und die Beschreibung der Daten. Sie können die Beschreibung eines Elementes (falls vorhanden) erhalten, wenn Sie den Pointer über ein zugehörige Baumelement bewegen. Die Beschreibung wird in einem Ausklapphinweis angezeigt.

MIB-Datenbanken können allgemein oder spezifisch sein, für einen besonderen Hersteller, ein besonderes Modell und die Geräteklasse. Essential NetTools wird vertrieben mit einem MIB-Basissatz, der für die meisten Geräte ausreichend ist. Sie können sich immer Datenbanken von der öffentlichen Webseite http://www.mibdepot.com/ beschaffen. Speichern Sie diese in das Applikationsverzeichnis (standardmäßig C:\Programme\EssNetTools3\SNMP\MIB) und starten das Programm erneut. Beachten Sie, das Sie immer in der Lage sind die Daten ohne eine Begrenzung abzufragen, sogar wenn Sie nicht die richtige MIB-Datenbank für das Gerät besitzen. MIB-Datenbanken stellen nur visuell lesbare Beschreibungen der abgefragten Daten und deren Verwendungszweck bereit.

SysFiles

Sie können dieses Tool zur Bearbeitung der fünf wichtigsten Systemdateien benutzen: Dienste, Protokolle, Netzwerke, Hosts und LMHosts. Wenn das Programm gestartet wird, liest das Tool Datensätze von diesen Dateien, wie weiter unten gezeigt wird:



Dieses Tool ist für Computerspezialisten gedacht, deshalb bearbeiten Sie diese Dateien nur, wenn Ihnen genau bewusst ist, was Sie tun.

Rechtsklicken auf das Programmfenster öffnet ein Menü mit folgenden Befehlen:

Auswahl löschen – entfernt den/die ausgewählten Datensatz/-sätze.
Alle löschen – entfernt alle Datensätze.

Optionen

Sie können den Dialog **Einstellungen => Optionen** zur Konfiguration der erweiterten Optionen benutzen.

Werkzeuge

NetStat

Vollständigen Pfad anzeigen – aktivieren Sie diese Checkbox, wenn NetStat den vollständigen Prozesspfad und den dazugehörenden Port anzeigen soll (z.B. 'C:\Files\Program.exe' ist ein Vollpfad, wogegen 'Program.exe' ein kurzer Pfad ist).

Portnummern in Dienstnamen konvertieren – Aktivieren Sie diese Checkbox, wenn NetStat Dienstnamen anzeigen soll anstelle von Portnummern. Zum Beispiel: wenn die Checkbox aktiviert ist, wird Port 21 als ftp angezeigt und Port 23 als telnet. Das Programm konvertiert den numerischen Wert, unter Benutzung der unter Windows installierten Dienstdatei, zu einem Dienstnamen. Sie können diese Datei mit dem Tool SysFiles editieren.

DNS-Auflösung abschalten – aktivieren Sie diese Checkbox wenn das Programm keine DNS-Rückwärtssuche auf die IP-Adressen durchführen soll. Wenn Sie diese Fuktion aktivieren, bleibt die Spalte Hostname in NetStat leer.

NBScan und PortScan

Subnet-Grenzen ausschließen – aktivieren Sie diese Checkbox, wenn das Programm IP-Adressen mit dem Ende .0 oder .255 überspringen soll.

Bei neuen Abfragen Liste leeren – aktivieren Sie diese Checkbox, wenn das Programm jedesmal die Auflistung leeren soll, wenn Sie die Abtastung eines neuen IP-Adressbereich starten. Wenn die Checkbox nicht aktiviert ist, wird das Programm die Ergebnisse aller vorheriger Abfragen weiter aufbewahren und neue Elemente automatisch nach IP-Adressen einsortieren.

Intervalle automatisch aktualisieren – Setzt automatische Aktualisierungsintervalle für NetStat und ProcMon, wenn die automatische Aktualisierung eingeschaltet ist. Für ProcMon kann der automatische Aktualisierungsintervall für die Ansammlung der CPU-Auslastungsstatistiken spezifiziert werden.

Bedienoberfläche

Warntöne

NetAudit Sicherheitslückenerkennung, Externe Verbindungserkennung – aktivieren Sie diese Checkbox, um einige der Programmereignisse mit Warntönen zu untermalen. Zum Wechseln der Standardsounddateien, klicken Sie auf den Button **[Durchsuchen]** in der Nähe der Ereignisbeschreibung und lokalisieren Sie eine neue Sounddatei im WAV-Format. Zum Testen der Datei klicken Sie auf den Button mit dem Lautsprecher-Icon.

Visuelle Effekte

Listenfarben wechseln – aktivieren Sie diese Checkbox, wenn das Programm die Dateillisten zweifarbig anzeigen soll. Klicken Sie auf Farbe 1 und Farbe 2 um die Zeilenfarben zweifarbig einzustellen.

Farbe - Neues NetStat-Element – benutzen Sie diese Checkbox zur Einstellung der temporären Hervorhebungsfarbe für neue NetStat-Einträge.

Farbe – Gelöschte NetStat-Elemente – benutzen Sie diese Checkbox zur Einstellung der Hervorhebungsfarbe, der in der Liste zum Löschen markierten Einträge.

Maus Hot-Tracking – wenn diese Checkbox aktiviert ist, wird ein visuelles Feedback eingeblendet, wenn der Pointer über ein Element geführt wird; Sie können auch ein Element auswählen indem Sie den Pointer anhalten.

Flache Bildlaufleiste – flacht die Bildlaufleiste in allen Programmanzeigen ab (nicht verfügbar unter Windows XP/Vista).

Geostandort

Geostandort ist eine IP-Länderzuordnung für IP-Adressen. Wenn diese Funktionalität aktiviert ist, überprüft Essential NetTools eine Internetdatenbank um Länderinformationen zu jeder IP-Adresse zu beschaffen. Sie können das Programm so konfigurieren, dass der ISO-Ländercode, der Ländername oder die Landesflagge in der Nähe der IP-Adresse angezeigt werden. Sie können Geostandort ebenso abschalten. Für einige IP-Adressen, wie reservierte Adressen (z.B. 192.168.*.* oder 10.*.*.*) kann keine Information beschafft werden. In solchen Fällen, wird der Ländername nicht angezeigt oder falls Sie die Landesflaggenoption benutzen, wird eine Flagge mit Fragezeichen eingeblendet.

Weil die IP-Zuordnung sich laufend ändert, ist es wichtig, dass Sie immer eine aktuelle Version von Essential NetTools haben. Eine aktuelle Datenbank ist in jeder Essential NetTools-Version enthalten. Eine aktuelle Datenbank besitzt 98% Treffsicherheit. Ohne Updates, fällt die Treffsicherheit jedes Jahr prozentual um ungefähr 15%.

Verschiedenes

Mit Windows starten – wenn diese Checkbox aktiviert ist, startet das Programm automatisch jedesmal wenn Sie Windows starten.

In die Systemablage minimieren – wenn diese Checkbox aktiviert ist, wird das Programm nicht geschlossen wenn Sie auf das 'x-Zeichen' in der oberen rechten Fensterecke klicken. Stattdessen wird es in die Systemablage minimiert. Zum Beenden das Programms benutzen Sie den Befehl **Datei => Beenden**.

Bei Minimierung in der Taskleiste nicht anzeigen – aktivieren Sie diese Checkbox, wenn der Programm-Button nicht in der Taskleiste angezeigt werden soll. Bei Aktivierung der Checkbox, benutzen Sie das Systemablage-Icon um das Programmfenster nach einer Minimierung wieder zu öffnen.

Beim Toolwechsel die Fokussierung auf die Eingabefelder legen – aktivieren Sie diese Checkbox wenn das Programm bei jedem Toolwechsel den Fokus automatisch auf die Eingabefelder, wie IP-Adressfelder legen soll.

IP-Adressfelder automatisch ausfüllen – wenn diese Checkbox aktiviert wird, füllt das Programm das Feld **End-IP-Adresse** in NBScan, PortScan und NetAudit automatisch aus, wenn Sie das Feld **Start-IP-Adresse** ausfüllen.

Individual-Ping-/TraceRoute-Mitteilung – ermöglicht Ihnen, die Standardmitteilung in Ping- und TraceRoute-Paketen zu ändern. Zur Nutzung dieser Fähigkeit, aktivieren Sie diese Checkbox und geben Ihren eigenen Meldungstext in die Textbox unten ein.

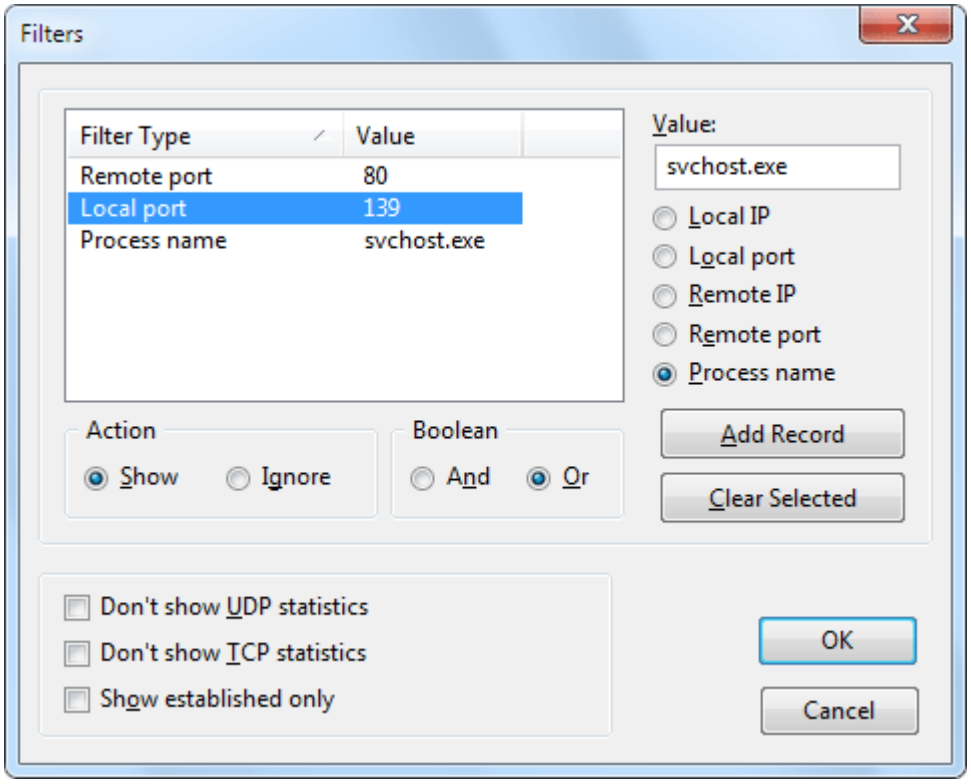
Automatische Updates aktivieren – wenn diese Checkbox aktiviert ist, wird das Programm automatisch auf der TamoSoft-Webseite nach Updates suchen.

Intervall zwischen Überprüfungen (Tage) – ermöglicht Ihnen einen Überprüfungsintervall für Updates festzulegen.

Jetzt prüfen – führt unmittelbar eine Update-Überprüfung durch.

Filter

Dieser Dialog ermöglicht Ihnen Filter zu konfigurieren, die zur Informationsanzeige im Fenster NetStat benutzt werden. Standardmäßig listet NetStat alle Netzwerkverbindungen Ihres Computers auf. Diese Liste ist natürlich ziemlich lang, aber Sie können einige für Sie unwichtige Elemente ausfiltern.



Zur Erstellung eines neuen Filters, geben Sie einen **Wert** ein, wählen den Filtertyp (Lokale IP, Lokaler Port usw.) und klicken auf **[Datensatz hinzufügen]**. Zum Entfernen eines Filters, wählen Sie diesen aus der Liste aus und klicken auf **[Auswahl entfernen]**. Wenn Sie einen oder mehrere neue Filter erstellt haben, sollten Sie eine **Aktion** wählen. Wenn Sie **Anzeigen** wählen, blendet NetStat nur die Verbindungen ein, die mit dem(n) Filter(n) übereinstimmen. Wählen Sie **Ignorieren**, wird NetStat keine Verbindung einblenden, die mit dem(n) Filter(n) übereinstimmt. Falls Sie mehrfache Filter erzeugt haben, können Sie ebenso die Bool'sche Logik wählen: es kann entweder AND (Filter 1 und Filter 2 und Filter 3 usw.) oder OR (Filter 1 oder Filter 2 oder Filter 3 usw.) benutzt werden. Die Bildschirmabbildung weiter unten illustriert einen Regelsatz, der NetStat veranlasst die Verbindungen auszublenden, bei denen der entfernte Port 80 oder der lokale Port 139 ist oder der Prozessname svchost.exe ist.

Zusätzlich können Sie die folgenden Basisfilter benutzen:

UDP-Statistiken nicht anzeigen – aktivieren Sie diese Checkbox, wenn keine UDP-Verbindungen im NetStat-Fenster angezeigt werden sollen.

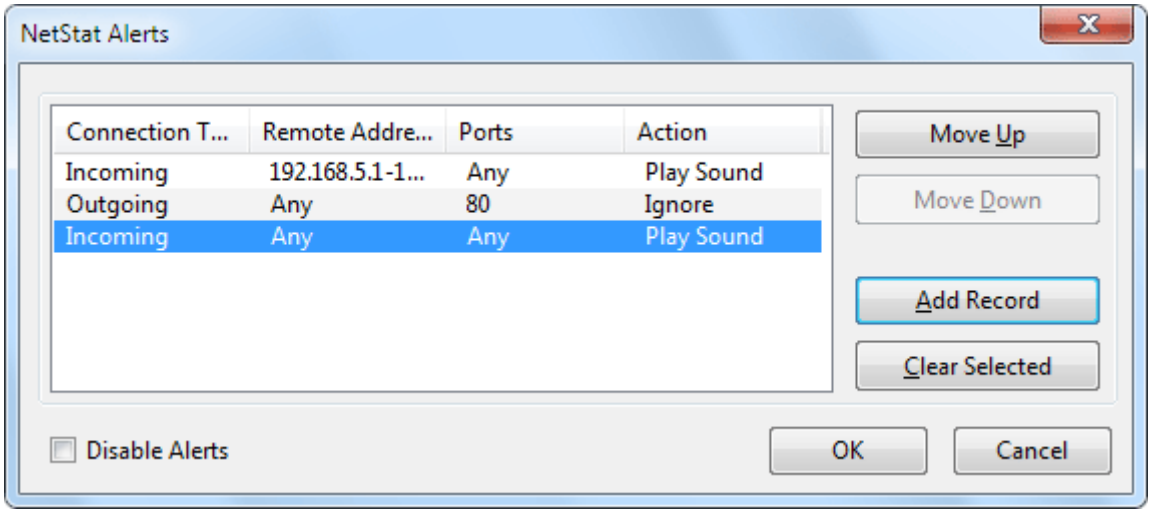
TCP-Statistiken nicht anzeigen – aktivieren Sie diese Checkbox, wenn keine TCP-Verbindungen im NetStat-Fenster angezeigt werden sollen.

Nur Bestehende Verbindungen anzeigen – aktivieren Sie diese Checkbox, wenn NetStat nur die bestehenden Verbindungen im NetStat-Fenster angezeigt werden sollen. Alle anderen Verbindungen (horchend, geschlossen usw.) werden nicht aufgelistet.

Sie können temporär Filter deaktivieren, wählen Sie dazu im NetStat-Kontextmenü den Befehl **Filter deaktivieren**.

Warnsignale

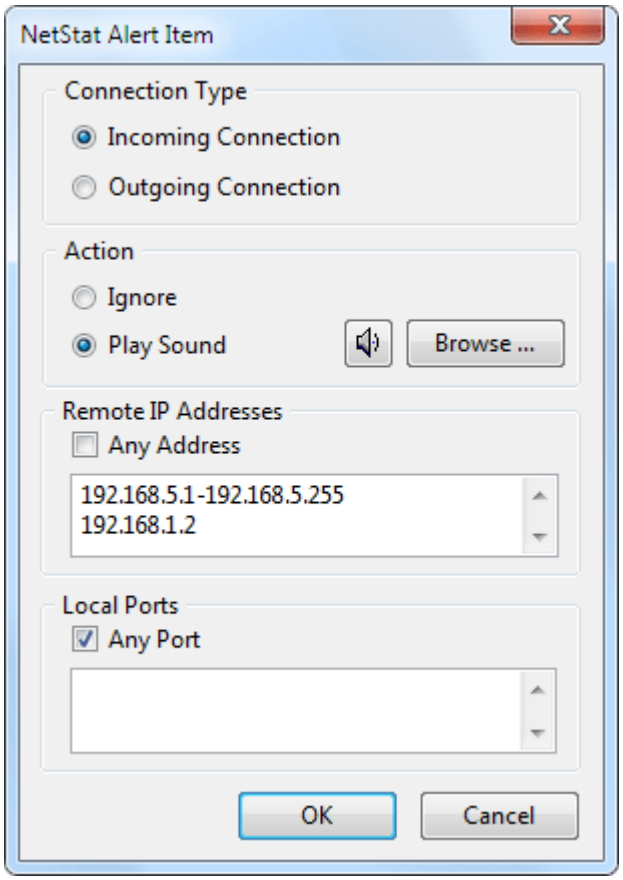
Dieser Dialog ermöglicht Ihnen, die Warnsignalliste für verschiedene ein- und ausgehende Verbindungen zu konfigurieren.



Die folgenden Warnsignaltypen stehen zur Verfügung:

- Eingehende Verbindung von einer spezifizierten IP-Adresse oder einem IP-Adressbereich
- Eingehende Verbindung zu einem spezifizierten lokalen Port oder Portbereich
- Ausgehende Verbindung zu einer spezifizierten IP-Adresse oder einem IP-Adressbereich
- Ausgehende Verbindung zu einem spezifizierten entfernten Port oder entfernten Portbereich

Um ein neue Warnsignal zu erstellen, klicken Sie auf den Button **[Datensatz hinzufügen]**.



Verbindungstyp – wählen Sie den Verbindungstyp: ein- oder ausgehend.

Aktion – wählen Sie die Aktion, die stattfindet, wenn die Warnung ausgelöst wird: **Sound abspielen** – spielt eine Sounddatei ab. Auswahl der Option **Ignorieren** lässt das Programm bestimmte Verbindungstypen von der Alarmierung ausschließen. Zum Beispiel, wenn Sie alle eingehenden Verbindungen überwachen möchten, können Sie dem lokalen Port 80 eine Warnung zuordnen, wenn der Verbindungstyp eingehend und die lokale Portnummer 80 ist, und wählen Sie die Aktion **Ignorieren** für diesen Alarm. Beachten

Sie, das die Warnfunktion auf das erste Auftreten einer Verbindung achtet, die dem spezifizierten Alarm entspricht; deshalb muss die ausgeschlossene Warnung die erste in der Auflistung sein, anderenfalls wird sie durch das Programm nicht gelesen und alle Verbindungen auf Port 80 lösen diesen Alarm aus.

Entfernte IP-Adressen – eine oder mehrere IP-Adressen oder ein Adressbereich, eine Verbindung von der eine Warnung ausgelöst wird. Ist die Checkbox **Jede Adresse** aktiviert, dann wird durch jede Adresse ein Warnton ausgelöst.

Lokale Ports, Entfernte Ports – ein oder mehrere lokale oder entfernte Ports oder ein Portbereich können festgelegt werden. Wenn die Checkbox **Jeder Port** aktiviert ist, dann löst jeder lokale oder entfernte Port einen Alarm aus, in Abhängigkeit zum unter **Verbindungstyp** angezeigten Verbindungstyp.

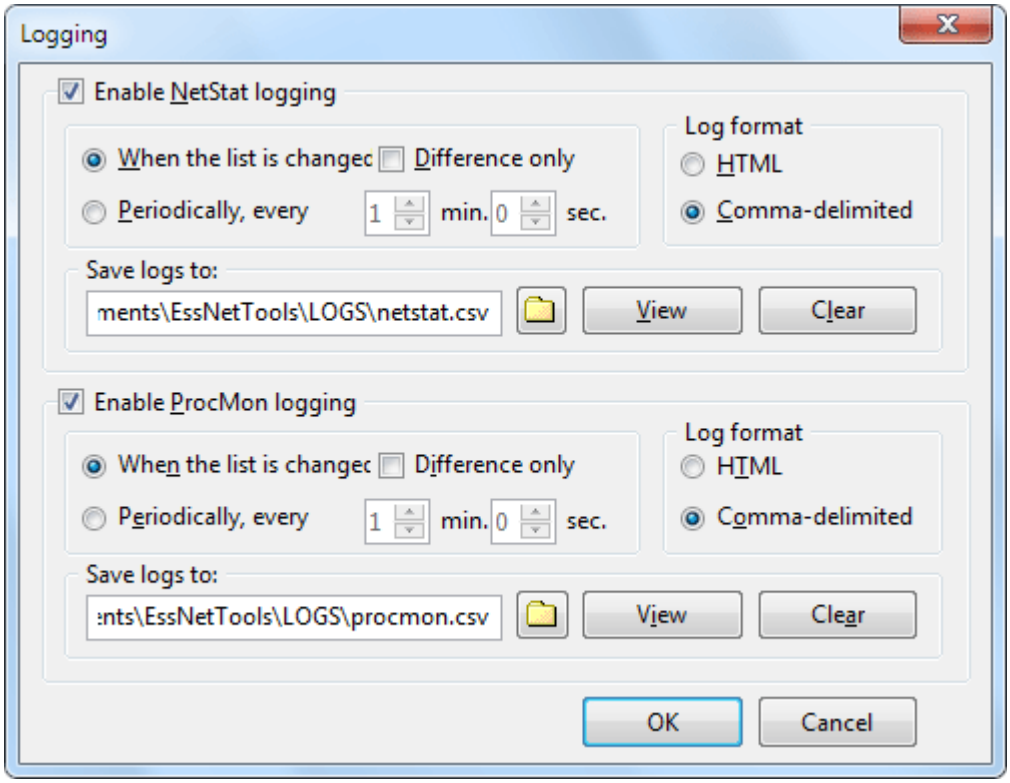
Nach dem die Warnung erstellt ist, können Sie diese bearbeiten, indem Sie in der Warnliste darauf doppelklicken. Sie können die Lesereihenfolge der Warnungen ändern, benutzen Sie dazu die Button **[Nach Oben]** und **[Nach Unten]** ändern. Sie können mit dem Button **[Auswahl löschen]** eine Warnung löschen.

Die Warnungen werden in absteigender Reihenfolge gelesen. Die Suche ist mit der ersten Übereinstimmung beendet; alle übrigen Warnungen werden nicht ausgewertet.

Aktivieren der Checkbox **Warnsignale deaktivieren** im Fenster **Warnungen**, deaktiviert temporär alle Warnungen.

Protokollierung

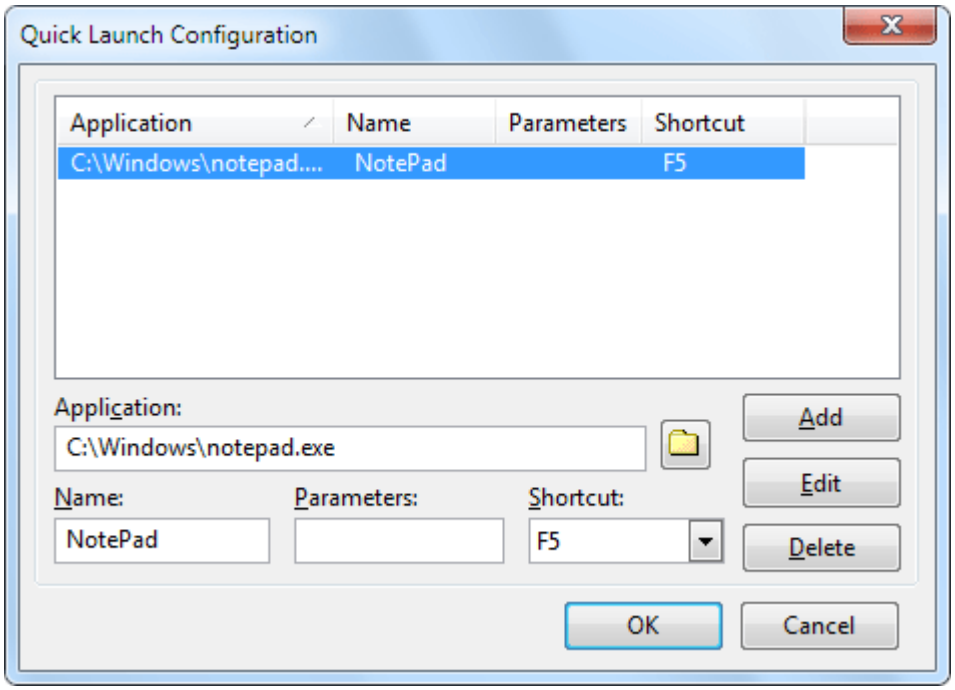
Dieser Dialog ermöglicht Ihnen die Protokollierung für NetStat und ProcMon zu aktivieren und zu konfigurieren.



Sie können entweder die aktuelle NetStat- oder ProcMonauflistung **Bei Änderung der Auflistung** oder **Periodisch** durch festgelegte Intervalle, vom Programm speichern lassen. Wenn Sie die Protokollgröße verkleinern möchten, aktivieren Sie die Checkbox **Nur Unterschiede**, es werden dann nur hinzugefügte oder gelöschte Einträge seit der letzten Listenänderung protokolliert. Sie können ebenso das Ausgabeformat bestimmen, HTML oder Kommagetrennt, den Dateinamen und den Pfad zur Speicherung der Protokolldatei festlegen.

Schnellstart

Sie können diesen Dialog dazu benutzen, neue Elemente dem Menü **Datei => Schnellstart** hinzuzufügen. Nach dem Hinzufügen neuer Menüelemente, können Sie das Programm als bequemen Startplatz für andere Applikationen benutzen.



Um ein neues Element hinzuzufügen, geben Sie im Feld **Applikation** den Pfad zu der Applikation und im Feld **Name** einen beliebigen Namen ein. Das Feld **Name** wird im Menü **Datei => Schnellstart** benutzt. Sie können auch optionale Parameter benutzen, diese werden an die Applikation übergeben und verbinden ein Tastaturkürzel mit dem Element, so dass Sie Ihre Applikation mit einem einzigen Klick starten können. Nachdem Sie diese Informationen eingegeben haben, klicken Sie auf den Button **[Hinzufügen]** und schließen diesen Dialog. Ein neues Element wurde dem Menü **Datei => Schnellstart** hinzugefügt.

Das Feld **Applikation** muss nicht unbedingt einen Dateinamen beinhalten. Sie können ebenso den Pfad zu einer nicht startbaren Datei eingeben, solange diese Datei mit einer Applikation verknüpft ist, z.B. eine MS Word-Datei. URLs wie 'http://www.yahoo.com' sind auch zulässig (diese startet Ihren Web-Browser und zeigt die Yahoo-Webseite).

Systemübersicht

Dieser Dialog zeigt detaillierte Informationen über Ihren Computer, z.B. CPU-Fähigkeiten, installierte Software, Speicherauslastung, usw. Zur Speicherung eines Berichtes ins XML-Format, klicken Sie auf den Button **[Bericht]**. Beachten Sie, dass nicht alle der technischen Ausdrücke im Fenster **Systemübersicht**, aus dem Englischen übersetzt werden können ohne ihre Bedeutung zu verlieren, deshalb zeigt dieses Fenster die Informationen nur in Englisch an, auch wenn Sie eine andere Sprache für die Bedienoberfläche benutzen.

Referenz

NetBIOS-Verzeichnis

Nachfolgend finden Sie die NetBIOS-Namensaufstellung eines Computers unter Windows.

Name	Hex-Suffix	Typ	Beschreibung
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<..._MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCP/IP Service
<computername>	52	U	DEC Pathworks TCP/IP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	Internet Information Server
<IS~computername>	00	U	Internet Information Server

Häufig gestellte Fragen (FAQ)

In diesem Kapitel finden Sie die Antworten auf einige der am häufigsten gestellten Fragen (FAQ). Die aktuellste FAQ steht immer unter http://www.tamos.com/products/nettools/faq.php zur Verfügung.

F. Meine Firewall warnt mich, dass Essential NetTools versucht sich mit dem Internet zu verbinden. Mir ist bewusst, dass einige Seiten in der Lage sind, Anwenderdaten durch Ihre Programme über das Internet aufzuspüren. Warum versucht Essential NetTools auf das Internet zuzugreifen?
A. Die Warnmeldung Ihrer Firewall zeigt nur an, dass Essential NetTools versucht IP-Adressen in Hostnamen aufzulösen, was zur Anzeige der Hostnamen im Tool NetStat erforderlich ist. Seit Essential NetTools zur Durchführung von DNS-Abfragen Ihren DNS-Server ansprechen muss, kommt es zwangsläufig zur Erzeugung dieser Warnung. Sie können diese Funktion abschalten (**Einstellungen => Optionen => DNS-Auflösung abschalten**), in diesem Fall ist die Auflistung NetStat nicht mehr in der Lage, Ihnen die Hostnamen anzuzeigen.

F. Ich versuche mit NBScan meine eigene IP-Adresse zu überprüfen., aber ich kann meine Computernamensliste nicht sehen.
A. Dies meint höchstwahrscheinlich, dass Ihr Computer entweder keine Ressourcenfreigabe anbietet oder er benutzt die Winsock-Version 1, die mit Windows 95 mitgeliefert wurde. In letzterem Fall, erwägen Sie stattdessen nbstat -A xxx.xxx.xxx.xxx zu benutzen oder ein Upgrade auf Winsock-Version 2 durchzuführen. Diese Begrenzung übernimmt keine Anzeige der Namenslisten anderer Computer (Winsock 1 arbeitet gerade so gut wie Winsock 2), doch nicht so gut wie NetAudit (Sie können mit NetAudit Ihren eigenen Computer überprüfen).

F. I überprüfe die Adresse xxx.xxx.xxx.xxx mit NBScan und erhalte kein Ergebnis aber nbstat zeigt mir die Namensliste.
A. Das hat zwei mögliche Gründe. Entweder haben Sie eine zu kurze Zeitüberschreitung eingestellt und die Antwort auf die Frage erreicht Ihren Computer nicht oder Sie benutzen nicht den Erweiterten Modus. Das Programm listet im Erweiterten Modus 100% der Computer, die auch nbstat auflisten kann. Lesen Sie bitte den Absatz über den Erweiterten Modus im Kapitel NBScan.

F. Ich überprüfe die Adresse xxx.xxx.xxx.xxx mit NBScan und nbstat, und ich erhalte kein Ergebnis. Die Person, zu deren Computer diese Adresse zugeordnet ist, überprüft dieselbe Adresse (seine eigene) und erhält die Namensliste seines Computers. Warum kann er diese sehen und ich nicht?
A. Da ist eine Firewall oder einige andere paketfilternde Geräte zwischen seinem und Ihrem Computer. Bestimmte Pakete können durch die Firewall-Einstellungen abgewiesen werden. Ebenso filtern einige der Internet-Service-Provider Pakete, ohne ihre Kunden zu informieren. Falls dies der Fall ist, sollten Sie das Netzwerk von einem andern Zugang aus überprüfen.

F. Wenn ich versuche mich mit einer freigegebenen Ressource zu verbinden, empfange ich die Fehlermeldung: 'Das Netzwerk ist nicht vorhanden oder nicht gestartet', aber ich bin damit verbunden!
A. Sie benutzen wahrscheinlich ein Einwahl-Netzwerk via Modem und vergaßen die Checkbox 'Ins Netzwerk einloggen' in den Verbindungseigenschaften zu aktivieren.

F. Wenn ich versuche mich mit einer freigegebenen Ressource zu verbinden, empfange ich die Fehlermeldung: 'Freigegebene Ressource nicht vorhanden', aber ich bin mir sicher, dass ich den korrekten Pfad zu der entfernten Freigabe eingegeben habe.
A. Stellen Sie sicher, dass Ihr Computername in der LMHost-Datei vorhanden ist und dass es ein einzigartiger Name ist. Es sollten keine 2 oder mehr Computer mit gleichem Namen in der LMHost-Datei stehen. Sie können überprüfen, ob Ihr Computer imstande ist den Namen zu verstehen; geben Sie dazu `ping computername` an der DOS-Eingabeaufforderung ein. Wenn sich der Computer erfolgreich anpingen lässt, benutzen Sie Essential NetTools um sich mit ihm zu verbinden.

F. Wenn ich den Befehl Computer öffnen auswähle oder versuche mich mit einer freigegebenen Ressource zu verbinden, blendet das Programm eine Sanduhr ein und es passiert eine Zeit lang nichts.
A. Haben Sie etwas Geduld :-) Gewöhnlich dauert es einige Sekunden, eine Verbindung herzustellen.

Information

Wie kann man CommView for WiFi kaufen

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 for WiFi verfügbar: die Standardlizenz nd die VoIP-Lizenz. Die teuere VoIP-Lizenz erlaubt alle Applikationsfunktionen, inklusive des VoIP-Analysers, wogegen die Standardlizenz den VoIP-Analyser nicht freigibt.

Überprüfen Sie unsere Webseite für die Einzel-Anwender- und Mehrfachanwenderlizenpreise. Eine lizensierte 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 Endanwenderlizenzabkommen, 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.tamos.com/order/

Nehmen Sie Kontakt mit uns auf

Web

http://www.tamos.com

E-Mail

sales@tamos.com (Gewerbliche Anfragen)
support@tamos.com (Alle anderen Fragen)

Mail und Fax

Postadresse:

PO Box 1385
Christchurch 8140
Neuseeland

Fax: +64 3 310 2413 (Neuseeland)

Fax: +1 917 591-6567 (USA)

Andere TamoSoft-Produkte

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. Ein Vollzugriff auf Rohdaten in Echtzeit ist auch möglich. CommView ist ein nützliches Werkzeug für LAN-Administratoren, Security-Experten, Netzwerker und für jeden der sich gerne ein Bild des Verkehrs auf einem PC oder in einem LAN-Segment machen will.

Mehr Information

CommTraffic

CommTraffic ist ein Netzwerk-Werkzeug zum Sammeln, Verarbeiten und zur Darstellung von Verkehr und Netzwerklaststatistiken in Netzwerkverbindungen, einschließlich LAN- und Wählverbindungen. Es zeigt den Verkehr und die Netzwerkauslastung für jeden Computer im Segment. Die Software bietet eine angenehme und anpassbare Oberfläche mit einem optionalen Tray-Icon-Menü, das allgemeine Netzwerkstatistiken darstellt. Sie können mit dem Programm Berichte über den Netzwerkverkehr und die Internetverbindungskosten (sofern vorhanden) erstellen. CommTraffic unterstützt alle möglichen Kostenpläne Ihres ISP, wie z. B. solche auf der Basis von Verbindungszeiten, Datenvolumen, Tageszeit und andere Einheiten. Sie können Alarme definieren, die Sie bei bestimmten Situationen informieren (z. B. bei einer bestimmten Last oder bei bestimmten Kosten). Ein Konfigurationsassistent leitet Sie durch das Setup und entdeckt automatisch Ihr Netzwerk oder Ihre Verbindungseinstellungen.

Mehr Information

SmartWhois

SmartWhois ist ein praktisches Werkzeug um Informationen über eine beliebige IP-Adresse, einen Hostnamen oder eine Domäne irgendwo auf der Welt zu bekommen. Es liefert automatisch Informationen zur IP-Adresse oder Domäne, unabhängig davon wo diese geografisch registriert wurden. In wenigen Sekunden erhalten Sie alle Informationen, die Sie über einen Nutzer wissen wollten: Domäne, Netzwerkname, Land, Staat/Bundesland und Stadt. Selbst wenn die IP-Adresse nicht in einen Hostnamen umgewandelt werden kann wird Sie SmartWhois nicht enttäuschen!

Mehr Information

CountryWhois

CountryWhois ist ein Hilfsmittel zur Identifizierung des geographischen Standortes einer IP-Adresse. CountryWhois kann zur Analyse von Server-Log-Dateien, zur Überprüfung von E-Mali-Nachrichtenköpfen, zur Idenfizierung von Online-Kreditkartenbetrügern oder für jede andere Gelegenheit benutzt werden, wo Sie schnell und exakt das Land der Ursprungs-IP-Adresse bestimmen müssen.

Mehr Information

Essential NetTools

Essential NetTools ist ein Satz von Netzwerkwerkzeugen, die sehr nützlich zur Netzwerkdiagnose und Netzwerkverbindungsüberwachung Ihres Computers sind. Das Programm ist ein Schweizer Taschenmesser für jeden, der machtvolle Werkzeuge für den Alltagseinsatz sucht. Das Programm enthält ein NetStat-Werkzeug, welches die Netzwerkverbindungen Ihres Computers anzeigt, ferner dessen offene Ports und deren Zuordnung zu den entsprechenden Anwendungen. Ferner enthält es einen schnellen NetBIOS-Scanner, ein NetBIOS-Auditing-Werkzeug zur Überprüfung der LAN-Sicherheit und einen Monitor für die externen Verbindungen zu den geteilten Ressourcen Ihres Computers. Es ist ebenso ein Prozessmonitor zur Anzeige der Informationen über die laufenden Programme und Services vorhanden. Weitere nützliche Werkzeuge sind z. B. Ping, TraceRoute, und NSLookup. Weitere Möglichkeiten sind die Berichterzeugung im HTML-, Text- und CSV-Format und die konfigurierbare Schnittstelle. Das Programm ist ein leicht zu benutzender und mächtiger Ersatz für Windows-Werkzeuge, wie nbtstat, netstat und NetWatcher. Die Applikation besitzt viele Profimöglichkeiten, die ein normales Windows nicht bietet.

Mehr Information

DigiSecret

DigiSecret ist eine leichtzubenutzende, sichere und mächtige Applikation zur Dateiverschlüsselung und zum gemeinsamen Dateizugriff. Es nutzt starke, etablierte Verschlüsselungsalgorithmen zur Erzeugung verschlüsselter Archive, selbstextrahierender Exe-Dateien zum Dateien-Sharing mit Kollegen und Freunden. DigiSecret beinhaltet ferner eine starke und intelligente Dateikompression. Sie benötigen nun keine ZIP-Dateien mehr, wenn Sie verschlüsselte und komprimierte DigiSecret-Dateien benutzen. Das Programm ist in die Windows- Shell integriert, so dass Sie Aktionen mittels Rechtsklick auf Dateien ausführen können. Zudem wird Drag&Drop voll unterstützt.

Mehr Information