TAKE CONTROL
IT'S YOUR SECURITY

TAMOSOFT

Essential NetTools

Help Documentation
Version 4.4

Contents

Introduction

About Essential NetTools

Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer's network connections. It is a Swiss Army knife for everyone interested in a set of powerful network tools for everyday use. It includes:

- **NetStat:** displays a list of your computer's inbound and outbound network connections, including the information on open TCP and UDP ports, IP address, and connection states. What makes it different from other NetStat utilities is the ability to map open ports to the owning application. Configurable alerts for incoming and outgoing connections are also available.
- **ProcMon:** displays the list of running processes with full information on the program location, manufacturer, process ID, and the loaded modules. With this tool, you can view CPU utilization statistics, identify hidden applications, kill running processes, and manage the usage of your PC's resources more effectively.
- **TraceRoute** and **Ping:** these familiar utilities featuring customizable options and convenient results presentation allow you to explore the Internet and troubleshoot connectivity problems.
- **PortScan**: an advanced TCP port scanner that allows you to scan your network for active ports. This tool features both conventional (full connect) and stealth (half-open) scanning modes.
- **HostAlive**: a network monitoring tool that periodically checks if a host is alive and running network services, such as an HTTP or FTP server.
- **EmailVerify**: checks if an e-mail address is valid by communicating with the corresponding mail server over SMTP.
- **NSLookup:** allows you to convert IP addresses to hostnames and vice versa, obtain aliases, and perform advanced DNS queries, such as MX or CNAME.
- **IPBlackList**: checks if an IP addresses is included in various IP address black lists: SPAM databases, open proxies and mail relays, etc. This tool helps you figure out why a given IP address is rejected by some network resources, such as mail servers.
- **NBScan:** a powerful and fast NetBIOS scanner. NBScan can scan a network within a given range of IP addresses and list computers offering NetBIOS resource-sharing service, as well as their name tables and MAC addresses. Unlike the standard nbtstat utility supplied with Windows, this tool provides a graphical user interface and easy management of the lmhosts file and features parallel scanning, which allows checking a class C network in less than one minute. NBScan can facilitate routine tasks often carried out by system integrators, administrators, and analysts.
- **RawSocket:** provides you with the ability to establish low-level TCP and UDP connections to troubleshoot and test different networking services. Multi-color output and a convenient interface make it a great tool for every network administrator or computer programmer.

- **WiFiMan** is a tool that shows wireless adapters installed on a computer, lists available wireless networks and allows you to manage connection profiles.

- **Shares**: monitors and logs external connections to your computer's shared resources, lists local shares, as well as provides a quick and easy way to connect to remote resources.

- **NetAudit** (NetBIOS Auditing Tool): allows you to perform various security checks on your network and/or individual computers offering the NetBIOS file sharing service. This tool can help you identify potential security flaws.

- **SNMPAudit:** Advanced SNMP device scanner. It allows you to locate SNMP devices in the selected network segment quickly and receive customizable data sampling from each of the devices. You can use SNMP browser for examining a device in detail.

- **SysFiles:** a convenient editor for the five important system files: services, protocol, networks, hosts, and lmhosts.

Other features include report generation in HTML, text, and comma delimited formats; quick IP address sharing between different tools; IP address geolocation; a comprehensive System Summary window, and a customizable interface.

What's New

Version 4.4

- Essential NetTools is now freeware.

Version 4.3

- WiFiMan: A new tool for working with wireless networks. Scan for available networks, manage profiles, monitor signal level, etc.
- Support for Windows 7.
- Improved NetStat and ProcMon report generation.
- Updated IP allocation map.
- A few other improvements.

Version 4.2

- New network tools have been added: HostAlive for service availability monitoring; EmailVerify for checking if an e-mail address is valid by communicating with the corresponding mail server; IPBlackList for checking if an IP address is included in various IP address black lists.
- All the tools now include real-time geolocation, i.e. all IP addresses are mapped to their country, and the country name and flag is displayed next to every IP address.
- A few bugs have been fixed.

Version 4.1

- Windows Vista support.

Version 4.0

- SNMPAudit – a new tool for exploring SNMP-enabled devices. A SNMP browser has been added for detailed examining of
- SNMP-enabled device states.
- Fully revised NetAudit tool. Increased overall performance and improved compatibility with modern network standards.
- User interface is changed for increased usability and simplicity of use.
- Expanded and improved NetStat. New customizable alert system for incoming and outgoing connections added, as well as icons representing processes in the current connections list. Various types of connections are colored, including the closed ones.
- Now the ProcMon module displays the CPU time allocation statistics per process.
- Automatic updates system allows you to quickly check for program updates at the TamoSoft Web site.
- User interface improvements that include customizable side bar buttons, ability to launch the standard Windows System
- Info utility, and other improvements.
- RawSocket now allows you to send arbitrary data including non-printing characters, such as 0x00.
- TraceRoute makes DNS-resolving in the background that significantly improves the module performance.

- A few bugs of the previous version are fixed.

Version 3.2

- A new System Summary window provides you with very detailed information on your computer.
- Improved logging that allows you to log only new connections or those processed in NetStat and ProcMon.
- Ping is now capable of pinging a range of IP addresses.
- New Quick Launch and Windows Tools menu items can be used to launch your favorite applications and access many commonly used Windows tools from one place.
- Raw UDP connections are now supported in addition to TCP.
- New connections are highlighted in NetStat.
- Local shared resources are now listed in Shares.
- SysFiles – a new tool that allows you to easily edit five important system files: services, protocol, networks, hosts, and lmhosts.
- Multilingual interface.

Version 3.1

- PortScan – a new tool for TCP port scanning.
- User-defined filters in NetStat.
- You can terminate TCP connections established by other applications.
- The program can automatically generate NetStat and ProcMon logs.
- A few other improvements.

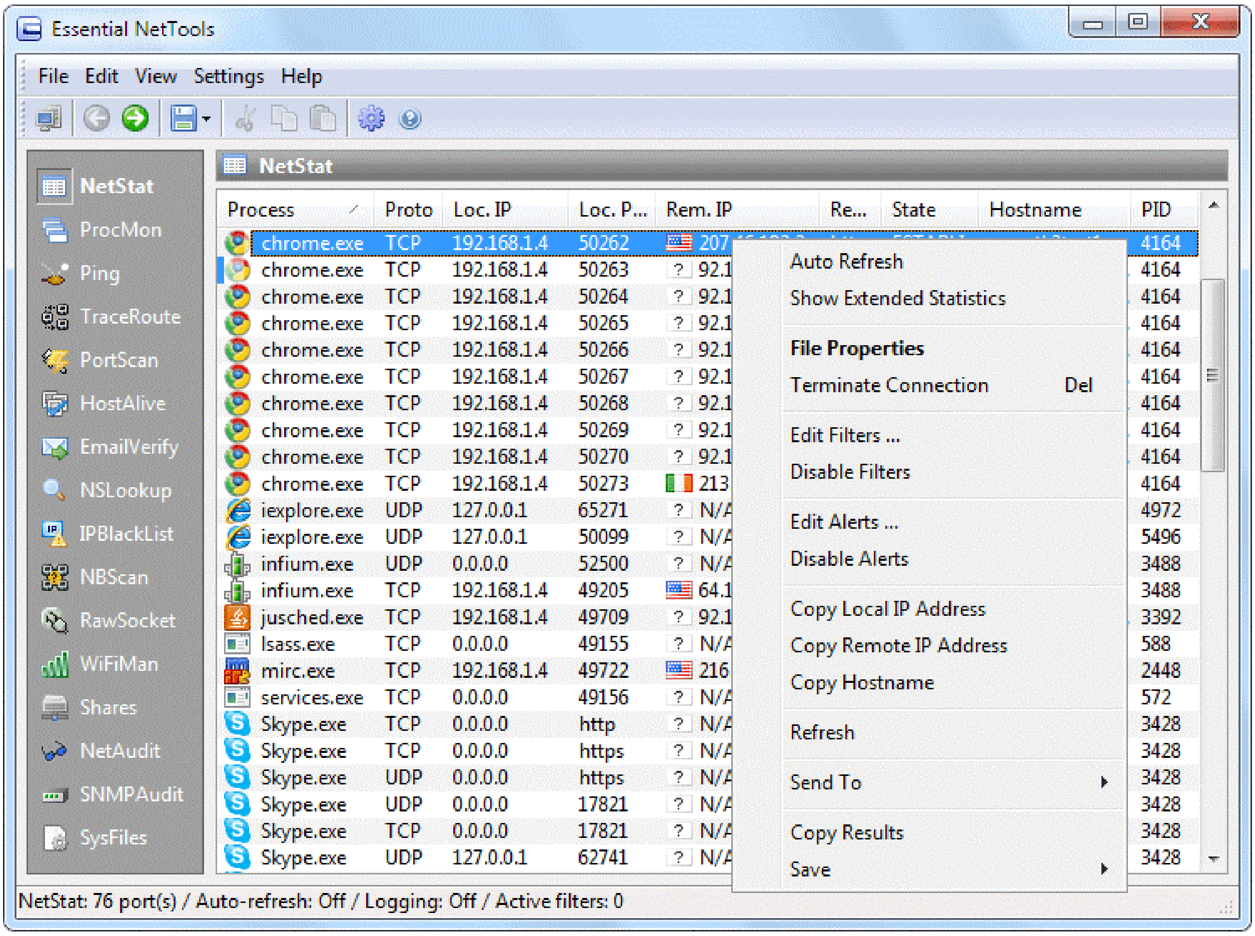
Version 3.0

- A new, improved interface.
- Ready for Windows XP.
- NetStat now maps open ports and connections to the owning application (Windows NT/2000/XP only).
- New tools: TraceRoute, Ping, NSLookup, and Process Monitor.

Using the Program

Interface Overview

The program's main window consists of a resizable side bar on the left, where you can select the tool to work with, and the main pane that displays the currently selected tool. The status bar at the bottom of the window displays the current status of the selected tool (e.g. Working or Idle). For detailed information on each tool, please refer to the corresponding chapters of this manual.



Process	Proto	Loc. IP	Loc. P...	Rem. IP	Re...	State	Hostname	PID
chrome.exe	TCP	192.168.1.4	50262	207				4164
chrome.exe	TCP	192.168.1.4	50263	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50264	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50265	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50266	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50267	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50268	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50269	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50270	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50273	213				4164
iexplore.exe	UDP	127.0.0.1	65271	? N/A				4972
iexplore.exe	UDP	127.0.0.1	50099	? N/A				5496
infium.exe	UDP	0.0.0.0	52500	? N/A				3488
infium.exe	TCP	192.168.1.4	49205	64.1				3488
jusched.exe	TCP	192.168.1.4	49709	? 92.1				3392
lsass.exe	TCP	0.0.0.0	49155	? N/A				588
mirc.exe	TCP	192.168.1.4	49722	216				2448
services.exe	TCP	0.0.0.0	49156	? N/A				572
Skype.exe	TCP	0.0.0.0	http	? N/A				3428
Skype.exe	TCP	0.0.0.0	https	? N/A				3428
Skype.exe	UDP	0.0.0.0	https	? N/A				3428
Skype.exe	UDP	0.0.0.0	17821	? N/A				3428
Skype.exe	TCP	0.0.0.0	17821	? N/A				3428
Skype.exe	UDP	127.0.0.1	62741	? N/A				3428

NetStat: 76 port(s) / Auto-refresh: Off / Logging: Off / Active filters: 0

Main Menu

File

- **System Summary** – shows a dialog with detailed information on your computer.
- **Windows Tools** – allows you to quickly access many commonly used Windows tools and utilities.
- **Quick Launch** – launches other network-related tools by TamoSoft, if they are installed on your system, as well as allows you to configure the program to launch your favorite applications.
- **Run** – opens the standard Windows "Run" dialog.
- **Save Report** – saves the output of the current tool to a file.
- **Logging** – opens the Logging dialog.
- **Exit** – closes the program.

Edit

- **Cut, Copy, Paste** – performs the standard text commands.

View

- **Tool Bar –** shows/hides the tool bar.
- **Status Bar –** shows/hides the status bar. **Side Bar –** shows/hides the side bar.
- **Customize Side Bar** – allows you to customize side bar buttons.
- **Local IP Address(es)** – displays your computer's IP addresses.
- **Previous Tool, Next Tool** – allows you switch to the next/previous tool.
- **NetStat, NBScan, etc.** – allows you to select the tool to work with.

Settings

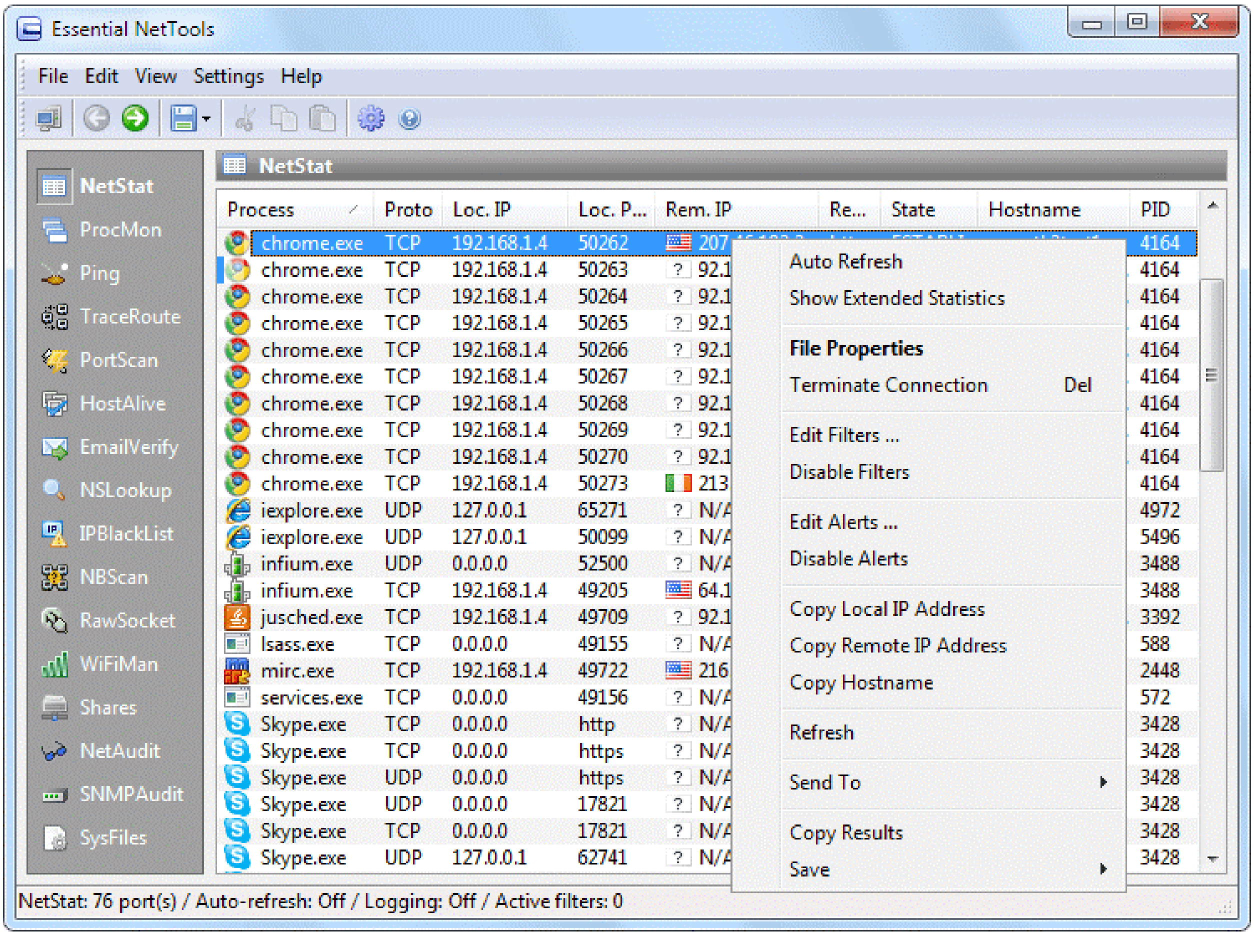
- **Fonts** – allows you to select the interface font and fixed-width font (the fixed-width font is used in some of the program's windows, such as NetAudit or NSLookup).
- **Options** – displays the Options dialog.
- **Language** – use this command to select the interface language.

Help

- **Contents** – opens the help file.
- **Search For Help On** – opens the Essential NetTools help index.
- **Check For An Update On The Web** – opens the update downloading dialog window. Please follow the instructions on the screen to download and install the latest upgrade for Essential NetTools from the TamoSoft web site.
- **About** – shows the About window.

NetStat

This tool is a replacement of the standard Windows netstat command-line utility. It displays all the inbound and outbound connections to your computer and lists all open ports. Additionally, NetStat maps open ports and established connections to the owning application.



Process	Proto	Loc. IP	Loc. P...	Rem. IP	Re...	State	Hostname	PID
chrome.exe	TCP	192.168.1.4	50262	207				4164
chrome.exe	TCP	192.168.1.4	50263	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50264	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50265	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50266	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50267	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50268	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50269	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50270	? 92.1				4164
chrome.exe	TCP	192.168.1.4	50273	213				4164
iexplore.exe	UDP	127.0.0.1	65271	? N/A				4972
iexplore.exe	UDP	127.0.0.1	50099	? N/A				5496
infium.exe	UDP	0.0.0.0	52500	? N/A				3488
infium.exe	TCP	192.168.1.4	49205	64.1				3488
jusched.exe	TCP	192.168.1.4	49709	? 92.1				3392
lsass.exe	TCP	0.0.0.0	49155	? N/A				588
mirc.exe	TCP	192.168.1.4	49722	216				2448
services.exe	TCP	0.0.0.0	49156	? N/A				572
Skype.exe	TCP	0.0.0.0	http	? N/A				3428
Skype.exe	TCP	0.0.0.0	https	? N/A				3428
Skype.exe	UDP	0.0.0.0	https	? N/A				3428
Skype.exe	UDP	0.0.0.0	17821	? N/A				3428
Skype.exe	TCP	0.0.0.0	17821	? N/A				3428
Skype.exe	UDP	127.0.0.1	62741	? N/A				3428

NetStat: 76 port(s) / Auto-refresh: Off / Logging: Off / Active filters: 0

Right-clicking on the window brings up a menu with the following commands:

Auto Refresh – switches on/off automatic refreshing of the list. The refresh interval is configurable (see Options).

Show Extended Statistics – displays an additional pane showing extended per-protocol statistics. **File Properties** – displays the file properties dialog for the process that owns the connection. **Terminate Connection** – closes the selected TCP connection.

Edit Filters – opens the Filters dialog.

Disable Filters – enables/disables all currently configured filters.

Edit Alerts – opens the Alerts dialog.

Disable Filters – enables/disables all currently configured Alerts.

Copy Local IP Address – copies the local IP address to the clipboard.

Copy Remote IP Address – copies the remote IP address to the clipboard.

Copy Hostname – copies the remote hostname to the clipboard.

Refresh – refreshes the list.

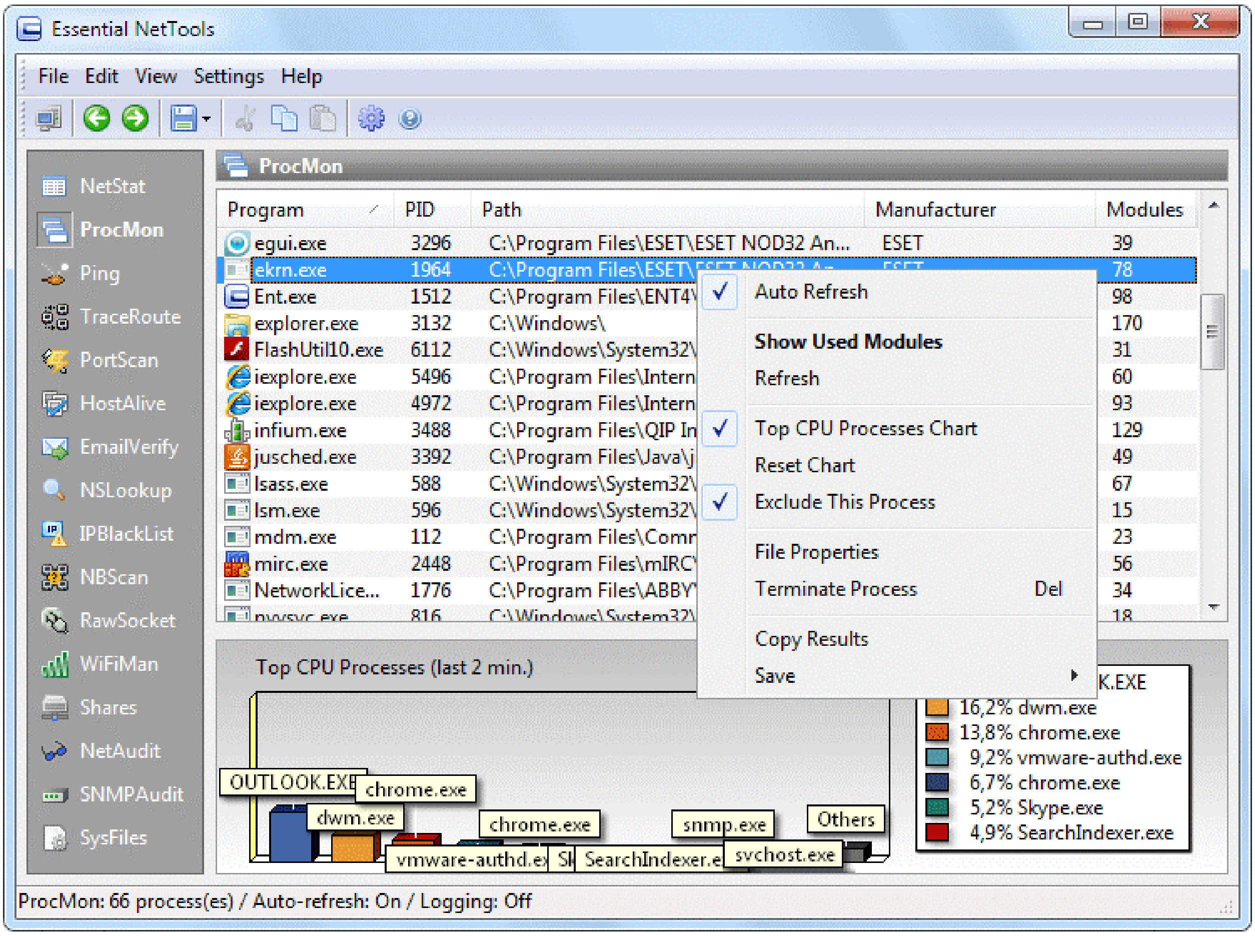
Send To – sends the selected IP address to other tools or to SmartWhois.

Copy Results – copies the NetStat table to the clipboard.
Save – saves the NetStat table to a file.

The program can be configured to not display all the connections, convert port numbers to service names, resolve IP addresses to hostnames, etc. New and closed connections are automatically highlighted for five seconds. See Options for more information.

ProcMon

ProcMon is a tool that displays the list of the processes (applications and services) currently running on your computer. The Program column shows the program name, the **PID** column shows the unique process ID, the **Path** column shows the full path to the program's executable file, the **Manufacturer** column shows the name of the file manufacturer, and the **Modules** column shows the number of modules used by the selected process. ProcMon is a handy tool for identifying hidden applications, killing running processes, and managing the usage of your PC's resources more effectively.



Program	PID	Path	Manufacturer	Modules
egui.exe	3296	C:\Program Files\ESET\ESET NOD32 An...	ESET	39
ekrn.exe	1964	C:\Program Files\ESET\		78
Ent.exe	1512	C:\Program Files\ENT4\		98
explorer.exe	3132	C:\Windows\		170
FlashUtil10.exe	6112	C:\Windows\System32\		31
iexplore.exe	5496	C:\Program Files\Intern		60
iexplore.exe	4972	C:\Program Files\Intern		93
infium.exe	3488	C:\Program Files\QIP In		129
jusched.exe	3392	C:\Program Files\Java\j		49
lsass.exe	588	C:\Windows\System32\		67
lsm.exe	596	C:\Windows\System32\		15
mdm.exe	112	C:\Program Files\Comn		23
mirc.exe	2448	C:\Program Files\mIRC\		56
NetworkLice...	1776	C:\Program Files\ABBY\		34
nvvsvc.exe	816	C:\Windows\System32\		18

ProcMon: 66 process(es) / Auto-refresh: On / Logging: Off

Right-clicking on the window brings up a menu with the following commands:

Auto Refresh – switches on/off automatic refreshing of the list. The refresh interval is configurable (see Options).

Show Used Modules – displays a dialog listing the modules (DLL files) used by the selected process.

Refresh – refreshes the list.

Top CPU Processes Chart – hides/shows the chart showing the top 10 CPU consuming processes.

Reset Chart – resets all the accumulated statistics and starts to collect the data over again.

Exclude This Process – excludes the currently selected process from the statistics.

File Properties – displays the file properties dialog for the selected process.

Terminate Process – terminates the selected process (use with caution).

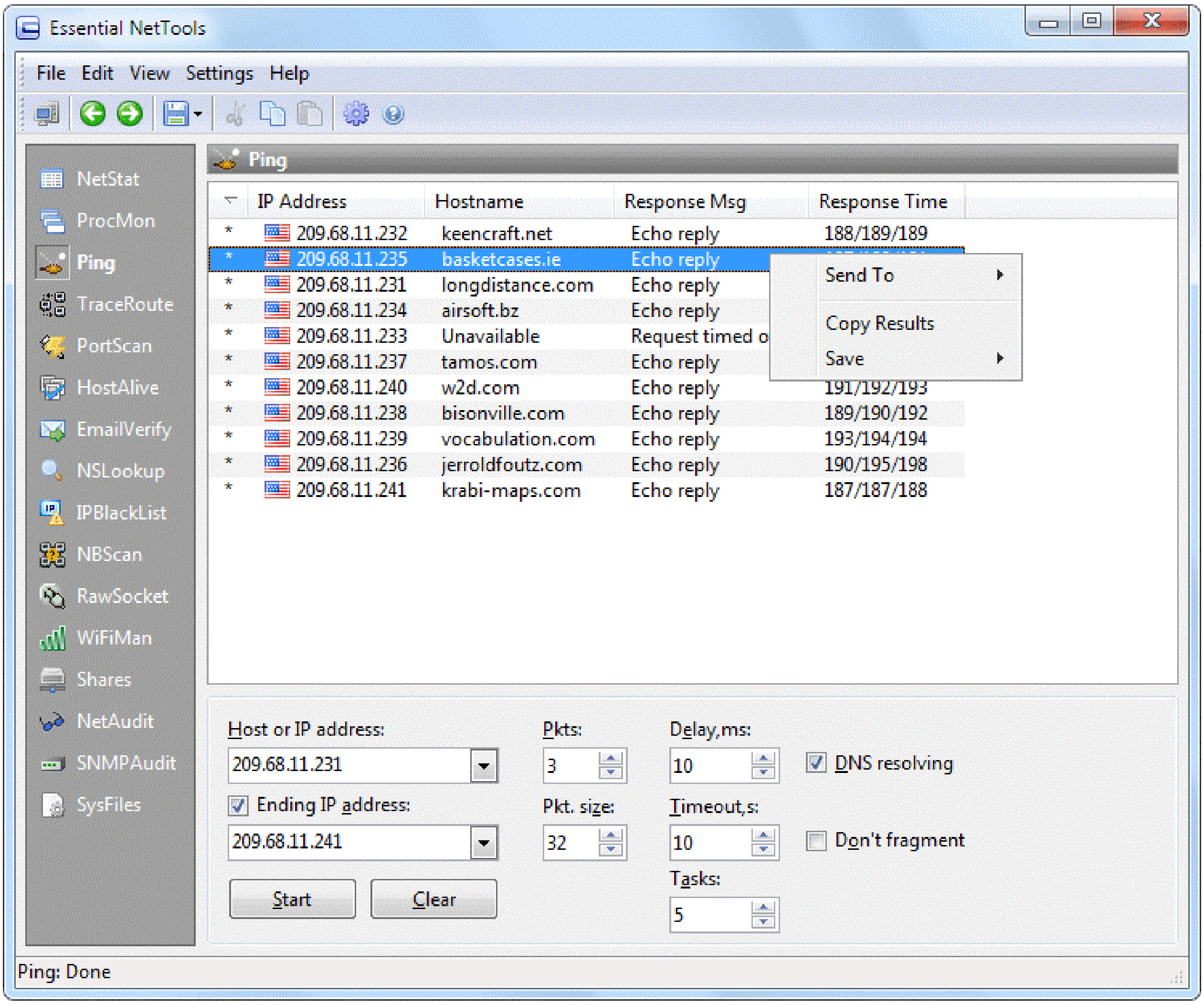
Copy Results – copies the ProcMon table to the clipboard.

Save – saves the ProcMon table to a file.

The CPU utilization diagram shows CPU resource allocation between the processes during the last several minutes. The top 10 CPU- consuming processes, including the completed ones are shown. The refresh interval for the CPU utilization chart is configurable (see Options).

Ping

Ping is a tool that lets you verify that a particular IP address exists and can accept requests by sending an Internet Control Message Protocol (ICMP) Echo request. Ping is used diagnostically to ensure that the host computer you are trying to reach is actually operating. If, for example, you cannot ping a host, then you will be unable to use File Transfer Protocol (FTP) to send files to that host. Ping can also be used with a host that is operating to see how long it takes to get a response back. If a host computer is operating, it normally sends back an Echo reply message.



	IP Address	Hostname	Response Msg	Response Time
*	209.68.11.232	keencraft.net	Echo reply	188/189/189
*	209.68.11.235	basketcases.ie	Echo reply	
*	209.68.11.231	longdistance.com	Echo reply	
*	209.68.11.234	airsoft.bz	Echo reply	
*	209.68.11.233	Unavailable	Request timed o	
*	209.68.11.237	tamos.com	Echo reply	
*	209.68.11.240	w2d.com	Echo reply	191/192/193
*	209.68.11.238	bisonville.com	Echo reply	189/190/192
*	209.68.11.239	vocabulation.com	Echo reply	193/194/194
*	209.68.11.236	jerroldfoutz.com	Echo reply	190/195/198
*	209.68.11.241	krabi-maps.com	Echo reply	187/187/188

Host or IP address: 209.68.11.231
☑ Ending IP address: 209.68.11.241
Pkts: 3
Pkt. size: 32
Delay,ms: 10
Timeout,s: 10
Tasks: 5
☑ DNS resolving
☐ Don't fragment

Ping: Done

This tool can work in two modes. If you uncheck the **Ending IP address** box, it will ping just one IP address, and each ping will be shown on a separate line. If you check the **Ending IP address** box, it will ping a range of IP addresses, and each address will be shown on a separate line. In the latter mode, the **Response Time** column will display minimum, average, and maximum times separated by slashes.

To use this tool, enter an IP address or hostname and click Start. The following options are available:

Pkts. – sets the number of packets to be sent to the remote host.
Delay– sets the interval (in milliseconds) between pings.
Pkt. size – sets the size (in bytes) of the data portion of the ICMP packet.
Timeout – sets the maximum time (in seconds) Ping will wait for the response from a host.

DNS resolving – check this box if you want TraceRoute to resolve IP addresses to hostnames.
Don't fragment – sets the Don't fragment flag in the packet.
Tasks – sets the number of simultaneous tasks when pinging a range of IP addresses. It is recommended to keep this number low if your PC does not have ample RAM, as a high number of parallel tasks might exhaust your system resources.

Right-clicking on the window brings up a menu with the following commands:

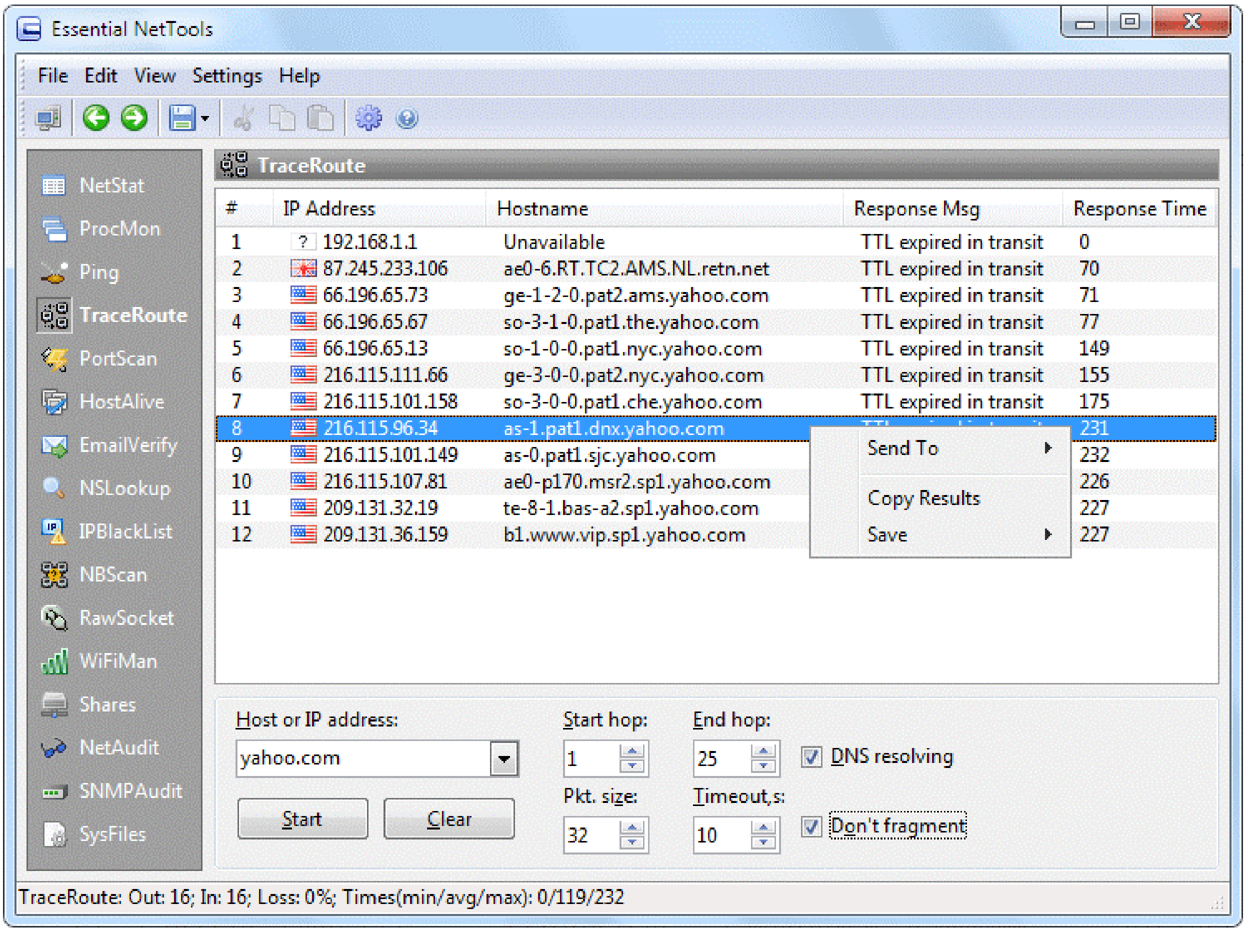
Send To – sends the selected IP address to other tools or to SmartWhois.
Copy Results – copies the Ping table to the clipboard.
Save – saves the Ping table to a file.

TraceRoute

TraceRoute is a tool that traces the route (the specific gateway computers at each hop) from a client machine to the remote host being contacted by reporting all the router IP addresses in between. It also calculates and displays the amount of time each hop took. TraceRoute is a handy tool for both understanding where problems exist in the Internet network and for getting a detailed sense of the Internet itself.

TraceRoute works by causing each router along a network path to return an Internet Control Message Protocol (ICMP) error message. An IP packet contains a Time-To-Live (TTL) value, which specifies how long it can go on its search for a destination before being discarded. Each time a packet passes through a router, its TTL value is decremented by one; when it reaches zero, the packet is dropped, and an ICMP TTL expired in transit error message is returned to the sender.

The TraceRoute program sends its first group of packets with a TTL value of one. The first router along the path will therefore discard the packet (its TTL is decremented to zero) and return the TTL expired in transit error. Thus, we have found the first router on the path. Packets can then be sent with a TTL of two, and then three, and so on, causing each router along the path to return an error, identifying it to us. Some routers silently drop packets with expired TTL; for such hops you will get the Request timed out error. Eventually, either the final destination is reached, or the maximum value is reached, and the TraceRoute ends. At the final destination, TraceRoute sends an ICMP Echo Request packet (ping), and if the destination computer is reachable, TraceRoute displays Echo reply in the Response Message column.



#	IP Address	Hostname	Response Msg	Response Time
1	192.168.1.1	Unavailable	TTL expired in transit	0
2	87.245.233.106	ae0-6.RT.TC2.AMS.NL.retn.net	TTL expired in transit	70
3	66.196.65.73	ge-1-2-0.pat2.ams.yahoo.com	TTL expired in transit	71
4	66.196.65.67	so-3-1-0.pat1.the.yahoo.com	TTL expired in transit	77
5	66.196.65.13	so-1-0-0.pat1.nyc.yahoo.com	TTL expired in transit	149
6	216.115.111.66	ge-3-0-0.pat2.nyc.yahoo.com	TTL expired in transit	155
7	216.115.101.158	so-3-0-0.pat1.che.yahoo.com	TTL expired in transit	175
8	216.115.96.34	as-1.pat1.dnx.yahoo.com	TTL expired in transit	231
9	216.115.101.149	as-0.pat1.sjc.yahoo.com		232
10	216.115.107.81	ae0-p170.msr2.sp1.yahoo.com		226
11	209.131.32.19	te-8-1.bas-a2.sp1.yahoo.com		227
12	209.131.36.159	b1.www.vip.sp1.yahoo.com		227

Host or IP address: yahoo.com

Start hop: 1

End hop: 25

Pkt. size: 32

Timeout,s: 10

☑ DNS resolving

☑ Don't fragment

TraceRoute: Out: 16; In: 16; Loss: 0%; Times(min/avg/max): 0/119/232

To use this tool, enter an IP address or hostname and click **Start**. The following options are available:

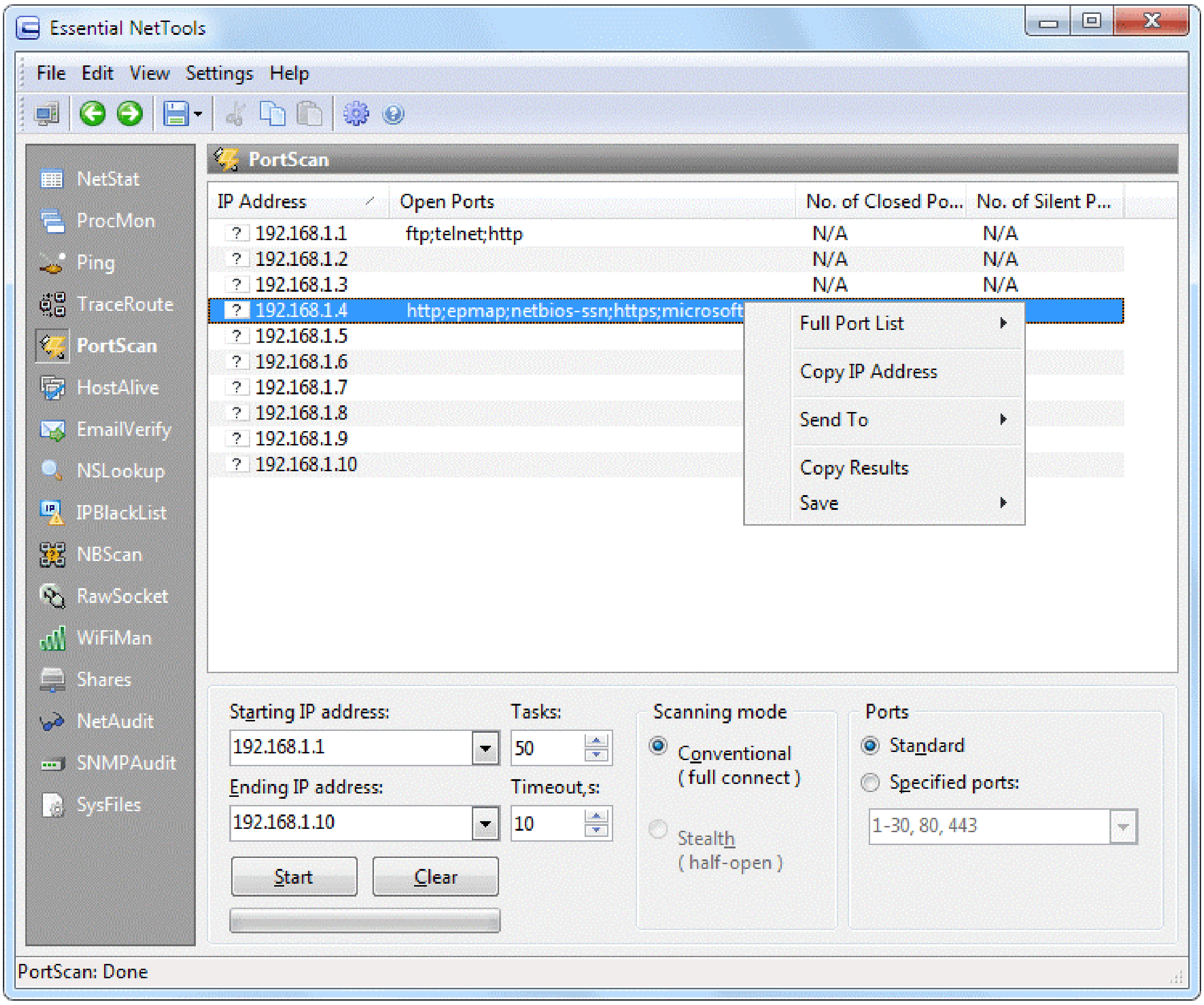
Start hop – allows you to set the hop from which to start tracing. It is often useful to set a value higher than 1 if the first several hops of the route are always the same; by setting a higher value you can save some time.
End hop – allows you to limit the number of hops to trace.
Pkt. size – sets the size (in bytes) of the data portion of the ICMP packet.
Timeout – sets the maximum time (in seconds) TraceRoute will wait for the response from a router.
DNS resolving – check this box if you want TraceRoute to resolve IP addresses to hostnames.
Don't fragment – sets the Don't fragment flag in the packet.

Right-clicking on the window brings up a menu with the following commands:

Send To – sends the selected IP address to other tools or to SmartWhois.
Copy Results – copies the TraceRoute table to the clipboard.
Save – saves the TraceRoute table to a file.

PortScan

PortScan is a TCP scanner, a tool that detects if certain TCP ports are open and can accept connections. TCP scanners are usually used for checking if the remote computer runs services (e.g. Telnet or FTP), as well as for security analysis. A port scan includes sending data to the user-defined list of ports and interpreting the response received to identify whether the ports are open.



IP Address	Open Ports	No. of Closed Po...	No. of Silent P...
? 192.168.1.1	ftp;telnet;http	N/A	N/A
? 192.168.1.2		N/A	N/A
? 192.168.1.3		N/A	N/A
? 192.168.1.4	http;epmap;netbios-ssn;https;microsoft		
? 192.168.1.5			
? 192.168.1.6			
? 192.168.1.7			
? 192.168.1.8			
? 192.168.1.9			
? 192.168.1.10			

Starting IP address: 192.168.1.1

Tasks: 50

Ending IP address: 192.168.1.10

Timeout,s: 10

Scanning mode

● Conventional (full connect)

○ Stealth (half-open)

Ports

● Standard

○ Specified ports: 1-30, 80, 443

PortScan: Done

Information for Windows XP SP2 and Vista Users

Windows XP Service Pack 2 and newer Windows versions limit the number of simultaneous incomplete outbound TCP connections to 10 per application. Upon reaching this limit, subsequent connection attempts are placed in a queue to be resolved at a fixed rate. This may significantly slow down an application that makes a large number of connection attempts. An example of such an application is Essential NetTools in port scanning mode (the PortScan tool).

Presently, no legitimate, official workarounds are available for this problem. There is, however, an unofficial patch that modifies the system files and removes this limitation. If you are running Windows XP Service Pack 2 and are dissatisfied with the PortScan speed or results quality (i.e. many open ports may remain undetected), you may try to install one of the unofficial patches available at http://www.lvllord.de/ . Warning: This patch can only be applied to Windows XP Service Pack 2. This patch is not supported by Microsoft.

Additionally, Windows XP Service Pack 2 and newer Windows versions removed support for raw sockets, making the Stealth scanning mode in the PortScan tool impossible. No unofficial patches are known at this time.

Before you start scanning, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above and specify the number of simultaneous connections and the connection timeout in the Tasks and Timeout spinboxes. Then you should select the scanning mode: **Conventional** or **Stealth**. In the conventional mode, a TCP connection is established between your computer and the computer you are scanning. In the stealth mode, the connection is initiated, but not finalized. This scanning technique is also known as half-open or SYN scanning: The program sends a SYN packet (as if we are going to open a connection) to the target host, and the target host responds with a SYN ACK (this indicates the port is listening) or RST ACK (this indicates the port is not listening) packet. Stealth scans cannot be logged by the target host on the TCP level, although they can be logged by the intrusions detection systems (IDS) working on the packet level. You may find this mode useful when testing the configuration and efficiency of your LAN's IDS. The stealth mode is available **only under Windows 2000/XP**, requires administrative privileges, and cannot be used to scan your own IP address (to scan your own IP address, use the conventional mode or just look at the NetStat tool to see the list of open ports). Also, please note that running firewall software (including the built-in Windows XP firewall) on **your** computer may affect the scanning results in the stealth mode; therefore, it is recommended to temporarily disable such software during the scanning process.

Finally, you should select the list of ports to be probed. The **Standard** list includes the following 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, and 8080. If you'd like to use a custom list, you can select the **Specified ports** option and enter your own list. The syntax for entering ports is simple: you can either enter individual ports or port ranges, and you must separate these entries with commas. Below you can find a few examples of valid port lists:

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

When all the options are set, click **Start** to start scanning. The scanning speed can be modified by selecting **Settings** => **Options** in the program menu (see Options for details).

During the scanning process, the information about the ports is being added to the list. The **Open Ports** column lists the TCP ports that accepted the connection. The **No. of Closed Ports** column displays the number of ports that rejected connections, while the **No. of Silent Ports** column displays the number of ports that ignored connections attempts. In the conventional mode, the last two columns do not display these numbers, because this mode can only detect open ports, but cannot distinguish between closed and silent ports. In other words, in the conventional mode, all the ports that are not open are considered closed. In the stealth mode, the ports that replied with an RST ACK packet are considered closed, while those ports that completely ignored our SYN packets are considered silent, which may indicate that they are protected by a firewall.

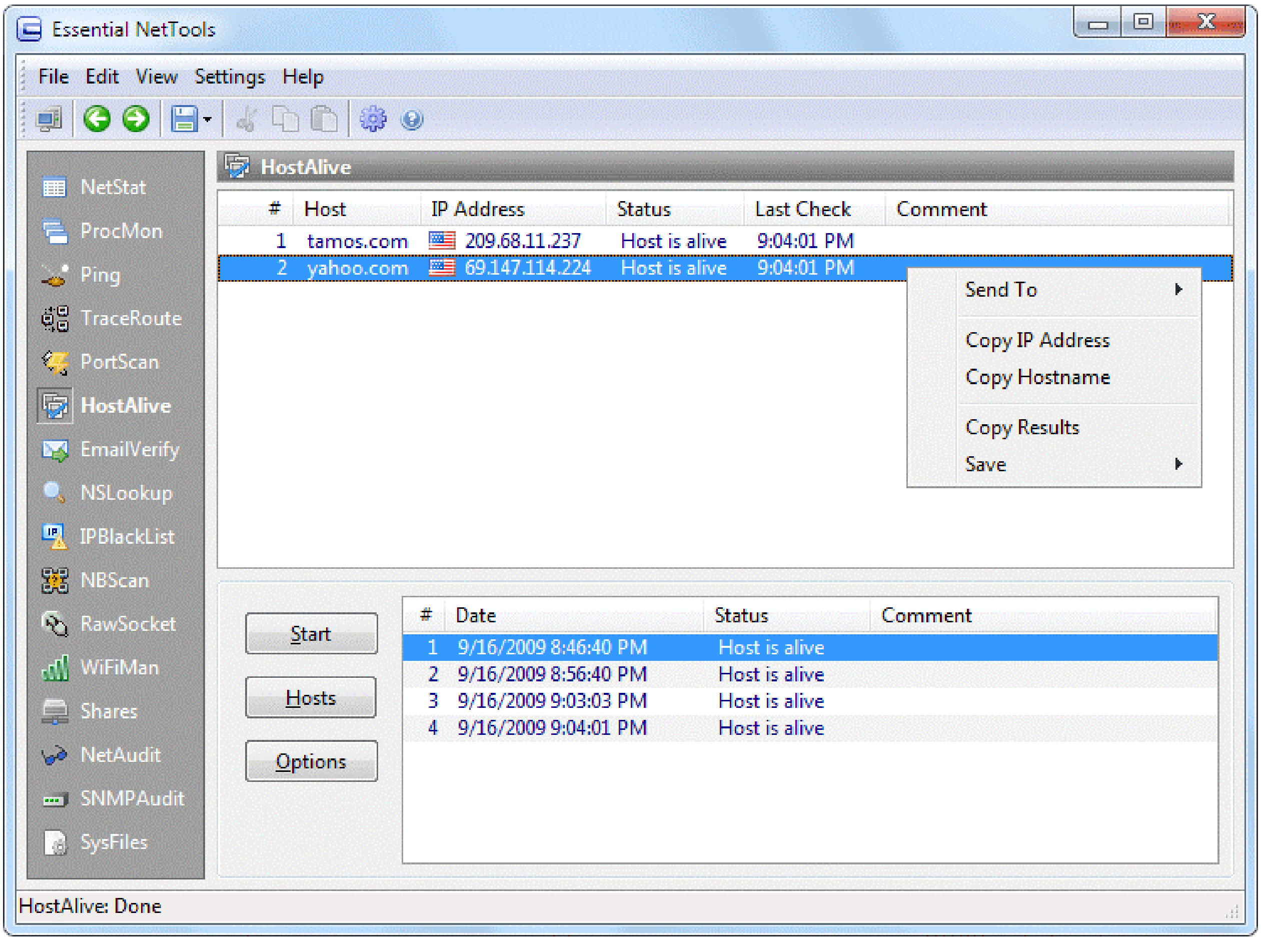
Right-clicking on a listed computer brings up a menu with the following commands:

Full port list – displays the complete list of open, closed, and silent ports. Since the ports lists are normally very long, this command is useful for displaying such long lists.
Copy IP Address – copies the selected computer's IP address to the clipboard.

Send To – sends the selected IP address to other tools or to SmartWhois.
Copy Results – copies the PortScan table to the clipboard.
Save – saves the PortScan table to a file.

HostAlive

HostAlive is a tool that periodically checks if a remote host or group of hosts is alive. HostAlive is based on a simple principle: It sends a network packet to the destination host and waits for a response. For example, it can check if the HTTP service on the remote host is up and running. The type of check and interval are configurable.

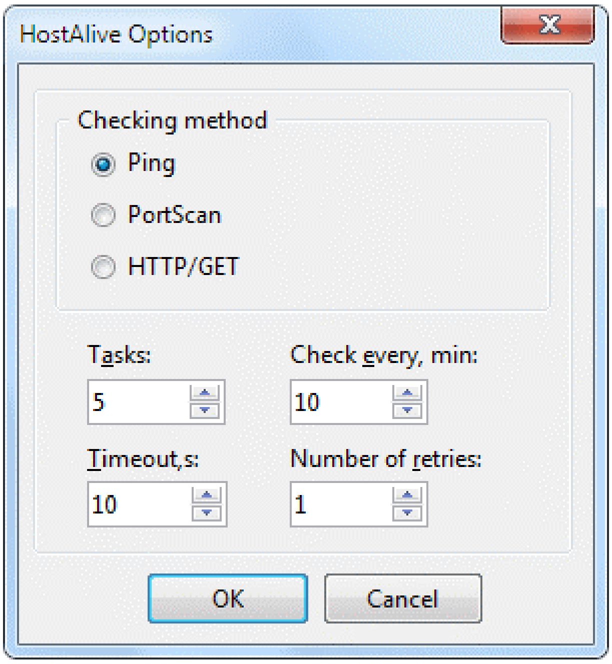


#	Host	IP Address	Status	Last Check	Comment
1	tamos.com	209.68.11.237	Host is alive	9:04:01 PM	
2	yahoo.com	69.147.114.224	Host is alive	9:04:01 PM	

#	Date	Status	Comment
1	9/16/2009 8:46:40 PM	Host is alive	
2	9/16/2009 8:56:40 PM	Host is alive	
3	9/16/2009 9:03:03 PM	Host is alive	
4	9/16/2009 9:04:01 PM	Host is alive	

HostAlive: Done

To create a list of hosts to be checked, click on the **Hosts** button. Enter the names or IP addresses of the hosts to be checked. To configure the type of check, click on the **Options** button and configure the desired type:


HostAlive Options

Checking method

● Ping

○ PortScan

○ HTTP/GET

Tasks: 5

Check every, min: 10

Timeout,s: 10

Number of retries: 1

Three checking methods are available:

- **Ping:** A standard check using ICMP ping packets. This is a generic check type that tells you that the host is connected to the network and the operating system is alive. It does not tell you if a specific network service, such as HTTP or POP3, is running. Note that hosts behind firewalls may not reply to ping packets.
- **PortScan:** A check based on the host's ability to accept a TCP connection. For example, you can check if the POP3 service is running by scanning TCP port 110.
- **HTTP/GET:** A check for Web servers that verifies that the remote host accepts connections on the standard HTTP port and replies with a correct HTTP response. The standard HTTP port is 80, but you can enter a custom value.

The following options are also available:

Tasks – configures the number of simultaneous jobs the tool can launch.
Check every, min – sets the interval in minutes between checks.
Timeout, s – configures how many seconds the tool should wait for a response from the host.
Number of retries – sets the number of attempts to be carried out.

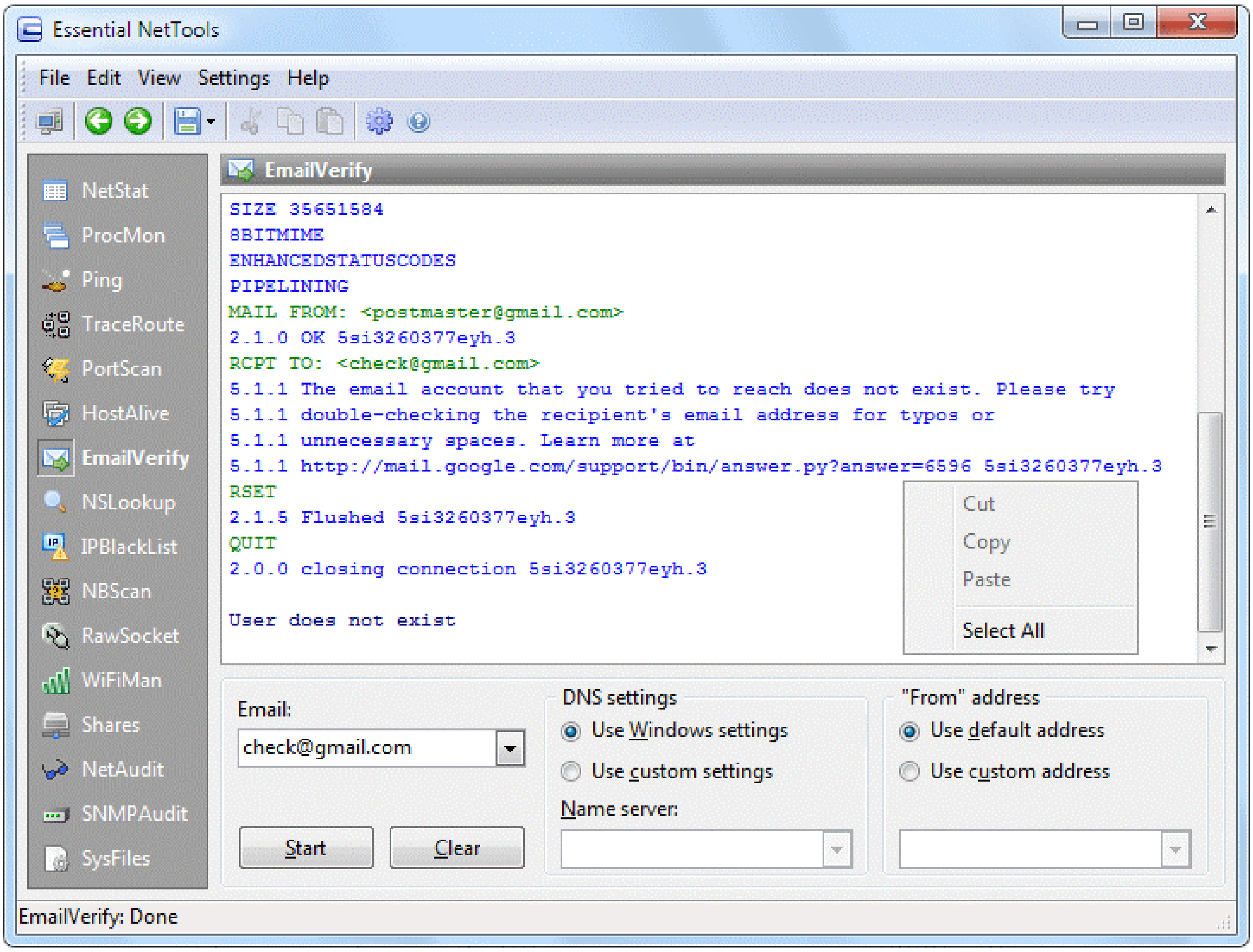
Once you have entered the list of the hosts to be checked and configured the options, click **Start** to initiate the process. The tool will keep on checking the hosts periodically until you click **Stop** or exit the applications.

Right-clicking on the window brings up a menu with the following commands:

Send To – sends the selected IP address to other tools or to SmartWhois.
Copy IP Address – copies the selected computer's IP address to the clipboard.
Copy Hostname – copies the selected hostname to the clipboard.
Copy Results – copies the HostAlive table to the clipboard.
Save – saves the HostAlive table to a file.

EmailVerify

EmailVerify is a tool that allows you to check if an e-mail address exists and accepts mail. This tool looks up MX records for the e- mail address (in other words, finds out what mail server handles e-mail for the given address) and then tries to connect to the mail server and deliver e-mail. No actual e-mail messages are being sent during the check.



```
SIZE 35651584
8BITMIME
ENHANCEDSTATUSCODES
PIPELINING
MAIL FROM: <postmaster@gmail.com>
2.1.0 OK 5si3260377eyh.3
RCPT TO: <check@gmail.com>
5.1.1 The email account that you tried to reach does not exist. Please try
5.1.1 double-checking the recipient's email address for typos or
5.1.1 unnecessary spaces. Learn more at
5.1.1 http://mail.google.com/support/bin/answer.py?answer=6596 5si3260377eyh.3
RSET
2.1.5 Flushed 5si3260377eyh.3
QUIT
2.0.0 closing connection 5si3260377eyh.3

User does not exist
```

Email: check@gmail.com

DNS settings
● Use Windows settings
○ Use custom settings
Name server:

"From" address
● Use default address
○ Use custom address

EmailVerify: Done

To check an e-mail address, enter it into the corresponding window and click **Start**. The log of the checking process will be displayed in the main window.

To find the mail server, EmailVerify must perform a few DNS queries. By default, the tool will use the DNS servers being used by Windows. In some non-standard cases, you may want to override these settings by checking the **Use custom settings** box and entering custom name server addresses.

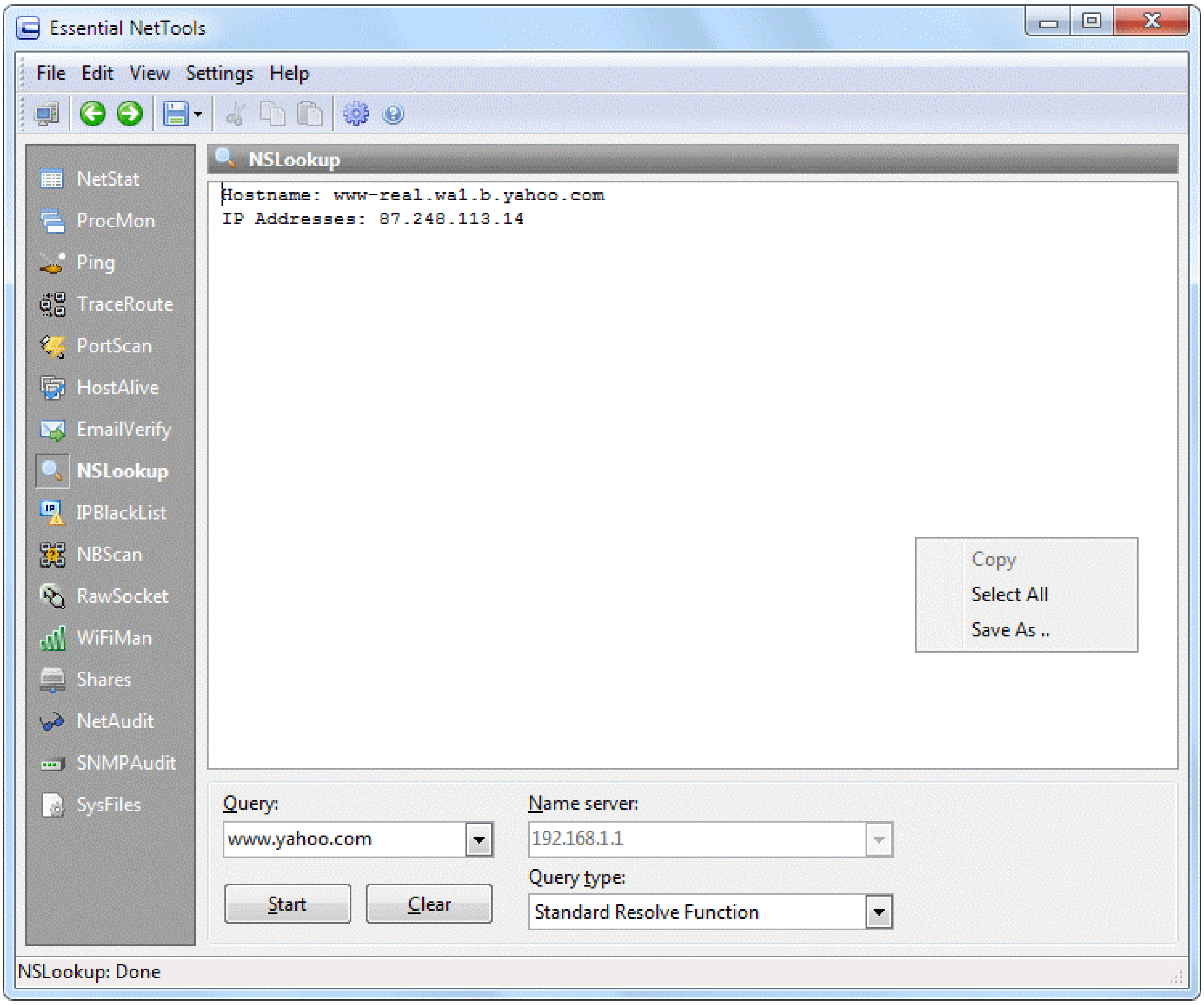
During the e-mail verification process, EmailVerify must provide the sender's address. By default, the tool uses the postmaster@domain address, where domain is the domain part of the e-mail address. For example, if you are checking user1@gmail.com, EmailVerify will use postmaster@gmail.com as the "From" address. You can change this by selecting the **Use custom address** option and specifying any other address.

It is important to remember that the results of this test may depend on the IP address you are connecting from, as well as the "From" address you are using. The mail server may reject mail from certain IP addresses or from all dynamic IP addresses. It may also reject mail from certain e-mail domains or specific accounts.

NSLookup

NSLookup is a tool that lets you enter a hostname (for example, "www.yahoo.com") and find out the corresponding IP address. It will also do reverse name lookup and find the hostname for an IP address you specify. Such conversion of hostnames to IP addresses and vice versa is the main NSLookup function; however, advanced users can also use it to perform specific queries, e.g. queries for Mail Exchange (MX) records. NSLookup works by sending a Domain Name System (DNS) query to your default DNS server (in case of the Standard Resolve Function), or to any DNS server you specify (in case of all other query types).

To perform the standard query, select **Standard Resolve Function** from the **Query type** list, enter an IP address or hostname in the **Query** field, and click **Start**. The program will display the query result in a few seconds. For standard queries, the program will always contact your default DNS server, so the **Name server** field is disabled.



```
Hostname: www-real.wa1.b.yahoo.com
IP Addresses: 87.248.113.14
```

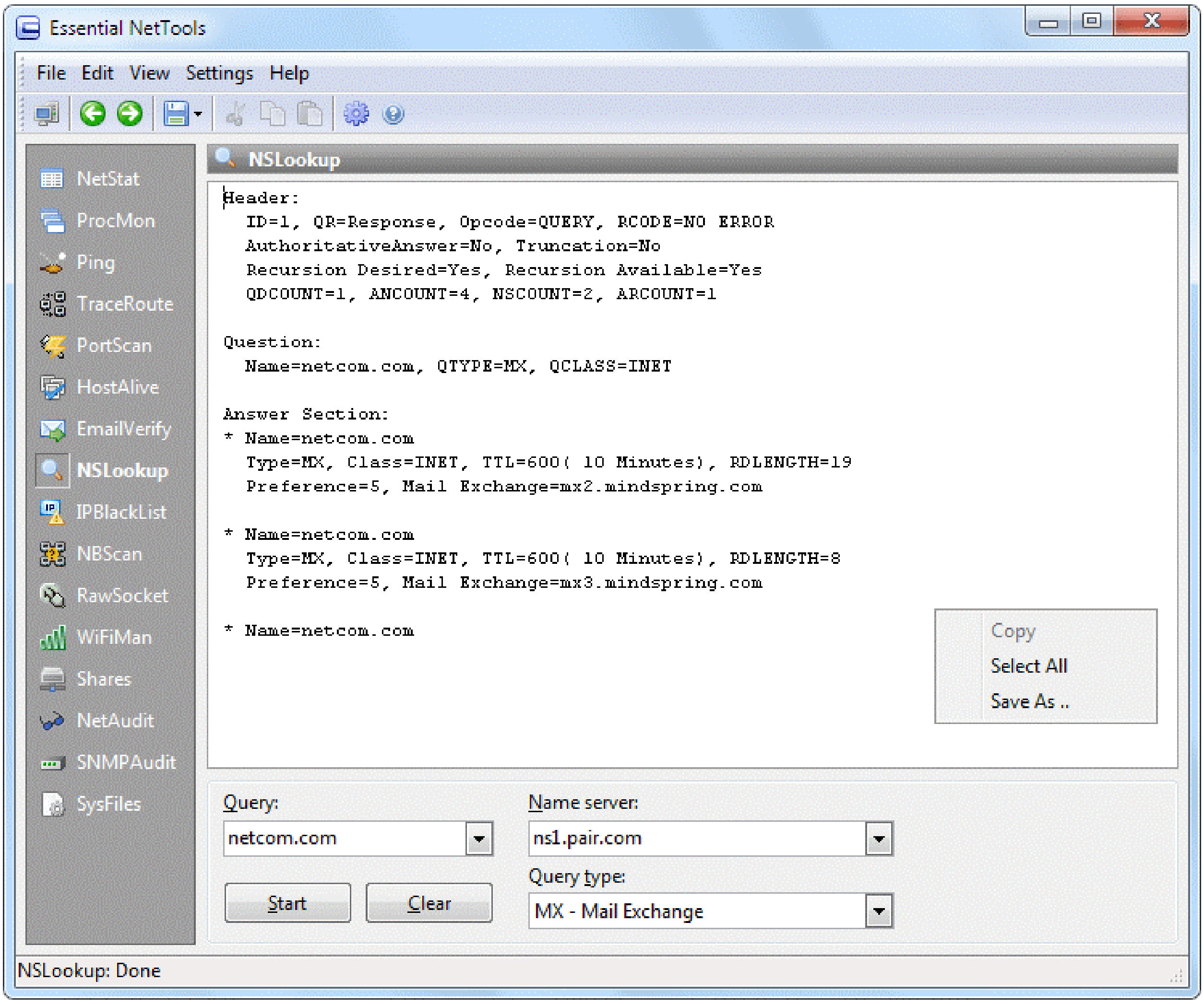
Query: www.yahoo.com

Name server: 192.168.1.1

Query type: Standard Resolve Function

NSLookup: Done

To perform non-standard queries, select the type of record you are requesting from the **Query type** list, enter your query in the **Query** field, and enter a DNS server address in the **Name server** field. When you run the program for the first time, the **Name server** drop-down list contains the list of your default DNS servers; you can select one from the list, or enter an arbitrary one, e.g. "ns1.pair.com".



```
Header:
  ID=1, QR=Response, Opcode=QUERY, RCODE=NO ERROR
  AuthoritativeAnswer=No, Truncation=No
  Recursion Desired=Yes, Recursion Available=Yes
  QDCOUNT=1, ANCOUNT=4, NSCOUNT=2, ARCOUNT=1

Question:
  Name=netcom.com, QTYPE=MX, QCLASS=INET

Answer Section:
* Name=netcom.com
  Type=MX, Class=INET, TTL=600( 10 Minutes), RDLENGTH=19
  Preference=5, Mail Exchange=mx2.mindspring.com

* Name=netcom.com
  Type=MX, Class=INET, TTL=600( 10 Minutes), RDLENGTH=8
  Preference=5, Mail Exchange=mx3.mindspring.com

* Name=netcom.com
```

Query: netcom.com

Name server: ns1.pair.com

Query type: MX - Mail Exchange

NSLookup: Done

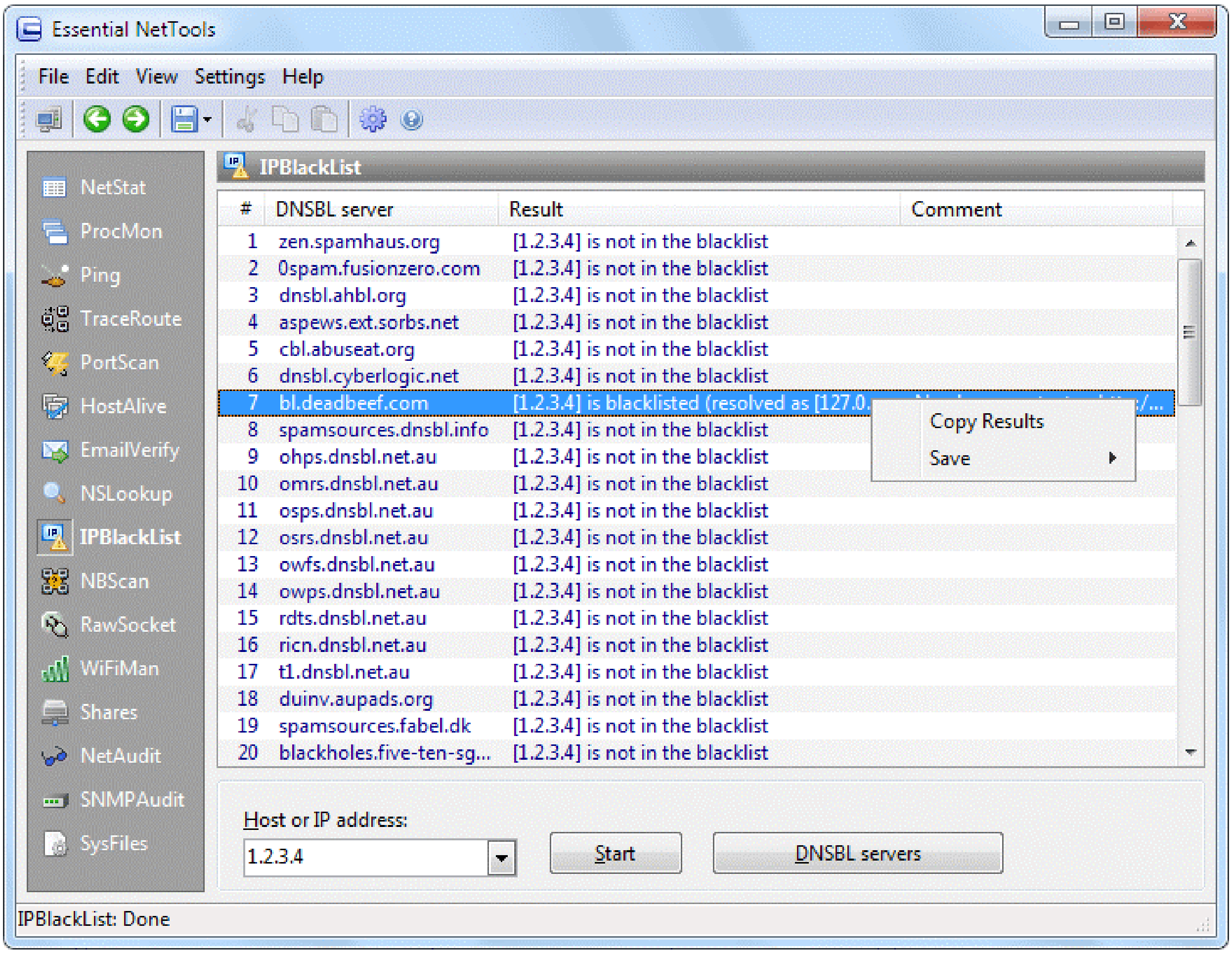
NSLookup offers many query types to choose from, and it takes some understanding of the Internet to perform any queries other than **Standard Resolve Function**. If you are a beginner and want to learn more about various query types, we suggest reading RFC 1034 and RFC 1035, or searching the web for query type names.

Right-clicking on the window brings up a menu with the following commands:

Copy – copies selected text to the clipboard.
Select All – selects all text in the window.
Save – saves the log to a file.

IPBlackList

IPBlackList is a tool for checking if an IP address is listed in various black lists, such as SPAM databases, banned IP addresses, open proxies or mail relays, etc. This tool is instrumental in figuring out why a given IP address is rejected by some network resources, such as mail servers.



#	DNSBL server	Result	Comment
1	zen.spamhaus.org	[1.2.3.4] is not in the blacklist	
2	0spam.fusionzero.com	[1.2.3.4] is not in the blacklist	
3	dnsbl.ahbl.org	[1.2.3.4] is not in the blacklist	
4	aspews.ext.sorbs.net	[1.2.3.4] is not in the blacklist	
5	cbl.abuseat.org	[1.2.3.4] is not in the blacklist	
6	dnsbl.cyberlogic.net	[1.2.3.4] is not in the blacklist	
7	bl.deadbeef.com	[1.2.3.4] is blacklisted (resolved as [127.0.	:/...
8	spamsources.dnsbl.info	[1.2.3.4] is not in the blacklist	
9	ohps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
10	omrs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
11	osps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
12	osrs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
13	owfs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
14	owps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
15	rdts.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
16	ricn.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
17	t1.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
18	duinv.aupads.org	[1.2.3.4] is not in the blacklist	
19	spamsources.fabel.dk	[1.2.3.4] is not in the blacklist	
20	blackholes.five-ten-sg...	[1.2.3.4] is not in the blacklist	

Host or IP address: 1.2.3.4

IPBlackList: Done

IPBlackList checks the entered IP address against the databases maintained by numerous DNSBL servers (click here for more information on this technology). In brief, this tool works as follows: For instance, you want to check if 1.2.3.4 is on the black list maintained by the antispam.somedomain.com server. IPBlackList sends a DNS query that looks like 4.3.2.1.antispam.somedomain.com to the default DNS server. If such a DNS record exists, i.e. the specified host address is resolvable to an IP address (according to the DNSBL specifications, such IP address must belong to the range of local IP addresses, i.e. 127.x.x.x.), then the IP address we are checking, 1.2.3.4, is blacklisted.

Please note that we do not maintain any of these lists, and therefore we cannot remove
you from any of them.

IPBlackList allows you to check an IP address against multiple DNSBL servers simultaneously. Essential NetTools includes a list of popular DNSBL servers, but you can use your own list by clicking on the **DNSBL servers** button.

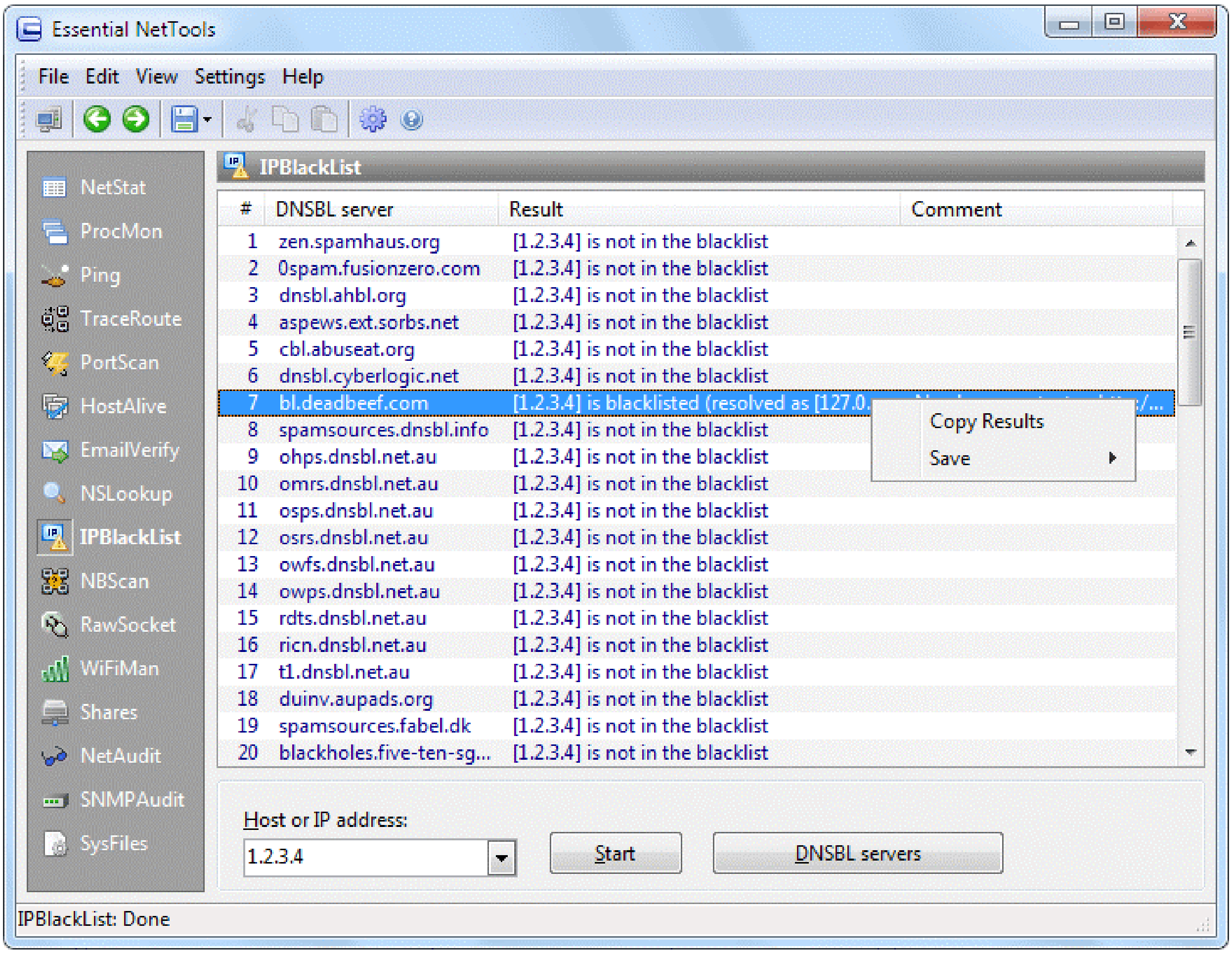
An up-to-date list of functioning DNSBL servers is available at
http://www.declude.com/Articles.asp?ID=97.

Right-clicking on the window brings up a menu with the following commands:

Copy Results – copies the IPBlackList table to the clipboard.
Save – saves the IPBlackList table to a file.

NBScan

NBScan is a NetBIOS Scanner, a powerful and fast tool for exploring networks. NBScan can scan a network within a given range of IP addresses and list computers offering NetBIOS resource sharing service as well as their name tables. Unlike the nbtstat utility supplied with Windows, this tool provides a friendly, graphical, user interface and easy management of the lmhosts file and features parallel scanning, which allows checking a class C network in less than 1 minute. Both Class C and B networks can be scanned. NBScan can facilitate routine tasks often carried out by system integrators, administrators, and analysts.



#	DNSBL server	Result	Comment
1	zen.spamhaus.org	[1.2.3.4] is not in the blacklist	
2	0spam.fusionzero.com	[1.2.3.4] is not in the blacklist	
3	dnsbl.ahbl.org	[1.2.3.4] is not in the blacklist	
4	aspews.ext.sorbs.net	[1.2.3.4] is not in the blacklist	
5	cbl.abuseat.org	[1.2.3.4] is not in the blacklist	
6	dnsbl.cyberlogic.net	[1.2.3.4] is not in the blacklist	
7	bl.deadbeef.com	[1.2.3.4] is blacklisted (resolved as [127.0.	
8	spamsources.dnsbl.info	[1.2.3.4] is not in the blacklist	
9	ohps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
10	omrs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
11	osps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
12	osrs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
13	owfs.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
14	owps.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
15	rdts.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
16	ricn.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
17	t1.dnsbl.net.au	[1.2.3.4] is not in the blacklist	
18	duinv.aupads.org	[1.2.3.4] is not in the blacklist	
19	spamsources.fabel.dk	[1.2.3.4] is not in the blacklist	
20	blackholes.five-ten-sg...	[1.2.3.4] is not in the blacklist	

Host or IP address: 1.2.3.4

IPBlackList: Done

Before you start scanning, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above and specify the number of simultaneous connections and the connection timeout in the Tasks and Timeout spinboxes. You can also enable the **Advanced Mode** (see the description below). Click **Start** to begin scanning.

When NBScan detects a computer that offers NetBIOS resource sharing within the set range, the information about the computer is added to the list. The **Name**, **Workgroup**, **IP Address**, and **MAC** address columns are self-explanatory. The **RS**, or **Resource Sharing** column, is used to assess whether the computer offers resource sharing: Some computers may not be configured to share resources; however, they respond to NetBIOS queries and are listed.

Left-clicking on a listed computer displays its name table in the lower window. If you have a problem interpreting name tables, you can take a look at the NetBIOS Table reference included in this help file.

Right-clicking on a listed computer brings up a menu with the following commands:

Open Computer – attempts to open the selected computer. If the computer is accessible, a new Windows Explorer window with remote resources will appear.

Add Item to LMHosts - adds a record associated with the selected computer to the lmhosts file in the appropriate format.

Add All Items to LMHosts - adds records associated with the listed computers to the lmhosts file in the appropriate format (computers that have no shared resources are not added).

Copy IP Address – copies the selected computer's IP address to the clipboard. **Copy MAC Address** – copies the selected computer's MAC address to the clipboard. **Send To** – sends the selected IP address to other tools or to SmartWhois.

Copy Results – copies the NBScan table to the clipboard.

Save – saves the NBScan table to a file.

Advanced Mode

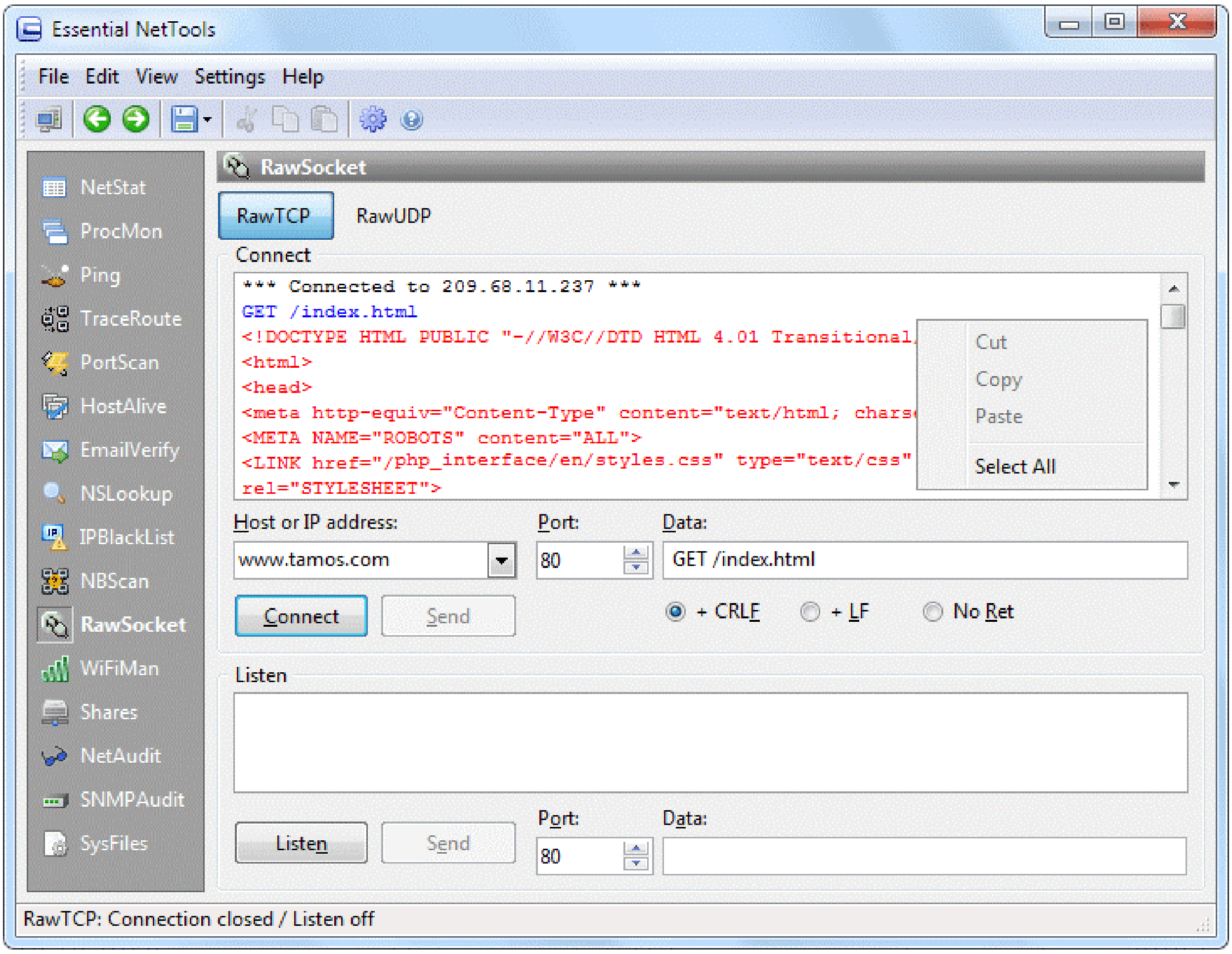
Because of some peculiarities in handling NetBIOS connections, a small percentage of computers can send replies to queries only to port 137, no matter from which port the query was sent. The advanced mode allows you to choose whether you want the program to receive replies sent to port 137. To switch to the advanced mode, check the **Advanced mode (bind to local port 137)** box. The advanced mode may not be available if the computer has logged on to the network. If the computer has already logged on, this menu item is disabled. If you want to use this mode, you should turn it on BEFORE logging on to the network. For example, if you use a dial-up connection to the Internet, you should first launch the program, and then check **Advanced mode (bind to local port 137)**, and then dial-up.

Important: Using the advanced mode can influence the operation of some of the Windows network services bound to port 137, e.g. you might not be able to use nbtstat or connect to remote computers. In order to restore the normal operation of such services, you should turn off the advanced mode, log off the network, and log on again.

The reason for these limitations is simple: There is only one port 137 on any system, and it is "owned" by the process that claimed the port first. If Essential NetTools was the first to bind to this port, the program can operate in the advanced mode, but the OS is unable to use it. If the OS binds to it first, then Essential NetTools cannot use the same port. Please remember that this mode is just an advanced feature, and you may not need to use it. In fact, it is quite probable that you will not notice any difference between the results obtained with the advanced mode turned on or off.

RawSocket

RawSocket provides you with the tools that allow you to send and receive raw data to/from an IP address, as well as listen for inbound TCP or UDP connections on any local port. It is useful in troubleshooting different networking services and understanding application-level protocols, such as POP, SMTP, or DAYTIME. The sample screen shot displays an HTTP session that you can establish using this tool:



```
*** Connected to 209.68.11.237 ***
GET /index.html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional,
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; chars
<META NAME="ROBOTS" content="ALL">
<LINK href="/php_interface/en/styles.css" type="text/css"
rel="STYLESHEET">
```

Host or IP address: www.tamos.com
Port: 80
Data: GET /index.html
● + CRLF ○ + LF ○ No Ret

Port: 80
Data:

RawTCP: Connection closed / Listen off

Connect

To connect to a remote host, enter an IP address or hostname, select a destination port, and click **Connect**. Once the connection is established, you can enter any data in the **Data** input field and click the **Send** button to send the data to the remote host. When sending data, you can toggle the characters used as a string delimiter: Line Feed (0x0A), Carriage Return + Line Feed (0x0D0A), or no delimiter at all. To send arbitrary characters (including non-printing ones) use [xx] structures, where xx is the hexadecimal code of the character being sent. For instance, the structure [48]ELLO will be translated into HELLO, as the ASCII-code of the 'H' character is 0x48. The data being sent is shown in blue; the data being received is shown in red.

Listen

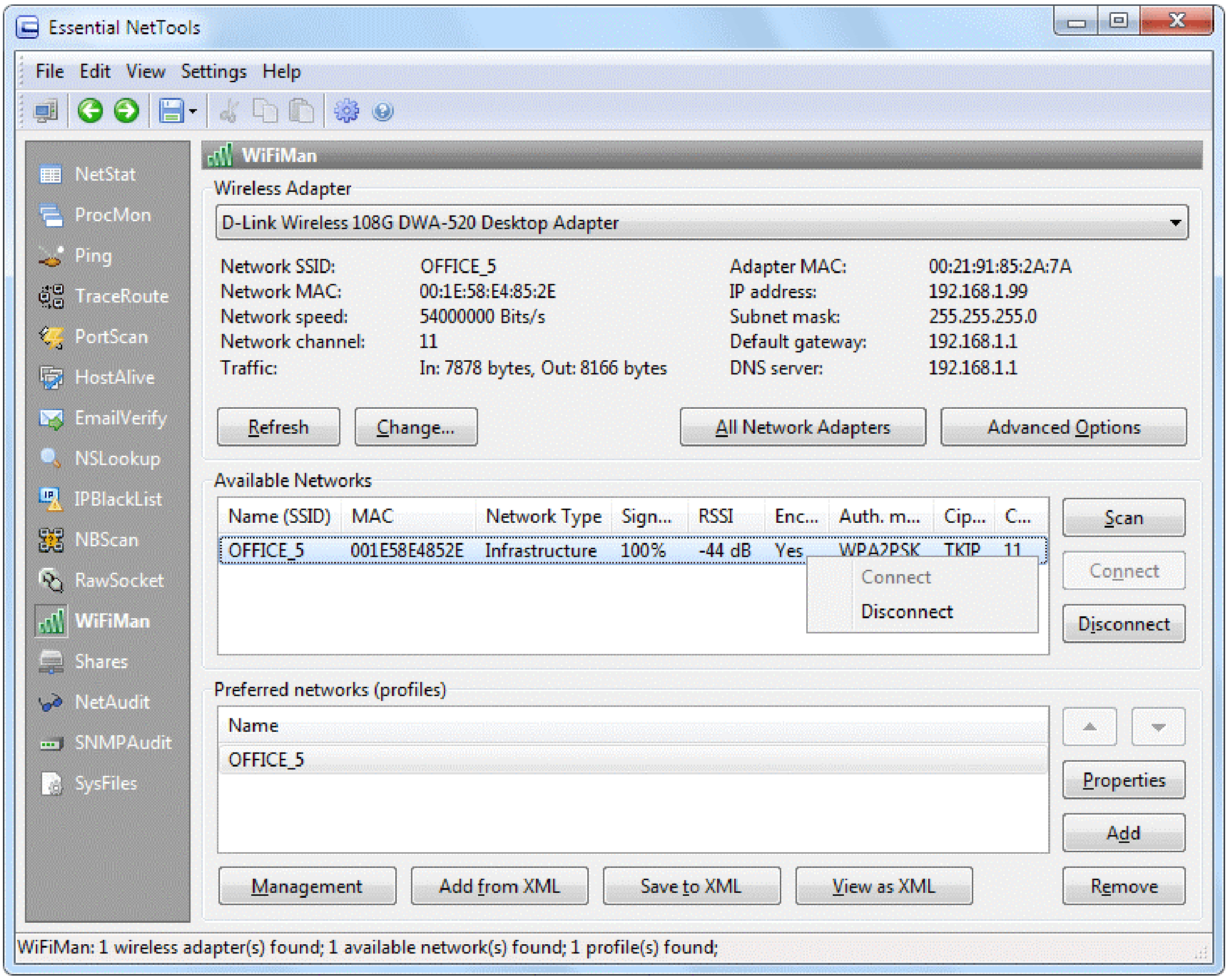
To listen for incoming connections, select a local port and click **Listen**. If a remote host connects to your PC, the information about that connection will be displayed in the window. If the remote host starts sending data to the open local port, the data being sent will be shown in red. You can send data to the remote host as described above. Your data will be shown in blue. To close the local port, click on the **Hang Up** button.

The information above applies to both **RawTCP** and **RawUDP**, with the only exception: Since UDP is a stateless, connectionless protocol; there is no **Connect** button in **RawUDP**. To send UDP data, you do not need to establish a connection. Rather, you just need to send the data out.

WiFiMan

WiFiMan is a tool that shows wireless adapters installed on a computer, lists available wireless networks and allows you to manage connection profiles.

Note: This module requires Windows XP SP2 or a newer operating system.



D-Link Wireless 108G DWA-520 Desktop Adapter

Network SSID:	OFFICE_5	Adapter MAC:	00:21:91:85:2A:7A
Network MAC:	00:1E:58:E4:85:2E	IP address:	192.168.1.99
Network speed:	54000000 Bits/s	Subnet mask:	255.255.255.0
Network channel:	11	Default gateway:	192.168.1.1
Traffic:	In: 7878 bytes, Out: 8166 bytes	DNS server:	192.168.1.1

Name (SSID)	MAC	Network Type	Sign...	RSSI	Enc...	Auth. m...	Cip...	C...
OFFICE_5	001E58E4852E	Infrastructure	100%	-44 dB	Yes	WPA2PSK	TKIP	11

Name
OFFICE_5

WiFiMan: 1 wireless adapter(s) found; 1 available network(s) found; 1 profile(s) found;

The interface of this tool consists of the following three groups: **Wireless Adapter**, **Available Networks**, and **Preferred Networks (profiles)**.

The **Wireless Adapter** group displays information about the selected network adapter. If you have more than one adapter installed, select the desired one from the list. For each adapter, you can view its basic parameters, including the details of the wireless network it is connected to. The following commands are available for this group:

- **Refresh** – refreshes information about wireless adapters.
- **Change…** – shows the dialog where you can change the parameters of the selected wireless adapter: **IP Address**, **Subnet mask**, **Default gateway**, **DNS server**, and **MAC address**.
- **All Network Adapters** – displays the dialog with the list of all network adapters and information about them. Use the corresponding buttons to enable, disable or restart the adapter.

- **Advanced Options** – allows you to configure a number of settings; you can select the network type, indicate whether Windows should be used for managing the adapter and select the mode used for connecting to a network. The following options are available for this dialog:
    - **Networks to access** – configures the behavior of the wireless network search. This option works in Windows Vista or newer operating systems only.
    - **Use Windows to configure settings** – this option is supported in Windows XP only.
    - **Automatically connect to** non-preferred networks – this option is supported in Windows XP only.

The **Available Networks** group lists available wireless networks along with their details. The following commands are available for this group:

- **Scan** – scans the air for available wireless networks.
- **Connect** – connects to the selected network.
- **Disconnect** – disconnects from the selected network.

Right-clicking on the record displays the context menu with the **Connect** and **Disconnect** commands.

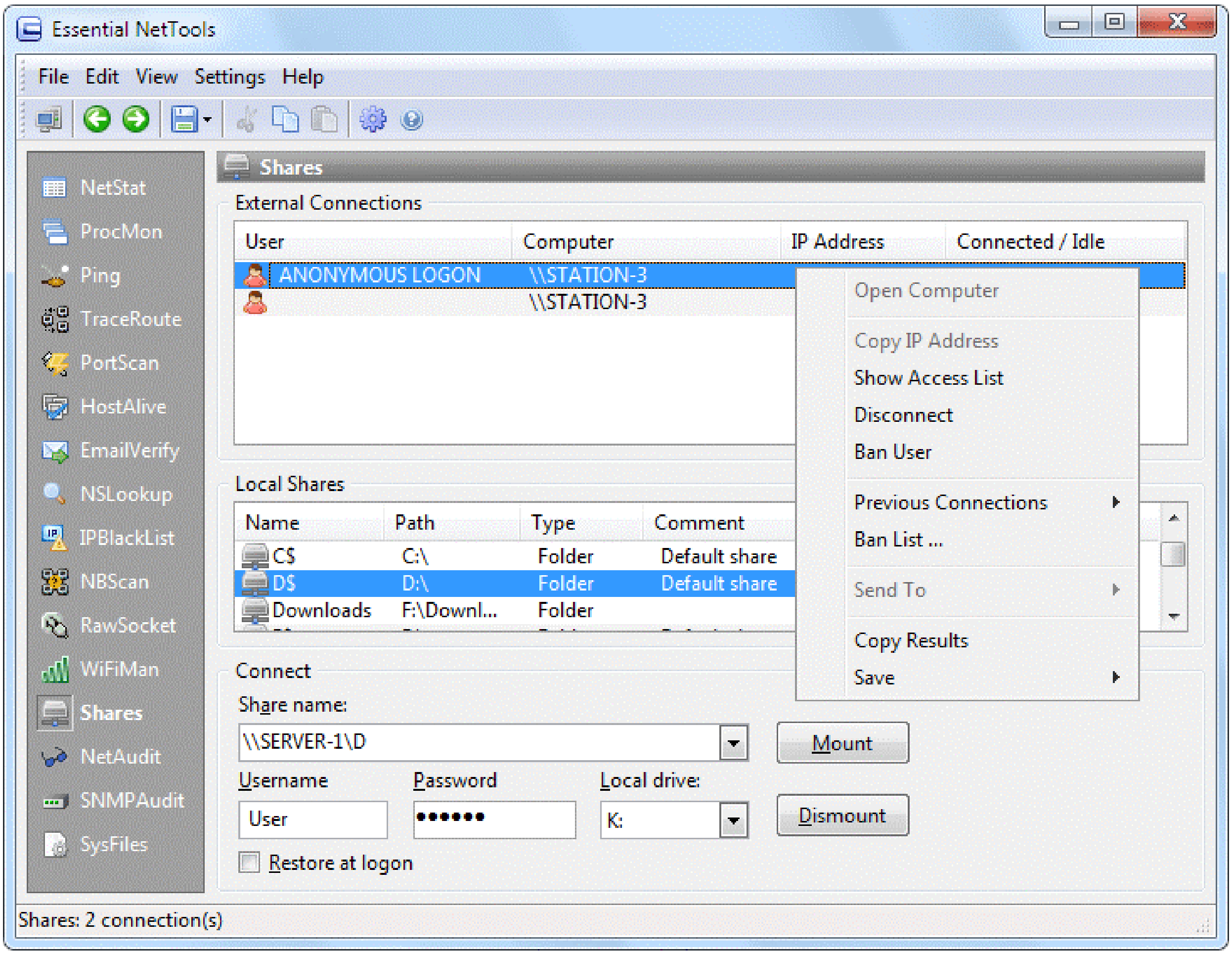
The **Preferred Networks (profiles)** group lists preset profiles for connecting to wireless networks. You can create, edit, or delete existing profiles. Exporting and importing profiles in XML format might be useful when you need to quickly transfer settings from one computer to another, or even distribute settings over a group of users. The following commands are available:

- **Management** – opens the standard dialog for managing wireless networks. This option is available in Windows Vista or newer operating systems. It is not available in Windows XP.
- **Add from XML** – adds a network profile from an XML file.
- **Save to XML** – saves a network profile to an XML file.
- **View as XML** – allows you to view the selected network profile as XML.
- **Properties** –click on this button (or double-click on the selected record) for the network profile configuration dialog to be shown. Authentication, data encryption, and other settings may be configured in this dialog.
- **Add** – adds a new network profile and allows you to configure its settings.
- **Remove** – deletes the selected profile from the preferred networks list.

If you'd like change to change the order of preferred network profiles, use the **Up** and **Down** buttons located to the right from the **Preferred networks (profiles)** list.

Shares

The **Shares** tool allows you to perform three tasks: watch connections to your resources, view local open shares, and connect to remote resources over the network.



Shares

External Connections

User	Computer	IP Address	Connected / Idle
ANONYMOUS LOGON	\\STATION-3		
	\\STATION-3		

Local Shares

Name	Path	Type	Comment
C$	C:\	Folder	Default share
D$	D:\	Folder	Default share
Downloads	F:\Downl...	Folder	

Connect

Share name: \\SERVER-1\D

Username: User

Password: ••••••

Local drive: K:

□ Restore at logon

Shares: 2 connection(s)

External Connections

When the program detects an external connection to your computer, it displays the information about the user as shown above. A new connection is also indicated by a sound alert and the tray icon color: the icon turns red.

Right-clicking on the window brings up a menu with the following commands:

Open Computer – attempts to open the selected computer. If the computer is accessible, a new Windows Explorer window listing remote resources will appear. You must have Client for Microsoft Networks installed to use this feature.

Copy IP Address – copies the selected computer's IP address to the clipboard.

Show Access List – brings up a window listing the local files accessed by the selected user.

Disconnect – disconnects the selected computer.

Ban User – adds the selected computer's name to the ban list. When a banned user tries to connect to your computer, he or she will be automatically disconnected.

Previous Connections – shows the log of previous connections and allows you to delete it.

Ban List – allows you to edit the ban list.

Send To – sends the selected IP address to other tools or to SmartWhois.

Copy Results – copies the connections table to the clipboard.

Save – saves the connections table to a file.

Important: Disconnecting or even banning users cannot be considered a serious security measure. By disconnecting a user, you instruct the operating system to terminate the current connection, but the user can still re-connect in a few seconds. This can only slow down such connections. If you notice an unauthorized connection, it is recommended that you change the access policy by setting passwords for shared resources.

Local Shares

This frame displays the list of shared resources on your computer.

Connect

You can use this tool for connecting to remote resources over the network. To map a remote resource to your local free drive, you should enter a valid share name in the **Share Name** field. A valid share name is a computer name preceded with 2 backslashes and followed by 1 backslash and a resource name. For example, in order to map the folder "COMMON" on computer "STATION1", you should type:

\\STATION1\COMMON

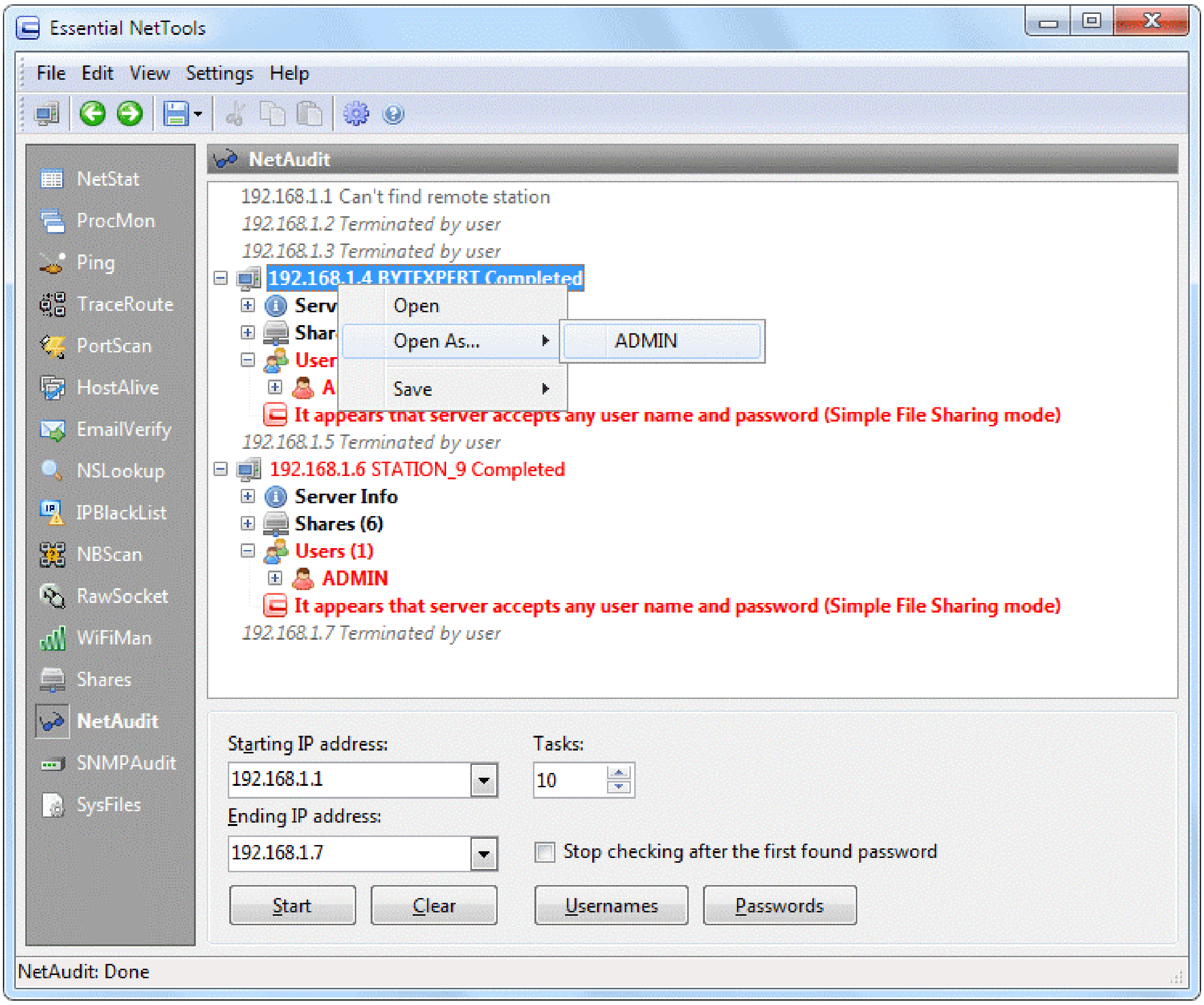
You should also enter a username and a password in the corresponding fields and select a free drive letter from the **Local Drive** drop-down list. Note that your computer should be able to resolve the remote computer name you specified to the corresponding IP address. It usually means that the IP address - computer name pair should be present in your lmhosts file. (You can add this pair using the SysFiles tool.)

Finally, click on the **Mount** button to map a share to a local drive. Check the **Restore at logon** box if you want your computer to re-connect to the shared resource at the next logon. To un-map a resource, click on the **Dismount** button. Please note that the **Dismount** command will attempt to disconnect the drive specified in the **Local Drive** field, so if multiple resources have been connected, you should select the corresponding drive letter.

NetAudit

NetAudit (NetBIOS Auditing Tool) is a tool for auditing networks and individual computers running NetBIOS file sharing service. This tool was originally written many years ago as a GNU command-line utility and became very popular. Our tool was written from scratch, but it was inspired by this popular utility.

Despite the fact that very powerful and expensive solutions exist to check hundreds of potential loopholes in a network, most security problems stem from incorrect configuration of NetBIOS resource sharing. With NetAudit you can easily audit your network and/or individual computers. Remember that you must obtain the permission of the network's administrator before auditing the network.



```
192.168.1.1 Can't find remote station
192.168.1.2 Terminated by user
192.168.1.3 Terminated by user
⊟ 192.168.1.4 BYTEXPERT Completed
  ⊞ Serv
  ⊞ Shar
  ⊟ User
    ⊞ A
  It appears that server accepts any user name and password (Simple File Sharing mode)
192.168.1.5 Terminated by user
⊟ 192.168.1.6 STATION_9 Completed
  ⊞ Server Info
  ⊞ Shares (6)
  ⊟ Users (1)
    ⊞ ADMIN
  It appears that server accepts any user name and password (Simple File Sharing mode)
192.168.1.7 Terminated by user
```

Starting IP address: 192.168.1.1

Ending IP address: 192.168.1.7

Tasks: 10

□ Stop checking after the first found password

NetAudit: Done

Before you start auditing, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above. Please note that the first 3 octets of the starting and ending IP addresses should be the same. You can customize the username and password lists by clicking on the **Usernames** and **Passwords** buttons correspondingly. These lists are used to check the possibility of potential intrusion, and you can customize them based on the name table obtained by NBScan or any other considerations. A null password is always added automatically as the first password to the list, because it is non-printable; however, it is often a good password to try. All supplied passwords are tried for all usernames. If you have previously modified the lists, you can restore the default values by clicking on the **Restore Defaults** button.

You can set the number of simultaneously audited addresses in the **Tasks** spinbox. You can also limit the audit of the individual host to the first successfully retrieved password by checking the **Stop checking after the first found password** box. This will allow you to stop searching for other passwords and proceed of the next address immediately.

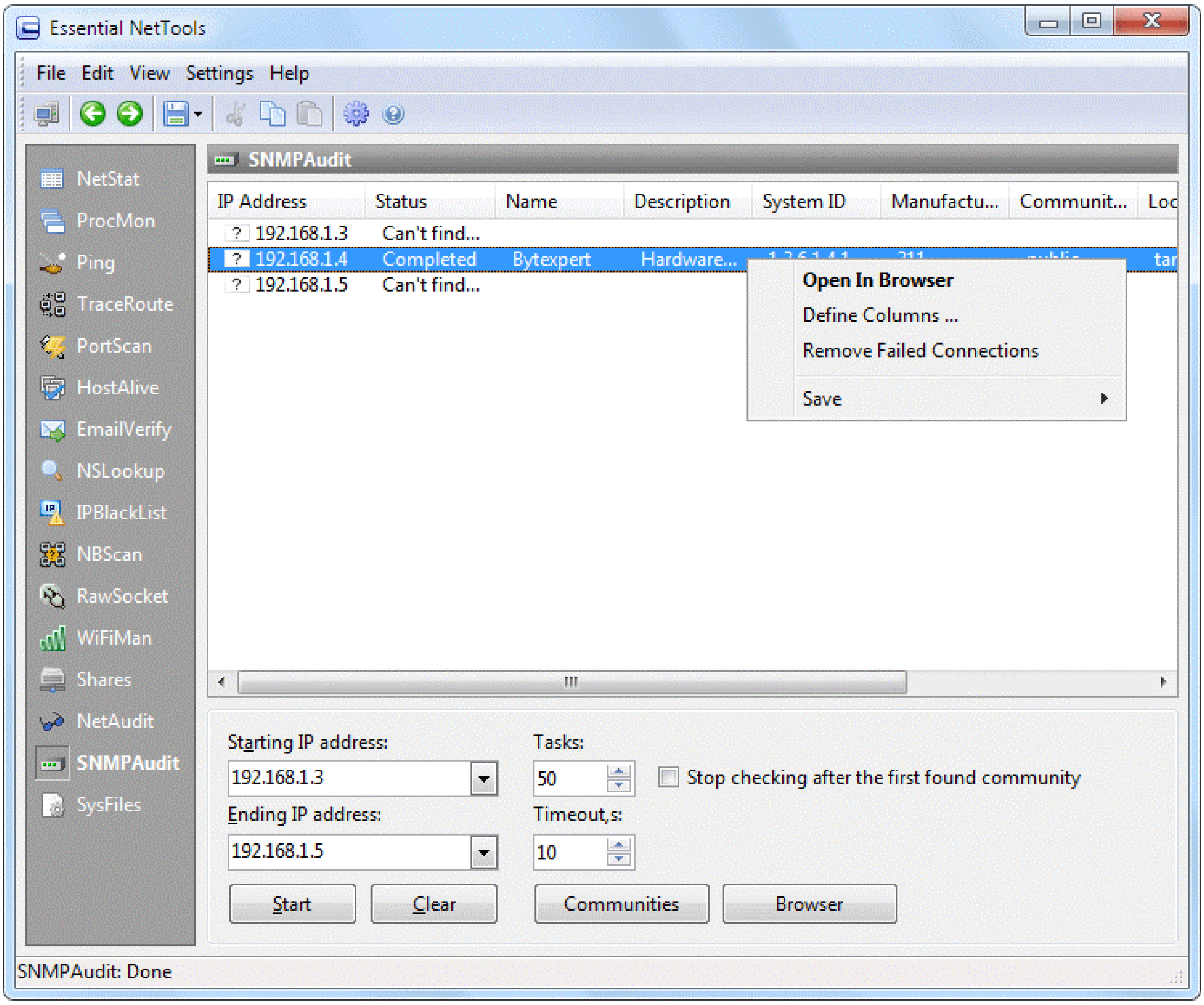
To start auditing, click on the **Start** button. You can stop the process at any moment by clicking on the **Stop** button. Remember that auditing a computer is a lengthy process that depends on many factors, and you should be prepared to wait for a long time, especially if you set a wide range of IP addresses. When NetAudit detects a security flaw in the computer being audited, an alert sound is played and the tray icon starts blinking.Right-clicking on the window brings up a menu with the following commands:

Copy – copies selected text to the clipboard.
Select All – selects all text in the window.
Save – saves the log to a file.

SNMPAudit

SNMPAudit is a tool for quick discovery of SNMP-enabled devices and obtaining selected information from them. This tool can be used to poll the devices that are present in the specified network address range. SNMP protocol (Simple Network Management Protocol) is used for managing various network devices, such as servers, routers, switches, etc. Having an SNMP-enabled device, it is possible to obtain a great amount of data regarding the status of the device and its functioning.

SNMP protocol uses the **community** term for indicating the affiliation of an SNMP device with some class according to the functionality of the device and its purpose. An SNMP-enabled device can be configured so that it belongs to several communities. When making a connection to an SNMP device, the console (i.e. Essential NetTools) indicates the community that the request is addressed to. It's important to know the community the device belongs to. If the community is not specified correctly, then the device will simply ignore the request. So, community is also used as an authorization element (the analog of a password), which is necessary to know in order to access an SNMP-enabled device and retrieve data from it.



IP Address	Status	Name	Description	System ID	Manufactu...	Communit...	Loc
? 192.168.1.3	Can't find...						
? 192.168.1.4	Completed	Bytexpert	Hardware...	1.3.6.1.4.1...	311	public	tar
? 192.168.1.5	Can't find...						

Starting IP address: 192.168.1.3

Tasks: 50

☐ Stop checking after the first found community

Ending IP address: 192.168.1.5

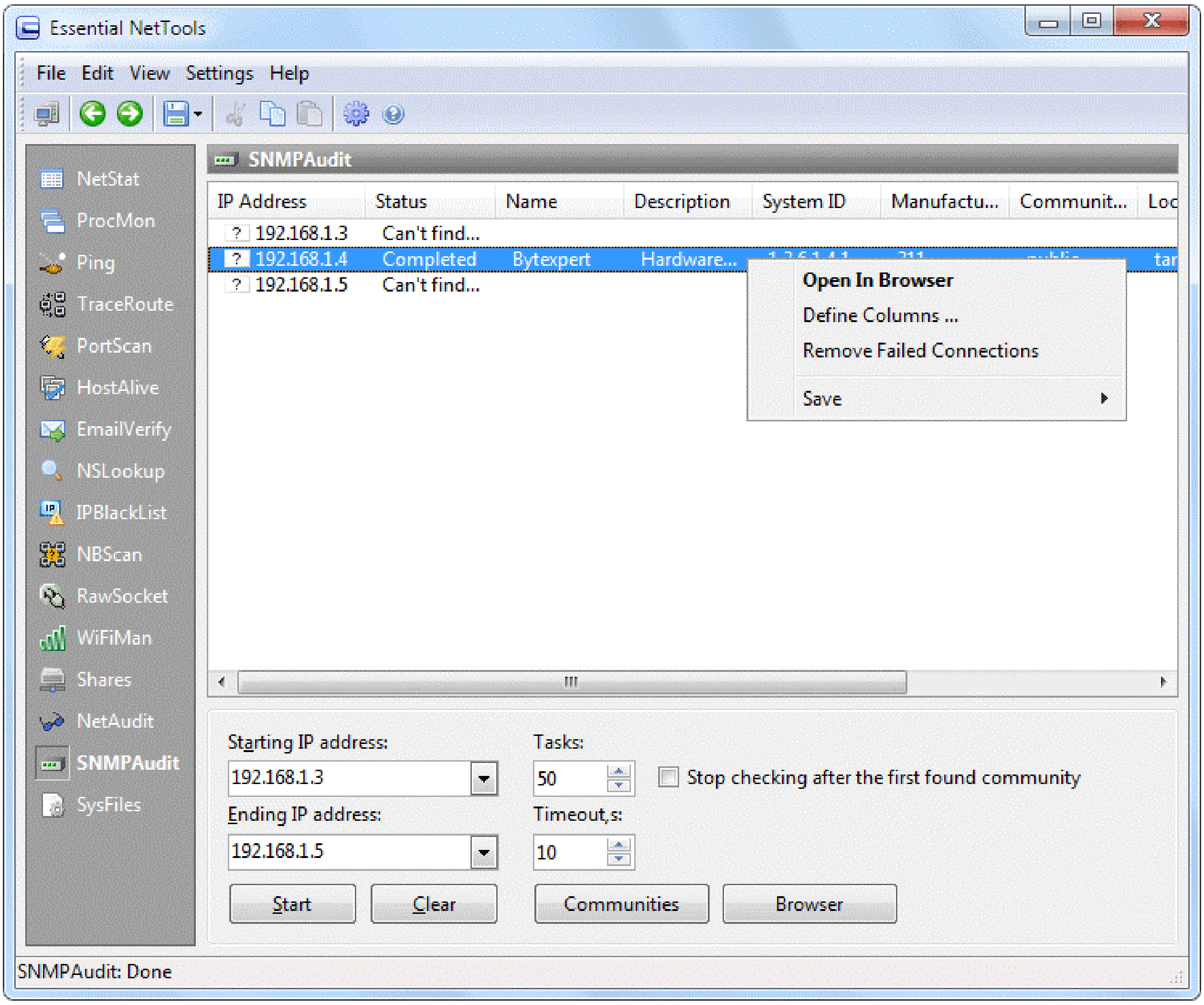
Timeout,s: 10

SNMPAudit: Done

The commonly used community name is "**public**". You can add your community to the list of queried communities by clicking the **Communities** button. Please note that **SNMPAudit** always checks for the availability of the **public** community, even if it is not in the community list. **Essential NetTools** will try each element (i.e. community) from the community list for every address from the specified range. If you are satisfied with just one discovered community per host, then check the **Stop checking at the first found**

community box. In this case, **SNMPAudit** will stop after the first community is found and will not check the remaining communities from the list. The program will then proceed querying other addresses from the specified range.

Before you start scanning, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above. Specify the number of simultaneous connections and connection timeout in the **Tasks** and **Timeout** spinboxes. Click on the **Start** button in order to start scanning. The IP addresses, status of the hosts being queried and other information will appear in the **SNMPAudit** window during the scan. If a host is not an SNMP-enabled device, you will see a "Can't find remote station" or "Connection rejected" message in the Status column (you can clear the list from failed connections by using the **Remove Failed Connections** command in the context menu). If you would like to stop scanning, click on the **Stop** button. Clicking on the **Clear** button will empty the list in the main window; however, your current settings such as starting and ending IP addresses, the number of simultaneous connections and connection timeout settings will be preserved.



IP Address	Status	Name	Description	System ID	Manufactu...	Communit...	Loc
192.168.1.3	Can't find...						
192.168.1.4	Completed	Bytexpert	Hardware...				tar
192.168.1.5	Can't find...						

Starting IP address: 192.168.1.3

Tasks: 50

□ Stop checking after the first found community

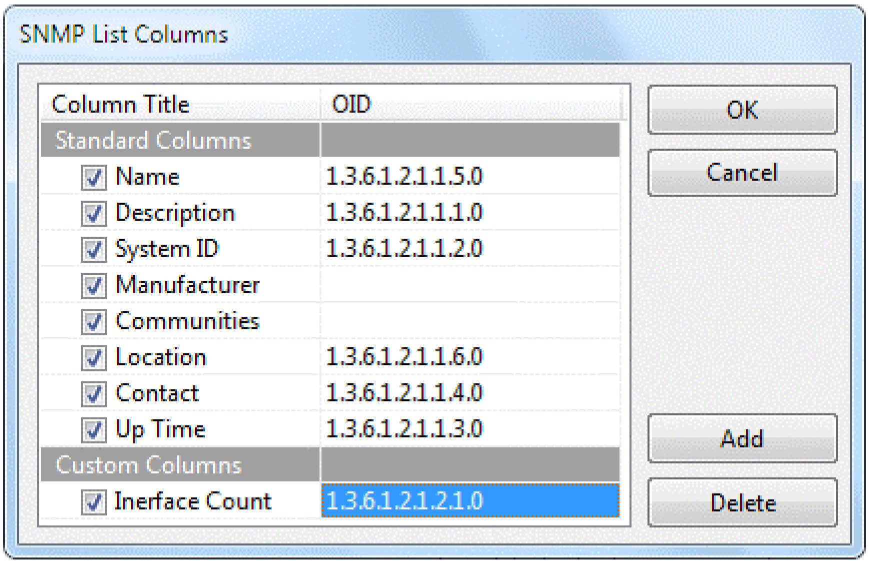
Ending IP address: 192.168.1.5

Timeout,s: 10

SNMPAudit: Done

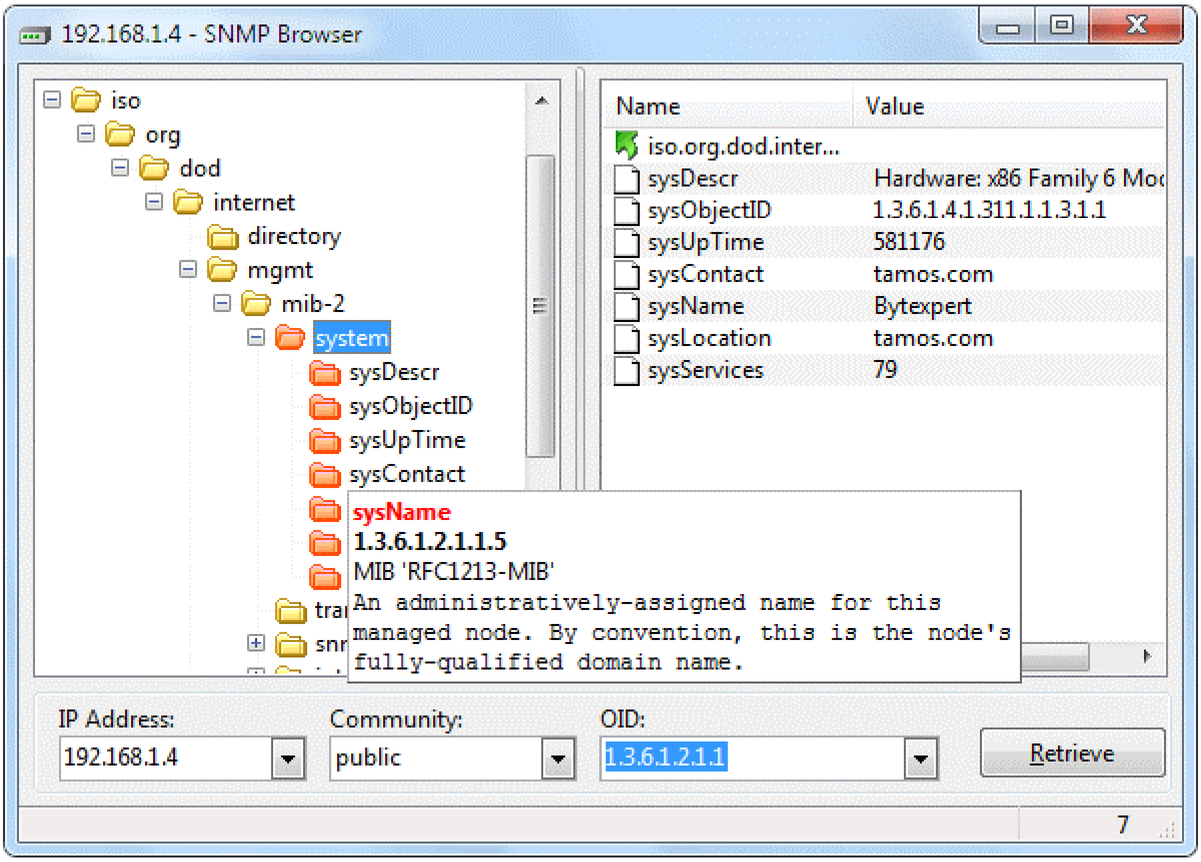
After discovering a device that belongs to a community from the list, SNMPAudit makes a query for the primary data characterizing the device, and displays the obtained result in the list. You can choose to display the following data columns in the main window of **SNMPAudit** tool: **Device Name**, **Device Description**, **Device Location**, **Device Manufacturer**, **System ID**, **Admin Contact Info**, and **Device Up Time**. Right-click on the main window and select **Define Columns** from the pop-up menu. You will then be able to check the columns that you want displayed and add custom defined data columns.

You cannot modify the settings of **Standard Columns** or delete them. When adding custom columns you must type in the correct path to SNMP data in the OID column. You can use the drop-down list or look for OID in the respective MIB database. If you would like to delete the column, select it and click on the **Delete** button.



Column Title	OID
Standard Columns	
☑ Name	1.3.6.1.2.1.1.5.0
☑ Description	1.3.6.1.2.1.1.1.0
☑ System ID	1.3.6.1.2.1.1.2.0
☑ Manufacturer	
☑ Communities	
☑ Location	1.3.6.1.2.1.1.6.0
☑ Contact	1.3.6.1.2.1.1.4.0
☑ Up Time	1.3.6.1.2.1.1.3.0
Custom Columns	
☑ Inerface Count	1.3.6.1.2.1.2.1.0

If you would like to examine a particular SNMP-enabled device from the list of queried devices, double-click on it or select it and click on the **Browse** button. An SNMP Browser window will open.



Name	Value
iso.org.dod.inter...	
sysDescr	Hardware: x86 Family 6 Moc
sysObjectID	1.3.6.1.4.1.311.1.1.3.1.1
sysUpTime	581176
sysContact	tamos.com
sysName	Bytexpert
sysLocation	tamos.com
sysServices	79

sysName
1.3.6.1.2.1.1.5
MIB 'RFC1213-MIB'

```
An administratively-assigned name for this
managed node. By convention, this is the node's
fully-qualified domain name.
```

IP Address: 192.168.1.4
Community: public
OID: 1.3.6.1.2.1.1

SNMP Browser allows you to explore all available data for the given community received from an SNMP device. If the appropriate description exists in the MIB database, you will also be able to read the description of the retrieved data.

Enter the IP address of the device, community, and starting OID in the SNMP browser window. Click **Retrieve** or just hit Enter. The program will retrieve all underlying data levels beginning with the specified OID. The retrieved data structure will be displayed in the left pane. If you are not sure which OID to start with, choose the starting value from the tree on the left. In this case, the **OID** field will be automatically filled with the full path to the selected tree element. Usually, all the data belongs to the **iso.org** or **1.3** branches – please choose OID **1** or **1.3** for retrieving all available data from the selected device.

The actual data received from the device will be displayed in the right pane. Data fields retrieved from the device will be displayed in the left pane and marked with the highlighted icons.

By default, the right pane only displays the data corresponding to the selected tree element (Windows Explorer style). If you'd like to display all data from the subsequent layers, right click on the list and choose **Show All Values** from the pop-up menu.

You can open as many SNMP browser windows as you wish.

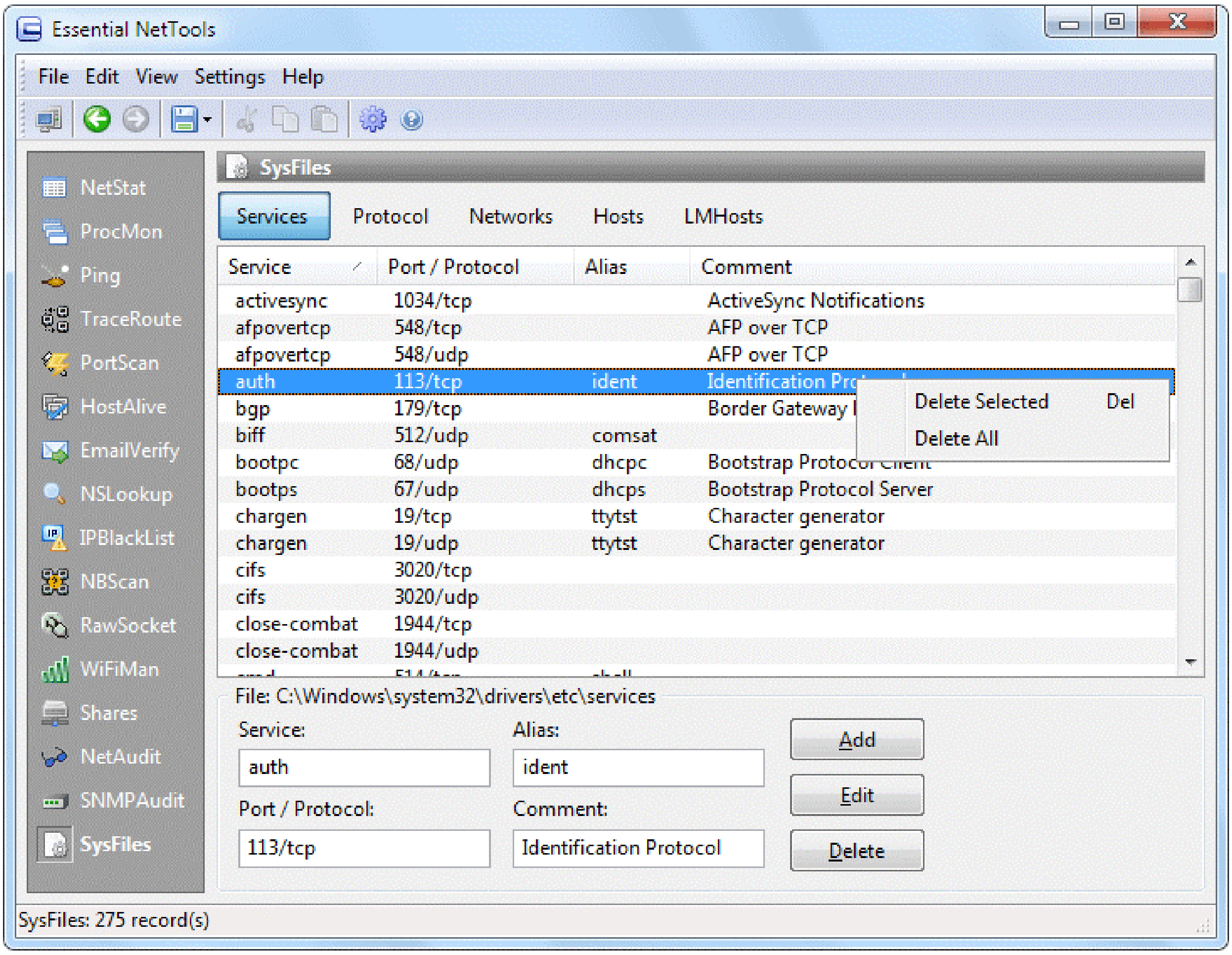
MIB Databases

With the first browser launch, Essential NetTools will load MIB databases from the program folder (by default C:\Program Files\EssNetTools3\SNMP\MIB) and display them as a tree view. MIB stands for Management Information Base and OID stands for Object ID. MIB databases contain the access paths to various data (OID) of the SNMP-enabled devices and the description of the data. You can get the description of an element (if available) by moving the mouse cursor over the corresponding tree element. The description will be displayed in the pop-up hint.

MIB databases may be generic or specific for a particular vendor, model, and device class. Essential NetTools is distributed with the basic MIB set, which is sufficient for the majority of the devices. You can always obtain specific databases from the public web site http://www.mibdepot.com/. Save them in the application folder (by default C:\Program Files\EssNetTools3\SNMP\MIB) and restart the program. Please note that you are still able retrieve the data without any limitations even if you do not have the right MIB database for the device. MIB databases only provide human-readable descriptions of the retrieved data and its purpose.

SysFiles

You can use this tool for editing for the five important system files: services, protocol, networks, hosts, and lmhosts. When the program is started, this tool reads records from these files as shown below:



Service	Port / Protocol	Alias	Comment
activesync	1034/tcp		ActiveSync Notifications
afpovertcp	548/tcp		AFP over TCP
afpovertcp	548/udp		AFP over TCP
auth	113/tcp	ident	Identification Pro
bgp	179/tcp		Border Gateway I
biff	512/udp	comsat	
bootpc	68/udp	dhcpc	Bootstrap Protocol Client
bootps	67/udp	dhcps	Bootstrap Protocol Server
chargen	19/tcp	ttytst	Character generator
chargen	19/udp	ttytst	Character generator
cifs	3020/tcp		
cifs	3020/udp		
close-combat	1944/tcp		
close-combat	1944/udp		

File: C:\Windows\system32\drivers\etc\services

Service: auth

Alias: ident

Port / Protocol: 113/tcp

Comment: Identification Protocol

SysFiles: 275 record(s)

This tool is intended for computer professionals, so please don't edit these files unless you know exactly what you are doing.

Right-clicking on the window brings up a menu with the following commands:

Delete Selected – removes the selected record(s).
Delete All – removes all records.

Options

You can use the **Settings** => **Options** dialog to configure the program's advanced options.

Tools

NetStat

Show full process path – check this box if you want NetStat to display the full path to the process owning the port (e.g. "C:\Files\Program.exe" is a full path, whereas "Program.exe" is a short path).

Convert port numbers to service names – check this box if you want NetStat to display service names rather than numbers. For example, if this box is checked, port 21 is shown as ftp, and port 23 as telnet. The program converts numeric values to service names using the SERVICES file installed by Windows. You can edit this file using the SysFiles tool.

Disable DNS resolving – check this box if you do not want the program to perform reverse DNS lookups of the IP addresses. If you check it, the Hostname column in NetStat will be blank.

NBScan and PortScan

Exclude subnet boundaries – check this box if you want the program to skip IP addresses ending with .0 and .255.

Clear the list on new query – check this box if you want the program to clear the NBScan or PortScan list every time you start scanning a new range of IP addresses. If this box is not checked, the program will preserve the results of all previous scans and auto-sort new items by IP address.

Auto-refresh intervals - Sets the auto-refresh intervals for NetStat and ProcMon if auto-refreshing is on. For ProcMon it is also possible to specify the auto-refresh interval for gathering CPU utilization statistics.

Interface

Sound Alerts

NetAudit security flaw detection, **External connection detection** - check these boxes to accompany some of the program events with sound alerts. To change the default sound files, click on the Browse button next to the event description and locate a new sound file in the .WAV format. To test the file, click on the button with a speaker icon.

Visual Effects

Alternate list colors – check this box to have the program display the file list in the two-color mode. Click on Color 1 and Color 2 to customize the line colors in the two-color mode.

New NetStat item color – use this box to customize the color used to temporarily highlight new entries in the NetStat window.

Removed NetStat item color – use this box to customize the color used to highlight the entries that are about to be removed from the list in the NetStat window.

Mouse hot-tracking – when this box is checked, there is a visual feedback when the mouse passes over list items, and you can select items by pausing the mouse.

Flat scroll bars – makes the scroll bars of all tables in the program look flat (not available under Windows XP/Vista).

Geolocation

Geolocation is IP-to-country mapping for IP addresses. When this functionality is enabled, Essential NetTools checks the internal database to provide information on the country any IP address belongs to. You can configure the program to show **ISO country code**, **Country name**, or **Country flag** next to any IP address. You can also disable geolocation. For some IP addresses, such as reserved ones (e.g. 192.168.*.* or 10.*.*.*) no information on the country can be provided. In such cases, the country name is not shown, or if you use the **Country flag** option, a flag with a question mark is displayed.

As IP allocation is constantly changing, it is important that you always have an up-to-date version of Essential NetTools. A fresh, up- to-date database is included in every Essential NetTools build. A fresh database has 98% accuracy. Without updates, the accuracy percentage falls by approximately 15% every year.

Miscellaneous

Run on Windows startup – if this box is checked, the program is automatically launched every time you start Windows.

Minimize to tray when main window is closed – if the box is checked, the program does not close when you click on the "x" mark the top right corner of the window. Rather, it is minimized to the system tray. To close the program, use the **File** => **Exit** menu command.

Hide from taskbar on minimization – check this box if you do not want to see the program's button on the Windows taskbar when you minimize the program. If this box is checked, use the program's system tray icon to restore the program after minimizing.

Move focus to input box when switching tools – check this box if you want the program to automatically move focus to the input boxes, such as IP address fields, every time you switch from one tool to another.

Auto-complete IP address fields – if this box is checked, the program automatically completes the **Ending IP address** field in

NBScan, PortScan, and NetAudit when you fill out the **Starting IP address** field.

Custom ping/traceroute message – allows you to change the default string contained in ping and traceroute packets. To use this feature, check this box and type your own message in the textbox below.

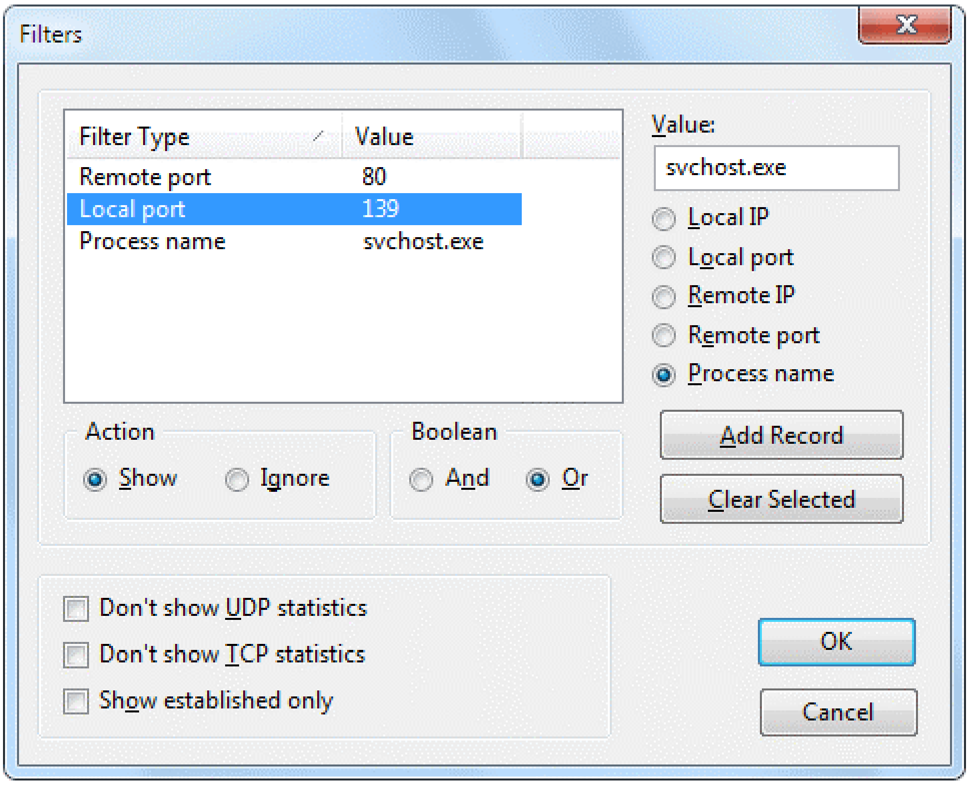
Enable automatic updates – if this box is checked, the program will automatically look for the updates at the TamoSoft web site.

Interval between checks, days – allows you to specify how often the program will check for updates.

Check Now – makes the program check for updates immediately.

Filters

This dialog allows you to configure the filters used for displaying the information in the NetStat window. By default, NetStat lists all of your computer's network connections. This list is usually rather long, and you may want to filter out some of the items that are unimportant to you.



Filters

Filter Type	Value
Remote port	80
Local port	139
Process name	svchost.exe

Value: svchost.exe

○ Local IP
○ Local port
○ Remote IP
○ Remote port
● Process name

Action: ● Show ○ Ignore

Boolean: ○ And ● Or

□ Don't show UDP statistics
□ Don't show TCP statistics
□ Show established only

To create a new filter, enter the **Value**, select the filter type (**Local IP**, **Local Port**, etc.), and click **Add Record**. To remove a filter, select it from the list and click **Clear Selected**. Once you have created one or several new filters, you should select the **Action**. If you select **Show**, NetStat will display only the connections that match the filter(s). If you select **Ignore**, NetStat will not display any connection that matches the filter(s). If you have created multiple filters, you should also choose **Boolean** logic to be used: it can be either **And** (Filter 1 and Filter 2 and Filter 3, etc.) or **Or** (Filter 1 or Filter 2 or Filter 3, etc.). The screen shot above illustrates a rule set that makes NetStat hide the connections where the remote port is 80, or local port is 139, or process name is svchost.exe.

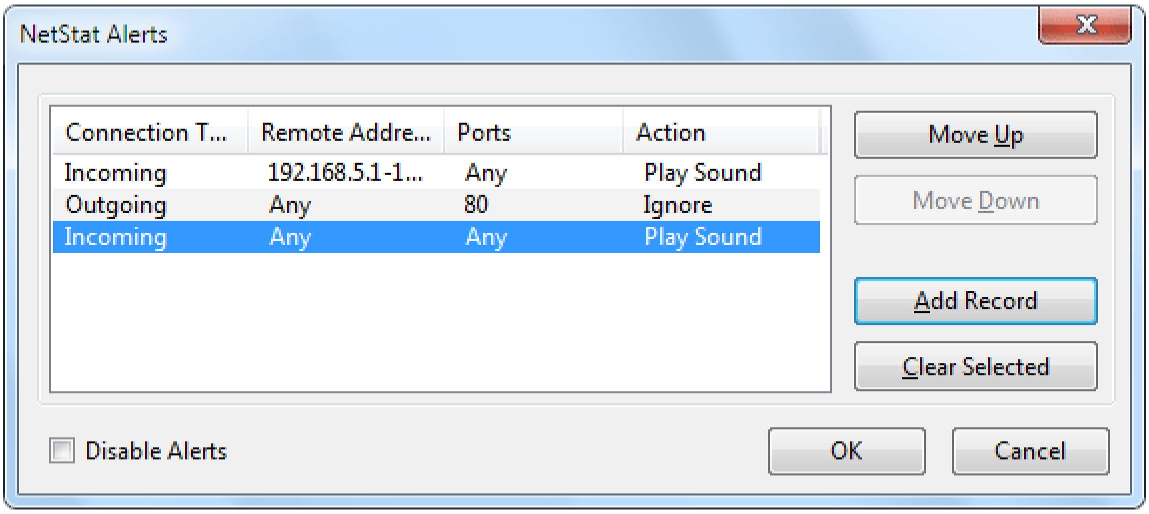
Additionally, you can use the following basic filters:

Don't show UDP statistics – check this box if you don't want to have UDP connections listed in the NetStat window.
Don't show TCP statistics – check this box if you don't want to have TCP connections listed in the NetStat window.
Show established only – check this box if you want the NetStat window to list established connections only. All other connections (listening, closing, etc.) will not be listed.

You can temporarily disable filters by selecting the **Disable Filters** command in the NetStat context menu.

Alerts

This dialog window allows you to configure the alert list (Alerts) for various types of incoming and outgoing connections.



NetStat Alerts

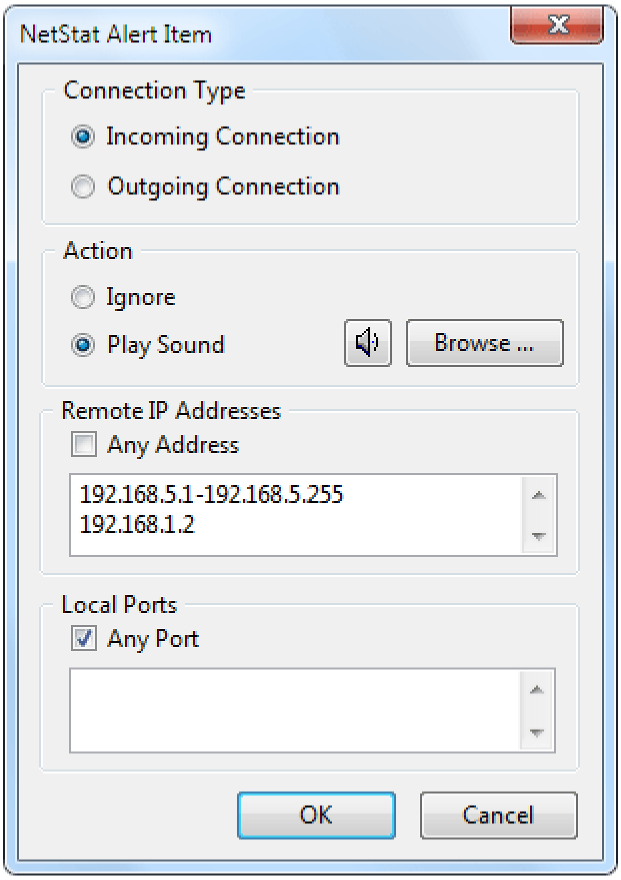
Connection T...	Remote Addre...	Ports	Action
Incoming	192.168.5.1-1...	Any	Play Sound
Outgoing	Any	80	Ignore
Incoming	Any	Any	Play Sound

□ Disable Alerts

The following alerts types are available:

- Incoming connection from a specified IP address or range of IP addresses.
- Incoming connection to a specified local port or range of local ports.
- Outgoing connection to a specified IP address or range of IP addresses.
- Outgoing connection to a specified remote port or range of remote ports.

In order to create a new alert, click on the **Add Record** button.



NetStat Alert Item

Connection Type

● Incoming Connection

○ Outgoing Connection

Action

○ Ignore

● Play Sound

Remote IP Addresses

□ Any Address

192.168.5.1-192.168.5.255
192.168.1.2

Local Ports

☑ Any Port

Connection Type – choose the connection type: incoming or outgoing.

Action – choose the action that will take place once the alert is triggered: **Play Sound** – play the sound file. Choosing the **Ignore** option will make the program exclude a certain type of connection from the alert list. For example, if you would like to monitor all incoming connections but to the local port 80, you can define an alert where the connection type is Incoming and the local port number is 80, and choose the **Ignore** action for it. Please note, that the alert function is looking for the first occurrence of a connection matching the specified alert; therefore, the excluded alert must be the first in the list of alerts, otherwise it will not be read by the program and all connections to port 80 will still trigger the alarm.

Remote IP Addresses – one or several IP addresses, or the range of addresses, a connection from which will trigger an alert. If the **Any Address** box is checked, then any connection will trigger an alert.

Local Ports, **Remote Ports** – one or several local or remote ports, or a range of ports can be specified. If the box **Any Port** is checked, then any local or remote port, depending on the connection type, indicated in Connection Type will trigger the alert.

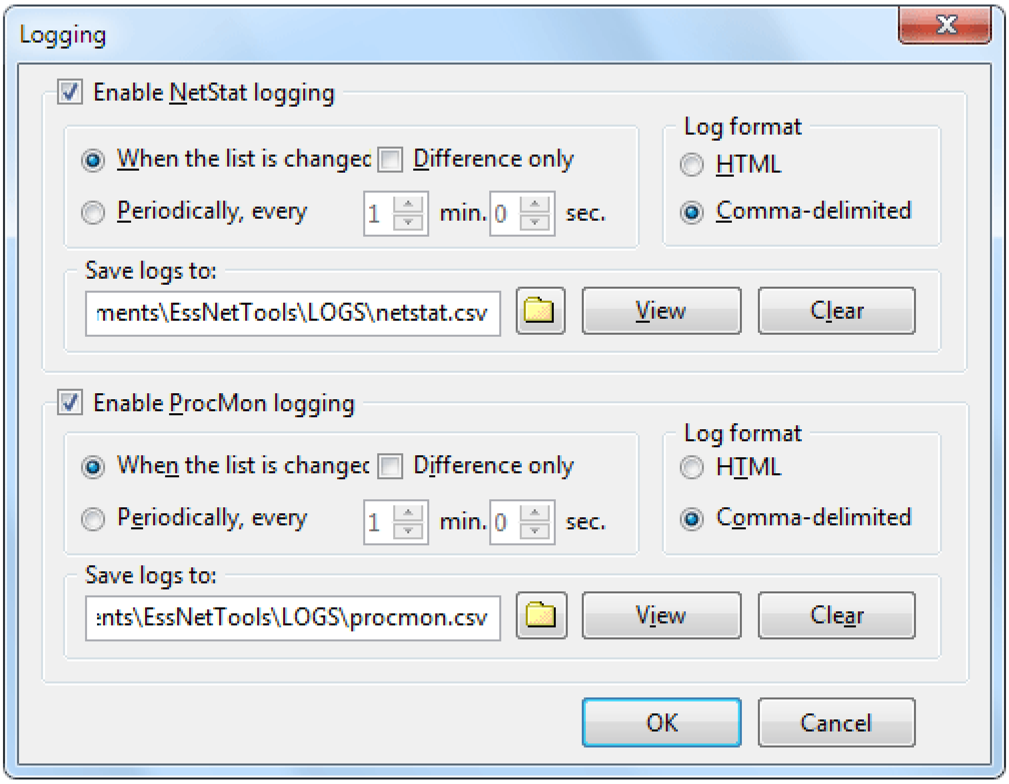
After the alert is created you can edit it by double-clicking on it in the list of alerts. You can change the order in which the alerts are read by the program using the **Move Up** and **Move Down** buttons. You can delete an alert by clicking on the **Clear Selected** button.

The alerts are read in the descending order. The search is finished with the first match; all remaining alerts are not evaluated.

Check the **Disable Alerts** box in the Alerts window to temporarily disable all alerts.

Logging

This dialog allows you to enable and configure logging for NetStat and ProcMon.



Logging

☑ Enable NetStat logging

● When the list is changec ☐ Difference only

○ Periodically, every 1 min. 0 sec.

Log format

○ HTML

● Comma-delimited

Save logs to: ments\EssNetTools\LOGS\netstat.csv

☑ Enable ProcMon logging

● When the list is changec ☐ Difference only

○ Periodically, every 1 min. 0 sec.

Log format

○ HTML

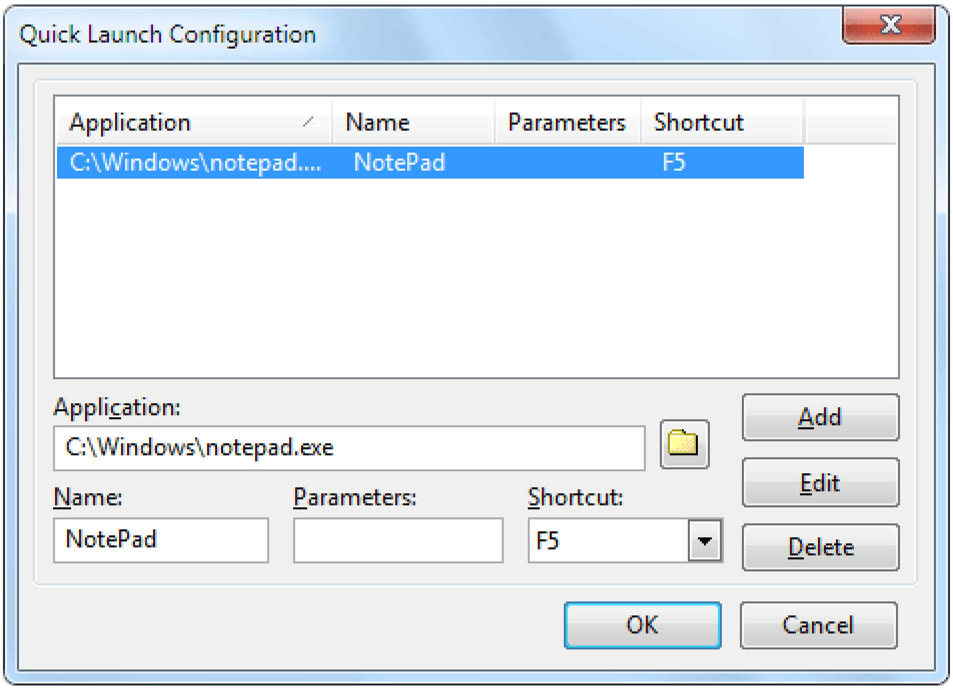
● Comma-delimited

Save logs to: :nts\EssNetTools\LOGS\procmon.csv

You can either have the program save the current NetStat or ProcMon list **When the list is changed**, or **Periodically**, at user-defined intervals. If you want to minimize the log size, you may want to check the **Difference only** box, which will make the program log only those entries that have been added or deleted since the last time the list was changed. You can also select the output format, **HTML** or **Comma-delimited**, and specify the file name and path to save logs to.

Quick Launch

You can use this dialog to add new items to the **File => Quick Launch** menu. By adding new items to the menu, you can use the program as a convenient "launch pad" for other applications.



Application	Name	Parameters	Shortcut
C:\Windows\notepad....	NotePad		F5

Application: C:\Windows\notepad.exe

Name: NotePad

Parameters:

Shortcut: F5

To add a new item, enter the path to the application file in the **Application** field and an arbitrary name in the **Name** field. The **Name** field will be used in the **File => Quick Launch** menu. You can also optionally use **Parameters** that will be passed to the application file, and assign a shortcut to the item, so that you could launch your application with a single click. Once you've entered this information, click **Add** and close this dialog. A new item will be added to the **File => Quick Launch** menu.

The **Application** field does not necessarily have to contain a file name. You can also enter the path to a non-executable file, as long as this file is associated with an application, e.g. an MS Word file. URLs such as "http://www.yahoo.com" are also acceptable (this would launch your web browser and point to the Yahoo web site).

System Summary

This dialog displays very detailed information about your computer, e.g. CPU features, installed software, memory utilization, etc. To save a report in XML format, click **Report**. Please note that since almost all of the technical terms in the System Summary window cannot be translated from English without losing their meaning, this window will display information in English only, even if you use a different language for the program interface.

Reference

NetBIOS Table

Below is the interpretation of NetBIOS name tables used by computers running Windows.

Name	Hex Suffix	Type	Description
<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

Frequently Asked Questions

In this chapter you can find answers to some of the most frequently asked questions. The latest FAQ is always available at http://www.tamos.com/products/nettools/faq.php.

Q. My firewall software warns me that Essential NetTools is "attempting to access the Internet." I am aware that some sites are able to track users by collecting the information sent by their programs via the Internet. Why does Essential NetTools "attempt to access the Internet"?

A. What alerts your firewall is the attempt to resolve IP addresses to hostnames, which is necessary for showing the hostnames in the NetStat tool. Since Essential NetTools has to contact your DNS servers to make a DNS query, it inevitably triggers the alarm. You can disable this feature (**Settings** => **Options** => **Disable DNS resolving**), but in this case the NetStat table will not be able to show you the hostnames.

Q. I try to use NBScan to check my own IP address, but I cannot see my computer's name table.

A. This most probably means that your computer either doesn't offer resource sharing or it has Winsock version 1 originally shipped with Windows 95. In the latter case, consider using nbtstat -A xxx.xxx.xxx.xxx instead, or upgrading to Winsock version 2. This limitation doesn't apply to viewing other computers' name tables (Winsock 1 works just as good as Winsock 2), nor to NetAudit (you can audit your own computer with it).

Q. I check the address xxx.xxx.xxx.xxx by NBScan and get no results, but nbtstat gives me the name table.

A. Two possible reasons. You either set a very short timeout and the response to the query couldn't reach your computer in time, or you are not using the Advanced Mode. In Advanced Mode, the program lists 100% of the computers nbtstat can potentially list. Please read the Advanced Mode paragraph in the NBScan chapter.

Q. I check the address xxx.xxx.xxx.xxx by both NBScan and nbtstat and get no results. The person to whose computer this address is assigned checks the same address (his own) and gets his own computer's name table. Why can he see it and I can't?

A. There is a firewall or some other packet-filtering device between his computer and your computer. Certain packets may be rejected because of the firewall settings. Also, some Internet Service Providers filter packets without informing their customers. If that is the case, you may want to audit the network from a different account.

Q. When I try to mount a share, I receive the "The network is not present or not started" error, but I am connected!

A. You are probably using Dial-Up Networking and you forgot to check "Log on to network" box in the connection properties.

Q. When I try to mount a share, I receive the "Shared Resource Not Found" error, but I know I typed the correct path to the remote share.

A. Make sure that the computer name is present in the lmhosts file and that it is a unique name in the file. There should not be 2 or more computers with the same name in the lmhosts file. You can check whether your computer is capable of "understanding" the name by typing ping computername in the DOS prompt. If the computer is successfully pinged, you can use Essential NetTools to connect to it.

Q. When I select the Open Computer command or try to mount a share, the program displays an hourglass and nothing happens for some time.

A. Well, be patient :-) Usually it takes several seconds to establish a connection.

Contact Us

Questions? Comments? Suggestions? Bug reports? Don't hesitate to contact us.

http://www.tamos.com/

If you have a question that is not answered in this manual, please take a minute to check our Frequently Asked Questions page before contacting technical support. There is a good chance that you will find the answer there. When describing your problem, please be as specific as possible. A detailed description of the problem will help us solve it much faster. Please don't forget to mention the OS version, the program version and build (**Help** => **About**), and all other details that you think may be relevant.