Essential NetTools

User Manual

Introduction

About Essential NetTools

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

- **NetStat:** displays the 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. (This feature is available under Windows NT/2000/XP.)
- **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.
- **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.
- **Shares:** monitors and logs external connections to your computer's shared resources, as well as provides a quick and easy way to connect to remote resources that gives Windows 98/Me users NT user-level connectivity features. Unlike Windows NT, Windows 98/Me has no user-level connectivity after the boot: you can specify a password, but not a username. This tool allows you to set both a username and a password.
- **LMHosts:** a convenient editor of the lmhosts file integrated with NBScan.
- **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.
- **RawTCP:** provides you with the ability to establish low-level TCP connections to troubleshoot different networking services. Multi-color output and a convenient interface make it a great tool for every network administrator or computer programmer. TraceRoute and Ping: these familiar utilities featuring customizable options and a convenient results presentation allow you to explore the Internet and troubleshoot connectivity problems.
- **NSLookup:** allows you to convert IP addresses to hostnames and vice versa, obtain aliases, and perform advanced DNS queries, such as MX or CNAME.
- **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 identify hidden applications, kill running processes, and manage the usage of your PC's resources more effectively.

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

What's New

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.

Version 2.2

- You can now scan Class B networks with NBScan (registered version only).

Version 2.1

- NBScan now lists MAC addresses.
- With NBScan you can scan multiple LAN segments preserving the previous scans' results.
- CSV (comma-delimited) format is available when saving NBScan reports.
- LMHosts allows you to specify a #DOM tag.
- A new TCP Raw Connect tool has been added.
- The interface font can be customized.
- A few bugs fixed in NBScan.

Version 2.02

- You can now add the whole NBScan list to the lmhosts file with one mouse click.
- When you use the DNS tool to resolve a hostname, you can send the obtained IP address to NBScan or NetAudit using the context menu.
- Computer names containing spaces and special characters are now added to the lmhosts file in the correct format.
- Multiple record selection is allowed when working with the lmhosts file.

Version 2.01

- This version fixes a few bugs in HTML report generation found in the previous version of the program.

Version 2.0

Essential NetTools version 2.0 has undergone a major re-design and introduces the following new features and enhancements:

- The source code was re-written from scratch. The new version is much more compact and works faster.
- New NetStat tool that displays TCP and UDP connection information.
- New Watch tool that monitors external connections to your computer.
- New convenient LMHosts editor.
- Now opens remote computers with one mouse click.
- HTML report generation for NetAudit.
- Many other new nice features.

License Agreement

Please read the following terms and conditions carefully before using this software. Your use of this software indicates your acceptance of this license agreement. If you do not agree with the terms of this license, you must remove this software from your storage devices and cease to use the product.

Copyright
This software is copyright 1998-2002; TamoSoft, Inc. Essential NetTools is a trademark of TamoSoft, Inc. The use and copyright of this software is governed by international copyright treaties. TamoSoft, Inc. retains full title and rights to this software and documentation, and in no way does the license granted diminish the intellectual property rights of TamoSoft, Inc. You must not redistribute the registration codes provided, either on paper, electronically, or in any other form.

Evaluation Version
This is not free software. You are hereby licensed to use this software for evaluation purposes without charge for a period of 30 days. Using this software after the evaluation period violates copyright laws and may result in severe civil and criminal penalties.

Registered Version
One registered copy of this software may be used by a single person who uses the software personally on one or more computers, or it may be installed on a single workstation used non- simultaneously by more than one person, but not both.

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

Governing Law
This Agreement will be governed by the laws of the Republic of Cyprus.

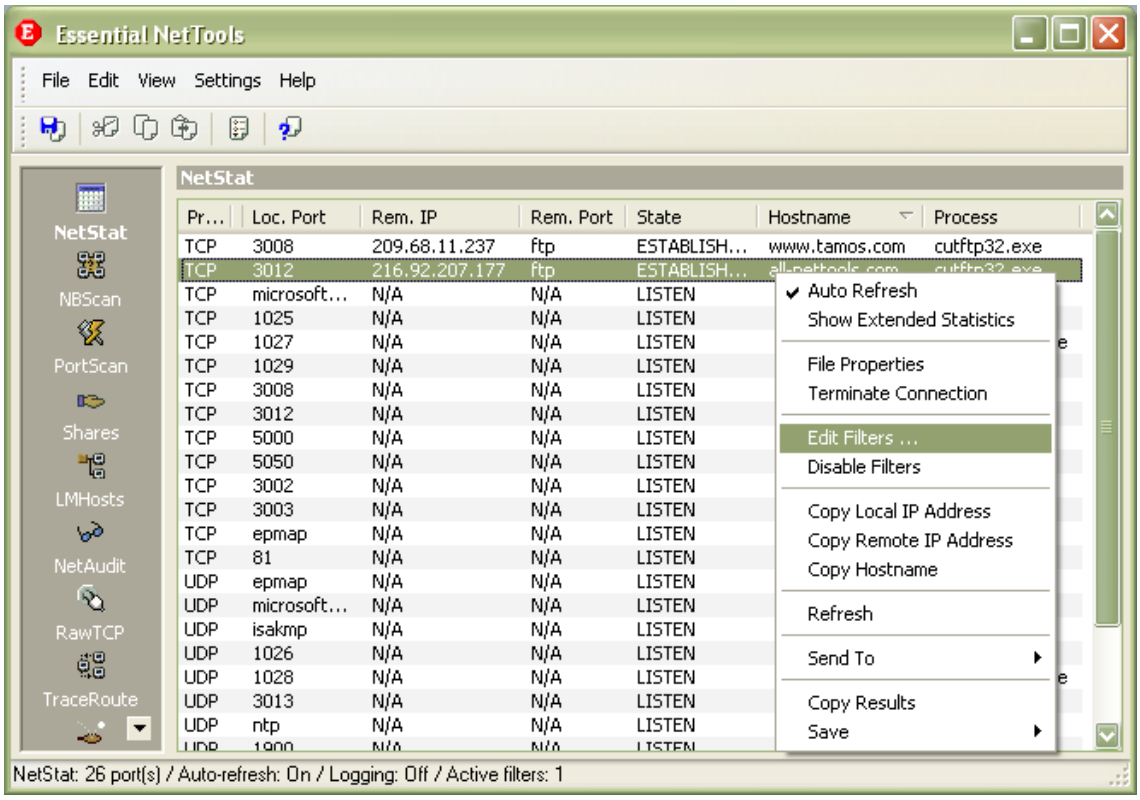
Distribution
This software may be distributed freely in its original unmodified and unregistered form. The distribution has to include all files of its original distribution. Distributors may not charge any money for it. Anyone distributing this software for any kind of remuneration must first contact us for authorization.

Other Restrictions
You may not modify, reverse engineer, decompile or disassemble this software in any way, including changing or removing any messages or windows.

Using the Program

Interface Overview

The program's main window consists of the 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.



Main Menu

File
Save Report – saves the output of the current tool into to a file.
Quick Launch – launches other network-related tools by TamoSoft, if they are installed on your system.
Logging – opens the Logging dialog.
Exit – closes the program.

Edit
Cut, Copy, Paste – performs the standard text commands.

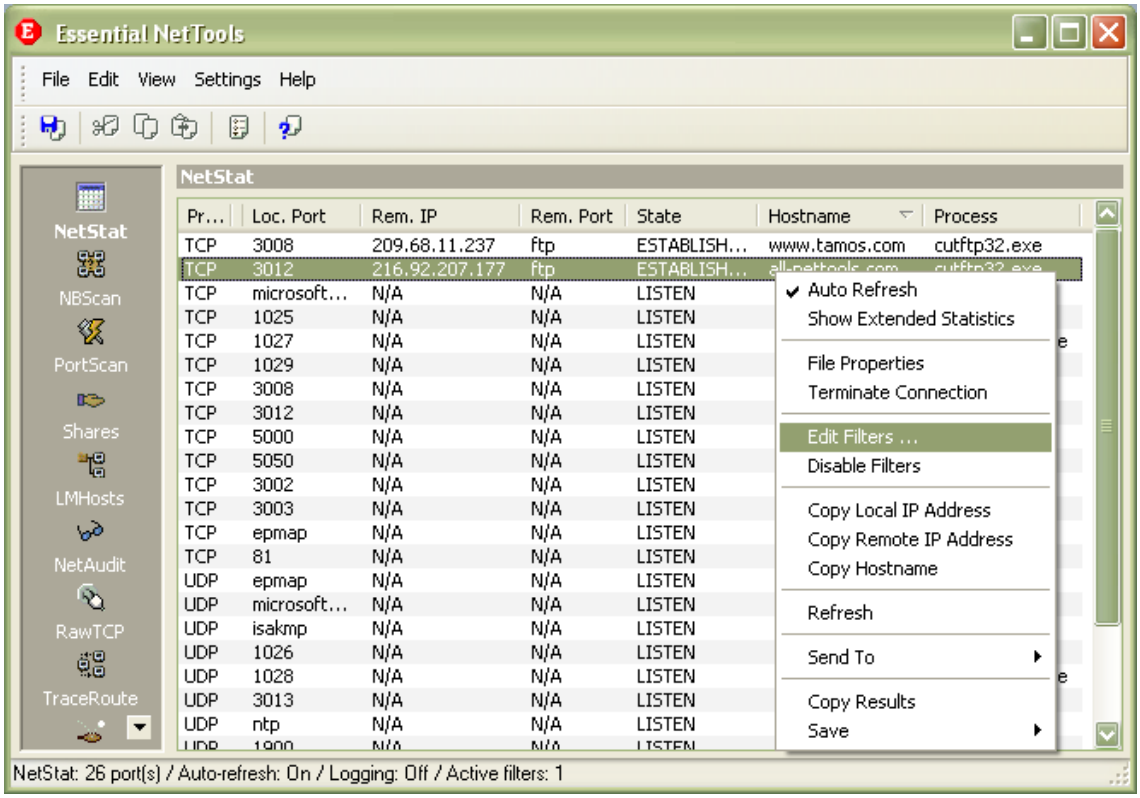
View
Tool Bar – shows/hides the tool bar.
Status Bar – shows/hides the status bar.
Side Bar – shows/hides the side bar.
Local IP Address(es) – displays your computer's IP addresses.
NetStat, NBScan, etc. – allows you to select the tool to work with.

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.
Advanced NBScan Mode – switches on/off the advanced mode in NBScan.

Help
Contents – opens the help file.
Search For Help On – opens the Essential NetTools help index
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. (This feature is available under Windows NT/2000/XP.)



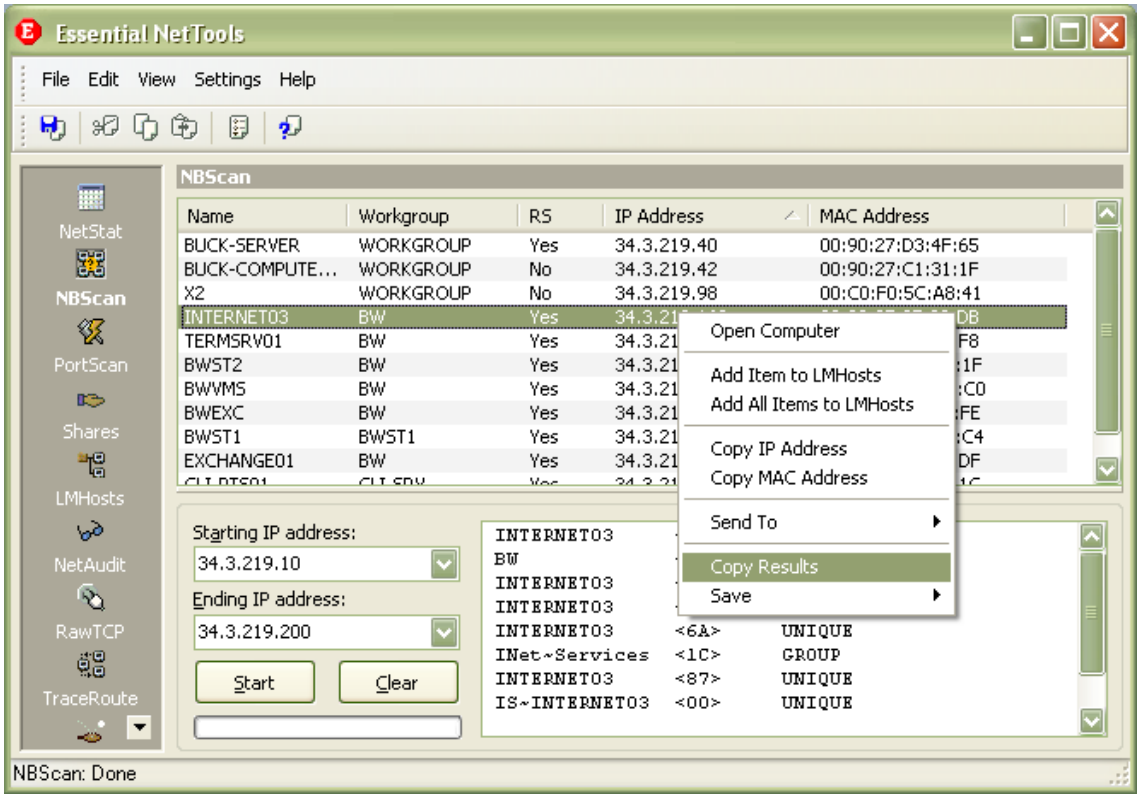
Right-clicking on the window brings up a menu with the following commands:

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 (Windows NT/2000/XP only).
Terminate Connection – closes the selected TCP connection.
Edit Filters – open the Filters dialog.
Disable Filters – enables/disables all currently configured filters.
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 not to display all the connections, convert port numbers to service names, resolve IP addresses to hostnames, etc. See Options for more information.

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.



Before you start scanning, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above. When the range is set, click **Start** to start scanning. The scanning speed can be modified by selecting **Settings** => **Options** in the program menu (see Options for details).

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. Check the #PRE flag on the LMHosts tab before adding if you want the name to be preloaded into the name cache.
Add All Items to LMHosts - adds records associated with the listed computers to the lmhosts file in the appropriate format (computers which have no shared resources are not added). Check the #PRE flag on the LMHosts tab before adding if you want the names to be preloaded into the name cache.
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, click on the program menu and select **Settings** => **Advanced NBScan Mode**. When this mode is on, a bullet is displayed next to the menu item. The advanced mode may not be

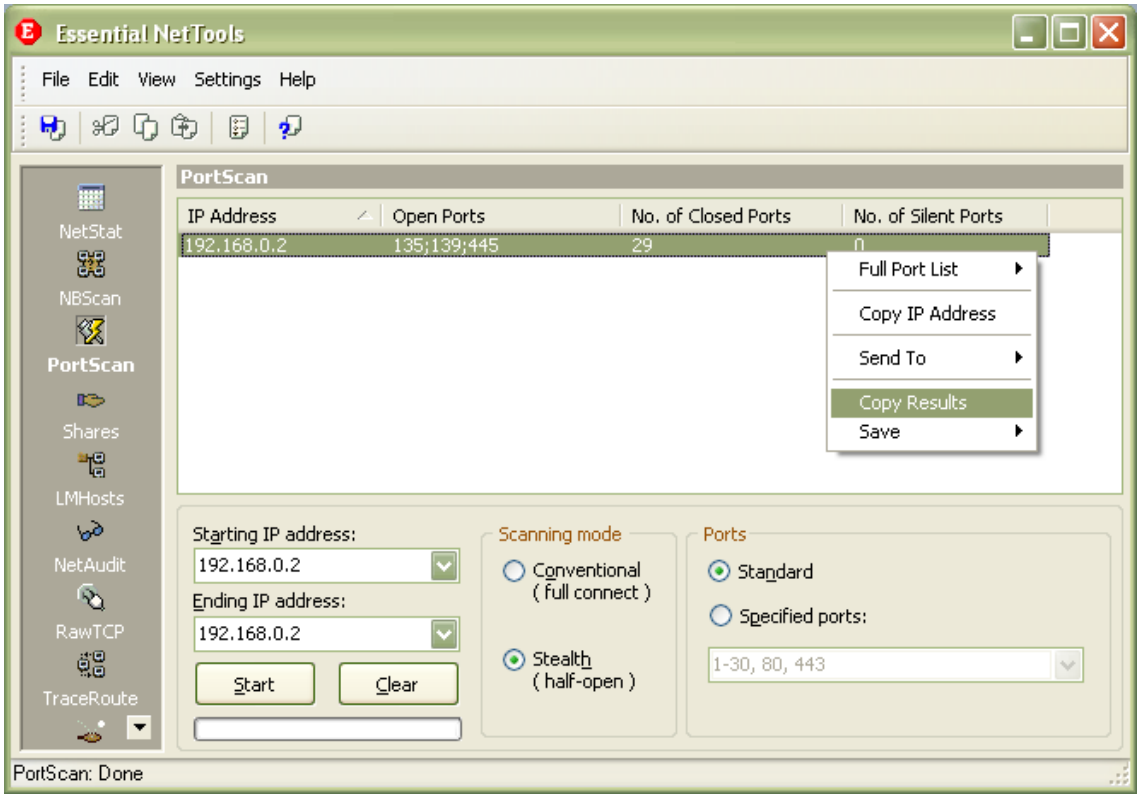
available if the computer has logged on to the network. If the computer has already logged on, this menu item is disabled. If you want to use this mode, you should turn it on BEFORE logging on to the network. For example, if you use a dial-up connection to the Internet, you should first launch the program, then check **Advanced NBScan Mode**, 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's quite probable that you will not notice any difference between the results obtained with the advanced mode turned on or off.

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.



Before you start scanning, you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above.

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're scanning. In the stealth mode, the connection is initiated, but not finalized. This scanning technique is also know 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 you 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).

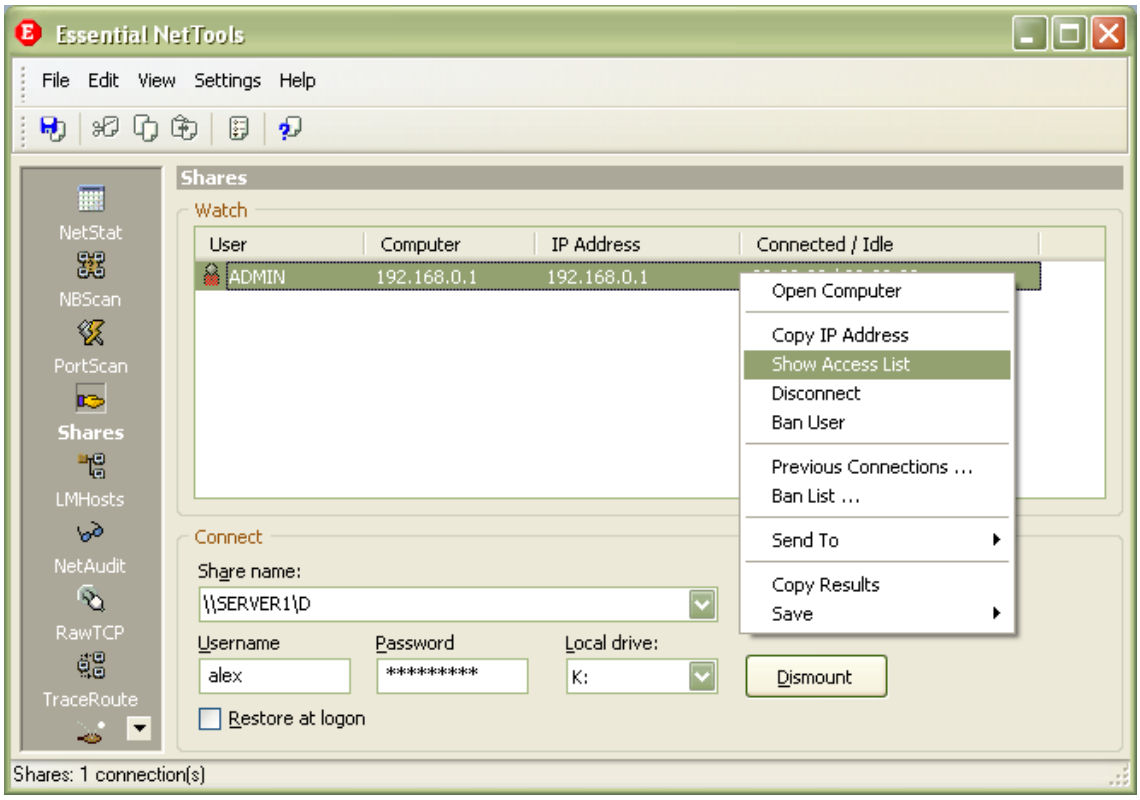
During the scanning process the information about the ports is being added to the list. The **Open Ports** column lists the TCP ports that accepted the connection. The **No. of Closed Ports** column displays the number of ports that rejected connections, while the **No. of Silent Ports** column displays the number of ports that ignored connections attempts. In the conventional mode, the last two columns don't 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.

Shares

The **Shares** tool allows you to perform two tasks: watch connections to your resources and connect to remote resources over the network.



Watch

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.
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.
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.

Connect

You can use this tool for connecting to remote resources over the network. It is convenient for Windows NT/2000/XP users and indispensable for Windows 98/Me users. Unlike Windows NT/2000/XP, Windows 98/Me has no user-level connectivity after the boot: you can specify a password, but not a username. This tool gives Windows 98/Me machines NT user-level connectivity features: You can set both a username and a password. Windows NT/2000/XP users can also use this tool for connecting to remote resources.

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

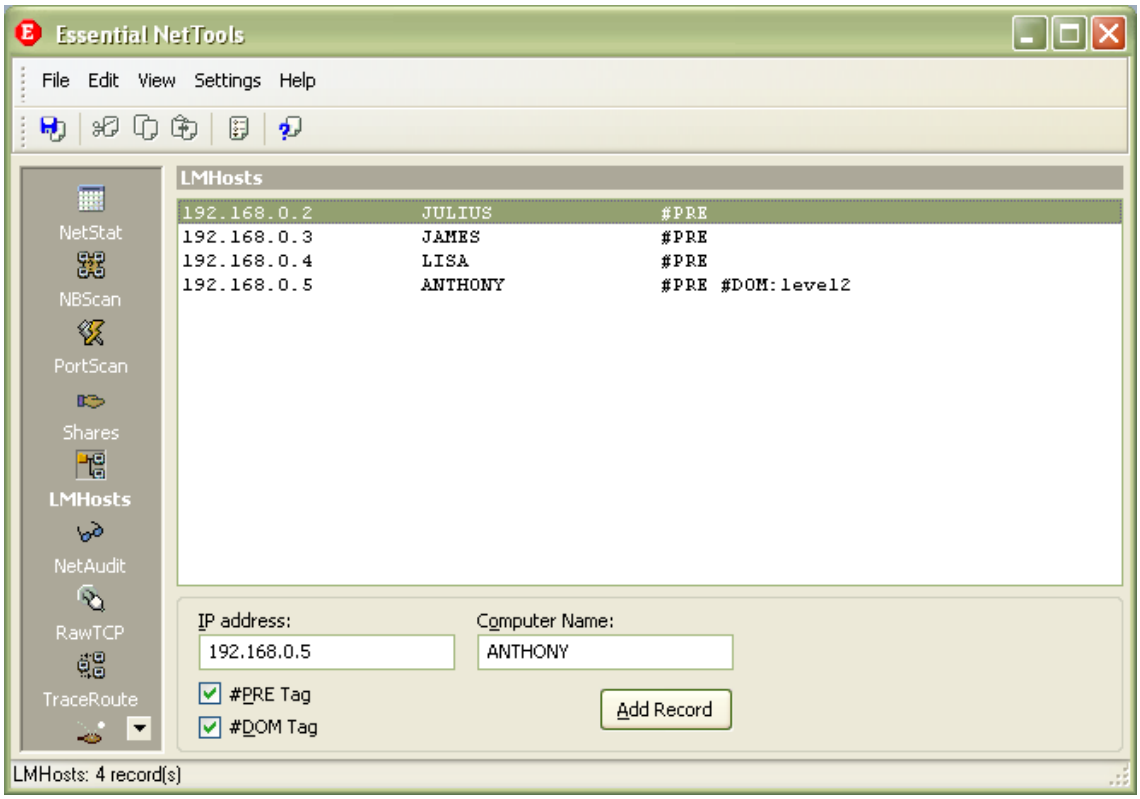
You should also enter a username and a password in the corresponding fields and select a free drive letter from the **Local Drive** drop-down list. Note that your computer should be able to resolve the remote computer name you specified to the corresponding IP address. It usually means that the IP address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

You can also use this tool for mapping remote resources of Windows 95/98/Me computers.

LMHosts

You can use this tool for managing your lmhosts file. When the program is started, this tool lists valid lmhosts records as shown below:



Use the **Add Record** button to add new records to the lmhosts file. If the file does not exist, it will be automatically created. By checking the **#PRE Tag** box, you can make sure that the computer name is preloaded into the name cache. By checking the **#DOM Tag** box, you can associate the entry with a domain; you will be prompted for the domain name. Adding a record also automatically reloads the name cache (corresponds to the nbtstat –R command).

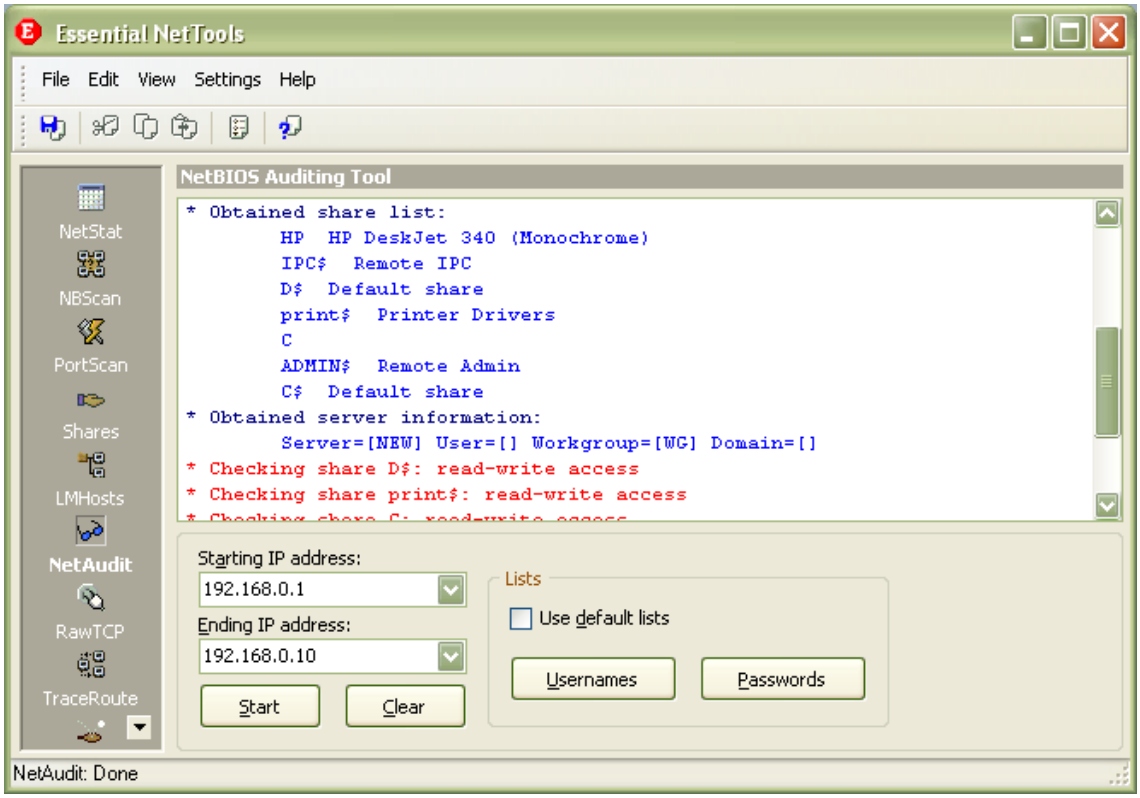
Right-clicking on the window brings up a menu with the following commands:

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

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.



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. If you want the program to use built-in NetAudit lists, you can do so by checking the **Use default lists** box. The evaluation version of the program allows you to use built-in lists only; custom lists can be used only in the registered version.

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.

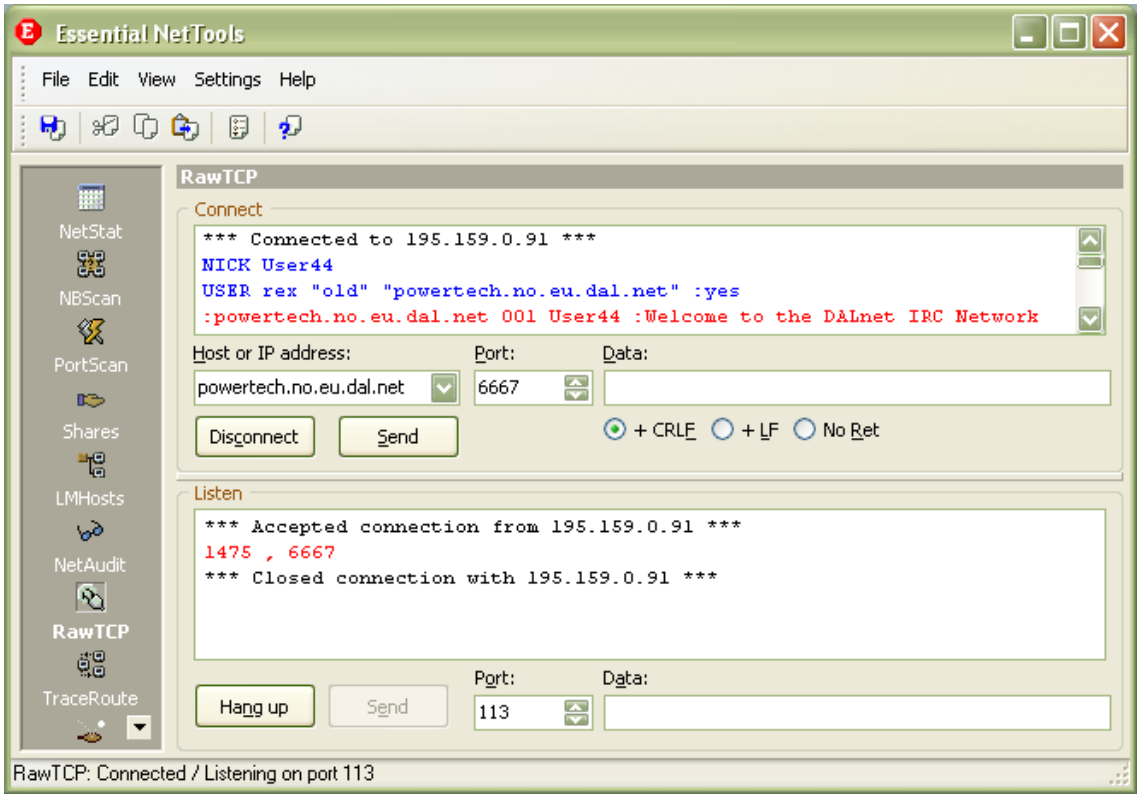
Below is a sample NetAudit output:

```
* Checking 192.168.0.9 ...
* Obtained NetBIOS name table:
        SKY             <00>
        SKY             <20>
        SKYGROUP        <00>
        SKY             <03>
        SKYGROUP        <1E>
        DAN             <03>
```

```
        SKYGROUP         <1D>
        ..__MSBROWSE__.  <01>
* Trying username "ADMINISTRATOR", password "": failed
* Trying username "ADMINISTRATOR", password "ADMINISTRATOR": failed
* Trying username "ADMINISTRATOR", password "GUEST": failed
* Trying username "ADMINISTRATOR", password "ROOT": failed
* Trying username "ADMINISTRATOR", password "ADMIN": failed
* Trying username "ADMINISTRATOR", password "PASSWORD": failed
* Trying username "ADMINISTRATOR", password "TEMP": failed
* Trying username "ADMINISTRATOR", password "SHARE": failed
* Trying username "ADMINISTRATOR", password "WRITE": failed
* Trying username "ADMINISTRATOR", password "FULL": failed
* Trying username "ADMINISTRATOR", password "BOTH": failed
* Trying username "ADMINISTRATOR", password "READ": failed
* Trying username "ADMINISTRATOR", password "FILES": failed
* Trying username "ADMINISTRATOR", password "DEMO": failed
* Trying username "ADMINISTRATOR", password "TEST": failed
* Trying username "ADMINISTRATOR", password "ACCESS": failed
* Trying username "ADMINISTRATOR", password "USER": failed
* Trying username "ADMINISTRATOR", password "BACKUP": failed
* Trying username "ADMINISTRATOR", password "SYSTEM": failed
* Trying username "ADMINISTRATOR", password "SERVER": failed
* Trying username "ADMINISTRATOR", password "LOCAL": failed
* Trying username "GUEST", password "": failed
* Trying username "GUEST", password "ADMINISTRATOR": failed
* Trying username "GUEST", password "GUEST": succeeded
* Obtained share list:
        IPC$              Remote IPC
        E$                Default share
        D$                Default share
        C
        ADMIN$            Remote Admin
        C$                Default share
* Obtained server information:
        Server=[SKY] User=[] Workgroup=[SKYGROUP] Domain=[]
* Checking share E$: access denied
* Checking share D$: access denied
* Checking share C: read-write access
* Checking share ADMIN$: access denied
* Checking share C$: access denied
* Finished checking 192.168.0.9
```

RawTCP

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



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. The data being sent is shown in blue; the data being received is shown in red.

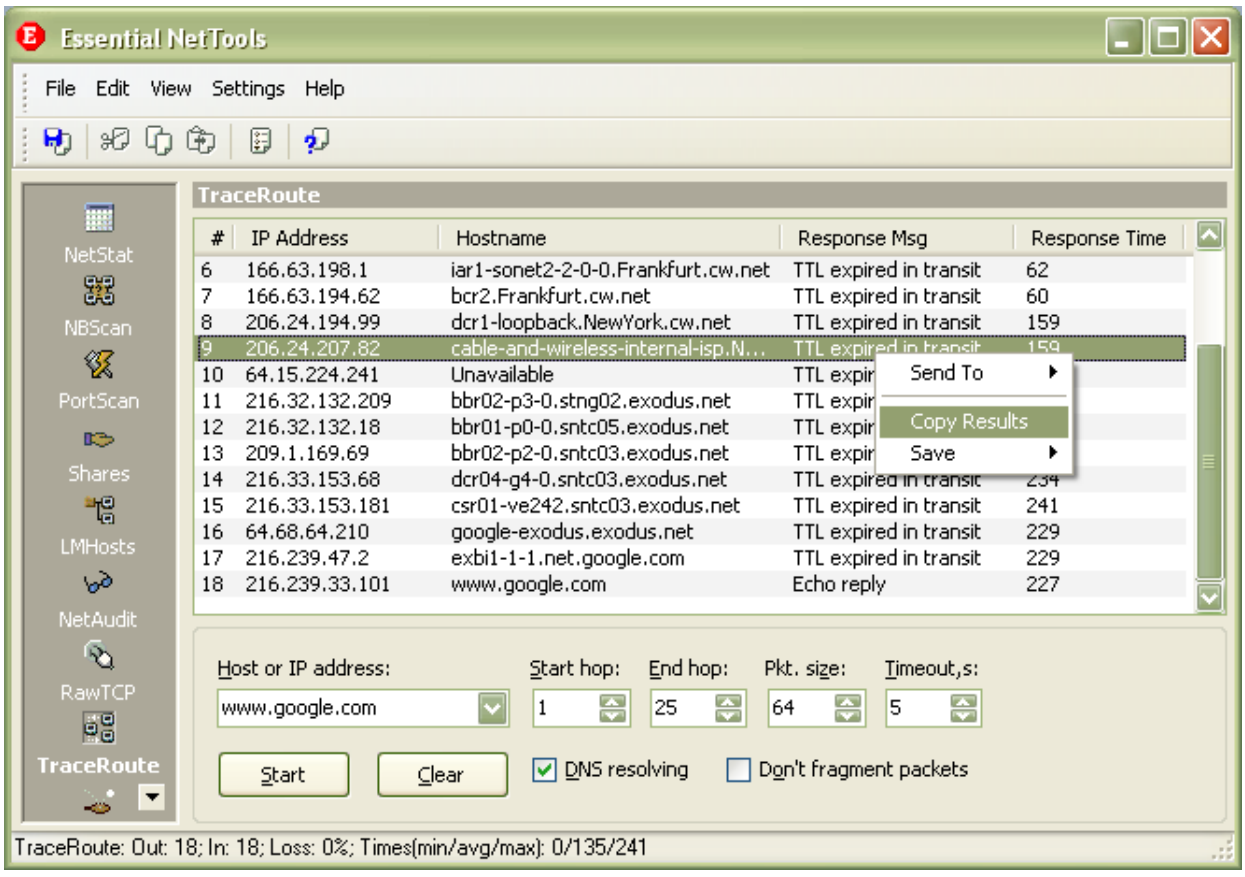
Listen
To listen for incoming connections, select a local port and click **Listen**. If a remote host connects to your PC, the information about such connection will be displayed in the window. If the remote host starts sending data to the open local port, the data being sent will be shown in red. You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

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 both for 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.



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

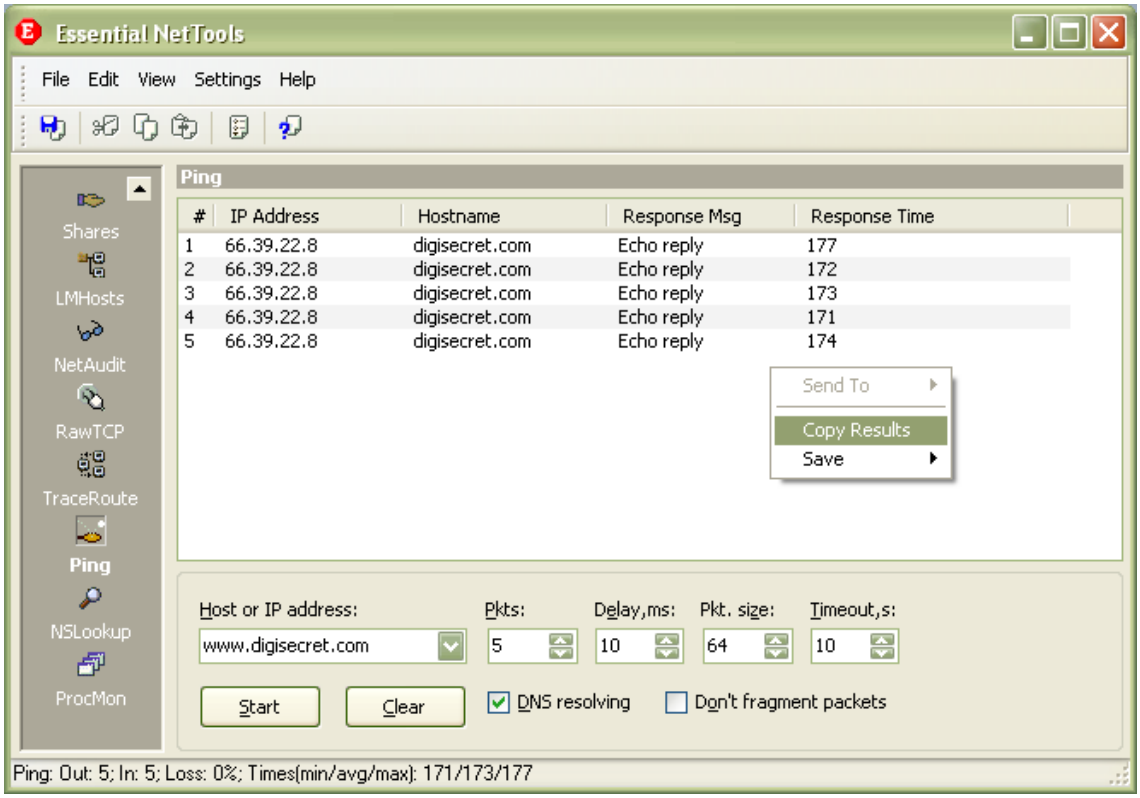
Start hop – allows you to set the hop from which to start tracing. It is often useful to set a value higher than 1 if the first several hops of the route are always the same; by setting a higher value you can save some time.
End hop – allows you to limit the number of hops to trace.
Pkt. size – sets 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 packets – 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.

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 a host computer you are trying to reach is actually operating. If, for example, you can't ping a host, then you will be unable to use the 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.



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 packets – sets the *Don't fragment* flag in the packet.

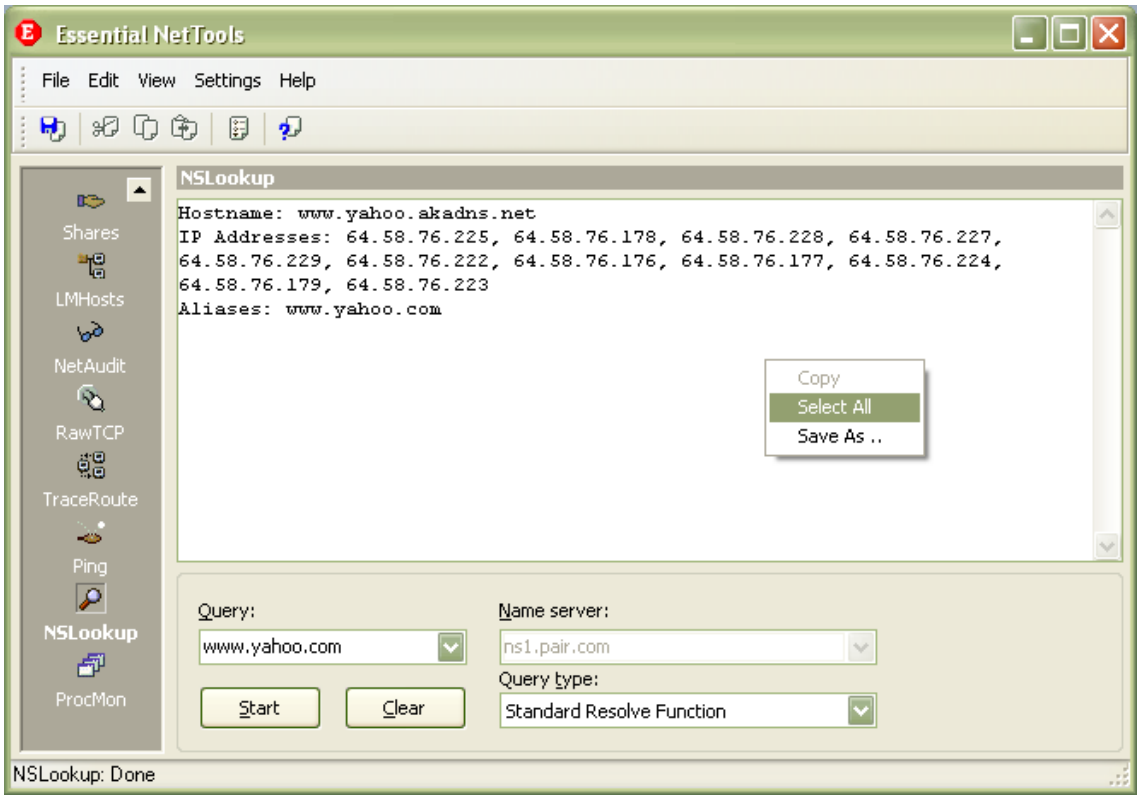
Right-clicking on the window brings up a menu with the following commands:

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

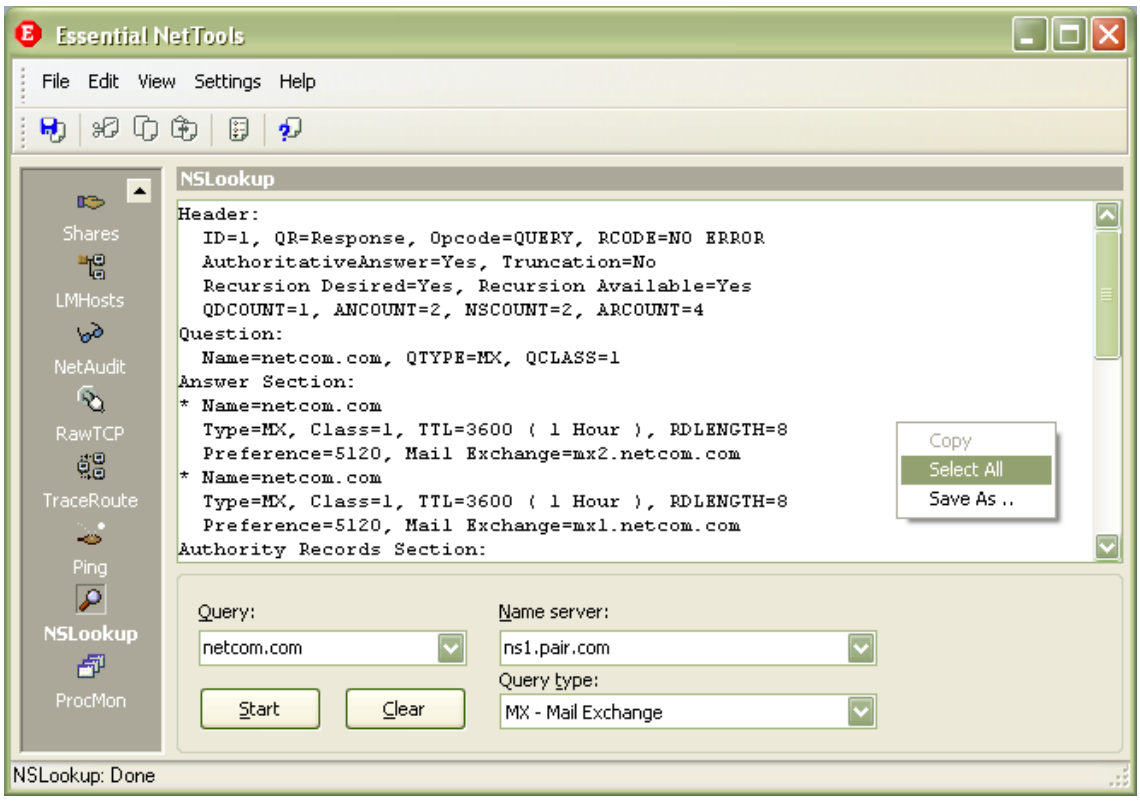
NSLookup

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.



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".



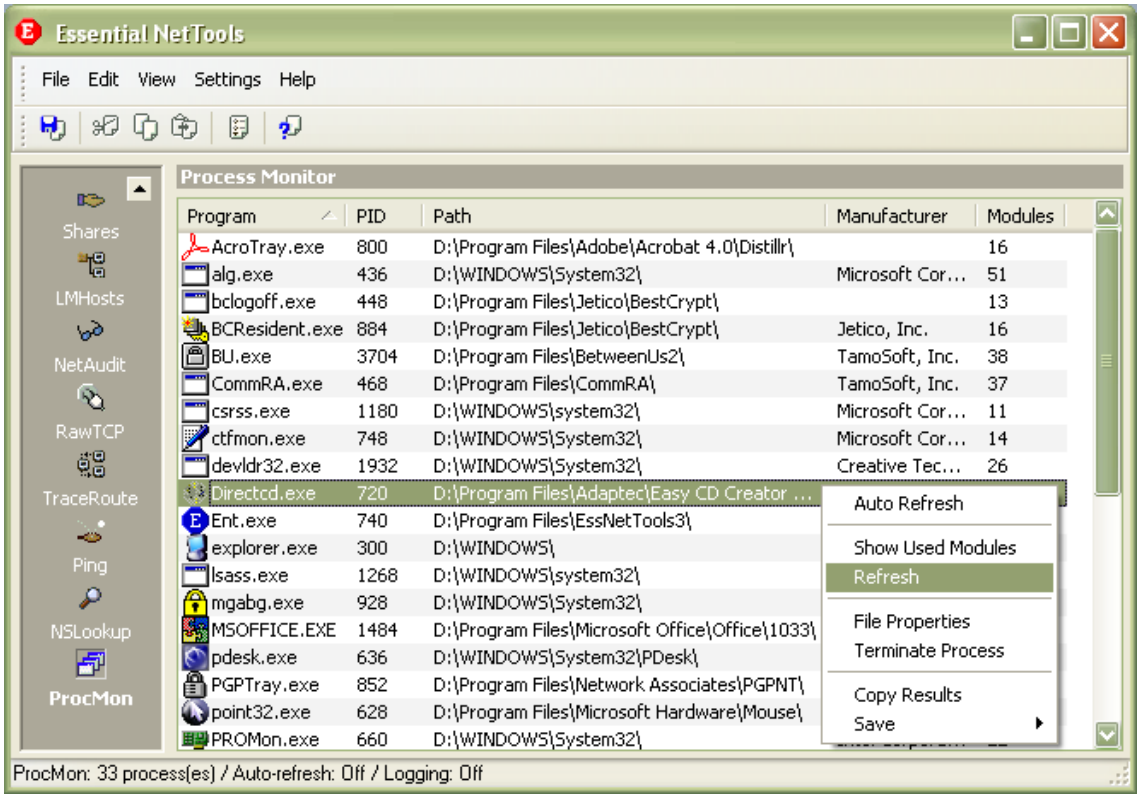
NSLookup offers many query types to choose from, and it takes some understanding of the Internet to perform any queries other than **Standard Resolve Function**. If you are a beginner and want to learn more about various query types, we suggest reading RFC 1034 and RFC 1035, or searching the web for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

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.



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.
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 – save the ProcMon table to a file.

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. Depending on your Windows version, the SERVICES file is located in different folders: in Windows 95/98/Me you can find it in the \Windows folder, and in Windows NT/2000/XP you can find it in the \Winnt\system32\drivers\etc folder. You can manually edit this file if you want to add more ports/service names.

Disable DNS resolving – check this box if you don't 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.

Number of sockets – sets the number of simultaneous queries sent by NBScan and PortScan in one cycle. For example, if the query timeout is set to 5 seconds and the number of sockets is set to 25, the program sends 25 queries, then waits for 5 seconds, then sends another 25 queries and waits for another 5 seconds, and so on. With such settings a Class C network can be scanned by NBScan within approximately 50 seconds. For PortScan, the speed depends on the number of ports you are scanning. The maximum number of sockets is 100.

Query timeout – sets the timeout for NBScan and PortScan queries in seconds. This is the time NBScan and PortScan wait for responses to queries. The default value is 3 seconds, which is normally long enough to receive replies from most of the computers being scanned. However, the response time may vary from network to network and from connection to connection, and it is influenced by many factors; therefore, you can decrease this value if you feel that the connection is fast enough.

Auto-refresh intervals

Sets the auto-refresh intervals for NetStat and ProcMon if auto-refreshing is on.

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.

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).

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 doesn't close when you click on the "x" mark in 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 don't 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.

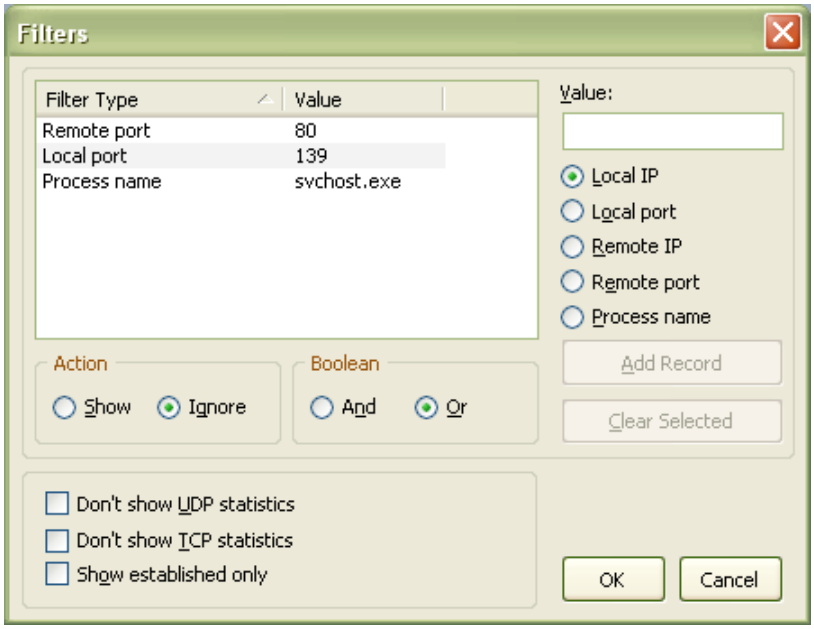
Move focus to input box when switching tools – check this box if you want the program to automatically move focus to the input boxes, such as IP address fields, every time you switch from one tool to another.

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.

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.



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 filter, 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 the **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*. Note that since the process name is available only under Windows NT/2000/XP, the process name filter is not available under Windows 98/Me.

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.

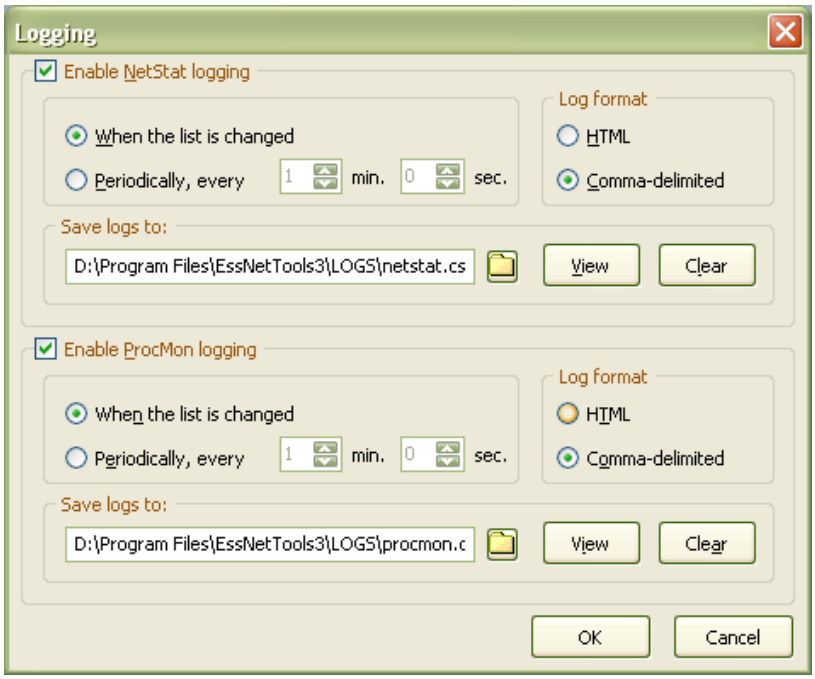
Don't show TCP statistics - check this box if you don't want to have TCP connections listed in the NetStat window.

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.

Logging

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



You can either have the program save the current NetStat or ProcMon list **When the list is changed**, or **Periodically**, at user-defined intervals. You can also select the output format, **HTML** or **Comma-delimited**, and specify the file name and path to save logs to.

Reference

NetBIOS Table

Below is the interpretation of NetBIOS name tables used by computers running Windows NT/2000/XP and Windows 95/98.

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 can't 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 that 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's 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'm 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's 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.

Q. Will there be a German, French, Italian, Dutch, etc. version of Essential NetTools?
A. Currently we don't plan to release any versions with localized interface, but we do plan to provide users with manuals in foreign languages. Want to help? Translate the manual (this help file) shipped with the program into one of these languages and get a license for free. But contact us first please.

Information

How to Purchase Essential NetTools

This program is a 30-day evaluation version. If you would like to continue using it after 30 days, you must purchase it. Below is the pricing for the fully functional unrestricted version of the program:

License	Price, US
1 User License	$29.00

Visit our site for pricing on multi-user licenses.

As a registered customer, you are entitled to:

Free updates that will be released within 1 year from the date of purchase;
Information on updates and new products;
Free technical support.

We accept credit cards orders, orders by phone and fax, checks, and wire transfers. Prices, terms, and conditions are subject to change without notice; please check our web site for the latest product offerings and prices.

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

Contacting Us

Web

http://www.tamos.com

E-mail

sales@tamos.com (Sales-related questions)
support@tamos.com (All other questions)

Mail and Fax

Mailing address:

PO Box 1385
Christchurch 8015
New Zealand

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

Other Products by TamoSoft

CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity capable of capturing and analyzing network packets. It gathers information about data passing through your dial-up connection or Ethernet card and decodes the analyzed data. With CommView you can see the list of network connections and vital IP statistics and examine individual packets. Packets are decoded down to the lowest layer with full analysis of the most widespread protocols. Full access to raw data is also provided in real time. CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

More information

SmartWhois

SmartWhois is a handy utility for obtaining information about any IP address, hostname, or domain in the world. Unlike standard whois utilities, it automatically delivers information associated with an IP address or domain no matter where it is registered geographically. In just a few seconds, you get all you want to know about a user: domain, network name, country, state or province, and city. Even if the IP address cannot be resolved to a hostname, SmartWhois won't fail!

More information

DigiSecret

DigiSecret is an easy-to-use, secure, and powerful application for file encryption and sharing. It utilizes strong and time-proven encryption algorithms for creating encrypted archives, self-extracting EXE files, and sharing files with your associates and friends. DigiSecret also includes powerful and intelligent file compression; you no longer need .zip files when you can have encrypted and compressed DigiSecret files. The program is integrated with the Windows shell, and you can perform operations on files by right-clicking on them. It also fully supports drag-and-drop operations.

More information