

NetResident[®]

Help Documentation

Copyright © 2006-2011 TamoSoft

Introduction

About NetResident

NetResident is an advanced network content monitoring program that captures, stores, analyzes, and reconstructs network events such as e-mail messages, Web pages, downloaded files, instant messages and voice conversations. NetResident uses advanced monitoring technology to capture the required data from the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format.

While NetResident is similar to network analyzers in many respects, it focuses on high-level protocols that are used to transfer content over the Internet or LAN. With NetResident, you don't need a profound understanding of networking technologies, have to use complex packet capturing and analysis software, or dig through network packets in order to reconstruct the actual data; NetResident does all the work for you and presents only the Web pages, e-mails, instant messages, or downloaded files as requested. NetResident is used by network administrators to enforce IT policy, parents to monitor their children's communication on the Internet, and by forensic experts to gain crucial information.

If you are one of the many network professionals who uses TamoSoft's network monitoring solutions, CommView or CommView for WiFi, NetResident will process the log files generated by your packet monitoring program and retrieve e-mail messages, Web pages, and other types of content for quick analysis.

What's New

Version 2.0

- Added file transfer capturing for all supported IMs.
- The latest versions of Live Messenger are supported.
- Added FTP capture filter.
- A few bug fixes.

Version 1.9

- Improved ICQ support.
- Improved HTTP proxy support.
- Improved SOCKS 4 and SOCKS 5 proxy support.
- Added AOL Mail, Mail.ru and Yandex.Pochta support.
- Updated parsers for Gmail, Hotmail and Yahoo! Mail to match the latest changes in these services.
- A few bug fixes.

Version 1.8

- Many updates to protocol parsers that allow the application to correctly handle instant messages and Web-based e-mails by using the latest protocols.
- Support for attachments in outgoing Web-based e-mail messages.
- An updated network driver to improve performance in heavily loaded LAN environments.
- A few other bug fixes and interface improvements.

Version 1.7

- IPv6 support
- Improved application performance when running on multi-core CPU computers
- Added more event notification options
- Added configurable real-time traffic filtering options for HTTP and mail protocols
- Windows 7 support
- Added optional minimization to the system tray area
- Old database records can be archived
- Updated parsers for Gmail and Yahoo! Mail to match the latest changes in these services
- A few bug fixes

Version 1.6

- Support for Web-based mail systems (Gmail, Hotmail, Yahoo! Mail)
- Automatic log file importing
- Improved event management (priority levels and comments)
- Configurable path to the NetResident database
- A few bug fixes

Version 1.5

- The database of events is now searchable
- You can set keyword-based alarms
- Improved database engine performance
- A few bug fixes

Version 1.4

- New and improved high-performance database engine
- Improved VoIP support
- Improved ICQ support
- Optional PromiSwitch tool for monitoring in switched network environments
- New license types: Pro and Lite
- A few bug fixes

Version 1.3

- Improved VoIP support
- Remote connections to NetResident service are now possible
- Additional event details (port numbers and timestamps)
- Windows Vista support
- A few bug fixes

Version 1.2

- Support for IRC (Internet Relay Chat) protocol
- Support for Telnet protocol
- Support for VoIP (Voice over IP)
- Database import and export
- A few bug fixes

Version 1.1

- Support for Yahoo and Jabber instant messaging protocols
- Improved log import that supports many 3rd party capture file formats
- Configurable database size management that can be used to automatically delete old events.
- A few bug fixes

Using the Program

Before You Begin: Network Visibility

The key to successful network monitoring is the visibility of network traffic. If you need to monitor only one computer on the network, there is no network visibility question: You can simply install and run NetResident on that computer. However, if you need to monitor multiple computers on a LAN, it's important that you understand how to achieve network visibility, i.e. the ability to "see" network traffic of other stations from a single observation point.

In brief, to monitor other computers on your LAN, you need to install NetResident on a gateway computer, or use a switch with a "port mirroring" feature, or use a hub. There are many possible network layouts, so if you are new to network monitoring, we recommend that you read the detailed, illustrated white paper by TamoSoft, [Promiscuous Monitoring in Ethernet and Wi-Fi Networks](#) (a [PDF](#) version is also available.)

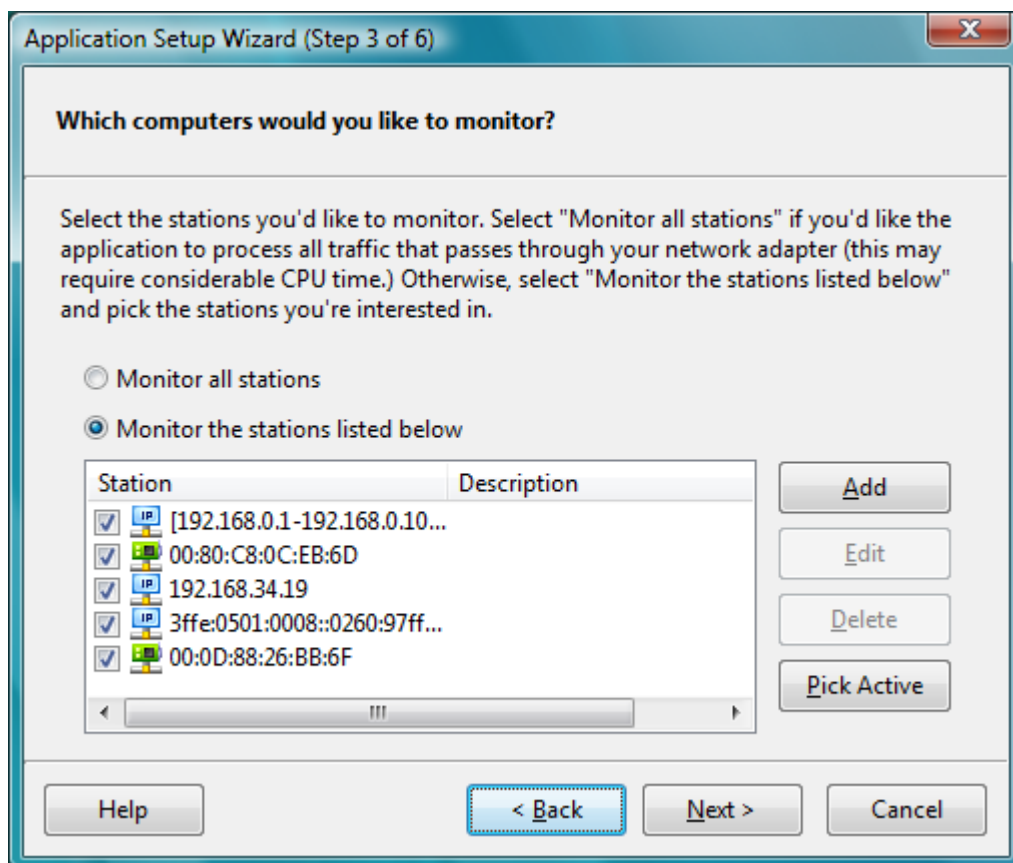
An optional utility for monitoring switch-based Ethernet networks is available. Please see the [PromiSwitch Tool](#) chapter for more information.

Setup Wizard

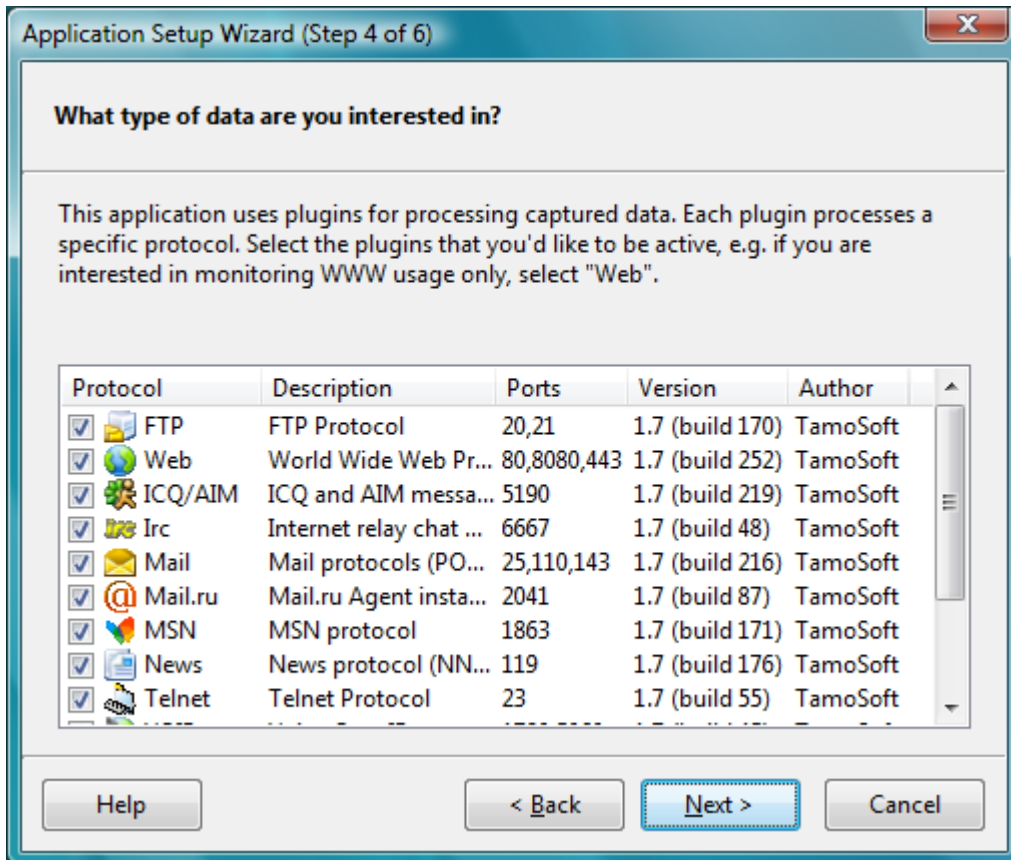
Before you can begin monitoring your network, you must configure NetResident. The Setup Wizard will help you configure NetResident with just a few mouse clicks. If you didn't start the wizard when you first launched the program, you can always do so by clicking **Tools => Setup Wizard**.

Click **Next** on the welcome screen and go to the adapter selection screen. The adapter selection screen has a drop-down list that allows you to specify the correct network adapter for monitoring. If your computer has a dial-up connection or is connected to the LAN via an Ethernet adapter, you will have only one adapter in the menu. Select it. If your computer serves as the Internet gateway for the LAN or has more than one network adapter, you will need to select the adapter that you would like NetResident to monitor. Some network adapters cannot operate in promiscuous mode. If you use such an adapter, please check the **Use non-promiscuous mode** box. This option must always be selected for wireless (802.11) adapters. For dial-up and VPN adapters, please select the **WAN miniport** adapter. Click **Next** to go to the stations selection screen.

The program will try to discover the workstations on your network and provide a list of nodes that you may want to monitor. The easiest way to configure this option is to select the **Monitor all stations** radio button. This will make NetResident collect all data from the network. You can always reconfigure this behavior and specify which stations you would like to monitor at a later time. Please see the [Monitored Stations](#) chapter for more information.



Click the **Next** button to go to the plugins selection screen. NetResident processes network traffic using protocol plugin modules. If you do not need to view the data transmitted over a particular network protocol, you may disable the corresponding plugin by unchecking the box next to the protocol name. Please read the [Plugins](#) chapter for more information.



The next screen allows you to configure the network monitoring behavior of the program. Select the **On Windows Startup** option if you'd like the program to start monitoring the network as soon as Windows starts, or select **On NetResident Startup** option if you'd like to monitor the network only when NetResident is running. Click **Next** and then **Finish** on the next screen to save the configuration settings.

Interface Overview

NetResident can display current information using views that can be changed using the **Events => Views** menu item or by clicking the corresponding button on the toolbar. The program's appearance may vary depending on the selected view, but basically, the main application window has three sections that present the data in a structured format and allow you to filter and sort network events and access them quickly.

Note: Depending on your [search settings](#), the main program window may contain several tabs: The **All Data** tab that shows all captured information as well as other tabs that correspond to your [Search Set\(s\)](#). The data structure inside the tabs is explained below.

The **Group View** shows network events grouped by the dates they occurred, network protocols, and hosts engaged in communications. Checking or unchecking the boxes next to a group will include/exclude the events that belong to the group to/from the **Event List** section. The hosts are grouped into **Parties** that represent the parties involved in the communication process. Party A includes all IP addresses/hostnames on the local side of the communication. If you only use one network interface to connect to the Internet, you will usually have only one entry under this Party. However, if you use your LAN adapter as the main Internet connection method, but also use your Dial-Up adapter occasionally, or if you have an IP address dynamically assigned to your computer each time you connect, you will have several entries in this Party. Party B includes all remote hosts that have communicated with the local host(s). Please refer to [Arranging the Data](#) for more information.

The **Explorer View** is similar to the Group View except that it shows network events grouped by network protocols only. We suggest that you use this view if you would like to see the events of the specified protocol: i.e. all ICQ messages for the specified period of time. Clicking on the plus sign will expand the nodes, allowing you to select and view the desired network events. Please refer to [Arranging the Data](#) for more information.

The **Event List** section displays a list of events available for viewing under the following columns:

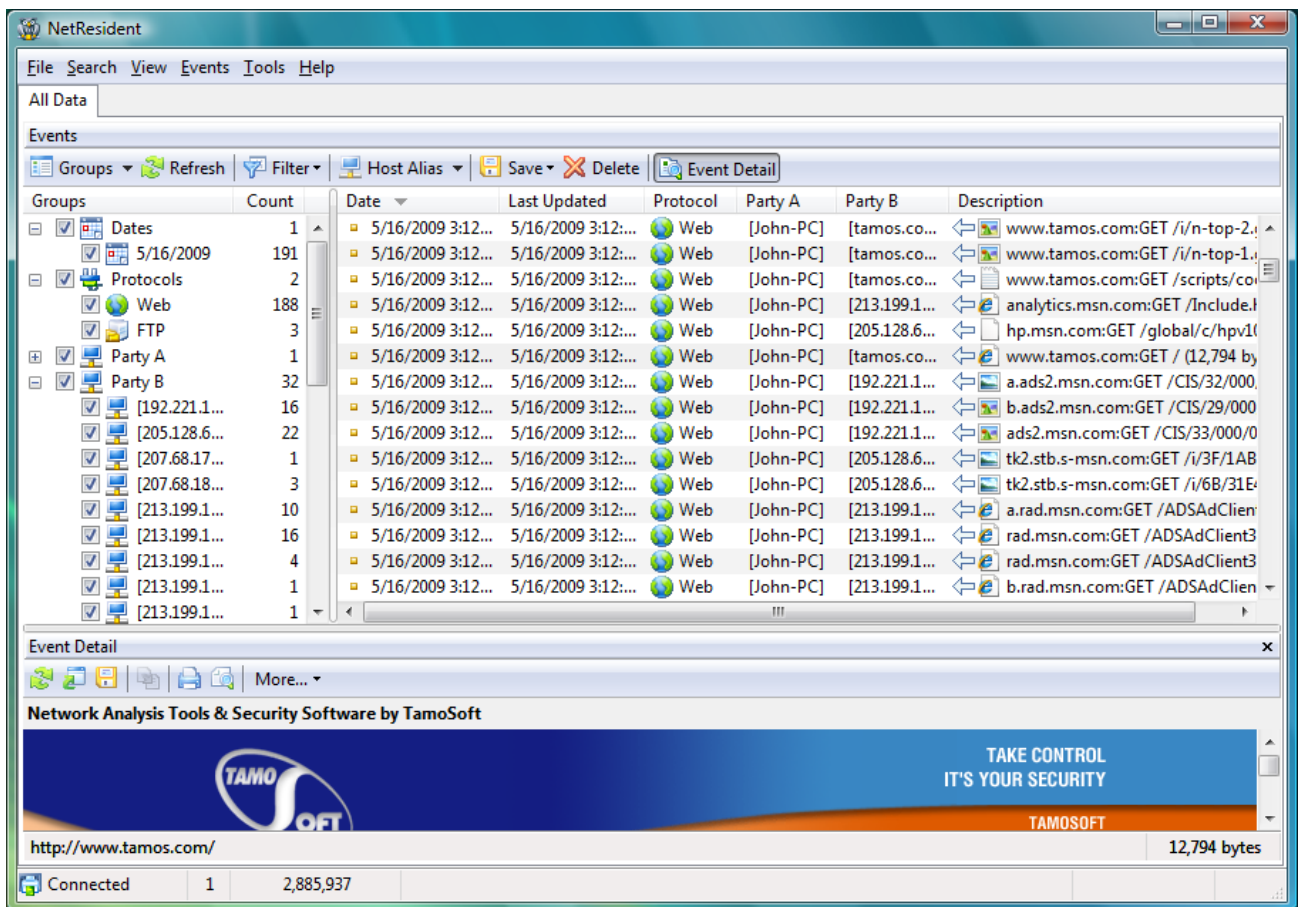
Date – the date the event occurred
Protocol – the protocol used for data transmission
Party A, Party B – indicates the hosts that sent and received data
Port A, Port B – the ports used for data transmission
Last updated – the date and time the event was last updated
Description – displays the event summary
ID – event ID (invisible by default)
Priority – user-defined event priority (invisible by default)
Comment – user-defined event comment (invisible by default)
Flags – event flags (invisible by default)

The **Event Detail** section displays the actual contents of the event selected in the **Event List** section. It can only display one event at a time.

The main window also has a **Status** section for displaying system messages produced by the program.

NetResident consists of two parts: The NetResident console that connects to the NetResident service, processes the data, groups it, and presents it to the user and the NetResident service that monitors the network, captures the data, and stores it in the [database](#) for processing and viewing.

NetResident uses network protocol plugin modules for processing the collected data. You can enable or disable certain plugins to make sure that you see only the desired data.



Main Menu	
File	
Connect	Makes a connection to the NetResident Service
Disconnect	Disconnect from the NetResident Service
Manage Database	Launches the Database Management Wizard
Import Logs	Launches the Log Import Wizard
Exit	Closes the program
Search	
Find	Searches the events for the specified string
Find Again	Repeats the search
New Search Set	Launches the Search Set Wizard
Delete Search Set	Deletes the currently active Search Set
Edit Search Set	Edits the currently active Search Set
View	
Status Window	Shows/hides the Status Window
Status Bar	Shows/hides the Status Bar
Events	
Refresh/ Stop Refreshing	Refreshes all events/stops the refreshing in progress

Filter	Allows you to set event filters
Save	Saves the current event list or event details to a file
Delete	Deletes selected events from the database
Event Detail	Shows/hides the Event Detail section
Views	Switches the main window's views
Host Display Mode	Changes the mode for displaying the hosts in the Group View and Events List sections
Tools	
Aliases	Displays the Aliases dialog
Options	Displays the Options dialog
Setup Wizard	Launches the Setup Wizard
Anti-Switch Tool	Starts the PromiSwitch application
Languages	Allows you to select the language of the user interface
Help	
Contents	Launches NetResident help
Search For Help On ...	Shows NetResident help index
Check for an Update on the Web...	Check for an update on the TamoSoft Web site
About	Shows the About window

Arranging the Data

NetResident is a powerful network monitoring application that presents a detailed picture of user network activities. On a busy network, you may see hundreds of thousands of network events such as e-mail messages, Web pages, instant messages, etc. Arranging the data in a way that enables you to find the events you are looking for is essential when using NetResident. We have implemented several filtering options that will allow you to display only the data you are interested in.

NetResident has **Explorer** and **Group** views that group the network events differently. We suggest that you look at both of those and choose the one that is most convenient for your needs.

The **Group View** section on the left side of the program's main window allows you to filter the network events by date, network communication party, or network host.

Groups	Count	Date	Last Updated	Protocol	Party A	Party B	Description
✓ Dates	1	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[tamos.co...	www.tamos.com:GET /i/n-top-2...
5/16/2009	191	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[tamos.co...	www.tamos.com:GET /i/n-top-1...
✓ Protocols	2	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[tamos.co...	www.tamos.com:GET /scripts/co...
Web	188	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	analytics.msn.com:GET /Include.l...
FTP	3	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[205.128.6...	hp.msn.com:GET /global/c/hpv10...
✓ Party A	1	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[tamos.co...	www.tamos.com:GET / (12,794 by...
Party B	32	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[192.221.1...	a.ads2.msn.com:GET /CIS/32/000...
[192.221.1...	16	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[192.221.1...	b.ads2.msn.com:GET /CIS/29/000...
[205.128.6...	22	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[192.221.1...	ads2.msn.com:GET /CIS/33/000/0...
[207.68.17...	1	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[205.128.6...	tk2.stb.s-msn.com:GET /i/3F/1AB...
[207.68.18...	3	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[205.128.6...	tk2.stb.s-msn.com:GET /i/6B/31E...
[213.199.1...	10	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	a.rad.msn.com:GET /ADSAdClie...
[213.199.1...	16	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	rad.msn.com:GET /ADSAdClient3...
[213.199.1...	4	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	rad.msn.com:GET /ADSAdClient3...
[213.199.1...	1	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	b.rad.msn.com:GET /ADSAdClie...
[213.199.1...	1	5/16/2009 3:12...	5/16/2009 3:12...	Web	[John-PC]	[213.199.1...	b.rad.msn.com:GET /ADSAdClie...

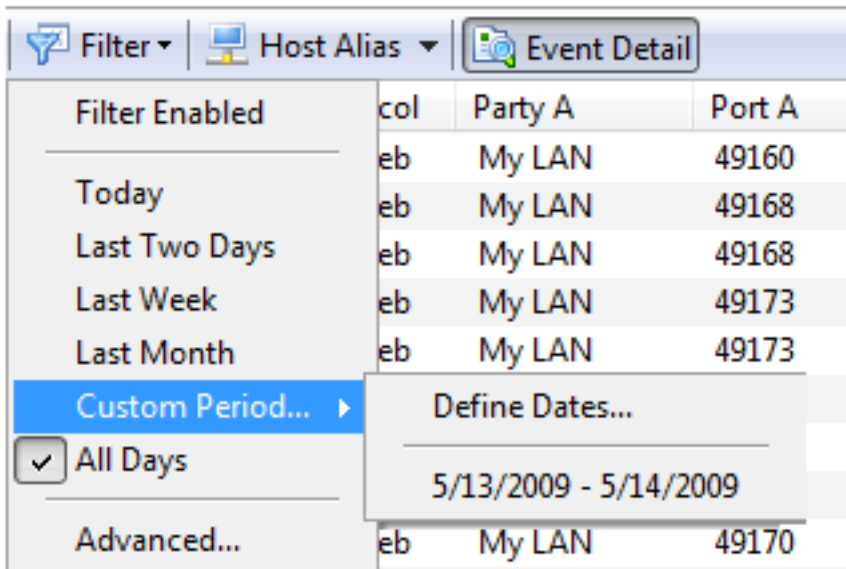
- **Dates** – check the boxes next to the dates of the network events you are interested in. Events occurring on other dates will be ignored and will not be displayed in the **Event View** section. Please note that unchecking the boxes in the **Group View** section will not delete the data from the database. You can reconfigure the **Group View** section to display other events that have been logged.
- **Protocols** – check the box next to the protocols that you want to view. For example, if you would like to view e-mail messages, then select the **Mail** protocol.
- **Party A / Party B** – allows you to filter network events by party from the network communication. You will find specific network hosts under Party A or Party B. Check or uncheck the boxes next to them to monitor network events generated by these hosts.

Please note that you can combine filters: For instance, if you would like to view only Web pages downloaded from a particular server on a certain day, please select the date in the **Dates** section, select **Web** in the **Protocols** section, and specify the host in the **Party B** section. All other events that do not match the criteria will be ignored.

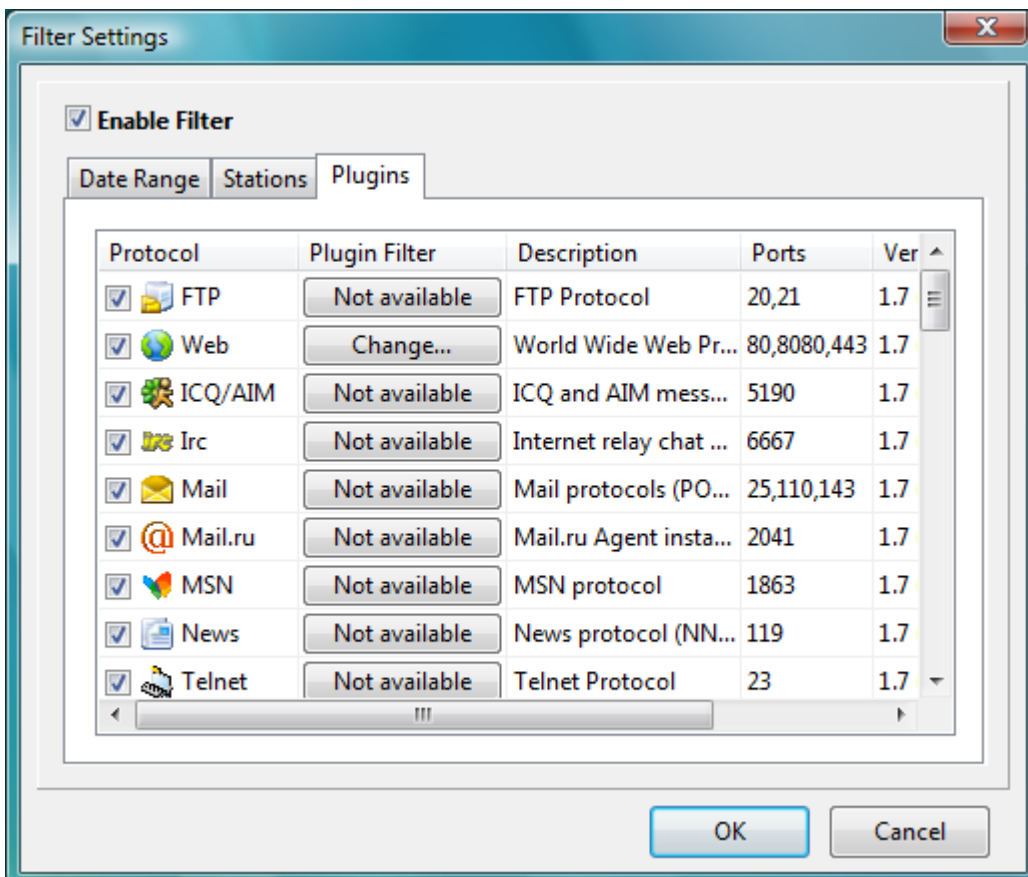
A more flexible date filter is available in the **Events => Filter** menu or by clicking the **Filter** toolbar button. You can specify a predefined period:

- **Today** – shows all network events that occurred today
- **Last Two Days** – shows all network events that occurred during the last two days
- **Last Week** – shows all network events that occurred during the last week
- **Last Month** – shows all network events that occurred during the last month

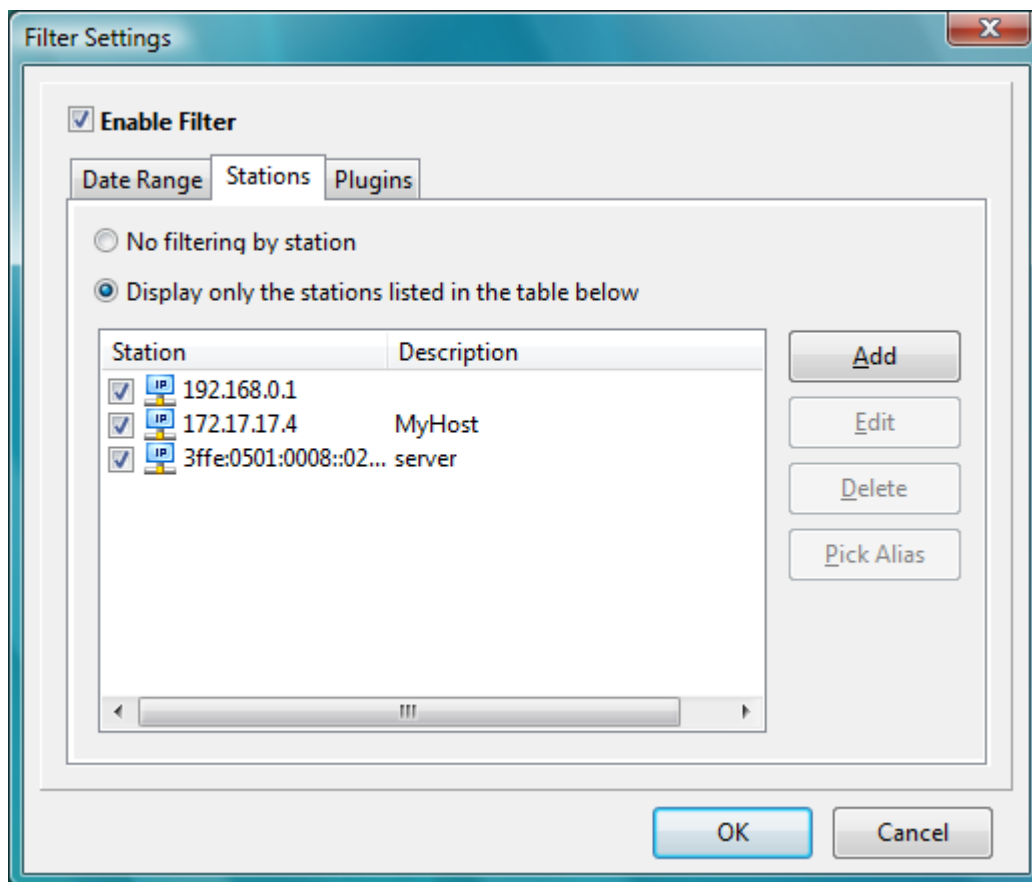
Selecting **All Days** from the menu will make the program display events for the entire monitoring period. You can also specify the date range under the **Custom Period** menu item by selecting **From** and **To** dates in the corresponding drop-down lists.



More advanced filtering options are available under the **Events => Filter => Advanced** menu. You can also filter the events by network protocol plugins or by stations.



The **Plugins** page displays all currently installed plugins. Active plugins have checked boxes next to their names. If you need only certain plugins (for instance, you need to view web pages and e-mails only), disable the unnecessary plugins by unchecking the corresponding boxes. If the specified plugin supports additional event filtering, you can change this filter by clicking on the **Change** button in the corresponding column. Please refer to the [Plugins](#) chapter for detailed plugin description.



NetResident allows you to display the data received only from selected stations (computers, routers, or other devices connected to your LAN). In that case, NetResident will only show the data from/to computers listed in the table in the **stations** section. You can add other stations by selecting **Display only stations listed in the table below**, clicking the **Add** button and specifying the IP address, IP addresses range, or MAC address of the station. If you have previously assigned aliases to hosts, you can click the **Pick Alias** button and choose a station from the list of aliases. You can also enter an optional description for each added station. Edit a station by selecting it and clicking the **Edit** button. If you'd like to remove a station from the list, select it and click on the **Delete** button.

Click **OK** to save the filter configuration or click **Cancel** to discard the settings.

If you would like to disable the filter temporarily without discarding the filter settings, uncheck the **Enable Filter** checkbox.

Important: The filter settings only affect the data displayed in the program's main window. The filter settings do not change the data collection or data storage behavior of the program. Data collection settings are described in the [Configuring NetResident](#) chapter of the present manual, and the data storage options are described in the [Database Management](#) chapter.

The **Explorer View** section on the left side of the program's main window allows you to filter network events by network protocols.

Expand the desired nodes by clicking the plus sign (+) to the left of the node. If you would like to view web pages, expand the Web node. The expanded node allows you to see network events of the specified protocol grouped by date. If you would like to see network events that occurred on a specific day, select the desired group on the left and view the network events themselves on the right. The Explorer View is similar to the Group View except for the way it groups network events.

Browsing Network Events

NetResident shows data exchange on the network in the form of network events. Examples of events include an e-mail message, a file downloaded via FTP, a downloaded Web page, or an ICQ instant message. After you have configured the data filtering options, the **Event List** section displays the raw list of events that NetResident has filtered from the database.

Each line in the Event List table represents a network event.

Date ▾	Last Updated	Protocol	Party A	Port A	Party B	Description
5/16/2009 3:12...	5/16/2009 3:12:51 PM	Web	My LAN	49714	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49714	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49717	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49714	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49717	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49714	[tamos.co...	www.tam
5/16/2009 3:12...	5/16/2009 3:12:50 PM	Web	My LAN	49717	[tamos.co...	www.tam

Event Detail

Edit alias 'My LAN'

Create alias for bw-in-f103.google.com (74.125.43.103)

Aliases...

Copy Address ▶

SmartWhois ▶

Record priority

Record comment

Record flags

Copy

Select All

The table has the following columns:

- **Date** – the date and time the event began.
- **Last updated** – the date and time the event was last updated.
- **Protocol** – the network protocol used for data transmission. The name of the protocol corresponds to the name of the plugin module responsible for processing the particular event.
- **Party A / Party B** – sending and receiving parties in the network data exchange. An example of parties would be a computer downloading a Web page and a Web server hosting the page, or a computer receiving e-mails and the mail server hosting the mailbox.
- **Port A/Port B** – the ports used for data transmission.
- **Description** – a brief description of the network event that includes the size of the transmitted object.
- **ID** – event ID (invisible by default)
- **Priority** – user-defined event priority (invisible by default)
- **Comment** – user-defined event comment (invisible by default)
- **Flags** – event flags (invisible by default)

Parties A and B participating in a connection may be displayed by their IP or MAC address or by the hostname associated with the IP address of the Party. The display options can be configured in the **Events => Hosts Display Mode** menu.

You can substitute IP or MAC addresses with easy-to-remember, human-readable names ([aliases](#)). Right-click on any network event and select the address from the pop-up menu to create an alias for the Party A or Party B host, or to open the list of aliases.

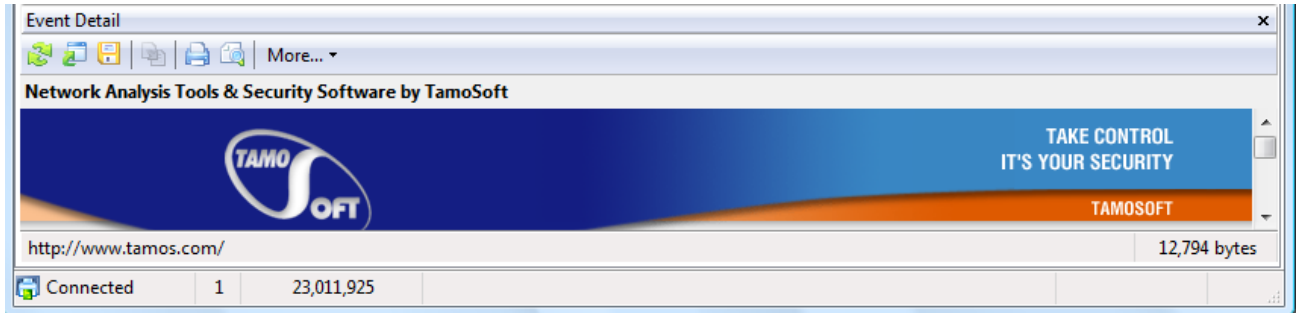
Save the event list to the HTML file by selecting **Events => Save List...** or click the corresponding button on the toolbar.

To view a network event in the Event Detail section, click on the event line in the **Event List**. Right-clicking on an event and selecting **Event Detail** from the pop-up menu will hide the Event Detail section.

Important: Some columns may be missing in the Explorer View (depending on the selected record group). For instance, if the specified protocol is selected, the corresponding column with the protocol name will be missing.

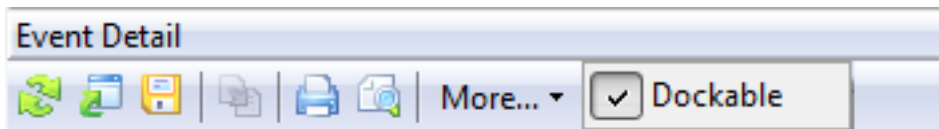
Viewing Event Details

The **Event Detail** section of the main window displays the reconstructed network event. To display the **Event Detail** section, click **Events => Event Detail** or right-click on a network event in the **Event View** section and select **Event Detail** from the pop-up menu. Alternately, you can click on the corresponding button on the toolbar to display the **Event Detail** section. NetResident protocol plugins process the data and reconstruct the entire Web page, e-mail message, instant messenger chat session, etc.



Once a network event is selected in the **Event View** section of the main window, NetResident will query the database and reconstruct the event details, displaying the results in the **Event Detail** section. Besides displaying the event itself, the program shows useful service information about the event, such as HTTP headers for Web pages, e-mail headers for e-mail messages, and FTP session logs for FTP file transfer sessions.

The **Event View** section has a toolbar and menu that offer different options, depending on the type of event selected.



You can drag the **Event View** section and place it anywhere in the program's main window. To bring the panel back, drag it over the main window until it attaches itself to a side of the window. To disable automatic docking, right-click the window header and uncheck the **Dockable** box.

The **Event Detail** section menu offers the following options:

Interface Settings – allows you to configure the font settings for the displayed event

Copy – copies the selected data to the clipboard

Select All – selects all data related to the network event

In addition to the general options mentioned above, each NetResident plugin offers plugin-specific options (depending on the network event type) that you can see in this menu. For instance, the **Show Login/Password** option displays the login and password used for mail sessions (for incoming e-mail messages only); the **View Headers** option displays HTTP Session headers (for Web pages only), etc.

Configuring NetResident

NetResident configuration options are available under the **Tools => Options** menu. If you are a novice user or not familiar with networking, we suggest that you launch the Setup Wizard to guide you through the configuration process.

The **Options** window allows you to configure NetResident to suit your needs. Select a category from the menu on the left side of the window to configure the options available for each menu item.

Interface: General

Allows you to change the interface font settings, configure the update mode .

If you prefer NetResident to run in the background, you can configure NetResident to run minimized by checking the **Show icon in the tray** box. Additionally, you may want to enable the **Hide from the taskbar on minimization** option if you want to hide the application from the taskbar on minimization.

Please check the **Enable automatic updates** box to enable updates. Also, you can configure the interval NetResident will check for updates: enter the desired value in the **Interval between checks, days** field. Clicking the **Check Now** button will make NetResident check for updates immediately.

Network: Startup

Allows you to configure the network monitoring function performed by [NetResident Service](#).

If you need to monitor your network constantly, select the **On Windows Startup** option. When this radio button is selected, NetResident Service will be launched on Windows startup and begin monitoring the network. You can launch NetResident and view the monitoring results at any time.

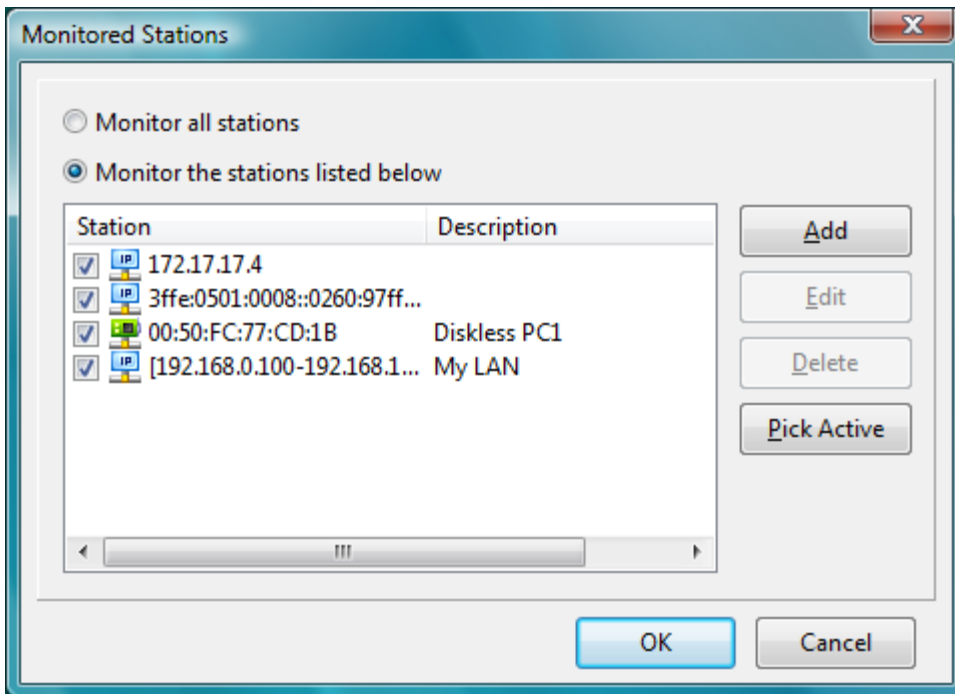
If you use NetResident periodically and don't need to monitor your network all the time, we suggest that you select the **On NetResident startup** option. This will allow you to save disk space and reduce the CPU load. By selecting this option, NetResident Service starts along with the NetResident application and starts monitoring the network. Network data collection will stop once you close the application.

Network: Targets

The **Targets** menu option has a drop-down list that allows you to specify the correct network adapter for monitoring the network. If your computer has a dial-up connection or is connected to the LAN via an Ethernet adapter, you will only have one adapter on the list; select it. If your computer serves as the Internet gateway for the LAN or has more than one network adapter, you will need to select the adapter you would like to monitor with NetResident. Some network adapters cannot operate in promiscuous mode; if you use such an adapter check the **Use non-promiscuous mode** box. This option must always be selected for wireless adapters. For dial-up and VPN adapters, select the **WAN miniport** adapter.

To analyze network data from all computers on your network, enable the **Monitor all stations** option. If you are on a busy network, you may wish to narrow the range of stations that NetResident monitors. Click the **Advanced** button and select the **Monitor the stations listed below** radio button. Check the boxes next to the selected stations. If the **Advanced** button is grayed out, disable the **Monitor all stations** option and the button will become available.

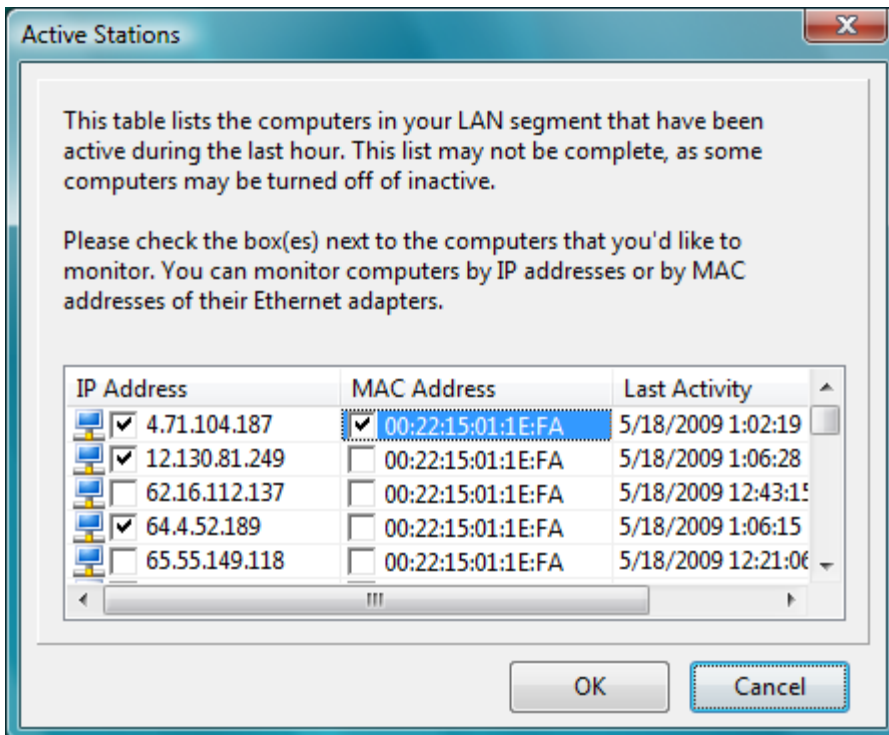
Monitored Stations



You can add a new station by clicking the **Add** button and entering the IP or MAC address or a range of IP addresses. The **Description** field is used for entering any information about the added station(s). This field is optional.

Click **OK** to save the settings or **Cancel** to discard the changes. Use the **Edit** and **Delete** buttons for changing or removing the stations on the list. If you want to disable the monitoring of a particular station temporarily, without removing it from the list, uncheck the box next to it.

You may also want to add active stations by clicking on the **Pick Active** button and checking the active stations discovered by NetResident:



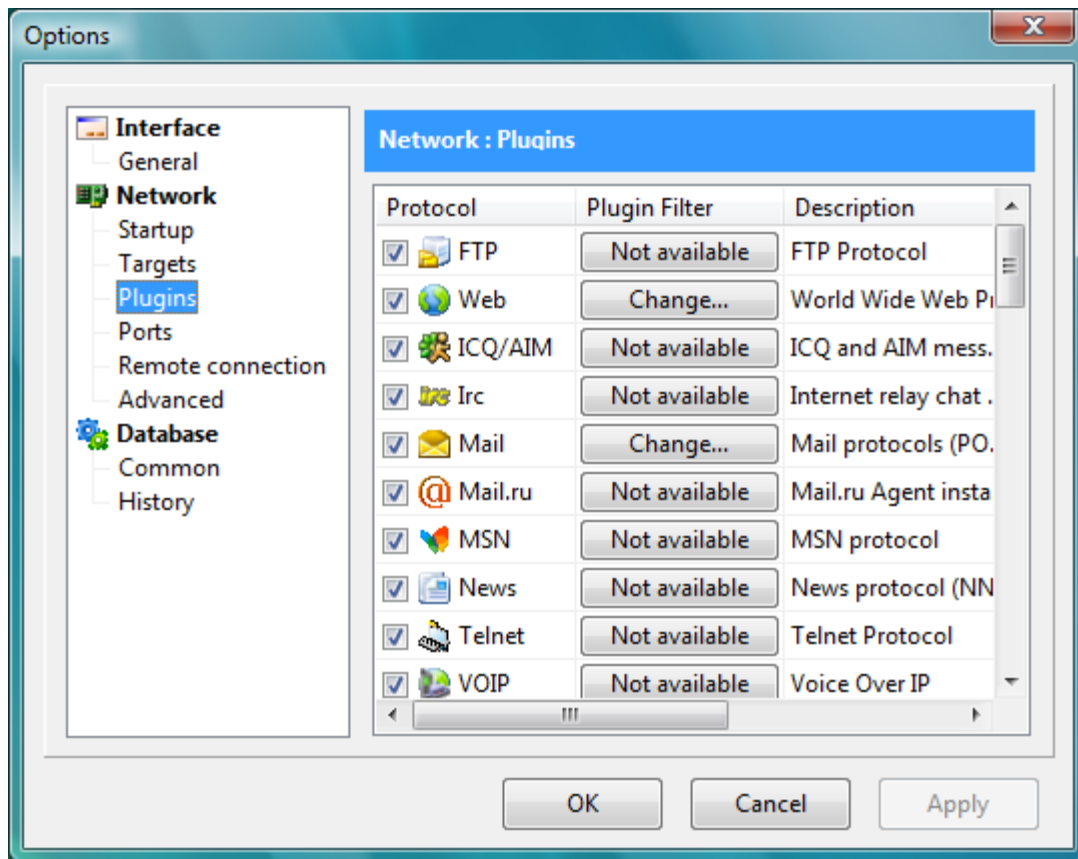
Select the desired addresses by checking the corresponding boxes and click **OK**. The selected addresses will be added to the list of stations for monitoring.

Please note that the list of stations can be incomplete, as some stations could be switched off or have changed their addresses. Also, some stations could be hidden behind firewalls. Please use this list as your reference only.

If you are unsure whether you should choose MAC or IP addresses for identifying the monitored stations, please refer to the [FAQ](#) chapter.

Network: Plugins

This page displays the list of currently installed plugins used by NetResident. If you don't use some of the plugins, we suggest that you disable them by unchecking their respective checkboxes in order to reduce CPU load and disk space utilization.



You can also use the internal plugin filters for specifying additional filter criteria that would result in reducing the number of captured events (and, of course, disk space utilization). To change the filter settings, click on the **Change** button of the respective plugin. See more detailed information in the [Plugins](#) chapter of the manual.

Note: Only Web and Mail plugins have plugin filters currently.

Network: Ports

This page allows you to configure the port numbers used by NetResident for traffic monitoring.

By default, NetResident Service is configured to monitor traffic on all possible ports (1-65535). This ensures that all possible network data would be intercepted. However, significant CPU time is required to process all (even unwanted) intercepted network packets. If you experience performance-related problems, try to narrow down the number of ports used for data interception. For instance, if you monitor traffic on a local office network where most traffic is generated by transferring files from one computer to another by means of Microsoft Windows, you may want to exclude this traffic by entering the following line:

```
139,445
```

The line above disables monitoring of ports 139 and 445. If you don't know what network ports are or don't experience any performance-related difficulties when running NetResident, don't change any values on this page.

You can specify one or several ports separated by commas or a port range. Please note that the port exclusion will be applied to both source and destination ports.

Network: Remote connections

This page allows you to configure remote connections to NetResident service. Please see the [Remote Connections to NetResident Service](#) chapter for more information.

Network: Advanced

This page allows you to configure the program's logging behavior. The **Enable service** logging option is turned on by default and the logging is set to the **Quiet** level. If you experience problems with NetResident, the TamoSoft support team may ask you to change the service logging level if additional information is required. NetResident service messages are written to the DebugCWS.log file located in the application folder and the TamoSoft support team may request that you send this file by e-mail. Please note that the log file may be considerable in size if the **Verbose** option is selected. Always zip the log file before sending it to customer support.

The **Automatic import** option that is available on this page is intended for automatic importing of the log files that contain captured network traffic. To enable this option, check the **Enable automatic import** box and select the folder that contains the required log files.

Note: The folder that contains the log files to be imported must be local, i.e. it must reside on the same computer where the NetResident Service is running.

Database: Common

NetResident has its own database that contains all captured and analyzed network information. Database files are located in the application folder by default. This page allows you to change the database location (if necessary for some reason). Select the desired folder where the database should be located and click **Apply**.

Database: History

Since the database contains records of all events captured by NetResident, the database size increases with time. To reduce space occupied by these records and increase the program's performance, you may want to enable the database size limitation mode by checking the **Limit database size** box. The **Delete the events older than** field contains the number of days NetResident will keep records. Older records are automatically deleted. Alternatively, you may want to archive old records instead of deleting them. To archive your records, check the **Create archive copies in** box and specify the path you want the archive records to be saved to. Use the [Database Management Wizard](#) if you want to restore previously stored archive records.

You can empty the database automatically each time you finish working with the program by checking the **Clear the database on exit** box.

Advanced Search

Advanced search allows you to search for virtually any data in the NetResident database, simplifying the analysis of captured network events. The search engine is capable of searching for specific data types, such as Web page contents, URL text, e-mail message headers, etc. The search fields are specific for every NetResident [plugin](#). You can search and create alarms for the data that has been already captured or for the data that will be captured in the future. Two data types are used in this search: **Search Target** and **Search Set**.

A Search Target is simply a search criterion that is used by NetResident when processing the database. It may be a keyword in the HTML text, e-mail message, URL address, etc. Search Target options vary for every NetResident plugin. A Search Set consists of one or many Search Targets that makes it possible to combine several search criteria.

Click **Search** => **New Search Set** to create a new Search Set. The Search Set wizard will help you create a new search filter with a few mouse clicks. Click **Next** on the welcome screen and proceed to the Search Set options screen.

Search Set Wizard (Step 2 of 4)

Search Set options

Name:

Search Set Logic

Event present in any search target (OR)

Event present in each search target (AND)

New Search Target

Delete Search Target

Available search targets

Selected search targets

>>

>

<

<<

Help < Back Next > Cancel

To create a set, you need to specify a unique name, select **Search Set logic**, and then select Search Targets that will be included in a set. Note that you have to first enter a Search Set name for all other options to become available. Click **New Search Target** to create a Search Target, and then click **Next** on the welcome screen. When creating a new Search Target, you must specify a unique name, select a desired plugin, the plugin field that will be used when searching, and its value. For example, if you want to search Web pages for the word "bomb," you should give the Search Target a unique name (e.g. "Bomb"), select the "Web" plugin, select the "Text" field, and enter the keyword (or several keywords) you're interested in (e.g. "bomb" or "bomb, explosive").

Hint: It's possible to specify several values at a time by separating them with commas.

Search Target Wizard (Step 2 of 3)

Search Target options

Name: Bomb

Plugin: Web

Field: Text (Document text without tags)

Value: bomb

Match Case

Whole Word

Apply to future events only

Help < Back Next > Cancel

The following additional options are also available:

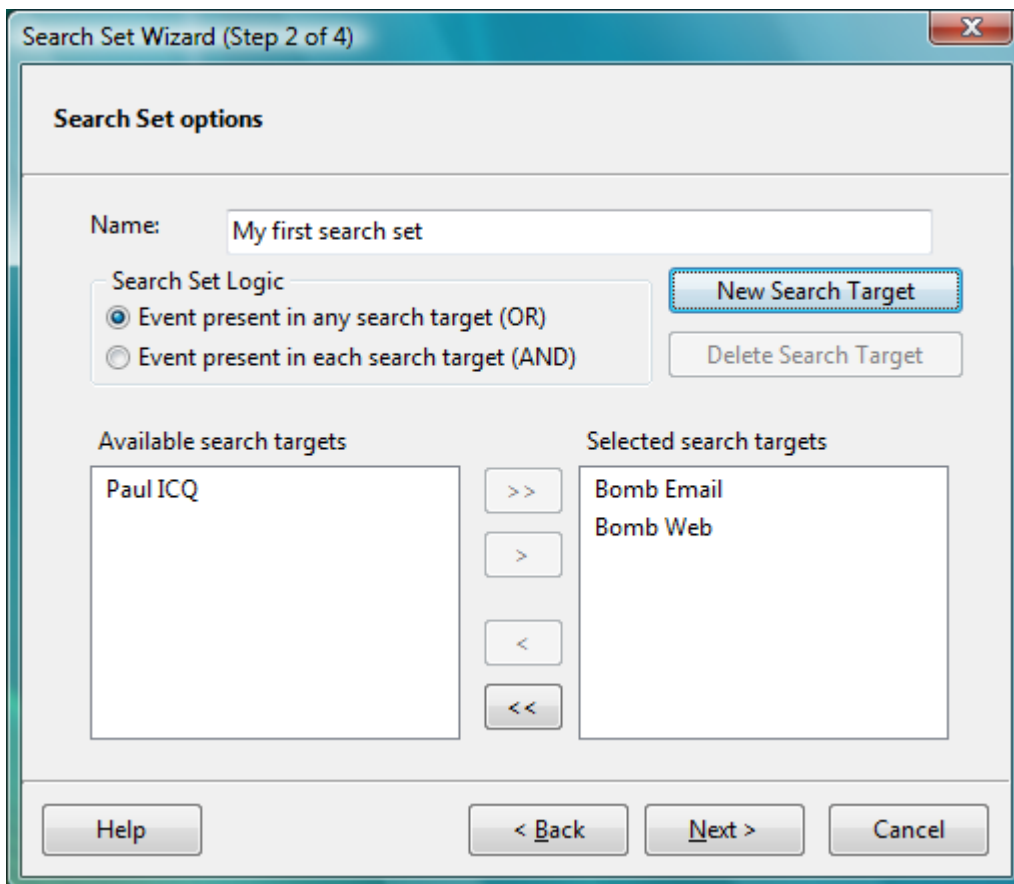
Match Case – when this option is selected, the case of the letters entered as the search word must match the case of the letters in the events to be searched.

Whole Word – if this option is selected, substrings will be ignored e.g. "sensitive" won't match "insensitive."

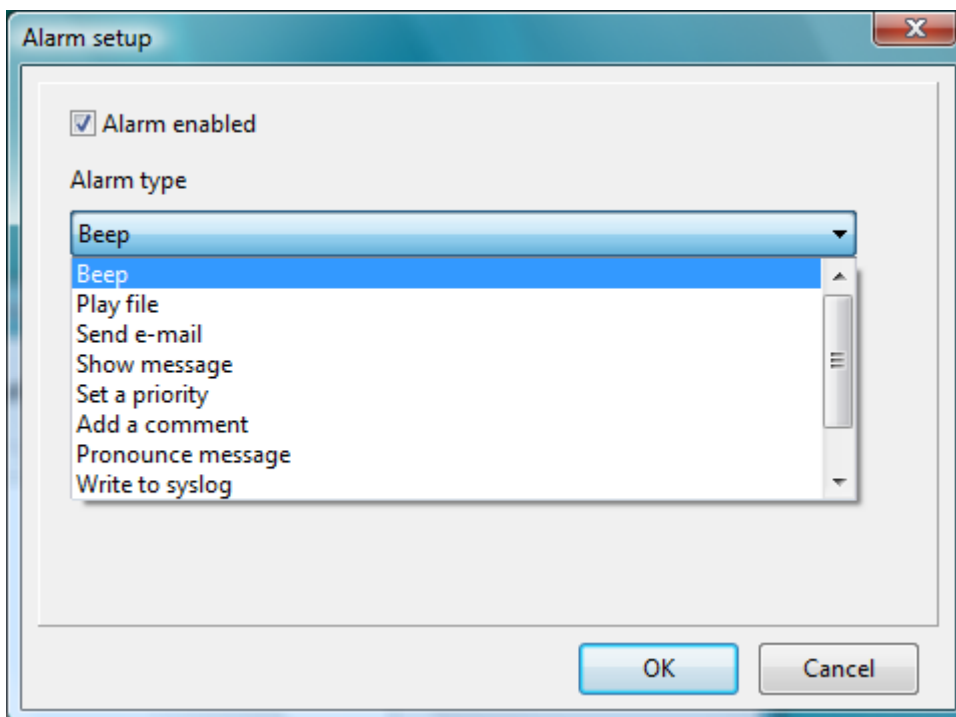
Apply to future events only – if this option is selected, a search will be performed for new records only. Otherwise, all records in the database, including previous ones, will be processed.

Note: Every Search Target requires additional database processing, so try to minimize the number of Search Targets to reduce the consumption of computer resources. In other words, delete the Search Targets that you don't need anymore, as a large number of Search Targets increases computer resource utilization.

Now click **Next** and then **Finish** to close the Search Target wizard.



Select the desired Search Targets by moving them from the **Available search targets** list to the **Selected search targets** list. Click on the **Next** button to select the desired notification type.



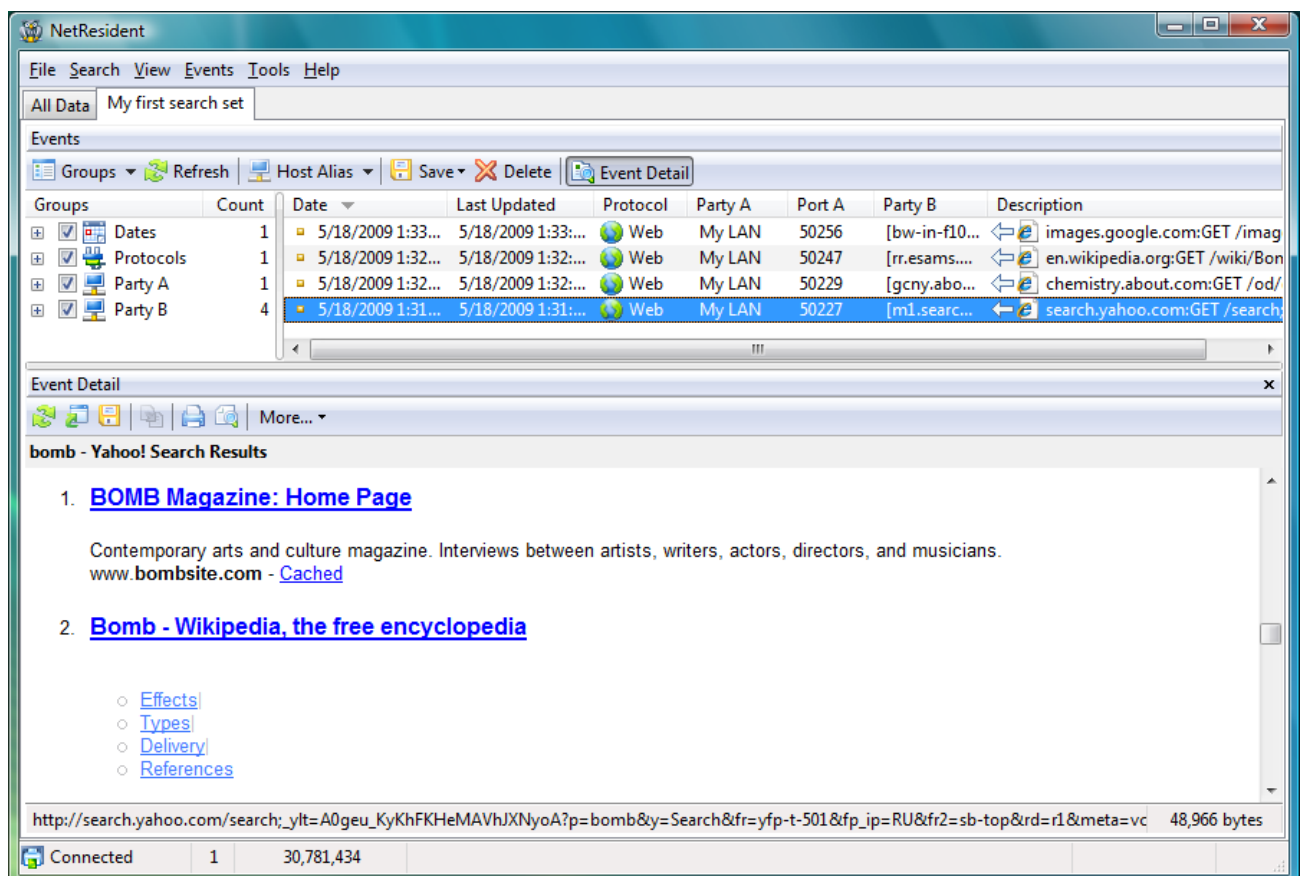
The **Search Set notification selection** window allows you to select the actions to be performed when the Search Set contents match your search criteria. The following actions are available:

- **Beep:** The computer beeps.
- **Play file:** Plays the specified WAV file.
- **Send e-mail to:** Sends e-mail to the specified e-mail address. You MUST configure NetResident to use your SMTP server prior to sending e-mail. Use the **E-mail Setup** button to enter your SMTP server settings. Usually, an e-mail message can also be used to send alerts to your instant messaging application, cell phone, or pager. For example, to send a message to an ICQ user, you should enter the e-mail address as ICQ_USER_UIN@pager.icq.com, where ICQ_USER_UIN is the user's unique ICQ identification number, and allow EmailExpress messages in the ICQ options. Please refer to your instant messenger documentation or cell phone operator for more information. The **E-mail message text** field can be used to add an arbitrary message to the e-mail notification.
- **Show message:** Shows a notification with the specified text.
- **Set a priority:** Sets the event priority.
- **Add a comment:** Adds a comment for the event.
- **Pronounce message:** Makes Windows speak the specified text using the text-to-speech engine. By default, Windows only comes with English computer voices, so Windows may not be able to pronounce messages correctly if the text is entered in a language other than English.
- **Write to syslog:** Sends the message to the specified IP address using the syslog protocol.
- **Send SNMP trap:** Sends the message to the specified IP address using the SNMP protocol. The MIB file containing OID descriptions is available upon request.
- **Launch application:** Launches the specified application (additional command line parameters are supported).

If you need to temporarily disable any of the actions, uncheck their respective checkboxes.

Note: The Beep, Play File, Pronounce message, Launch application, and Show Message options work only if the NetResident console is active.

Select the desired notification actions and click **Next**. The Search Set that you've just created will be registered in the database and the corresponding tab with its name will be available in the main program window. All records that match your Search Target(s) will be displayed on this tab.



If you would like to modify or delete a Search Set, use the corresponding items located in the **Search** menu.

Aliases

Aliases are easy-to-remember, human-readable names that can substitute for MAC or IP address displayed in the **Group View** and **Event View** sections of the program's main window. This can make it easier to recognize and analyze network events.

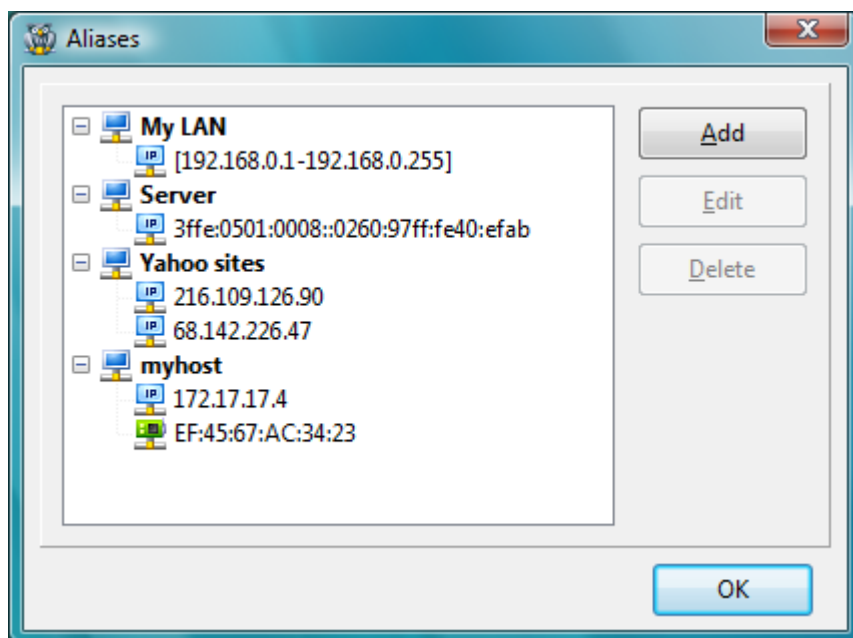
Once an alias is assigned to an IP or MAC address, it will replace the corresponding address in the **Group View** and **Event View** sections of the main window. You can choose how the hosts participating in the communications are displayed: by **IP Address**, by **MAC Address**, or by **Host Alias**. Configure how hosts are displayed in the **Events => Host Display Mode** menu.

The program is capable of resolving IP addresses to hostnames. Check the **Resolve numeric IP addresses to hostnames** item in the **Events => Host Display Mode** menu to enable IP addresses resolution.

An alias may also be assigned to a range of IP addresses. This is very convenient, as it allows you to have just one name for a group of network devices – for instance, all computers on a LAN.

Each alias is unique. However, you can assign the same alias to several MAC or IP addresses, thus forming a group. This is useful if a computer has several network addresses and you would like to identify them all by one name.

You can add, edit, or delete aliases by clicking **Tools => Aliases**



Click the **Add** button to add a station. Enter an alias name and click the **Add** button. A dialog window will open prompting you to enter the address for the alias and select its type: **IP Address**, **IP Address Range**, or **MAC Address**. If you would like to add a range of IP addresses, select the **IP Address Range** radio button and enter the starting and ending IP addresses for the range in the corresponding fields.

Click the **OK** button to update the list of aliases or click **Cancel** to discard the changes. You can edit an alias by selecting it and clicking on the **Edit** or **Delete** buttons.

You may also assign aliases to hosts by right-clicking on a network event in the **Event View** section of the main window and choosing a corresponding item from the pop-up menu.

Importing Packet Log Files

NetResident uses its monitoring and logging capability for network data analysis and presentation. It can also allow you to import packet capture files saved by other TamoSoft network monitoring packages: CommView and CommView for WiFi, as well as by some other 3rd party network monitoring applications.

Launch the Log Importing Wizard by clicking **File => Import Logs**. You will be prompted to select the file for import and configure the import options. The imported file may have been recorded some time ago and you may want to import the file with the current date assigned to all events in the log. Otherwise, all data will be imported with its original date in accordance with the internal time stamp from the log file.

Note: This option is not available for all types of log files.

Important: Some or all of the events in the log file may be deleted from the database right after the import because the application might be configured to delete old events. If the time stamps in the log file are older than the number of days specified in the application options, consider using the current date when importing the log file, or increase the event time frame in the application options. Please see the description of the [Database: History](#) option for more information.

You may import only the events that you are interested in instead of importing the entire log file. Check the **Use current service filters while importing the data** checkbox. The import wizard will then use the current filter settings for the NetResident service.

Please make sure that current **Group View** and [filter](#) settings allow NetResident to display the data being imported. Otherwise, you won't be able to see it in the main window, even if the data is successfully imported into the database, until you change these settings.

Click the **Next** button to import the selected file. You can wait until the import is completed or click on the **Finish** button to continue importing in the background. In this case, the program will notify you when the import is completed. Importing can be cancelled at any time by clicking on the **Cancel** button.

NetResident supports importing log files using a command line. If you would like to use a command line when importing, start NetResident and specify the log file name as the first command line parameter. Please note that the name of a log file must include the full path.

Important: If a file name or its path contains spaces, it must be enclosed in quotation marks (" ").

Examples:

```
NETRESIDENT.EXE C:\mylog.ncf
```

```
NETRESIDENT.EXE "D:\DATA\October 12.cap"
```

```
NETRESIDENT.EXE "D:\Captured data\log file.pkt"
```

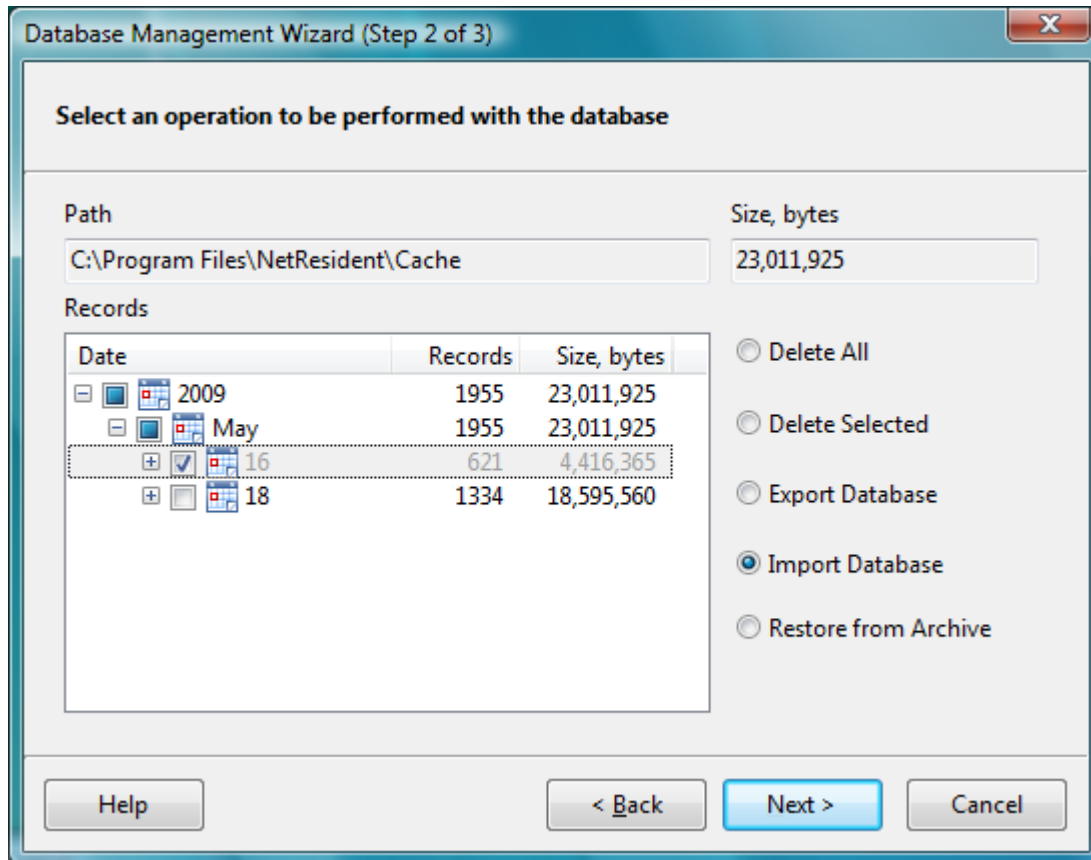
Note: Log file import is not available to Lite License users.

Database Management

All captured and analyzed network information is saved to the NetResident database. The database may eventually grow so large that it will affect the program's performance. Records may also become obsolete over time. In these instances, we suggest you remove unnecessary records using the **Database Management Wizard**.

Click **File => Manage Database** to launch the **Database Management Wizard**.

Click the **Next** button to view the current state of the database, its size and the number of records. Also, select the operation to perform with the database.



View current network events saved in the NetResident database on this page. The **Date** column allows you to find the records by the date (year, month, day) the recorded network events occurred. The **Records** column displays the number of network events for the period, selected in the **Date** column. To delete all network events in the database, select the **Delete All** option, or to delete the records for a specified time period (day, month, year), check the corresponding box and select the **Delete Selected** option.

Important: The records will be permanently deleted and cannot be recovered!

If you'd like to save the database for further use on another computer, select **Export Database**. NetResident will save the database in a file that can be viewed later by selecting the **Import Database** option.

Note: Database Export writes all events from the database to a file. Database import deletes all records in your current database!

If you need to restore data from an archive, select the **Restore from archive** option. Note that event dates are also imported from an archive, so you may need to change the filter settings for the records to be shown. If the database size limitation option is enabled, event records are automatically archived at the end of the day, and the archive would contain duplicated records. To prevent this from happening, you need to either disable the database size limitation option or delete the required records manually.

Choose the desired operation and click the **Next** button. When you select Import or Export options, you will be prompted for a database file name. If the **Restore from archive** option is selected, you will need to indicate which folder in the archive contains the records for the desired date. Database maintenance may take a significant amount of time. Data monitoring and logging will be paused while the changes are being entered into the database.

NetResident Service

The NetResident Service runs in the background capturing network traffic, analyzing it, and adding it to the database. The service starts automatically on Windows startup and is active at all times. Depending on the program configuration, it captures the traffic at all times or only when NetResident is launched. This behavior is configured in the **Tools => Options, Network => Startup** window in the menu. Please refer to the [Network: Startup](#) section of the manual for more information.

Normally, you would not need to start or stop NetResident Service manually. Should you need to do so, the service can be controlled from the NetResident program group (**Stop / Start NetResident Service** items) or in **Control Panel => Administrative Tools => Services**.

Remote Connections to NetResident Service

Note: Please refer to the [FAQ](#) chapter for information on licensing the NetResident service and console deployed on different computers.

As mentioned before, NetResident consists of two parts: The NetResident console that connects to the NetResident service, processes the data, groups it, and presents it to the user and the NetResident service that monitors the network, captures the data, and stores it in the [database](#) for processing and viewing. The connection between the service and console is made over TCP/IP, which means that you can connect to NetResident service running on any computer, as long as you can connect to it over TCP/IP and know the password.

When you start NetResident, it initiates a connection to the NetResident service you connected to last time (by default, this is the local PC). To connect to another NetResident service, do the following:

- Click **File => Disconnect** to disconnect from the NetResident service you're currently connected to.
- Click **File => Connect**.
- Select the **Connect to local service** option if you would like to connect to NetResident service running on the computer that you are currently using. If you would like to connect to a remote computer running NetResident, select the **Connect to remote service** option.
- If you selected the **Connect to remote service** option, specify the IP address of the computer you would like to connect to and the password in the **Remote Service** and **Password** fields respectively.
- Click **OK**.

Please note that remote connections to NetResident service are disabled by default for security reasons. To enable this option, NetResident service should be properly configured on the computer to which you want to connect. To configure NetResident, start the program and select **Tools => Options => Network => Remote connection**. Check the **Allow remote connections to this service** box and specify the password for connecting to the service in the **Password** field. Confirm the password by entering it once again in the **Confirm password** field and click **OK**.

Note: You will never be prompted for a password when connecting to NetResident service locally.

Plugins

NetResident uses a protocol module plugin system for processing and displaying network events. Every plugin is responsible for processing one network protocol or a number of protocols. The NetResident installation package comes with the following protocol plugins:

- **Web** – processes the data transmitted over HTTP protocol. This plugin is responsible for displaying Web pages.
- **Mail** – processes the data transmitted over POP3, SMTP, and IMAP protocols. These protocols are used by e-mail client and server software for e-mail message exchange.
- **News** – processes the data transmitted over NNTP protocol. This protocol is used for newsgroup message posting and viewing.
- **ICQ/AIM** – processes the data transmitted over [ICQ](#) and [AOL](#) instant messaging protocols.
- **MSN** – processes the data transmitted over [MSN](#) instant messaging protocol version 8.
- **FTP** – processes the data transmitted over FTP protocol used for downloading/uploading files from/to FTP servers.
- **Yahoo** – processes the data transmitted over [Yahoo](#) instant messaging protocol.
- **Jabber** – processes the data transmitted over XMPP protocol. This protocol is used for instant messaging by various [Jabber](#) clients, including [Google Talk](#). Please note that the **Jabber** plugin is unable to capture SSL-encrypted messages.
- **IRC** – processes the data transmitted over Internet Relay Chat protocol.
- **Telnet** – processes the data transmitted over Telnet protocol.
- **VoIP** – processes the data transmitted over SIP protocol using RTP voice streams.
- **WebMail** – processes e-mail messages sent or received via the Web interface of Web-based mail systems.
Note: The **Web** plugin is required for **WebMail** to operate properly.

Note: Playback of captured voice streams is not available to Lite License users.

The plugin modules are located in the Plugins subfolder in the application folder. By default, all plugins are enabled and active, i.e. they process network data and save it to the database. If you are not interested in processing and storing the data transmitted over certain protocols, you can [disable](#) the corresponding plugins in order to decrease CPU load and disk space utilization.

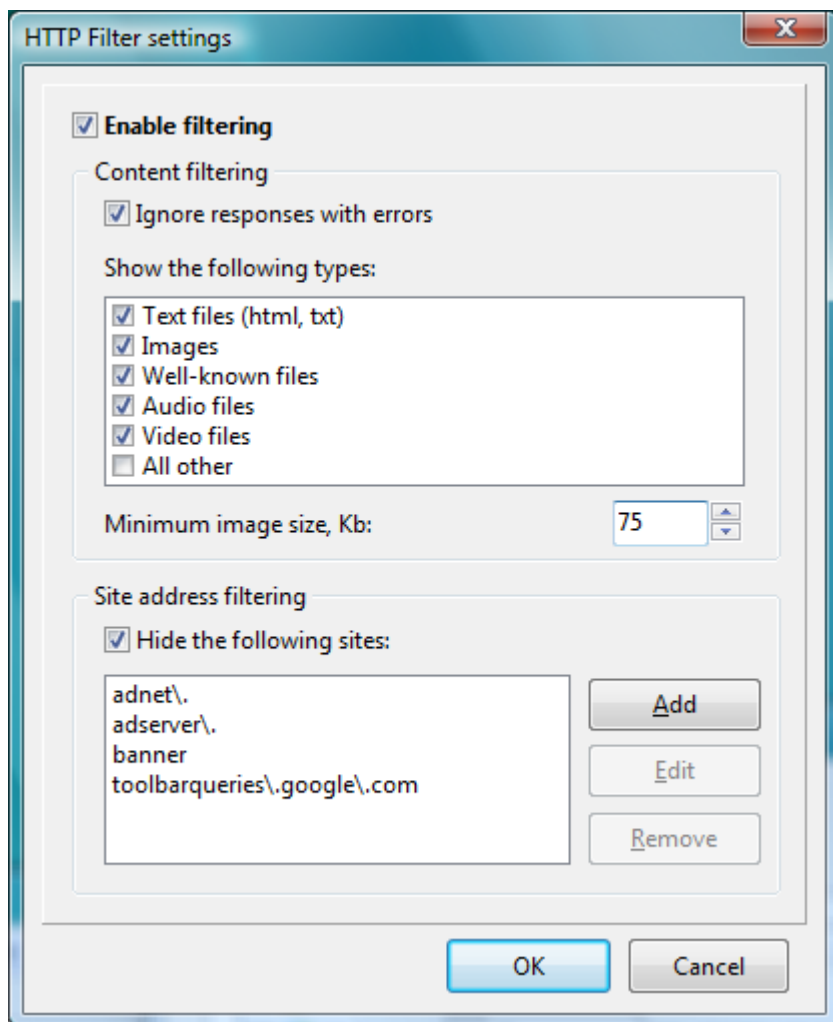
Additional plugin modules from [TamoSoft](#) can be added to NetResident as they become available. Place the plugin module file into the Plugins subfolder in the application folder. After adding a plugin, restart the NetResident service to load the new module. Click the **Stop NetResident Service** / **Start NetResident Service** menu items in the NetResident program group to restart the service.

Some NetResident plugins can be configured to hide captured events (they won't be displayed in the event list, but they will be stored in the database) or even to filter out events during capturing altogether (they will be neither stored in the database nor displayed). The latter type is referred to as a "capture filter".

To configure a plugin to hide events, select **Events => Filter => Advanced**. Go to the **Plugins** tab. Select the desired plugin and click the **Change** button. To configure capture filtering, select **Tools => Options** and click **Plugins**. Select the desired plugin and click on the **Change** button to change its settings. The following options are available:

HTTP Filter

Displaying a Web page requires a large amount of auxiliary files to be loaded by a browser automatically when opening the web page. The purpose of this filter is to hide all auxiliary files in order to reduce the amount of displayed records.



Please check the **Enable filtering** box for the HTTP filter to become active. If you would like to temporarily disable the filter, uncheck this box.

The **Show the following types** list allows you to specify the file types that will (or will not, depending on the settings) be shown as network events.

- **Text files** – text and html files (Web pages)
- **Images** – images
- **Well-known files** –archives (.zip, .rar, .arj, etc.), MS Office documents (.doc, .xls) and other well-known files won't be displayed when this box is checked
- **Audio files** – audio files
- **Video files** – video files
- **All other** – any other file type

Unchecking the corresponding boxes will make NetResident hide the respective files from the event list. For instance, if you uncheck the **Images** box, you won't be able to see any images on the list. Unchecking the corresponding boxes will make NetResident remove the respective file types from the list. If you uncheck all boxes, you won't see HTTP network events at all.

Minimum image size, Kb – this option sets the minimum size the image must match to be displayed. Most images on the web (except photos) are quite small. If you would like NetResident to display images, but you don't want to see banners and page elements, set the desired value in this field.

Ignore responses with errors – when enabled, this option hides error requests/responses (most users should enable this option to reduce the amount of junk records)

Another part of the HTTP filter is site address filtering. It allows you to hide specific sites using their name as the filter criterion.

Hide the following sites – enables/disables site address filtering.

When enabled, the site address filter will hide all sites meeting the filtering criteria (specified in the **Site Address Filtering** frame). Please use the following basic syntax for specifying filter criterions:

. – any symbol
\. – the dot symbol
\d – a digit (from 0 to 9)

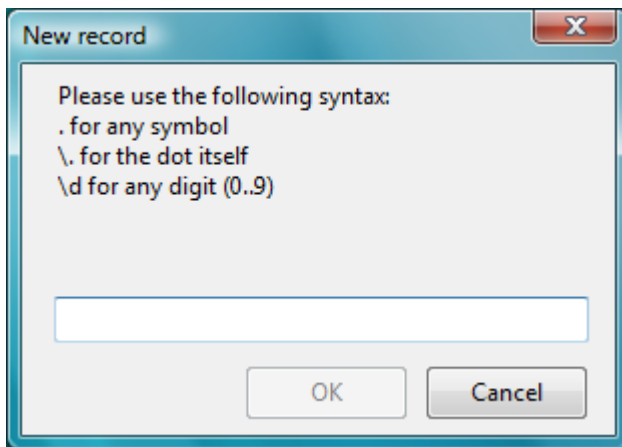
NetResident uses standard regular expressions for filtering. You can find more information regarding regular expressions and their syntax at <http://www.regular-expressions.info/reference.html>

Criteria examples:

Google\.com – hides sites containing "google.com" in their domain name
www\.google\.com – hides "www.google.com"
\.org\$ – hides all sites from the .ORG domain
\d – hides all sites that have a digit in their domain name

Note: If you only specify the domain as a criterion (.org, .com, etc.), the \$ character should be placed at the end of the string.

To add a filter criterion, please click the **Add** button on the right side of the window.

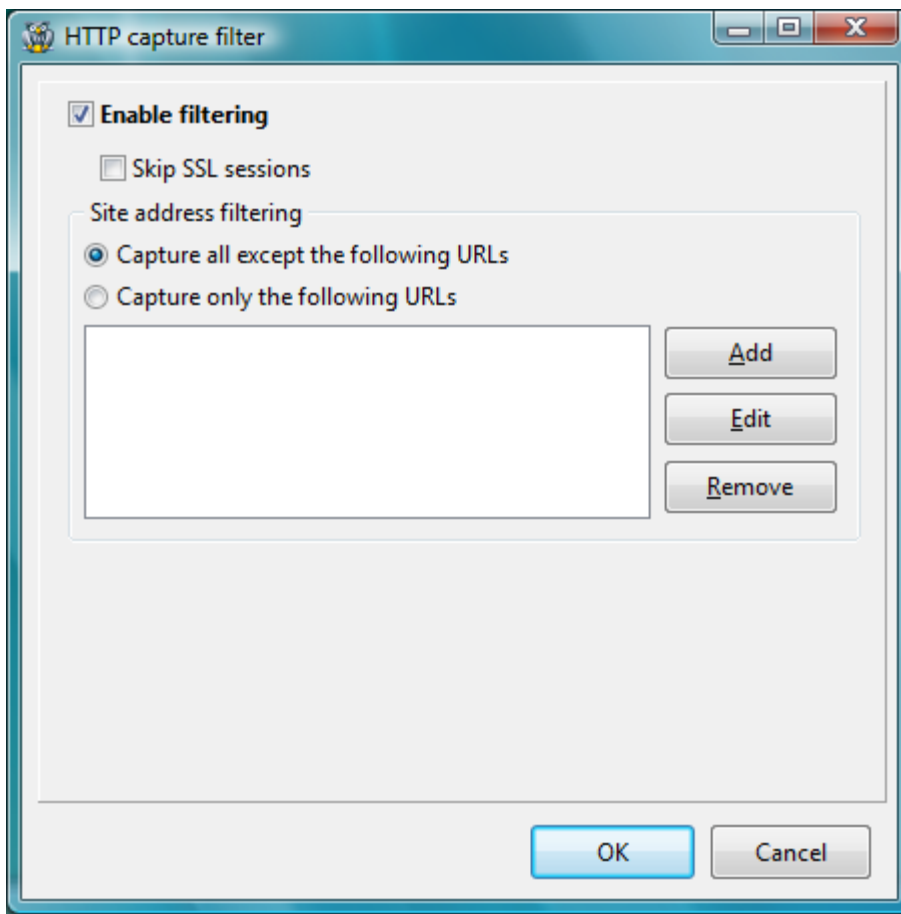


The **Add Record** window will open. Please specify a desired criterion and click on the **OK** button. The window will close and the respective record will be added to the filter criteria list.

To remove a record, please select it in the list and click the **Remove** button. To edit a record, select the desired record and click the **Edit** button.

HTTP Capture Filter

The purpose of this filter is similar to the previous one, except that it filters out events before saving them to the database. This reduces the amount of required disk space and CPU load while processing the database.



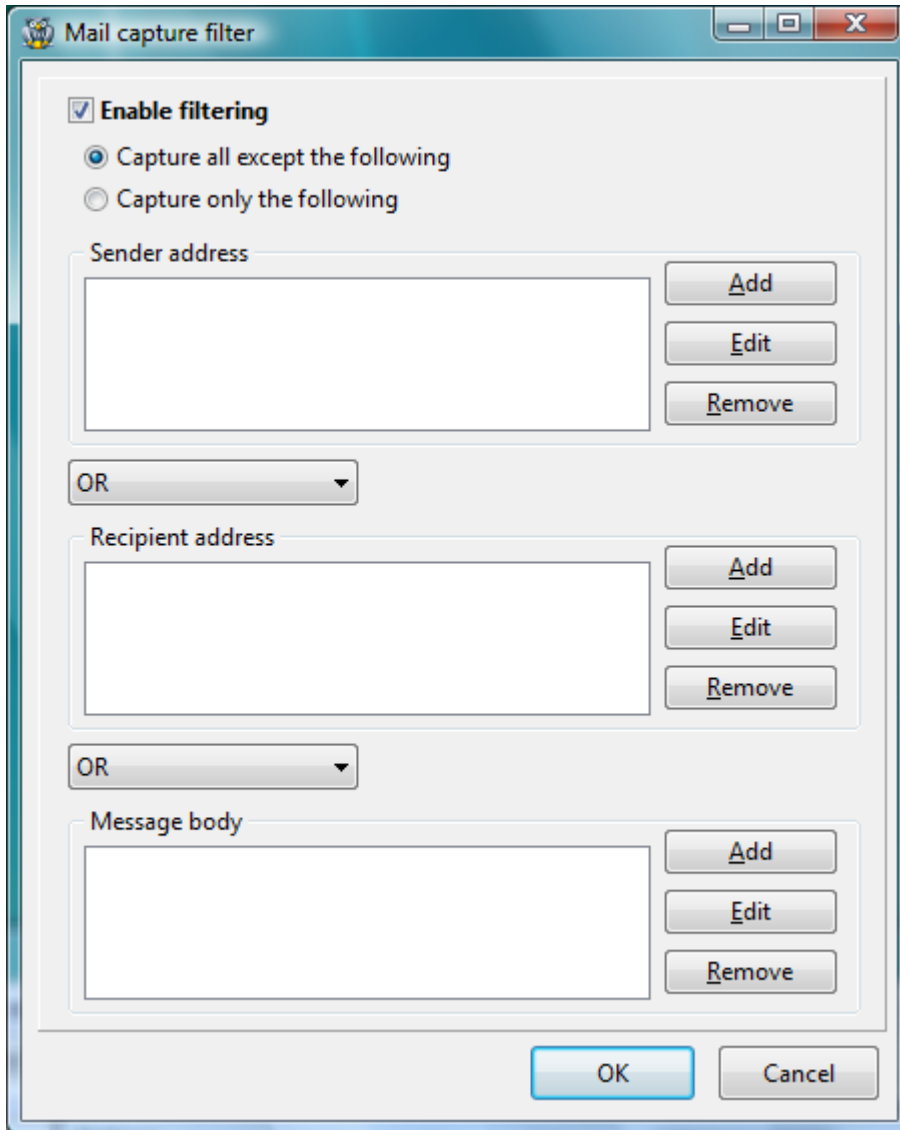
Check the **Enable filtering** box for the HTTP filter to become active. If you would like to temporarily disable the filter, uncheck this box.

Check the **Skip SSL sessions** box to disable capturing of HTTPS sessions.

The **Site Address Filtering** frame allows you to configure the list of URLs you'd like the application to filter. More information on the syntax for specifying filter criteria (regular expressions) is given above. Two filtering modes are available: recording only the events matching filter criteria (the **Capture only the following URLs** option) or recording all events except the ones that match the criteria (the **Capture all except the following URLs** option).

Mail Capture Filter

This filter is for filtering e-mail messages and it is similar in functionality to the previous one.



The image shows a Windows-style dialog box titled "Mail capture filter". At the top left, there is a small icon of a bird. The dialog has a standard Windows title bar with minimize, maximize, and close buttons. The main content area is light gray and contains the following elements:

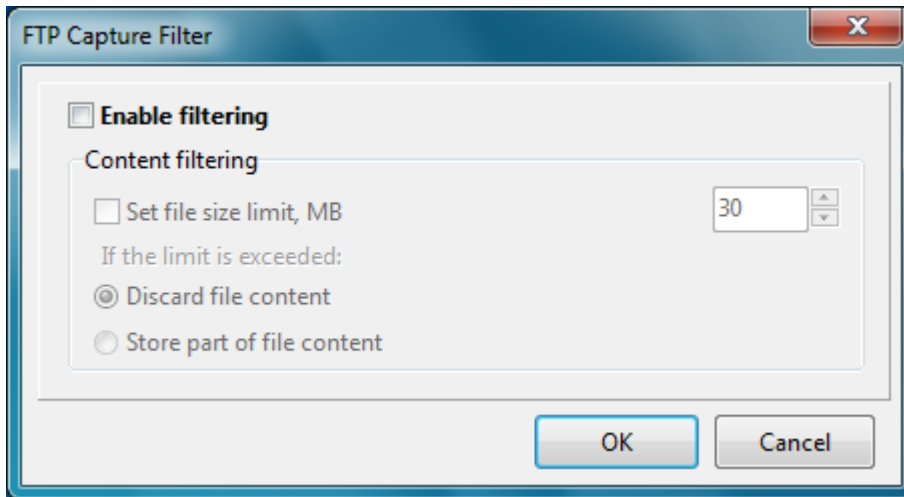
- A checked checkbox labeled "Enable filtering".
- Two radio buttons: "Capture all except the following" (selected) and "Capture only the following".
- A section for "Sender address" with a large text input field and three buttons: "Add", "Edit", and "Remove".
- A dropdown menu showing "OR" with a downward arrow.
- A section for "Recipient address" with a large text input field and three buttons: "Add", "Edit", and "Remove".
- Another dropdown menu showing "OR" with a downward arrow.
- A section for "Message body" with a large text input field and three buttons: "Add", "Edit", and "Remove".
- At the bottom, there are two buttons: "OK" and "Cancel".

Check the **Enable filtering** box for the Mail capture filter to become active. If you would like to temporarily disable the filter, uncheck this box.

Events can be filtered out by sender/recipient addresses and keywords in the message body. Boolean (AND/OR) logic is used to combine filter conditions. More information on the syntax for specifying filter criteria (regular expressions) is given above. This filter allows recording either all e-mail messages matching the filter conditions (the **Capture only the following** option) or recording all events except the ones that match filter the conditions (the **Capture all except the following** option).

FTP Capture Filter

Capturing data exchange via FTP protocol may result in storing many large files in the application database. The purpose of this filter is to limit the limit the size of such files.



Check the **Enable filtering** box to enable the filter. If you would like to temporarily disable the filter, uncheck this box.

Check the **Set file size** box and specify the required maximum file size in Megabytes in the corresponding field on the right.

The following options can be applied to the files that exceeding the specified limit:

- **Discard file content**- when enabled, NetResident discards the content of the captured file and sets the file size to zero. The program keeps a record of the captured file in the database, but the file content is unavailable.
-
- **Store part of file content** – when selected, only the part of file content is stored. The part above the file size limit is discarded.

PromiSwitch Tool

Note: Use this tool at your own risk. Never use this tool unless you are the network administrator of the LAN you are connected to. Using this tool may disrupt network connectivity. No technical support is available for this tool.

The PromiSwitch tool is designed for providing network visibility in switch-based networks where no port-mirroring option is available in the switches being used. Please refer to our white paper, [Promiscuous Monitoring in Ethernet and Wi-Fi Networks](#) for more information on this subject. This tool will attempt to ensure network visibility by taking advantage of the ARP protocol weaknesses. It is highly recommended that you use port mirroring rather than PromiSwitch whenever possible.

Start PromiSwitch and select the desired network adapter that will be used for station monitoring. Indicate the desired IP range by filling in the **Scan from:** and **Scan to:** fields, then click the **Start Scan** button. To abort the scanning process, click the **Stop Scan** button. After scanning completes, discovered workstations (including their IP and MAC addresses) will be shown in the list.

Check the boxes next to stations that you would like to monitor and click the **Start** button. The PromiSwitch tool will periodically send special network packets to selected stations. This will redirect the traffic between the gateway and the selected stations to your station, providing network visibility. You can also have the internal traffic between any two stations redirected to your station, which can be achieved by selecting **Internal** in the **Traffic** drop-down list and selecting two stations.

The **Options** window allows you to change some of the program's options, such as clearing the station list on new scan, automatic packet sending on start-up, and the interval between packets.

Frequently Asked Questions

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

Q. What is the difference between NetResident Lite and NetResident Pro?

Two license types are available for NetResident: Lite and Pro.

- Pro: All features are available.
- Lite: All features except VoIP support and the ability to import packet log files from other applications are available.

Q. I plan to install the NetResident service on one computer and then connect to it using the console from another computer. What should I do to comply with the license agreement?

A. According to the EULA, a single user license allows you to operate one copy of NetResident by one user account in the operating system. Installing and using the product on multiple computers, regardless of the installation or usage type (service or console) requires that you obtain the number of licenses corresponding to the number of installations.

Q. My HTTP plugin does not always display HTML pages correctly. For instance, some images are not displayed. Why is this so?

A. A typical HTML page represents a collection of a dozen of independent objects – HTML code, images, CSS styles, and others. A browser requests each of these objects; however, most of these objects are cached (saved to the computer hard drive for future access) and hence not requested from the network every time a Web page is viewed. NetResident does not have access to your browser's cache; therefore it cannot 'see' these objects. This is not a problem with NetResident; you can always reload the Web page in your browser (you need to perform a complete reload, in MSIE this is achieved by clicking on the Refresh button while holding down the Shift key). This will allow NetResident to log and store all Web page elements.

Q. Which address (IP or MAC) should I use in order to identify a station that I'd like to monitor?

A. If you have DHCP enabled in your network, each computer with a unique MAC address is assigned a different IP address for every session. In this case, you should identify your stations by MAC addresses. This will make the program assign all network events where the specified MAC address is present to the particular station and prevent the list of stations from becoming overpopulated. In some cases, you may encounter a different MAC address for each host. If you have a static IP address assigned to your network adapter and other stations on your LAN, you should use IP addresses to identify stations. We recommend using [aliases](#) for MAC and IP addresses as it makes recognition and analysis of network events much easier.

Q. When I try to import CommView or CommView for WiFi log files, I am unable to display the contents of some of the files. I believe I have all parameters set correctly regarding the event viewer and filtering.

A. It's important to understand that the import procedure has its own filter and the content displaying mechanism has its own filter. When you were importing the file, the content was possibly filtered out during the import phase if you applied filters. Once the import phase is over, the application uses the display filter to show the contents. There is a chance that the application is configured to show only the data collected during the last two days, while the logs contained sessions that were outside this time frame. You may want to disable the display filter to have the application show the data.

Q. Why NetResident service insists on starting if I just want to review LOG files and not capture current data?

A. The database is maintained by the service. The GUI is simply a console that "talks" to the service. All data processing and filtering is performed by the service as well, so it has to be running.

Q. I have NetResident set up to start monitoring only when the application is running, and not to start with Windows. I noticed that after I shut down NetResident, the service process, "tfsnrs.exe" continues to run in Task Manager. Why does it continue to run?

A. Running the service and monitoring are different things. The service must be active at all times to be able to "talk" to the GUI. This doesn't mean that the service is capturing data at all times. It is capturing data only on demand. In theory, if the application is configured to capture data only when the GUI is running, one could start the service when the GUI starts and stop it when the GUI stops, but starting the service is a bit slow and, most importantly, that cannot be done remotely, when the service and GUI are running on different machines. That is something we plan to implement in the future. The fact that the service is running in the background shouldn't worry you because when it's not monitoring the network it doesn't consume considerable system resources.

Q. Can you give some performance metrics when NetResident is being used to monitor a heavily loaded network?

A. The program's performance depends on the CPU speed and RAM size. If you use the default monitoring settings, i.e. when all the plugins are enabled and all the ports are being monitored, an average Pentium4 3Ghz PC with 512 Mbytes of RAM can monitor a fully utilized 100 Mbit link. To monitor faster network links, you should set up [filtering by station](#), limit the [ports](#) being monitored, and disable unnecessary [plugins](#). The performance also depends on the type of traffic being monitored, so additional filters should be applied only if you experience performance problems.

Q. For some ICQ and AIM chat sessions, one of the parties' ID number is shown as "Not detected." Why is it not detected?

A. This happens when an ICQ or AIM chat session (including the authentication phase) begins before NetResident starts capturing network packets. If capturing is started in the middle of a chat session, the ID can sometimes be found (as it is contained in some service packets, which are sent intermittently), although this cannot be guaranteed.

Q. Can your VoIP module be used for logging Skype conversations?

A. No, sorry. Skype uses robust encryption; it's impossible to decrypt Skype conversations.

Q. Why does NetResident not show the amount of transferred data in terms of bytes?

A. NetResident does not always store transferred data in its original form. Rather, it processes it for more convenient presentation. It's not uncommon for a single network session to be divided into several separate events, or several network sessions to be combined into one event. Besides, some transferred data simply is not supposed to be processed by current NetResident plugins. That said, NetResident cannot and is not supposed to display reliable network data statistics. If you're interested in network traffic statistics, you may want to use another TamoSoft product, [CommTraffic](#).

Q. I use WireShark and I noticed that it could no longer capture packets after NetResident had been installed.

A. There is a known conflict between WinPcap, the driver used in WireShark and many similar products, and the driver used in NetResident. There is a simple workaround: Start capturing packets with WireShark **before** you start capturing packets with NetResident. In this case, both products will be able to capture data simultaneously. If you start capturing with NetResident first, WinPcap will fail to capture any packets for a reason unknown to us.

Information

How to Purchase NetResident

This program is a 30-day evaluation version. If you would like to continue using it after 30 days, you must purchase it. Two license types are available for NetResident: Lite and Pro.

- Pro: All features are available.
- Lite: All features except VoIP support and the ability to import packet log files from other applications are available.

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 8140
New Zealand

Fax: +64 3 359 0392 (New Zealand)

Fax: +1 917 591 6567 (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 a 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](#)

CommView for WiFi

CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g/n networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry. CommView for WiFi captures every packet on the air to display important information such as a list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for WiFi can help you view and examine packets, pinpoint network problems, perform site surveys, and troubleshoot software and hardware.

[More information](#)

TamoGraph

TamoGraph is a powerful and user-friendly wireless site survey tool for collecting, visualizing, and analyzing 802.11 a/b/g/n Wi-Fi data. It provides information on signal strength, noise and interference, channel allocation, and data rates, etc. By using TamoGraph, businesses can dramatically reduce the time and costs that are involved in deploying and maintaining WLANs and improve network performance and coverage.

[More information](#)

CommTraffic

CommTraffic is a network utility for collecting, processing, and displaying traffic and network utilization statistics for network connections, including LAN and dial-up. It shows traffic and network utilization statistics for each computer in the segment. The software provides a very attractive and customizable interface, with an optional tray icon menu that displays general network statistics. You can also generate reports that reflect the network traffic volume and Internet connection expenses (if any). CommTraffic supports virtually any rate plan your ISP might use, such as one based on connection time, traffic volume, time of the day, or other measures. You can set alarms that will inform you when certain criteria (e.g. amount of traffic, expenses) are reached. A configuration wizard will guide you through the setup and automatically detect your network or connection settings.

[More information](#)

CountryWhois

CountryWhois is a utility for identifying the geographic location of an IP address. CountryWhois can be used to analyze server logs, check e-mail address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address. What makes CountryWhois different from similar tools is its very high accuracy (over 98%), unprecedented speed of processing (a 100 MB log file is processed within one second), regular updates that keep the ever-changing IP address database up-to-date, an array of supported import and export formats, command-line mode, and a convenient interface.

[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](#)

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. The program includes a NetStat utility that shows your computer's network connections and open ports and maps them to the owning application. It also features a fast NetBIOS scanner, a NetBIOS Auditing Tool for checking LAN security, and a monitor of external connections to your computer's shared resources, as well as a process monitor that displays information about all the programs and services running on your computer. Other useful tools are included, such as Ping, TraceRoute, and NSLookup. Additional features include report generation in HTML, text, and comma delimited formats and a customizable interface. The program is an easy-to-use and powerful replacement for such Windows utilities as nbtstat, netstat, and NetWatcher. It incorporates many advanced features that standard Windows tools can't offer.

[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](#)