



Colasoft Capsa User Manual

Colasoft Co., Ltd

Floor 10, Building 1, South Chengdu Hi-Tech Plaza,
3# West Fucheng Avenue, Hi-Tech Zone,
Chengdu 610041
P.R. China

Tel: +1 888-467-2634 (USA)
+86 28-8512-0922 (China)
Fax: +86 28-8512-0911

www.colasoft.com

Content

OVERVIEW	5
COLASOFT CAPSA , PROFESSIONAL AND ENTERPRISE	5
VERSION AND UPGRADE	6
<i>Checking version</i>	6
<i>Version upgrade</i>	7
<i>Edition upgrade</i>	7
INSTALL AND UNINSTALL	8
SYSTEM REQUIREMENTS.....	8
INSTALLATION AND CONFIGURATION.....	8
<i>Installation Environment</i>	8
<i>Switch and port monitoring</i>	12
<i>Installing Colasoft Capsa</i>	13
<i>Uninstall</i>	13
GETTING STARTED	14
LAUNCHING COLASOFT CAPSA	14
LICENSE INFORMATION.....	14
<i>Serial number</i>	15
<i>License key</i>	15
PRODUCT ACTIVATION.....	15
<i>Privacy statement</i>	15
<i>Confirmation ID</i>	16
REGISTRATION TO CUSTOMER SERVICE.....	17
USER WIZARD.....	17
START CAPTURE	19
PACKET CAPTURE	19
USING A PROJECT FOR CAPTURE AND ANALYSIS.....	20
<i>Blank project, saved project and project template</i>	20
<i>Opening multiple projects</i>	20
CAPTURE SOURCES	20
PROJECT WINDOW.....	23
<i>Menu bar</i>	24
<i>Toolbar</i>	26
<i>Context menus</i>	27
<i>Start Page</i>	27
<i>Dock windows</i>	28
<i>Tab views</i>	31
SYSTEM OPTIONS.....	54
<i>Options - General</i>	54
<i>Options – Format</i>	56
<i>Options - Decoder</i>	57

Options - Analyzer	58
RESTARTING CAPTURE.....	60
AUTOMATIC CAPTURE.....	61
PROJECT SETTINGS	62
PROJECT SETTINGS - GENERAL	62
PROJECT SETTINGS - ADAPTER	64
PROJECT SETTINGS - FILTER	66
PROJECT SETTINGS - NETWORK.....	68
PROJECT SETTINGS - LOG	70
Email log.....	71
FTP transfer log.....	73
HTTP log.....	74
DNS log.....	74
MSN Log.....	75
Other IM Logs	77
PROJECT SETTINGS - DIAGNOSIS	77
DATA MANAGEMENT	79
SAVING	79
COPYING AND PASTING	80
IMPORTING AND EXPORTING.....	80
PRINTING	83
STATISTICS.....	84
MATRIX	85
MATRIX DISPLAY OPTIONS.....	86
USER HIDDEN NODES	87
INVISIBLE NODES	88
DIAGNOSES.....	89
DIAGNOSIS REFERENCES - APPLICATION LAYER.....	89
DIAGNOSIS REFERENCES - TRANSPORT LAYER.....	91
DIAGNOSIS REFERENCES - NETWORK LAYER.....	93
DIAGNOSIS REFERENCES - DATA LINK LAYER.....	95
GRAPHS	96
GRAPHING STATISTICS	96
GRAPH DISPLAY OPTIONS.....	97
HIGHLIGHT AN ITEM	99
COMPARE MODE	100
SAVING GRAPHS.....	101
REPORTS	102
REPORTS OPTIONS.....	103
STATISTIC REPORTS.....	104
FILTERS	105

ADDING A PROJECT FILTER.....	106
ACCEPTING OR REJECTING A FILTER.....	107
SAVING, EDITING AND REMOVING A FILTER.....	108
IMPORTING AND EXPORTING FILTERS.....	109
SIMPLE FILTERS.....	110
ADVANCED FILTERS.....	114
FILTER TABLE.....	116
COMMAND LINE PARAMETERS.....	118
TCP RECONSTRUCTION.....	119
NAME TABLE.....	120
ADDING TO NAME TABLE	120
NAME TABLE WINDOW.....	121
LOGS.....	122
GENERATING LOG FILES.....	124
LOG FILE FORMATS	125
DECODING PACKETS	126
PACKET DECODERS.....	126
DECODE VIEW	127
HEX AND ASCII VIEW.....	128
TOOLS.....	130
COLASOFT PACKET BUILDER.....	130
<i>Packet list</i>	132
<i>Editing packet</i>	133
<i>Sending packet</i>	136
COLASOFT PACKET PLAYER.....	138
<i>Replay packet</i>	140
COLASOFT MAC SCANNER.....	142
<i>Scan network</i>	143
COLASOFT PING TOOL.....	145
<i>Ping multiple addresses/domains</i>	147
<i>Options</i>	149
EXTERNAL TOOLS.....	151
SEND PACKET.....	155
CUSTOMIZING USER INTERFACE	157
TOOLBAR	157
COLUMNS.....	158
SORTING DATA	159
DOCK WINDOWS.....	159
PERFORMANCE OPTIMIZA TION.....	160

Overview

Welcome to Colasoft Capsa.

Designed for packet decoding and network diagnosis, Colasoft Capsa monitors the network traffic transmitted over a local host and a local network, helping network administrators troubleshoot network problems. With the ability of real time packet capture and accurate data analysis, Colasoft Capsa makes your network transparent before you, letting you fast locate network problems and efficiently resolve hidden security troubles.

With the help of Colasoft Capsa, you can easily accomplish the following tasks:

1. Network traffic analysis
2. Network communication monitoring
3. Network problems diagnosis
4. Network security analysis
5. Network performance detecting
6. Network protocol analysis

Colasoft Capsa supports monitoring multiple adapters (enterprise edition only), letting you view the traffic passing through your network via different adapters.

Advanced analyzers provide more detailed information about network traffic, allowing you to view the analyzed data of email messages, FTP transfers, HTTP requests and DNS analysis.

Simple filters and advanced filters can narrow the target hosts, letting you quickly focus on suspect traffic and identify the source of network troubles.

Statistics and graphs let you view network communications in various ways, bring you an overall and visual impression of your network.

The featured Diagnoses list network diagnosis events and provide possible reasons and solutions; Matrix dynamically shows you mapped network traffic between network nodes, and Reports provide real time statistic reports of global network or specific groups.

Four built-in network tools Packet Builder, Packet Player, MAC Address Scanner and Ping Tool, make it possible for you to create, edit and send out packets, replay packet files, scan Mac addresses, ping IP addresses and domains during monitoring. In addition, external Windows applications or tools can be customized to add to the program.

Flexible and intuitive interface is the outstanding feature of Colasoft Capsa, you can easily switch from an overall statistics to the details of a specific network node, and even a rookie user can start to manage it in a few moments.

Colasoft Capsa, professional and enterprise

This manual serves for Colasoft Capsa 6.7 series, including two editions: professional and enterprise. The two share many features. When the text refers to "Colasoft Capsa" without further qualification, it applies equally to either edition.

The professional edition offers all the necessary features of a great network monitoring tool at an inviting price, it can meet IT professionals' basic needs in network traffic monitoring and protocol analysis.

The enterprise edition has many more advanced features than the professional edition, such as capturing loopback packets on local host, available statistic graphs and reports, advanced packets filters, simultaneously monitoring multiple adapters, etc.

Edition differences

The following table presents the main differences between Colasoft Capsa professional edition and enterprise edition. The features marked with Yes are available.

Feature		Professional Edition	Enterprise Edition
Adapters	Ethernet compatible adapters	Yes	Yes
	Loop-back adapters	N/A	Yes
Adapter amount opened in a project		One	Multiple
Network profile		N/A	Customizable
Summary statistics snapshot		N/A	Yes
Packet filters		Simple	Simple and Advanced
Graphs		N/A	Yes
Matrix		N/A	Yes
Reports		N/A	Yes
Network diagnoses		Yes	Yes

Version and upgrade

Version is a particular release of a software product. A version number is assigned by a software developer to identify a particular program at a particular stage, before and after public release. Successive public releases of a program are assigned increasingly higher numbers. Version numbers usually include decimal fractions. Major changes are usually marked by a change in the whole number (e.g. Colasoft Capsa 6.0 and Colasoft Capsa 5.0), whereas for minor changes only the number after the decimal point increases (e.g. Colasoft Capsa 5.2 and Colasoft Capsa 5.5).

A version may have a couple of editions, whereas an edition may be involved in different versions of a software product. Actual deployment features vary by product edition. In Colasoft Capsa version 5.0 and latter, the editions are professional and enterprise.

Colasoft Capsa has two kinds of upgrade: version upgrade and edition upgrade, each is subject to specific policy. You are always welcome to upgrade your product from a previous version to the latest one, whatever the upgrade is major or minor, or from the edition professional to enterprise.

Checking version

You can easily check your product version or the latest version of Colasoft Capsa.

- **Current version**

In some cases when you contact Colasoft you are required to provide your product version. To check product version, open **Help** menu and choose **About Colasoft Capsa....**

- **Checking for the latest version**

Colasoft suggests you to check for the latest version regularly. You may click **Colasoft Home Page** in the **Help** menu or visit <http://www.colasoft.com/analyzer/> to get the latest upgrades information.

Version upgrade

You can free upgrade your product to a newer version if your purchased maintenance hasn't expired when the newer version is released. Otherwise you need to purchase a renewal maintenance.

The maintenance doesn't affect the use of product, if you wouldn't like to renew your product, you are allowed to continue using the purchased version.

Edition upgrade

You can upgrade your product from an inferior edition to an advanced edition. For example, if you purchase Colasoft Capsa professional originally and would like to upgrade it to Colasoft Capsa enterprise, you just need to pay the price difference between these two editions.

Install and Uninstall

Colasoft Capsa is easy to install and configure for a variety of operating environments. This chapter describes the minimum system requirements for Colasoft Capsa and presents recommended configuration according to different network scale. It illustrates how to install the program in various environments, explains how to configure your system to get desired network data and gives some topologic examples.

Note: Please do not install Colasoft Capsa on a public machine or server to prevent unauthorized access to the program.

System requirements

Colasoft Capsa can be installed on many Windows operation systems, such as Windows 2000, Windows XP and Windows 2003. Your system's performance and configuration will affect the running status of Colasoft Capsa. The following minimum requirements are the base line to install and run Colasoft Capsa normally; it would be better if your system has a higher configuration, especially in a busy or big network.

Minimum requirements:

- P3 500 CPU
- 256 MB RAM
- Windows 2000 (SP 4 or later), Windows XP (SP 1 or later), Windows 2003 (SP2 or later), Windows Vista and x64 Edition
- Internet Explorer 5.5 or higher

Recommended requirements:

- P4 3.0G CPU
- 512 MB RAM or more
- Windows 2000 (SP 4 or later), Windows XP (SP 1 or later), Windows 2003 (SP2 or later), Windows Vista and x64 Edition
- Internet Explorer 5.5 or higher

Notes:

- Supports Windows XP/2003 x64 Editions.
- Dual CPU servers are not supported.
- You are required to have the "Administrator" level privileges on supported operating system in order to load and unload device drivers, or to select a network adapter for using the program to capture packets.

Installation and configuration

Colasoft Capsa can monitor and analyze the data transmitted in intranet and/or between intranet and extranet, or over VLAN; however, only with correct installation and configuration can the program work properly. The following sections introduce how to install and configure Colasoft Capsa in different network environments, including shared network and switched network.

Installation Environment

Shared network and switched network are two common network environments today, before install Colasoft Capsa, you should first know about the topology of your network.

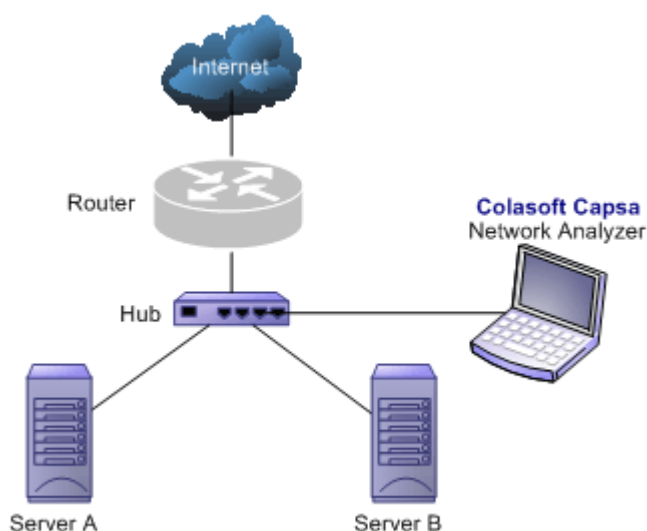
- **Shared network**

A shared network is also known as hubbed network which is connected with a hub.

Hubs are commonly used to connect segments of a LAN. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. A passive hub serves simply as a conduit for the data, enabling it to go from one device (or segment) to another. So-called intelligent hubs include additional features that enable an administrator to monitor the traffic passing through the hub and to configure each port in the hub. Intelligent hubs are also called manageable hubs. A third type of hub, called a switching hub, actually reads the destination address of each packet and then forwards the packet to the correct port.

With a shared environment, Colasoft Capsa can be installed on any host in LAN. The entire network data transmitted through the Hub will be captured, including the communication between any two hosts in LAN.

Topology illustration 1:



- **Switched network**

Switch is a network device working on the Data Link Layer of OSI. Switch can learn the physical addresses and save these addresses in its ARP table. When a packet is sent to switch, switch will check the packet's destination address from its ARP table and then send the packet to the corresponding port.

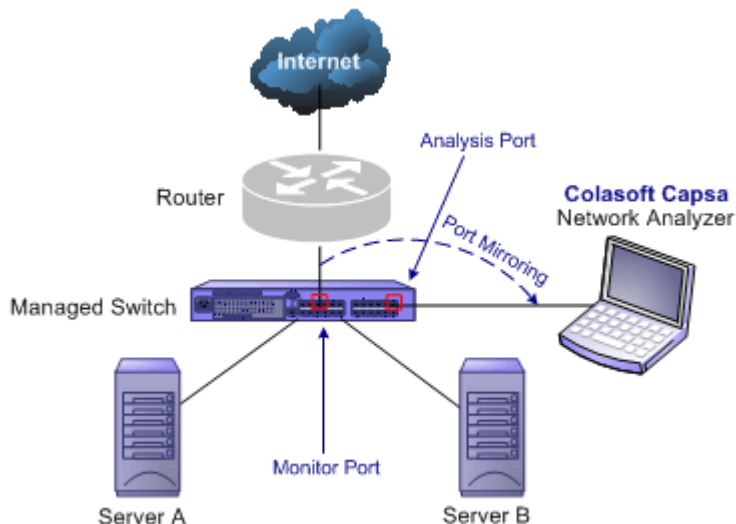
- **Network with managed switches**

Generally all three-layer switches and partial two-layer switches have the ability of network management; the traffic going through other ports of the switch can be captured from the debugging port (mirror port/span port) on the core chip. To analyze the traffic going through all ports, Colasoft Capsa should be installed on this debugging port (mirror port/span port).

The following table presents the advantages and disadvantages of using a switch with mirror port.

Advantage	Disadvantage
No additional facility required No need to change network topology	Occupies a switch port Possible influence to network transmission performance when meeting huge traffic

Topology illustration 2:



◦ Network with unmanaged switches

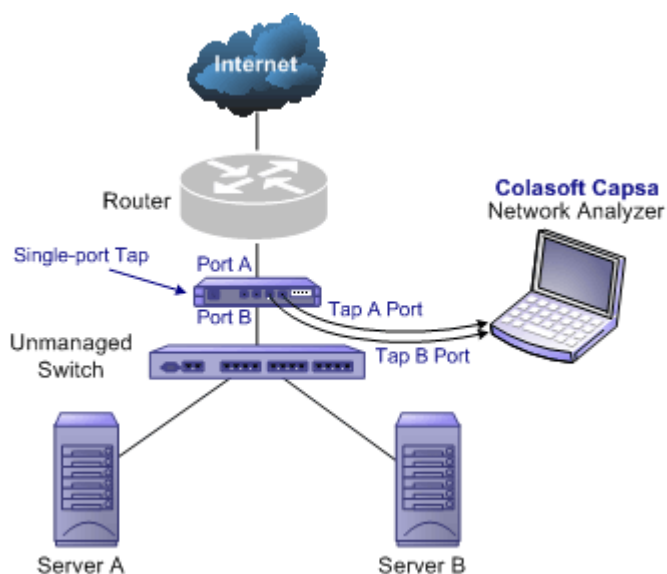
If your switch has no management function, you can:

Connect a tap with the line to be monitored

Taps can be flexibly placed on any line in network. When the requirement for network performance is very high, you can add a tap to connect your network. The following table presents the advantages and disadvantages of using a tap.

Advantage	Disadvantage
No influence to network transmission performance	High cost
No interference with data stream and raw data	Additional facility (tap) required
Does not occupy IP address, free from network attacks	Requires dual adapters
No need to change network topology	Can not connect Internet

Topology illustration 3:

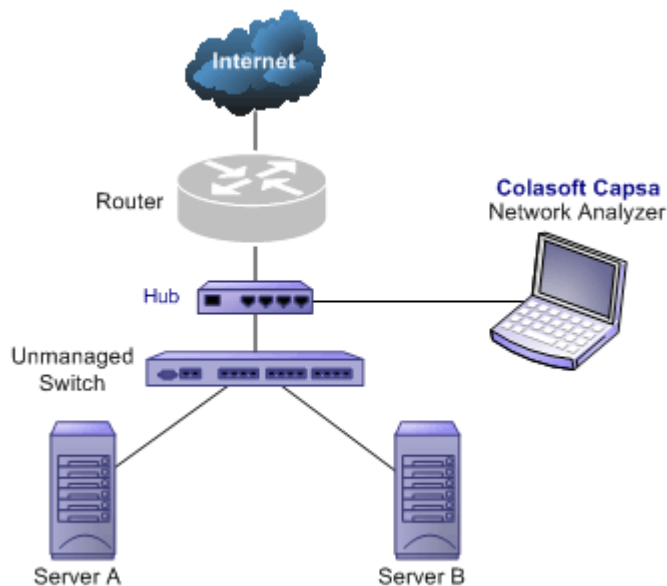


Connect a hub with the line to be monitored

Working on share mode, hubs are applicable for small networks.

Advantage	Disadvantage
Low cost No need to be configured No need to change network topology	Additional facility (hub) required Interference to network transmission performance when meeting huge traffic Not applicable for big networks

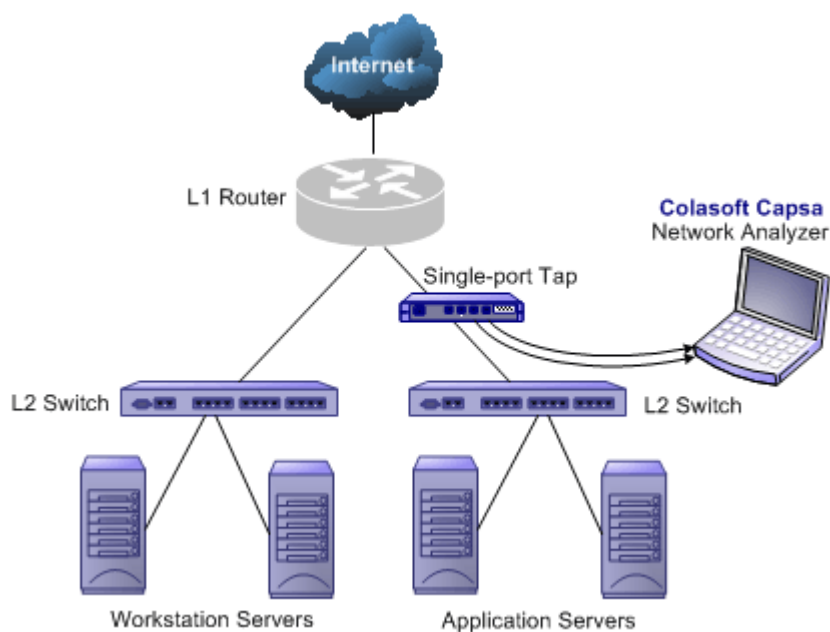
Topology illustration 4:



- Monitoring a network segment**

In the case when you only need to monitor the traffic in a network segment (e.g. Finance department, Sales department, etc.), you can connect the server on which Colasoft Capsa is installed and the network segment with a exchange facility. The exchange facility can be hub, switch or proxy server.

Topology illustration 5:



Note: Commonly management switches have the function of port mirroring (spanning); however, the port mirroring configuration of one brand's switch may differ from others, please refer to the documentation that comes with your switch for information on the availability of this feature and the configuration instructions.

Switch and port monitoring

Switch is a network exchange facility operating at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model. Classified by working protocols, there are two-layer switch, three-layer switch, four-layer switch and multiple-layer switch. Switch also can be classified into managed switch and unmanaged switch. Generally, three-layer switch and above has management function (managed switch).

Unlike hubs, switches prevent promiscuous sniffing. In a switched network environment, Colasoft Capsa (or any other Colasoft Capsa) is limited to capturing broadcast and multicast packets and the traffic sent or received by the PC on which it is running.

However, most modern switches (management switches) support "port mirroring", which is a feature that allows you to configure the switch to redirect the traffic that occurs on some or all ports to a designated monitoring port on the switch. With this feature, you can monitor the entire LAN segment in switched network environment. Please refer to the documentation coming with your switch for the availability information about this feature and configuration instructions.

If your switch does not support "port mirroring", you can install Colasoft Capsa on a workstation connected to the same hub as your Internet gateway, or on your Internet gateway (if acceptable), thus you can monitor all network traffic between your intranet and the Internet.

A list of some managed switches (with port monitoring/spanning) which are commonly used is available on our website.

Configuring a switch

Colasoft Capsa should be installed on the host/server connected with the switch's mirror port (span port).

Mirror port configuration:

- Mirror the way out port to the management port (mirror port), in this way the entire data transmitted into/out of LAN can be monitored.
- Mirror all way out ports to the management port (mirror port), in this way not only the entire data transmitted into/out of LAN but also the communication among hosts in LAN can be monitored. (Recommend)

Note: Different brands' switches may apply different mirror port configurations, please refer to the instructions coming with your switch.

The following are two examples for CISCO switch using the "monitor" command in configuration mode:

Format:

#monitor session number source interface mod_number/port_number

#monitor session number destination interface mod_number/port_number

Examples:

Mirror session 1: mirror port 1-10 to port 12

#monitor session 1 source interface 1/1-10

#monitor session 1 destination interface 1/12

Mirror session 2: mirror port 13-20 to port 24

#monitor session 2 source interface 2/13-20

#monitor session 2 destination interface 2/24

Change the corresponding parameters when there are multiple mirror sessions or modules.

Installing Colasoft Capsa

Before install Colasoft Capsa, please carefully read the system requirements and the ReadMe file that comes with the program. To avoid possible incompatibilities, it is recommended that you uninstall any earlier or trial version of Colasoft Capsa and close all running applications.

Installation Process:

- When you launch the installation file, the first window you will see is the Welcome screen, telling you that Colasoft Capsa will be installed on your machine.
- Read the **License Agreement** carefully in the next screen to understand our terms and conditions concerning possession and use of Colasoft Capsa. You must accept the terms of the license agreement to continue the installation.
- The next screen presents the important information from the ReadMe file.
- The next **Select Destination Location** dialog suggests the default location in which to install Colasoft Capsa. Use the browse button to designate an alternate installation location.
- The next **Select Components** dialog for you to select install which build-in tool listed in this page.
- Select a start menu folder in the next screen. Use the browse button to designate an alternate start menu folder.
- Select **Additional Tasks** in the next screen.
- Now you are Ready to Install Colasoft Capsa on your machine. Click **Install** to start installation.
- When installation is complete, the final setup complete screen is displayed. From this dialog, you may choose to view the ReadMe file or launch the program.

Uninstall

To uninstall Colasoft Capsa and its components, select one of the following:

- Choose **Uninstall** from Colasoft Capsa program group.
- Open the **Control Panel** window and double click the **Add/Remove programs** icon, search the list for **Colasoft Capsa** and then remove it.

Getting Started

After install Colasoft Capsa on your machine, there are a few more things to do before it can start capturing packets. This chapter describes how to launch the program and make it available for packet capture.


Launching Colasoft Capsa

You can launch Colasoft Capsa using the following ways:

- **Launch from the setup wizard**

Select **Launch Colasoft Capsa 6.x** when you finish setup to start the program immediately.

- **Launch from the desktop**

Check the option **Create a desktop icon** in the setup wizard, an additional icon of **Colasoft Capsa**  will be placed on your desktop. To start the program, just double click on the icon.

- **Launch from the quick launch menu**

Check the option **Create a Quick Launch icon** in the setup wizard, then you can start it from the quick launch menu in the task bar.

- **Launch from the Start menu**

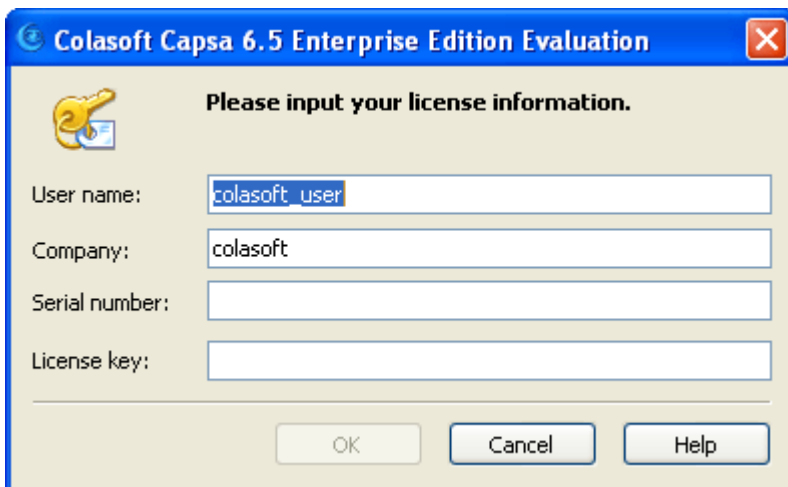
Open the **Start** menu and select **All Programs**, then click the program name from **Colasoft Capsa 6.x enterprise/Professional**.

- **Invoke from command line**

Use the *Capsa.exe [/command1 <file>]* format to invoke Colasoft Capsa.

License information

When you run Colasoft Capsa for the first time, a dialog will pop up requiring you to enter license information.



The image shows a Windows-style dialog box titled "Colasoft Capsa 6.5 Enterprise Edition Evaluation". It has a yellow question mark icon in the top-left corner. The main text says "Please input your license information." Below this, there are four text input fields: "User name:" (containing "colasoft_user"), "Company:" (containing "colasoft"), "Serial number:" (empty), and "License key:" (empty). At the bottom, there are three buttons: "OK", "Cancel", and "Help".

Please enter your serial number and license key correctly. Your license information will be remembered and the dialog will not

appear again unless you reinstall Colasoft Capsa.

Serial number

A serial number is used for the identification of Colasoft Capsa to avoid usage of counterfeit license keys. When you finish payment, a delivery email with the serial number, license key and other product information enclosed will be sent to you. For the first time you run the program or if you reinstall the program, you will be required to enter the serial number. It must match with the corresponding license key, otherwise you could not unlock the product.

Note: Please keep your serial number in a safe place. You will need to provide it when you activate product by email/fax, or register to the [Colasoft Customer Service](#).

License key

A license key is an authorization number indicating that Colasoft grants you the right to use this program. When you finish payment, a delivery email with serial number, license key and other product information enclosed will be sent to you. For the first time you run the program or if you reinstall the program, you will be required to enter the serial number.

The license key is a private number, if you lose your license key, you can retrieve it from the [Colasoft Customer Service](#), or contact service@colasoft.com.

Product activation

Colasoft Product Activation is an anti-piracy technology designed to verify that software products have been legitimately licensed. This aims to reduce a form of piracy known as casual copying. Activation also helps protect against hard drive cloning. Activation is quick, simple, and unobtrusive, and it protects your privacy.

Product Activation works by verifying that a software program's license key has not been used on more personal computers than intended by the software's license. You must use the license key and a serial number in order to install the software and then it is transformed into an installation ID number. You use an activation wizard to provide the installation ID number and serial number to Colasoft either through a secure transfer over the Internet, or by fax/email. A confirmation ID is sent back to your machine to activate your product.

If you overhaul your computer by replacing a substantial number of hardware components, it may appear to be a different PC. You may have to reactivate Colasoft Capsa. It is allowed to reactivate the program no more than five times per day.

Privacy statement

The Colasoft Product Activation is an anti-piracy technology designed to verify that the software products have been legitimately licensed.

When you activate Colasoft Capsa over the Internet, you are not required to send any personal information to Colasoft, the product activation is completely anonymous.

When you activate Colasoft Capsa by fax or email, you are required to send the serial number and installation ID number displayed on your screen to Colasoft. The installation ID number includes an encrypted form of the product ID and a hardware hash, or checksum. No personally identifying data is included or required. The confirmation ID is simply an unlocking code for the Colasoft Capsa installation on that particular PC. The information that you provide will be securely stored by Colasoft and will be protected

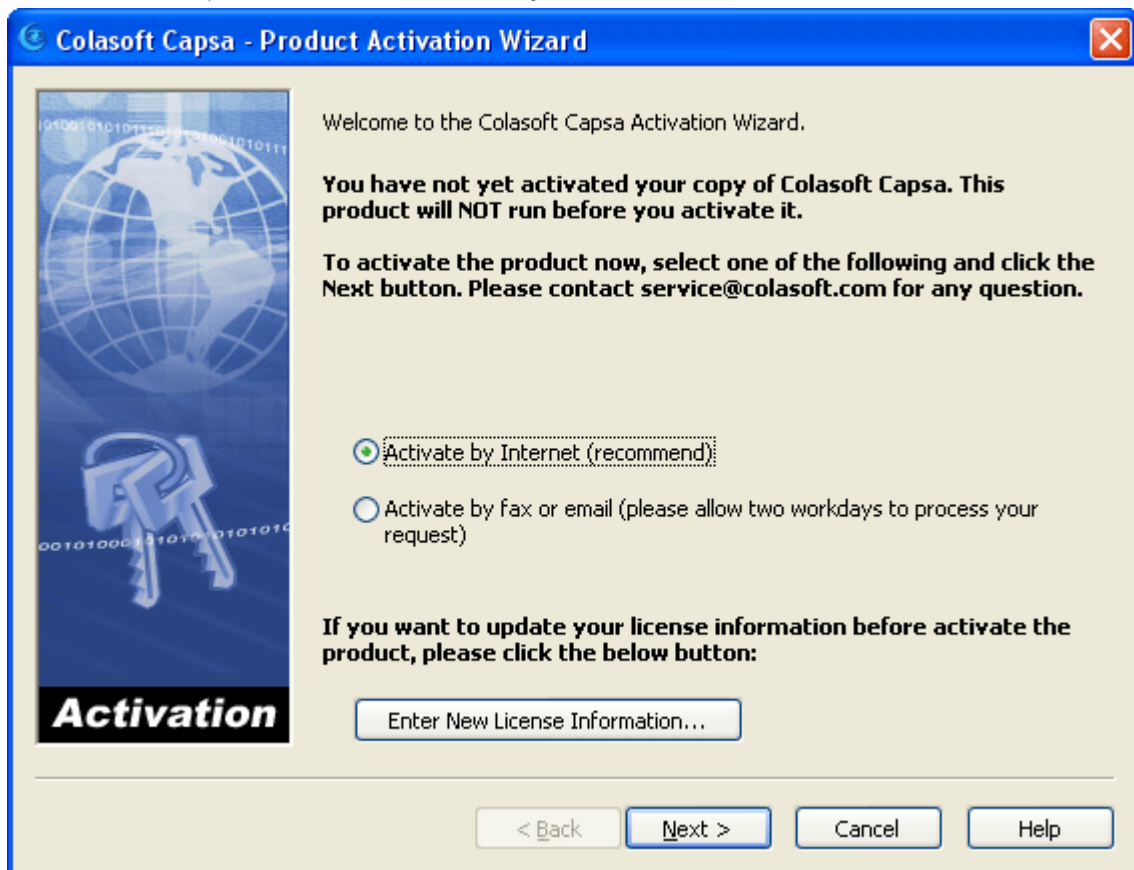
from disclosure to any third parties without your consent.

During the product activation process, Colasoft creates a unique hardware identification that represents the configuration of the PC at the time of activation. The hardware identification does not include any personal information, any information about software or the data that may reside on your PC, or any information about the specific make or model of your PC. The hardware identification identifies only the PC and only for the sole purpose of product activation. Colasoft Capsa can detect the minor changes to your PC configuration. You will be required to reactivate product if you reinstall operating system or use Colasoft Capsa on another PC.

Confirmation ID

The confirmation ID is very important to activate your product successfully. You can only run Colasoft Capsa for no more than 15 times before it is activated.

After you correctly enter the serial number and license key, a dialog will appear to require you to activate your product. You may choose to activate product over the Internet, or by fax or email.

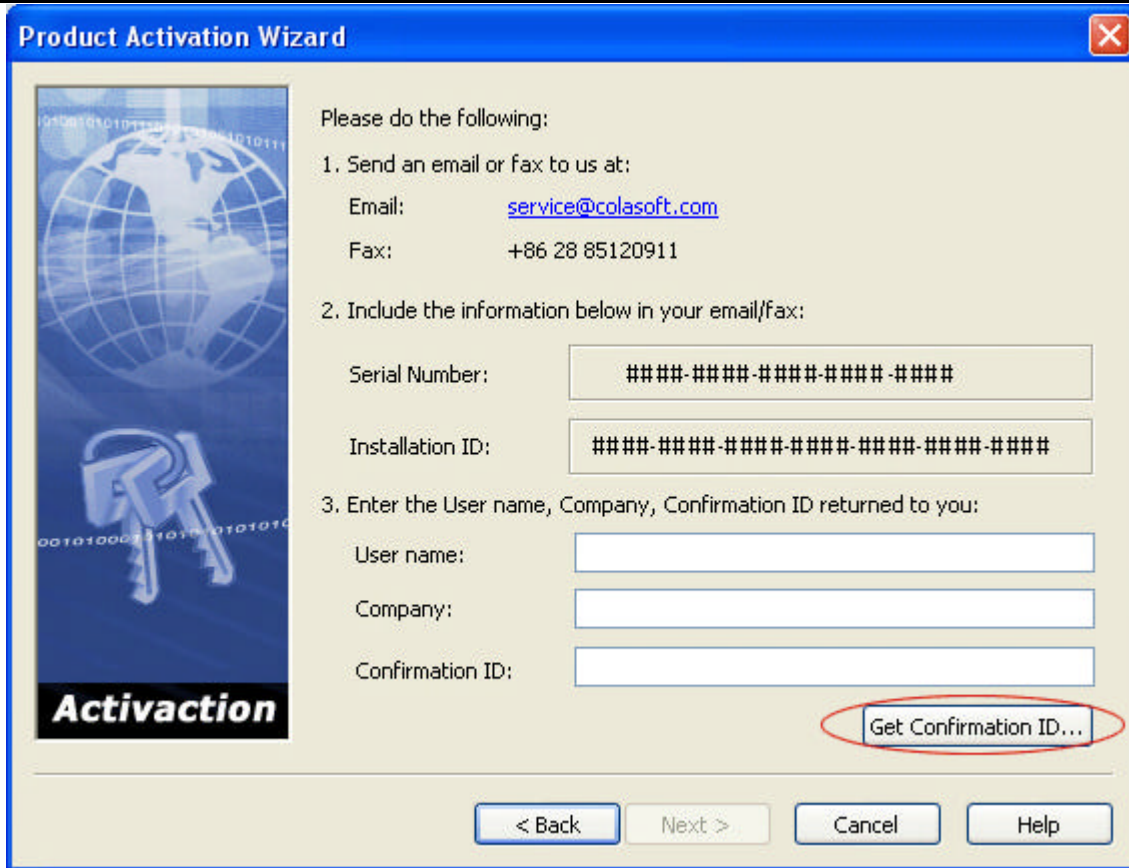


- **Activate product over the Internet (recommend)**

It is very quick and easy, the activation process will only take a few seconds with a couple of clicks.

- **Activate by fax or email**

If you select to activate product manually, it will need more time to finish. Please click the **Get Confirmation ID...** button showed on the third page of the product activation wizard. After receiving your request, an IE window will be opened and show you the Confirmation ID created by our system. Enter the **Confirmation ID** as required, your product will be activated immediately.



The image shows a 'Product Activation Wizard' window. On the left is a graphic with a globe and the word 'Activation'. The main area contains instructions and input fields. Step 1 shows contact information. Step 2 shows fields for 'Serial Number' and 'Installation ID', both containing placeholder text. Step 3 shows fields for 'User name', 'Company', and 'Confirmation ID'. A 'Get Confirmation ID...' button is circled in red. At the bottom are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

Product Activation Wizard

Please do the following:

1. Send an email or fax to us at:
Email: service@colasoft.com
Fax: +86 28 85120911
2. Include the information below in your email/fax:
Serial Number: #####-#####-#####-#####
Installation ID: #####-#####-#####-#####-#####-#####
3. Enter the User name, Company, Confirmation ID returned to you:
User name:
Company:
Confirmation ID:

Get Confirmation ID...

< Back Next > Cancel Help

Or, please provide us the **Serial Number** and **Installation ID** showed on the second page of the product activation wizard. We will send back your confirmation ID as soon as possible.

Registration to Customer Service

When you run the program for the first time a dialog will appear to remind you to register your product. You are recommended to register your product at your earliest convenience for getting timely customer services from Colasoft, please check the first option to connect with the Colasoft website for an immediate registration.

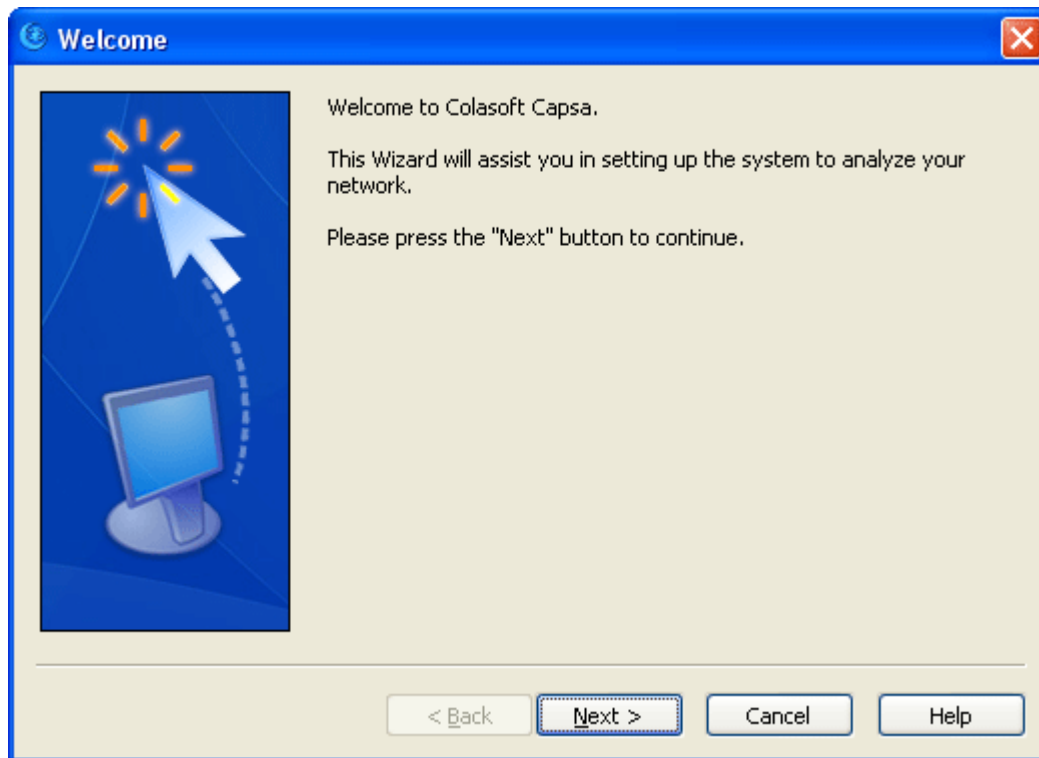
After registration and log in, you can download the latest release or gain the license key for new version, review your product, retrieve license key, change your profile and get other services from Colasoft.

You may also use the following URL:

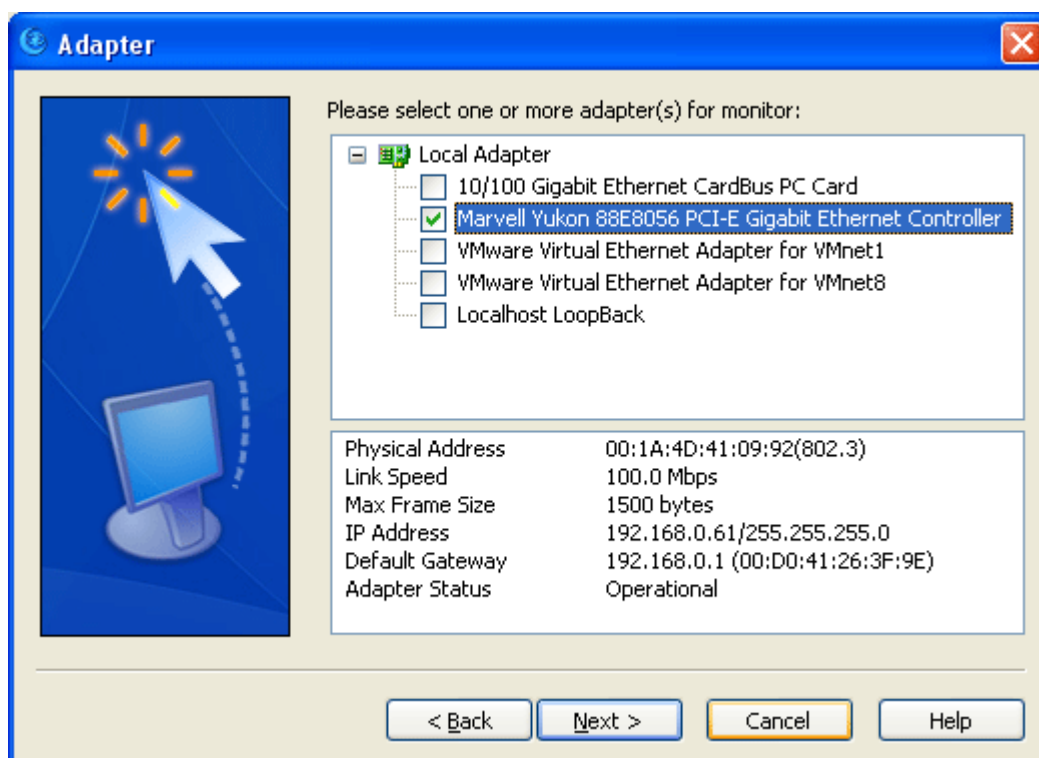
https://secure.colasoft.com/customer/main.php?module=customer_cp&action=register.

User Wizard

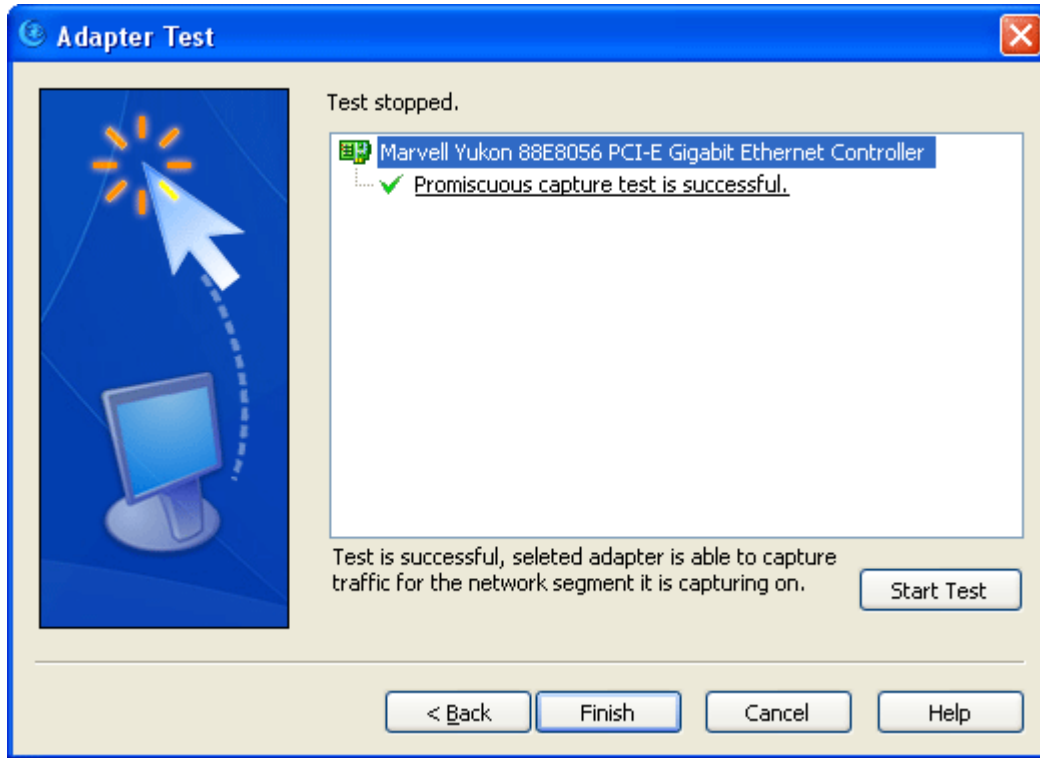
This Wizard will appear upon the first run of the program after its installation, providing adapter setting and adapter test options.



Adapter Selection: you can select multiple adapters.



Adapter Test: test the adapter/adapters selected in the previous page.





- The green tick means the test is successful.
- The red cross means the test is failed.
- The yellow exclamation mark means the test is in process and there are already some test results. More details can be seen if you move your Mouse to the Item.

Test duration is displayed at the bottom. There is no limit for test duration, you have to stop it manually.

When test is over, whether it is successful or not, the time display will be replaced by a description of the test result. If you press **Next** before the test is over or without pressing Stop button, a prompt will pop up to notify you "stop testing first".

User Wizard allows you to select and test adapter/adapters to check out whether the installation and the deployment is correct.

Start capture

Colasoft Capsa stands by if it does not receive a start capture command. To start capturing packets, click the **Start Capture Now** button in the **Start Page**, or click the icon  in the toolbar. The label on the icon will change to **Stop Capture**  when capture is under way.

Alternatively, you can select the **Start Capture** or **Stop Capture** command from the **Project** menu. You can also start and/or stop capture using command line parameters. You will be required to assign adapter before packets are captured and analyzed, see the **Packet Capture** chapter to get more descriptions about how to select adapter and how to view captured results.

Packet Capture

Colasoft Capsa can capture packets from multiple adapters, once you give it the **Start Capture** instruction and designate the adapter, it starts capturing packets in a project. You can open two or more projects to focus on different packets, each project has

its own settings and parameters. This chapter introduces how to select a capture source for a project, how to view captured packet information and how to save results for future analysis or comparison.

Using a project for capture and analysis

A project is a scheme of capture settings and a container for captured data. You can save a project to hard disk for reuse at a later time. Project is an essential ingredient in Colasoft Capsa, you must create a new project or open an existing project before you start capturing packets or performance other functions.

Colasoft Capsa captures network traffic and analyzed packets on the conditions of project settings. Without project, you could not do anything even just view old data. Therefore the first thing you should do after launch the program is to create/open a project. You can choose to create a blank project, select a project template or open an existing project. Details are described in below sections.

Blank project, saved project and project template

For the first time to use Colasoft Capsa, you can simply click the **Start Capture Now** button to automatically apply the predefined settings for capture. You don't need to set project settings, except you have to select the adapter for this project. Each time when you create a new project, you may always use the blank project to save the time for setting. If you want to change the settings during capture, you could click the **Adapter**, **Filter** or **Analyzers** icon in the toolbar, or **General Settings...** from the Project menu to open the **Project Settings** dialog, and after alteration, save the project or save it as a template.

You can open a saved project (if applicable) with its data and settings from the **Start Page** or by clicking the **Open** icon; but when you start capture, Colasoft Capsa will clear or reset some contents in the project buffer.

Colasoft Capsa supports project templates, you can first customize the settings for a project and then save it as a template. Project templates can be easily loaded from the **Start Page**.

Opening multiple projects

Colasoft Capsa allows you to open multiple projects for focusing on different packets, each project has its own project window, capture adapter and project settings, which requires you to operate individually.

Multiple projects let you compare your network under different conditions, helping you find out network problems more easily. For example, when you have two network segments, you can open two projects: *Project 1* focuses on segment 1 and *Project 2* focuses on segment 2.

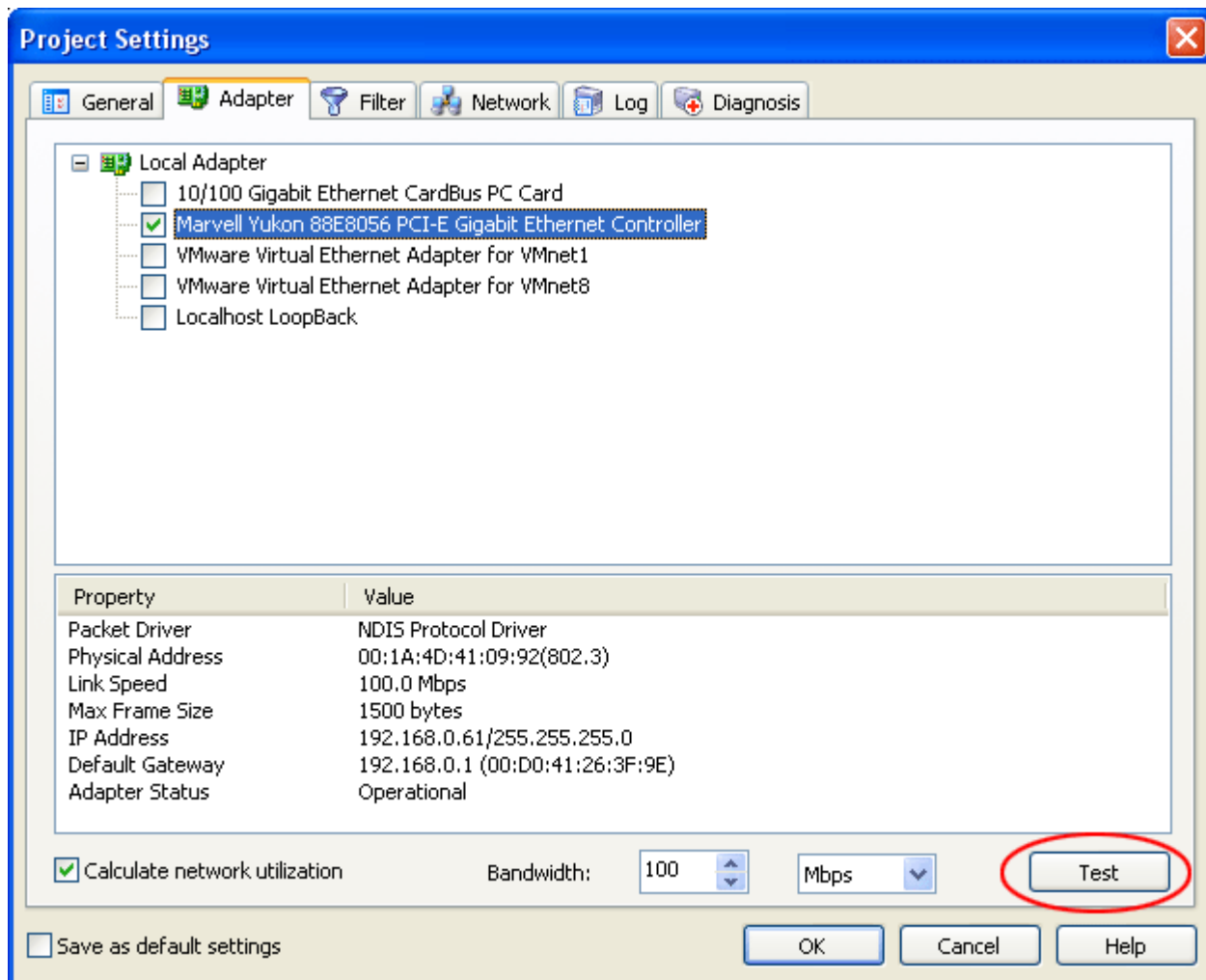
Note: It may reduce your system performance if you open multiple projects and capture packets simultaneously.

Capture sources

For the first time when you start a capture, you must designate the adapters for the project. Even if you only have one adapter, you still need to confirm it. If you check the option **Always show project settings when start capture** in the **Project Settings - General** page, Colasoft Capsa will remember your adapter selection and in the future capture, will not require you to select again.

Colasoft Capsa supports capturing packets from multiple adapters simultaneously (unique to enterprise edition). To start capture, you must select a valid adapter at a minimum. All supported adapters are listed in the **Project Setting - Adapter** page, you can highlight an adapter to see its property information in the lower pane. The adapter selected will be marked with a tick in the check

box.



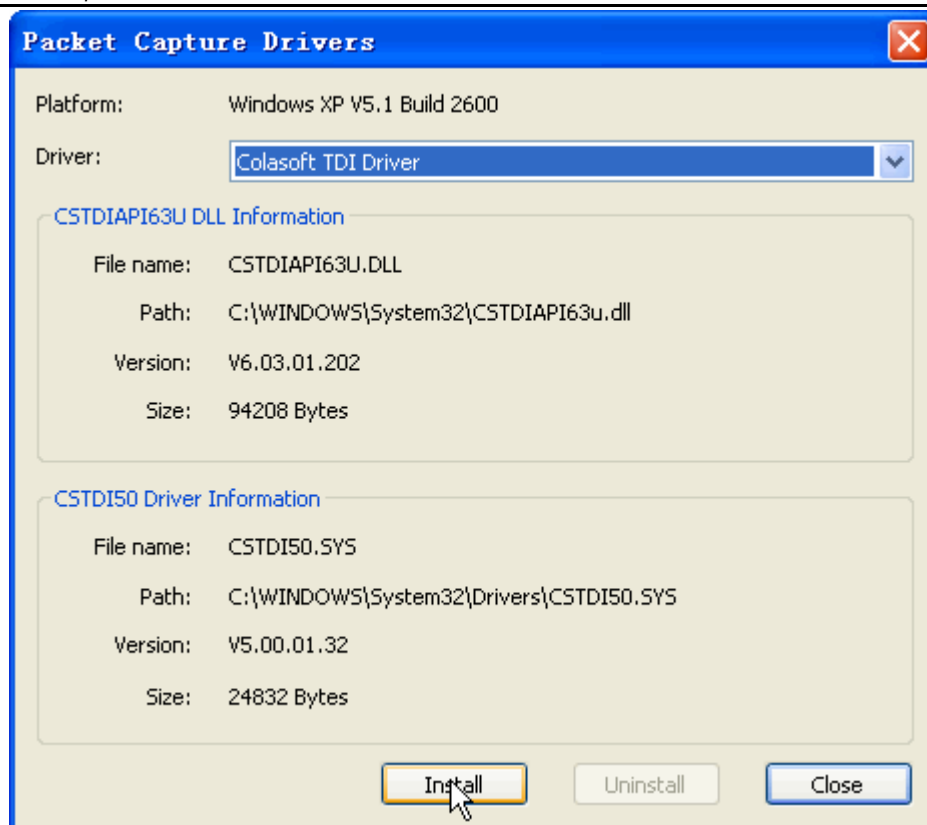
Colasoft Capsa can capture packets from the following sources:

- **Ethernet adapters**

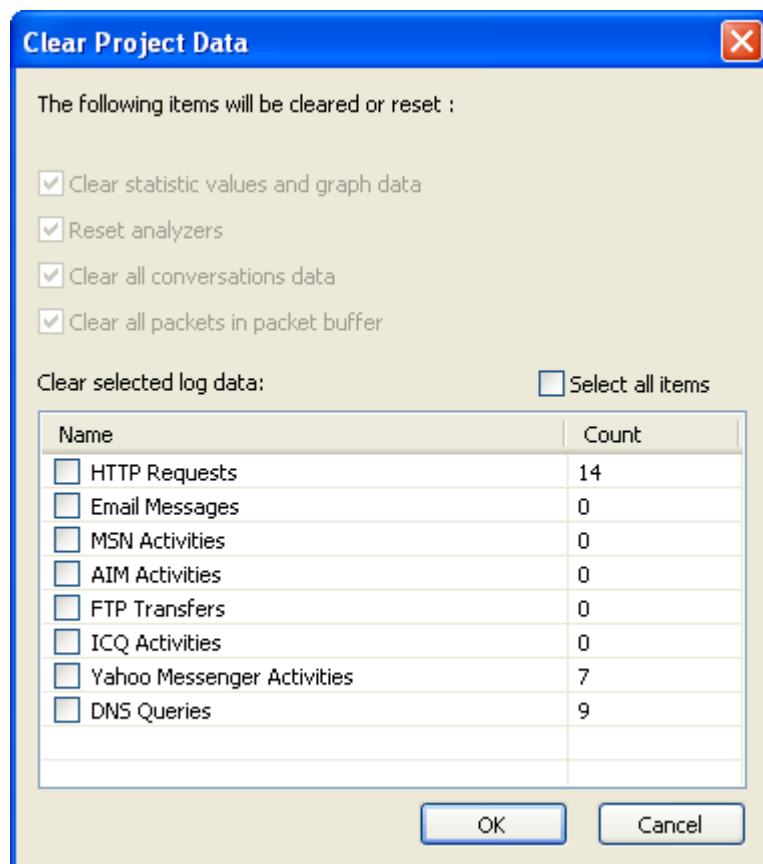
Colasoft Capsa works with the most of common Ethernet adapters in marketplace.

- **Localhost TDI loopback traffic**

Colasoft Capsa can capture The TDI loopback traffic on your local host, but you must install the Colasoft TDI Driver first: open the **Tools** menu and click **Packet Capture Drivers...**, select **Colasoft TDI Driver** from the **Driver** combo box and push **Install**. After finish the installation, your localhost LoopBack adapter will be added to the Local Adapter list in the Project Setting - Adapter page.



It is allowed to change adapters during the capture process; however, some data in the project buffer will be cleared or reset if you do so.



Project window

The project window of Colasoft Capsa is composed of the following components:

- **Window title**

The window title shows the product name and the active project's name.

- **Menu bar**

The menu bar provides many useful commands in Colasoft Capsa.

- **Toolbar**

The toolbar contains the buttons for the most commonly used menu commands, you can add or remove the toolbar buttons.

- **Start Page**

The start page is the first screen you can see when you begin a new capture, which offers some common project operations.

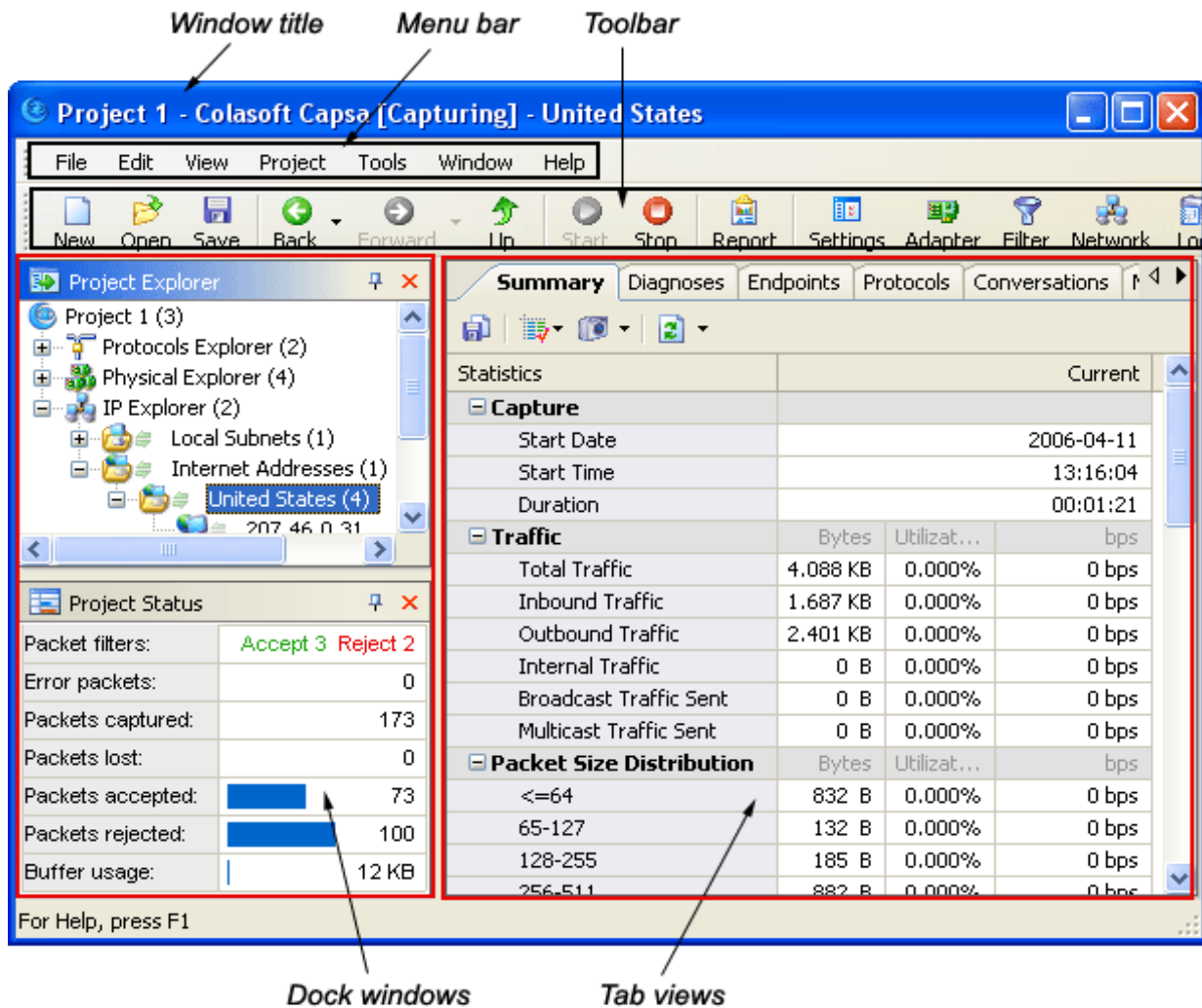
- **Dock windows**

At the left section of user interface by default, the dock windows include **Project Explorer** and **Project Status**. The project explorer dock window lists all network nodes and protocol nodes, letting you quickly select a target to view related information in tab views. The project status dock window offers the overview information of project.

- **Tab views**

Including **Summary**, **Diagnoses**, **Endpoints**, **Protocols**, **Conversations**, **Packets**, **Matrix**, **Logs**, **Graphs** and **Reports** view, each presenting different information of the same node selected from the project explorer dock window.

More descriptions about these components can be found in the sections below.



Menu bar

This is a listing of Colasoft menus, with a brief description of each item's function. Menu items followed by suspension points (for example, **Save As...**) open a dialog or window. You can make menu choices either by navigating the menus or by using the Ctrl key combinations shown beside certain items in the menus.

Command	Hot Key	Description
File menu		
New	Ctrl+N	Creates a new project.
New From Template...		Opens a new project from the saved templates.
Open...	Ctrl+O	Opens an existing project.
Save	Ctrl+S	Saves the current project to a file.
Save As...		Saves the current project with a new name.
Save As Template...		Saves the current project as a template.
Close		Closes the current project.
Print...	Ctrl+P	Prints the current window in a format appropriate to its type.

Print Preview		Previews the print effect.
Print Setup...		Configures printer functions in the Print Setup dialog.
Import Packet File...		Imports the packets saved in a packet file to the current project.
Export Packet File...		Exports the packets in the current project to packet file.
Recent File		A list of recently opened packet files, with the most recently opened listed first. You can select a file from this list to open it.
Exit		Quits Colasoft Capsa.
Edit Menu		
Cut	Ctrl+X	Cuts the selection and copies to the clipboard.
Copy	Ctrl+C	Copies the selection to the clipboard.
Paste	Ctrl+V	Pastes the current contents of the clipboard.
Delete	Del	Deletes the current selections from Colasoft Capsa.
Find...	Ctrl+F	Finds a specific item in the Project Explorer dock window and Endpoints, Protocols, Packets, Conversations and Logs views.
Find Previous	Shift+F3	Backs to the previous packet if applicable.
Find Next	F3	Goes to the next packet if applicable.
Select All	Ctrl+A	Selects all items in the current window.
View Menu		
Toolbar		Contains many convenient icons for menu commands.
Status Bar		Displays status alerts in a bar at the bottom of the project window.
Go To		Chooses a condition to jump to.
Project Explorer		Hides or shows the Project Explorer dock window.
Project Status		Hides or shows the Project Status dock window.
Show Adapter Vendor		Hides or shows the adapter vendor where displays the Mac address.
Show Host Name		Shows the alias for hosts.
Show Port Name		Shows the alias for ports.
Refresh	F5	Refreshes the contents of the current view.
Project Menu		
Start Capture	F2	Starts capturing packets. When capture is under way, the item is displayed as inactive.
Stop Capture		Stops capturing packets. The item is displayed as active when capture is under way.
Clear Packet Buffer...		Discards all the packets in the packets buffer.
Clear Project Data...		Opens the Clear Project Data dialog and the selected items will be cleared.
General Settings...		Opens the Project Settings - General dialog.
Choose Adapter...		Opens the Project Settings - Adapter dialog.
Packet Filter...		Opens the Project Settings - Filter dialog.

Network Profile...		Opens the Project Settings - Network dialog.
Log Setting...		Opens the Project Settings - Log dialog.
Diagnosis Setting...		Opens the Project Settings - Diagnosis dialog.
Tools Menu		
Name Table		Opens the Name Table window.
Filter Table		Opens the Filter Table window.
Packet Capture Drivers...		Opens the Packet Capture Drivers dialog where you can install additional drivers for packet capture.
Colasoft Ping Tool		Opens the Colasoft Ping Tool dialog to ping one or more IP addresses and domain names.
Colasoft Packet Player		Opens the Colasoft Packet Player dialog to replay packet files.
Colasoft Mac Address Scanner		Opens the Colasoft Mac Address Scanner dialog to scan the IP address and Mac address in subnet.
External Tools		Opens the Custom Tools dialog to invoke other applications or tools.
Options...		Opens the Options dialog.
Window Menu		
New Window		Opens an additional window for viewing the information of the current project.
Close		Closes the current project window.
Next		Switches to the next window in sequence the current window.
Previous		Switches to the previous window in sequence the current window.
At the bottom of the Window menu is a numbered list of open windows, with a checkmark beside the name of the current or front-most window. Selecting a window from this list makes it the current window and brings it to the front of the display.		
Help Menu		
Contents		Launches the contents page of the Help documentation.
Search...		Launches the help search
Index		Launches the help index.
Technical Support		Loads the technical support page of the Help documentation.
Activate Product...		Launches the product activation wizard.
Check for Latest Version		Opens the Colasoft website to check for the latest version available.
Colasoft on the Web		Opens the Colasoft website, where you can check for the latest version, register product, send feedback, visit the Colasoft home page or the protocol website.
About Colasoft Capsa...		Opens the About Colasoft Capsa window where you can find the version, copyright and license information of the product.

Toolbar

The toolbar provides the button navigation for frequently-used tasks in Colasoft Capsa. By default, each button appears with an icon and a name presenting its function; to hide the text, open the **View** menu and move the cursor over **Toolbar**, then uncheck **Icon Text**.



You can add more buttons to the toolbar. Choose **Customize...** from the **View - Toolbar** menu to open the **Customize** dialog. Alternately, you can right click on the toolbar and choose **Customize....** The **Customize** dialog lets you manage add-in items that appear in the toolbar. To remove buttons from the toolbar, click the **Toolbar Options** at the right of the toolbar, then move the cursor over the **Add or Remove Buttons** and the **Standard** command, then uncheck the buttons you would not like to appear in the toolbar.

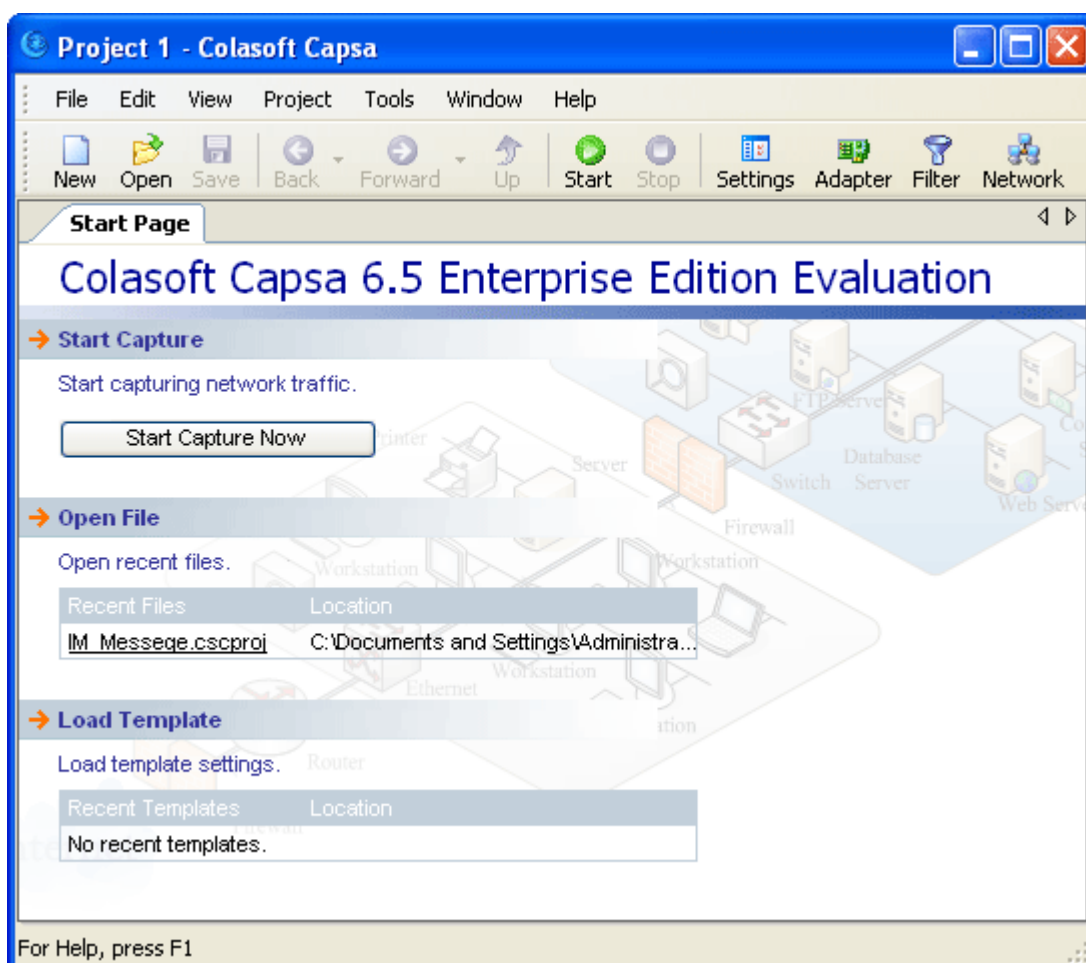
To hide the toolbar, right click on the toolbar and uncheck **Standard**.

Context menus

Many features of Colasoft Capsa can be launched from the context menus. With a right click on the display, you can open the context menu bar which contents vary with the current view or current selection. The context menus are described with corresponding display in the **Dock windows** and **Tab views** section below.

Start Page

Each time when you open a new project, you can see a start page which offers some quick links of the most common project operations:



- **Start Capture**

You can immediately start capturing packets by clicking the **Start Capture Now** button, Colasoft Capsa will automatically apply the predefined settings of the blank project.



- **Open File**


You can open a recently saved project file from the list; some contents in this project buffer will be cleared or reset when you start capturing new packets.

- **Load Template**

Colasoft Capsa supports project templates, you may save a project as template. When you open a template, Colasoft Capsa will load its settings for capture.

Dock windows

Colasoft Capsa has two flexible dock windows: **Project Explorer** and **Project Status**, you can hide them or change their position very easily. To hide a dock window, just click the  icon at the top of the dock window, it will dwindle into a button on the left of project window (by default) and will not show its contained information unless you place your mouse cursor on it. To recover the display, keep your mouse on the button and when the dock window appears, click the  icon again.

A dock window can also be closed if you click the  icon, you can open it again by clicking its name in the **View** menu or the icon from the toolbar.

To change the position of a dock window, you may push your mouse cursor on it and keep the left button down when dragging it. It will go back to the previous position if you double click on the name pane.

The following is the common commands contained in the context menu of dock windows, which can be opened with a right click in anywhere of a dock window.

Command	Description	Applicability
Copy (Ctrl+C)	Copies the selection as a text file and puts it on the clipboard.	Project Explorer dock window
Copy Tree	Copies the data tree as a text file and puts it on the clipboard.	Project Explorer dock window
Hide Project Explorer	Unshows the Project Explorer dock window.	Project Explorer dock window
Add to Name Table...	Adds or edits an alias.	Project Explorer dock window
Resolve Host Name	Resolves the name of the selected host.	Project Explorer dock window
Expand All Subnodes	Shows all subnodes.	Project Explorer dock window
Collapse All Subnodes	Unshows all subnodes.	Project Explorer dock window
Find	Finds an item in the Project Explorer .	Project Explorer dock window
Find Next	Finds next item in the Project Explorer .	Project Explorer dock window
Refresh	Refreshes the current view.	Project Explorer dock window
Show Value	Shows data in value.	Project Status dock window

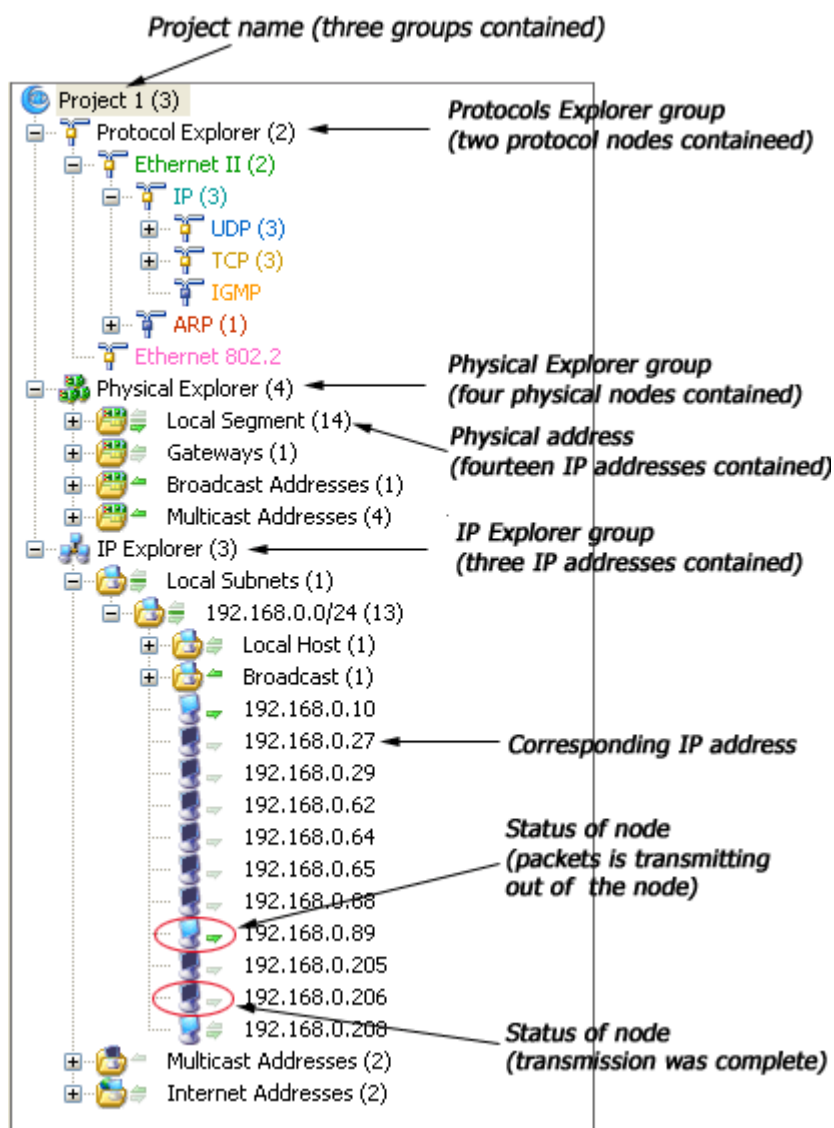
Show Percentage

Shows data in percentage.

Project Status dock window

Project explorer

The **Project Explorer** dock window is on the left section of project window by default, which allows you to view the current status of each node and quickly switch among global statistics and the details of specific network nodes; you can not see it if no project is created or opened. There are three groups in the project explorer: **Protocol Explorer**, **Physical Explorer** and **IP Explorer**.



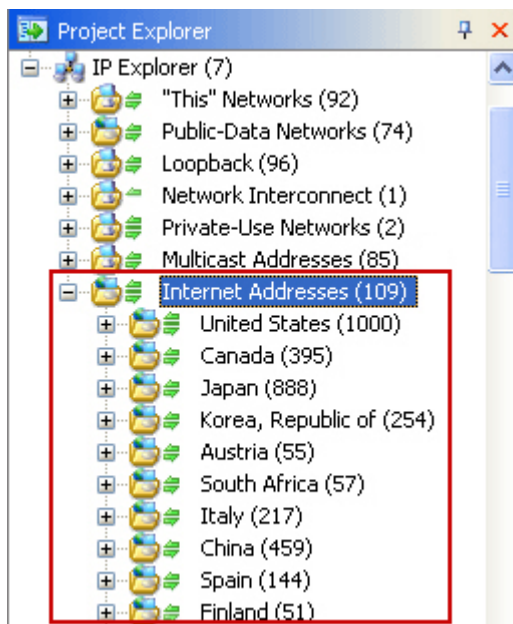
Name	Description
Protocol Explorer	This group lists network endpoints by protocol.
Physical Explorer	This group lists network endpoints by physical address. There are four sub-groups: Local Segment , Gateways , Broadcast Addresses and Multicast Addresses .
IP Explorer	This group lists network endpoints by IP address. There are four sub-groups: Local Subnets , Private-Use Networks , Broadcast Addresses , Multicast Addresses and Internet Addresses .

In the **Physical Explorer** and **IP Explorer** group, the arrows on the right of the each node's icon indicate the current status of

the node. The node's icon and the arrows will green when the node transmitting packets and become to grey when transmission complete. The upper arrow indicates packets transmitted in, the below one indicates packets transmitted out from the node.

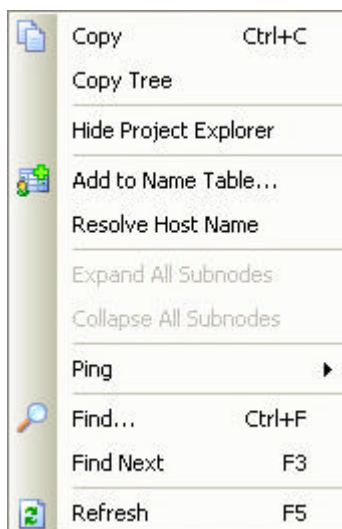
The number in bracket indicates the amount of the sub-nodes. Colasoft Capsa can list up to 1000 sub-nodes. If a node has more than 1000 sub-nodes, e.g. 2000, then the node will be showed as xxx (2000) when collapsed and xxx (1000/2000) when expanded.

Furthermore, the captured addresses will be grouped under countries in the **Internet Addresses** of **IP Explorer** group if you check the **Group IP address by its country** in the **General** page of **Project Settings** dialog.



The **Project Explorer** dock window and the tab views on the right section of project window are consistent in displaying data. When you select a node in this dock window, the data displayed in tab views changes accordingly.

The figure below is the right-click context menu of this dock window. In addition to the common context commands, there is special command in this context menu - **Ping**. The **Ping** command used to invoke the build-in ping tool to ping the IP address of the selected node in the **Physical Explorer** and **IP Explorer** group.



The name of listed hosts can be resolved manually with the **Resolve Host Name** command from the context menu with a right

click on the display. It is also allowed to make alias and change text color from this dock window.

Project status

The **Project Status** dock window presents some general information of the current project.

Project Status	
Packet filters:	Accept 3 Reject 0
Error packets:	0
Packets captured:	31,788
Packets lost:	0
Packets accepted:	100%
Packets rejected:	0%
Buffer usage:	79.97%

Item	Description
Enabled filters	Shows the number of accepted filter and rejected filter.
Packets captured	Shows the total number of captured packets since the capture started.
Packets lost	Shows the number or percentage of lost packets.
Packets accepted	Shows the number or percentage of packets matching the filters accepted for analysis, the progress bar displaying the proportion of the packets accepted in the total packets captured.
Packets rejected	Shows the number or percentage of packets matching the filters excluded for analysis, the progress bar displaying the proportion of the packets rejected in the total packets captured.
Buffer usage	Shows the buffer memory used so far in packet capture as a number or percentage, and graphically by a progress bar which fills more of the width of the display as memory is used: when 80% of the capture buffer is used, the color of the bar changes from blue to yellow, eventually showing red as memory use approaches 100%.

The items **Packets dropped**, **Packets accepted**, **Packets rejected** and **Buffer usage** can be displayed either as value (by default) or percentage, you can select from the context menu with a right click. In addition, with double clicks on the **Enabled filters**, **Packets accepted** and **Packets rejected** item, Colasoft Capsa will open the **Project Settings - Filter** page, or **Project Settings - General** page for the **Buffer usage** item, in which you can modify the settings of filter or buffer usage. The **Project Status** window can be hidden and its position is alterable

Tab views

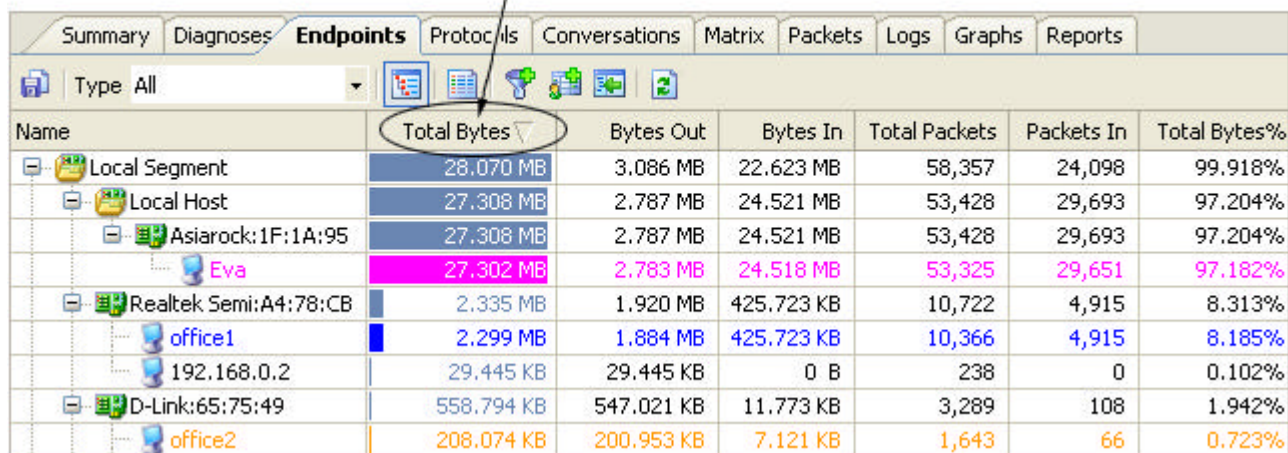
Colasoft Capsa has seven tab views, each focusing on different network information. The table below offers the main usage of these views.

Tab View	Description
Summary	Presents the summary statistics of global network or specific network nodes.
Diagnoses	Presents the diagnosis events of global network or specific network nodes.
Endpoints	Categorizes and displays network traffic by hierarchical endpoints, physical endpoints, or IP endpoints.
Protocols	Categorizes and displays network traffic by protocol.

Conversations	Shows the Physical, IP, TCP and UDP conversations between pairs of endpoints, the reconstruction of TCP streams is available.
Matrix	Shows the network traffic between two nodes in real time. The nodes were arranged in an elongated ellipse and lines between communicating nodes indicate the traffic.
Packets	Shows a list of captured packets in the order they were received and offers the detailed information of packet decode.
Logs	Records the network communications of email messages, HTTP requests, FTP transfers, DNS analysis, MSN activities, AIM activities, ICQ activities and Yahoo Messenger activities. Primarily from any enabled advanced analyzers.
Graphs	Presents a variety of graphs displaying network statistics in real time, based on the node you select from the Project Explorer dock window and consistent with the Summary view. You can use the Compare Mode to view two different graphs simultaneously.
Reports	Displays the real time statistics of summary statistics, diagnosis events and top 10 addresses, and all available graphs.

Each tab view (except the **Graphs** view, **Matrix** view and **Reports** view) has its own column/sub-column options, you can right click on the column heading bar and select more columns to display. In the **Endpoints** view, **Protocols** view and **Conversations** view, with a click or double clicks on a column heading, you can sort the data in this column by ascending or descending, which helps you easily find the source of top traffic.

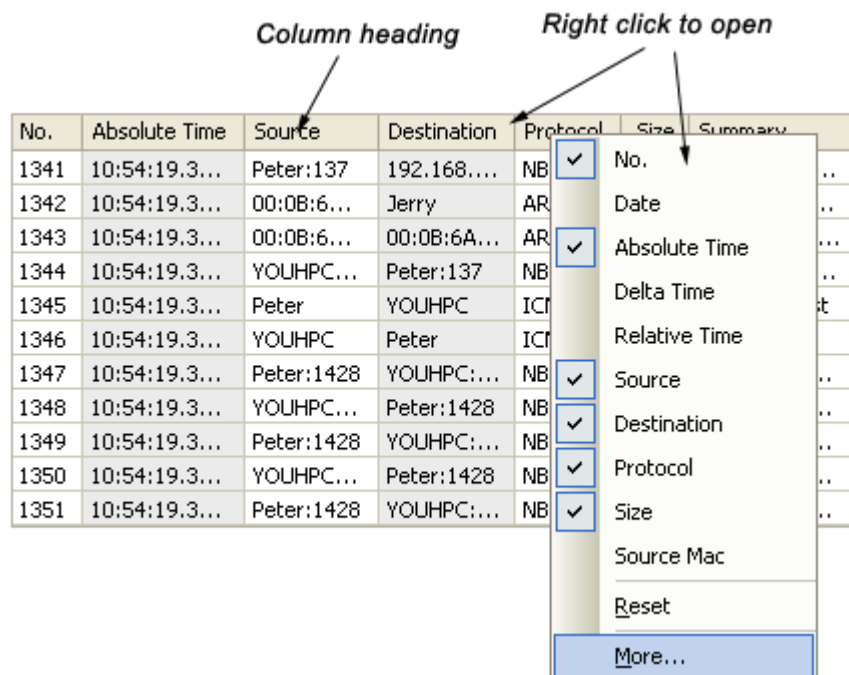
Sort endpoints by Total Bytes



Summary	Diagnoses	Endpoints	Protocols	Conversations	Matrix	Packets	Logs	Graphs	Reports
Type All									
Name	Total Bytes	Bytes Out	Bytes In	Total Packets	Packets In	Total Bytes%			
Local Segment	28.070 MB	3.086 MB	22.623 MB	58,357	24,098	99.918%			
Local Host	27.308 MB	2.787 MB	24.521 MB	53,428	29,693	97.204%			
Asiarock: 1F:1A:95	27.308 MB	2.787 MB	24.521 MB	53,428	29,693	97.204%			
Eva	27.302 MB	2.783 MB	24.518 MB	53,325	29,651	97.182%			
Realtek Semi: A4:78:CB	2.335 MB	1.920 MB	425.723 KB	10,722	4,915	8.313%			
office1	2.299 MB	1.884 MB	425.723 KB	10,366	4,915	8.185%			
192.168.0.2	29.445 KB	29.445 KB	0 B	238	0	0.102%			
D-Link: 65:75:49	558.794 KB	547.021 KB	11.773 KB	3,289	108	1.942%			
office2	208.074 KB	200.953 KB	7.121 KB	1,643	66	0.723%			

You can switch among various views to see different packet information of a specific node by first selecting the node from the **Project Explorer** dock window. If you find a suspicious item in a tab view, the **Locate Explorer Node** command in the context menu (except the **Summary** view, **Graphs** view and **Reports** view) is able to let you find and highlight its location in the **Project Explorer** dock window by IP address, physical address or protocol, and at the same time, other tab views accordingly display the relevant information of this node.

The columns showed in tab views can be customized; you may show/hide specific columns or change the position of a column.



The following is the common commands contained in the context menu of tab views, which can be opened with a right click in anywhere of a tab view. The particular context commands of each view are described in the sections below.

Command	Description	Applicability
Copy (Ctrl+C)	Copies the selection as a text file and puts it on the clipboard.	All tab views except Graphs view, Matrix view, Reports view.
Copy Column	Copies the selected column as text and puts it on the clipboard.	Endpoints view, Protocols view, Packets view, Conversations view, Logs view.
Custom Columns	Shows/hides columns or changes the position of columns.	Endpoints view, Protocols view, Packets view, Conversations view, Logs view.
Locate Explorer Node	Locates the current node in the Project Explorer .	Endpoints view, Protocols view, Packets view, Conversations view, Matrix view, Logs view.
Make Filter...	Opens the Packet Filter dialog and makes a new filter on the basis of the selection.	Endpoints view, Protocols view, Packets view, Conversations view, Matrix view, Logs view.
Add to Name Table	Adds or edits an alias.	Endpoints view, Packets view, Conversations view, Matrix view, Logs view.
Select All	Selects all items.	All tab views except Graph view, Matrix view, Reports view.
Refresh	Refreshes the current view.	All tab views except Graph view.

Summary view

Associated with your selection in the **Project Explorer**, the **Summary** view provides general statistic information of the selected node. When you select the project root node, you can get the statistics of your global network; if you select a specific network node, the view will present the particular information of this node.

Display Options

Save as Take snapshot Refresh Sub-column

Summary Diagnosis Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports

Statistics Current

Capture

Start Date	2007-08-16
Start Time	16:17:57
Duration	00:00:24

Physical Errors

802.3 Errors

Traffic

	Bytes	Packets	Utilization	bps	pps
Total Traffic	1,639 KB	22	0.003%	2,624 ...	4
Broadcast Traffic Sent	262 B	1	0.000%	0 bps	0
Multicast Traffic Sent	0 B	0	0.000%	0 bps	0

Packet Size Distribution

	Bytes	Packets	Utilization	bps	pps
<=64	1,188 KB	19	0.001%	1,024 ...	2
65-127	200 B	2	0.002%	1,600 ...	2
128-255	0 B	0	0.000%	0 bps	0
256-511	262 B	1	0.000%	0 bps	0
512-1023	0 B	0	0.000%	0 bps	0
1024-1517	0 B	0	0.000%	0 bps	0
>=1518	0 B	0	0.000%	0 bps	0

TCP Packets

TCP Connections

DNS Analysis

SMTP Analysis

POP3 Analysis

FTP Analysis

HTTP Analysis


All Instant Messenger Activities

MSN Activities

AIM Activities

ICQ Activities

Yahoo Messenger Activities

By default, only some sub-columns are displayed. To view more statistic information in different columns, right click in the display and put the mouse pointer on **Choose Current Sub-columns** and then check columns from the context menu. Alternately, you can use the icon  to check more sub-columns.

The following table shows the information titles presented in the **Summary** view (when the project root node is selected).


Title	Description
Capture	Offers the information of start date, start time and duration of this capture.
General Errors	Offers the statistics of general errors, including total errors, CRC errors, alignment errors, overrun errors and underrun errors.
Physical Errors	Offers the statistics of physical errors.
802.3 Errors	Offers the statistics of 802.3 errors.
Traffic	Offers the information of total traffic, broadcast traffic and multicast traffic.
Packet Size Distribution	Offers the statistics of packets based on size class.

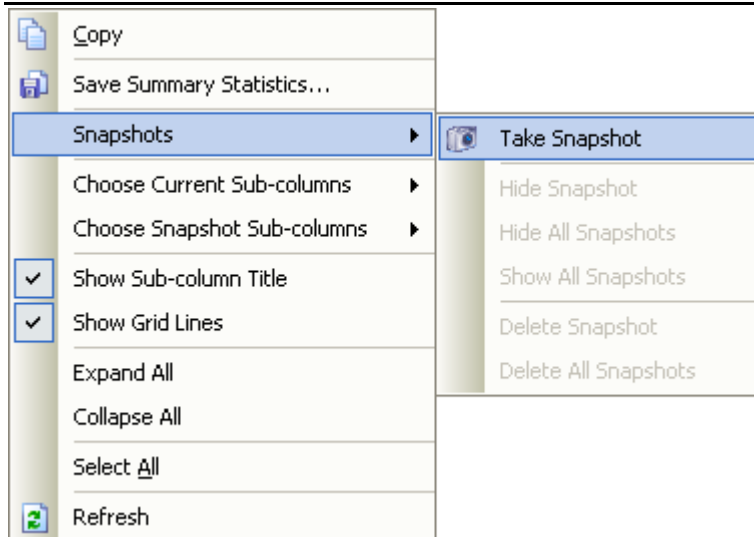
Most Common Packet Sizes	Offers the packet statistics of the most common sizes.
TCP Packets	Offers the statistic information of TCP packets analyzed by the TCP analyzer.
TCP Connections	Offers the statistic information of TCP connections analyzed by the TCP analyzer.
DNS Analysis	Offers the statistic information of DNS connections analyzed by the DNS analyzer.
SMTP Analysis	Offers the statistic information of SMTP connections and messages analyzed by the advanced Email analyzer.
POP3 Analysis	Offers the statistic information of POP3 connections and messages analyzed by the advanced Email analyzer.
FTP Analysis	Offers the statistic information of FTP transfers analyzed by the advanced FTP analyzer.
HTTP Analysis	Offers the statistic information of HTTP requests analyzed by the advanced HTTP analyzer.
All Instant Messenger Activities	Offers the statistic information of all instant messenger activities.
MSN Activities	Offers the statistic information of MSN activities.
AIM Activities	Offers the statistic information of AIM activities.
ICQ Activities	Offers the statistic information of ICQ activities.
Yahoo Messenger Activities	Offers the statistic information of Yahoo Messenger activities.

Click on the + (plus) or - (minus) signs at the left margin to expand or collapse individual items of the display.

In addition to the common context commands as other tab views, this view also has the following special commands:

Command	Description
Save Summary Statistics...	Saves the summary statistics to a file.
Snapshots	Takes a snapshot for summary statistics; shows, hides or deletes a snapshot.
Choose Current Sub-columns	Chooses the columns to show corresponding statistics.
Choose Snapshot Sub-columns	Chooses the columns to take snapshot.
Display Sub-column Title	Displays the title of the sub-columns.
Display Grid Lines	Displays the grid lines for the view.
Expand All	Expands all items and displays the sub-columns.
Collapse All	Collapses all items and hides the sub-columns.

You can take snapshots for the summary statistics at any time, which will be very helpful if you want to compare your network state in the future. To get snapshots, click the icon  or right click on the view to open the context menu, select the **Snapshots** command and **Take Snapshot** from the sub-context menu. Repeat the operations to take multiple snapshots. There is no limit to the snapshots taken, but you can only see up to 16 snapshots on the display.



Diagnoses view

The **Diagnoses** view presents the diagnosis events of global network or selected network node. You can find a diagnosis statistics according to network layers from the upper view, whereas the corresponding events are listed in the lower subview, each event is assigned a severity level. By double clicking on an event, Colasoft Capsa will open an **Event Relative Packets** window showing the related packet information to this event. To get a detailed description and remedy suggestion, push the **References** tab in the lower subview (if applicable).

The diagnosis settings can be customized in the **Project Settings - Diagnosis** page by clicking the  button from the toolbar.

Save As Display options Refresh

Summary **Diagnoses** Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports

Name	Count
All Diagnosis Events	8,078
Application Layer	132
Transport Layer	2,366
TCP Connection Refused	28
TCP Fast Retransmissions	1
TCP Port Scan	2
TCP Repeated Connect Attempt	2,084
TCP Reset Connection	245
TCP Retransmissions	4
Network Layer	17,200
ICMP Port Unreachable	4
IP Low Time-To-Live	17,196

Events





0 0 0 0

All Diagnosis Events: 8,078

Seve...	Layer	Event	Destination	Packet
Information	Application ...	HTTP Server Slow Response Time (321 ms From Packet 4...	202.106.18...	46196
Notice	Network La...	IP Low Time-To-Live (See Packet 46200)	227.1.2.7	46200
Warning	Transport L...	TCP Repeated Connect Attempt (See Packet 44744)	192.168.7.77	46201
Notice	Network La...	IP Low Time-To-Live (See Packet 46204)	227.1.2.7	46204

Show events of the selected item

The **Diagnoses** view labels events with the following severity level icons:

Severity Level	Icon	Description
Information		Indicates a normal message, no corrective action is required.
Notice		Indicates normal but significant conditions, may require special handling.
Warning		Indicates an error condition that requires attention and should be addressed soon.
Critical		Requires immediate intervention by administrators to prevent serious problem to the network.

Click on the + (plus) or - (minus) signs at the left margin to expand or collapse individual items of the display.

In addition to the common context commands as other tab views, this view also has the following special commands:

Command	Description
Upper View	
Save Diagnosis Statistics...	Saves the diagnosis statistics to a file.
Show Grin Lines	Displays the grid lines for the view.

Expand All	Expands all sub-items.
Collapse All	Collapses all sub-items.
Subview – Events	
Show Relative Packet in New Window	Opens a new window to show relative packets information; alternately, you can double click on the event.
Show Diagnosis Level	Shows/unshows the events of selected diagnosis level.
Export Diagnosis Events...	Exports the selected events to a file.

Endpoints view

The **Endpoints** view presents the detailed communications of each endpoint in network. You may use the combo box to select a display type.

- **All**

Displays all hierarchical address range, including physical addresses and IP addresses.

- **Physical**


Displays endpoints by physical address.

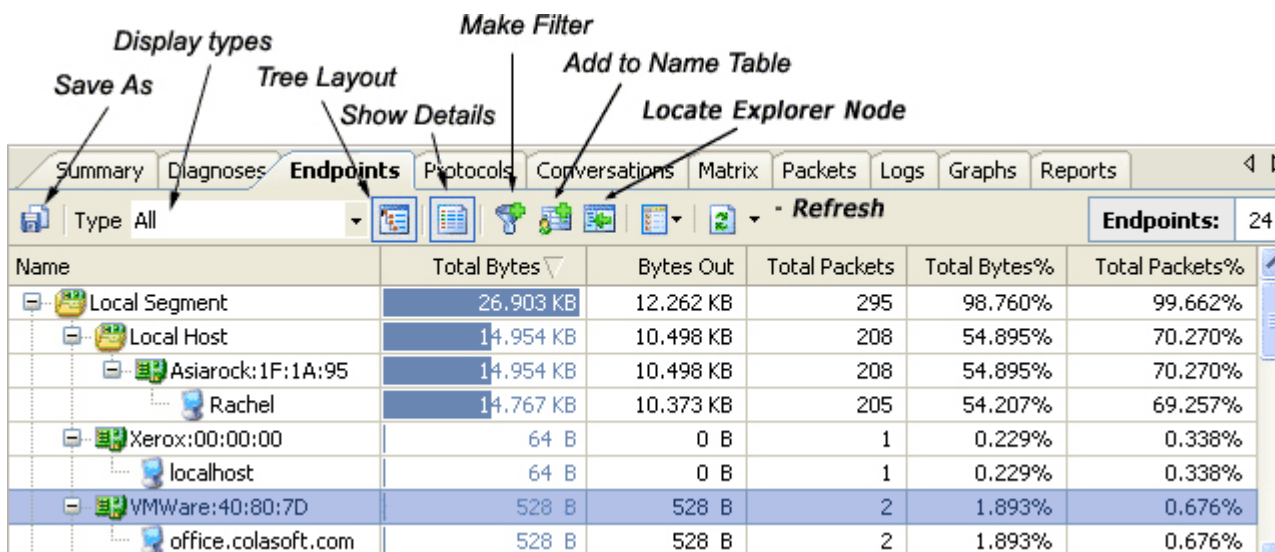
- **IP**

Displays endpoints by IP address.

Click on the + (plus) or - (minus) signs at the left margin to expand or collapse individual items of the display.

The percentage columns present the percentage of total traffic, outbound traffic, inbound traffic and internal traffic. The bottom sub-views offer the packet and connection details of the active endpoint, which can also be viewed in a new window when you double click on the endpoint.

When the **Show Details** button  pressed down, you can see the packets related to the current endpoint shown in the lower sub-view. You may also double click on a row to open an **Endpoint Details** window.



Name	Total Bytes	Bytes Out	Total Packets	Total Bytes%	Total Packets%
Local Segment	26.903 KB	12.262 KB	295	98.760%	99.662%
Local Host	14.954 KB	10.498 KB	208	54.895%	70.270%
Asiarock:1F:1A:95	14.954 KB	10.498 KB	208	54.895%	70.270%
Rachel	14.767 KB	10.373 KB	205	54.207%	69.257%
Xerox:00:00:00	64 B	0 B	1	0.229%	0.338%
localhost	64 B	0 B	1	0.229%	0.338%
VMWare:40:80:7D	528 B	528 B	2	1.893%	0.676%
office.colasoft.com	528 B	528 B	2	1.893%	0.676%

In addition to the **common context commands** as other tab views, this view also has the following special commands:

Command	Description
Save Endpoint Statistics...	Saves the selected endpoint and its statistics to a file.
Expand All Sub nodes	Expands the hierarchical list of endpoints.
Collapse All Sub nodes	Collapses the hierarchical list of endpoints.

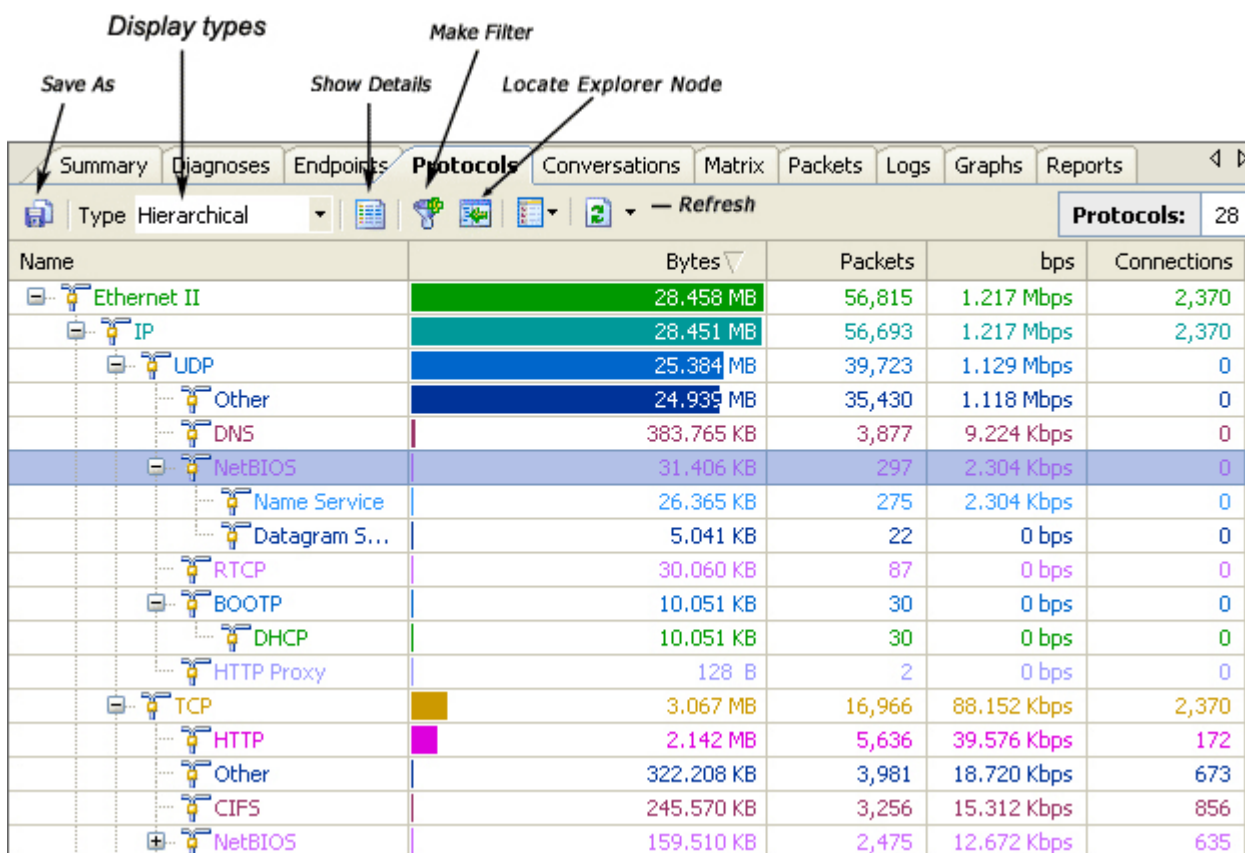
Protocols view

The **Protocols** view displays the information of protocols used by network communications. The bottom sub-views offer the packet and connection details of the active protocol, which can also be viewed in a new window when you double click on the protocol.

You may use the combo box to select a display type.

- **All**
Displays all hierarchical protocols.
- **Physical**
Displays protocols based on Ethernet II. For example, ARP, IP, IPv6, IPX, and so on.
- **IP**
Displays protocols based on IP protocol. For example, HTTP, MSN, DNS, NetBIOS, and so on.

Notes: The **TCP - Other** and **UDP - Other** are the protocols Colasoft Capsa did not support yet now.



Display types

Make Filter

Show Details

Locate Explorer Node


Summary | Diagnoses | Endpoints | **Protocols** | Conversations | Matrix | Packets | Logs | Graphs | Reports

Type: Hierarchical | Refresh

Protocols: 28

Name	Bytes	Packets	bps	Connections
Ethernet II	28.458 MB	56,815	1.217 Mbps	2,370
IP	28.451 MB	56,693	1.217 Mbps	2,370
UDP	25.384 MB	39,723	1.129 Mbps	0
Other	24.939 MB	35,430	1.118 Mbps	0
DNS	383.765 KB	3,877	9.224 Kbps	0
NetBIOS	31.406 KB	297	2.304 Kbps	0
Name Service	26.365 KB	275	2.304 Kbps	0
Datagram S...	5.041 KB	22	0 bps	0
RTCP	30.060 KB	87	0 bps	0
BOOTP	10.051 KB	30	0 bps	0
DHCP	10.051 KB	30	0 bps	0
HTTP Proxy	128 B	2	0 bps	0
TCP	3.067 MB	16,966	88.152 Kbps	2,370
HTTP	2.142 MB	5,636	39.576 Kbps	172
Other	322.208 KB	3,981	18.720 Kbps	673
CIFS	245.570 KB	3,256	15.312 Kbps	856
NetBIOS	159.510 KB	2,475	12.672 Kbps	635

Click on the + (plus) or - (minus) signs at the left margin to expand or collapse individual items of the display.

When the **Show Details** button  pressed down, you can see the packets related to the current protocol shown in the lower sub-view. You may also double click on a row to open an **Protocol Details** window.

In addition to the **common context commands** as other tab views, this view also has the following special commands:

Command	Description
Save Protocol Statistics...	Saves the selected protocol and its statistics to a file.
Expand All Sub nodes	Expands the hierarchical list of protocols.
Collapse All Sub nodes	Collapses the hierarchical list of protocols.

Conversations view

The **Conversations** view dynamically presents the real-time status of Physical, IP, TCP and UDP conversations between pairs of endpoints, the sub-views offer the related packets and reconstructed stream the active conversation. This view will be replaced by Connections if you open a project file or packet file of version 5.5 or before.

Sub-view	Description
Packets	Shows the related packets to the current connection. A connection will be kept in the Conversations view for two minutes after it is closed; when it is cleared from the connection list, you can still find its related packets in the Packets view.
Stream	Unique to TCP connections list. Offers the reconstructed TCP stream of the selected item.
Data	Unique to UDP conversations list. Offers the reconstructed UDP data of the selected item.

Conversations type Show Details Locate Explorer Node Conversations summary

Export Make Filter Refresh

Summary Diagnoses Endpoints Protocols **Conversations** Matrix Packets Logs Graphs Reports

Physical Conversations: 26

Conversation:

Physical

IP

TCP

UDP

Endpoint1 ->	<- Endpoint2	Pkts ->	<- Pkts	Bytes/Sec ->	<- Bps
Realtek Semi:A4:7...	FF:FF:FF:FF:FF:FF	13	0	11 Bps	0 Bps
Asiarock:5A:C0:63	FF:FF:FF:FF:FF:FF	2	0	22 Bps	0 Bps
Linksys:D4:4F:56	01:80:C2:00:00:00	95	0	32 Bps	0 Bps
Asiarock:5A:CF:7A	Realtek Semi:A4:78...	50	45	36 Bps	25 Bps
Asiarock:5A:CF:7A	Amigo Tech:26:3F:9E	404	559	318 Bps	2.014 K...
00:14:85:CA:F5:22	FF:FF:FF:FF:FF:FF	2	0	1 Bps	0 Bps
00:0F:EA:35:2C:1C	FF:FF:FF:FF:FF:FF	2	0	3 Bps	0 Bps
Asiarock:5A:CF:7A	FF:FF:FF:FF:FF:FF	1	0	64 Bps	0 Bps
Asiarock:8F:08:9F	FF:FF:FF:FF:FF:FF	4	0	5 Bps	0 Bps

Packets

No.	Relative Time	Source	Destination	Size
12	0.000000	192.168.0.28:3325	209.237.237.101...	64
13	0.257804	192.168.0.28:2184	207.46.0.31:msnp	64
14	0.563397	207.46.0.31:msnp	192.168.0.28:2184	66
16	0.666863	192.168.0.28:2184	207.46.0.31:msnp	64

Sub-tab: show the related packets of the selected conversation

• Conversation list

The conversation list reveals what TCP and UDP conversations your network is making, captured conversations are circularly stored to keep the display real time and dynamic. Colasoft Capsa will clear those conversations having been closed for more than two minutes when the list reaches 1000 conversations. The conversation related packets can be seen in the **Packets** view, HTTP conversations, Email conversations, FTP conversations and DNS conversations can be seen in the **Logs** view, when a conversation is cleared from the conversation list, you may find the corresponding information from these views.

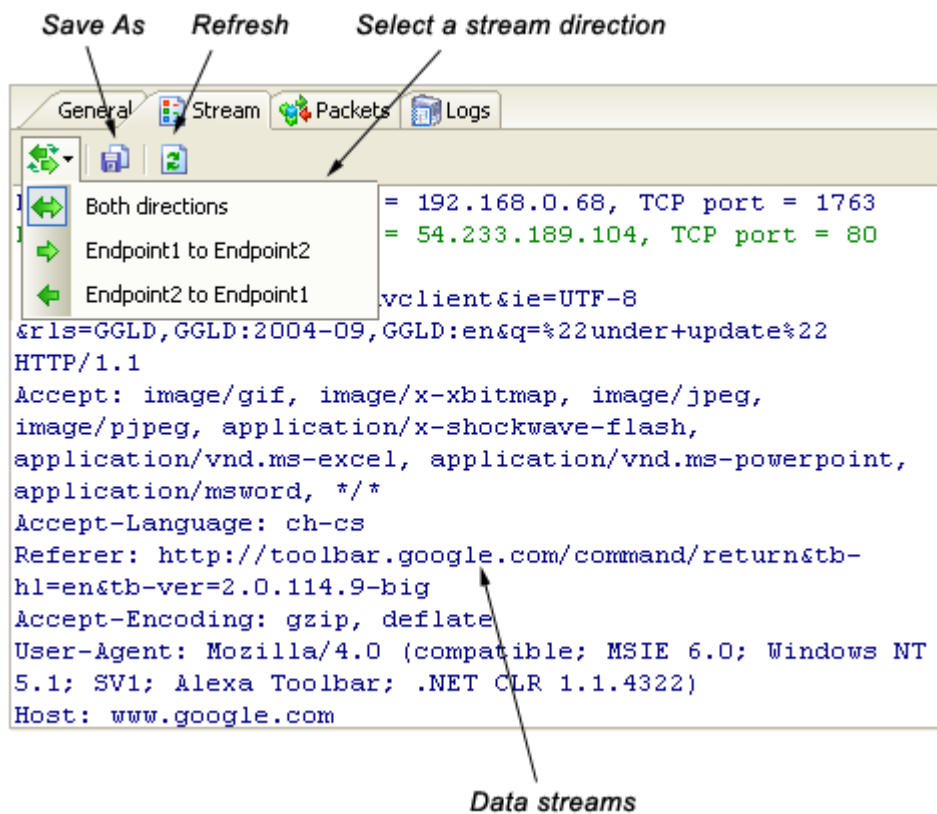
You can view the conversation details by switching the sub-tabs at the lower section of the display, or in the new opened **Conversation Details** window with double clicks on the selected conversation. When the **Conversation Details** window is opened, the data displayed in it will be kept even after the connection is cleared from the connection list.

In addition to the common context commands as other tab views, this view also has the following specific commands:

Command	Description
View Details in New Window	Opens a new window to show the conversation details; alternately, you can double click on the conversation.
Show Conversations	Defines a condition and shows matching conversations.
Export Conversations...	Exports the conversations to a file.
Send Packet	Send captured packets from defined NICs.

• TCP stream

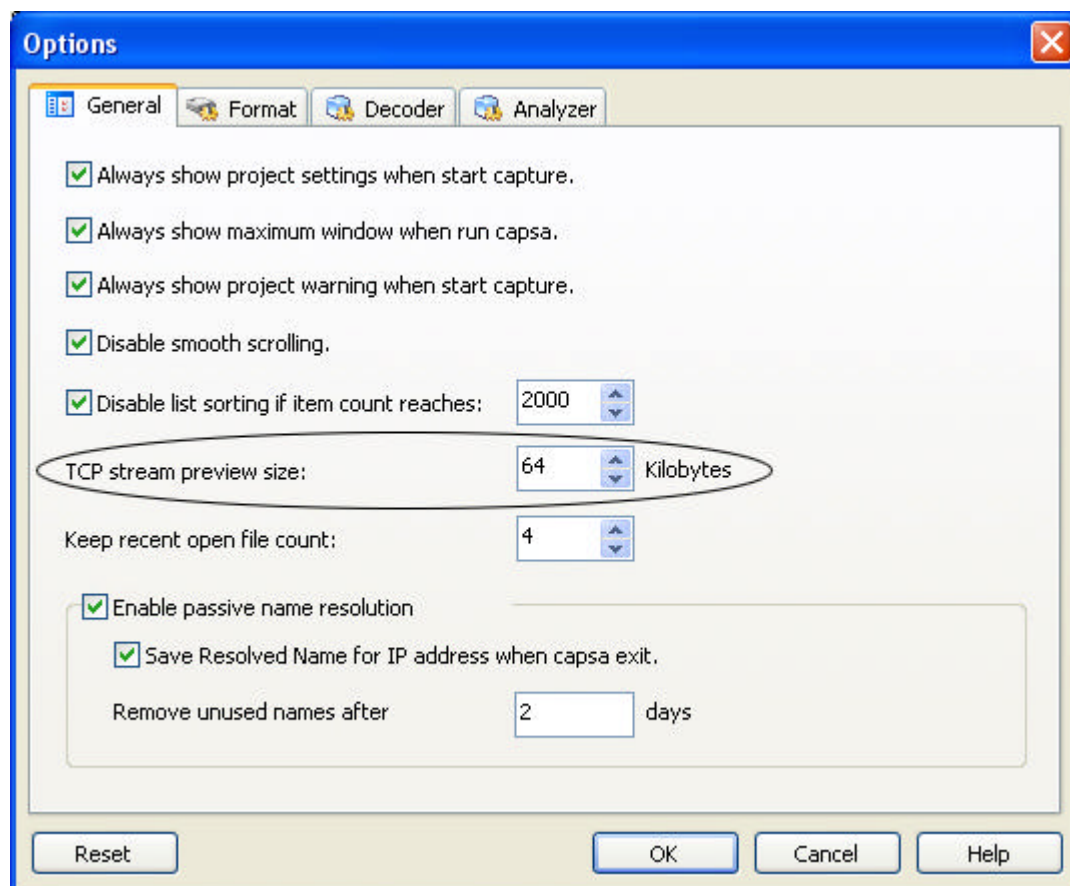
From this view, you can see the reconstructed data streams of the selected conversation. The data streams of different directions can be distinguished by color, e.g. blue is for endpoint 1 to endpoint 2, green is for endpoint 2 to endpoint 1.



By default, the data streams are showed as ASCII. You can change the display to EBCDIC with a right click in the view and select the Show as EBCDIC command from the context menu.

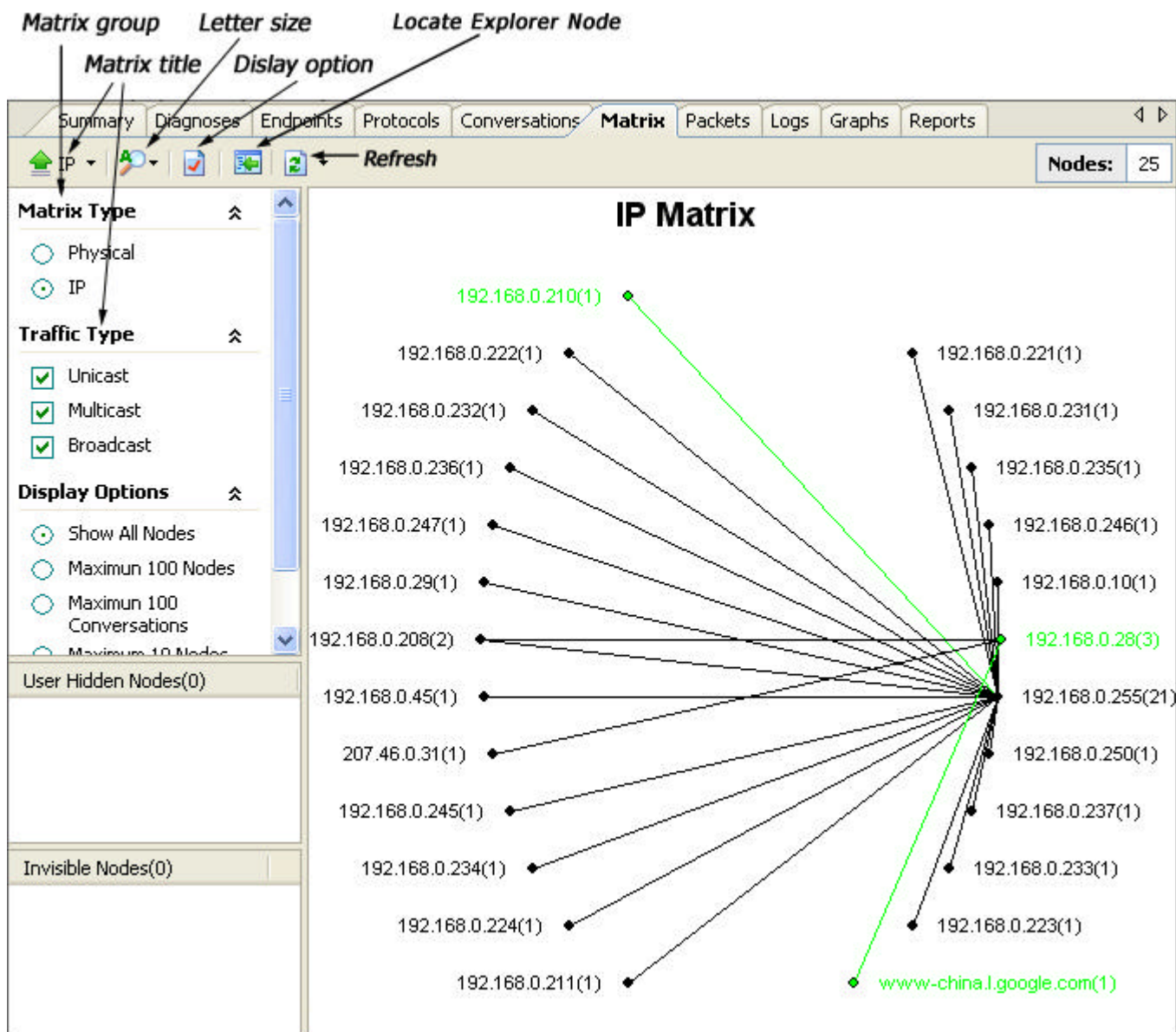
To save the TCP streams to a text file, press the Save As icon from the toolbar or select the command from the context menu.

The preview size of TCP streams can be customized by opening the Options dialog from the Tools menu. When a TCP stream goes beyond the size defined, only the contents within the size are shown. To view the whole contents, you must redefine the preview size to a larger value.



Matrix view

The Matrix view shows the network traffic statistics. The line weight indicate the volume of traffic between nodes arranged in an extensive ellipse indicate the traffic. You can quickly switch among global statistics and the details of specific network nodes by switch the corresponding nodes in the **Project Explorer**. There will no data displayed in this view if open a project file or packet file of version 5.5 or before.



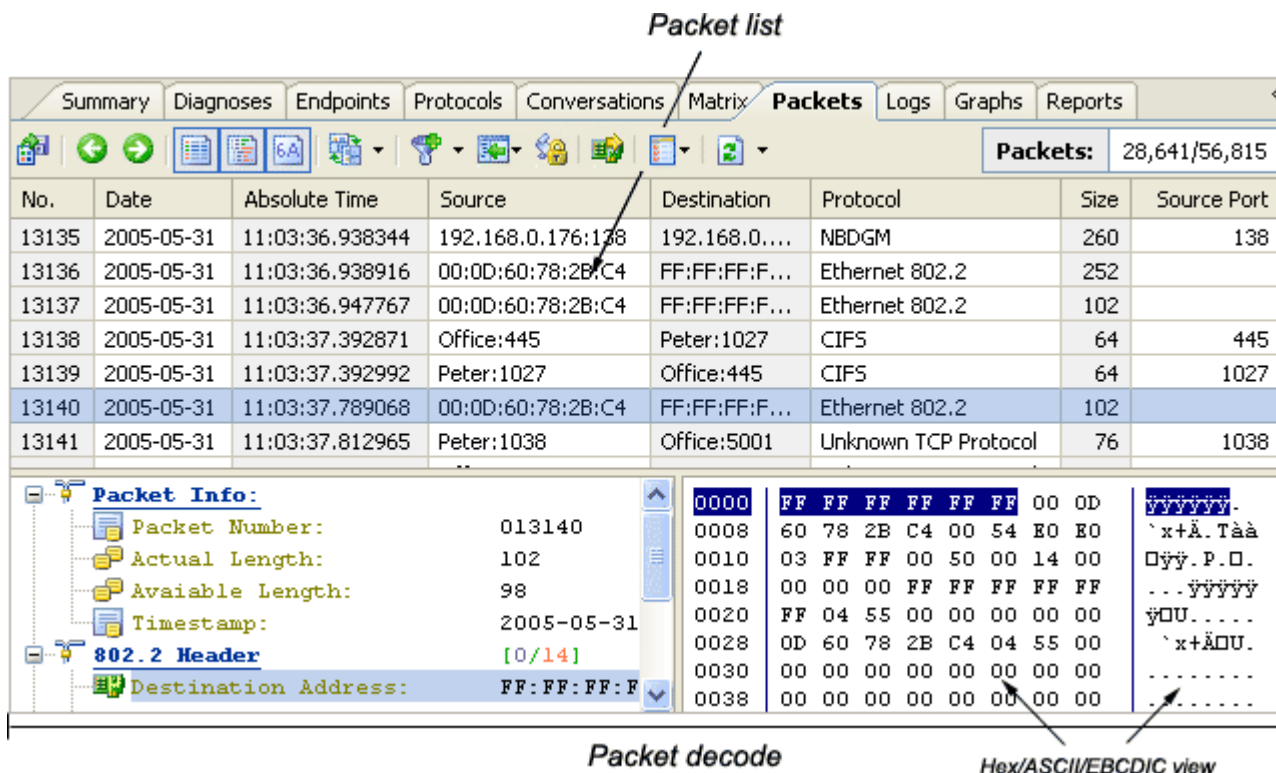
The table below describes each of the parameters used to set up or save a statistic matrix.

Parameter	Description
Matrix group	The matrixes are grouped by matrix type, traffic type and display options.
Matrix title	The title of the matrix.
Font size	Select the display font size
Matrix option	Select the display style of the nodes, lines and background.
User Hidden Nodes	Show the hidden nodes if you hide them manually.
Invisible Nodes	Show the hidden nodes if you choose a rule from the Display Options.

Packets view

The **Packets** view presents a list of captured packets and the packet decode information in Hex, ASCII and EBCDIC. The following sections describes how to view a packet and its decode information, how to find related packets, and how to change the layout of this view.

Packet list



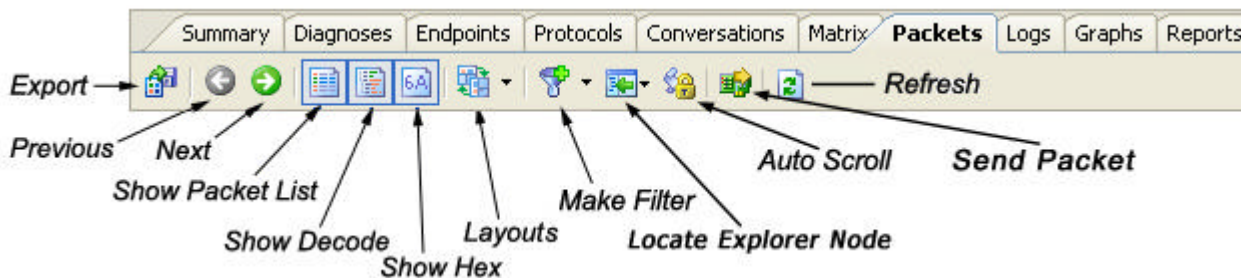
Packet Info:

- Packet Number: 013140
- Actual Length: 102
- Available Length: 98
- Timestamp: 2005-05-31
- 802.2 Header [0/14]
- Destination Address: FF:FF:FF:F

Packet decode

Hex/ASCII/EBCDIC view

The figure below is toolbar of **Packets** view.



Export

Previous

Next

Show Packet List

Show Decode

Show Hex

Layouts

Make Filter

Locate Explorer Node

Auto Scroll

Send Packet

Refresh

Button	Description
Export	Exports selected packets to a file in public formats such as Text and HTML.
Previous	Backs to the previous packet if applicable.
Next	Goes to the next packet if applicable.
Show Packet List	Show the packet list if check on this button.
Show Decode	Show the packet decode window if check on this button.
Show Hex	Show the Hex decode window if check on this button.
Layouts	Select a layout of these three windows from the three predefined layouts. By default, the packet decode information are showed at the bottom of the Packets view.
Make Filter	Opens the Packet Filter dialog and makes a new filter on the basis of the selection.
Auto Scroll	The packet list will display the newest packet always if check this button. But when you select an item in the view, this button will stop execution until you check it again.

Refresh


Refreshes the current view.

- **Packet list**

Matching to the setting of **Packet buffer size** and **When buffer is full** in the **Project Settings - General** page, the packet list view offers the list of packets captured from the node selected in the **Project Explorer**.

By default, the packet decode information are showed at the bottom of the **Packets** view. Click the layout icons to change the display. A packet decode window can be opened when you double click on a packet.

In addition to the **common context commands** as other tab views, this view also has the following special commands:

Command	Description
Decode Packet in New Window	Opens a new window to show packet decode information; alternately, you can double click on the packet.
Highlight Packet	Highlights the current packet.
Packet Comment	Adds, edits or deletes a comment for the current packet; the packet with a comment is marked with  .
Summary	Shows the packet summary. Automatic - show the uppermost protocol summary IP Summary - show the packet summary of IP protocols; if no IP protocols, show the uppermost protocol summary TCP/UDP Summary - show the packet summary of TCP/UDP protocols; if no TCP/UDP protocols, show the uppermost protocol summary
Export Packet...	Exports selected packets to a file.
Send Packet	Sends captured packets from defined NICs.
Set Relative Packet	Sets the current packet as the relative packet.
Select Related Packets	Selects and highlights the related packets by source, destination, source and destination, protocol or port.
Hide Selected Packets	Only shows the unselected packets.
Hide Unselected Packets	Only shows the selected packets.
Unhide All Packets	Shows all packets.

The columns in the **Packets** view offer many packet details. You can select more or less columns to show: right click on the column heading bar and choose the **More...** command to open the **Select Column** dialog, check the column headings you want to display.


If you only want to view those packets related to the current selection, you can first choose **Select Related Packets** and a condition from the context menu, Colasoft Capsa will highlight all related packets; then right click to open the context menu again and select **Hide Unselected Packets**.

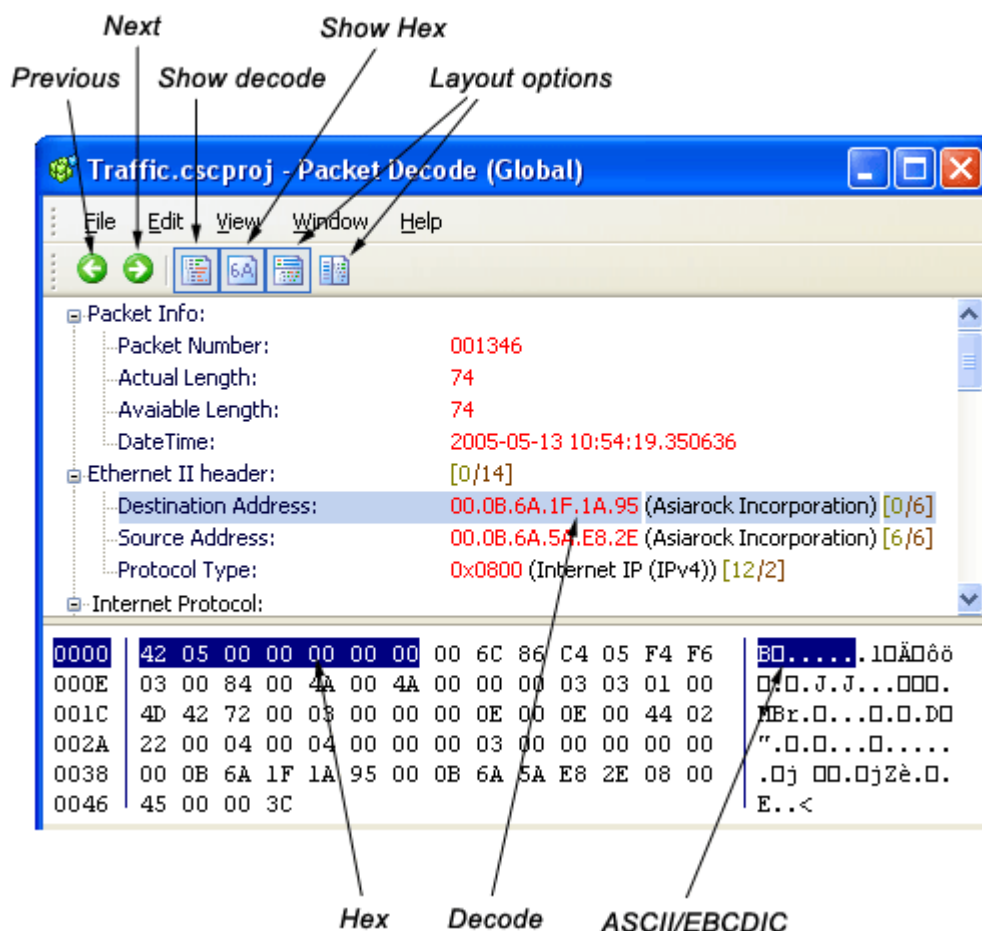
The table below lists the column headings available in the **Packets** view and the specific meaning they indicate.


Default	Column Heading	Description
*	No.	The packet number which is set automatically by Colasoft Capsa.
*	Absolute Time	The actual time when the current packet is transmitted.
*	Source	The IP address or physical address where the current packet is transmitted from.
*	Destination	The IP address or physical address where the current packet is transmitted to.
*	Protocol	The protocol used by the current packet in transmission.
*	Size	The bytes of the current packet.
*	Summary	The summary for the current packet.
	Date	The date when the current packet is captured.
	Delta Time	The time span between the current packet and the previous packet.
	Relative Time	The time span between the current packet and the relative packet (if no relative packet is defined, the first packet is the relative packet).
	IP Identifier	The identification number of an IP packet.
	Source Physical	The physical address where the current packet is transmitted from.
	Destination Physical	The physical address where the current packet is transmitted to.
	Source IP	The IP address where the current packet is transmitted from.
	Destination IP	The IP address where the current packet is transmitted to.
	Source Port	The port number where the current packet is transmitted from.
	Destination Port	The port number where the current packet is transmitted to.
	Comment	The comment made for the current packet.

You can rearrange the column heading bar by changing a column's position or width.

- **Packet decode**

The packet decode view is a part of the Packets view, presenting the decode information of selected packet, you can use the icon  to show or hide it. Alternately, the packet decode information can be showed in the Packet Decode window with double clicks on a packet row.



To show the Hex view, click the icon , which contains the actual packet contents in raw hexadecimal on the left and its ASCII (or EBCDIC) equivalent on the right. The packet information in the packet decode view, Hex and ASCII/EBCDIC view are consistent, when you select a section in one of these views, the corresponding portions will be highlighted in the other views.

You may choose to show packet contents as ASCII or EBCDIC from the context menu by a right click in the Hex view. If you want to save the data, you can select Copy Hex or Copy Text.

The layout of the Packet Decode window can be changed; use the icon  and  to rearrange the display.

The context menus of the packet decode view and Hex and ASCII/EBCDIC view contain the following useful commands:

Command	Description
Copy (Ctrl+C)	Copies the selection and puts it on the clipboard.
Copy Tree	Copies the packet decode tree and puts it on the clipboard.
Expand All	Expands all items of the display.
Collapse All	Collapses all items of the display.
Copy Hex	Copies the selected Hex codes and puts it on the clipboard.
Copy Text	Copies the selected ASCII/EBCDIC text and puts it on the clipboard.

Show ASCII	Shows the decoded information as ASCII.
Show EBCDIC	Shows the decoded information as EBCDIC.

Logs view

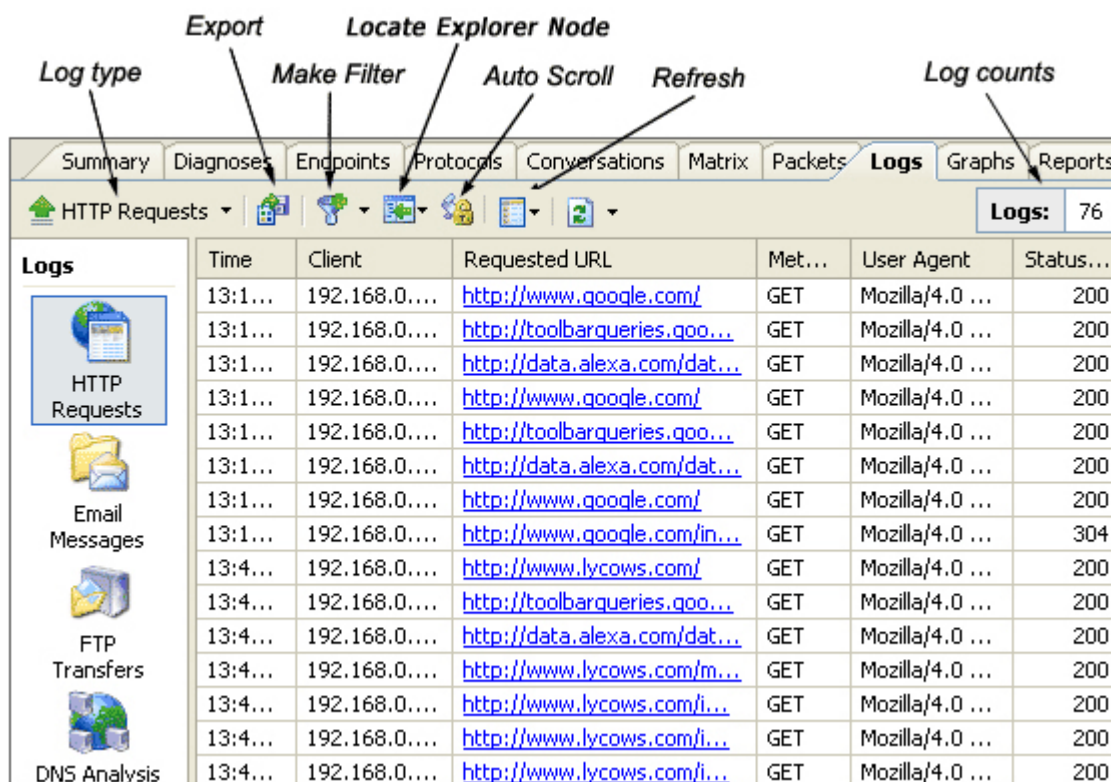
The **Logs** view of Colasoft Capsa includes **FTP Transfers** view, **Email Messages** view, **HTTP Requests** view and **DNS Analysis** view, from which you can find the records of TCP conversations, email messages, web accesses and DNS analysis; in addition, in this **Logs** view you can monitor activities of four kinds of instant messengers: MSN, AIM, ICQ and Yahoo Messenger.

In addition to the common context commands as other tab views, this view also has the following specific commands:

Command	Description
Open	Opens the reconstructed contents of the current log in a new window.
Delete	Deletes the selected logs.
Show Port in Client/Server Column	Shows/unshows the port number in the Client and Server column.
Export Log...	Exports the logs to a file.

• Logs - HTTP requests


This view presents the information of captured web accesses, you can open a listed URL with double clicks.



The screenshot shows the 'Logs' tab selected in the Colasoft Capsa interface. The toolbar at the top of the Logs pane includes buttons for 'Log type', 'Export', 'Make Filter', 'Locate Explorer Node', 'Auto Scroll', 'Refresh', and 'Log counts'. The main display area shows a list of HTTP requests. The left sidebar contains icons for 'HTTP Requests', 'Email Messages', 'FTP Transfers', and 'DNS Analysis'.

Time	Client	Requested URL	Met...	User Agent	Status...
13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
13:1...	192.168.0...	http://www.google.com/in...	GET	Mozilla/4.0 ...	304
13:4...	192.168.0...	http://www.lycows.com/	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://www.lycows.com/m...	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200
13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200

Note: a web page may be parsed into several URLs, the URLs end with .css and .js can not be opened.


By default, Colasoft Capsa only captures the web requests from port 80. To capture the web requests from other ports, click the Log icon  in the toolbar to open the Project Setting - Log page, then double click the HTTP Log on the left and append ports to the Monitor Port pane on the right, use a semicolon to separate each two ports. You may also modify other settings of HTTP Log in this page.

• Logs - email messages


Colasoft Capsa can capture and analyzed the email messages transmitted in plain text, email list and related information are displayed in the **Email Message** view. To view the reconstructed email contents, you can double click on the selected email, it will be opened with your email client software; alternately, you can right click and select the **Open** command from the context menu. Encrypted email messages can not be captured and reconstructed.

Note: Captured emails may contain virus, please be cautious when you open email.

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports							
Email Messages							Logs: 46
Date	Time	Sender Na...	Sender Email	Receiver Name	Receiver Email	Subject	Size
2005-05-30	13:11:17	"Smith"	<test1@colasoft.c...	"egaew"	<egaew@dgmawe...	egeing	589
2005-05-30	13:57:39	"karolin"	Mail Delivery Subsy...	"Smith"	<test1@colasoft.c...	Returne...	2792
2005-05-30	13:58:19	"Smith"	<test1@colasoft.c...	"Smith"	<smithe@diangr.v...	agaefga	573
2005-05-30	13:59:29	"Smith"	<test1@colasoft.c...	"hellowW"	<hellowW@siang.c...	Hello	572
2005-05-30	14:00:43	"Smith"	<test1@colasoft.c...		<karolin@colasoft....	agegwa	590

To change the settings of email log, click the **Log** icon  in the toolbar to open the **Project Setting - Log** page, then double click the **Email Log** to edit.

• Logs - FTP transfers


You can view the detailed records of FTP uploads and downloads in this view. The FTP transfers are analyzed by the FTP analyzer of Colasoft Capsa, to change the analysis settings for FTP transfers, click the Log icon  in the toolbar to open the **Project Setting - Logs** page and select the **FTP Log** to edit.


FTP Transfers

Logs: 50

No.	Client	Server	Transfe...	Account	File Path/Name	Duration
3	Nicholas:1394	61.132....	10:17:46	webmaster@lo...	/htdocs/Terms of Use after.doc	00:00:00.738994
4	Nicholas:1396	61.132....	10:18:06	webmaster@lo...	/htdocs/TCPStreamView	00:00:00.739306
5	Nicholas:1400	61.132....	10:18:51	webmaster@lo...	/htdocs/Capsa50u.chm	00:00:32.754044
6	Nicholas:1405	61.132....	10:20:56	webmaster@lo...	/htdocs/Datasheet_Capsa_en.doc	00:00:10.088762
7	Nicholas:1407	61.132....	10:21:07	webmaster@lo...	/htdocs/Datasheet_Capsa_en.pdf	00:00:12.098103
7	Nicholas:1410	61.132....	10:21:18	webmaster@lo...	/htdocs/Capsa_TechSpecs.pdf	00:00:03.824860
9	Nicholas:1419	61.132....	10:23:49	webmaster@lo...	/htdocs/Screenshot/Capsa4.0/TCP09...	00:00:01.409582
10	Nicholas:1426	61.132....	10:24:25	webmaster@lo...	/htdocs/doc.zip	00:00:03.621225
11	Nicholas:1428	61.132....	10:24:48	webmaster@lo...	/htdocs/design.rar	00:00:06.533059
12	Nicholas:1432	61.132....	10:25:52	webmaster@lo...	/htdocs/Affiliate Program After.doc	00:00:01.974887
13	Nicholas:1433	61.132....	10:25:55	webmaster@lo...	/htdocs/Download License Agreeemen...	00:00:01.911898
14	Nicholas:1434	61.132....	10:25:58	webmaster@lo...	/htdocs/Privacy Statement After.doc	00:00:02.974855
15	Nicholas:1439	61.132....	10:26:02	webmaster@lo...	/htdocs/Reseller Program After.doc	00:00:01.397690







• Logs - DNS analysis

This view shows the details of DNS analysis results. The DNS Advanced Analyzer in Colasoft Capsa analyze the DNS requests, replies and status. The DNS analysis are analyzed by the DNS analyzer of Colasoft Capsa, to change the analysis settings for DNS analyses, click the **Log** icon  in the toolbar to open the **Project Setting - Logs** page and select the **DNS Log** to edit.

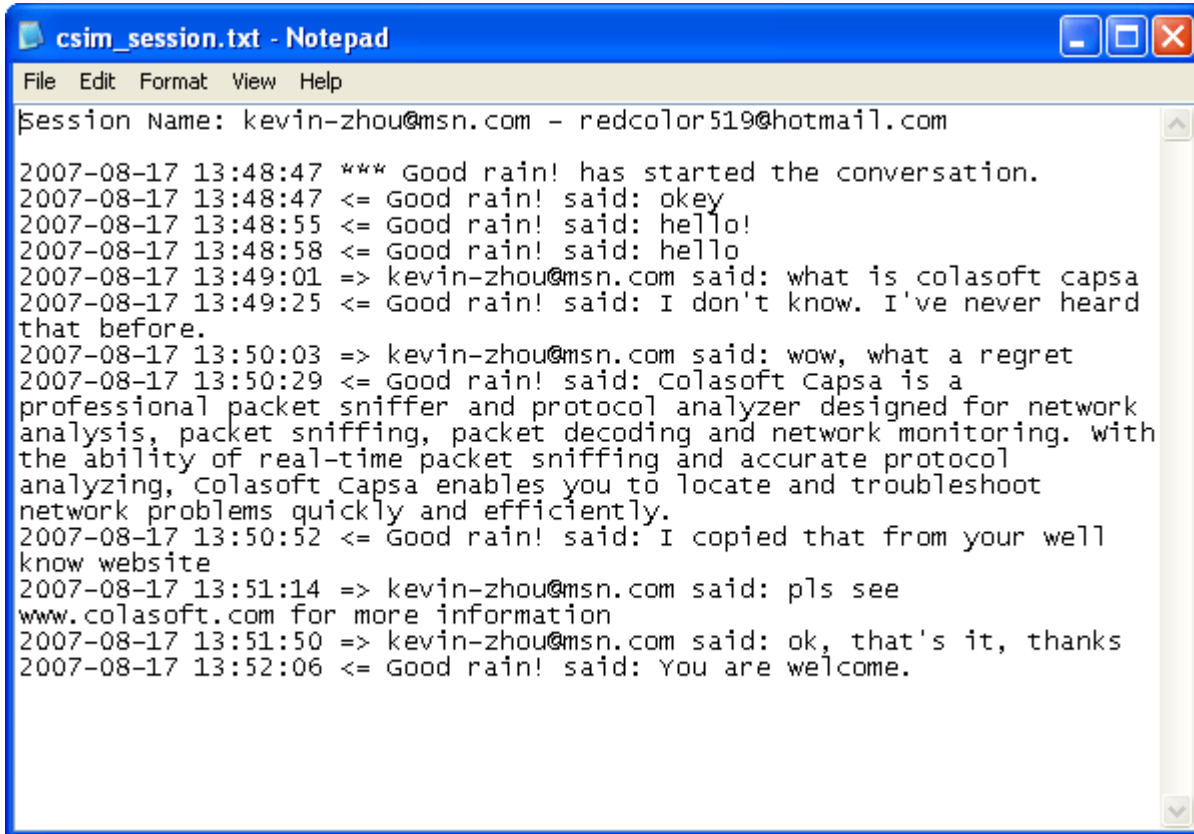
Summary	Diagnoses	Endpoints	Protocols	Conversations	Matrix	Packets	Logs	Graphs	Reports
 DNS Analysis							Logs: 35		
Time	Client	Server	Query	Status	Result				
13:39:01	192.168.0...	61.139.2.6...	www.symantec.com	Success	CNAME=www.symantec....				
13:39:19	192.168.0...	61.139.2.6...	liveupdate.symant...	Success	CNAME=liveupdate.syma...				
13:39:40	192.168.0...	61.139.2.6...	www.google.com	Success	CNAME=www.l.google.c...				
13:39:42	192.168.0...	61.139.2.6...	toolbarqueries.go...	Success	CNAME=toolbarqueries.l...				
13:39:56	192.168.0...	61.139.2.6...	www.colasoft.com	Success	A=67.15.229.157				
13:39:58	192.168.0...	61.139.2.6...	toolbarqueries.go...	Success	CNAME=toolbarqueries.l...				
13:40:28	192.168.0...	61.139.2.6...	www.etherlook.com	Success	A=67.15.229.155				
13:40:52	192.168.0...	61.139.2.6...	www.protocolbase...	Success	A=64.246.27.57				
13:41:11	192.168.0...	61.139.2.6...	www.msn.com	Success	CNAME=www.msn.com.n...				

• Logs - MSN Activities


In MSN Logs view you can monitor real-time information of all MSN activities, including date, time, node, session name, as well as the message content.

Summary	Diagnosis	Endpoints	Protocols	Conversations	Matrix	Packets	Logs	Graphs	Re
 MSN Activities							Logs: 15		
Logs		Date Time	Node1	Session Name	Content				
 HTTP Requests  Email Messages  MSN Activities  AIM Activities  FTP Transfer		2007-08-17 13:...	192.168...	[unknown@207.46....	*** kevin-zhou@msn.com has starte				
		2007-08-17 13:...	192.168...	[unknown@207.46....	=> kevin-zhou@msn.com said: hello				
		2007-08-17 13:...	192.168...	[unknown@207.46....	=> kevin-zhou@msn.com said: test				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	*** Good rain! has started the conv				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: okey				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: hello!				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: hello				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	=> kevin-zhou@msn.com said: what				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: I don't know. I\'				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	=> kevin-zhou@msn.com said: wow				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: Colasoft Capsa				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: I copied that fro				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	=> kevin-zhou@msn.com said: pls s				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	=> kevin-zhou@msn.com said: ok, b				
		2007-08-17 13:...	192.168...	kevin-zhou@msn.co...	<= Good rain! said: You are welcom				

All MSN messages are listed in time sequence, to view messages of a specific session, you can click the desired session name in the session name column, then a text file will pop up to show all the messages of the selected session.



```
csim_session.txt - Notepad
File Edit Format View Help
Session Name: kevin-zhou@msn.com - redcolor519@hotmail.com
2007-08-17 13:48:47 *** Good rain! has started the conversation.
2007-08-17 13:48:47 <= Good rain! said: okey
2007-08-17 13:48:55 <= Good rain! said: hello!
2007-08-17 13:48:58 <= Good rain! said: hello
2007-08-17 13:49:01 => kevin-zhou@msn.com said: what is colasoft capsa
2007-08-17 13:49:25 <= Good rain! said: I don't know. I've never heard
that before.
2007-08-17 13:50:03 => kevin-zhou@msn.com said: wow, what a regret
2007-08-17 13:50:29 <= Good rain! said: Colasoft Capsa is a
professional packet sniffer and protocol analyzer designed for network
analysis, packet sniffing, packet decoding and network monitoring. With
the ability of real-time packet sniffing and accurate protocol
analyzing, Colasoft Capsa enables you to locate and troubleshoot
network problems quickly and efficiently.
2007-08-17 13:50:52 <= Good rain! said: I copied that from your well
know website
2007-08-17 13:51:14 => kevin-zhou@msn.com said: pls see
www.colasoft.com for more information
2007-08-17 13:51:50 => kevin-zhou@msn.com said: ok, that's it, thanks
2007-08-17 13:52:06 <= Good rain! said: You are welcome.
```

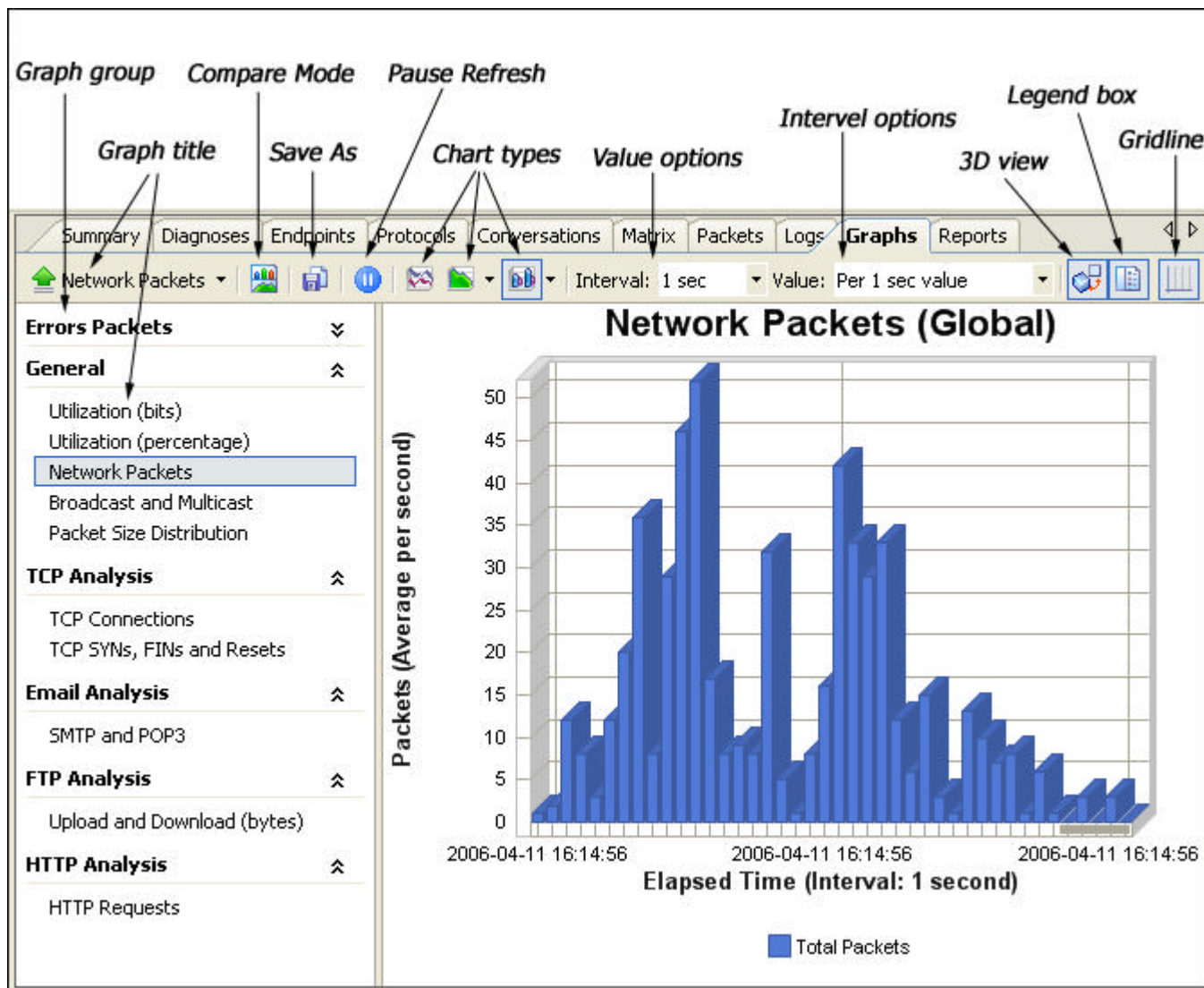
To change the settings of MSN log, click the Log icon  in the toolbar to open the Project Setting - Log page, then double click the MSN Log to edit.

- **Logs – Other Instant Messenger Activities**

Views of other instant messengers are same as MSN view, please refer to MSN view for more information.

Graphs view

Unique to Colasoft Capsa enterprise edition. The **Graphs** view graphically presents the statistic data of the current node. It contains a number of graph groups and multiple graph titles, including errors vs total packets, network utilization, packet size distribution, packet size details and many more. The available graph titles and display options will vary with the specific node you select from the **Project Explorer**.

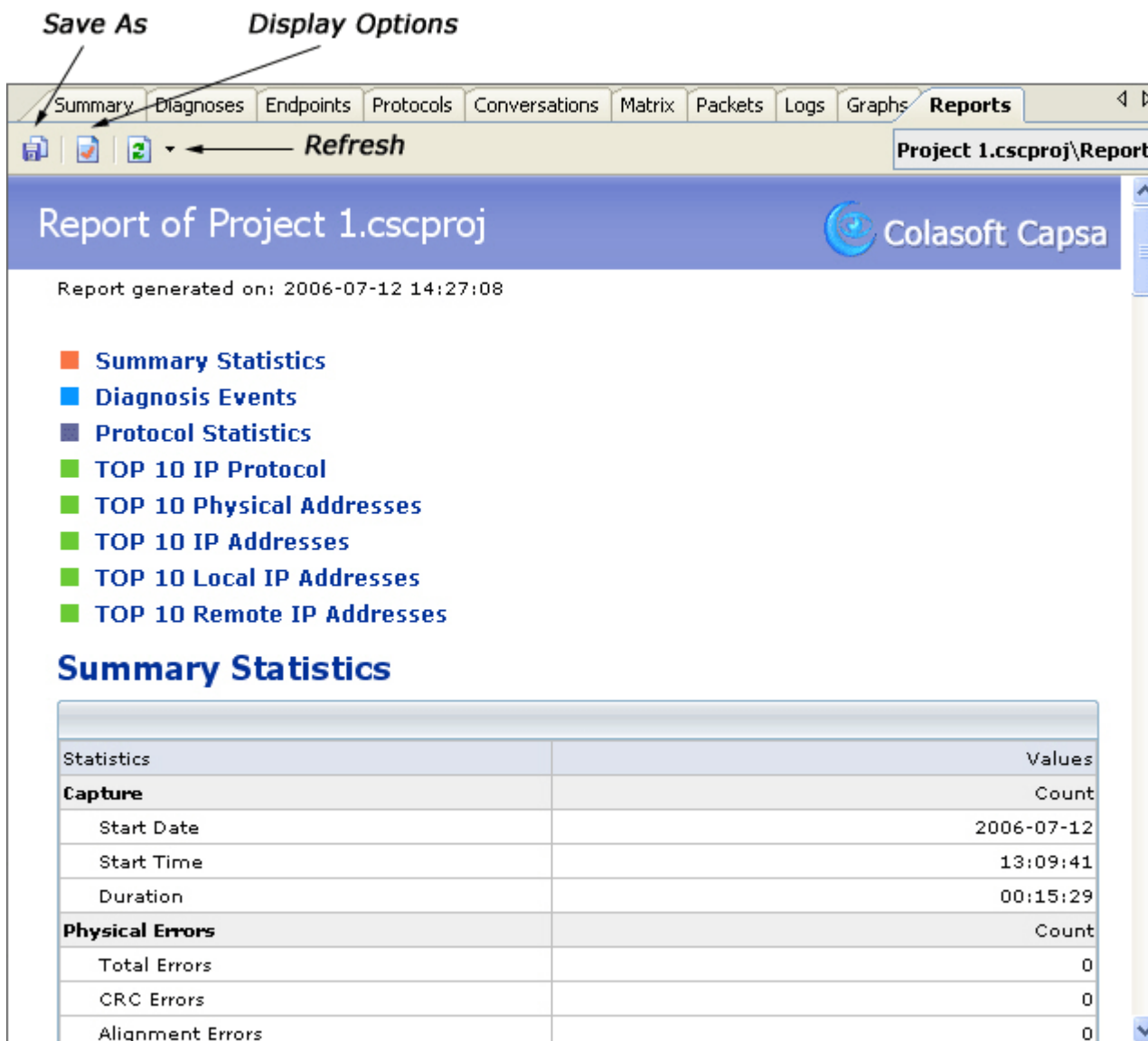


The table below describes each of the parameters used to set up or save a statistic graph.

Parameter	Description
Graph group	Available graphs are grouped by analyzer, each analyzer has one graph group; the General group contains some commonly used statistic graphs, involving multiple analyzers.
Graph title	The title of the graph.
Save As	Saves the graph to a *.bmp, *.emf and *.png file.
Pause Refresh	Temporarily halts refreshing the display.
Chart types	The chart types which are available for the current node and the selected graph title.
Value	Selects a value type to see the graphic data.
Interval	Selects a scale to set the refresh and sampling interval.
3D view	Shows the graph in three-dimensional view.
Legend box	Shows or hides the explanation of the colors appearing on the graph.
Gridline	Shows or hides the gridlines on the graph.

Reports view

Unique to Colasoft Capsa enterprise edition. A project report contains the statistic information of summary statistics, diagnosis events, protocol statistics, top 10 IP protocol, top 10 physical addresses, top 10 IP addresses, top 10 local IP addresses, top 10 remote IP addresses, and all available graphs with the current settings.



Save As **Display Options**

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs **Reports**

Project 1.cscproj\Report

Report of Project 1.cscproj


Report generated on: 2006-07-12 14:27:08

- Summary Statistics
- Diagnosis Events
- Protocol Statistics
- TOP 10 IP Protocol
- TOP 10 Physical Addresses
- TOP 10 IP Addresses
- TOP 10 Local IP Addresses
- TOP 10 Remote IP Addresses

Summary Statistics

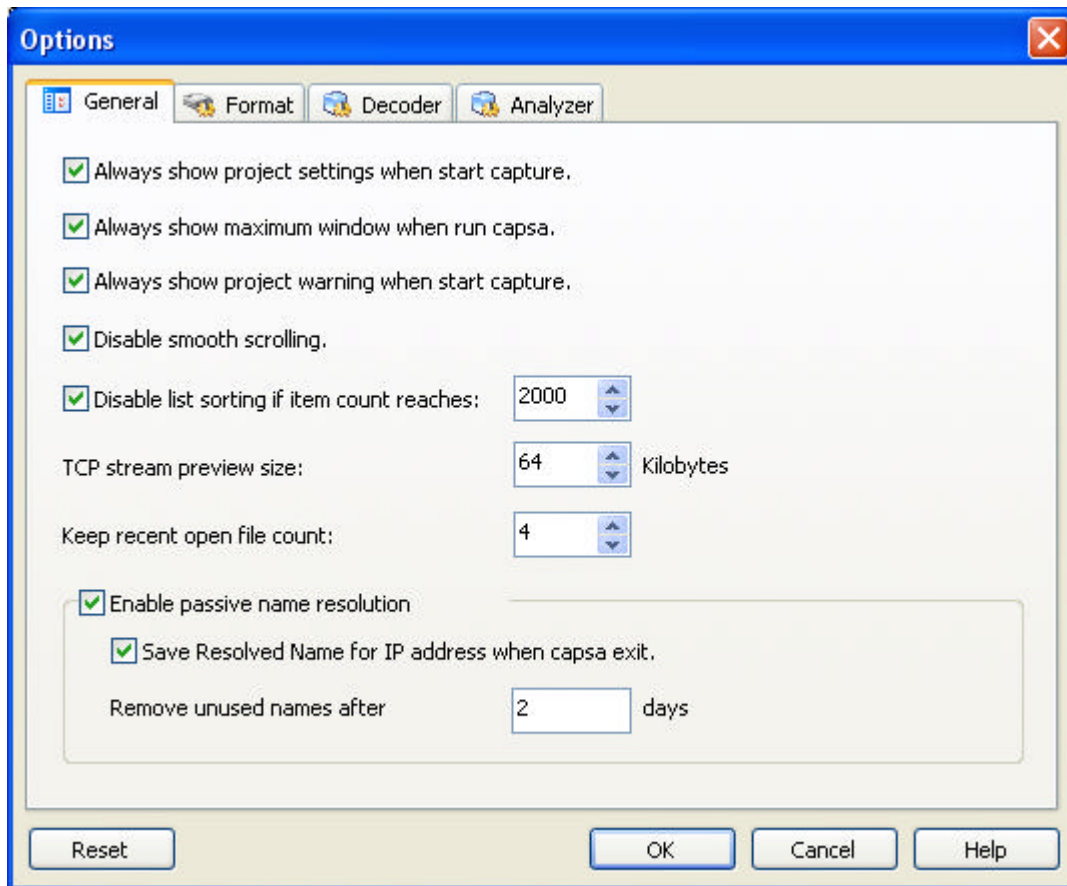
Statistics	Values
Capture	Count
Start Date	2006-07-12
Start Time	13:09:41
Duration	00:15:29
Physical Errors	Count
Total Errors	0
CRC Errors	0
Alignment Errors	0

System options

The Options dialog contains some global options which apply to all the projects in Colasoft Capsa. There are four pages in this dialog - **General**, **Format**, **Decoder** and **Analyzer**. Choose **Options...** under the Tools menu or click the Options  button in the toolbar to open the Options dialog, where you can make general options, define the packet decoder, enable analysis models and choose the display format.

Options - General

The **General** options let you set most popular settings of the project.



- **Always show project settings when start capture.**

If checked, Colasoft Capsa will always open the **Project Settings** dialog each time when you start a capture.

- **Always show maximum window when run Capsa.**

If unchecked, Colasoft Capsa will remember the last setting of project window size and apply to next time when you run Capsa again.

- **Always show project warning when start capture.**

If unchecked, Colasoft Capsa will not show the warning dialog when you start a new capture.

- **Disable smooth scrolling.**

Instant scrolling will be enabled in effect if you check this option.

- **Disable list sorting if item count reaches:**

The sorting function will be disabled when the listed items reach the limitation. The default count is 2000.

- **TCP stream preview size:**

You may customize the preview size of TCP stream, the default size is 64 KB. When a TCP stream goes beyond the limitation, only the contents within the defined size are shown in the **Stream** view.

- **Keep recent open file count:**

Define a limit for keeping recent open file.

- **Enable passive name resolution**

Enable passive name resolution, Colasoft Capsa will automatically resolve the name of captured IP address.

- **Save Resolved Name for IP address when Capsa exit.**

By default, Colasoft Capsa will automatically save the resolved names for IP addresses when you exit. If unchecked, the resolved names will lose when you exit without saving them.

- **Remove unused names after**

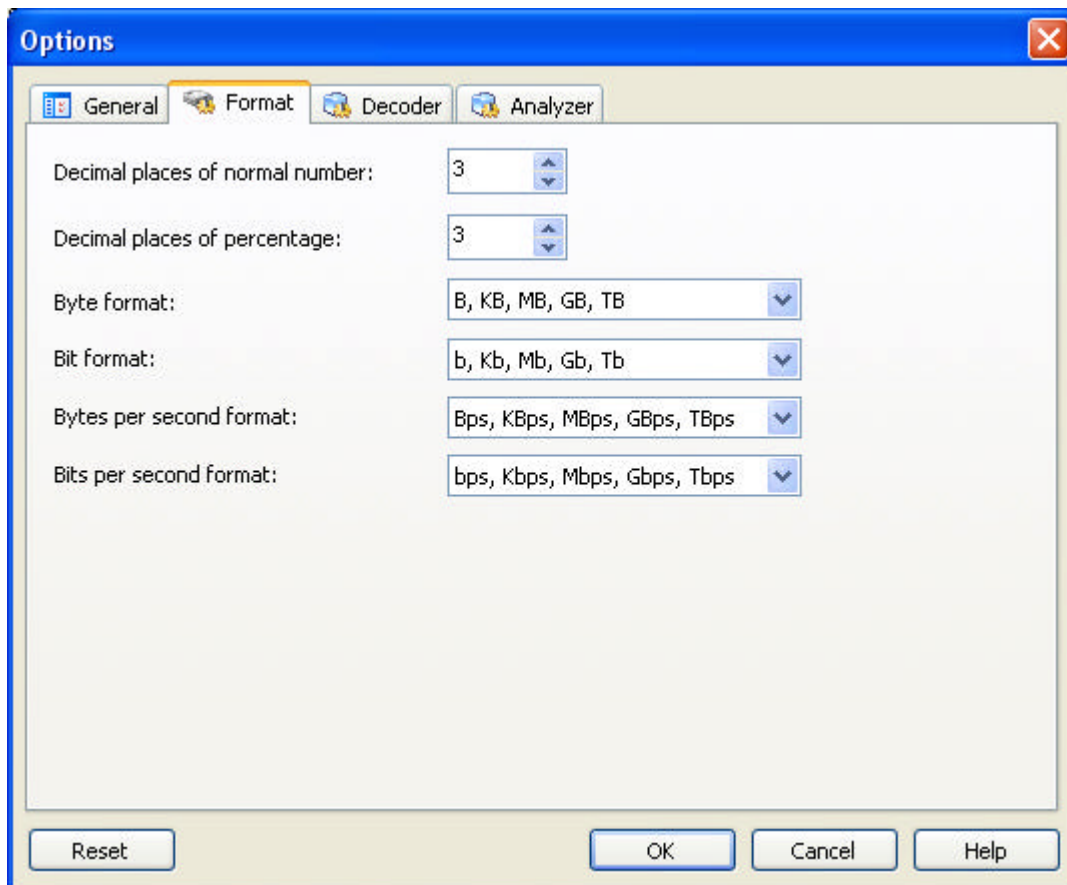
Colasoft Capsa will remove the resolved names which unused more than 2 days in default.

- **Reset**

Click this button to restore the predefined settings.

Options – Format

The **Format** dialog let you customize the format of data display. You can define the formats for data display, including decimal places of normal number, decimal places of percentage, byte format, bit format, bytes per second format and bits per second format.



- **Decimal places of normal number**

The display precision of a number. You can customize the decimal places though the thousandth in default.

- **Decimal places of percentage**

The display precision of a percentage. You can customize the decimal places though the thousandth in default.

- **Byte format**

By default, Colasoft Capsa displays packets sizes and the traffic in an appropriate byte unit, such as **B**, **KB**, **MB**, **GB**, or **TB**.

Which unit is selected depends on how large each packet or the current traffic is. Users can define the unit from the combo box.

- **Bit format**

By default, Colasoft Capsa displays packets sizes and the traffic in an appropriate bit unit, such as **b**, **kb**, **Mb**, **Gb** or **Tb**.

Which unit is selected depends on how large each packet or the current traffic is. Users can define the unit from the combo box.

- **Bytes per second format**

Rate at which bits of information are transmitted. Colasoft Capsa displays the rate of information in an appropriate unit, such as **Bps**, **KBps**, **MBps**, **GBps** or **TBps**. Users can define a display format from the combo box.

- **Bits per second format**

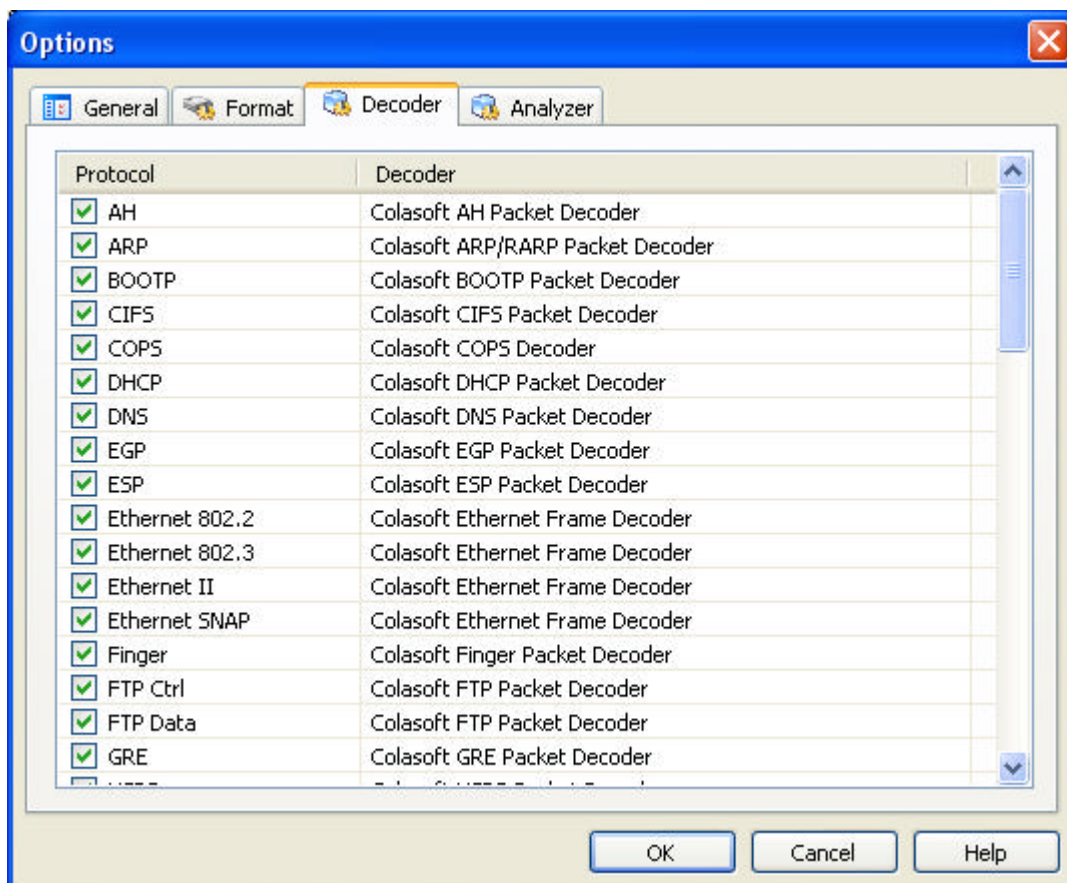
Rate at which bits of information are transmitted. Colasoft Capsa displays the rate of information in an appropriate unit, such as **bps**, **Kbps**,

Mbps, **Gbps** or **Tbps**. Users can define a display format from the combo box.

Options - Decoder

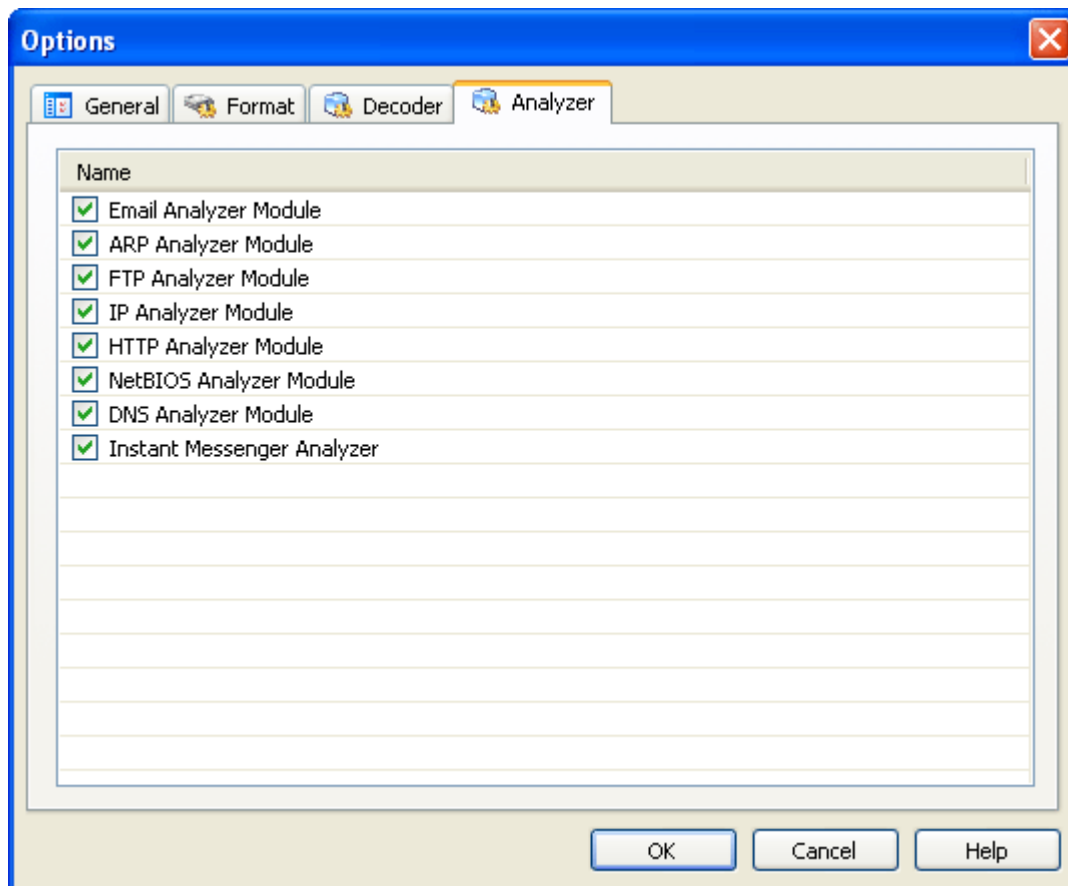
The packet decoders are the essential engines to decode packets. All available decoders are enabled by default, but you can close those you don't need to increase the program performance. If you close a decoder in the list, Colasoft Capsa will not decode the specific protocol elements when encounters a packet of the same type until you enable it again, as a result you can not view the decode information of that packet.

To open the **Options - Decoder** page, select **Options...** from the Tools menu and then press the **Decoder** tab. All decoders are listed by protocol and marked with a tick indicating they are enabled, use the check box before every decoder to disable it.



Options - Analyzer

The **Analyzer** page list the advanced analyzers, all of them are enabled in default. To reduce resource occupation and improve the global efficiency, users can close a analyzer by uncheck the box before it to get more clear view of the analysis results.

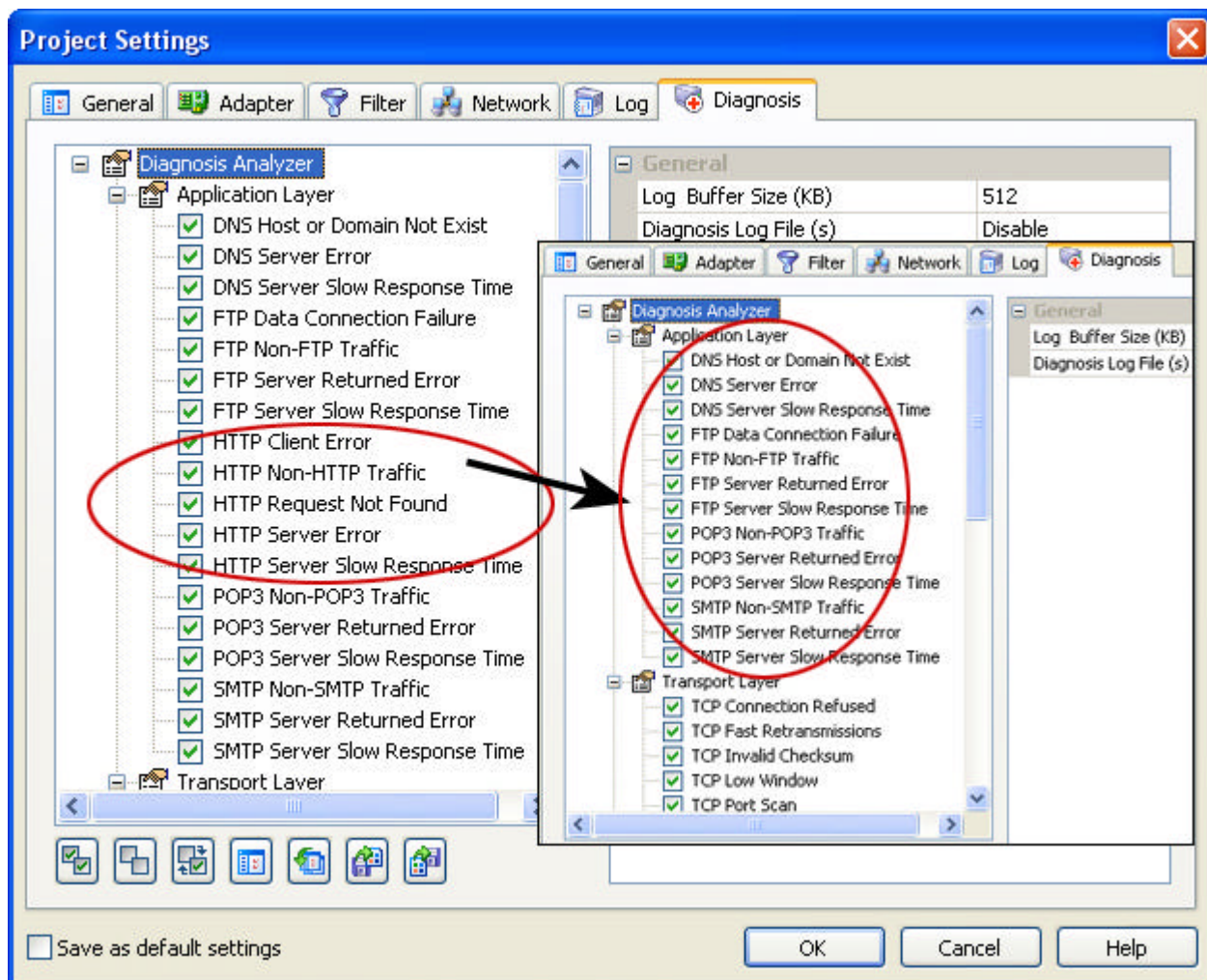


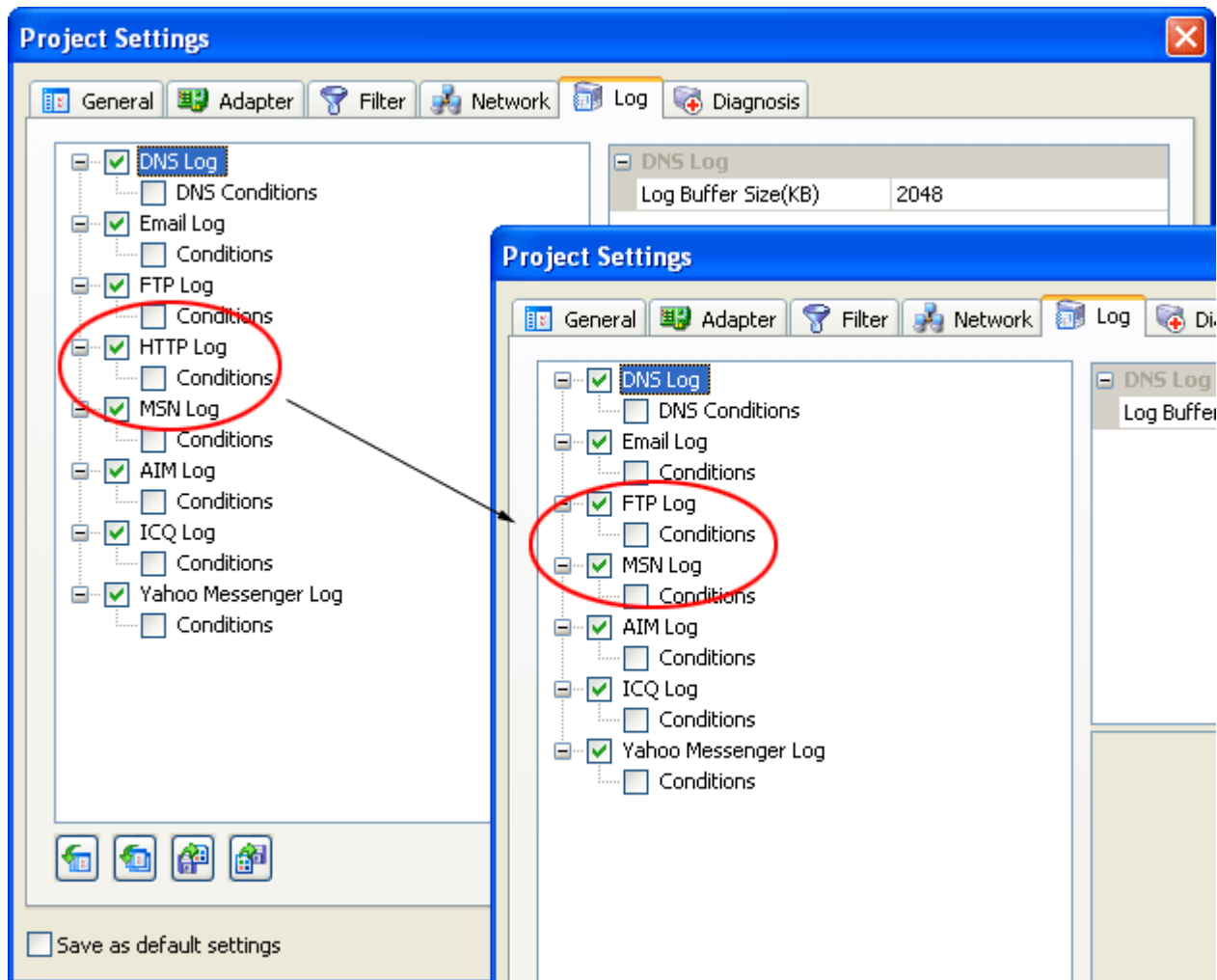
When you disable an analyzer in the **Analyzer** page, Colasoft Capsa will stop analyzing the corresponding protocol elements or displaying the analysis results in the relative views or settings until you enable it again. The following table is the views affected by every analyzer.

Analyzer	Relative views or settings
Email Analyzer Module	Summary view, Logs view, Reports view, Graphs view, Project Settings - Diagnosis, Project Settings - Log
ARP Analyzer Module	Diagnosis view, Reports view, Project Settings – Diagnosis
FTP Analyzer Module	Summary view, Logs view, Reports view, Graphs view, Project Settings - Diagnosis, Project Settings – Log
IP Analyzer Module	Diagnosis view, Reports view, Project Settings – Diagnosis
HTTP Analyzer Module	Summary view, Logs view, Reports view, Graphs view, Project Settings - Diagnosis, Project Settings – Log
NetBOIS Analyzer Module	Resolves host name passively if uncheck this module.
DNS Analyzer Module	Summary view, Logs view, Reports view, Project Settings - Diagnosis, Project Settings – Log

Instant Messenger Analyzer
Summary view, Logs view, Reports view, Project Settings - Diagnosis, Project Settings – Log

For example, uncheck the HTTP Analyzer Module. The statistic information **HTTP Analysis** in the **Summary** view, **Logs** view, **Reports** view, **Graphs** view and the **HTTP Requests** group in the **Logs** view are disable. And in the **Project Settings** dialog, the **HTTP Events** in the **Diagnosis** page and the **HTTP Log** in the **Log** page are disabled too.

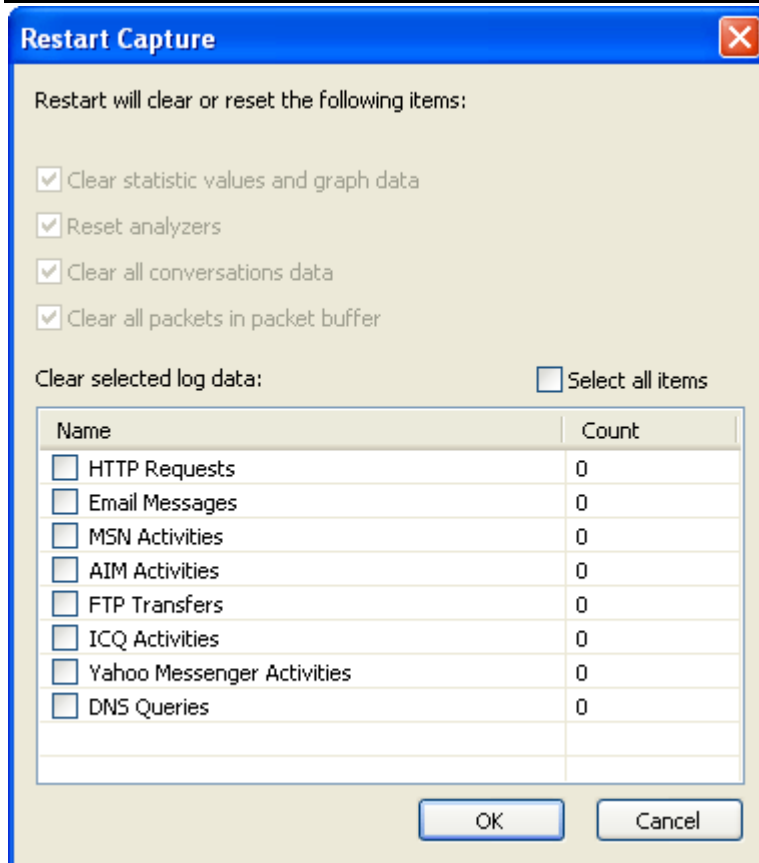




Restarting capture

When you stop the current capture, all of the packets currently in the buffer are retained. If you then restart capture, Colasoft Capsa will clear or reset some items from the packet buffer in order to keep the data displayed accurate and up to date. These items include statistic values, graph values, logs, conversations and the packets stored in the packet buffer.

The log data of advanced analyzers can be cleared optionally, including email messages, FTP transfers, HTTP requests, DNS analysis, four IM activities and diagnosis events. If you don't want to lose these data, you should save the project before restart capture.



Automatic capture

It is allowed to set Colasoft Capsa to automatically open a project and start capturing packets, the data saved in the project will be cleared.


On the default installation category of Colasoft Capsa, the command line would be started from:

C:\Program Files\Colasoft Capsa 5.0 Enterprise

To automatically open a project file .cscproj or load a template file .csctemp, the command would be:

Capsa50u.exe/autostart <Project File or Template File>

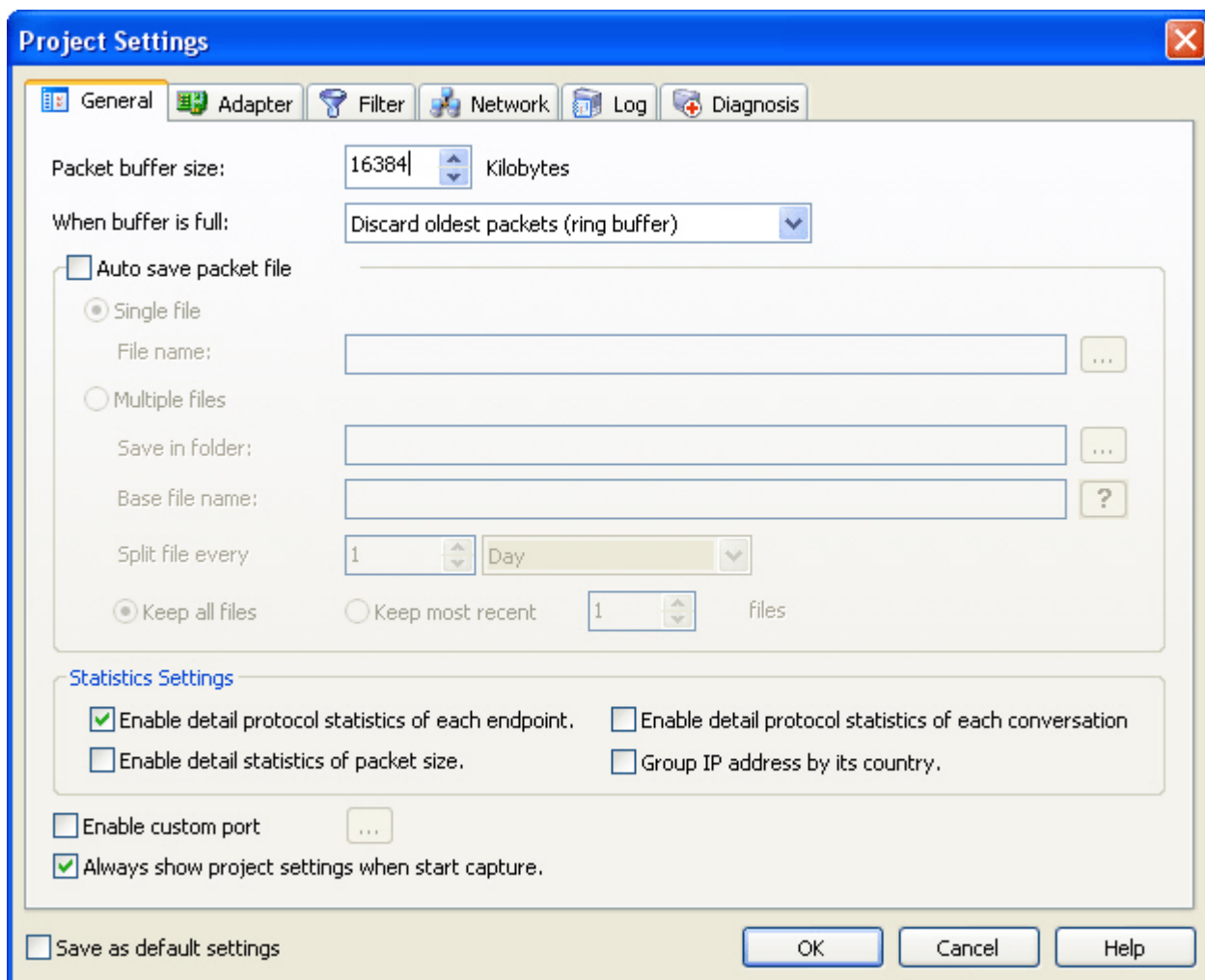
Project settings

In Colasoft Capsa, every project has its own adapters, filters and analyzers, the **Project Settings** dialog lets you customize the settings for the current project. You can define project settings before starting capture or during the process of capture. Click the **Settings**  button in the toolbar to open a **Project Settings** dialog, where you can make general options, change project adapter, add or modify filters, customize network profile, set conditions for logs and select diagnosis events.

Notice: If you check the **Set as default settings** option and confirm, the current project settings will be saved as default and will be applied to any new created project.

Project settings - general

This page provides some general project options.



The screenshot shows the 'Project Settings' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with tabs for 'General', 'Adapter', 'Filter', 'Network', 'Log', and 'Diagnosis'. The 'General' tab contains the following settings:

- Packet buffer size:** A text box containing '16384' and a unit dropdown set to 'Kilobytes'.
- When buffer is full:** A dropdown menu set to 'Discard oldest packets (ring buffer)'.
- Auto save packet file:** An unchecked checkbox.
- Single file:** A radio button selected. Below it is a 'File name:' text box and a browse button (...).
- Multiple files:** An unselected radio button. Below it are 'Save in folder:' and 'Base file name:' text boxes, each with a browse button (...).
- Split file every:** A text box containing '1' and a unit dropdown set to 'Day'.
- Keep all files:** A radio button selected.
- Keep most recent:** An unselected radio button. Below it is a text box containing '1' and a unit dropdown set to 'Files'.
- Statistics Settings:** A section with four checkboxes:
 - ☒ Enable detail protocol statistics of each endpoint.
 - ☐ Enable detail protocol statistics of each conversation.
 - ☐ Enable detail statistics of packet size.
 - ☐ Group IP address by its country.
- Enable custom port:** An unchecked checkbox with a browse button (...).
- Always show project settings when start capture:** A checked checkbox.
- Save as default settings:** An unchecked checkbox at the bottom left.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

- **Packet buffer size**

By default the packet buffer size is 16384 KB. You may change the value, but you must take the size of your system memory into account, because captured data is stored in the packet buffer and, when you save a project, the data contained in it will be saved to your hard disk.

The size you set will also affect the packet list view. The bigger size you set, the more packets you can see in the packet list view.

- **When buffer is full**

When the number of captured packets reaches the packet buffer size you have specified, Colasoft Capsa will do one of the following:

- **Discard oldest packets (ring buffer)**

It is recommended to discard the oldest packets when the packet buffer is full, Colasoft Capsa will store new packets and keep the packet buffer up to date.

- **Discard new packets**

All new captured packets will be discarded after being analyzed and will not be saved to the packet buffer.

- **Discard all old packets**

Colasoft Capsa will empty the packet buffer and then append new packets to it.

- **Stop capture**

Colasoft Capsa will stop capturing new packets.

Note: Don't choose this option if you would not like to cease capture.


- **Auto save packet file**

If checked, Colasoft Capsa will automatically save packets to a single file or split files as you define.

- **Single file**

All packets are saved to a same file.


- ♦ **File name**

Specifies a name for the packet file. Click the  button on the right to open a dialog for defining a save path for the packet file.


- **Multiple files**

Packets are saved to the files split by time or size. To reduce the total size, you may choose to only keep the most recent files.

- ♦ **Save in folder**

Specifies a folder name and the save path for all files. Click the  button on the right to open a dialog for defining a save path for the folder.

- ♦ **Base file name**

The portion of a file name to the left of the period separator. Colasoft Capsa allows very long file names. Click the  button to view an example of the base file name.

- ♦ **Split file every**

Chooses a rule for splitting the file if the file size is too big. You can split files by time or file size - months, days, hours, minutes, KB, MB.

- ♦ **Keep all files**

Saves all split files in the defined save path.

- ♦ **Keep most recent**

Specifies the number of most recent files for saving.

- **Statistics Settings**

You can save system resources if uncheck the following statistics options.

- **Enable detail protocol statistics of each endpoint.**

If check this option (by default), you will not see detail protocol statistic information of endpoints (except root nodes).

- **Enable detail statistics of packet size.**

If uncheck this option (by default), you will not see the statistics of **Most Common Packet Sizes** in the **Summary** view.


- **Enable detailed protocol statistics of each conversation**

If check this option (by default), you will not see the detailed protocol statistics of each conversation in the **Conversations** view.

- **Group IP address by its country**

If uncheck this option (by default), the captured IP addresses will not be grouped under countries in the **IP Explorer** group of the **Project Explorer** dock window.

- **Enable custom port**

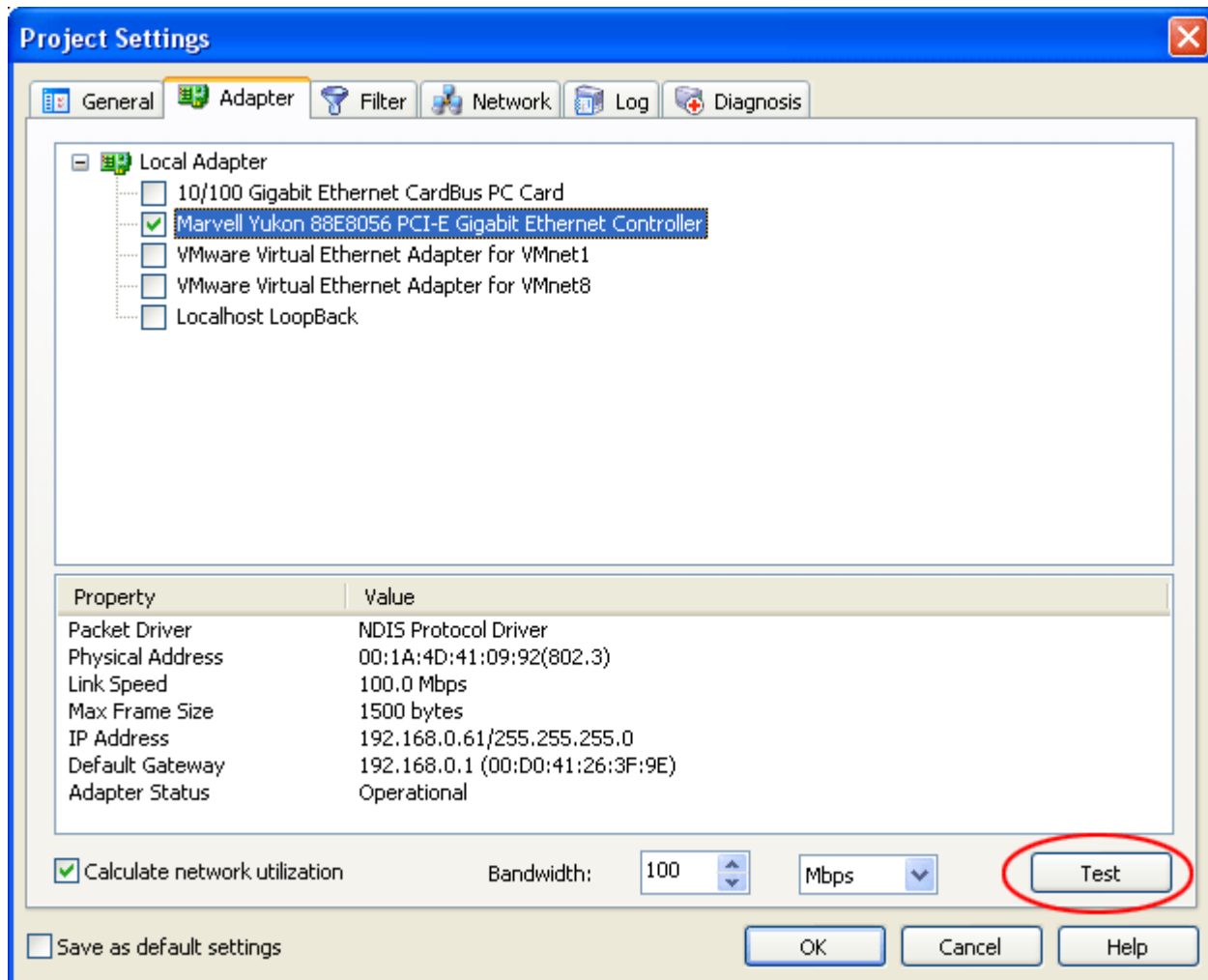
Check this option if you want Capsa to monitor non-standard ports, and then click the button  to add ports.

- **Always show project settings when start capture**

If checked, Colasoft Capsa will always open the **Project Settings** dialog every time when you start a new capture.

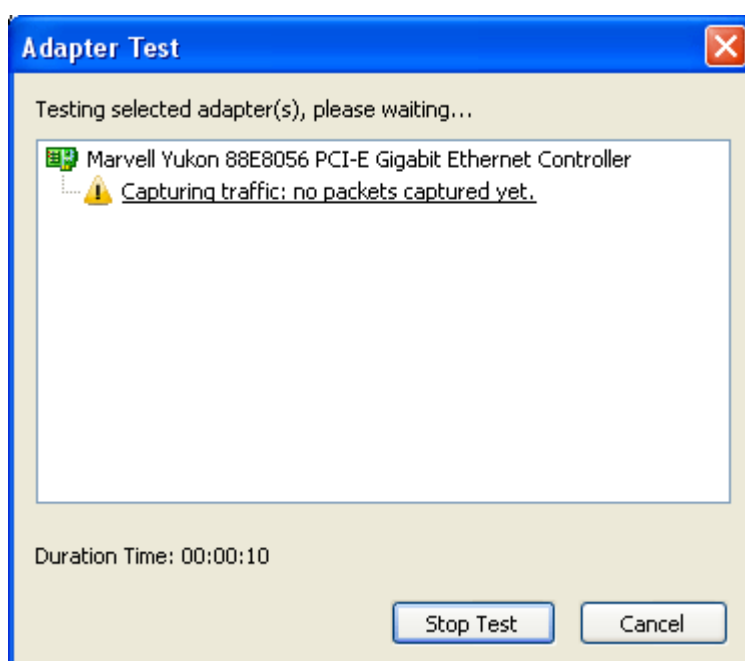
Project settings - adapter

Each time when you start a new capture, you are required to select the adapter. Available adapters are listed in the **Project Settings - Adapter** page, you can choose one or more adapters (only one adapter can be opened in the professional edition) for the current project. When an adapter is highlighted, some brief descriptions about this adapter will be showed on the lower **Property** pane. In this page you can also test the selected adapter. See "[Capture sources](#)" for more references.

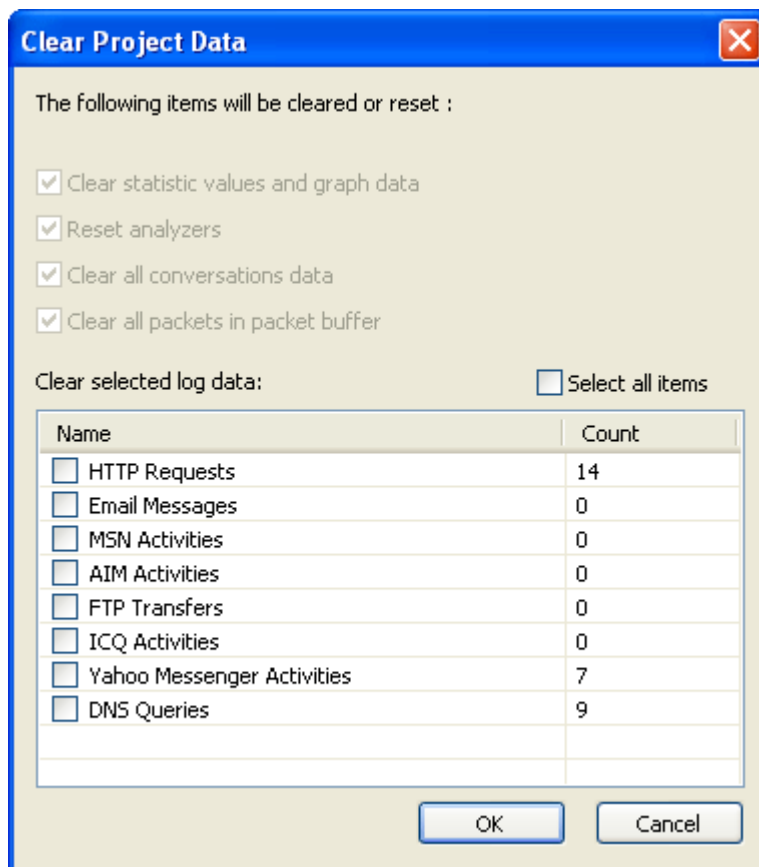


- **Test**

To test a adapter you just need to select on adapter and click test at the right bottom, a dialog box will pop up and show the test information.

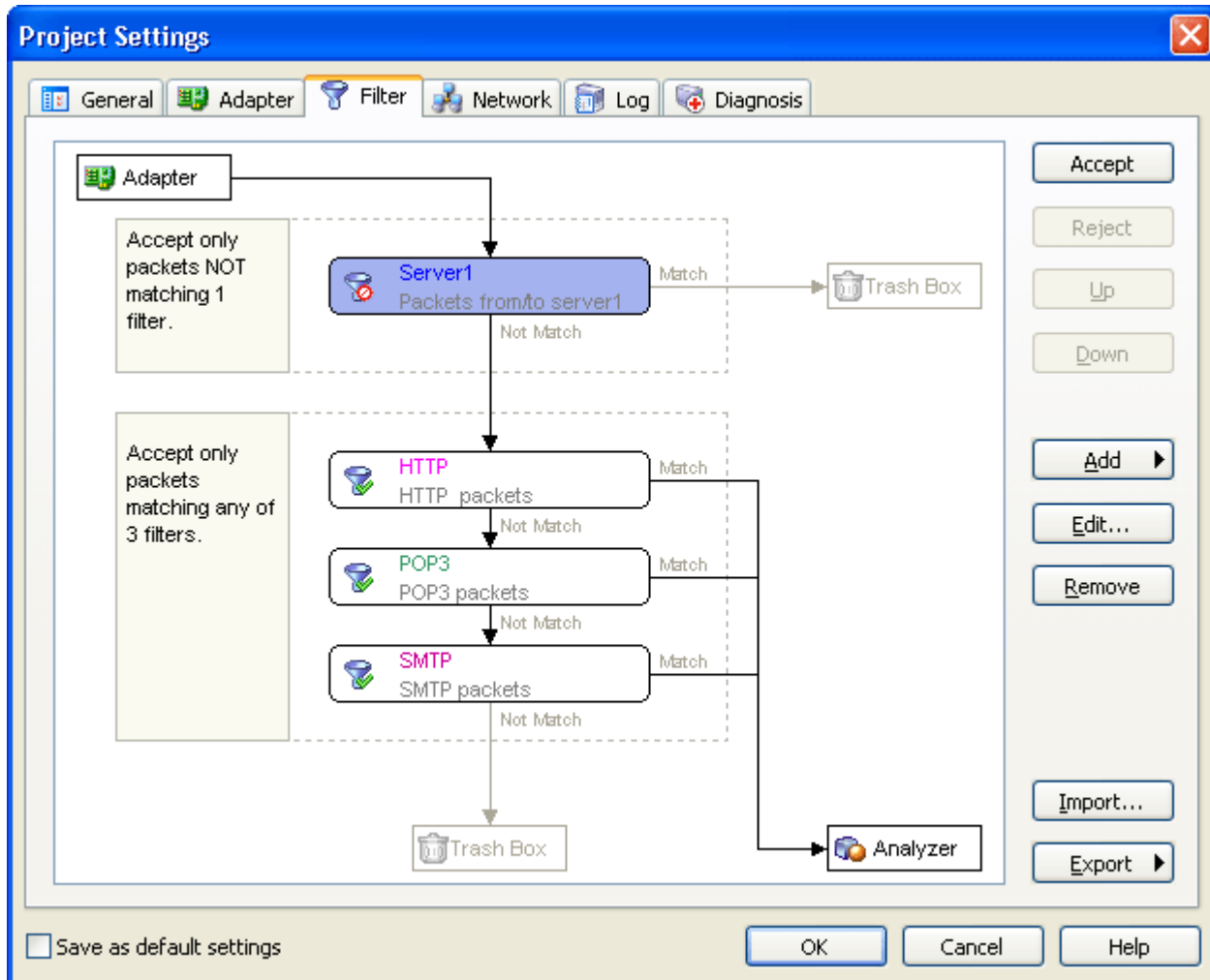


It is allowed to change adapter during the capture process, however, in order to keep the data displayed accurate and up to date, any change to adapter settings will clear or reset some project items, e.g. statistic values, graph data, analyzers, conversations and packet buffer. Log data are optionally cleared, including email messages, FTP transfers, HTTP requests and diagnosis event logs.



Project settings - filter

This page allows you to set filters for analyzing packets. You can add a new filter or select from the **Filter Table** lists some predefined filters, or import filter from a file.



- **Accept**

By clicking this button (if applicable), you can change the current filter's status, Colasoft Capsa will accept the packets matching this filter for analysis.

- **Reject**

By clicking this button (if applicable), you can change the current filter's status, Colasoft Capsa will not accept the packets matching this filter for analysis.

- **Up**

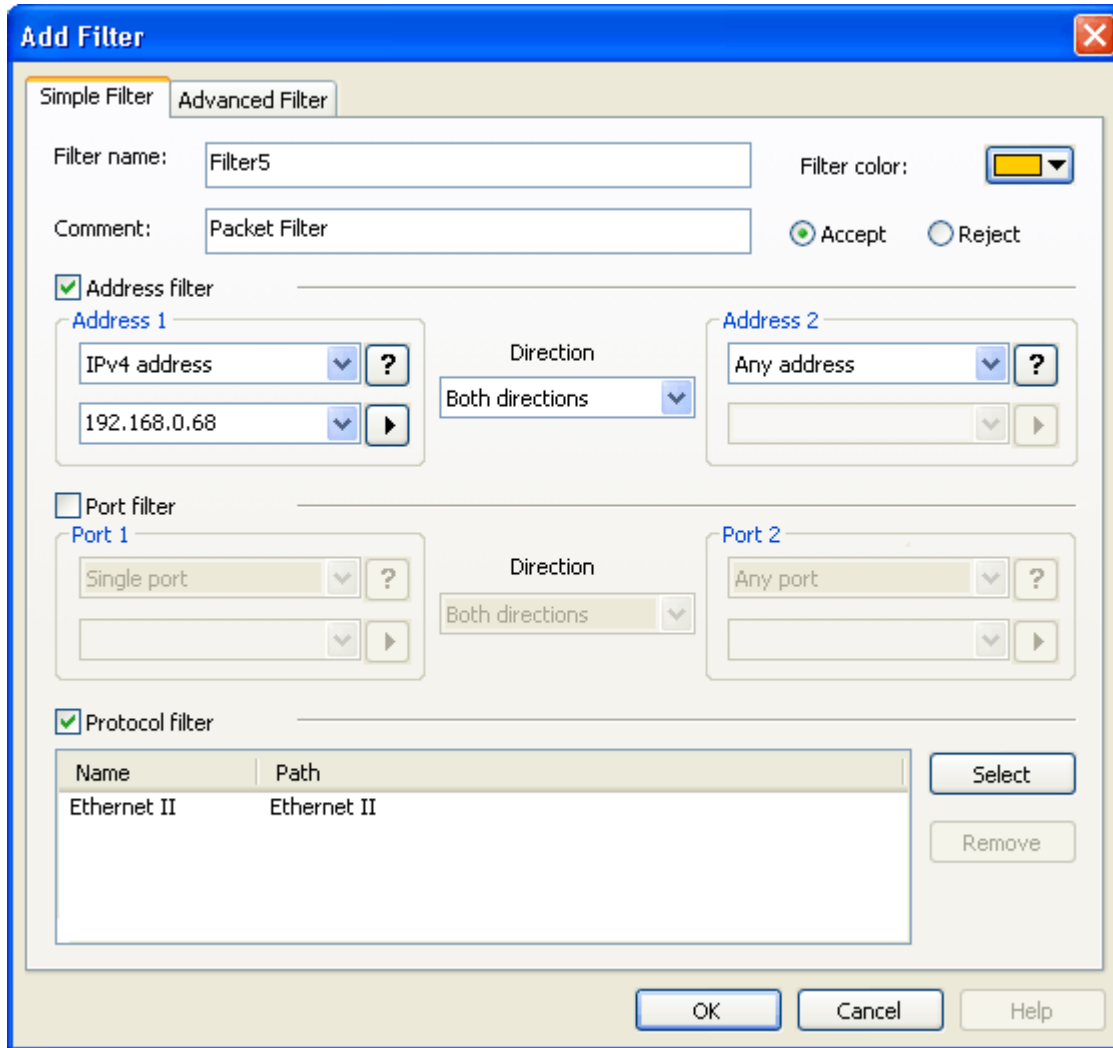
By clicking this button (if applicable), you can move up the current filter.

- **Down**

By clicking this button (if applicable), you can move down the current filter.

- **Add**

Click on this button and choose to create a new filter or add from the **Filter Table**. When you choose **New**, Colasoft Capsa will open the **Add Filter** dialog, where you can insert a simple filter or an advanced filter. When you choose **From Filter Table**, you can check one or more predefined filters and decide the rule. The new added filters will be graphically displayed one by one, which status and position can be changed with the **Accept**, **Reject**, **Up** or **Down** button.




The **Add Filter** dialog box is shown with the **Advanced Filter** tab selected. It contains the following fields and controls:

- Filter name:** Filter5
- Filter color:** A color selection dropdown showing yellow.
- Comment:** Packet Filter
- Accept/Reject:** Radio buttons for **Accept** (selected) and **Reject**.
- Address filter:** A checked checkbox.
 - Address 1:** A dropdown menu set to **IPv4 address** with a value of **192.168.0.68**.
 - Direction:** A dropdown menu set to **Both directions**.
 - Address 2:** A dropdown menu set to **Any address**.
- Port filter:** An unchecked checkbox.
 - Port 1:** A dropdown menu set to **Single port**.
 - Direction:** A dropdown menu set to **Both directions**.
 - Port 2:** A dropdown menu set to **Any port**.
- Protocol filter:** A checked checkbox.
 - A table with two columns: **Name** and **Path**.

Name	Path
Ethernet II	Ethernet II
 - Select** and **Remove** buttons.

At the bottom are **OK**, **Cancel**, and **Help** buttons.

- **Edit...**

To modify the current filter, click the **Edit...** button and open the **Modify Filter** dialog, note that the modifications made from this dialog is only project-related. To modify the filters in the global **Filter Table**, you must open the **Filter Table** by clicking the button  in the toolbar.

- **Remove**

When this button pressed down, the current filter will be removed from filter list and can not be recovered.

- **Import...**

You can import filter from a saved filter file.

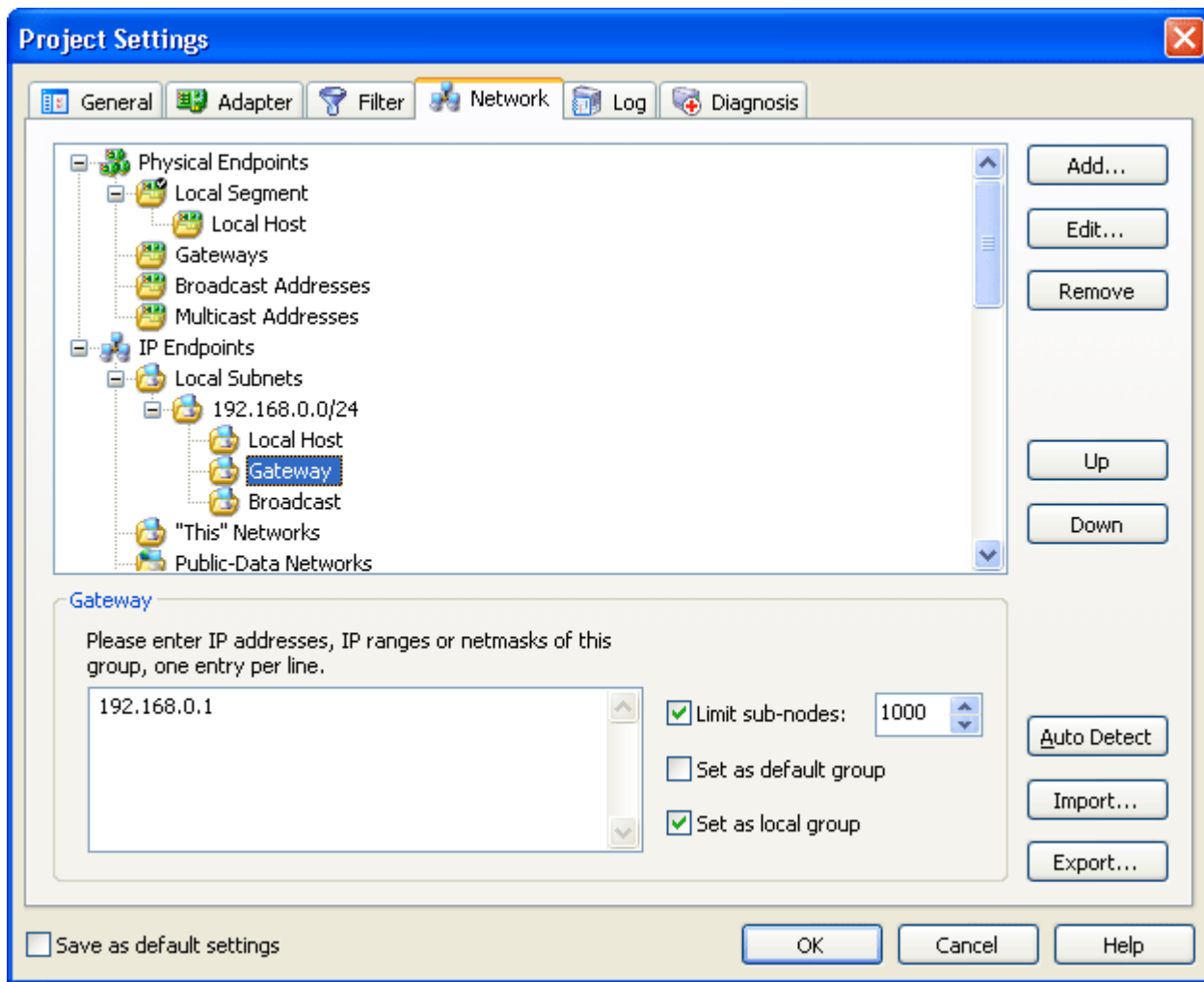
- **Export**

Click on this button and choose to export all filters or just selected ones.

Project settings - network

Colasoft Capsa lets you configure your own network profile (enterprise edition only). In the **Network** page of **Project Settings**, you can customize one or more physical endpoints or IP endpoints, accordingly the network nodes in the **Project Explorer** will be reassigned or renamed.

The **Auto Detect** button is to automatically detect your network configuration, you may also load a network profile from a file, or save your current settings to a file.



- **Add**
By clicking this button (if applicable), you can add a new group as a sub-group in the selected group.
- **Edit**
By clicking this button (if applicable), you can change the group's name.
- **Remove**
Deletes a selected group from the list (if applicable).
- **Up**
By clicking this button (if applicable), you can move up the current group.
- **Down**
By clicking this button (if applicable), you can move down the current group.
- **Auto Detect...**
Auto detects the settings of current NIC, gains the information of network configuration and the gateway.
- **Import...**

Import a network profile in *.cscnet format.

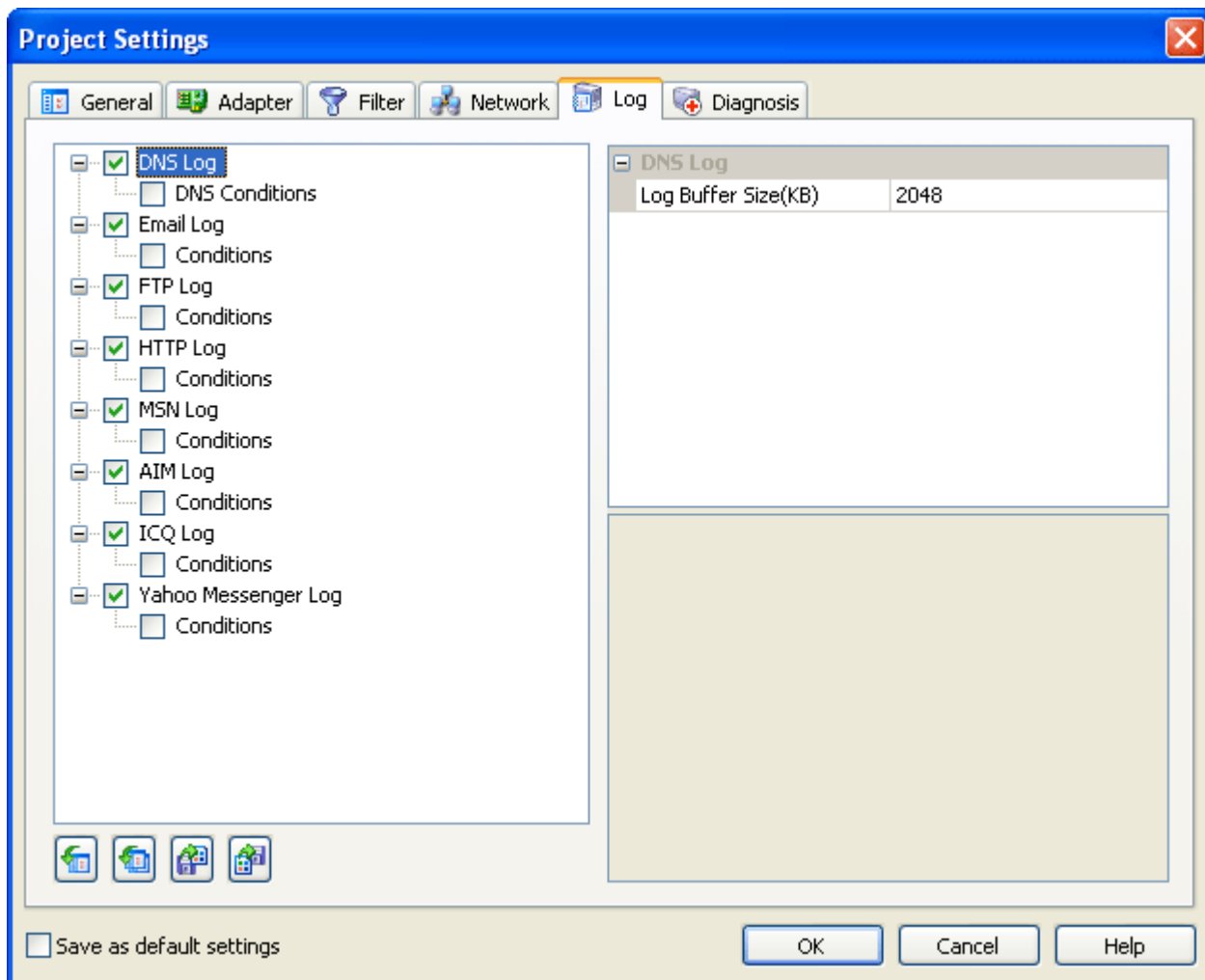
- **Export...**

Export the current network profile to file in *.cscnet format.

Project settings - Log

Log setting dialog box is a place where you can set up conditions for these listed logs. You can also reset conditions to the default settings, or import a specific log setting, or export the current log settings. To save the current settings as default settings you need to tick in the bottom box. You can open this dialog box by clicking the **Log** button in the toolbar. .

The settings or modifications made in this page will impact the results displayed in the **Logs** view.



- **Reset**

Resets the selections to default position.

- **Reset All**

Resets all selections to default position.

- **Import**

Import a log file in *.cscdiag format.

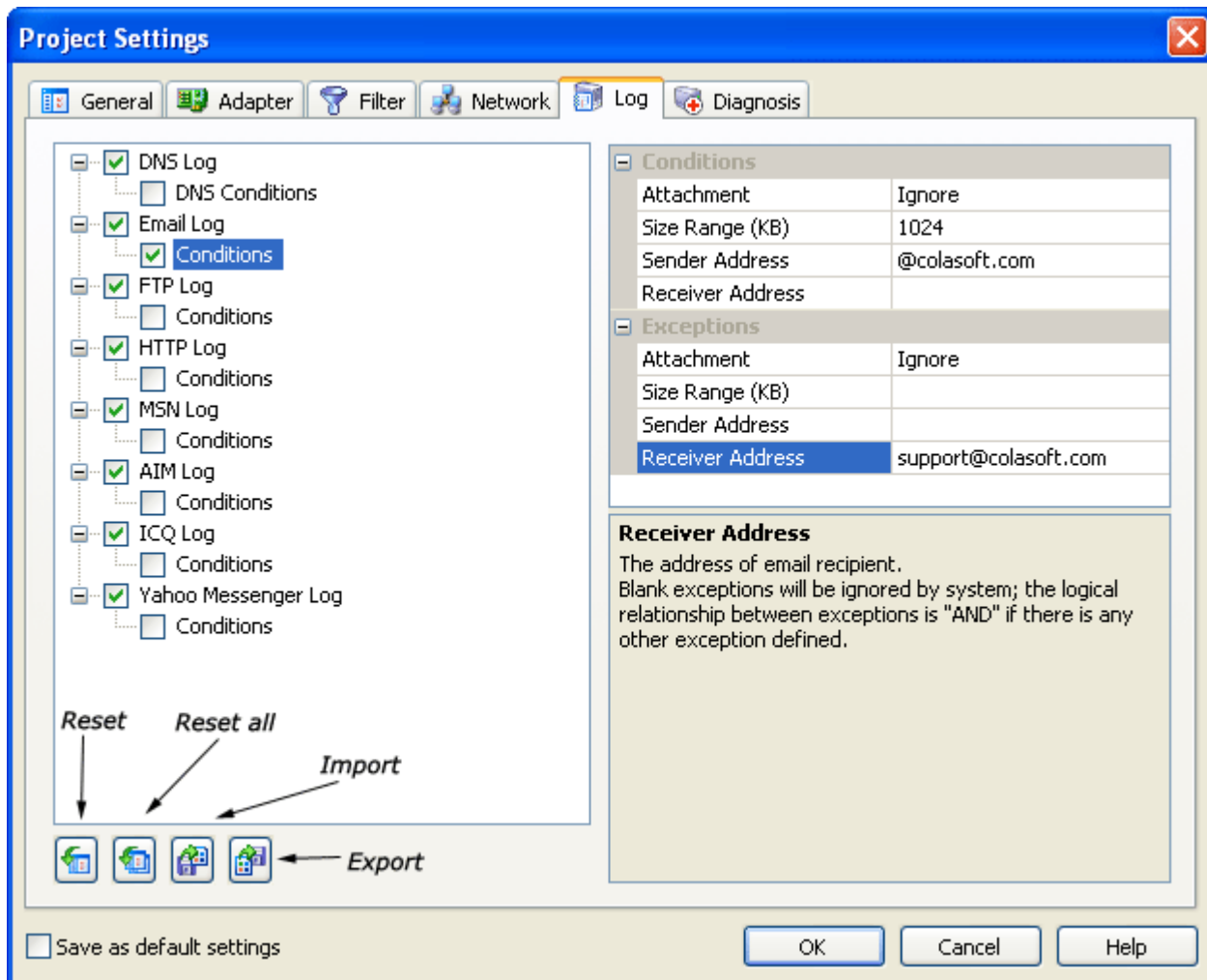
- **Export**


Export the current settings of log page into a file in *.csdiag format.

Email log

In the setting page, you can define the email log's buffer size, select log file format, enable Colasoft Capsa to save email contents and set conditions for the display of email logs. The settings or modifications made in this page will impact the results displayed in the **Logs - Email Messages** view.

See the figures below as setting examples.



By default, the email log is enabled and the log buffer size is preset as 1024 KB. If you disable the email log, you can not see any email log information from the **Logs - Email Messages** view. The log buffer size is customizable; when the email log buffer is full, Colasoft Capsa will discard the oldest email logs and append the new ones to it. By clicking the browse button  and check **"Save log file to disk"**, you can select to save all captured email logs to a single file or multiple files which are split by time or size.

- **Conditions**


Check this option and then you can define one or more conditions for logging, blank conditions will be ignored by system, system will log all items if there is no condition defined; the logical relationship between conditions is "AND" if there are more than one condition defined.

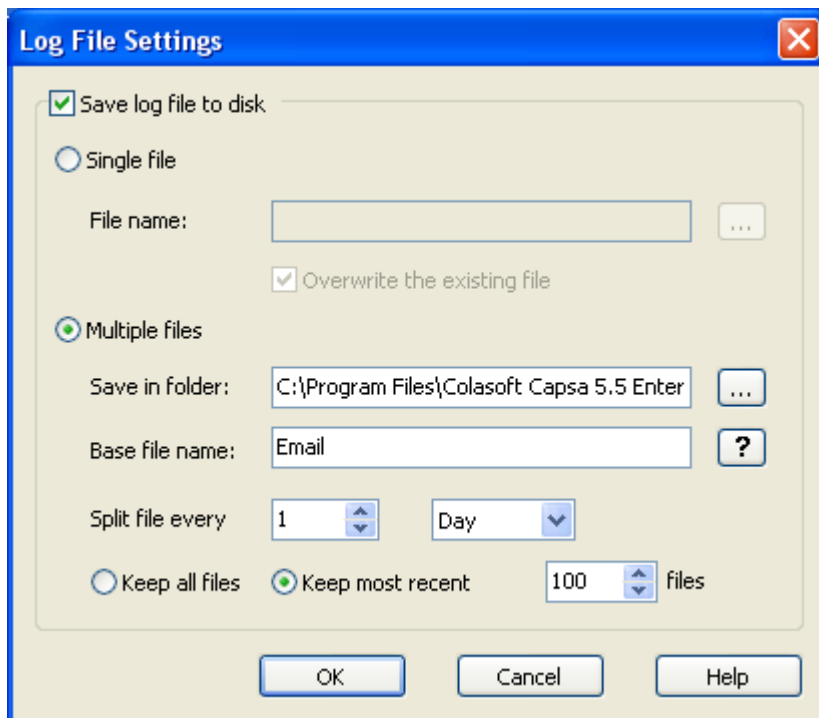
Exceptions

Define the logging conditions of being excluded by system, the logical relationship between exceptions is "AND" if there are more than one exception defined.

Save Email Contents

To view the real contents of a logged email, you must enable Colasoft Capsa to save email contents and designate a location in advance. When this option is disabled (by default), you can only see email log information in the **Logs - Email Messages** view and can not open the email.


By clicking the browse button  and check **Save log file to disk**, you can select to save all captured email logs to a single file or multiple files which are split by time or size.



- **Single file**

All packets are saved to a same file.


- **File name**

Specifies a name for the packet file. Click the  button on the right to open a dialog for defining a save path for the packet file.


- **Multiple files**

Packets are saved to the files split by time or size. To reduce the total size, you may choose to only keep the most recent files.

- **Save in folder**

Specifies a folder name and the save path for all files. Click the  button on the right to open a dialog for defining a save path for the folder.

- **Base file name**

The portion of a file name to the left of the period separator. Colasoft Capsa allows very long file names. Click the .

button to view a example of the base file name.

- **Split file every**

Chooses a rule for splitting the file if the file size is too big. You can split files by time or file size - months, days, hours, minutes, KB, MB.

- **Keep all files**

Saves all split files in the defined save path.

- **Keep most recent**

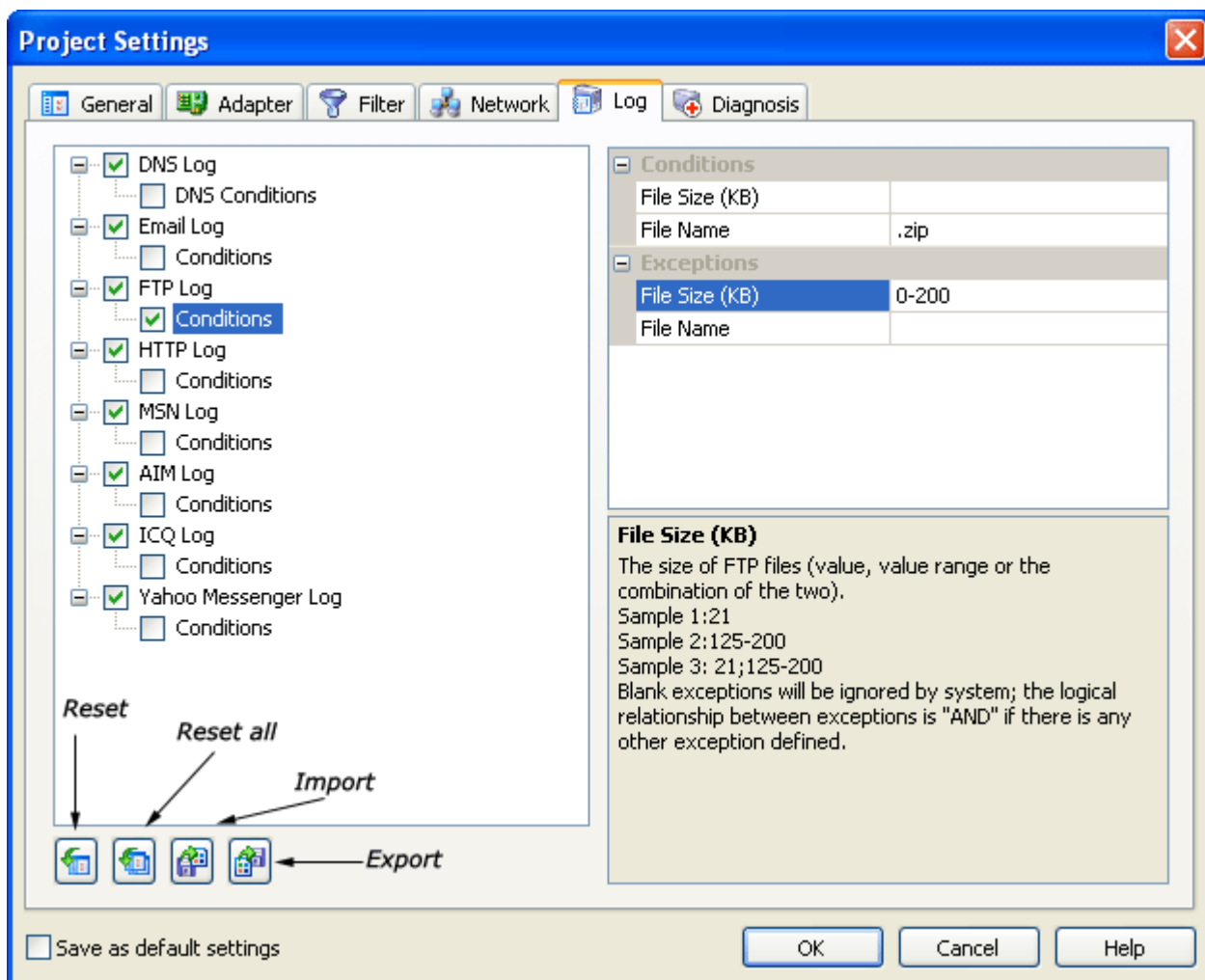
Specifies the number of most recent files for saving.

FTP transfer log

In the setting page, you can define the FTP log's buffer size, select log file format, and set conditions for the display of FTP logs. The settings or modifications made in this page will impact the results displayed in the **Logs - FTP Transfers** view.

The setting operations in this page are similar as email log, please refer to **Email log** for more descriptions.

See the figure below as setting examples.

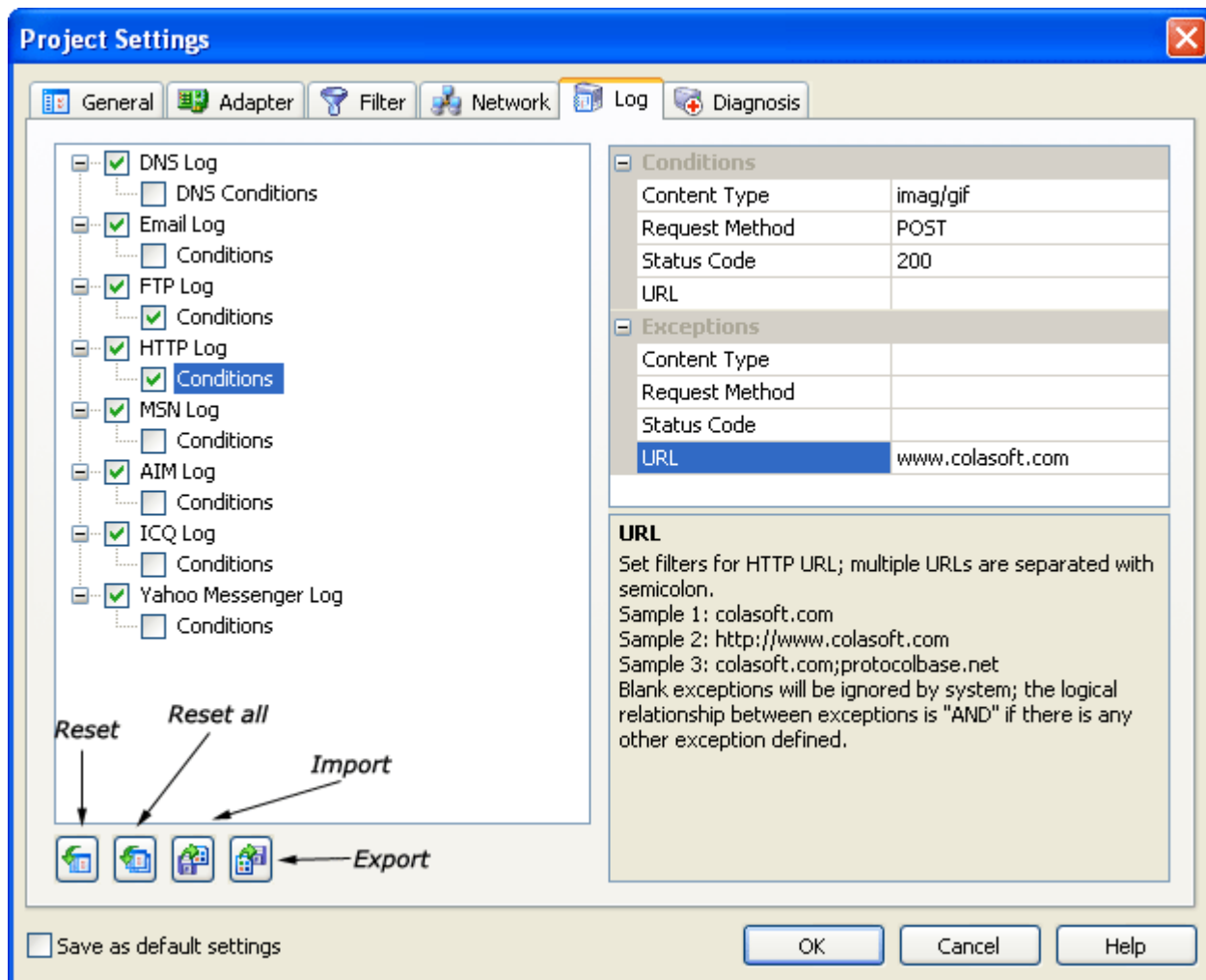


HTTP log

In the setting page, you can define the HTTP log's buffer size, select log file format, and set conditions for the display of HTTP logs. The settings or modifications made in this page will impact the results displayed in the **Logs - HTTP Transfers** view.

The setting operations in this page are similar as email log, please refer to **Email log** for more descriptions.

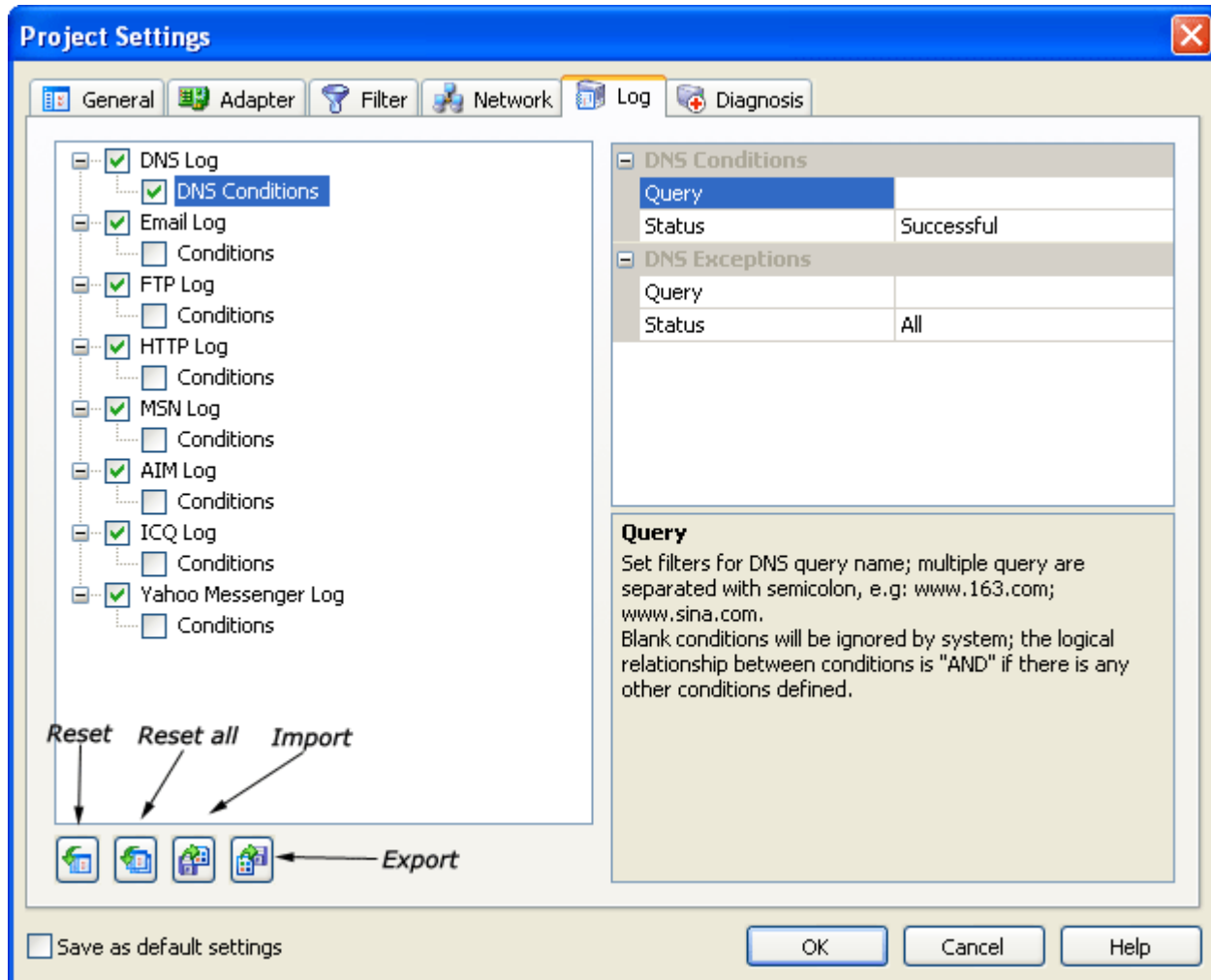
See the figure below as setting examples.



DNS log

In the setting page, you can define the DNS log's buffer size, select log file format, and set conditions for the display of DNS logs. The settings or modifications made in this page will impact the results displayed in the **Logs - DNS Analysis** view.

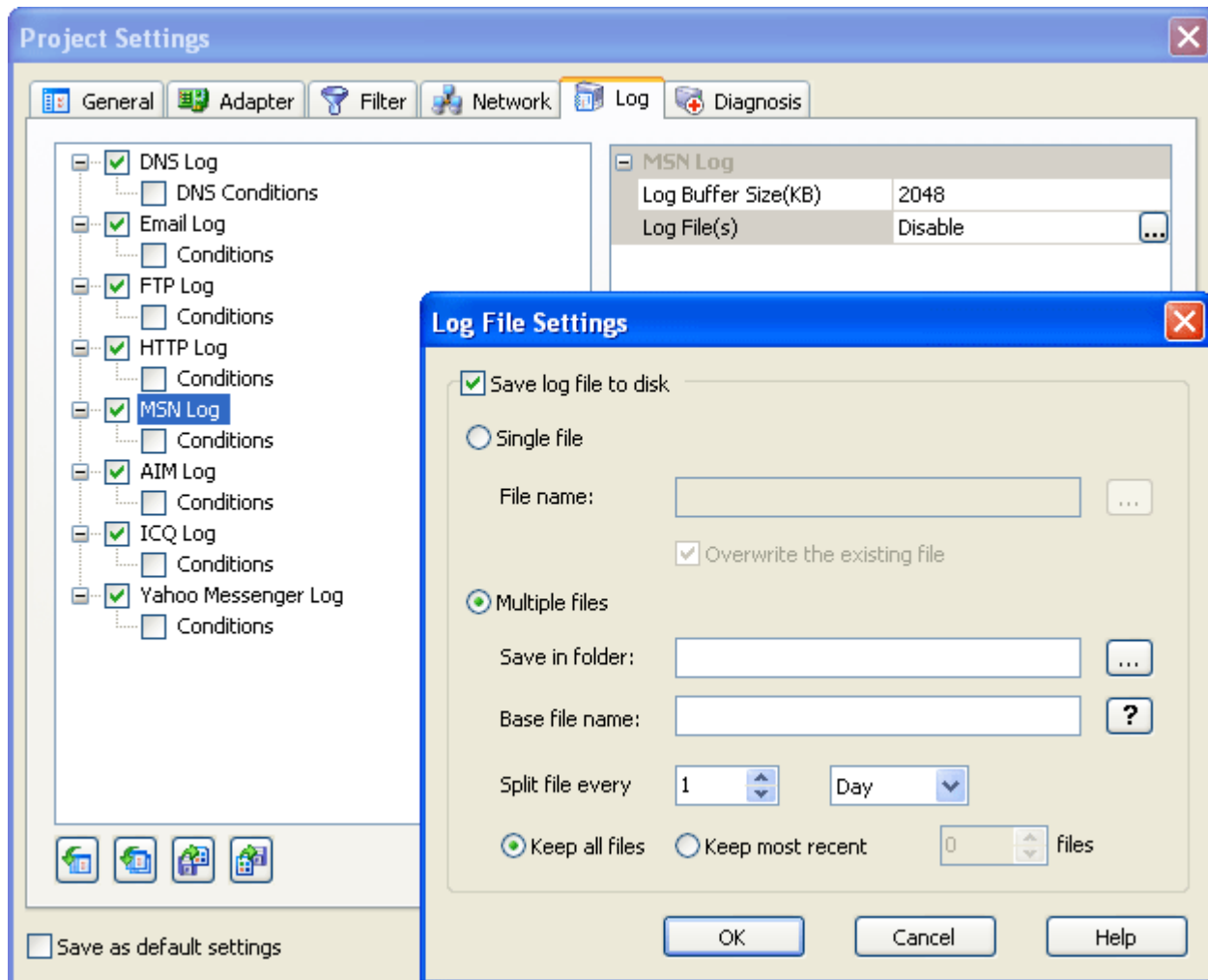
See the figures below as setting examples.



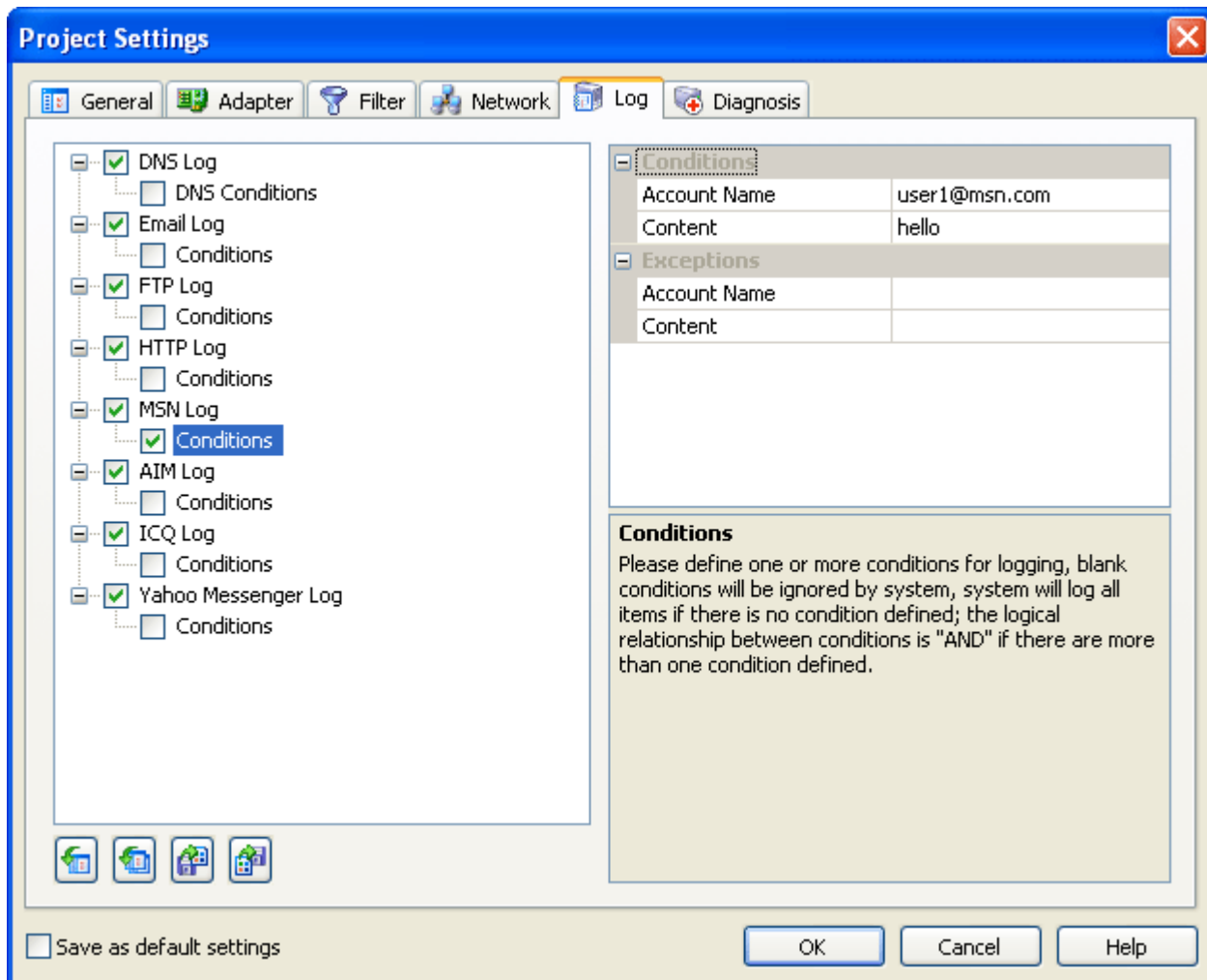
MSN Log

To enable MSN log settings, you have to tick in the box next to "MSN Log". In this dialog box you can define the log buffer size(KB) and decide whether to save log files to disk.

If you want to save the log files in the disk for future reference, you can click "...", then a "Log File Settings" dialog box will pop up, where you can make detailed saving settings.



Conditions is a place where you can make settings for Account Name and Content. Blank conditions will be ignored by system, system will log all items if there is no condition defined.



The settings or modifications made in MSN Log page will affect the results displayed in the Logs - MSN Activities view.

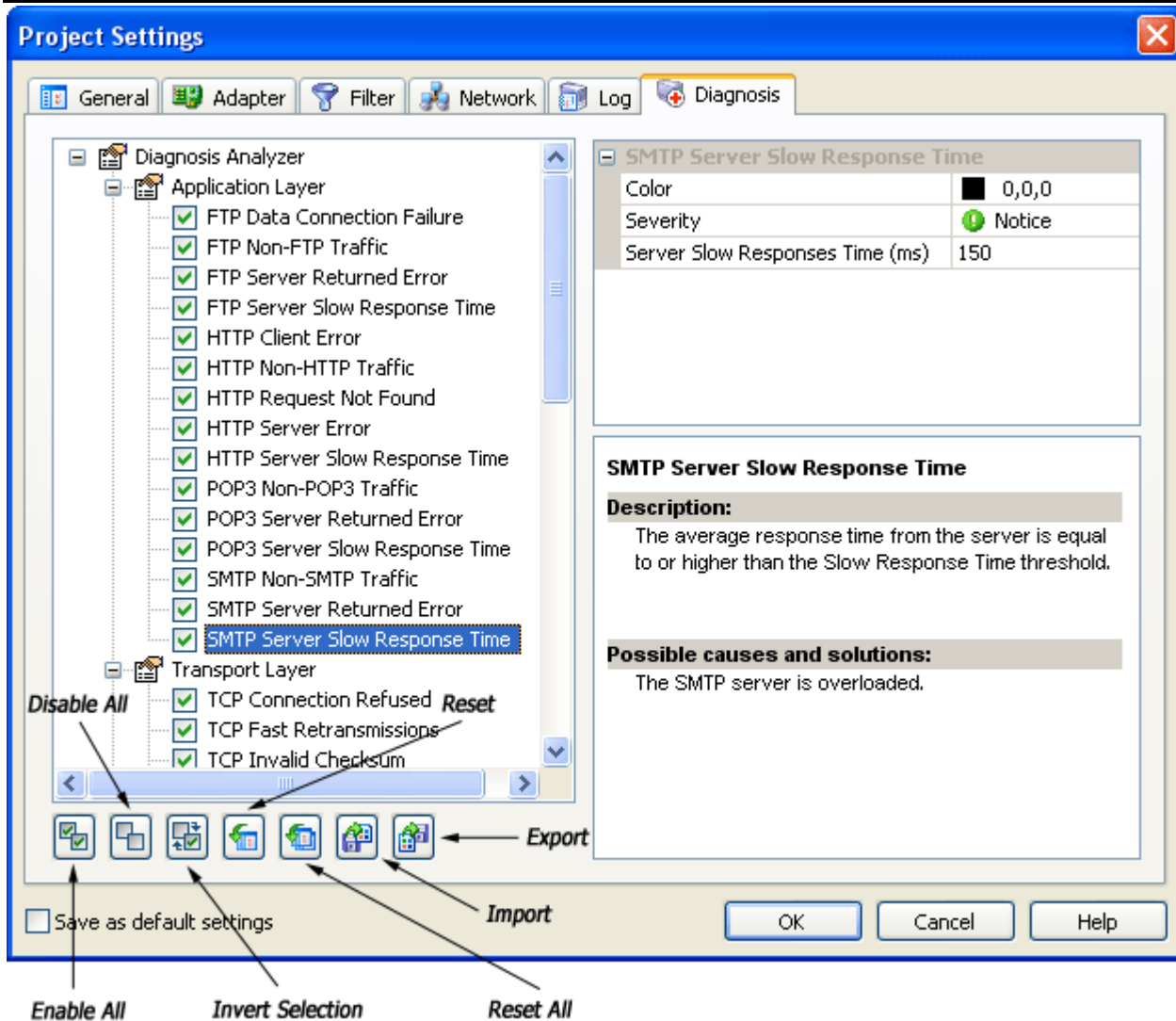
Other IM Logs

The settings or modifications of other IM Logs are similar with that of **MSN Log**; please refer to **MSN Log** for more information

Project settings - Diagnosis

This setting page lists all available diagnosis events, all are enabled by default. You can view the description and other references for an event in the right section when it is highlighted in the left section, the color, severity level and some other parameters (if applicable) can be customized.

If you disable a diagnosis event in this page, you will not see it in the **Diagnoses** view.



- **Enable All**
Enables all listed diagnosis events, Colasoft Capsa will diagnose all network events. The more diagnosis events enabled the more resource and memory will be occupied.
- **Disable All**
Disables all listed diagnosis events, Colasoft Capsa will not diagnose network event.
- **Invert Selections**
Inverts the position of all events.
- **Reset**
Resets the selections to default position.
- **Reset All**
Resets all selections to default position.
- **Import**
Imports a diagnosis file in *.csdiag format.
- **Export**

Exports the current settings of diagnosis page into a file in *.cscdiag format.


Data management

When your project buffer is full, Colasoft Capsa will discard some packets to keep the displayed packets up-to-date, use the assistant functions of Colasoft Capsa you can protect important packet information from being discarded. Colasoft Capsa allows you to copy, export, print and import packet information, details are described in the sections below.

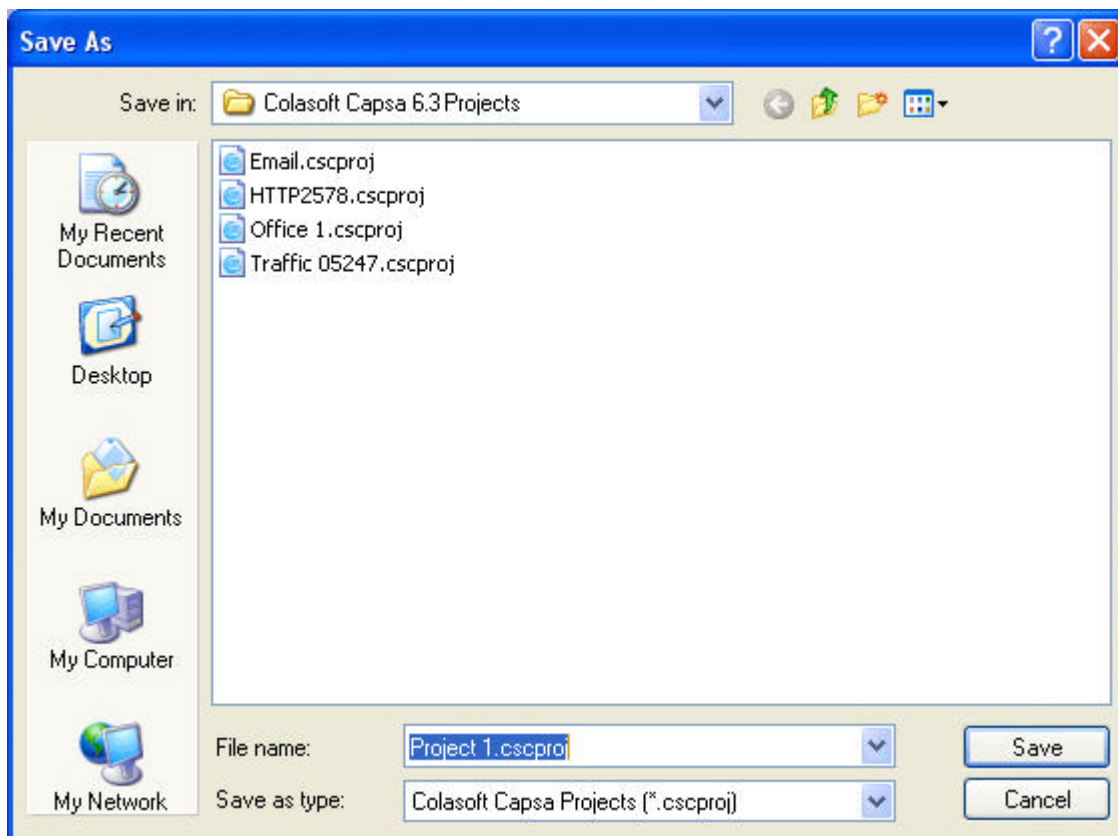
Saving

Saving a project


To save a project with all its settings and captured packets, you can:

- Use standard keyboard command **Ctrl + S**.
- Click the icon  in the **Toolbar**.
- Select the **Save** command from the **File** menu.

The project will be saved as .cscproj file and stored in hard disk, when you want to have a review in the future, use the **Open** command from the **File** menu or **Start Page** and select the file name to open it.



Saving project data

By clicking the **Save As** icon , you can save project data from the **Summary** view, **Diagnoses** view, **Endpoints** view, **Protocols** view, **Connections - General** and **Connections - Stream** view to a text file. The charts in the **Graph** view can be saved in .bmp format.

Saving as template

You may save the settings defined to a template file and be applied to new projects in future. There are two ways to save as template:

- **Save from the File menu**

Open the File menu and select **Save As Template...**

- **Save from the Project Settings dialog**

Click the **Save As Default Template...** button from any page of the **Project Settings** dialog.

Copying and pasting

If you want to save packet information to a file, you can make a selection first in the project window (use the **Shift** key or the **Ctrl** key to select multiple items, if applicable), right click and choose a **Copy** command, then open a file and paste the selection to it.

There are several kinds of **Copy** command in Colasoft Capsa:

Command	Description
Copy	Copies the selected item in text format.
Copy Tree	Copies all involved items in a tree.
Copy Hex	Copies the Hex contents of packet decode.
Copy Text	Copies the text contents of packet decode.
Copy Column	Copies a specific column in text format.

Copied contents can be pasted to Excel, Word, and other Windows applications.

Importing and exporting

Import from a file

In addition to the files in *.cscpkt (Capsa 5.x and 6.x Packet File) and *.cpf (Capsa 4.0 Packet File) format, you may also import data from Network Associates Sniffer packet files, EtherPeekv7/ TokenPeek / AiroPeekv9 / OmniPeekv9 packet files, *.dmp (TCP DUMP) and raw packet files. The Matrix view will blank and the Conversations view will displayed as Connections view if import a project file or packet file of version 5.5 or before.

Import steps:

- Select **Import from File...** from the **File** menu.
- Specify the file name, file type and open mode in the opened dialog.
- Confirm your operation in the enquiry dialog.
- A pop-up dialog will inform you when the file is successfully imported.

Import Option
✕

File Information

Create Time:	2006-01-12 02:23:35	File Size:	1.635 MB
File Format:	Colasoft Capsa 5.5 Packet File	Packet Count:	4698
First Packet Time:	2006-01-12 10:22:52	Last Packet Time:	2006-01-12 10:23:34

☐ **Range**

2006-01-12 10:22:52
2006-01-12 10:23:34

☒ **By time:**

2006-01-12 10:22:52
2006-01-12 10:23:34

☐ **By No.:**

1
940
1879
2819
3758
4698

☐ **By size:**

0 B
327.566 KB
655.133 KB
0.960 MB
1.280 MB
1.599 MB

Packet Buffer

Packet Buffer Size: Kilobytes


When buffer is full, discard oldest packets (ring buffer)
▼

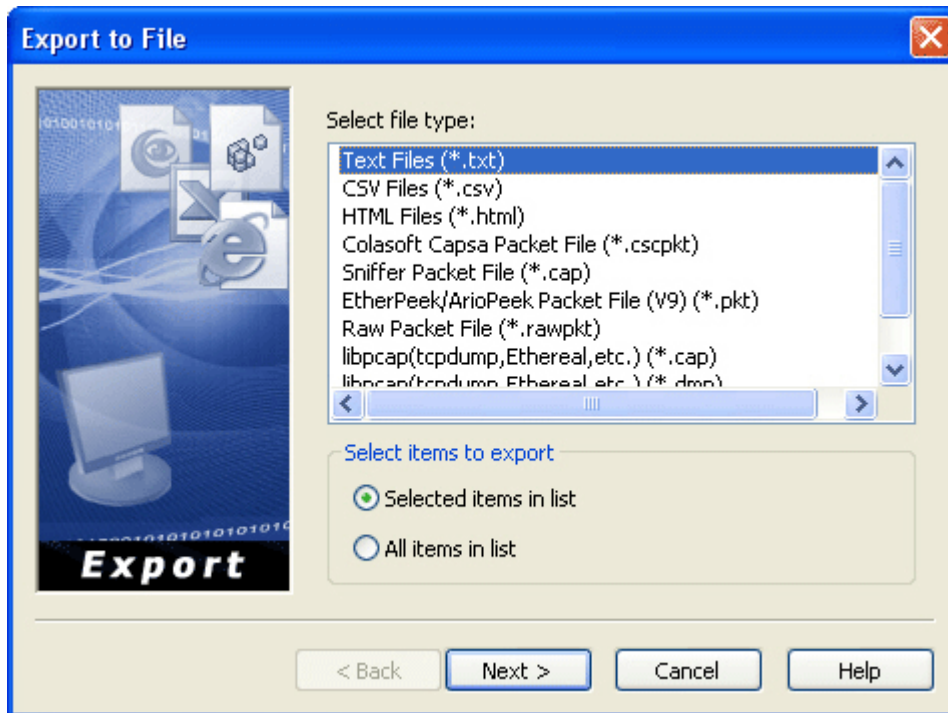
< Back
Next >
Finish
Cancel
Help

Export to a file

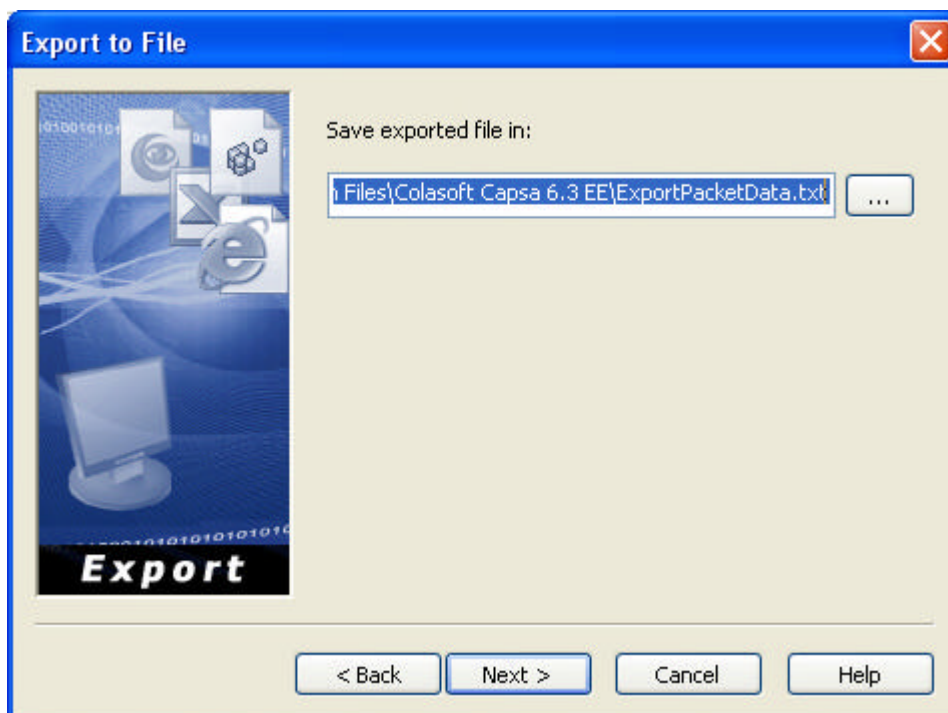
Captured packets and related information can be exported to a file in public formats such as Text and HTML. Packet list information can be exported from the **Packets** view, **Connections** view and **Logs** view.

Export steps: (take the **Packets** view as an example)

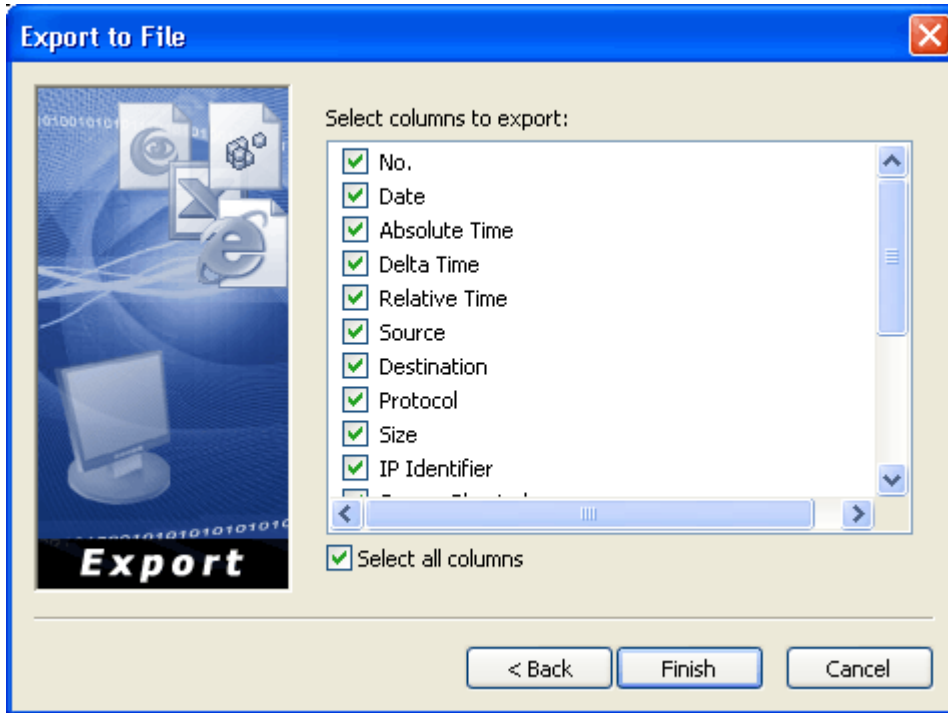
- Highlight the selected packets (use **Shift** or **Ctrl** key to select multiple items).
- Right click and select **Export Packet...**, or click the icon  from the toolbar.
- Specify the file type and items in the opened dialog.



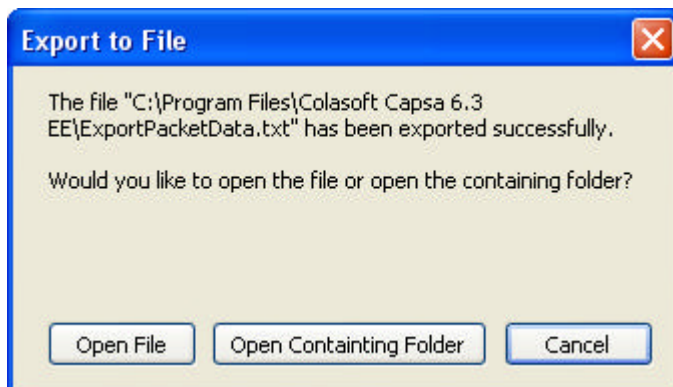
- Define the path to save the export file.




- Check the columns you want to export (only applicable for *.txt, *.csv and *.html format), then finish the export.



- A dialog will inform you when packets have been exported successfully; you can open the file from the dialog directly.



Printing

You can not print or print preview selected information during the capture process until you stop the program. When you choose the **Print** command from the **File** menu or click the icon  from the toolbar, only the visible listings will be printed. To print selected items, use **Shift** or **Ctrl** key to set a print scope. If you would like to print more columns' information, you must show desired columns first. Colasoft Capsa supports printer printing and PDF printing, you can use the **Print Setup** command in the **File** menu to define printing options.

The information of packet decode or connection details can not be printed directly from tab views, but you can print from the **Packet Decode** window or the **Connection Details** window.

Statistics

Colasoft Capsa calculates a variety of key statistics in real time, and presents these statistics either as numeric data or in intuitive graphical displays. You can save, copy and print these statistics, or generate statistic reports.

Summary statistics provide general statistic information of global network or a specific network node, including traffic, packet size distribution, most common packet sizes, TCP analysis and other statistic information from the advanced analyzers.

Snapshots are a helpful tool to record the summary data for a future reference.

Endpoints statistics present the details of network activities on every endpoint. You can choose to display all hierarchical endpoints, or just physical endpoints or IP endpoints.

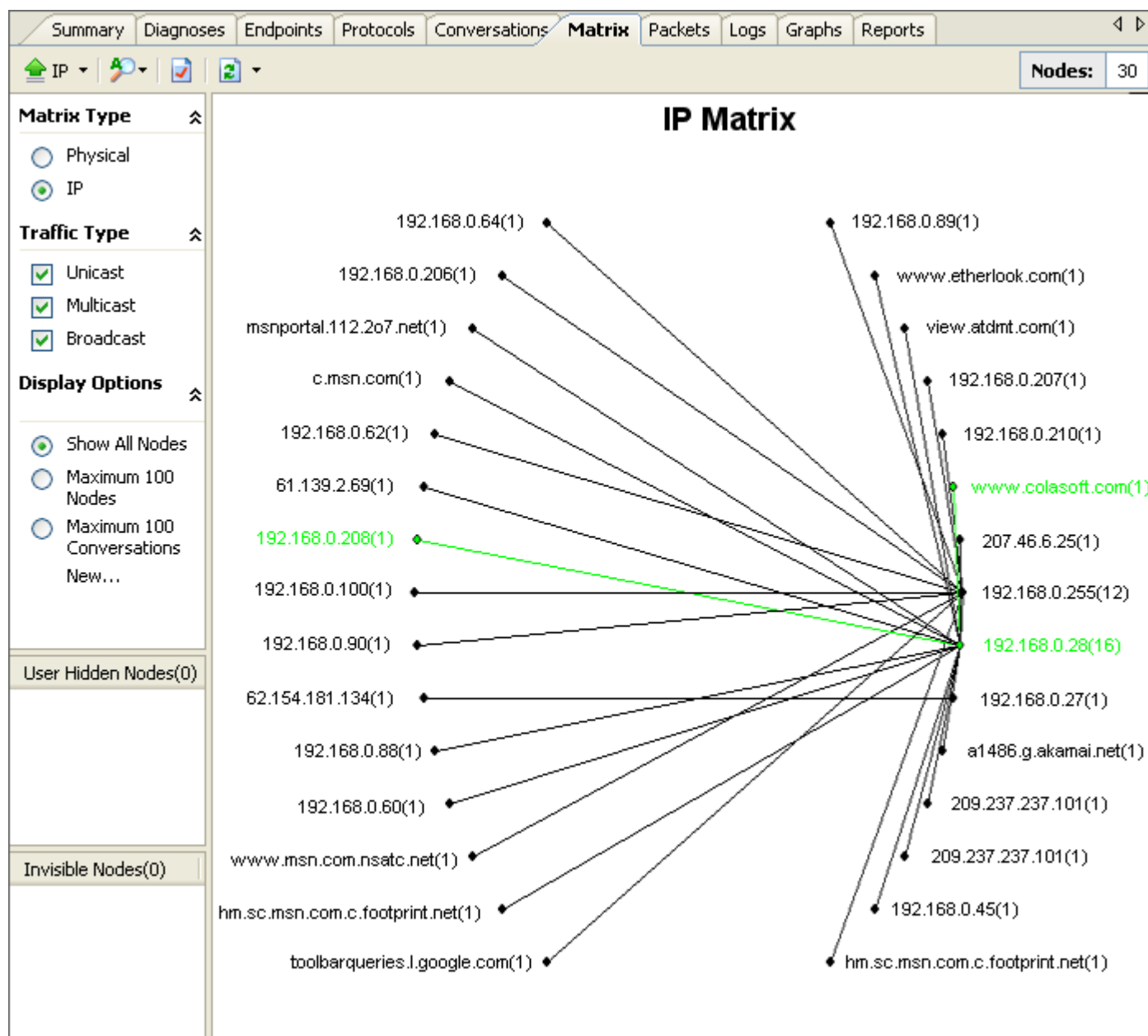
Protocols statistics present the information of protocols used in network communications. The display structure in this view is the same as the **Protocols** group in the **Project Explorer**.

Graph statistics (unique to enterprise edition) display the statistic information in graphical way. In addition to the common graphs like error packets, utilization, packet size distribution and packet size details, you can also see the graphic statistics based on the results from the advanced analyzers.

Reports statistics (unique to enterprise edition) are based on the above statistic information. A report contains summary statistics, protocol statistics, top 10 physical addresses, top 10 IP addresses, top 10 local IP addresses, top 10 remote IP addresses, and all available graphs.

Matrix

Unique to Colasoft Capsa enterprise edition. The **Matrix** view includes individual tools to customize the display types of network traffic. This lets you quickly create a picture of all the traffic or sending/receiving traffic. The nodes around an elongated ellipse display the hosts in your network, the line weight present the volume of traffic between nodes. The green color reveals the traffic is transmitting current now and the black color displays the transmission is completed by default. When you drag nodes to a new position, the connecting lines rubber-band. Colasoft Capsa will popup a notice if the captured nodes exceed 1000.



Matrix display options

The matrix view has two sections: matrix list and display pane. You can customize the matrix pictures by setting the parameters in the matrix list and display pane.

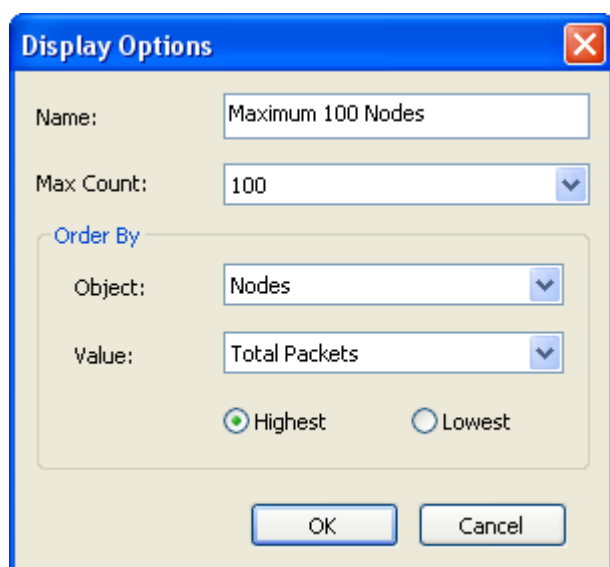
- **Display List**

The matrix list shows the matrix groups and the title of available matrix for the current node.

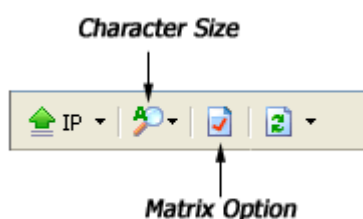
Group	Description
Matrix Type	Provides two types address matrix - Physical address and IP address.
Traffic Type	Provides three traffic types – Unicast, Multicast and Broadcast. By default this view shows the traffic of global network, you can select one or two types to view the specific traffic.
Display Options	Provides three predefined display options types and customizing display options.

- **Display Options**

This pane offers three predefined display options - **Show All Nodes**, **Maximum 100 Nodes** and **Maximum 100 Conversations**. You can also customize your own display options by click the **New...** button.



- **Display Pane**

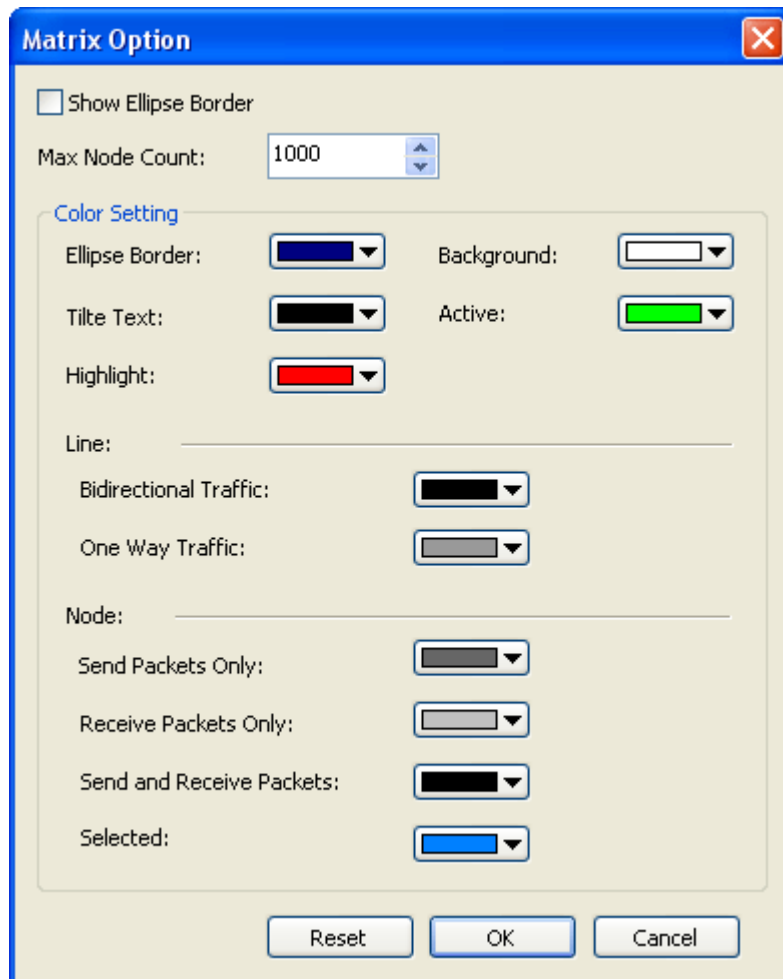


- **Character Size**

Click the dropdown button in the display pane to select a character display size.

Matrix Option

The **Matrix Option** includes **Show Ellipse Border**, **Max Node Count** and **Color Setting**.

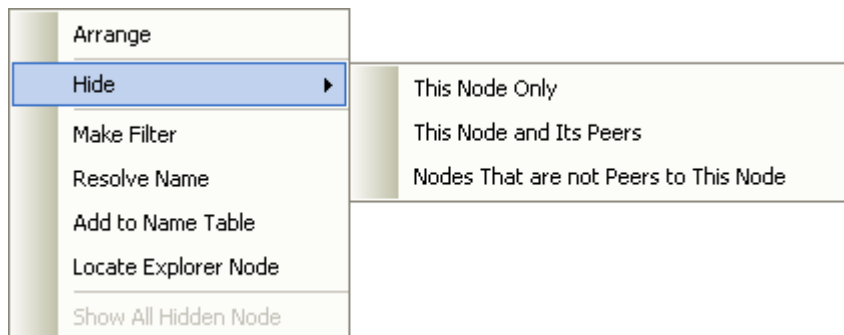


User Hidden Nodes

The **User Hidden Nodes** pane lists the nodes which have been temporarily hidden. You can hide the nodes you didn't interested in currently from the matrix picture.

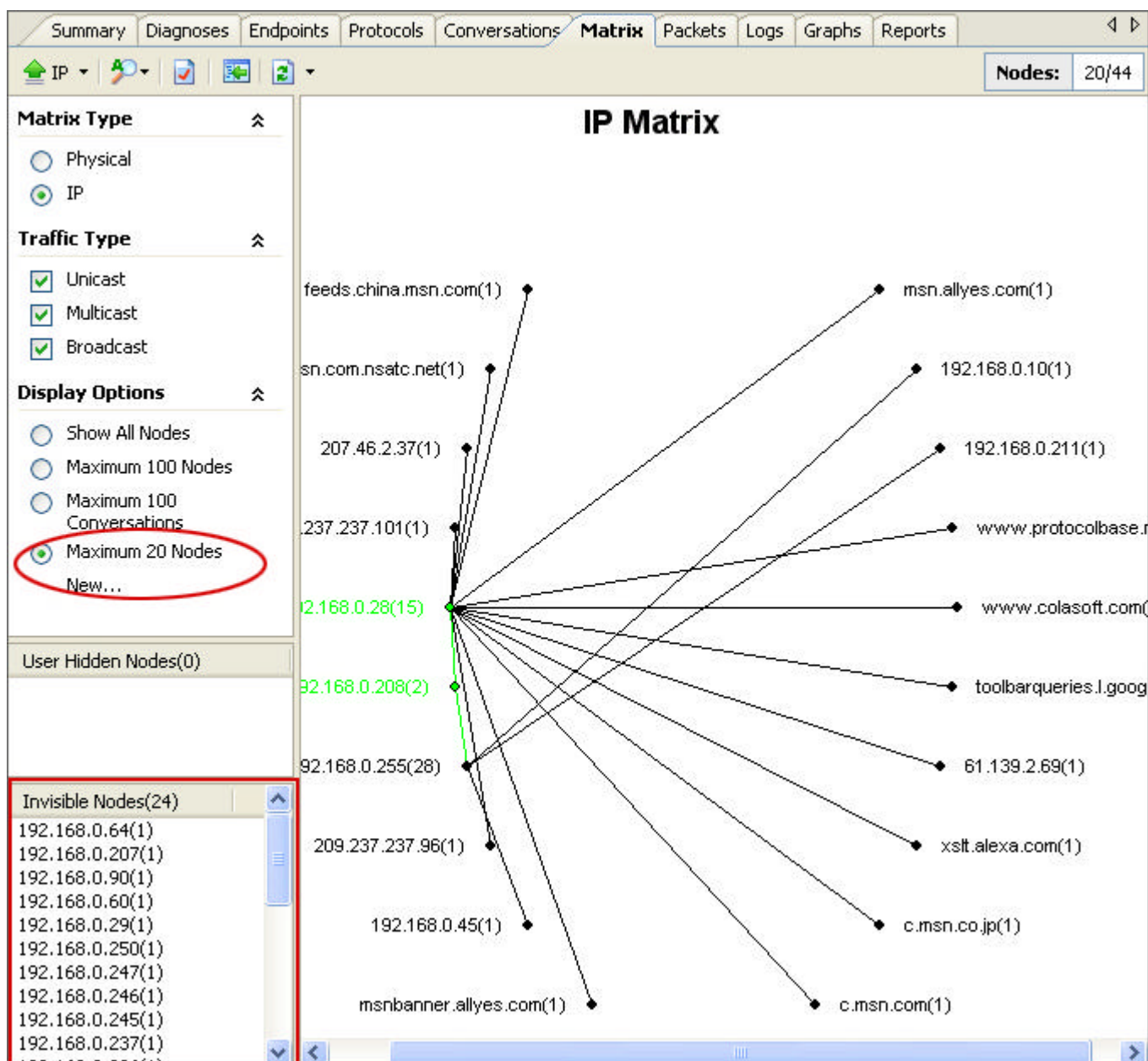


The number in the bracket on the header of the User Hidden Nodes pane shows the number of hidden nodes. In this pane, you can restore the selected nodes to the matrix by right-clicking in the pane and choosing **Show Selected Nodes** from the context menu, or restore all the hidden nodes by choosing **Show All Nodes**. To hide the nodes, select a node, right-click, choose the **Hide** command from the context menu, select **This Node Only**, **This Node and It's Peers** and **Nodes That are not Peers to This Node** from the sub-context menu.



Invisible Nodes

The **Invisible Nodes** pane lists the nodes which have been temporarily hidden in the matrix because they do not match the settings in the **Display Options** pane. The number in the bracket on the header of the **Invisible Nodes** pane shows the number of invisible nodes. You cannot restore these nodes unless you choose **Show All Nodes** in the **Display Options** list.




Diagnoses

Colasoft Capsa diagnoses your network from the captured packets and lists all diagnosis events with a severity level. From the Diagnoses view, you are not only able to see the event count by network layer, but also know event-related information such as source, destination, packet number, etc. The severity level indicates the event is an informational message, a minor error or a critical error.


The subviews in the lower section provide more and detailed information of the current row selected from the upper view, for example, when "**Application Layer**" is highlighted, the subview **Events** present all diagnosis events on the application layer. In addition to the default columns, you can reach more column information by clicking on the column bar and select "**More...**". Colasoft Capsa also lets you open a new window to show event-related packets with double clicks on an event. The subview "**References**" offer a description for the current event with possible causes and solutions, which is helpful for troubleshooting your network.

According to the severity levels of diagnosis, Colasoft Capsa contains four kinds of events:


- **Information**

The Information severity level (labeled as ) indicates the current event is a normal message, no corrective action is required.


- **Notice**

The Notice severity level (labeled as ) indicates the normal but significant conditions of the current event, it may require special handling.

- **Warning**

The Warning severity level (labeled as ) indicates an error has occurred which requires your attention and should be addressed soon.

- **Critical**

The Critical severity level (labeled as ) indicates the serious error conditions which requires immediate intervention by administrators.

This chapter provides a list of references information for all diagnosis events, including event description, possible causes and solutions.

Diagnosis references - application layer

Colasoft Capsa offers expert diagnosis for the following application layer events.

Severity: Notice

Event	Description	Threshold	Possible causes and solutions
Domain Name is Inexistent	The domain name referenced in the query does not exist.	Information	* The requested domain doesn't exist. * User types in an invalid domain.
DNS Server Slow Response Time	The average response time from the server is higher than the Slow Response Time threshold.		The web server is overloaded.
DNS Error	The server response to the required host		* Format error

	or domain is not implement.		* Server failure * Refused * Not Implemented * Reserved
HTTP Server Slow Response Time	The average response time from the server is equal to or higher than the Slow Response Time threshold.	Slow Response Time - 150 milliseconds	The web server is overloaded.
POP3 Server Slow Response Time	The average response time from the server is equal to or higher than the Slow Response Time threshold.	Slow Response Time - 150 milliseconds	The POP3 server is overloaded.
SMTP Server Slow Response Time	The average response time from the server is equal to or higher than the Slow Response Time threshold.	Slow Response Time - 150 milliseconds	The SMTP server is overloaded.
FTP Server Slow Response Time	The average response time from the server is equal to or higher than the Slow Response Time threshold.	Slow Response Time - 150 milliseconds	The SMTP server is overloaded.

Severity: Warning

Event	Description	Possible causes and solutions
HTTP Basic Authentication Failure	The failure of a HTTP client's authentication request results in the immediate denial of authentication.	Check for invalid login username or password.
HTTP Non-HTTP Traffic	A HTTP 80/TCP connection contains non-HTTP traffic.	* An application running on TCP port 80 produces non-HTTP traffic. * Verify the traffic content of source station and destination station.
HTTP Server Error	HTTP server returns a 5xx error code to indicate a server error; the client's request is usually valid.	
POP3 Logon Failure	A POP3 client fails to log in to a server.	Check for invalid login username or password.
POP3 Non-POP3 Traffic	A POP3 110/TCP connection contains non-POP3 traffic.	* An application running on TCP port 110 produces non-POP3 traffic. * Verify the traffic content of source station and destination station.
SMTP Logon Failure	A SMTP client fails to log in to a server.	Check for invalid login username or password.
SMTP Non-SMTP Traffic	A SMTP 25/TCP connection contains non-SMTP traffic.	* An application running on TCP port 25 produces non-SMTP traffic. * Verify the traffic content of source station and destination station.
SMTP Logon Failure	A SMTP client fails to log in to a server.	Check for invalid login username or password.
SMTP Non-SMTP Traffic	A SMTP 25/TCP connection contains non-SMTP traffic.	* An application running on TCP port 25 produces non-SMTP traffic.

		* Verify the traffic content of source station and destination station.
FTP Logon Failure	A FTP client fails to log in to a server.	Check for invalid login username or password.
FTP Non-FTP Traffic	A FTP control 21/TCP connection contains non-FTP control traffic.	* An application running on TCP port 21 produces non-FTP control traffic. * Verify the traffic content of source station and destination station.
FTP Data Connection Failure	An initiated FTP data connection fails to be created.	* A firewall blocks the FTP data connection. * The FTP server does not accept PASV FTP data connections.
Telnet Logon Failure	A Telnet client fails to log in to a server.	Check for invalid login username or password.

Severity: Information

Event	Description	Possible causes and solutions
HTTP Request Not Found	HTTP server returns this error when the requested URL was not found.	* User types in an invalid Uniform Resource Location (URL). * The connection to the web server is broken.
HTTP Client Error	HTTP server returns a 4xx error code other than 404 (Request Not Found) to indicate a client error.	

Severity: Critical

Event	Description	Possible causes and solutions
POP3 Server Returned Error	A POP3 connection or request is rejected by a POP3 server after a TCP connection has already been established.	* The client issues an invalid command. * The server is busy.
SMTP Server Returned Error	A SMTP connection or request is rejected by a SMTP server after a TCP connection has already been established.	* The client issues an invalid command. * The server is busy.
FTP Server Returned Error	A FTP connection or request is rejected by a FTP server after a TCP connection has already been established.	* The client issues an invalid command. * The server is busy.

Diagnosis references - transport layer

Colasoft Capsa offers expert diagnosis for the following transport layer events.

Severity: Notice

Event	Description	Threshold	Possible causes and solutions
TCP Reset Inactive Connection	An established TCP connection has been reset by one end of the connection after the Reset Inactive Connection threshold is reached.	Reset Inactive Connection - 15 seconds	* A TCP Server resets a client connection if the client has been idle for too long. * Many older Web browsers use Reset Connection to shut down their HTTP connections; however, newer browsers are better at complying with the TCP disconnection procedures. Due to the fact that many older browsers are

			still in use, TCP Reset Connection events are very common in many of today's LANs.
TCP Retransmission	The sender does not receive an acknowledgment (ACK) from the receiver, and therefore retransmits the packet.		<ul style="list-style-type: none"> * The acknowledgment packets are being transmitted via a slower path. * The network load is very high. * The receiver or router is overloaded.

Severity: Warning

Event	Description	Threshold	Possible causes and solutions
TCP Repeated Connect Attempt	A client is attempting multiple times to establish a TCP connection.		A firewall may be blocking the SYN packet sent from the client to the server, or ACK packet sent from the server to the client.
TCP Connection Refused	A client's initial TCP connection attempt has been rejected by the target host.		<ul style="list-style-type: none"> * A client is requesting a service that the host does not offer. * There are no more available resources on the server to accept new connections.
TCP Too Many Retransmissions	The percentage of retransmissions on a connection is equal to or higher than the Too Many Retransmissions threshold.	Too Many Retransmissions – 10%	<ul style="list-style-type: none"> * The acknowledgment packets are being transmitted via a slower path. * The network load is very high. * The receiver or router is overloaded.
TCP Fast Retransmission	A TCP sender retransmits a packet before Fast Retransmission threshold is reached.	Fast Retransmission – 150 milliseconds	<ul style="list-style-type: none"> * The acknowledgment packets are being transmitted via a slower path. * The network load is very high. * The receiver or router is overloaded.
TCP Invalid Checksum	The checksum of a TCP header and/or data is in error. The checksum value is calculated by the sender and written to the packet, and then recalculated from the received packet by the receiver. It indicates an error if the two values are different.		<ul style="list-style-type: none"> * There is a faulty device on the network. * If the checksum of all local packets are showed as invalid, it may be the checksum offload feature has been enabled; in this case, the adapter performs the cycle-intensive process of calculating CRC, the Windows TCP/IP stack does not calculate the IP and TCP checksums and leaves them as 0x0000. Colasoft Capsa collects the copy of each outgoing packet before it goes to the adapter. To fix this issue, you need to disable the adapter's Offload Transmit IP Checksum and Offload Transmit TCP Checksum feature in the advanced setting dialog.
TCP Zero Window Too Long	The window size of one end of a TCP connection being zero is longer than the time specified by the Zero Window Time threshold.	Zero Window Time – 500 milliseconds	<ul style="list-style-type: none"> * The receiver is very busy. * There are insufficient network buffers in the receiving station. * This is an indirect result of an application program's behavior. For example, the application may be waiting for some other events happening, or the application may not be releasing the frame buffer. * An application is very slow.
TCP Slow ACK	The time a connection has taken to	Slow ACK Time –	<ul style="list-style-type: none"> * The acknowledgment packets are being

	acknowledge data exceeds the average acknowledgment time of the connection plus the Slow ACK Time threshold.	250 milliseconds	transmitted via a slower path. * The network load is very high. * The receiver or router is overloaded.
TCP Port Scan	A local or remote station is scanning the network for opening TCP ports.		Port Scanning is an intrusion indicator.
UDP Invalid Checksum	The checksum of a UDP header and/or data is in error. The checksum value is calculated by the sender and written to the packet, and then recalculated from the received packet by the receiver. It indicates an error if the two values are different.		There is a faulty device on the network.

Severity: Information

Event	Description	Threshold	Possible causes and solutions
TCP Reset Connection	An established TCP connection has been reset by one end of the connection, this results in an abnormal termination of the TCP connection.		<ul style="list-style-type: none"> * A server drops the connection because of improperly configured resources or router problems. * A user aborts the Web connection due to slow response from a server. * Many older Web browsers use Reset Connection to shut down their HTTP connections; however, newer browsers are better at complying with the TCP disconnection procedures. Due to the fact that many older browsers are still in use, TCP Reset Connection events are very common in many of today's LANs.
TCP Window Frozen	The TCP window size has been stuck for three or more consecutive packets and has dropped below a percentage of the maximum observed window for this conversation.	Window Frozen – 50%	Check the source station for insufficient network application.
TCP Low Window	The TCP window size has dropped below a percentage of the maximum observed window for this conversation.	Low Window – 10%	Check the source station for insufficient network application.

Diagnosis references - network layer

Colasoft Capsa offers expert diagnosis for the following network layer events.

Severity: Notice

Event	Description	Possible causes and solutions
IP Time-To-Live	An IP packet with a time-to-live field set to 0 or 1 indicates that the packet is about to	<ul style="list-style-type: none"> * There is a routing table error somewhere in the network. * The packet is looping.

Too Low	expire.	<ul style="list-style-type: none"> * The originating IP host transmitted the packet with a low TTL to begin with. * Try to locate the source of the original packet.
IP Fragment Missing	An IP packet has been fragmented and one of the fragments is missing. This will usually result in a retransmission.	<ul style="list-style-type: none"> * A fragment has been dropped by a switch or router. * The traffic on the LAN is heavy.
IP Zero Broadcast Address	An IP packet is being sent with the old IP broadcast address of 0.0.0.0.	<ul style="list-style-type: none"> * This is an obsolete form of TCP/IP broadcast address. * Check the source endpoint for applications that may be sending this packet.

Severity: Warning

Event	Description	Possible causes and solutions
ICMP Destination Unreachable	A station receives an ICMP destination unreachable message.	The destination network does not exist.
ICMP Host Unreachable	A station receives an ICMP host unreachable message.	The destination host does not exist.
ICMP Net Unreachable	A station receives an ICMP network unreachable message.	The destination network does not exist.
ICMP Parameter Problem	A station sends an ICMP message indicating a parameter problem.	
ICMP Port Unreachable	A station receives an ICMP port unreachable message.	The destination port is not active on the station that sent the message.
ICMP Redirect for Host	A station receives an ICMP redirect message with the Code value set to 1 (redirect datagrams for the host).	A router may have sent the message to inform this station that a better route exists to its intended destination.
ICMP Redirect for Network	A station receives an ICMP redirect message with the Code value set to 0 (redirect datagrams for the network).	A router may have sent the message to inform this station that a better route exists to its intended destination.
ICMP Source Quench	A station receives an ICMP source quench message.	The station that sent the message may be down or rebooting.
IP Invalid Header Checksum	The checksum of an IP header is in error. The checksum value is calculated by the sender and written to the packet, and then recalculated from the received packet by the receiver. It indicates an error if the two values are different.	There is a faulty device on the network.
IP Duplicate Address	There is more than one MAC Address associated with the same IP address.	<ul style="list-style-type: none"> * The newly assigned network address is not unique in the network and conflicts with the existing network addresses. * The dynamically allocated network address is not proper. * If the MAC addresses are routers, this is not a problem.

Diagnosis references - data link layer

Colasoft Capsa offers expert diagnosis for the following data link layer events.

Severity: Warning

Event	Description	Threshold	Possible causes and solutions
ARP Too Many Unrequested Response	The percentage of unrequested ARP response of a physical node is equal to or higher than the Unrequested Responses threshold.	Unrequested Responses - 50%	Check the source and target physical node for possible ARP spoofing.
ARP Request Storm	The number of ARP request packets per second exceeds the ARP requests/sec threshold, indicating that an ARP request storm has been detected.	* Sample Time - second * ARP requests/sec - 10	Check the source station for the application that sent the ARP requests.
ARP Scan	A station is scanning the network address via ARP requests.		Check the source station for the application that performs the scanning.





Graphs

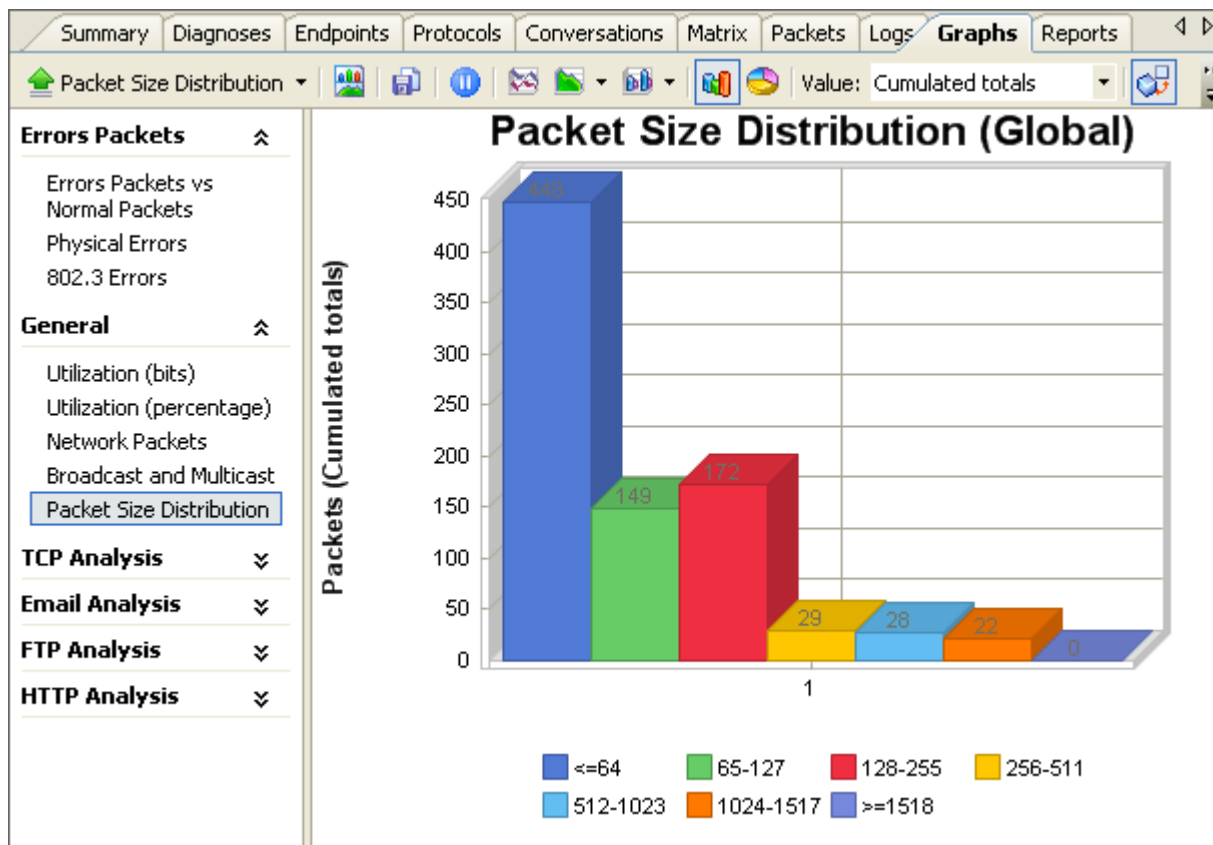
Unique to Colasoft Capsa enterprise edition. In addition to the standard statistical views, Colasoft Capsa also offers instant graphs which allow you to view your network situation in graphic way. You can view graphic statistics not only for a global network, but also for specific network nodes.

There are multiple graph titles and display options available; this chapter explains how to view graphs, how to select display options and how to save the graphic data.

Graphing statistics

The graphic data in the **Graph** view and the statistic information in the **Summary** view are consistent, you can see that from the following figures.

Summary						Diagnoses	Endpoints	Protocols	Conversations	Matrix	Packets	Logs	Graphs	Reports
<div>   </div>														
Statistics								Current						
+ Capture														
+ Physical Errors														
+ 802.3 Errors														
+ Traffic														
- Packet Size Distribution		Bytes		Bytes%		Bits		Bits%		Packets				
<=64		24.500 KB		19.800%		200.704 Kb		19.800%		392				
65-127		11.677 KB		9.437%		95.656 Kb		9.437%		143				
128-255		26.717 KB		21.592%		218.864 Kb		21.592%		170				
256-511		9.518 KB		7.692%		77.968 Kb		7.692%		29				
512-1023		19.653 KB		15.883%		161.000 Kb		15.883%		28				
1024-1517		31.671 KB		25.596%		259.448 Kb		25.596%		22				
>=1518		0 B		0.000%		0 b		0.000%		0				
+ TCP Packets														
+ TCP Connections														
+ DNS Analysis														
+ SMTP Analysis														
+ POP3 Analysis														
+ FTP Analysis														
+ HTTP Analysis														



Both the **Summary** view and **Graph** view offer statistical data about your network. However, the **Summary** view only presents the instant statistical data, whereas in **Graph** view you can see the historical data in a certain time span, e.g. last 120 seconds.

Note: By default, Colasoft Capsa only collects the data on intranet nodes continuously, the data collecting on an Internet node are not initiated until you select it.

Graphs go with the current node, to get global graphs, you must enable no filter and select the project root node in the **Project Explorer** dock window.

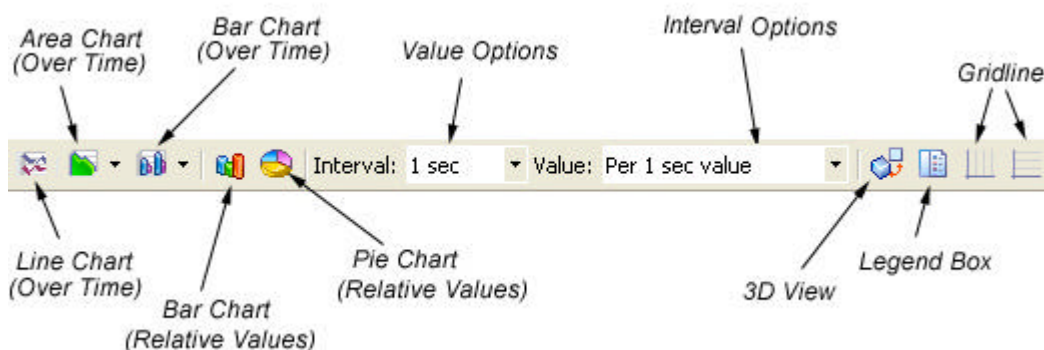
Graph display options

The **Graph** view has two sections: graph list and display pane. The graph list shows the graph groups and the title of available graphs for the current node, different nodes may have different graph groups and titles.

Group	Corresponding Analyzer	Description
Error Packets	None	Contains the graphs presenting the statistics of error packets.
General	All analyzers	Contains the commonly used statistic graphs.
TCP Analysis	TCP analyzer	Contains the graphs presenting the statistics of TCP connections.
Email Analysis	Email analyzer	Contains the graphs presenting the statistics of email messages.
FTP Analysis	FTP analyzer	Contains the graphs presenting the statistics of FTP transfers.
HTTP Analysis	HTTP analyzer	Contains the graphs presenting the statistics of HTTP requests.

There are a number of icons at the top of the graph display which may vary with the graph title you select from the graph list, you

can use these icons to control the display.



Colasoft Capsa provides the following chart types:

Type	Chart Options	Value Options	Interval Options
Line chart (Over Time)		Cumulated totals; Per second; Per interval value	1 sec; 5 sec; 30 sec; 60 sec; 120 sec; 300 sec; 600 sec; 3600 sec
Area chart (Over Time)	Normal stacked area; 100% stacked area; Clustered area	Cumulated totals; Per second; Per interval value	1 sec; 5 sec; 30 sec; 60 sec; 120 sec; 300 sec; 600 sec; 3600 sec
Bar chart (Over Time)	Side-by-side bar; Stacked bar; 100% stacked bar; Clustered bar	Cumulated totals; Per second; Per interval value	1 sec; 5 sec; 30 sec; 60 sec; 120 sec; 300 sec; 600 sec; 3600 sec
Bar chart (Relative Values)		Cumulated totals; Average per second; Last 1 second; Last 5 seconds; Last 30 seconds; Last 60 seconds; Last 120 seconds; Last 300 seconds; Last 600 seconds; Last 3600 seconds	
Pie chart (Relative Values)		Cumulated totals; Average per second; Last 1 second; Last 5 seconds; Last 30 seconds; Last 60 seconds; Last 120 seconds; Last 300 seconds; Last 600 seconds; Last 3600 seconds	

The interval options you select will affect the data displayed in this view, the following table presents the available sampling duration of every interval option.

	Interval Option	Sampling Duration
Global Node	1 sec	100 sec
	5 sec	500 secs
	60 sec	100 mins

	3600 sec	100 hours
Root Nodes	1 sec	4 mins
	2 sec	8 mins
	5 sec	20 mins
	10 sec	1 hour
	30 sec	2 hours
	60 sec	4 hours
	120 sec	8 hours
	300 sec	1 day
	600 sec	2 days
	1800 sec	5 days
	3600 sec	10 days

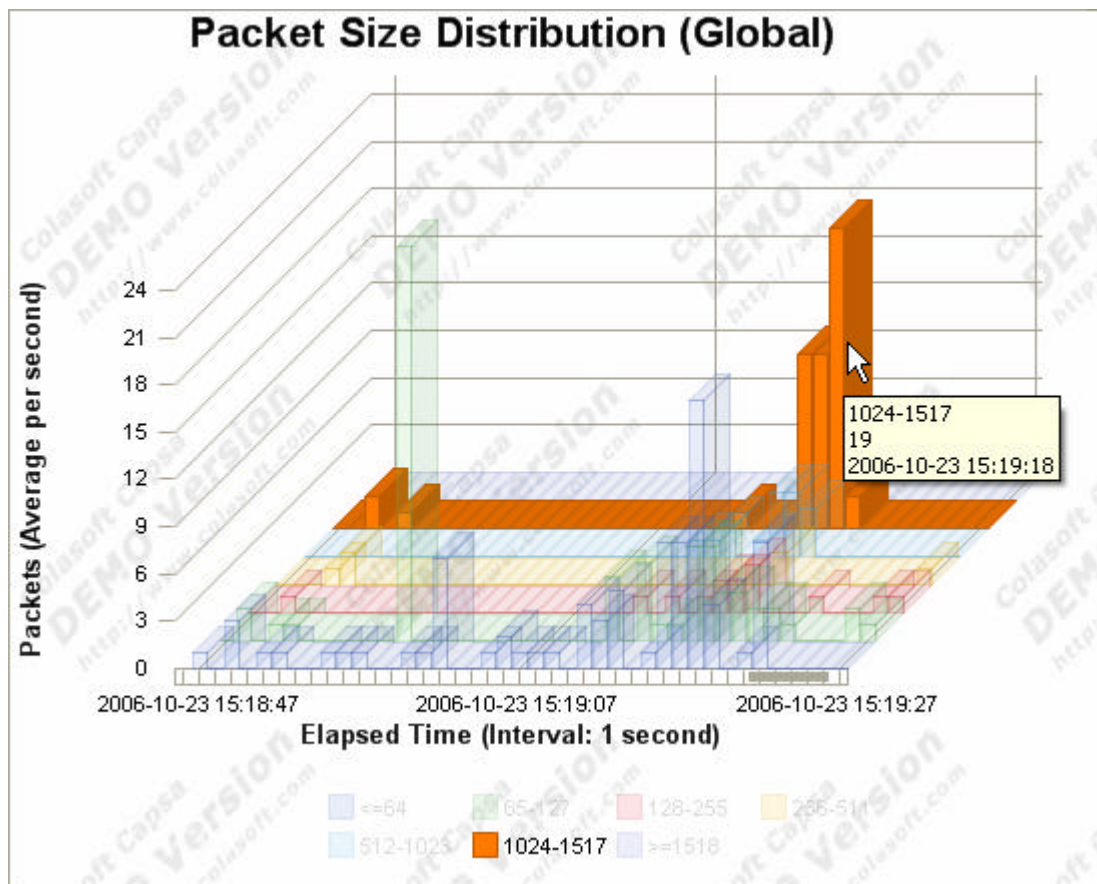
In addition to the alterable chart types and options, the appearance of graphs also can be controlled.

Icon	Usage
3D View	Change the graph display from two-dimensional to three-dimensional or reverse.
Legend Box	Toggle or untoggle the display of legends.
Vertical Gridline	Show or hide vertical gridline for the graph.
Horizontal Gridline	Show or hide horizontal gridline for the graph.


Highlight an item

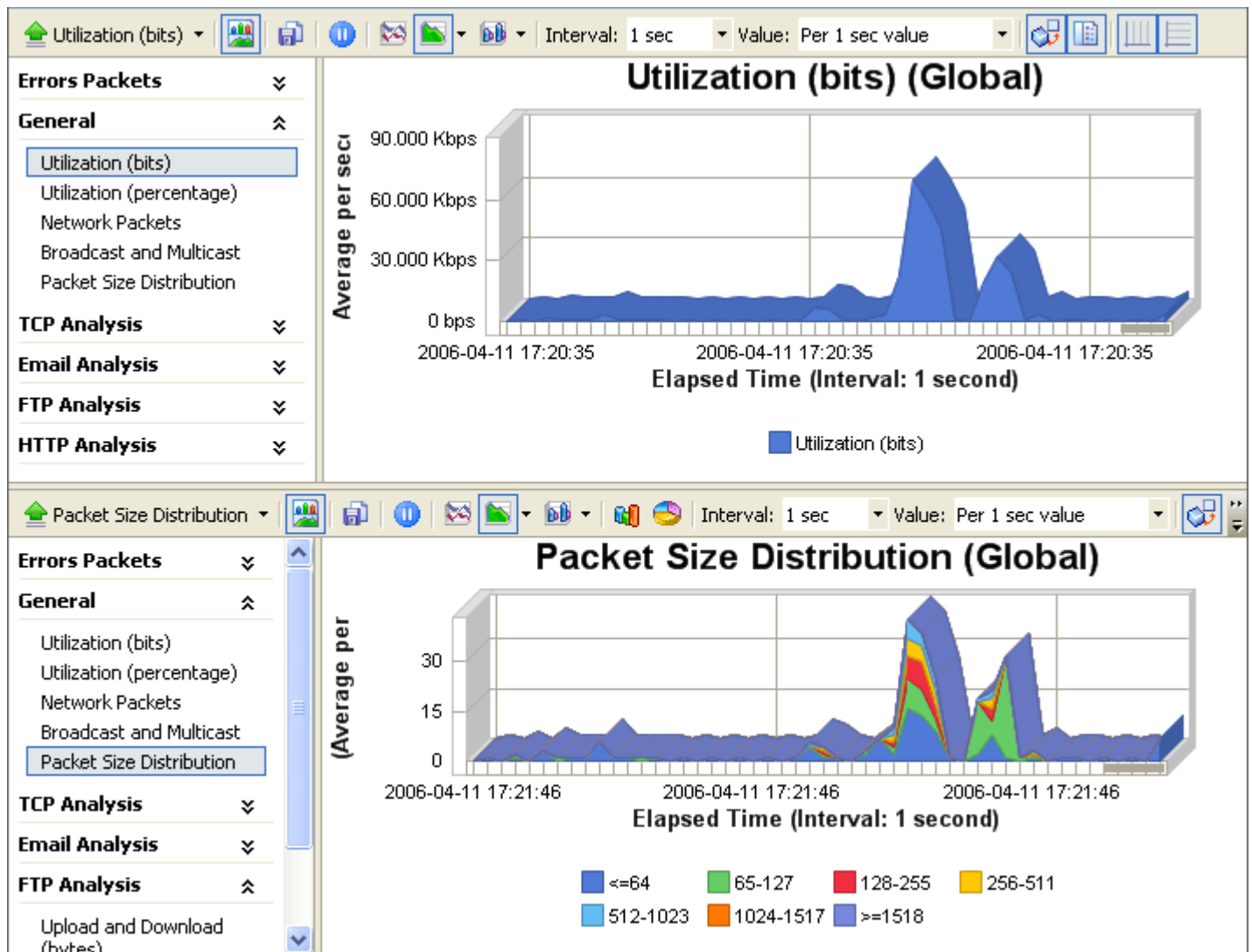
The highlight function in the Graphs view let you focus on any item displayed in graphs view. Colasoft Capsa will highlight the item you interested in when you push your mouse on it.

For example, selects the root node in the **Project Explorer** dock window, choose the **Packet Size Distribution** and the **1 sec** interval in the **Graphs** view and push the mouse cursor on the golden item. You will see the below figure - the items are fades except the golden item and a popup description under the mouse cursor. The description means there are **19** packets which size **1024-1517** bytes at the **15:19:18, 2006-10-13**.




Compare mode

The compare mode of graphs lets you compare two distinct graphs simultaneously in a view. Click the icon  from the toolbar to split the display into two sections, each section has its own graph groups and display options. You can select a same graph title and different display value or interval value, or two graph titles with same display value and interval value.




Saving graphs

You can save graphs from the **Graph** view as bmp/gif/jpg/png format. Click the icon  in the toolbar to open a **Save As** dialog, specify the file name and file type, then click **Save** to confirm. Colasoft Capsa saves one graph each time, repeat the above operations if you want to save multiple graphs.

Reports

Unique to Colasoft Capsa enterprise edition. The reports view provides the real time reports of global network or a specific groups. A report contains the statistic information of summary statistics, diagnosis events, protocol statistics, top 10 IP protocol, top 10 physical addresses, top 10 IP addresses, top 10 local IP addresses, top 10 remote IP addresses, and all available graphs with the current settings.

To get a HTML report, click the button . By default, reports are saved at: %My Documents%\Colasoft Capsa\Reports\Project Name, you can define the save path.

Report of Project 1




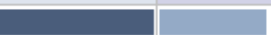


















Report generated on: 2005-09-09 20:08:28

- Summary Statistics
- Diagnosis Events
- Protocol Statistics
- TOP 10 Physical Addresses
- TOP 10 IP Addresses
- TOP 10 Local IP Addresses
- TOP 10 Remote IP Addresses
- Graphs

Summary Statistics


Statistics	Values				
Capture	Count				
Physical Errors	Count				
802.3 Errors	Count				
802.3 Total Errors	0				
802.3 One Collision	0				
802.3 More Collisions	0				
802.3 Max Collisions	0				
802.3 Deferrals	0				
Traffic	Count				
Packet Size Distribution	Bytes	Packets	Avg Utilization	Avg bps	Avg pps
<=64	72.750 KB	1,164	0.002%	1.524 Kbps	2.977
65-127	34.660 KB	456	0.001%	726.179 bps	1.166
128-255	35.486 KB	198	0.001%	743.488 bps	0.506
256-511	81.096 KB	224	0.002%	1.699 Kbps	0.573
512-1023	25.230 KB	42	0.001%	528.614 bps	0.107
1024-1517	171.389 KB	118	0.004%	3.591 Kbps	0.302
>=1518	0 B	0	0.000%	0.000 bps	0.000
Most Common Packet Sizes	Bytes	Packets	Avg Utilization	Avg bps	Avg pps
64 Bytes	72.750 KB	1,164	0.002%	1.524 Kbps	2.977
66 Bytes	16.500 KB	256	0.000%	345.698 bps	0.655
1510 Bytes	156.309 KB	106	0.003%	3.275 Kbps	0.271

TOP 10 IP Addresses

Name	Percentage Inbound	Percentage Outbound	Bytes	Packets
 webmaster	56.408%		39.085%	401.174 KB 1,900
 209.202.248.101	2.020%		27.999%	126.113 KB 196
 211.196.154.96	15.653%		8.145%	99.979 KB 736
 website	8.485%		4.064%	52.717 KB 370
 211.196.154.79	2.347%		7.688%	42.158 KB 126
 64.233.189.104	3.315%		2.399%	24.004 KB 128
 127.0.0.1	0.000%		0.000%	17.875 KB 286
 209.202.249.250	1.719%		1.793%	14.756 KB 58
 209.202.214.246	0.884%		2.002%	12.125 KB 40
 64.58.80.23	0.823%		0.555%	5.789 KB 30

Reports options

You can customize the reports by change the settings in the Report Options.

Click the  button to open the Report Options dialog and change the settings. The Summary Statistics, Diagnosis Statistics and Protocol Statistics were displayed in table format but the others were displayed in chart and table formats. Click the **Reset** button, the settings will be reset to default position.

Report Options

☒ Summary Statistics
☒ Diagnosis Statistics
☒ Protocol Statistics
☒ Top IP Protocols

☒ Top 10 Table
 ☐ Top 10 Chart

☒ Top Physical Addresses

☒ Top 10 Table
 ☐ Top 10 Chart

☒ Top IP Addresses

☒ Top 10 Table
 ☐ Top 10 Chart

☒ Top Local IP Addresses

☒ Top 10 Table
 ☐ Top 10 Chart

☒ Top Remote IP Addresses

☒ Top 10 Table
 ☐ Top 10 Chart

Reset

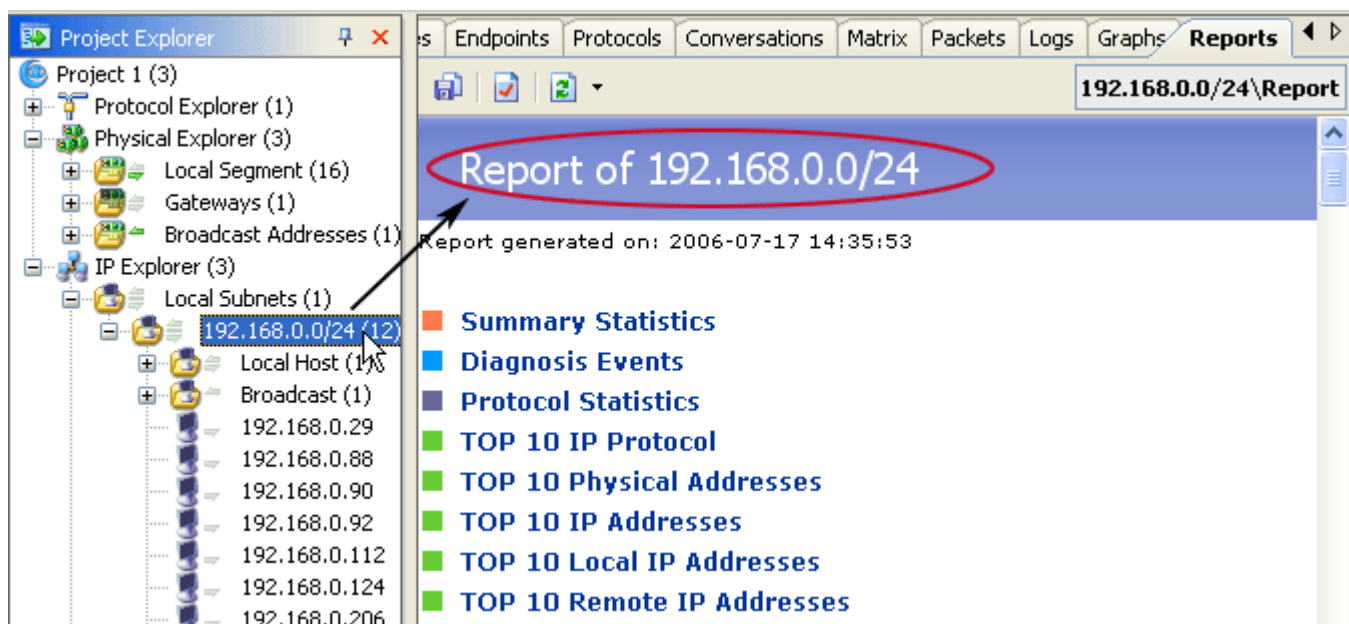
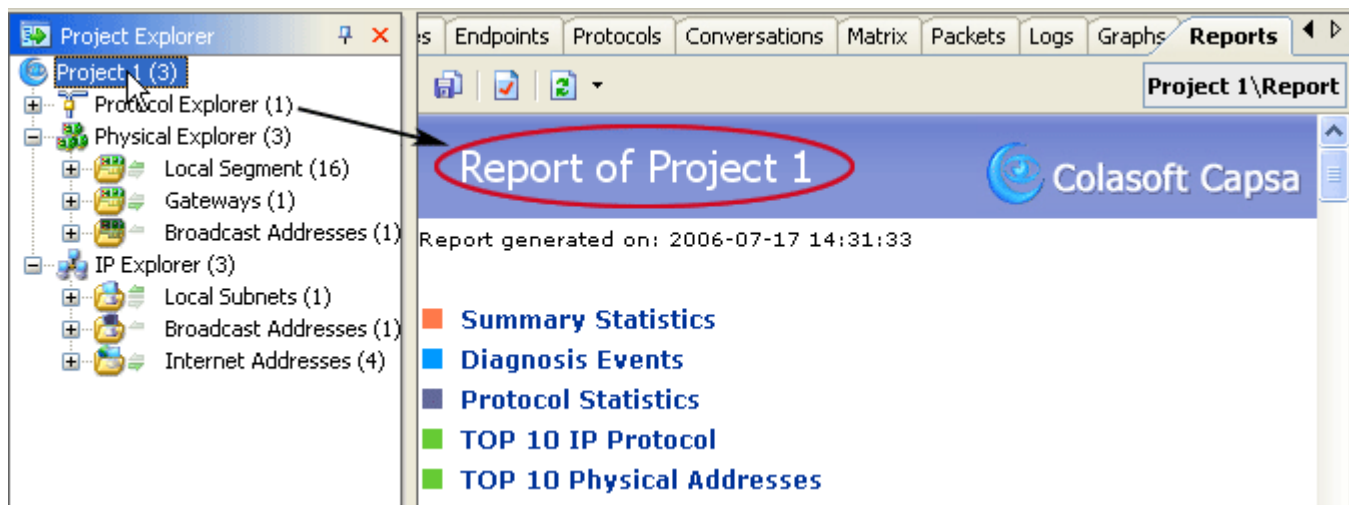
OK

Cancel

Help

Statistic reports

In this view, you can get statistic reports of the global network or a specific group. View a group or global statistic reports by selecting the corresponding group's name listed in the **Project Explorer**.



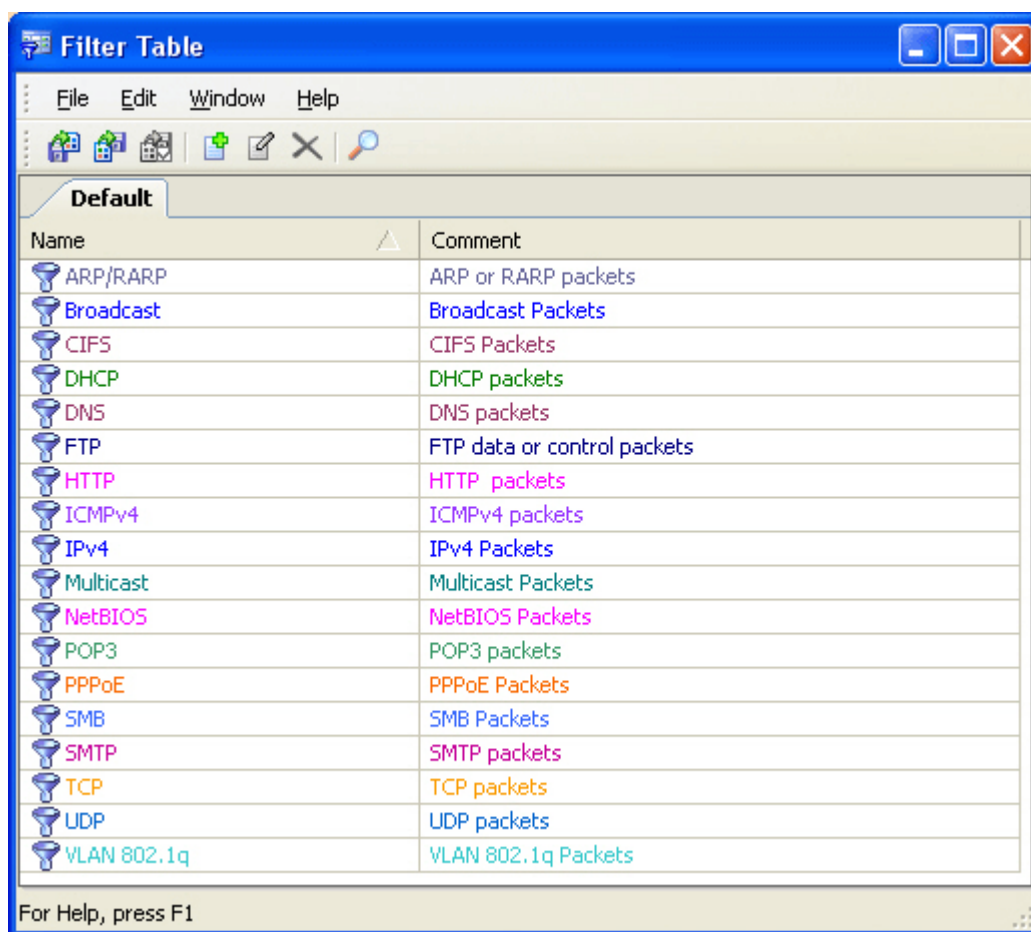
Filters

The filters in Colasoft Capsa decrease the packets to be analyzed and displayed, enabling you to focus on what you are really interested in. However, to get a primary impression of your network communications, you'd better not to set any filters unless you are practiced in using this program.

Colasoft Capsa has two kinds of filters: global filters and project filters.

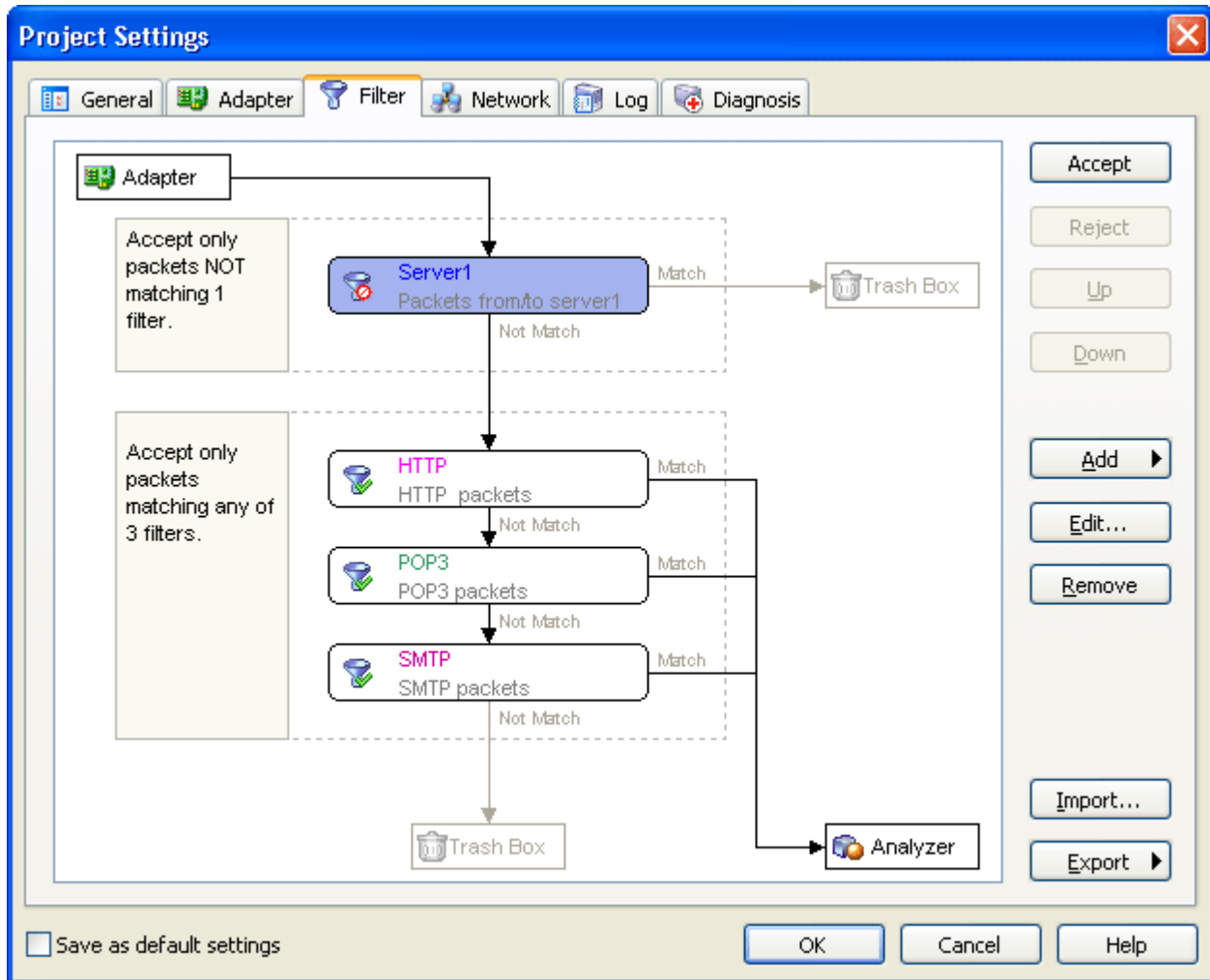
- **Global filters**

Some commonly used protocols filters are predefined and listed in the **Filter Table**, which can be applied to the current project by clicking the **Add** button and select **From Filter Table....** Please note that the modification to global filters must be made in the **Filter Table**.




- **Project filters**

You can define project filters in the **Project Settings - Filter** page. The filters defined in this page are only applied to the current project unless you tick the **Set as default settings** checkbox. Colasoft Capsa graphically displays project filters, you can easily accept, reject a filter or change its status. The flexibility of Colasoft Capsa lets you accept some filters and at the same time reject some others: the packets matching the **Accept** filters will be analyzed and the packets matching the **Reject** filters will be discarded.



This chapter describes how to create, modify, and use filters for network analysis, you may also find some examples which can help you be familiar with filters more quickly.

Adding a project filter

Click the filter icon  in the toolbar to open the **Project Settings - Filter** page, to add a project filter, you can choose to create a new one or select from the global **Filter Table** with predefined filters listed.

- **Add a new filter**

Click on the **Add** button and select **New...** to enter the filter setting page. The **Simple Filter** tab lets you quickly make the most commonly used filters by address, port and/or protocol. For example, if you check the box of **Address filter**, select **IP address** and enter **192.168.6.100** in **Address 1**, keep **Both directions** and select **IP address** and enter **221.236.12.213** in **Address 2**, after you confirm your operation and return to the previous page, you can see the filter you just define listed with a tick indicating that it is accepted. After click **Ok** to confirm, only the packets transmitted between **192.168.6.100** and **221.236.12.213** will be analyzed.

The **Advanced Filter** tab is for you to create more complex filters with a wider range of filter parameters, including address, port, protocol, packet value, packet size and packet pattern. You need to select a logical rule for a single filter, the logical rules can be **And**, **Or** or **Not**. See "**Advanced filters**" for more descriptions.

- **Add from filter table**

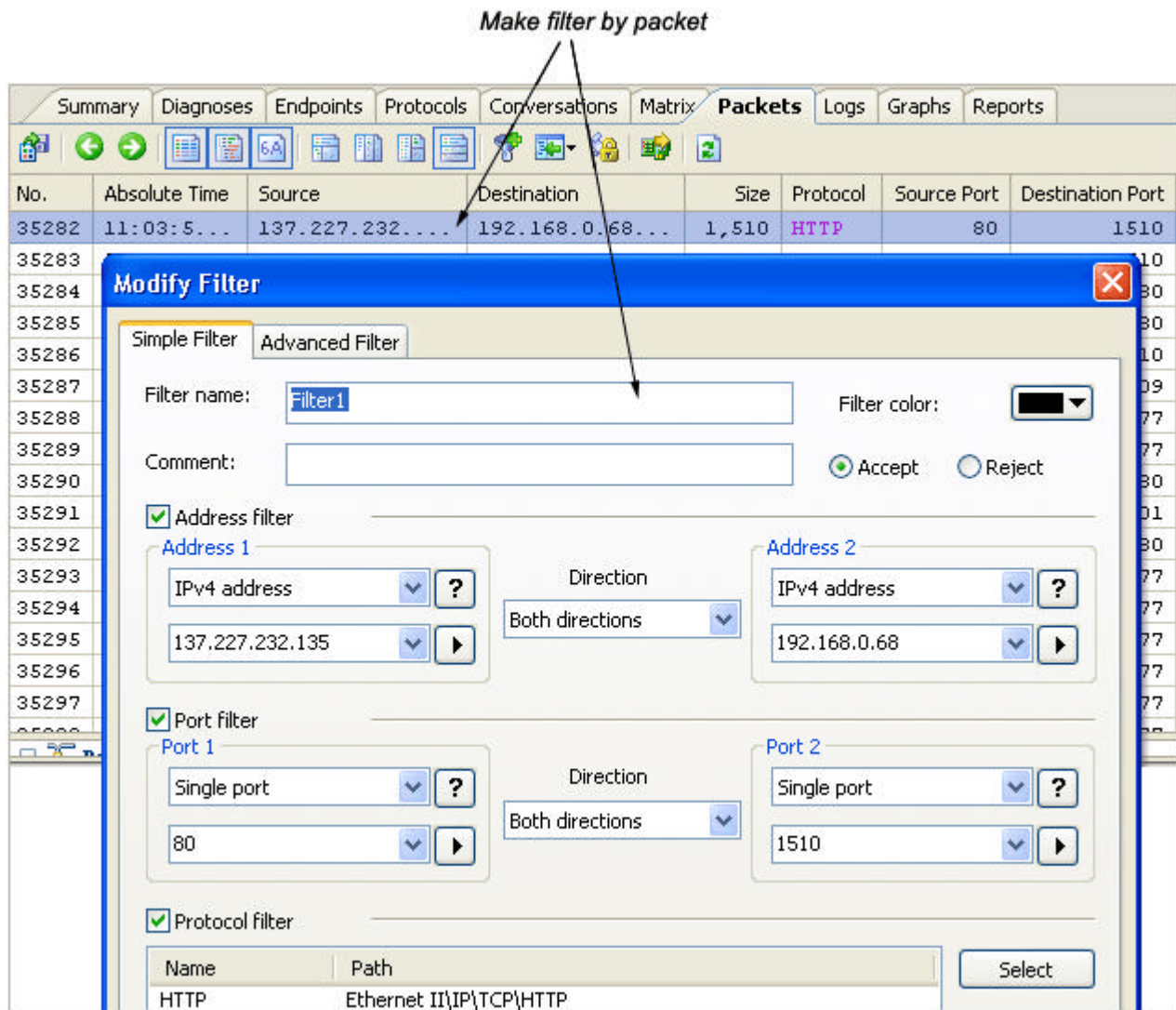
Click on the **Add** button and select **From Filter Table...** to open a dialog which lists all predefined filters, you can check one

or more filters, before confirm your selection, you need to decide a filter rule: accept or reject the packets matching filter for analysis.

- **Add by captured packet**

If you want to make a filter on the basis of a captured packet or item, just right click on the item and select **Make Filter...** from the context menu, Colasoft Capsa will fill in the filter automatically. This function is available for the **Diagnoses - Events** view, **Endpoints** view, **Protocols** view, **Packets** view, **Connections** view and **Logs** view.

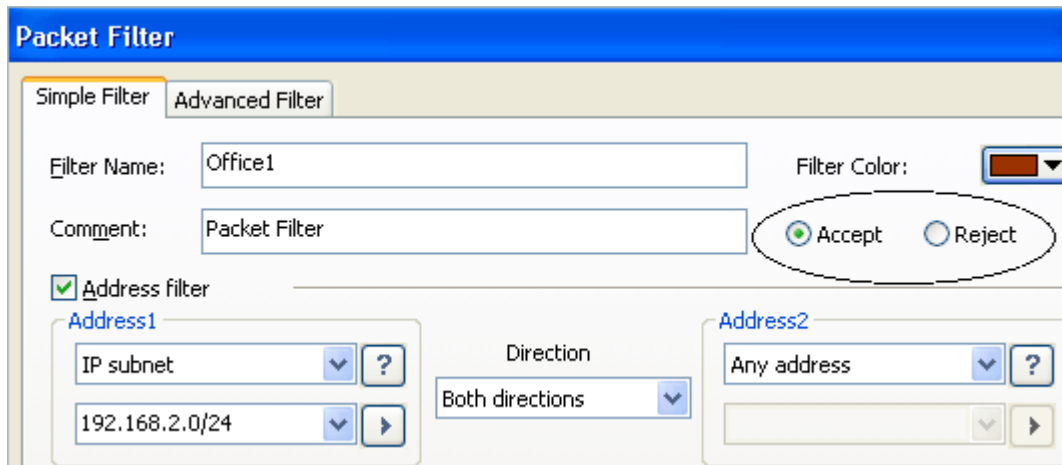
New filters can be made at any time and will go into effect immediately.



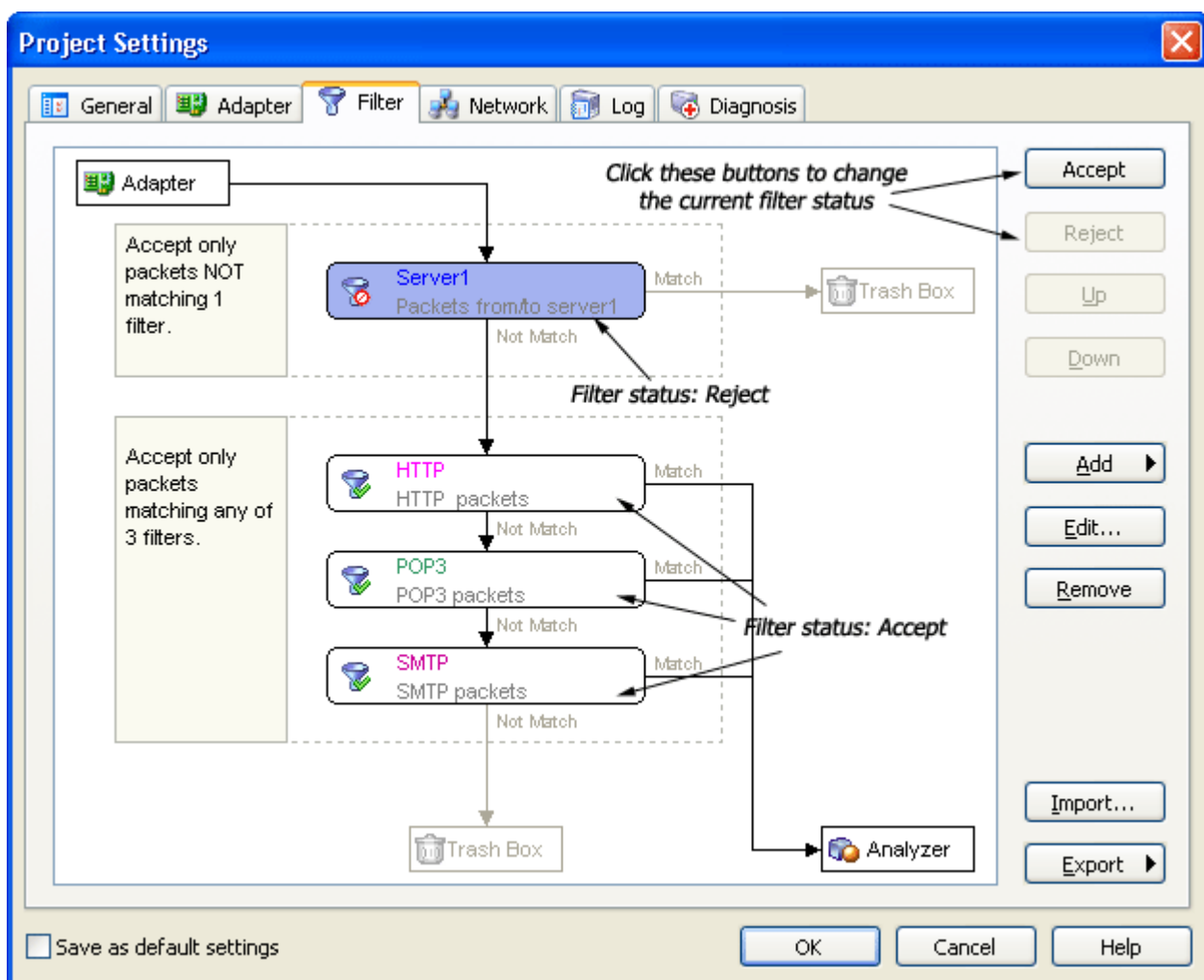
Accepting or rejecting a filter

In Colasoft Capsa you can accept some filters and at the same time reject some others. The packets matching to the accepted filter will be passed to analyzer and analyzed by Colasoft Capsa, and in reverse if you set the filter as a rejected filter. To accept or reject a filter, you can:

- Decide filter rule when adding/editing filter



- Change filter status with the **Add/Reject** button



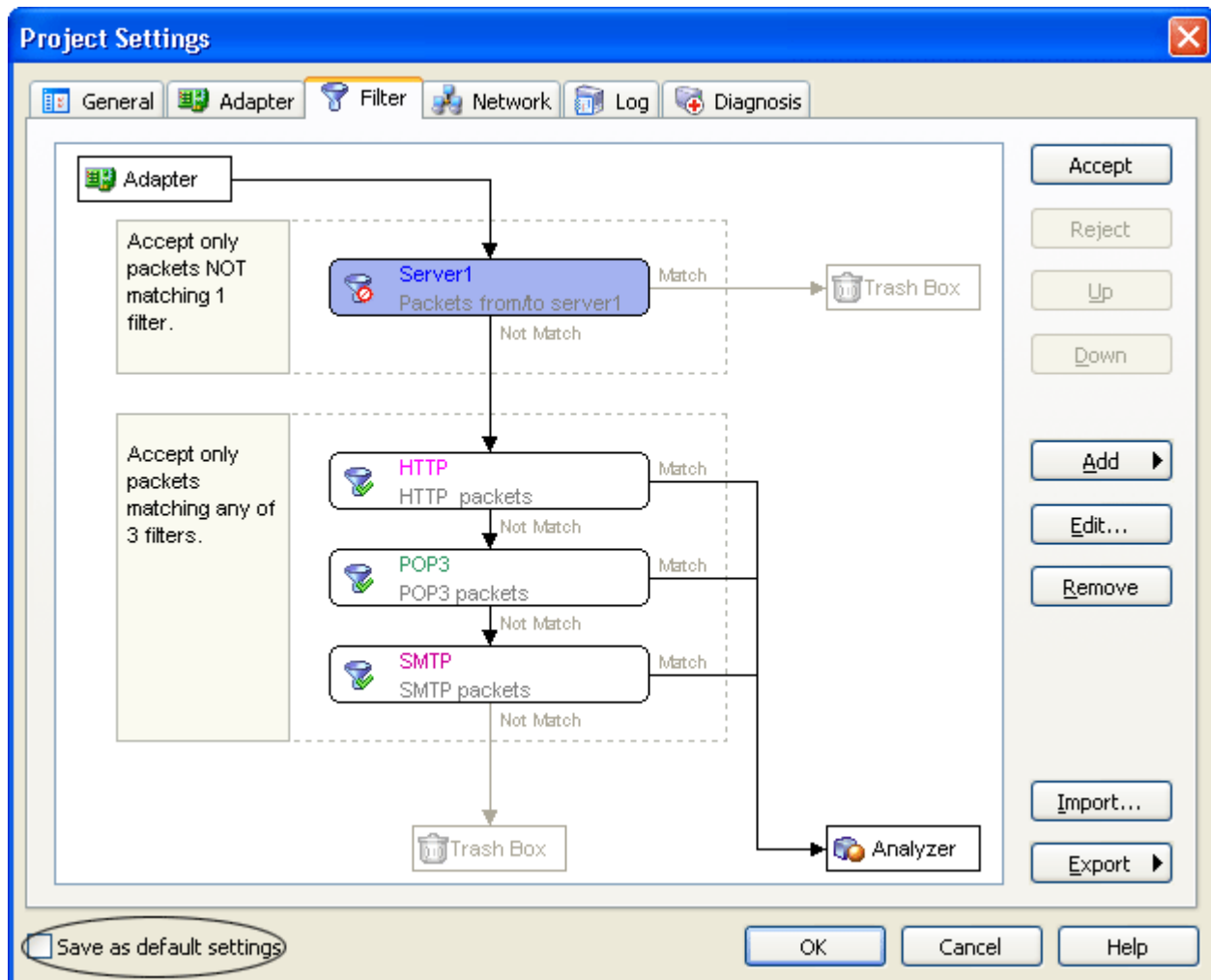
Saving, editing and removing a filter

• Saving a project filter

When you finish the setting of a filter and confirm, Colasoft Capsa will save the filter and list it in the **Project Settings - Filter** page. However, since the projects in Colasoft Capsa are all independent, the filter settings of a project can not be shared by other projects unless you designate the filter setting as default. With the command **Set as default Settings...**,

you can save a filter and its settings in the configuration category of system, each time when you open a new project, you can see the filter listed in the **Project Settings - Filter** page.

Both simple filters and advanced filters can be set as default.



- **Editing a filter**

To edit a filter, double click it from the filter list or use the **Edit** button. You can make modifications either in the capture process or when Colasoft Capsa stands by, after confirmation the modifications will be go into effect instantly.

Note: You are in danger of losing the specified parameters you have already entered as moving from the **Advanced Filter** page to the **Simple Filter** page, you have an opportunity to abort the operation when a warning appears.

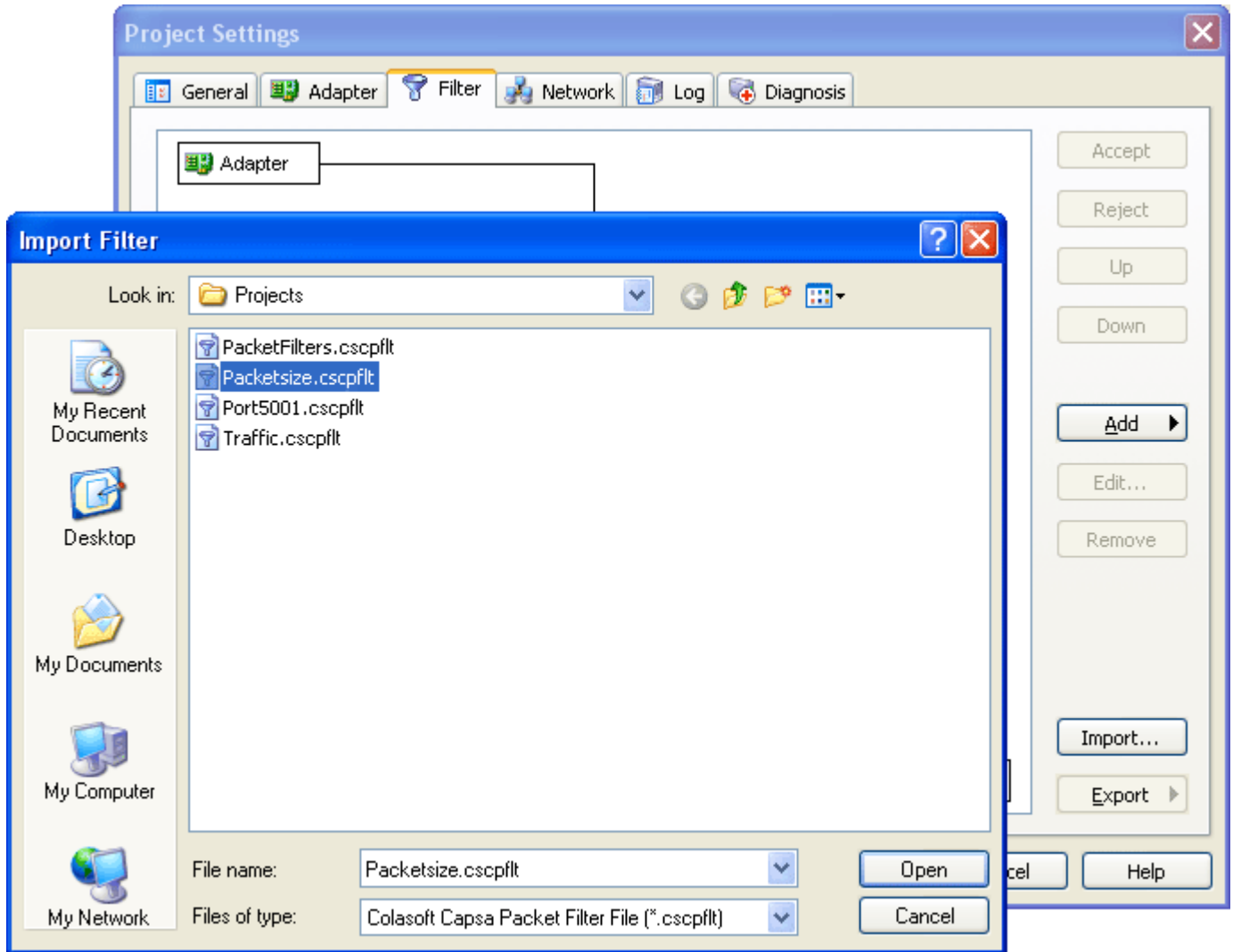
- **Removing a filter**

To delete a filter, make a selection from the filter list and click the **Remove** button. If you have set the filter as default, this operation will disable the previous setting.

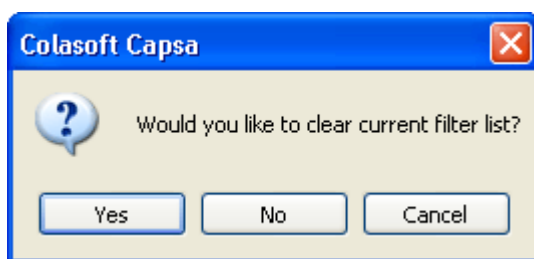
Importing and exporting filters

- **Import filters**

Colasoft Capsa lets you import filters from the files in .cscpfilt format. Click the **Import...** button and select **Import Filter from File...**, Colasoft Capsa will open the project file and list all available filter files, select one to open.



If you decide to clear the current filter list when asked, only the filters imported will be showed; if you select **No**, the filters imported will be appended to the current filter list.



- **Export filters**


To export filters, click the **Export...** button. When export filters, all the items in the filter list will be exported to a file in .cscpflt format, which can be imported later by other projects.

Simple filters

The **Simple Filter** page allows you to customize some commonly used filters by address, port and/or protocol in a single filter. When multiple parameters are chosen they are connected by logical **And** statements. That is, packets must match all of the conditions in order to match the filter.

Packet Filter

Simple Filter | **Advanced Filter**

Filter Name: Filter Color: 

Comment: ☒ Accept ☐ Reject

☒ Address filter

Address1

IP subnet

Direction

Both directions

Address2

Any address

☒ Port filter

Port1

Multiple ports

Direction

Both directions

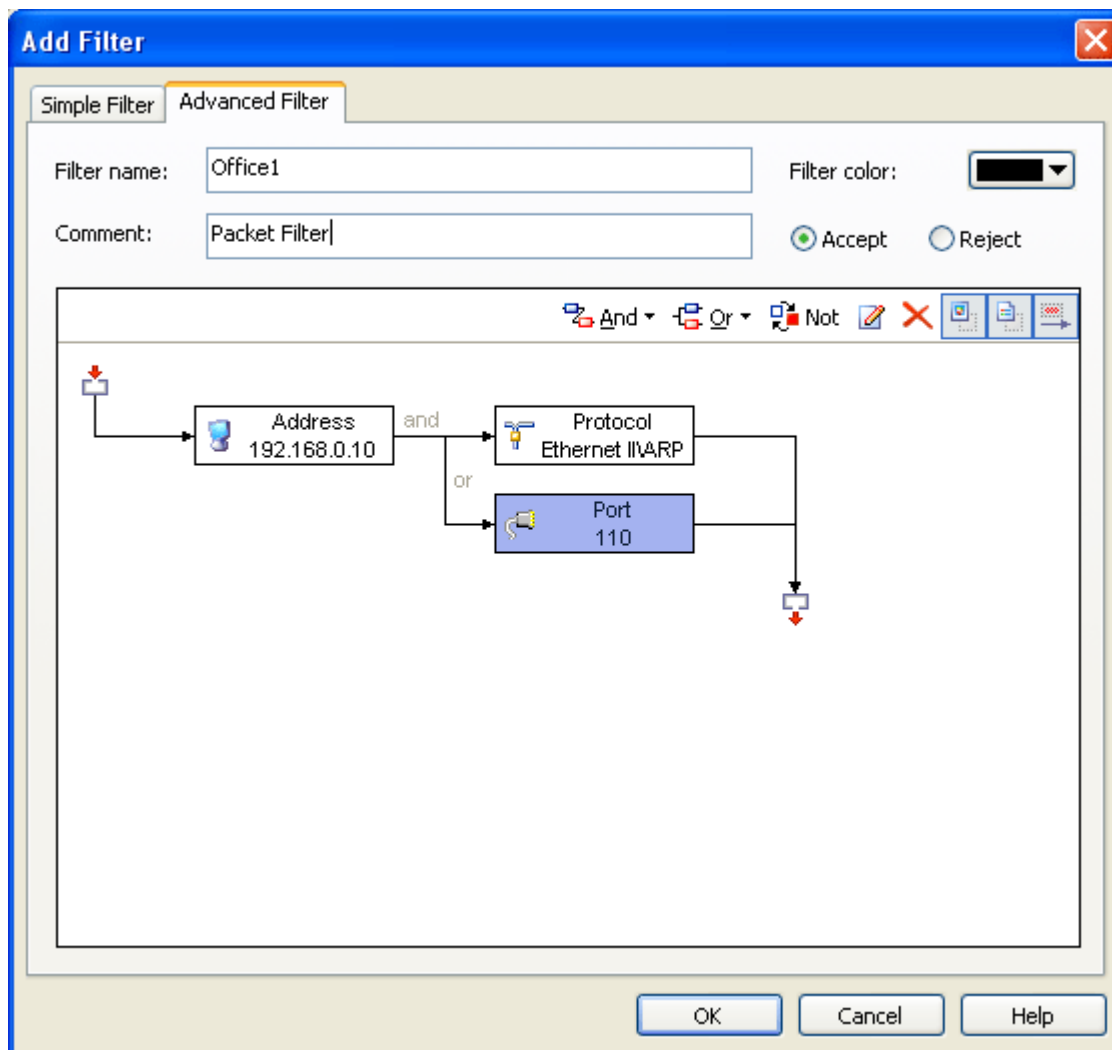
Port2

Any port


☒ Protocol filter

Name	Path
ICMP	Ethernet II\IP\ICMP
IGMP	Ethernet II\IP\IGMP


The simple filters defined can also be seen in the **Advanced Filter** page as below.

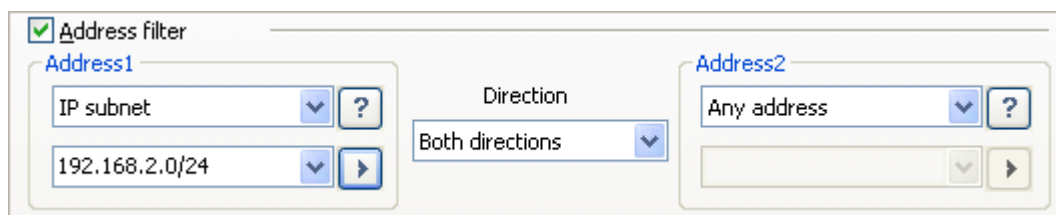


• Address filter

You can set an address filter by physical address, IP address, IP range and IP subnet. To define an address filter, check the checkbox of **Address filter** first, select an address type from the upper combo box of **Address1**, then input an address into the lower combo box or select from the name table. Click the  icon to get references if you are not familiar with address formats.

The combo box of **Direction** is for you to specify the send/receive relationship between the two addresses. You should select **Both directions** to match all packets going in either direction between address 1 and address 2, otherwise you could instead match only traffic going from address 1 to address 2, or match only traffic going the other direction.

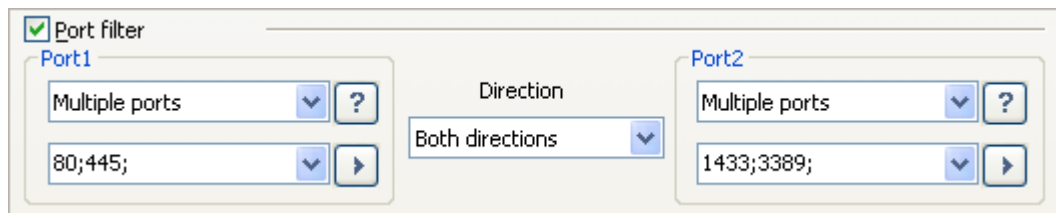
Similar as **Address1**, you must select an address type and enter a valid address in **Address2**, or simply choose **Any Address**. You can select an address from the name table for both **Address1** and **Address2** by clicking the  icon. Below is an example of address filter.



- **Port filter**

To define a port filter, check the **Port filter** checkbox, select a port type and input parameters with correct format in **Port1**. Notice that if you select **Multiple ports**, the ports you enter must be separated with semicolon. Other settings are similar as the **Address filter** section.

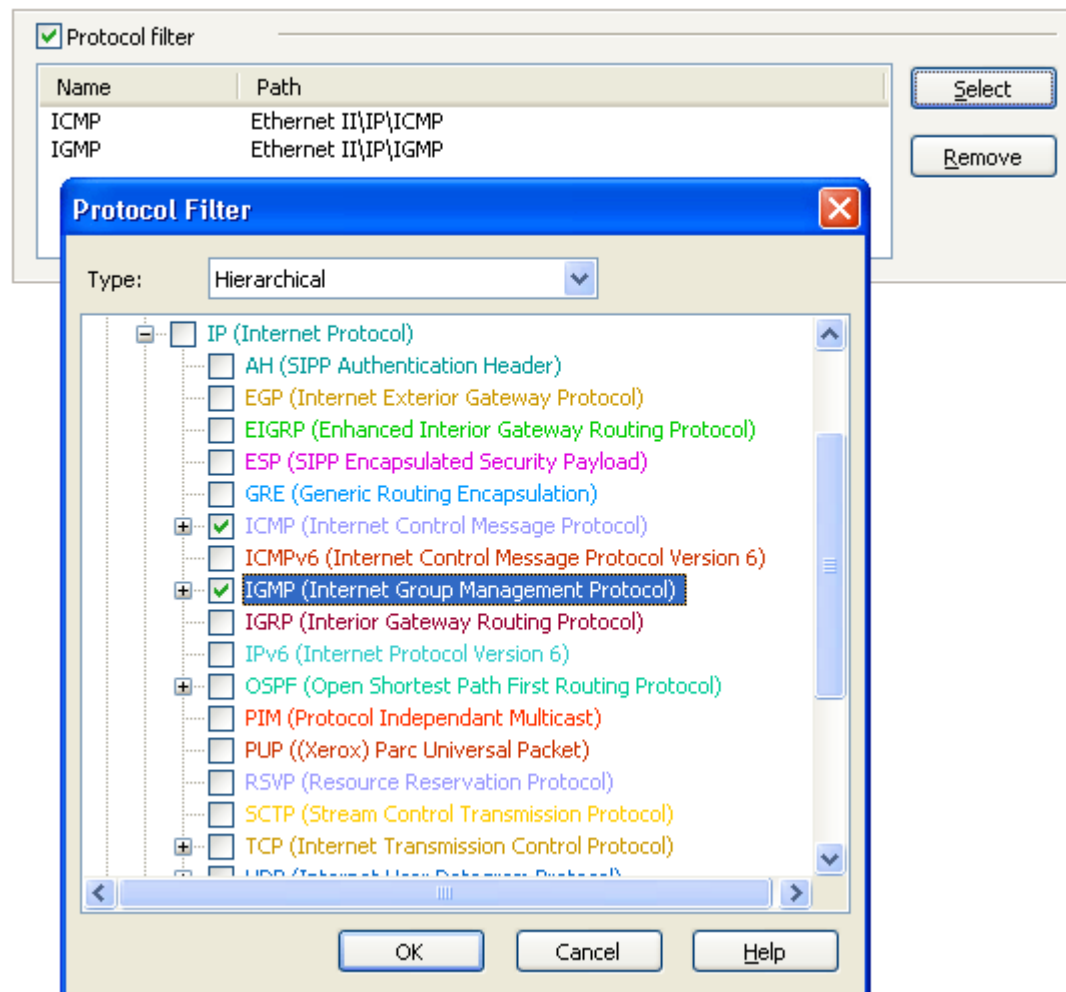
Below is an example of port filter.



- **Protocol filter**


To define a protocol filter, check the **Protocol filter** checkbox, click the **Select** button to open the **Protocol Filter** dialog, find protocols by the first alphabet of the protocol name, then select protocols by checking the corresponding check box and click **OK** to confirm your selection. The selected protocols are listed in the pane at the bottom of the **Simple Filter** page, you can delete a protocol item from the list with the **Remove** button.

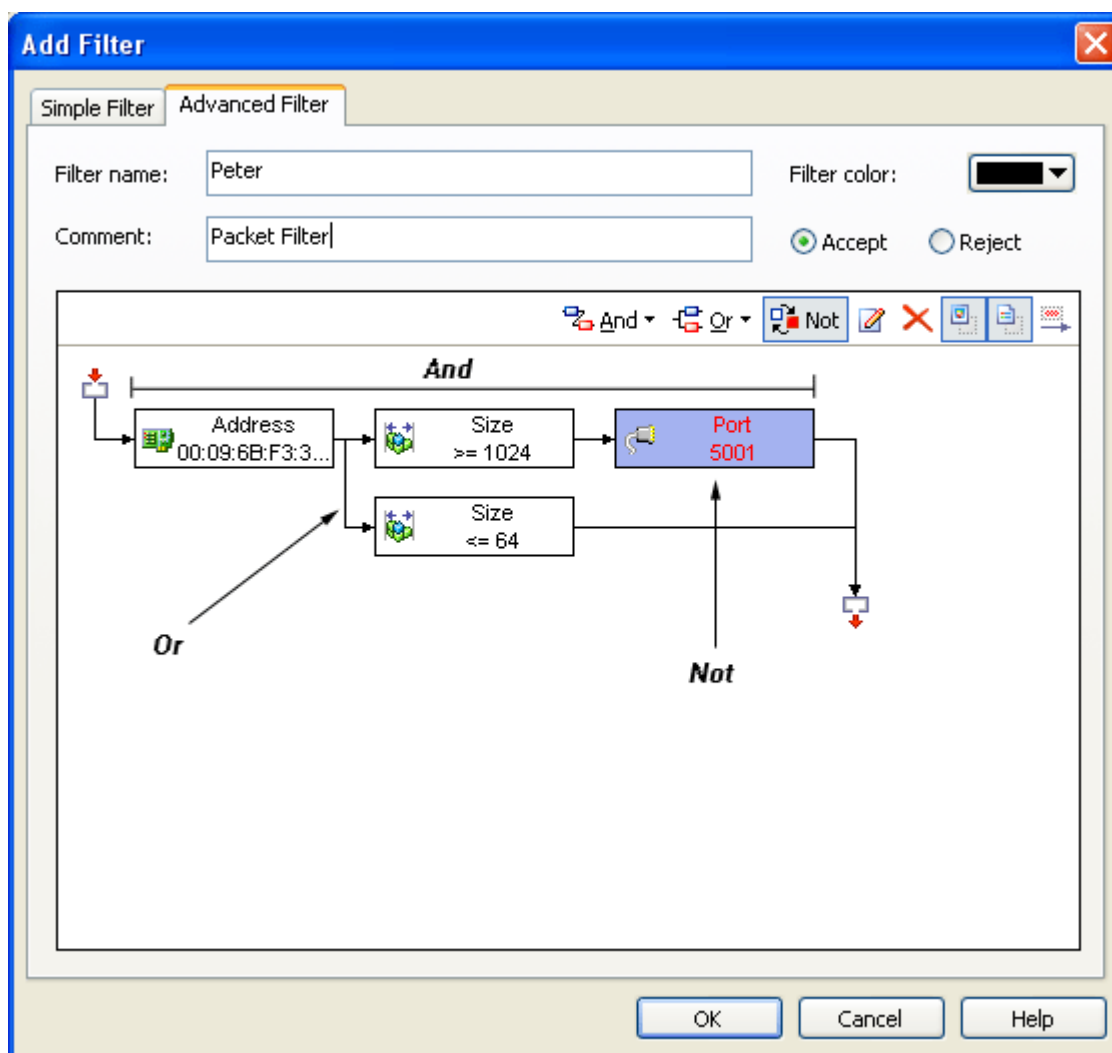
Below is an example of protocol filter.



Advanced filters

In addition to make simple filters by address, port and protocol, you can also choose packet size, packet value and packet pattern as filter parameters, which are available in the **Advanced Filter** page. Advanced filters are unique to Colasoft Capsa enterprise edition.

To create an advanced filter, click the **Filter** icon  from the toolbar to open the **Project Settings - Filter** page. Click the **Advanced Filter** tab, you can see a screen with some icons and the text **And**, **Or**, **Not** representing the rules for settings advanced filters. The filter name, filter color and comment can be customized, if you check the check box of **Set as default**, this advanced filter will appear in the filter list each time when you open a new project.



You should specify a rule before adding a new filter item using logical **And** or logical **Or** statement; logical **Not** statement is for you to not accept the current filter item. The table below provides brief descriptions for these rules and other commands available in the **Advanced Filter** page.

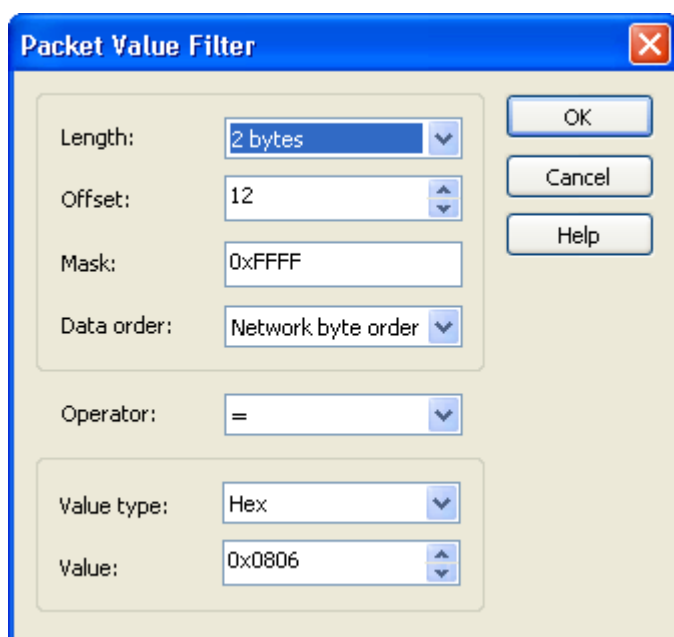
Command	Description
Set as default	The settings and rules in this filter will be saved, it will appear in the predefined filter list when you start a new project.
And	The logical And statement shows the relationship of these filters is paratactic, that is, the packet to be captured must meet all these filters.

Or	The logical Or statement shows the relationship of these filters is random.
Not	All packets except those matching the criteria inside this logical Not filter will now be passed to the next stage.
Edit	Opens the corresponding dialog to modify the parameters involved.
Delete	Deletes the selected filter.
Show Icon	Shows filter icon for each filter item.
Show Details	Shows details of each filter item.

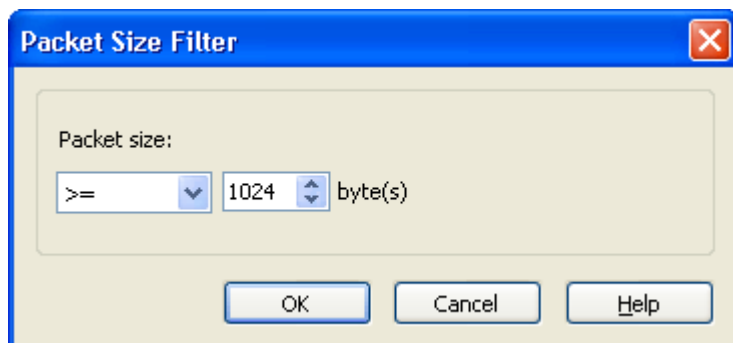
You may define **Address** filters, **Port** filters and **Protocol** filters in either the **Simple Filter** page or the **Advanced Filter** page, but **Packet Value** filters, **Packet Size** filters and **Packet Pattern** filters can only be defined in the **Advanced Filter** page. It is allowed to switch between the **Simple Filter** page and the **Advanced Filter** page, however, you are in danger of losing the specified parameters you have already entered as moving from the **Advanced Filter** to the **Simple Filter** page, you have an opportunity to abort the operation when a warning appears.

Click the rule **And** or **Or** and select a filter item to define, the rule **Not** is disabled unless you choose an existing filter item first. The following are some setting examples.

- **Packet Value filter**

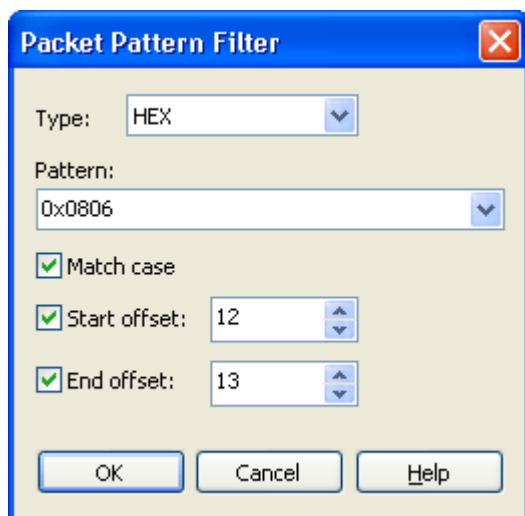


- **Packet Size filter**




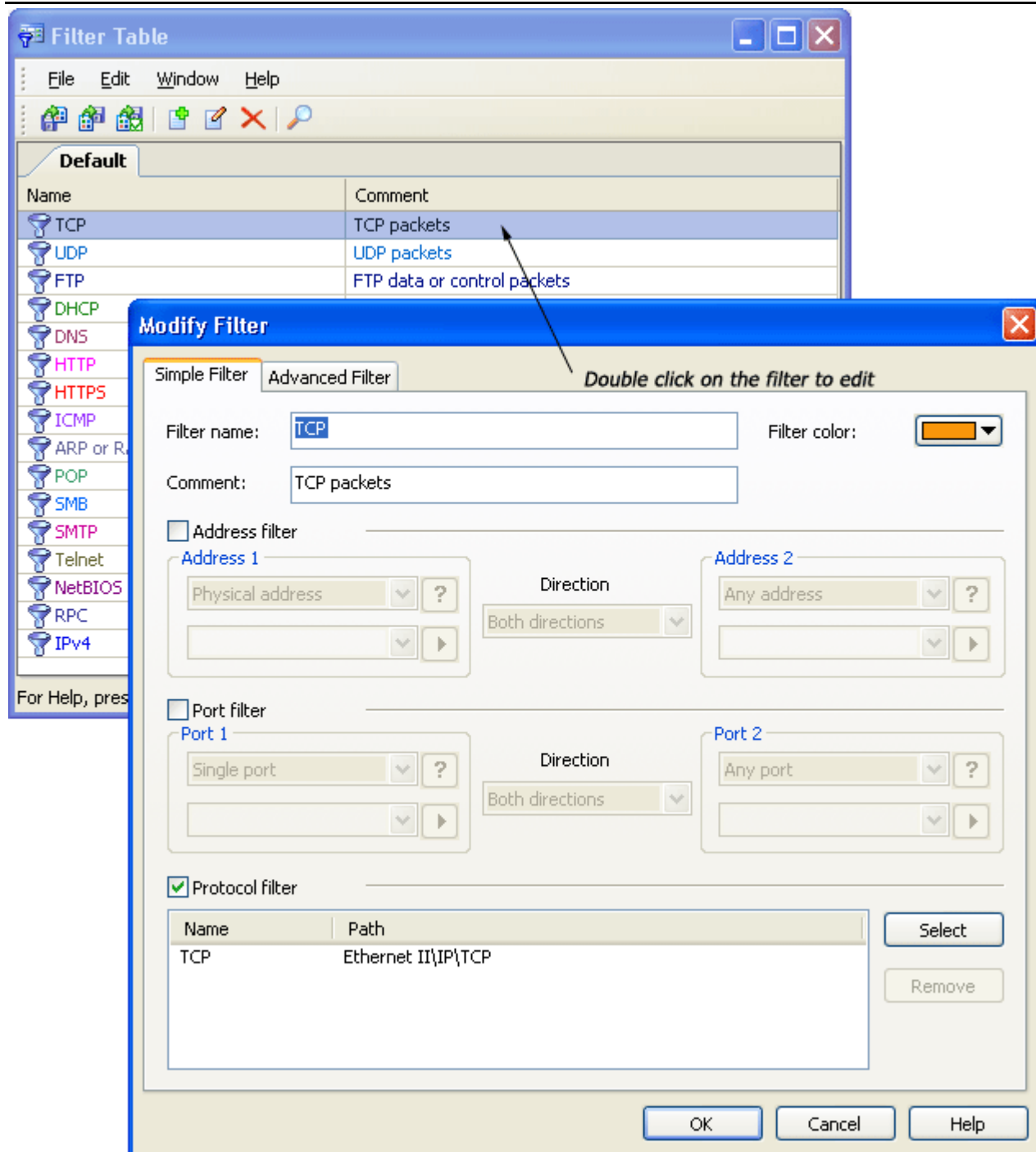
- **Packet Pattern filter**

You can set packet pattern filters by ASCII, HEX, UTF-8 or UTF-16.



Filter table

By clicking on the button  from the toolbar you can open the **Filter Table** which offers the most frequently used protocol filters predefined by system. This table lets you export, edit or delete the listed filter, you may also import filter from file or add a new filter. The change to this table is global.



Command Line Parameters

You can invoke Colasoft Capsa or launch the Help documentation using command line parameters. To open the command line window, you can click the **Start** menu and select the **Run...** command, input *capsa* in the **Run** dialog and click **OK** to confirm.

Then start the command line from the installation category of Colasoft Capsa, e.g. *C:\Program Files\ Colasoft Capsa 6.1 Enterprise*.

Command line formats:

- *Capsa.exe <.cscproj> | <.cscpkt> | <.cpf> | <.cap> | <.pkt> | <.rawpkt>* - opens an existing project or packet file.

Example: *Capsa.exe C:\Traffic05624.cscproj*

- *Capsa.exe /autostart <.csctemp>* - opens an existing template file and start capturing packets.

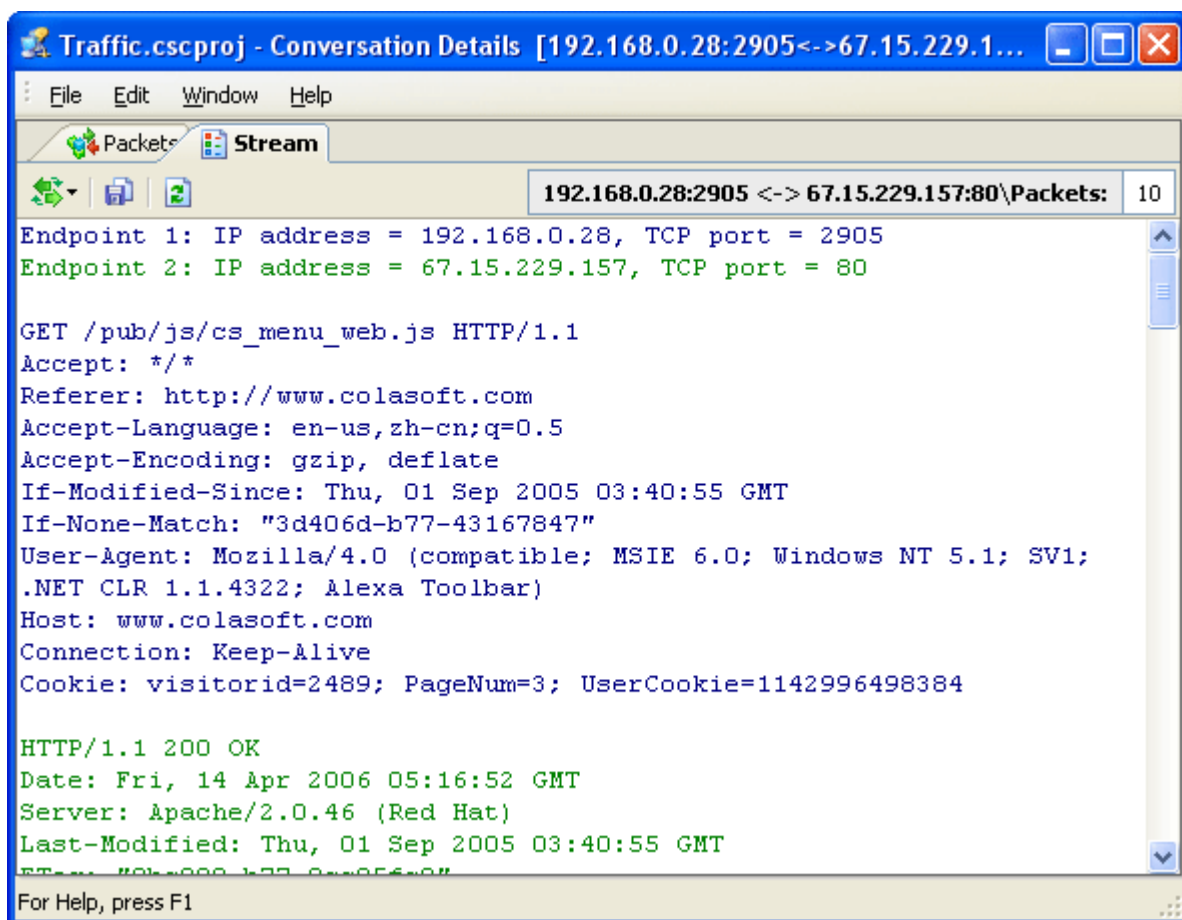
Example: *Capsa.exe/autostart "C:\Documents and Settings\Eva\Desktop\Traffic05624.csctemp"*

- *Capsa.exe /? or /help* - displays the Help information for command line.

TCP Reconstruction

Colasoft Capsa can reconstruct TCP conversations. The captured TCP conversations are listed in the **Conversations** view, to see the reconstructed contents, you should first select an item from the conversation list, then push the **Stream** sub-view tab at the lower section of the display, or double click the selected conversation to open the **Conversation Details** window, where you can see more conversation details, including streams and logs.

When a TCP stream is in plain text format, its contents are readable in the **Stream** view. Below is some example stream of a HTTP conversation.



To view a HTTP conversation in its original format, select a HTTP conversation from the Packets sub-view. All logged HTTP requests are presented in this sub-view, check to Stream sub-view or double click a URL to open it. A HTTP conversation may contain numbers of URLs, some of them can not be opened, e.g. the URLs ended with .css and .js.

Name Table

When you start capture, the nodes in your network will be automatically identified and displayed by their logical or physical addresses in the **Project Explorer** and tab views. The **Name Table** lets you create and edit the alternate name for physical addresses, IP addresses and ports.

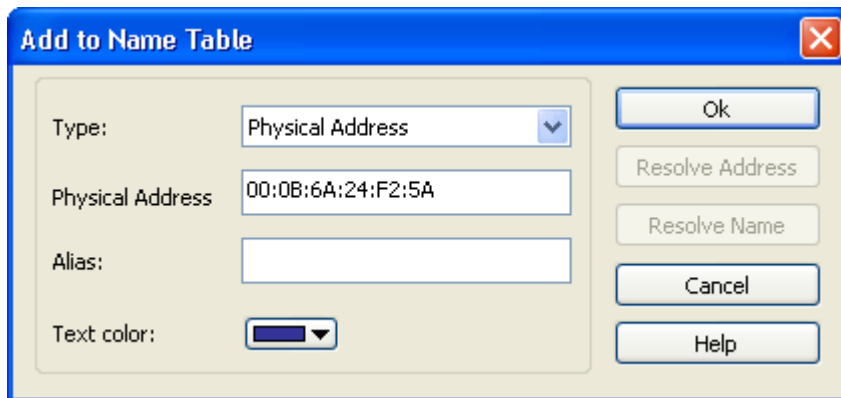
This chapter explains how to assign your own symbolic names to make packet-related information easy for recognition.

Adding to name table

You can add alias to the name table from the **Project Explorer** dock window or tab views.

- **Add from the Project Explorer dock window**

Select a node and the **Add to Name Table...** command from the context menu with a right click, then make alias and set color in the opened dialog.



- **Add from tab views**


You can make alias in all tab views except the **Summary** view, **Protocols** view and **Graph** view. Highlight a row and right click, select the **Add to Name Table** command and a type from the context menu, in the opened dialog give a new name to the selected item, you may also alter its color. Once you click **OK** to save the settings all the packets matching to your selection will be showed with the new name and color.

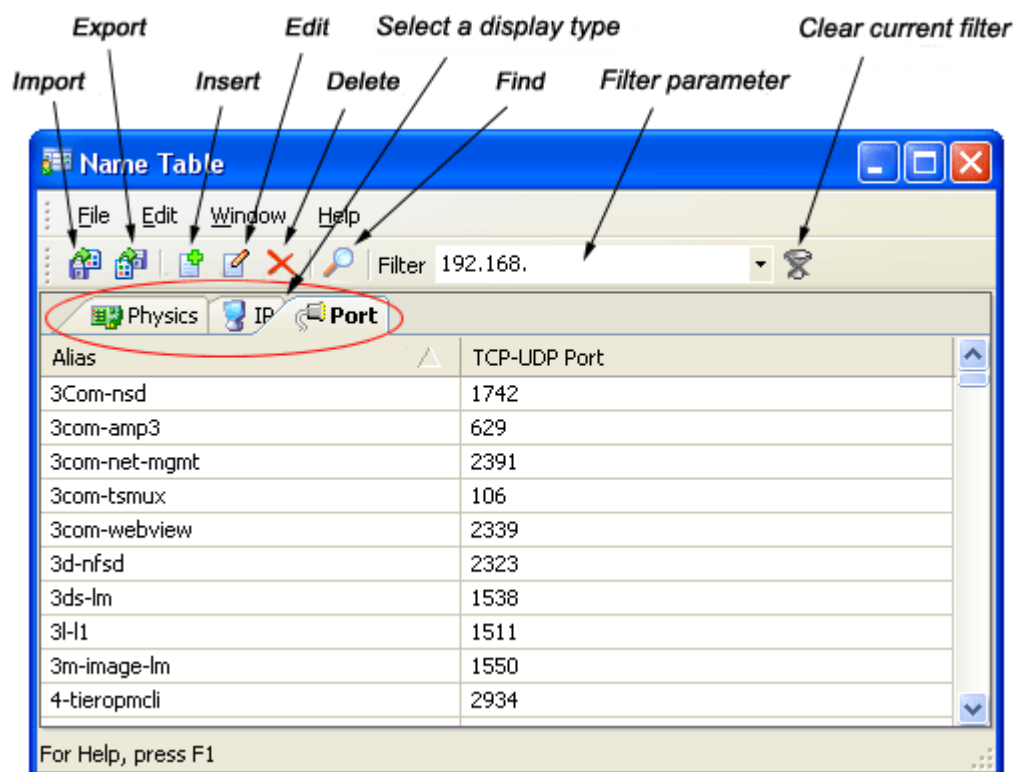
One packet may involve multiple aliases because you can alter the name for physical addresses, IP addresses and ports, e.g. *office1* for source IP and *office2* for destination IP.

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs					
No.	Absolute Time	Source	Destination	Protocol	
22	16:07:07.102354	office1:http	office2:1911	HTTP	
23	16:07:07.338653	office1:http	office2:1911	HTTP	
24	16:07:07.444256	office2:1911	office1:http	HTTP	
25	16:07:10.187158	localhost:1909	localhost:1909	UDP	
26	16:07:10.187527	localhost:1909	localhost:1909	UDP	
27	16:07:10.187662	office2:1912	www.colasoft...	HTTPS	
28	16:07:10.536590	localhost:1909	localhost:1909	UDP	

Alias for source IP
Alias for destination IP

Name table window

The **Name Table** window lets you insert, edit, delete or find alias. To open the **Name Table** window, click the **Tools** menu and select **Name Table**, or just click the icon  from toolbar. In the **Name Table** window, you can view alias for physical addresses, IP addresses and ports.



This window offers the following commands:

Name	Hot Key	Description
Copy		Copies the selection and put it to clipboard.
Insert...	Insert	Adds a new record to the alias list.
Edit...		Edits the name or text color of the selected alias.
Delete	Delete	Removes the selected record from the alias list.

Select All		Selects all alias records.
Find...	Ctrl+F	Finds an alias item in the list.
Filter		Set an alias condition to only display those records matching the filter.
Clear		Clear the current filter and display all records.

The alias records in the **Name Table** window are able to be printed, you may have a preview by the command in the **File** menu. To switch between the **Name Table** window and project windows, just open the **Window** menu and make a selection.

Logs

The logs in Colasoft Capsa can record global or scope-specific network events, containing four types of log primarily generated by the advanced analyzers: HTTP requests, email messages, FTP transfers, DNS analysis and four instant messenger activities: MSN activity, AIM activity, ICQ activities, and Yahoo Messenger Activities. Colasoft Capsa enables all logs by default, you can change each log's settings in the **Project Settings - Log** page. If a log is disabled, you will not see the results in the **Logs** view.



Summary Diagnosis Endpoints Protocols Conversations Matrix Packets Logs Graphs Re							
HTTP Requests						Logs: 296	
Time	Client	Server	Requested URL	Method	St...	Server	
10:38:42	192.168...	74.53.47...	http://www.umpcf...	GET	304	HTTP/	
10:38:42	192.168...	74.53.47...	http://www.umpcf...	GET	304	HTTP/	
10:38:43	192.168...	74.53.47...	http://www.umpcf...	GET	304	HTTP/	
10:38:43	192.168...	74.53.47...	http://www.umpcf...	GET	304	HTTP/	
10:45:04	192.168...	192.168.0...	http://192.168.0.1...	GET	200	HTTP/	
10:47:53	192.168...	218.30.82...	http://stat07.cp.ici...	GET	200	HTTP/	
10:48:58	192.168...	rad.msn.c...	http://rad.msn.co...	GET	200	HTTP/	
10:49:01	192.168...	msn.cdn.a...	http://msn.allves.c...	GET	200	HTTP/	
10:49:00	192.168...	rad.msn.c...	http://rad.msn.co...	GET	200	HTTP/	
10:49:02	192.168...	219.153.5...	http://msnms.allve...	GET	200	HTTP/	
10:49:10	192.168...	rad.msn.c...	http://rad.msn.co...	GET	200	HTTP/	
10:53:16	192.168...	72.14.255...	http://toolbar.qoo...	GET	200	HTTP/	
10:54:38	192.168...	218.30.82...	http://stat07.cp.ici...	GET	200	HTTP/	
10:57:35	192.168...	64.215.16...	http://c.icq.com/xt...	GET	200	HTTP/	
10:57:35	192.168...	64.215.16...	http://df.icq.com/c...	GET	200	HTTP/	
10:57:35	192.168...	64.215.16...	http://c.icq.com/xt...	GET	200	HTTP/	
10:57:37	192.168...	64.215.16...	http://df.icq.com/c...	GET	200	HTTP/	
10:57:38	192.168...	64.215.16...	http://df.icq.com/c...	GET	200	HTTP/	
10:57:39	192.168...	64.215.16...	http://df.icq.com/c...	GET	200	HTTP/	
10:57:40	192.168...	64.215.16...	http://df.icq.com/c...	GET	200	HTTP/	
10:58:09	192.168...	64.12.164...	http://cb.icq.com/c...	GET	404	HTTP/	
10:58:14	192.168...	207.46.96...	http://config.mess...	GET	200	HTTP/	
10:58:14	192.168...	131.107.1...	http://www.sgm.m...	POST	403	HTTP/	
10:58:26	192.168...	219.153.4...	http://images.zhao...	GET	200	HTTP/	
10:58:26	192.168...	219.153.5...	http://images.love...	GET	200	HTTP/	
10:58:26	192.168...	219.153.4...	http://msn.bitauto...	GET	200	HTTP/	
10:58:26	192.168...	202.104.2...	http://mscdn.allve...	GET	200	HTTP/	
10:58:26	192.168...	202.104.2...	http://mscdn.allve...	GET	200	HTTP/	
10:58:27	192.168...	125.76.23...	http://public.marry...	GET	200	HTTP/	
10:58:27	192.168...	60.28.241...	http://house.ynet...	GET	200	HTTP/	

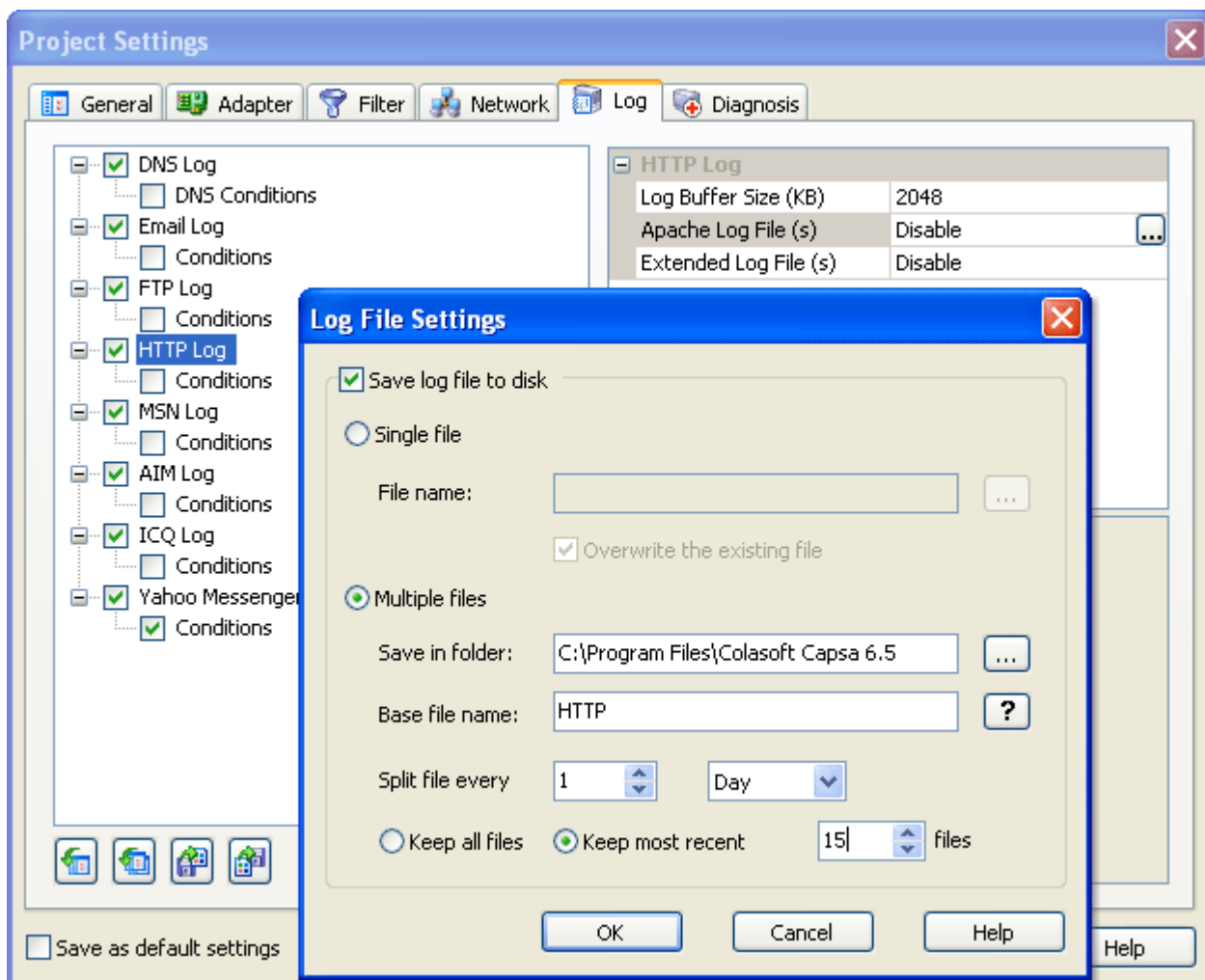
- **HTTP Requests** view - presents the information of captured web accesses. You can open a URL with double clicks on it or use the **Open** command from the context menu.
- **Email Messages** view - lists captured emails and such information as client, server, sender name, receiver name, etc.... To view the reconstructed contents of email, just double click the selection to open it with your email client, or use the **Open** command from the context menu.


Note: Captured emails may contain virus, please be cautious when you open an email.
- **FTP Transfers** view - offers the records of **FTP** uploads and downloads.
- **DNS Analysis** view – presents the analysis results of DNS requests and replies.
- **MSN Activity** view - offers the records of MSN activities.

- **AIM Activity** view - offers the records of AIM activities.
- **ICQ Activity** view - offers the records of ICQ activities.
- **Yahoo Messenger Activity** view - offers the records of Yahoo Messenger activities.


Generating log files

To generate log files, you should first enable the log file feature. Open the **Log** page by clicking the icon  in the toolbar, select a type on the left, then enable the selected log file on the right. Click the button  to open the **Log File Settings** dialog, where you can name the log file and designate file path. Colasoft Capsa will automatically generate log files if you check **Multiple files** and set the parameters; you may also customize the count of log files saved in your system.



By clicking the browse button  and check **Save log file to disk**, you can select to save all captured email logs to a single file or multiple files which are split by time or size.


- **Single file**
All packets are saved to a same file.
 - **File name**

Specifies a name for the packet file. Click the  button on the right to open a dialog for defining a save path for the packet file.


- **Multiple files**

Packets are saved to the files split by time or size. To reduce the total size, you may choose to only keep the most recent files.

- **Save in folder**

Specifies a folder name and the save path for all files. Click the  button on the right to open a dialog for defining a save path for the folder.

- **Base file name**

The portion of a file name to the left of the period separator. Colasoft Capsa allows very long file names. Click the  button to view a example of the base file name.

- **Split file every**

Chooses a rule for splitting the file if the file size is too big. You can split files by time or file size - months, days, hours, minutes, KB, MB.

- **Keep all files**

Saves all split files in the defined save path.

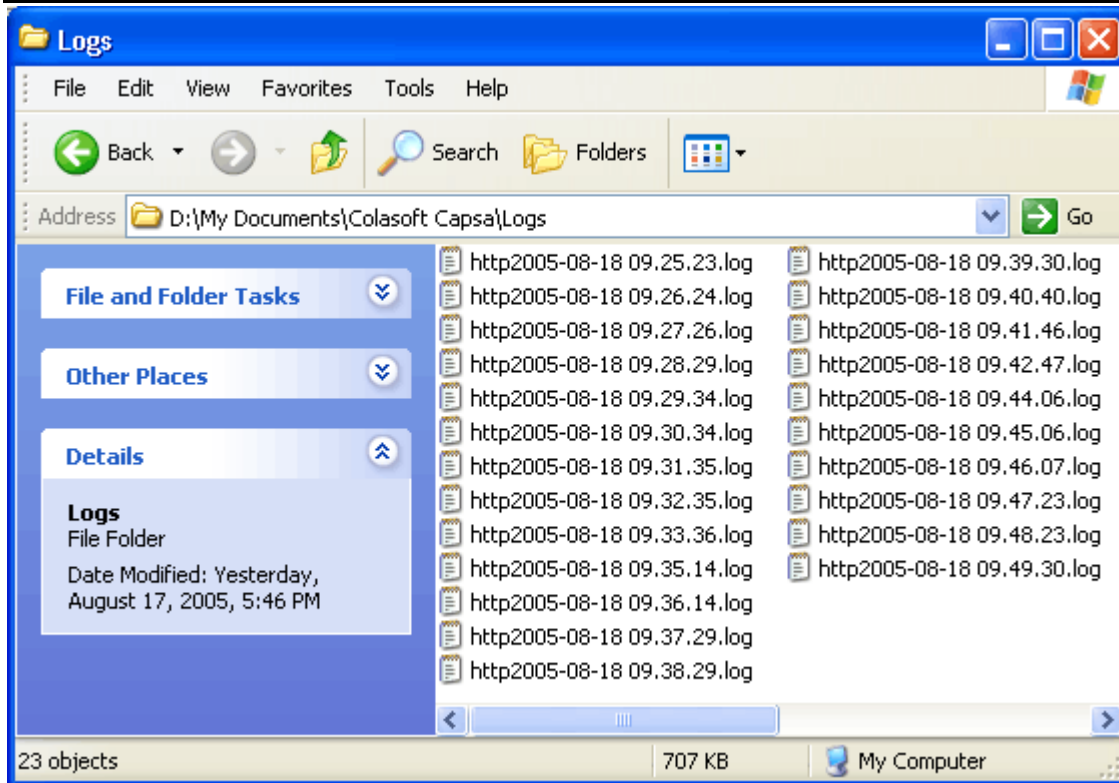
- **Keep most recent**

Specifies the number of most recent files for saving.

Log file formats

Colasoft Capsa generates HTTP, email, FTP or DNS log files only when these logs are enabled in the **Project Settings - Log** page, where you can designate analysis ports, set filters, select log location or customize other options. The format of log files is: *name%year-%month-%day hour.minute.second.log*. For example, a log generated on August 18th, 2005 09:25:23 AM with the base file name "http" is shown as *http2005-08-18 09.25.23.log*.

Logs can be saved to a single file or split files. If you select split files, Colasoft Capsa will automatically split log files by month, day, hour, minute, KB or MB.



Decoding Packets

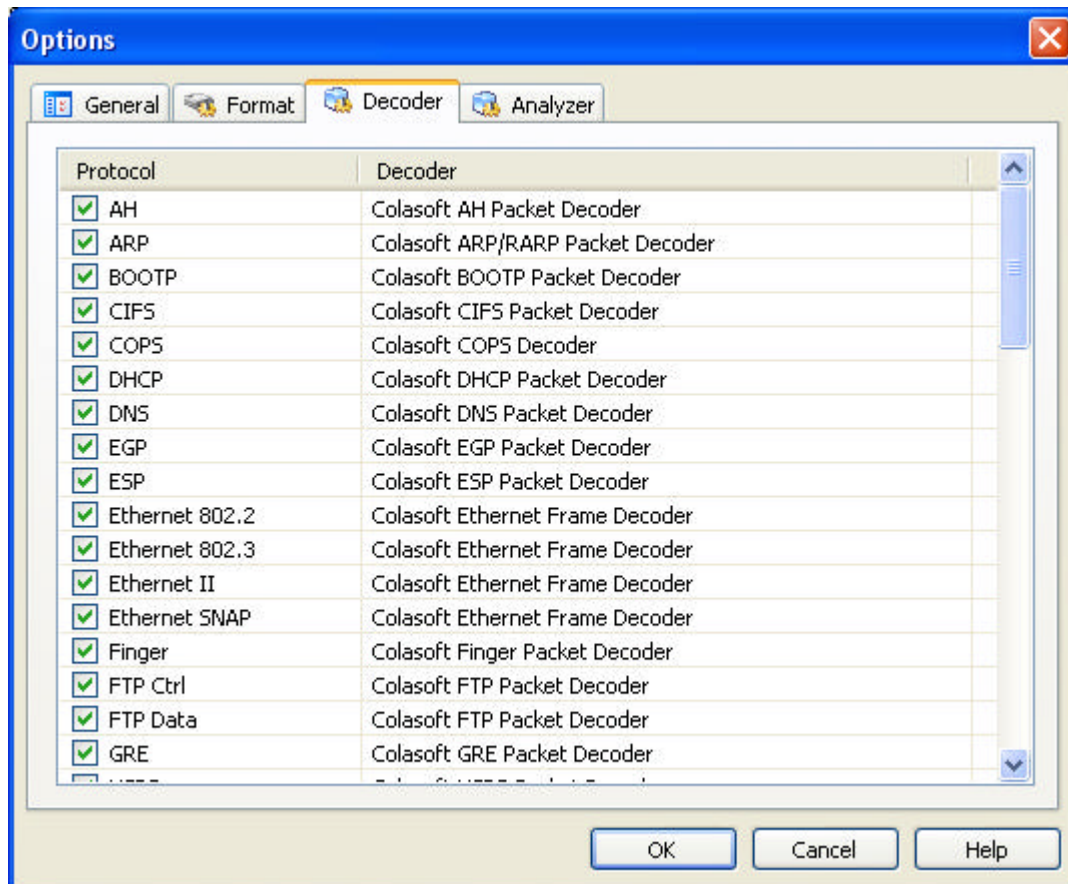
Colasoft Capsa analyzes and decodes packets and displays detailed packet information in the **Packets** tab view and its sub-views. Packet decoding information lets you look through the packets themselves, which is very useful in troubleshooting your network to track down security vulnerability or learning more knowledge about protocols and network services.

The following sections introduce the Colasoft Capsa decoders, describe how to read a packet's information and decode.

Packet decoders


The packet decoders are the essential engines to decode packets. All available decoders are enabled by default, but you can close those you don't need to increase the program performance.

To open the **Options - Decoder** page, select **Options...** from the **Tools** menu and then press the **Decoder** tab. All decoders are listed by protocol and marked with a tick indicating they are enabled, use the check box before every decoder to disable it.

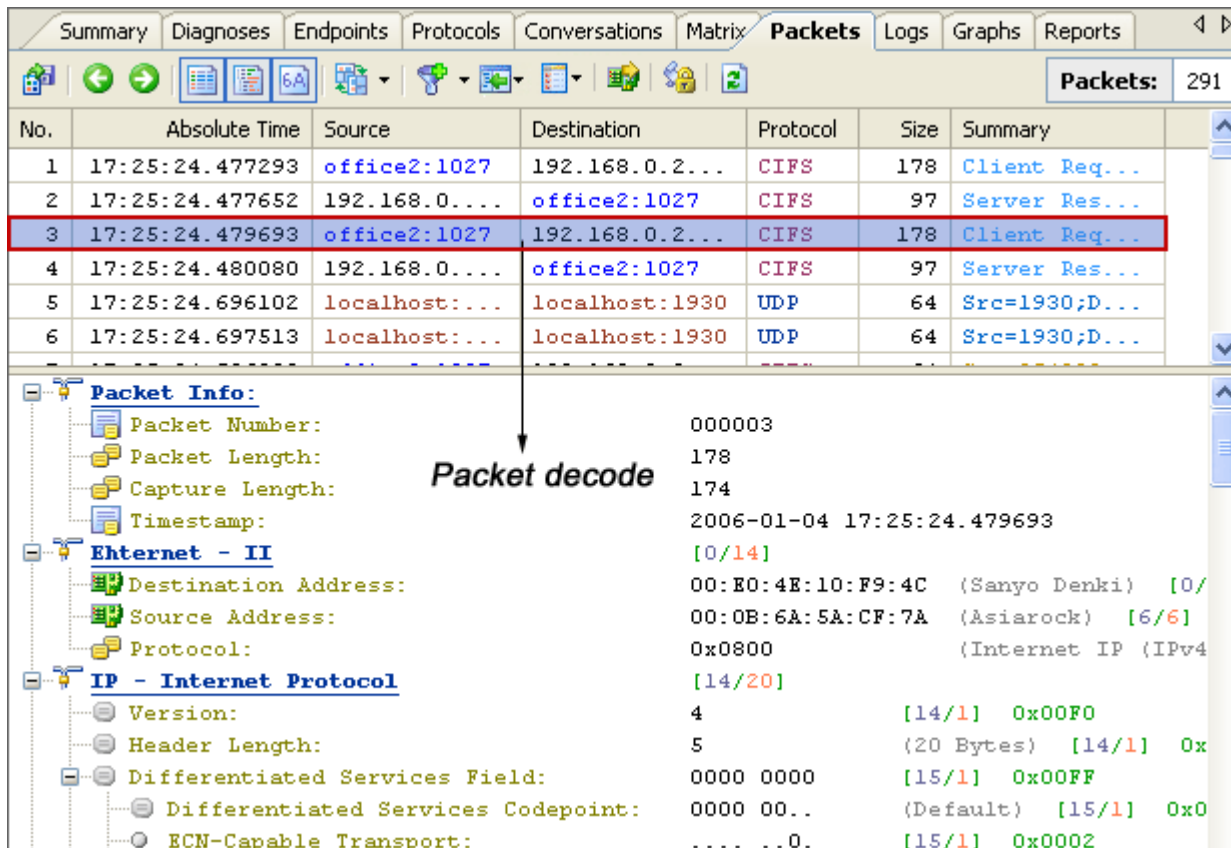


Note: The decoders are applicable to global packet decoding. When you disable a decoder in the **Decoders** dialog, Colasoft Capsa will continue not to use that decoder to decode the packets of the same type until you enable it again.

Decode view

To view the decode information of the current packet, press the **Show Decode** icon  in the toolbar to open the decode sub-view, or double click on the packet to open the **Packet Decode** window.

The packet decode view presents information based on the protocol used in packet transmission, click on the - minus or + plus signs in the margin to collapse or expand the view of any header section.



Summary **Diagnoses** **Endpoints** **Protocols** **Conversations** **Matrix** **Packets** **Logs** **Graphs** **Reports**

Packets: 291

No.	Absolute Time	Source	Destination	Protocol	Size	Summary
1	17:25:24.477293	office2:1027	192.168.0.2...	CIFS	178	Client Req...
2	17:25:24.477652	192.168.0....	office2:1027	CIFS	97	Server Res...
3	17:25:24.479693	office2:1027	192.168.0.2...	CIFS	178	Client Req...
4	17:25:24.480080	192.168.0....	office2:1027	CIFS	97	Server Res...
5	17:25:24.696102	localhost:...	localhost:1930	UDP	64	Src=1930;D...
6	17:25:24.697513	localhost:...	localhost:1930	UDP	64	Src=1930;D...

Packet Info:


- Packet Number: 000003
- Packet Length: 178
- Capture Length: 174
- Timestamp: 2006-01-04 17:25:24.479693
- Ethernet - II**
 - Destination Address: 00:80:4E:10:F9:4C (Sanyo Denki) [0/14]
 - Source Address: 00:0B:6A:5A:CF:7A (Asiarock) [6/6]
 - Protocol: 0x0800 (Internet IP (IPv4))
- IP - Internet Protocol**
 - Version: 4 [14/1] 0x00F0
 - Header Length: 5 (20 Bytes) [14/1] 0x...
 - Differentiated Services Field: 0000 0000 [15/1] 0x00FF
 - Differentiated Services Codepoint: 0000 00.. (Default) [15/1] 0x0...
 - ECN-Capable Transport:0. [15/1] 0x0002

The following decode information is added by Colasoft Capsa.

Name	Description
Packet Number	The packet number which is set automatically by Colasoft Capsa.
Packet Length	The bytes size of this packet.
Capture Length	The bytes size captured by Colasoft Capsa.
Timestamp	The actual time when the packet was captured.

The data in the decode view can be copied and pasted to the clipboard.

HEX and ASCII view

Push the **Show Hex**  icon in the **Packets** view or **Packet Decode** window to view the actual packet contents in Hex on the left and ASCII on the right (by default), or change ASCII decode to EBCDIC by choosing **Show EBCDIC** from the context menu with a right click on the Hex view.

The Hex view is graphically linked with the decode view, when you select a portion of packet contents in the decode view, Colasoft Capsa highlights the selected portion and the corresponding Hex data and ASCII/EBCDIC data in the Hex view.

Packet decode

Packet Info:

- Packet Number: 044725
- Packet Length: 1510
- Capture Length: 1506
- Timestamp: 2005-08-18 10:23:52.108324

Ethernet II Header

- Destination Address: 00:0B:6A:1F:1A:95 Asiarock [0/6]
- Source Address: 00:80:C8:21:64:D4 D-Link Sys [6/6]
- Protocol: 0x0800 Internet IP (IPv4) [12/2]

IP - Internet Protocol

[14/20]

Offset	Hex	ASCII
0000	00 0B 6A 1F 1A 95 00 80 C8 21 64 D4 08 00 45 00 05 D4 88	..j...!d..E....
0013	D0 40 00 2E 06 76 EB C0 43 C6 38 C0 A8 00 44 00 50 0B 65	.@...v..C.8...D.P.e
0026	F8 0C 18 28 E0 C7 C9 A1 50 10 60 6C 46 DF 00 00 28 C4 E8	...{....P.`1F...{..
0039	83 B4 47 26 D0 02 D4 AE B0 A5 9B 19 22 31 1C A5 CC 3E 25	..G "1...>%
004C	01 E1 64 DD AB 46 EE D0 07 CC 28 F3 41 37 6A 40 47 DE E7	..d..F...(.A7j@G..
005F	F1 CC 56 5D DA B2 E2 8D 8E B7 44 AF BA 35 2F B2 97 3B 0A	..V].....D..5/...;

Hex

ASCII

Tools

Colasoft Capsa provides users several useful tools - **Colasoft Packet Builder**, **Colasoft Ping Tool**, **Colasoft Mac Address Scanner** and **Colasoft Packet Player**, let users can build packet, ping IP addresses, scan IP and MAC addresses, replay packet file. Besides these four useful and handy tools, user can also customize to invoke other applications or tools from Colasoft Capsa, such as the **Tracert**, **Microsoft Office Word 2003**, **Notepad**, and etc.

Colasoft packet builder

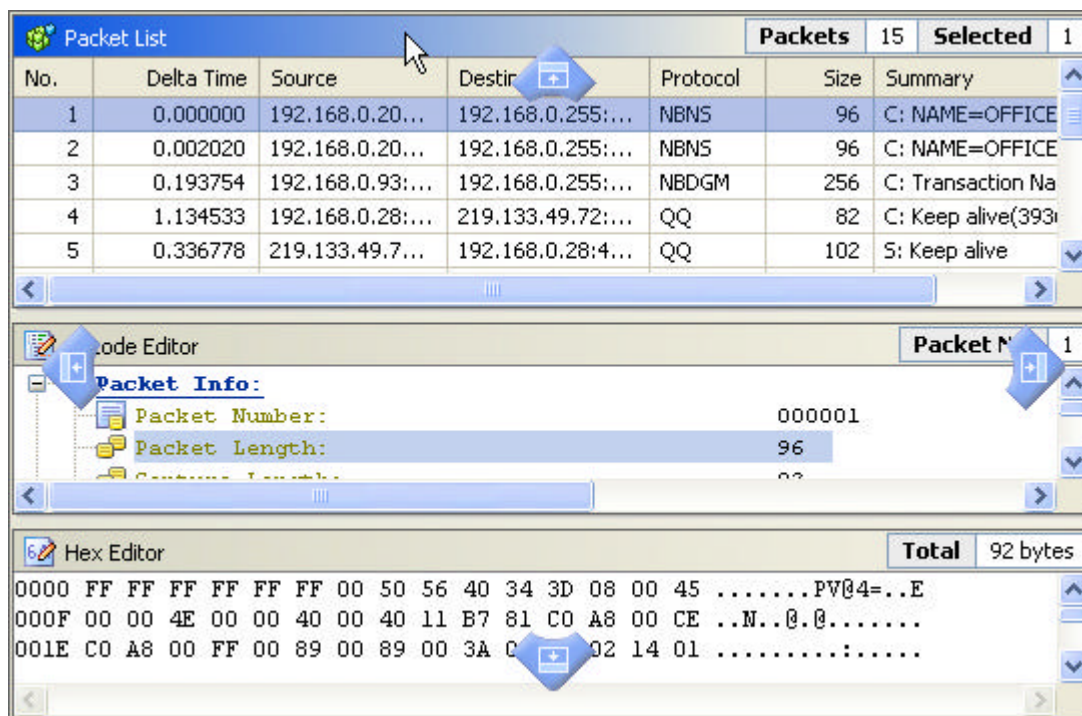
Packet Builder is a tool used for constructing your own custom packets and sending them into the network. You could use this feature to check your network for protection against attacks and intruders.

There are three ways to invoke Colasoft Packet Builder:

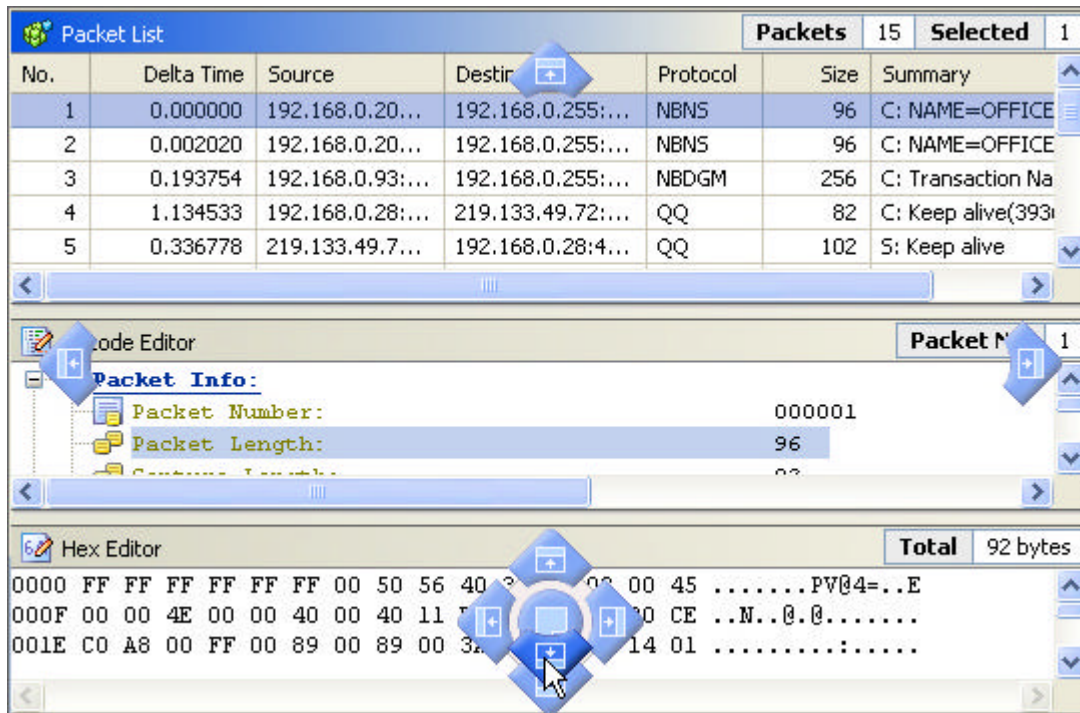
- Click the **Colasoft Packet Builder** command in the **Tools** menu.
- Open the **Start** button of Windows and choose **All Programs**. Click the **Colasoft Packet Builder** from the Colasoft Capsa application.
- Choose the **Run...** command from the **Start** button of Windows, input **PktBuilder.exe** command and click the **Enter** key.

You can select one of the provided templates and change the parameters in the decoder editor, hexadecimal editor and ASCII editor to create a packet. Any changes are immediately displayed in the other two windows.

To custom the layout of the three windows, please click the window header, hold on mouse and move it.



Hold on and drag your mouse to the position displayed in the below figure.



Packet List Packets: 15 Selected: 1

No.	Delta Time	Source	Destination	Protocol	Size	Summary
1	0.000000	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE
2	0.002020	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE
3	0.193754	192.168.0.93:...	192.168.0.255:...	NBDGM	256	C: Transaction Na
4	1.134533	192.168.0.28:...	219.133.49.72:...	QQ	82	C: Keep alive(393i
5	0.336778	219.133.49.7...	192.168.0.28:4...	QQ	102	S: Keep alive

Code Editor Packet No. 1

Packet Info:

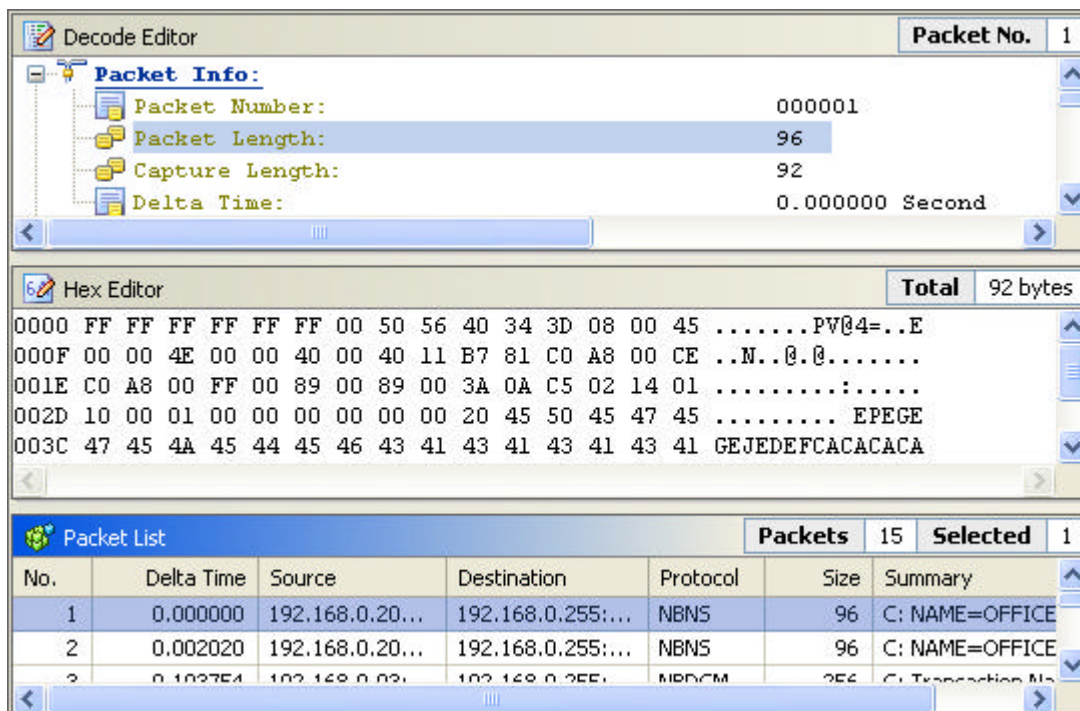
- Packet Number: 000001
- Packet Length: 96
- Capture Length: 92

Hex Editor Total: 92 bytes

```

0000 FF FF FF FF FF FF 00 50 56 40 34 3D 08 00 45 .....PV@4=..E
000F 00 00 4E 00 00 40 00 40 11 B7 81 C0 A8 00 CE ..N..@.@.....
001E C0 A8 00 FF 00 89 00 89 00 3A 0A C5 02 14 01 .....:.....
  
```

Then you will see the Packet List window move to the bottom.



Decode Editor Packet No. 1

Packet Info:

- Packet Number: 000001
- Packet Length: 96
- Capture Length: 92
- Delta Time: 0.000000 Second

Hex Editor Total: 92 bytes

```

0000 FF FF FF FF FF FF 00 50 56 40 34 3D 08 00 45 .....PV@4=..E
000F 00 00 4E 00 00 40 00 40 11 B7 81 C0 A8 00 CE ..N..@.@.....
001E C0 A8 00 FF 00 89 00 89 00 3A 0A C5 02 14 01 .....:.....
002D 10 00 01 00 00 00 00 00 20 45 50 45 47 45 .....EPEGE
003C 47 45 4A 45 44 45 46 43 41 43 41 43 41 43 41 GEJEDEFACACACA
  
```

Packet List Packets: 15 Selected: 1

No.	Delta Time	Source	Destination	Protocol	Size	Summary
1	0.000000	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE
2	0.002020	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE
3	0.193754	192.168.0.93:...	192.168.0.255:...	NBDGM	256	C: Transaction Na

Toolbar



Button	Description
Import	Colasoft Capsa supports import files in *.cscpkt, *.cpf, *.dmp, *.pkt and *.rawpkt format. The current packets will be cleared if you import a packet file.
Export	The packets listed in the Packet List and related information can be exported to a file in .cscpkt format.
Add	Creates a packet and it will be listed as the last packet in the Packet List. You can define the packet type from the five templates provided by Colasoft Capsa and the delta time.
Insert	Creates and Inserts a packet into the Packet List and it will be listed after the current packet. You can also define the packet type from the five templates provided by Colasoft Capsa and the delta time.
Copy	Copies the selected text or items in the three windows. In the Decode Editor, you can copy all involved items in a tree as a text file and puts it on the clipboard.
Paste	Pastes one or more packets in the Packet List window or paste some content in the Decode Packet window.
Delete	Deletes a packet in the Packet List or delete a period Hex/ASCII code in the Hex Editor .
Move Up	Clicks this button to move a packet once towards the first packet in the Packet List .
Move Down	Clicks this button to move a packet once towards the last packet in the Packet List .
Checksum	Clicks this button if you want Colasoft Packet Builder calculate the checksum automatically when you editor a packet decode.
Send	Sends selected packets to the wire.
Send All	Sends all packets in the packet list to the wire.
Adapter	Defines an adapter for sending packets to the wire.
About	Displays program information, version number and copyright.

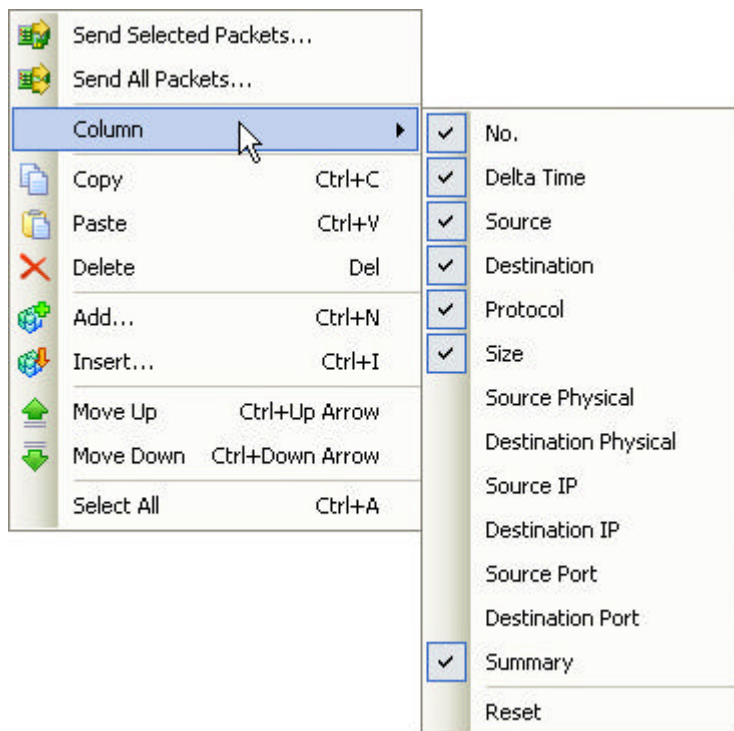
Packet list

This **Packet List** window displays packets and the relative information, allows users to edit the listed packet, such as copy, paste, delete, add, move up and so on.

Packet List							Packets	15	Selected	1
No.	Delta Time	Source	Destination	Protocol	Size	Summary				
1	0.000000	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE <1D>				
2	0.002020	192.168.0.20...	192.168.0.255:...	NBNS	96	C: NAME=OFFICE <1D>				
3	0.193754	192.168.0.93:...	192.168.0.255:...	NBDGM	256	C: Transaction Name ="...				
4	1.134533	192.168.0.28:...	219.133.49.72:...	QQ	82	C: Keep alive(393622003)				
5	0.336778	219.133.49.7...	192.168.0.28:4...	QQ	102	S: Keep alive				
6	3.905421	00:0D:88:47:...	FF:FF:FF:FF:FF...	ARP	64	Who is 192.168.0.62? T...				
7	0.304263	67.15.229.15...	192.168.0.28:1...	HTTPS	64	Seq=0833105606,Ack=...				
8	0.000420	192.168.0.28:...	67.15.229.157:...	HTTPS	58	Seq=0079580178,Ack=...				
9	1.598414	192.168.0.28:...	192.168.0.208:...	TCP	64	Seq=0628693960,Ack=...				
10	0.000026	192.168.0.28:...	192.168.0.208:...	TCP	64	Seq=0848293389,Ack=...				
11	0.000013	192.168.0.28:...	192.168.0.208:...	TCP	64	Seq=3222455537,Ack=...				
12	0.108485	192.168.0.20...	192.168.0.28:1...	TCP	64	Seq=1361267039,Ack=...				
13	0.000017	192.168.0.20...	192.168.0.28:1...	TCP	64	Seq=2602158200,Ack=...				

Right-clicks to open the context menu, you will see the available commands in this window. Users can define the display column


and edit packets.



Import packets

Colasoft Packet Builder supports *.cscpkt (Capsa 5.x and 6.x Packet File) and *.cpf (Capsa 4.0 Packet File) format, you may also import data from *.cap (Network Associates Sniffer packet files), *.pkt (EtherPeekv7/ TokenPeek / AiroPeekv9 / OmniPeekv9 packet files), *.dmp (TCP DUMP) and *.rawpkt (raw packet files).

There are two ways to import packets into Packet Builder:

- Click the import  button in the toolbar or the **Import...** command from the **File** menu.
- In addition, users can transmit captured packets from Colasoft Capsa application by right-click and choose the **Send to Packet Builder** command in the context menu of the **Packets** view.

Export packets


Users can export packets and relative information to a file in .cscpkt format.

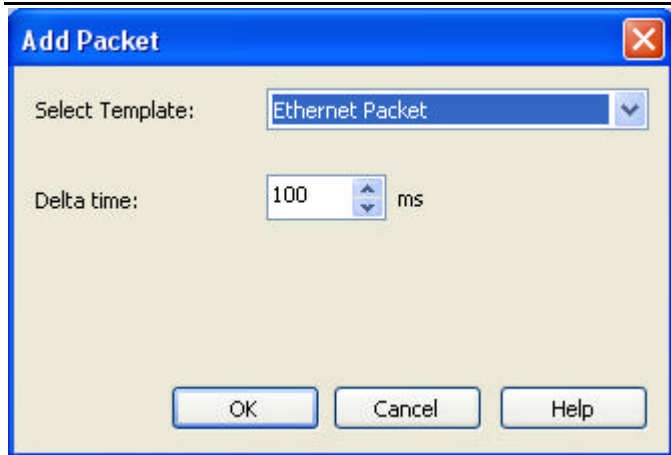
Editing packet

All listed packets and their decode information are editable. Users can create a most popular packet according to the template provided by Colasoft Packet Builder conveniently.

Create packet

There are two ways to create a packet - Add and Insert. The difference between these two ways is the new added packet's position in the **Packet List**. The new packet will be listed as the last packet in the list if add a packet, while the insert means the new packet will be listed after the current packet.

Click the add/insert  button to open an **Add Packet** dialog.



- **Select Template**

To create a packet, you need to specify the packet type by selecting the name from the **Select Template** combo box first. The templates contain several kinds of common-used packet - **Ethernet Packet**, **ARP Packet**, **IP Packet**, **TCP Packet** and **UDP Packet**.

- **Delta Time**


Then defines the delta time for the new packet. Delta time means the length of time between the new packet and the last packet in the **Packet List**, 100 millisecond in default. If you are inserting a packet, the delta time means the length of time between the current packet.

Notes: If there are no packets in the **Packet List**, this feature will not be enabled.

Editor packet

In addition to create packets, Colasoft Packet Builder allows users to edit the decoding information in the two editors - **Decode Editor** and **Hex Editor**. The feature of editing decoding information of packet is unique to Colasoft Packet Builder, as it is not supported by others packet builder program.

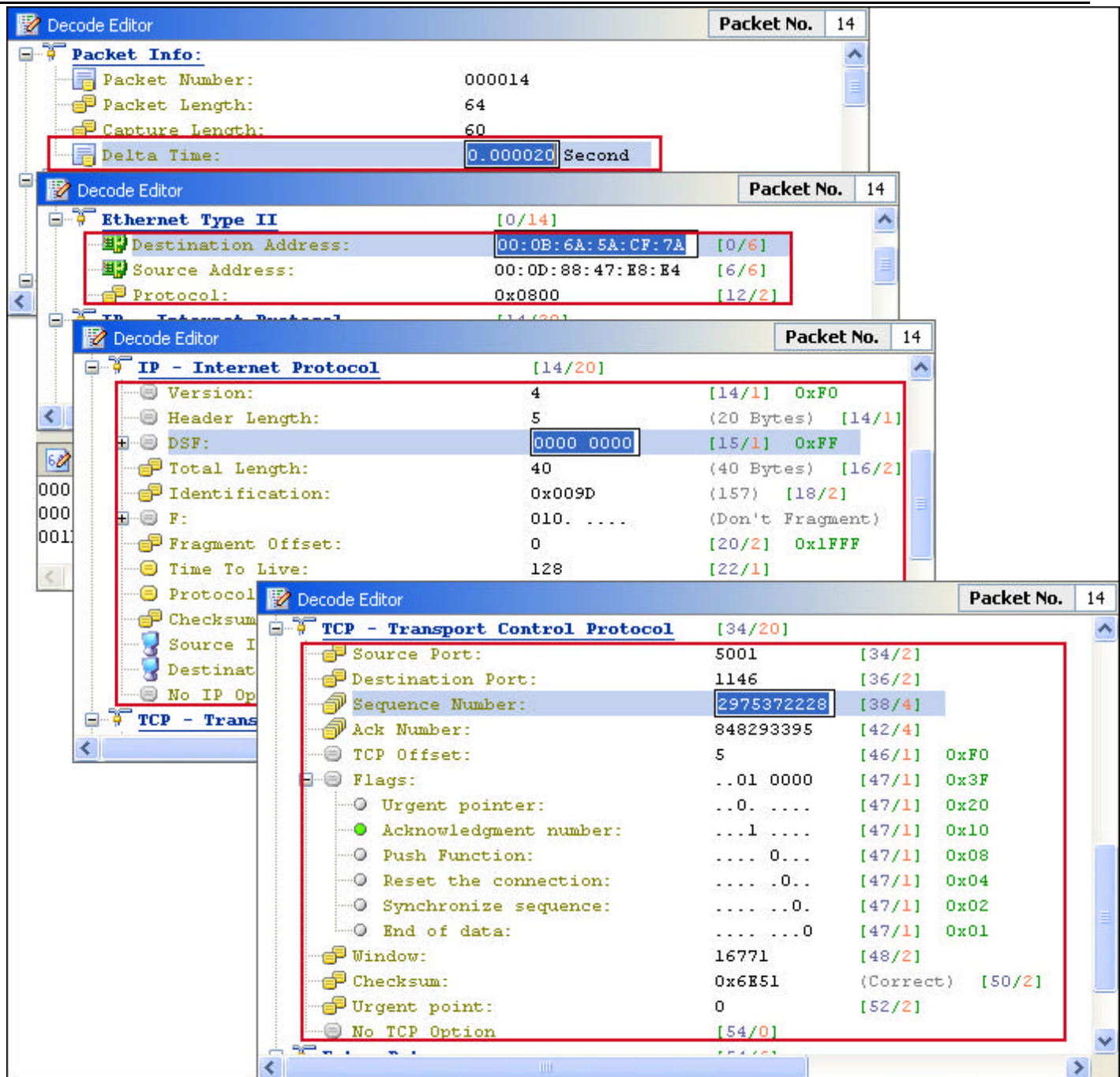
- **Decode Editor window**

Users can edit the packet decoding information by double clicks the decoding item. The corresponding information in the **Hex Editor** window and **Packet List** window will change with the modification of the decoding. Check the Checksum  button in the toolbar if you want system calculates the packet's checksum automatically.

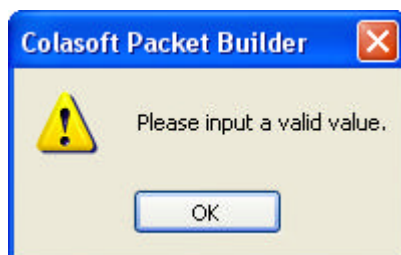
Except the Delta time, Colasoft Capsa provides the changeable decoding groups are different in every kind of packet.

Packet type	Applicability
ARP Packet	Ethernet Type II, Address Resolution Protocol
IP Packet	Ethernet Type II, Internet Protocol
TCP Packet	Ethernet Type II, Internet Protocol, Transport Control Protocol
UDP Packet	Ethernet Type II, Internet Protocol, User Datagram Protocol

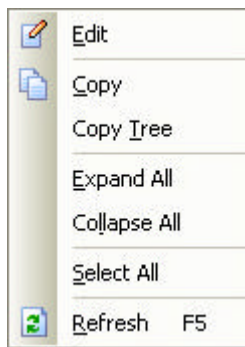
For a TCP packet, the decoding information grouped in the **Ethernet Type II**, **IP - Internet Protocol** and **TCP - Transport Control Protocol** are all changeable.



Notes: Colasoft Capsa will validate the entries in the editor. It will popup a window to inform you if the entry is incorrect and undo the modification. You may save the incorrect entry with the click the **Esc** key if you confirm the entries, though.



In addition, users can execute other operations, such as copy all involved items in a tree, expand/collapse content and so on, by right-click and choose the command from the context menu.




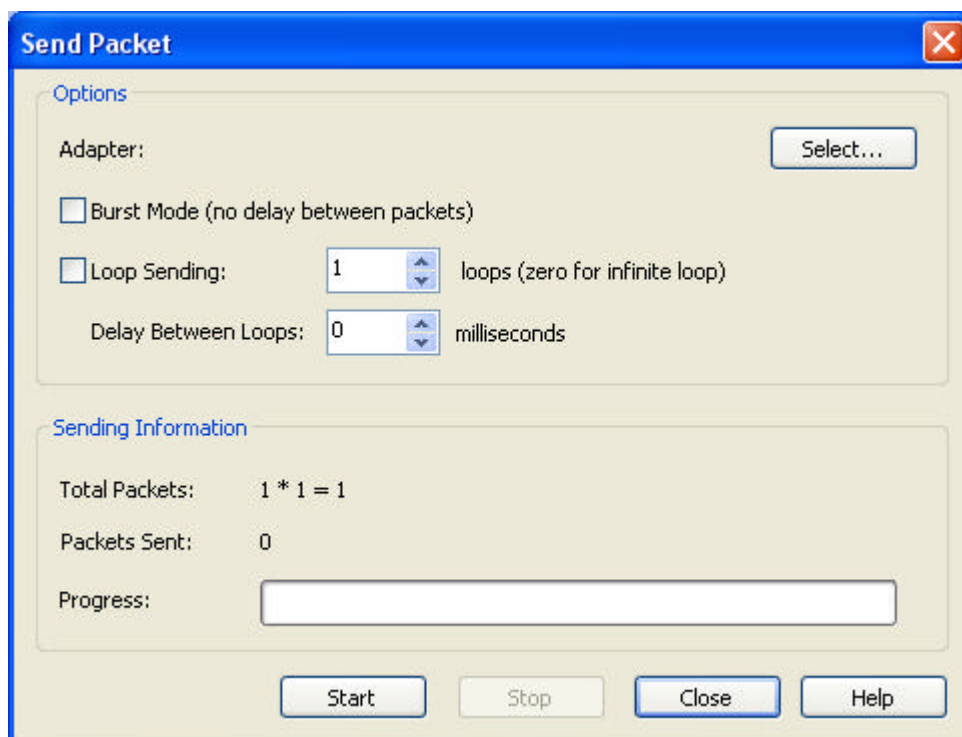
- **Hex Editor window**

The Hex editor displays the actual packet contents in raw hexadecimal on the left and its ASCII equivalent on the right. For your convenience, both the Hex and ASCII are changeable. The Hex used for modifying the hexadecimal code while the ASCII used for changing the packet text.

Sending packet

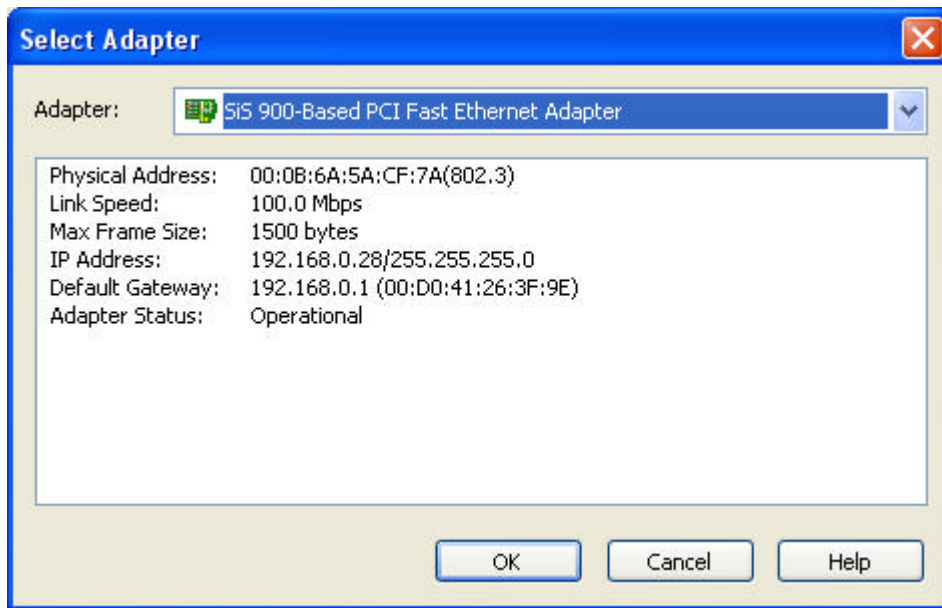
In addition to build packet, Colasoft Packet Builder supports sending packet too. This feature allows users to define many parameters than the Send Packet feature in the **Packets** view, such as define the interval between every packet and the delay between loops.

Click the send  button to open the **Send Packet** dialog.



- **Adapter**

Users can define a adapter for sending packet from if there are more than one adapters in the PC. Clicks the "Select" button on the right of "Adapter:" to open the **Select Adapter** dialog, chooses an adapter from the combo box. The window under the combo box will display the detailed information of the selected adapter.



- ♦ **Bust Mode**

Check this option, Colasoft Packet Builder will send packets one after another without intermission. If you want to send packet as the original delta time, please do not check this option.

- ♦ **Loop Sending**

Defines the repeated times of the sending execution, one time in default. Please enter zero if you want to keep sending packets until pause or stop it manually.

- ♦ **Delay Between Loops**

Appoints the interval between every loop if you defined the loop times more than one. Colasoft Packet Builder will send without interval between every loop in default.

- ♦ **Total Packets**

Displays the number of sending packets. For example, **4*5** means four packets are selected and each one will be sent five times. So Colasoft Packet Builder totally sent out **20** packets.

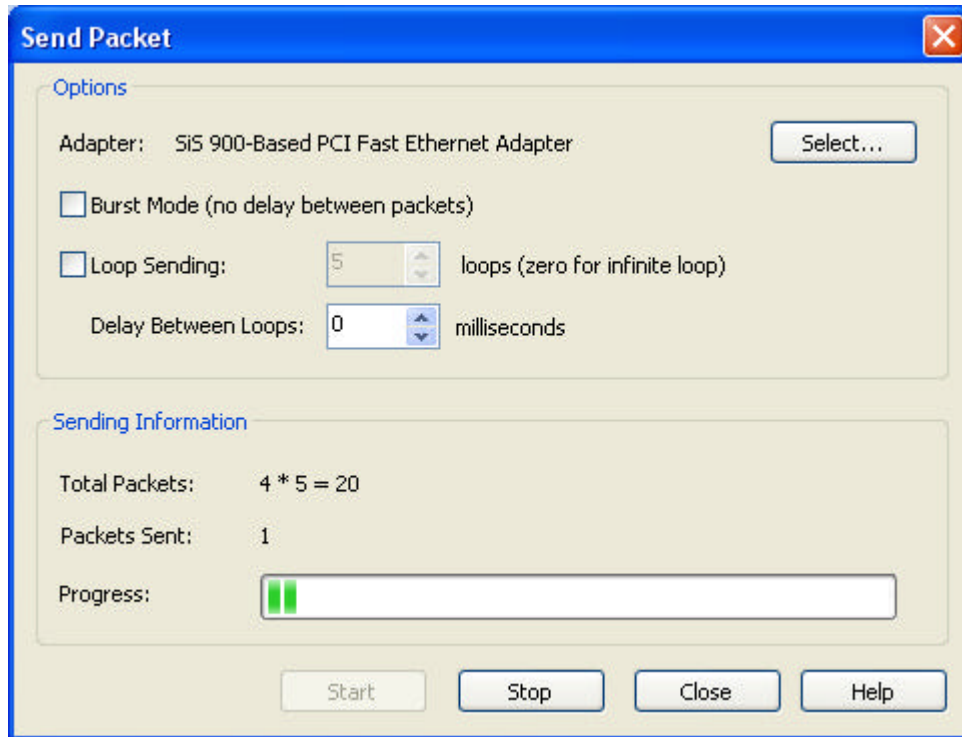
- ♦ **Packets Sent**

Shows the number of packets have been sent successfully. Colasoft Packet Builder will display the the packets sent unsuccessfully too if there is a packet did not sent out.

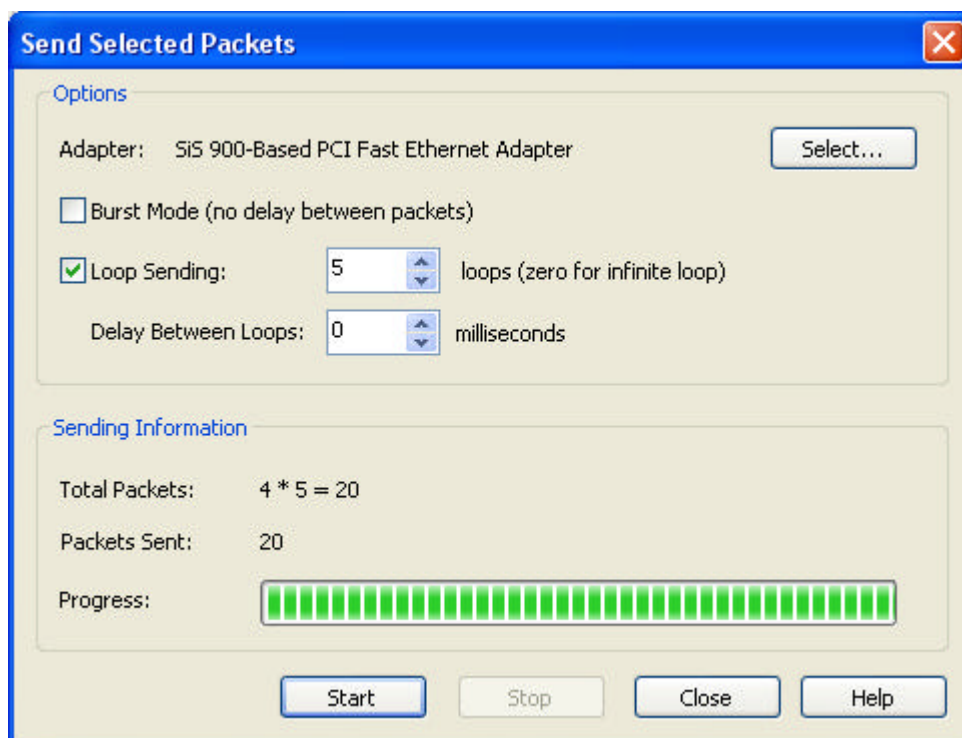
- ♦ **Process**

The process bar simply presents an overview of the sending process you are engaged in at the moment.

The **Stop** button will enable after start sending, let you can pause/stop the execution. You can modify the parameters after click the **Stop** button and then continue to send packets as the new settings.



After sending packets complete, the **Start** button will be enabled while the **Stop** button will be disabled.



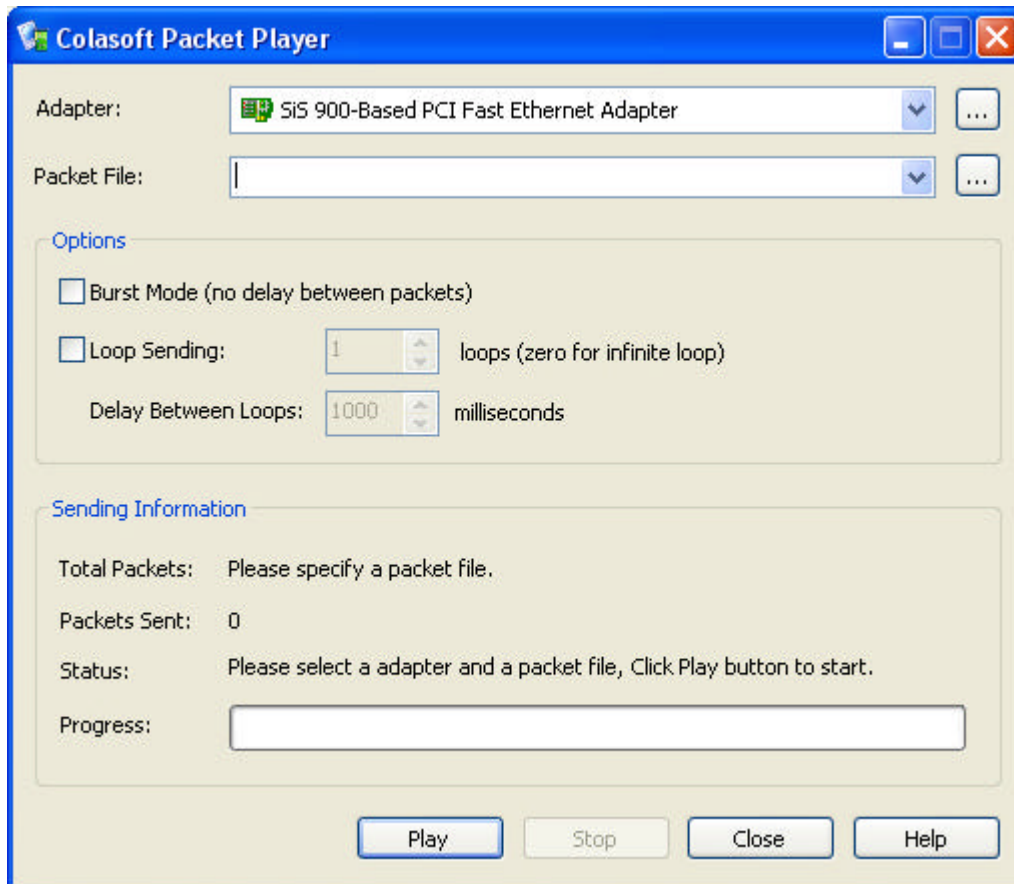
Colasoft packet player

Colasoft Packet Player is a replayer tool which allows you to replay packet files in .cscpkt.

There are three ways to invoke Colasoft Packet Player:

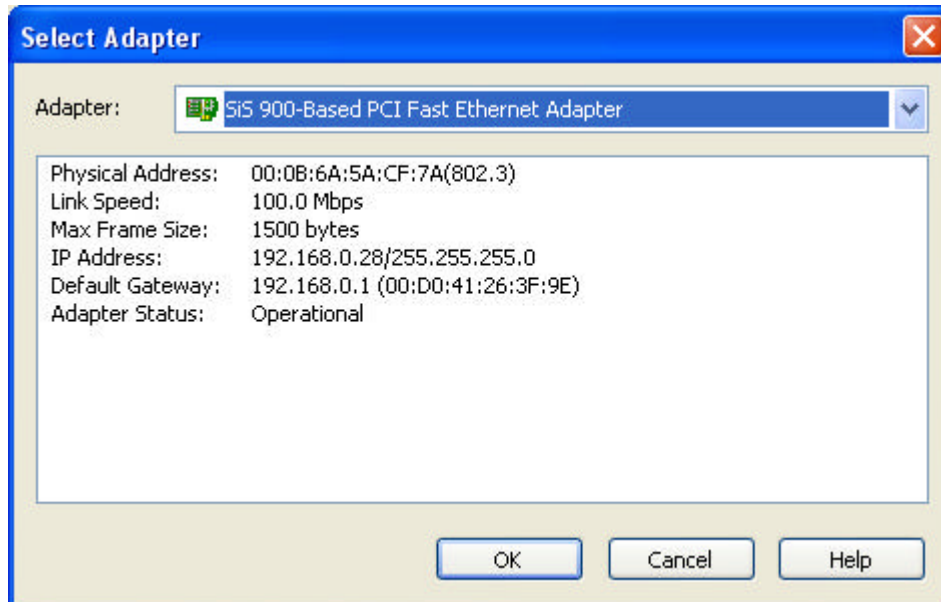
- Click the **Colasoft Packet Player** command in the **Tools** menu.

- Open the **Start** button of Windows and choose **All Programs**. Click the **Colasoft Packet Player** from the Colasoft Capsa application.
- Choose the **Run...** command from the **Start** button of Windows, input **PktPlayer.exe** command and click the **Enter** key.




- **Adapter**

Users can define a adapter for sending packet from if there are more than one adapters in the PC. Clicks the "Select" button on the right of "Adapter:" to open the **Select Adapter** dialog, chooses an adapter from the combo box. The window under the combo box will display the detailed information of the selected adapter.



- **Packet File**

Defines the packet file you want to send. Packet player supports Colasoft Capsa Packet File (.cscpkt) and Raw Packet File (.rawpkt) formats now, you can select a packet file by clicking the  button. Users also can replay a packet file have been sent out before from the combo box.

- **Bust Mode**

Checks this option, Colasoft Packet Builder will send packets one after another without intermission. If you want to send packet as the original delta time, please do not check this option.

- **Loop Sending**

Defines the repeated times of the sending execution, one time in default. Please enter zero if you want to keep sending packets until pause or stop it manually.

- **Delay Between Loops**

Appoints the interval between every loop if you defined the loop times more than one. Colasoft Packet Builder will send without interval between every loop in default.

- **Total Packets**

Displays the number of sending packets.

- **Packets Sent**

Shows the number of packets have been sent successfully. Colasoft Packet Builder will display the the packets sent unsuccessfully too if there is a packet did not sent out.

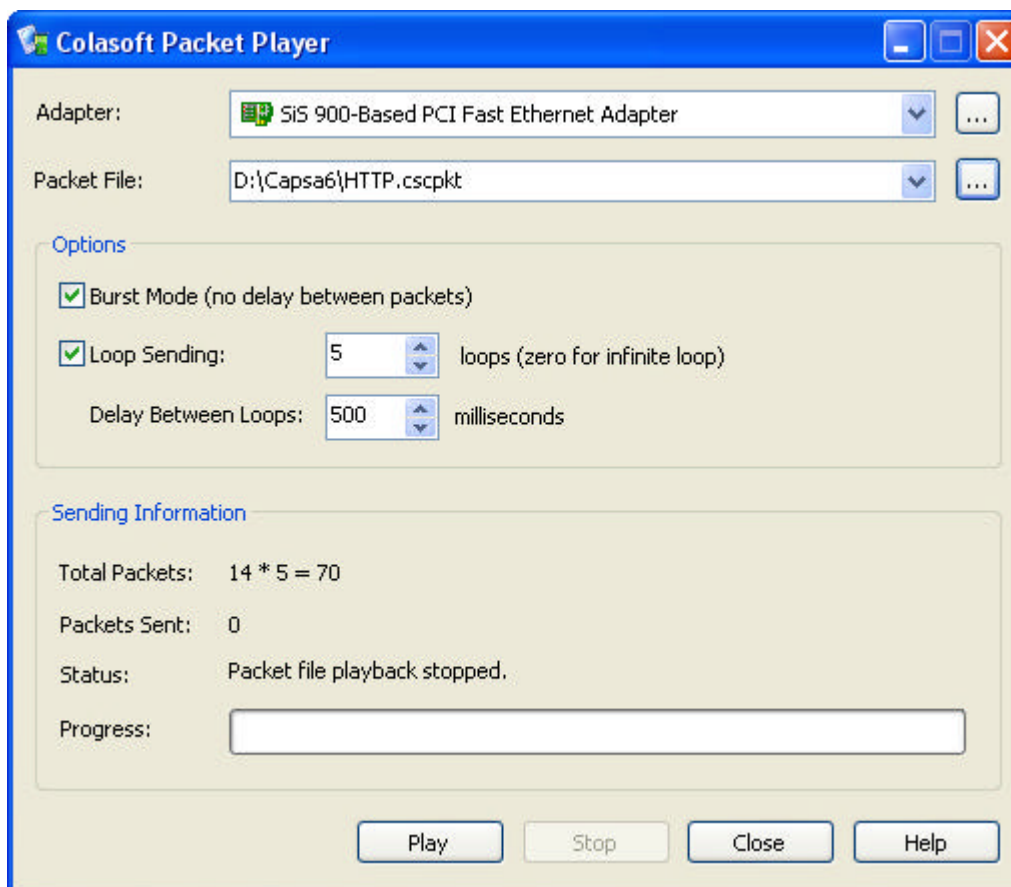
- **Progress**

The process bar simply presents an overview of the sending process you are engaged in at the moment .

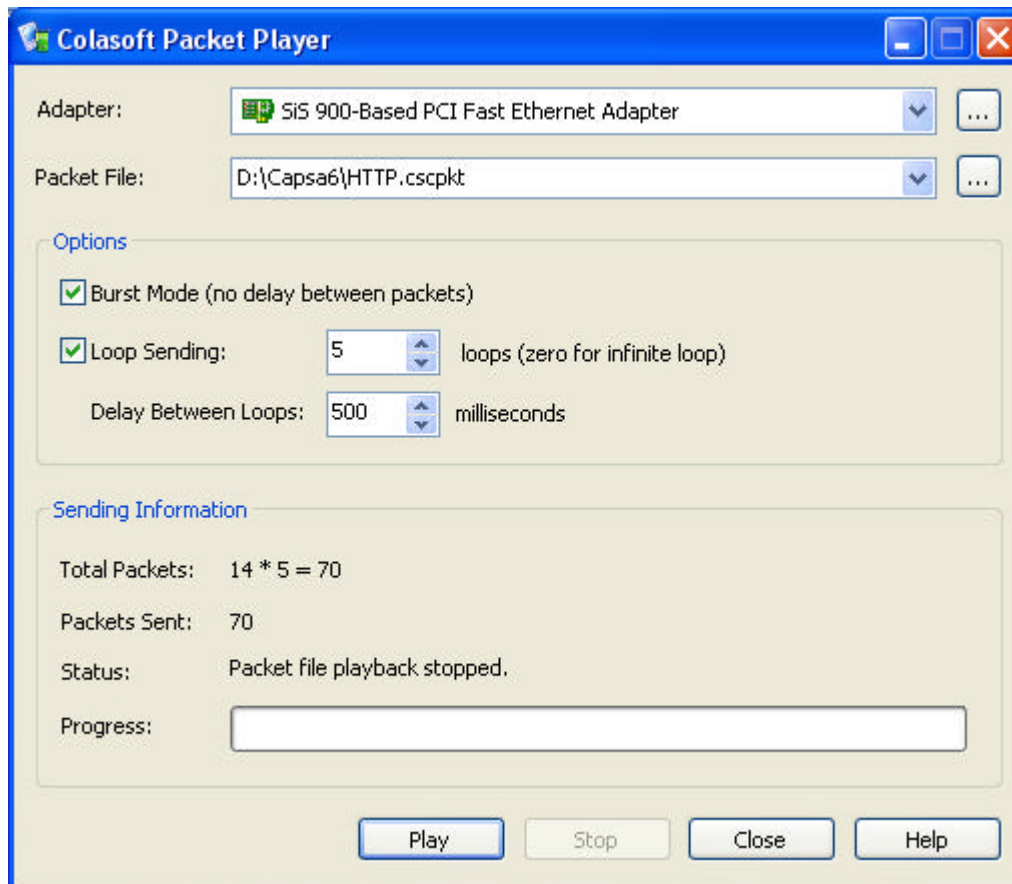
Replay packet

Sets the parameters as the below figure. It means the *HTTP.cscpkt* packet file will be replayed five times from the *SiS 900-Based PCI Fast Ethernet Adapter*, five hundred milliseconds delay between every loop, and the packets will be replayed without delay in

one loop . The Total Packets: $14 * 5 = 70$ means that there are fourteen packets in the selected packet file, every packet will be replayed five times and seventy packets will be replayed totally.



Then, click the **Play** button to start replay. After the replay is complete, the Packets Sent will change into **70** (see the below figure).

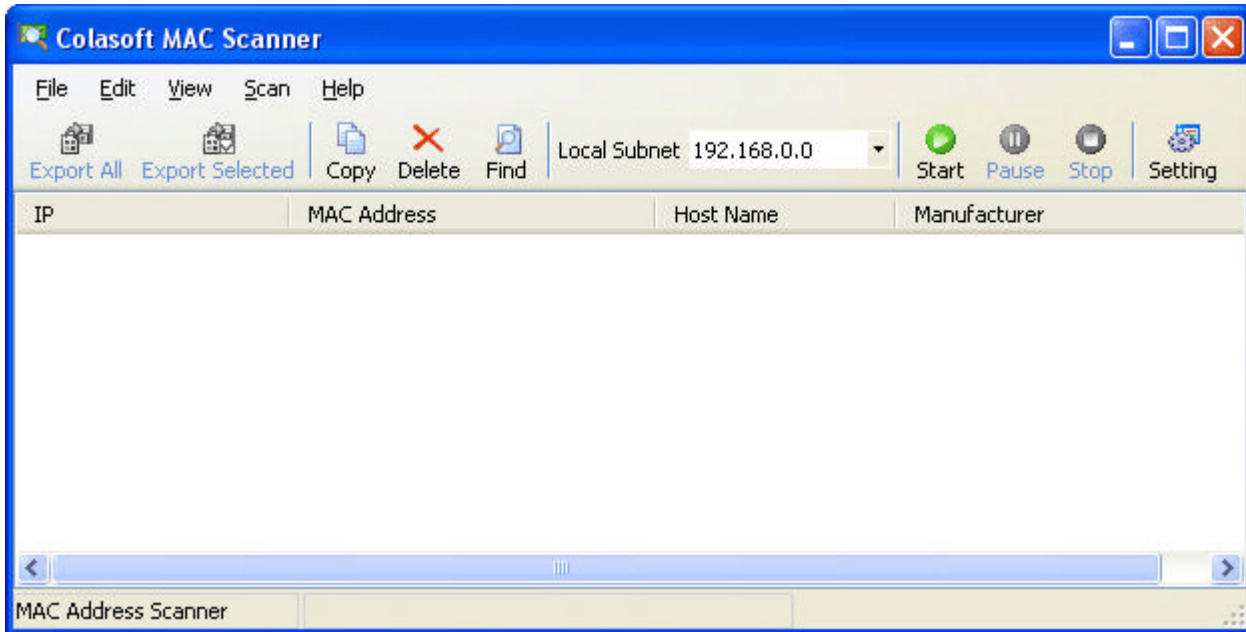


Colasoft MAC scanner

Colasoft MAC Scanner is a scan tool using to scan IP address and Mac address. It can automatically detect the all subnets of the NICs installed on the machine and scan the MAC addresses and IP addresses of defined subnets as your need.

There are three ways to invoke Colasoft MAC Address Scanner:

- Click the **Colasoft MAC Scanner** command in the **Tools** menu.
- Open the **Start** button of Windows and choose **All Programs**. Click the **Colasoft MAC Scanner** from the Colasoft Capsa application.
- Choose the **Run...** command from the **Start** button of Windows, input **Cmac.exe** command and click the **Enter** key.

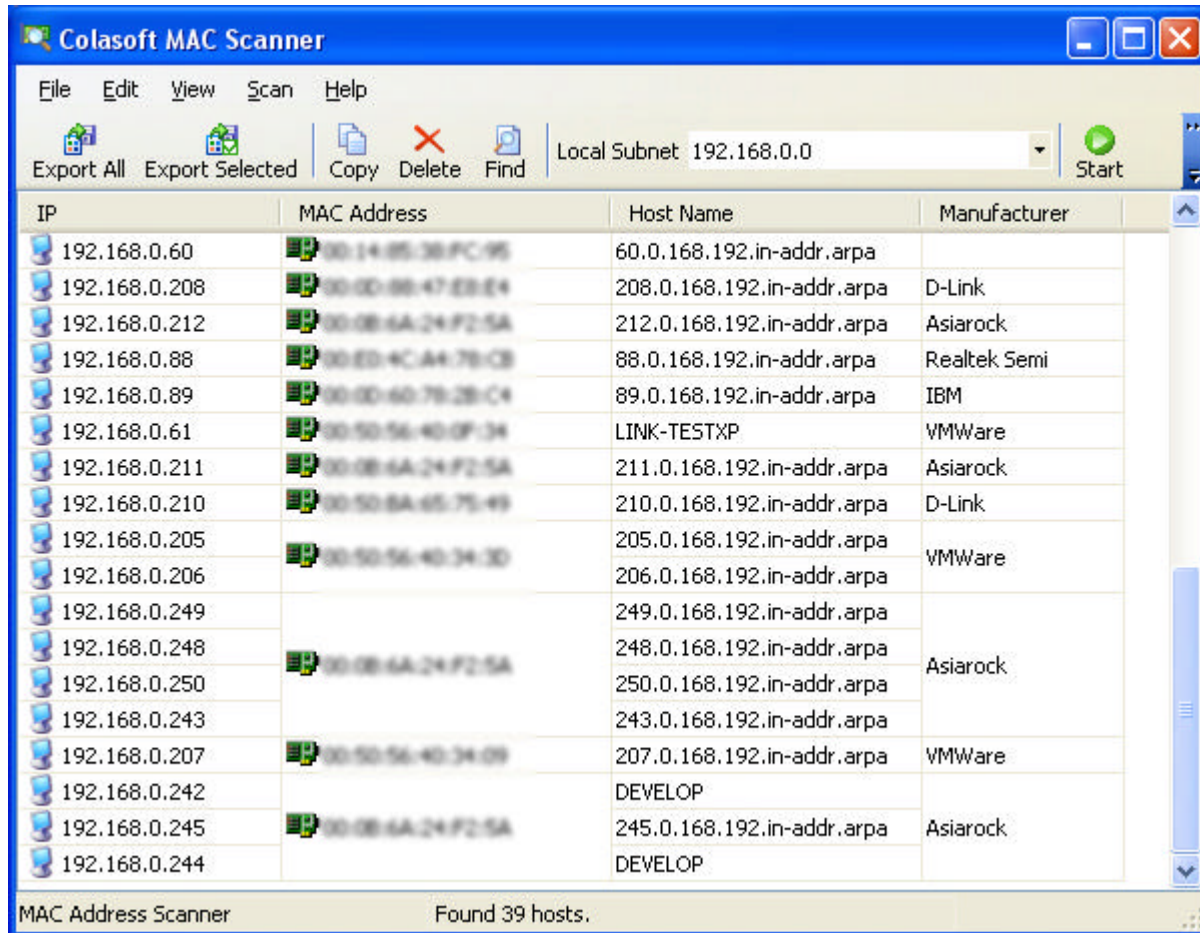


In the toolbar, there are some quick buttons that let you customize the type of graph.

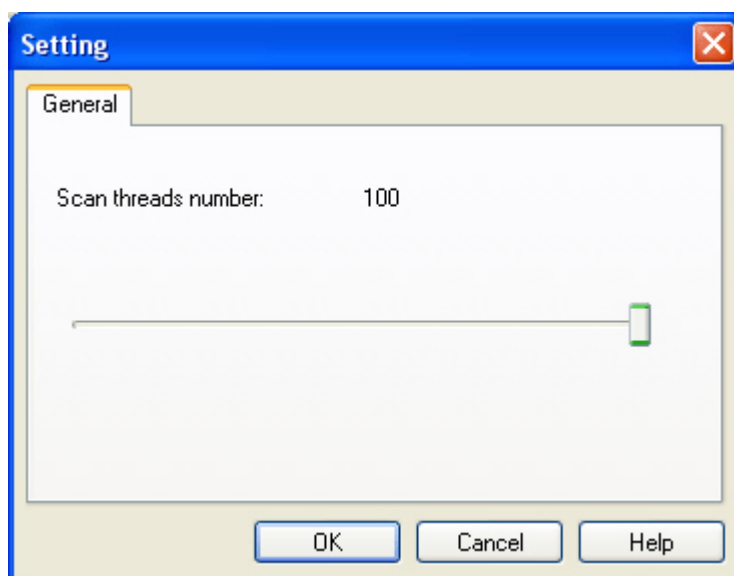
Button	Description
Export All	Exports the whole scan results to a *.txt and *.csv file.
Export Selected	Exports the selected item(s) of the scan results to a *.txt and *.csv file.
Copy	Copies the selected item(s) and puts it on the clipboard.
Delete	Deletes the selected IP addresses from the results list.
Find	Finds a specific item in the scan results.
Start	Start to scan a network.
Pause	Pause the scan operation for a while.
Stop	Stop the scan operation.
Settings	Defines the subsequent threads.

Scan network

Choose a subnet from the **Local Subnet** combo box and click the **Start** button or **F5** to execute scan. Colasoft Capsa will display the scanned results, including **IP address**, **MAC address**, **Host Name** and **Manufacturer** in the list. It will group all IP addresses according to MAC address if a MAC address configured multiple IP addresses. The scanned results can be exported into .txt file for future reference.



Users can custom own scan process by clicking the **Setting** button to open the **Setting** dialog.



You can custom the subsequent threads, range from 1 to 100. It will take more time to finish the scan operation if the subsequent thread is more less.

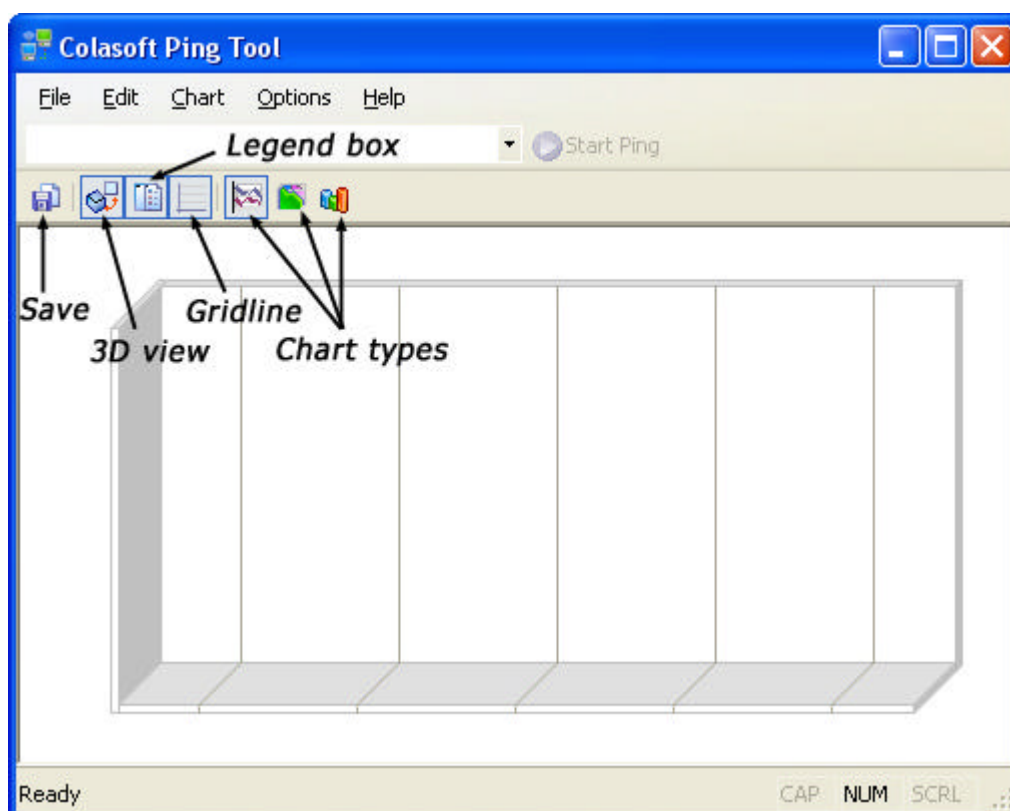
- **1** - Colasoft MAC Scanner will scan all address one after another.
- **10** - Colasoft MAC Scanner will generate 10 threads.

Colasoft ping tool

Colasoft Ping Tool is a handy ping utility for users.

There are four ways to invoke Colasoft Ping Tool:

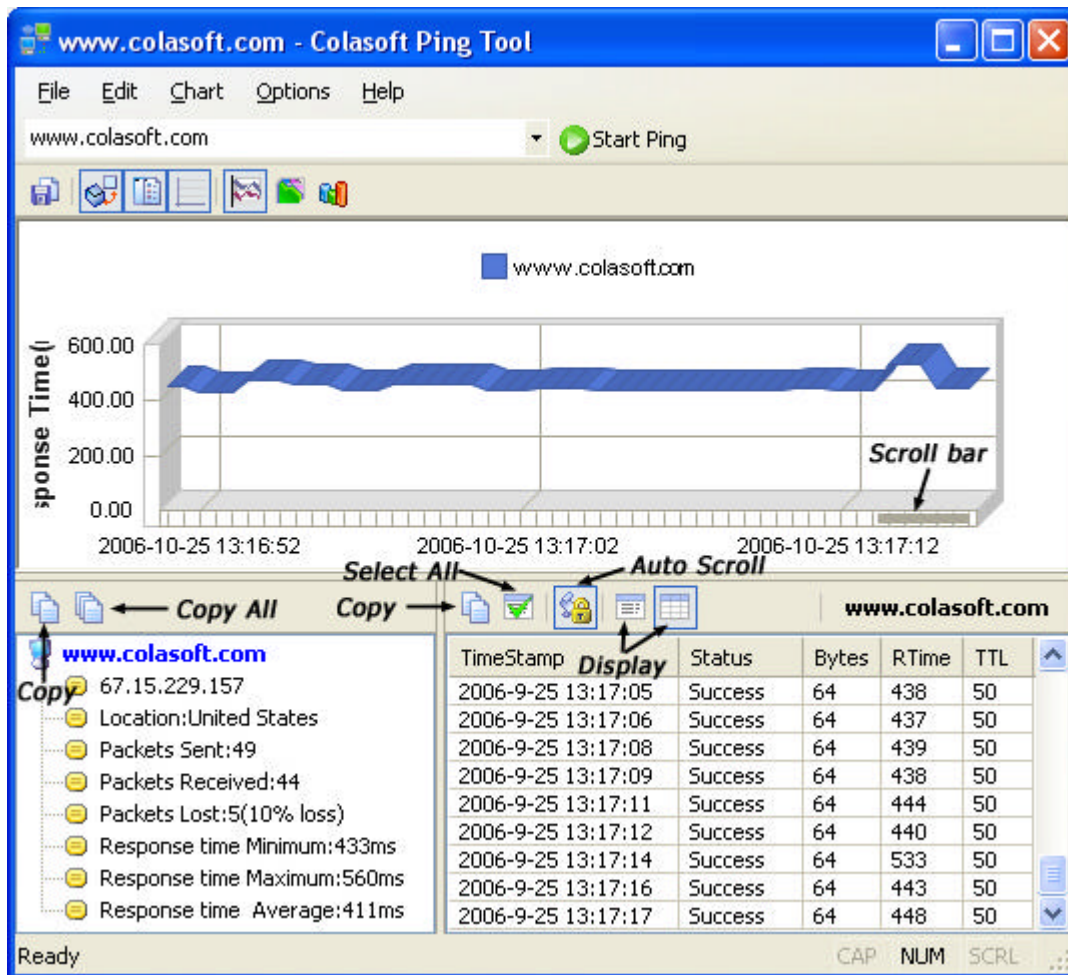
- Click the **Colasoft Ping Tool** command in the **Tools** menu.
- Select a packet in the **Packets** view or a node in the **Project Explorer**, right-click and choose the **Ping** command from the context menu (if applicable).
- Open the **Start** button of Windows and choose **All Programs**. Click the **Colasoft Ping Tool** from the Colasoft Capsa application.
- Choose the **Run...** command from the **Start** button of Windows, input **Cping.exe** command and click the **Enter** key.



In the toolbar, there are some quick buttons that let you customize the type of graph.

Button	Description
Save	Saves the graph to a *.bmp file.
3D view	Shows the graph in three-dimensional view.
Legend box	Shows or hides the explanation of the colors appearing on the graph.
Gridline	Shows or hides the gridlines on the graph.
Chart types	The chart types which are available for the current node and the selected graph title.

Enter an IP address and click the Start  button, stop the execution after a while.



There are three windows in the interface.

- **Graphic window**

The upper window reveals every ping command in graphic way, used for viewing the secular trend in Ping time. The X axes indicates the Ping real time, the Y axes reveals the Ping response time in ms. Moves the scroll bar in the graph to view historical graph.

- **Ping - Summary**

The Ping - Summary window lists all required IP addresses or domain names with its summary, such as IP address, location, packets Sent/received/lost and response time.

- **Ping - Details**

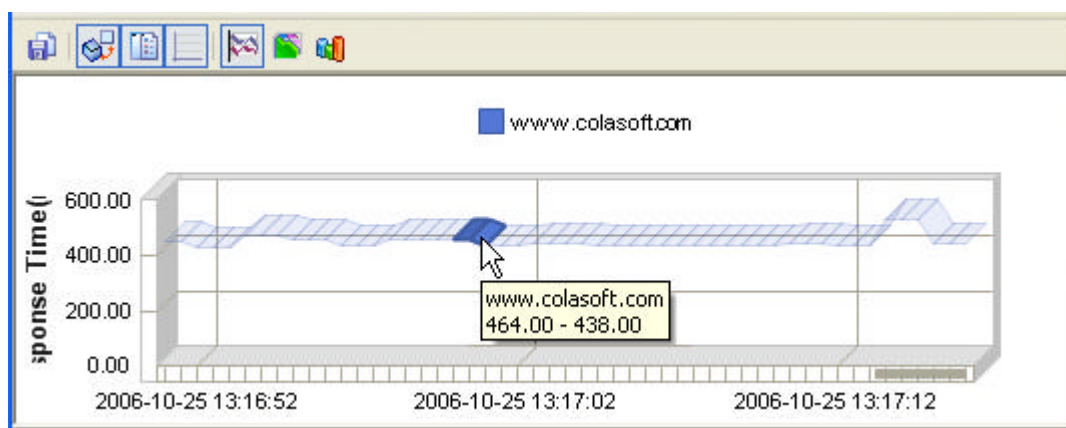
The Ping - Details window displays the details information of ping execution. When you select an IP address or a domain in the Ping - Summary window, the Ping - Details window will display the corresponding results. There are two kinds of display type classical and list. The classical view is same to the output of windows ping. While, the list view used the display format of Colasoft own, such as TimeStamp (in second), Status, Bytes, ResponseTime (in millisecond) and TTL. ResponseTime is the real time of local host receives the destination response.

The buttons in the Ping - Summary and Ping - Details window:

Button	Description
Copy	Copies the selected domain's summary information and puts it on the clipboard.

Copy All	Copies the all domains' summary information and puts it on the clipboard, if ping more than one address.
Copy	Copies the selected item in the details window and puts it on the clipboard.
Select All	Select all items listed in the details window.
Auto Scroll	The details list will display the newest packet always if check this button.
Display	Shows the details in classical view, Windows display type, or list view.

For a clear view, please move your mouse cursor to the graph. Colasoft Ping tool will highlight the specific node and node border upon it. An annotation will automatically popup which contains the domain name and response time. The response time in the annotation will be a range of time when your mouse cursor puts on the grid, while it will be a time if your mouse cursor puts on the grid line.

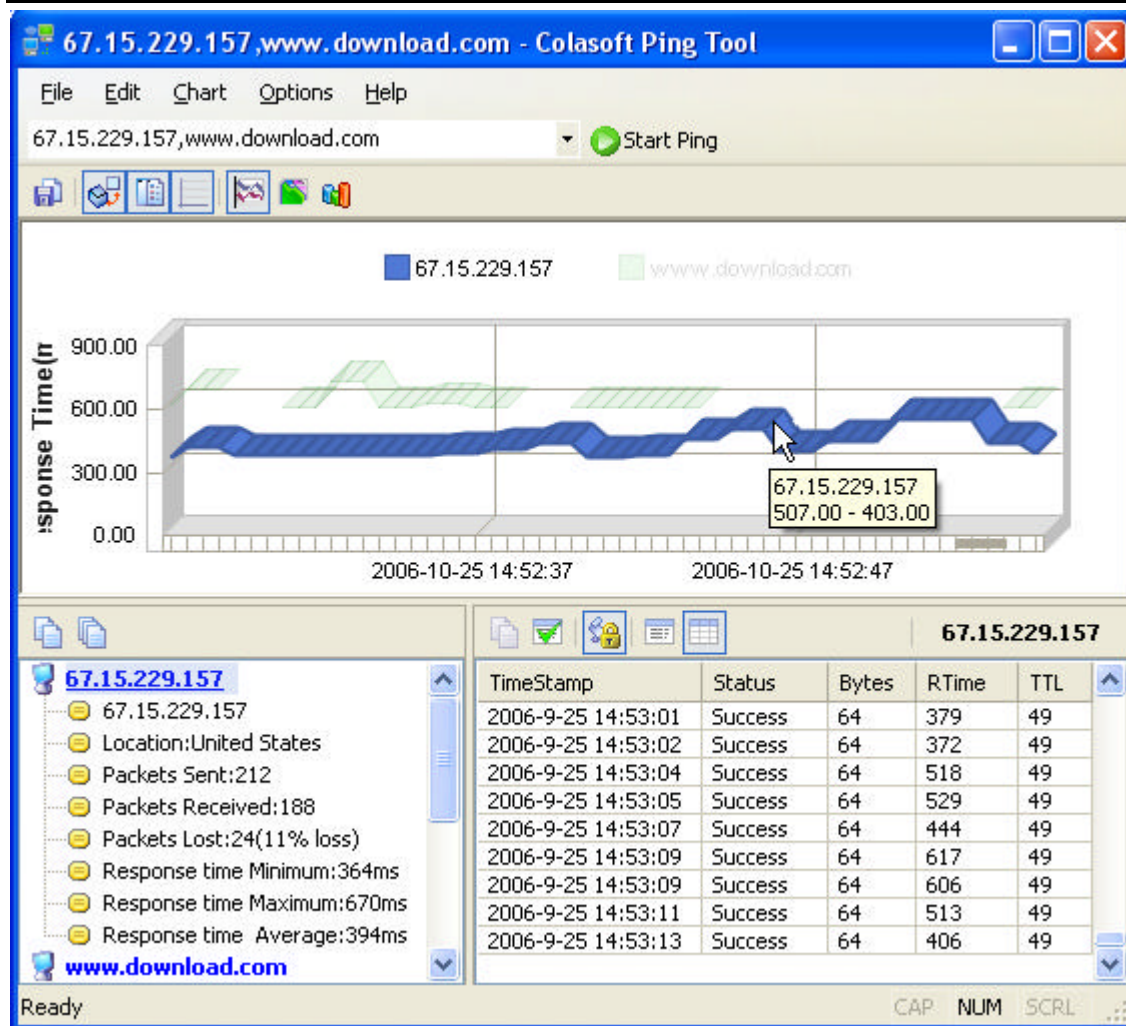


Ping multiple addresses/domains

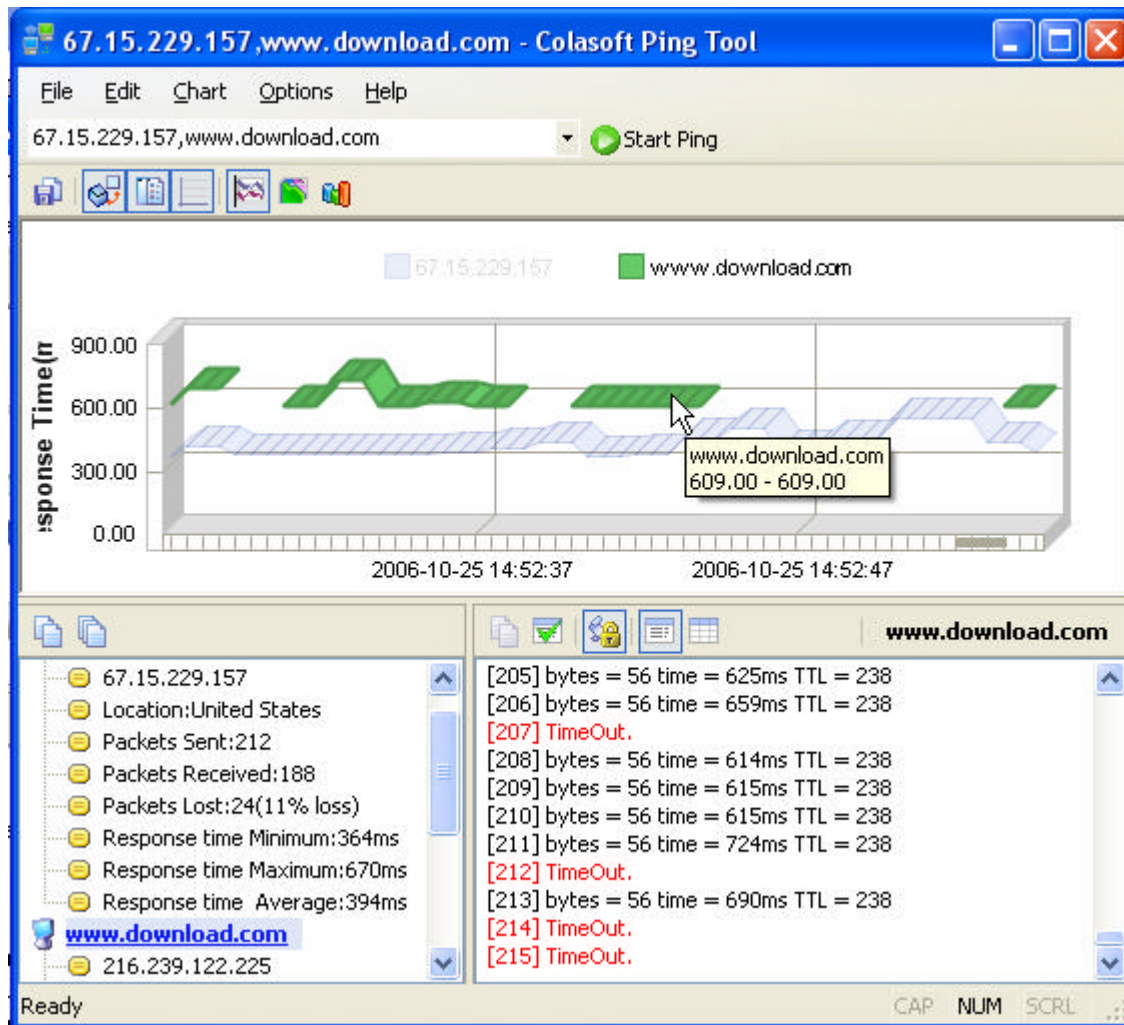
Colasoft Ping tool allows you to ping multiple IP addresses and domain names at one time without upper limit of the addresses' number. Enters IP addresses and domain name into the address pane, separate each other with a blank space, comma or

semicolon, then clicks the Start  Ping button to execute ping command.

For example, ping *67.15.299.157* and *www.download.com*. For a clear view of the graph of *67.15.299.157*, highlight the item of *67.15.229.157* with move your mouse cursor on it.



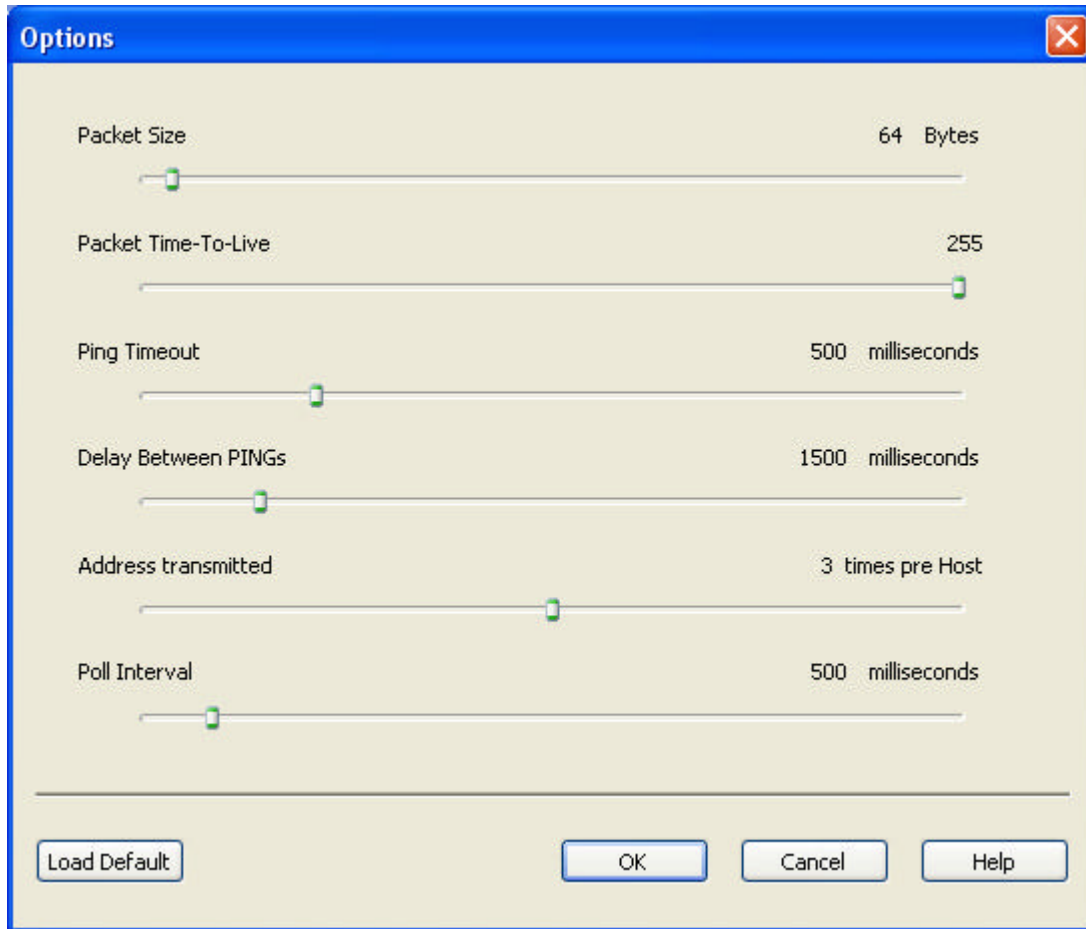
To view the details of www.download.com, select the domain name in the Ping - Summary window and move mouse to its graph. The Ping - Details window will display the corresponding information.



Options

Users can custom own parameters of the Ping command. Click the **Options...** command in the **Options** menu to open the dialog and modify the listed parameters.

The below figure is the parameter settings in default.

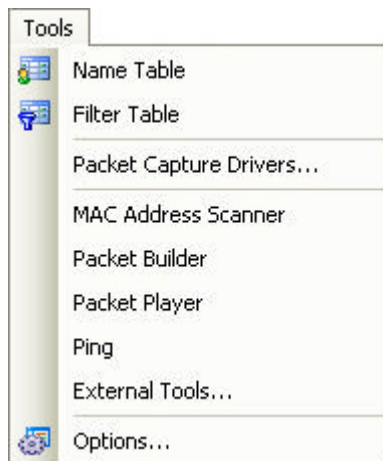


- **Packet Size**
Sets the size of ICMP packet when execute Ping command. The packet size range from 1 to 1024 bytes.
- **Packet Time-To-Live**
Indicates how many more hops this packet should be allowed to make before being discarded or returned, range from 1 to 255.
- **Ping Timeout**
The amount of time to allow for a response from the peer equipment, range from 100 to 2000 millisecond.
- **Delay Between PINGs**
The interval time between two pings, range from 100 to 10000 millisecond.
- **Address transmitted**
The amount of host or domain resolution, range from 1 to 5.
- **Poll Interval**
The refresh interval of graph, range from 100 to 5000.
- **Load Default**
Clicks this button to reset all parameters to default position.


External tools

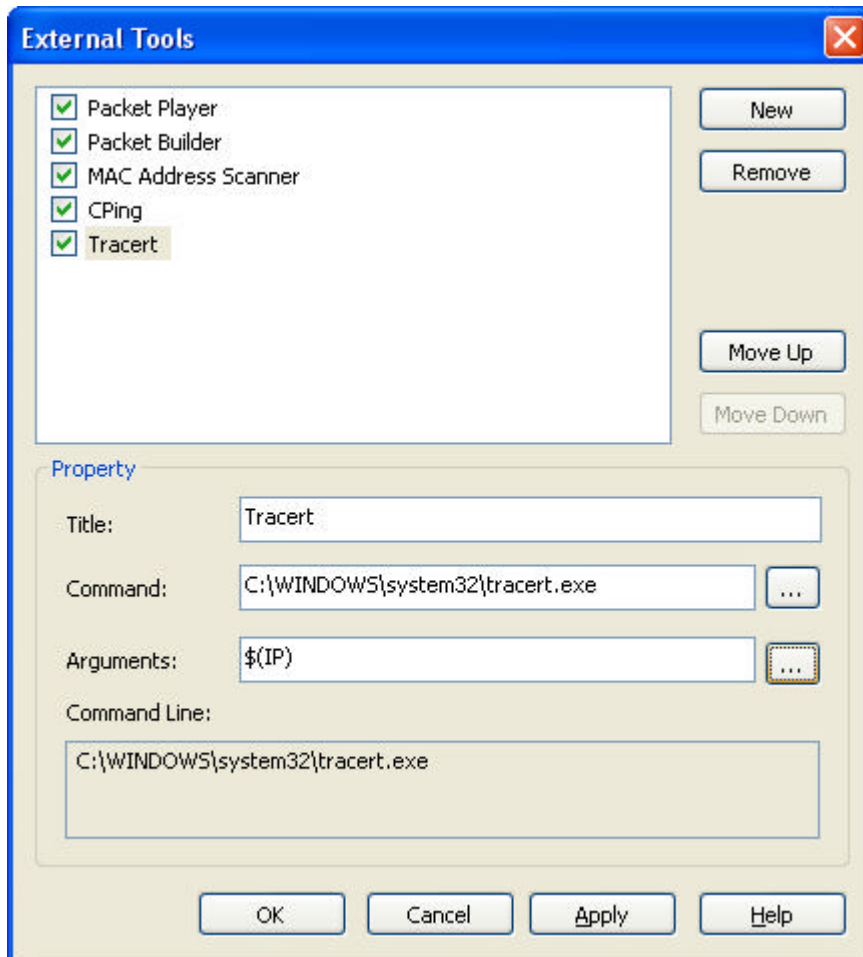
In addition to the four tools referred previous, users can customize to add other Windows applications and tools into Colasoft Capsa with the **External Tools**. You can not only invoke but also execute the added applications and tools via Colasoft Capsa.


The following figure is the tools menu in default.

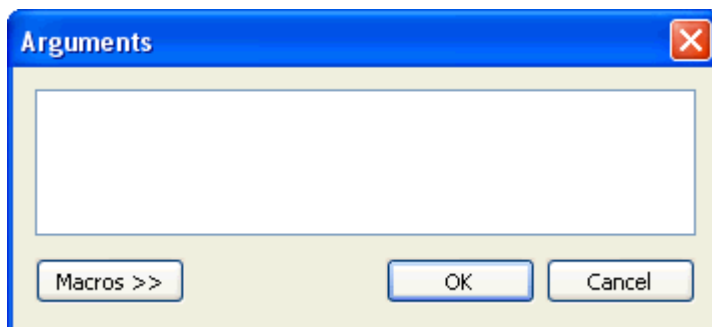


Click the **External tools...** command from the **Tools** menu to open the **External Tools** dialog page. The following is an example of how to add the **Tracert** command of Windows into Colasoft Capsa.

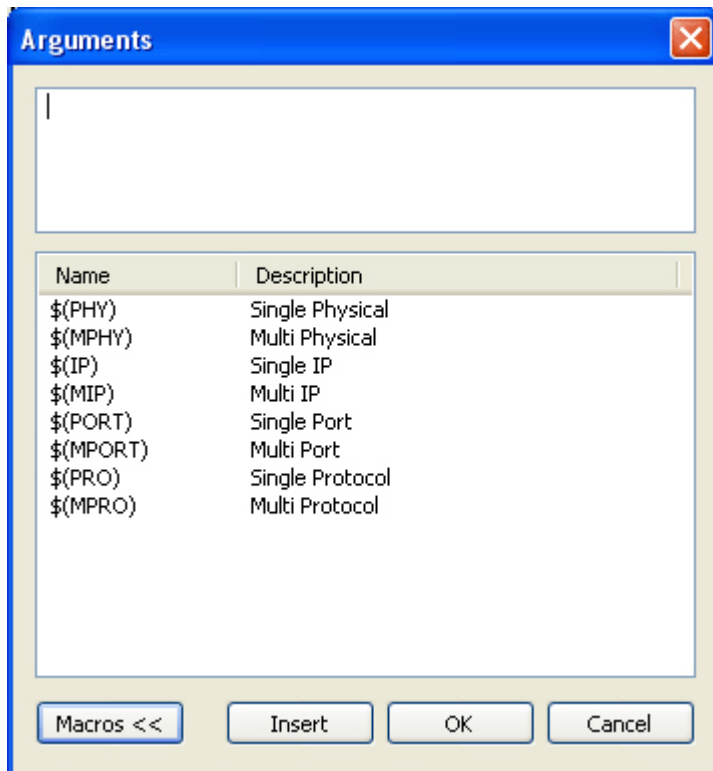
1. Click the **New...** button to enable the **Property** dialog box.
2. Name the tool as **Tracert**.
3. Enter the path of the program **C:\WINDOWS\system32\tracert.exe** or click the  button to choose the path.
4. Add the parameter **\$(IP)** into **Arguments**.



5. Click the  button to open the **Arguments** dialog.

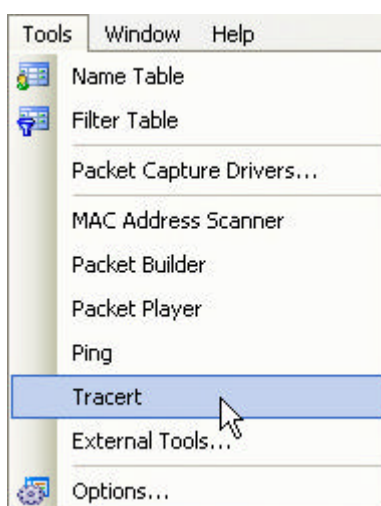


6. Click the **Macros >>** button to view the details.

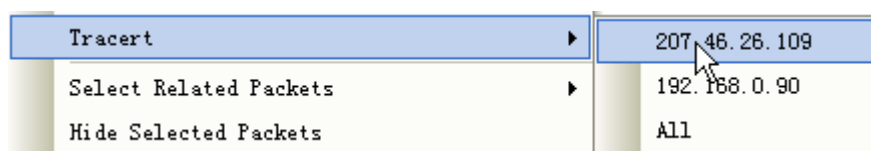


Colasoft Capsa lists the parameters **IP Address**, **Physical Address**, **Port** and **Protocol** in the window. You can add a parameter by selecting its name and clicking the **Insert** button. If the parameters did not listed, you can enter the parameters into the upper window manually, like as **-d**, **-h**, **-j** and **-w** in **Tracert** command. Every parameter should be separated with a blank space

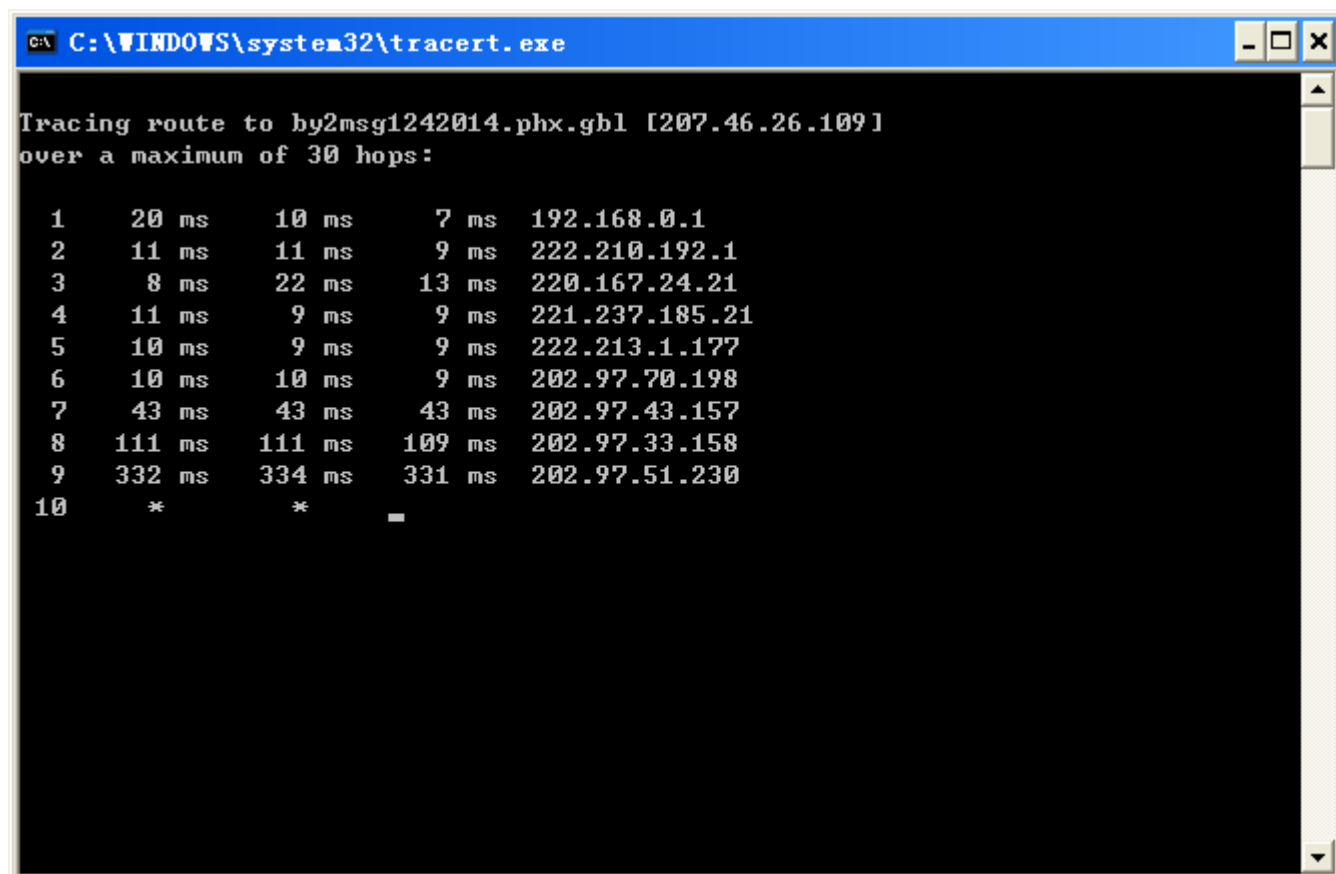
7. Choose the **IP Address** and click **Insert** button. Click the **OK** button to save the settings and back to the **External Tools** dialog.
8. Click the **Tracert** command in the **Tools** menu to execute the program.



In addition, you can execute to trace an IP with Colasoft Capsa conveniently. Select a packet in the Packets view and right click, choose the **Tracert** command. The source and destination IP address of the selected packet will be listed out, you can trace either one by its name or both by the **All** command.

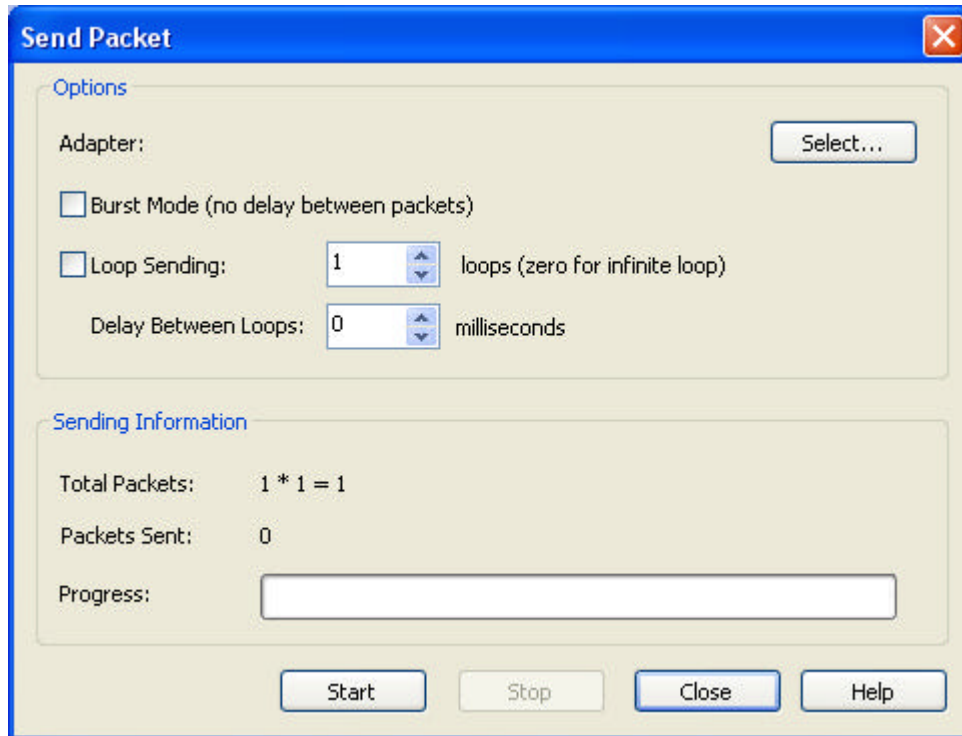


Now let's trace **207.46.26.109** by click its name. System will trace the this IP address and display the details of the execution in the popup window.



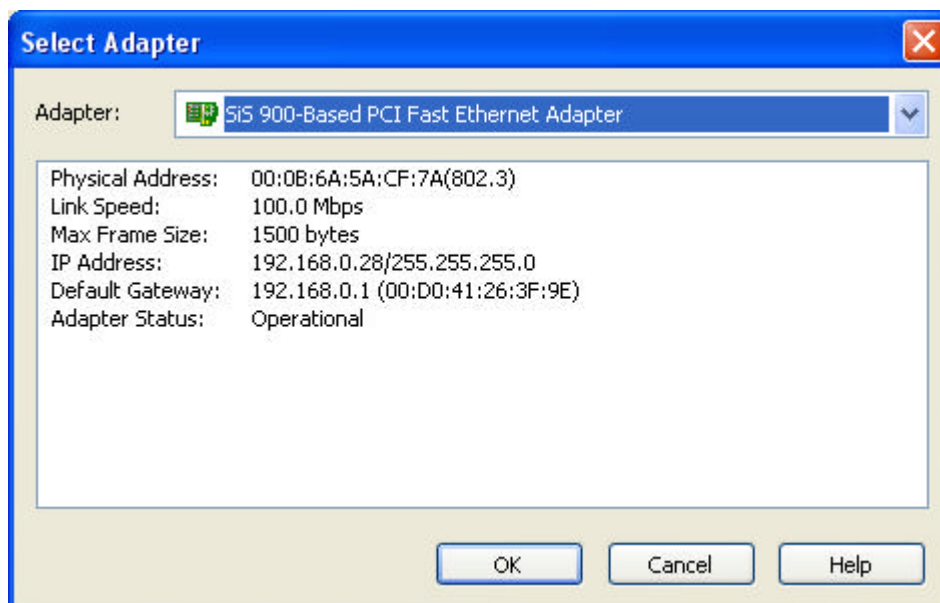
Send packet

Users can send the captured packets listed in the Packets view and Packets list sub-view of Conversations view. Select one or more packets and right click, choose the **Send Packet** command to open the **Send Packet** dialog.



- ◆ **Adapter**

Users can define a adapter for sending packet from if there are more than one adapters in the PC. Clicks the "Select" button on the right of "Adapter:" to open the **Select Adapter** dialog, chooses an adapter from the combo box. The window under the combo box will display the detailed information of the selected adapter.



- **Burst Mode**

Check this option, Colasoft Packet Builder will send packets one after another without intermission. If you want to send packet as the original delta time, please do not check this option.

- **Loop Sending**

Defines the repeated times of the sending execution, one time in default. Please enter zero if you want to keep sending packets until pause or stop it manually.

- **Delay Between Loops**

Appoints the interval between every loop if you defined the loop times more than one. Colasoft Packet Builder will send without interval between every loop in default.

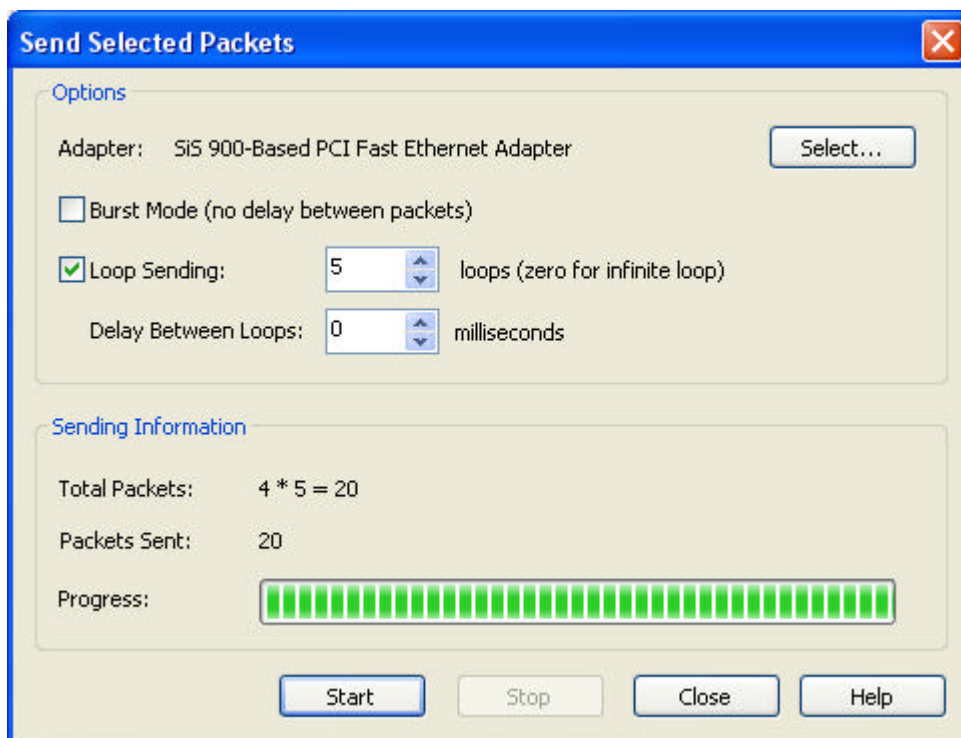
- **Total Packets**

Displays the number of sending packets. For example, **4*5** means four packets are selected and each one will be sent five times. So Colasoft Packet Builder totally sent out **20** packets.

- **Packets Sent**

Shows the number of packets have been sent successfully. Colasoft Packet Builder will display the the packets sent unsuccessfully too if there is a packet did not sent out.

A dialog will display the results of the execution. The sending parameters can be seen on the top on the dialog.



Customizing User Interface

Colasoft Capsa 's user interface is flexible and easy to use, sometimes you can change it's settings to get a clearer view. Basically the customizable sections or commands include the following:

Name	Description	Applicability
Toolbar*	Adds new toolbars or commands, shows or hides toolbar text ...	toolbar
Columns*	Shows or hides columns, changes the position of columns.	Summary view, Endpoints view, Protocols view, Packets list view, Conversations view, Logs view
Docked windows*	Shows or hides the project explorer bar...	Project Explorer , Project Status
Sorting*	Sorts the listed data on a specific condition.	Endpoints view, Protocols view, Conversations view
Highlight	Highlights the packet selected.	Packets list view
Packet Comment	Makes a comment for the current packet.	Packets list view
Show/Hide Packet List	Shows/hides the list of captured packets.	Packets view
Hide Selected/Unselected Packets	Filters the packets displayed.	Packets list view
Show/Hide Decode	Shows/hides the packet decode information.	Packets view
Show/Hide HEX	Shows/hides the HEX code of the current packet.	Packets view
Name Table	Makes an alias for the selected item.	Project Explorer docked window, Endpoints view, Packets list view, Conversations view, Matrix view, Logs view
Expand/Collapse All	Displays/undisplays all available data.	Project Explorer docked window, Summary view, Endpoints view, Protocols view, Matrix view, Packets decode view

The sections below give details about the items marked with *; for the explanation about those features not described in this chapter, please see the corresponding sections in this manual.

Toolbar

The toolbar includes some icons of frequently used commands, such as **New**, **Open**, **Save**, **Start**, and so on, you can customize the commands or options in the toolbar.

- **Hide toolbar**

Colasoft Capsa shows the standard toolbar by default. To hide the toolbar, open the **View** menu and put the mouse cursor on **Toolbar**, then uncheck **Standard**.

- **Hide toolbar text**

Colasoft Capsa shows the text under toolbar icons by default. To hide the toolbar text, open the **View** menu and put the mouse cursor on **Toolbar**, then uncheck **Icon Text**.

- **Customize toolbar**

Colasoft Capsa allows you to customize the toolbar commands, which is similar as the operation of Microsoft Office. You may open the **View** menu or right click on the toolbar, then select **Customize...** to modify the toolbar commands.

Columns

Colasoft Capsa displays captured data with corresponding column headings, you can select more columns to show more information, or alter the position of columns.

- **Show more columns**

Right click a column heading in a tab view (except the **Summary** and **Graph** view), select the **More...** command to open the **Select Column** dialog, check the columns to show or uncheck to hide.

- **Column display options**

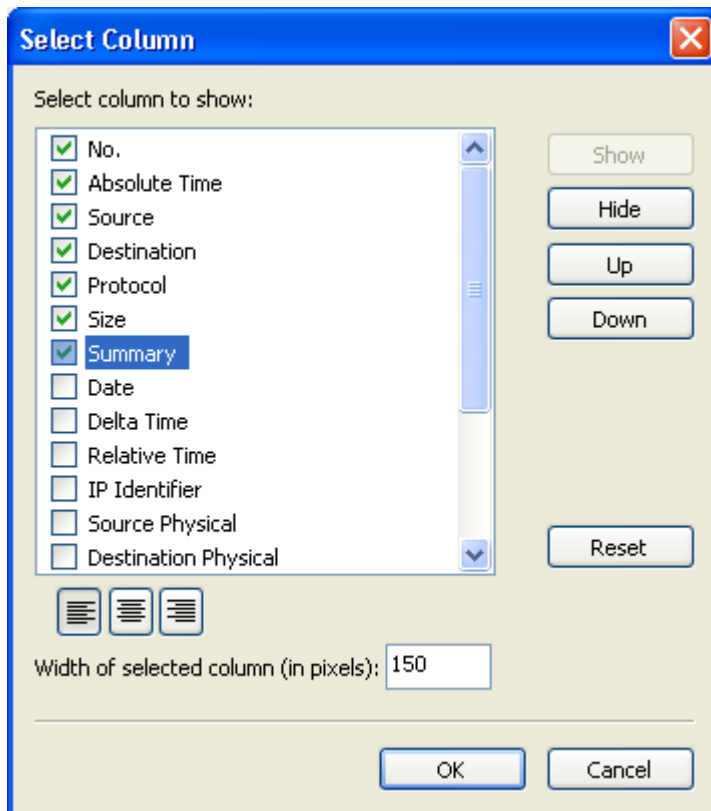
By default the data displayed in a column are aligned left, but they also can be aligned center or aligned right with the alignment options in the **Select Column** dialog.

- **Column width**

To increase or decrease the width of a column, just hold down the mouse button on the column line and move horizontally; or you may fix the width in pixel in the **Select Column** dialog.

- **Change position**

To change a column's position, move your mouse to the column, hold down the mouse button and drag the column to your intended position. You may also do the operation in the **Select Column** dialog with the **Up** or **Down** buttons.



Sorting data

Just with a click or double clicks on the column headings in the **Endpoints** view, **Protocols** view and **Conversations** view, the sort order will be changed. The icon ▼ indicates the data in this column is displayed by descending, and the icon ▲ indicates the data in this column is displayed by ascending.



Sort endpoints by Total Bytes

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports						
Type All						
Name	Total Bytes ▼	Bytes Out	Bytes In	Total Packets	Packets In	Total Bytes%
Local Segment	28.070 MB	3.086 MB	22.623 MB	58,357	24,098	99.918%
Local Host	27.308 MB	2.787 MB	24.521 MB	53,428	29,693	97.204%
Asiarock:1F:1A:95	27.308 MB	2.787 MB	24.521 MB	53,428	29,693	97.204%
Eva	27.302 MB	2.783 MB	24.518 MB	53,325	29,651	97.182%
Realtek Semi:A4:78:CB	2.335 MB	1.920 MB	425.723 KB	10,722	4,915	8.313%
office1	2.299 MB	1.884 MB	425.723 KB	10,366	4,915	8.185%
192.168.0.2	29.445 KB	29.445 KB	0 B	238	0	0.102%
D-Link:65:75:49	558.794 KB	547.021 KB	11.773 KB	3,289	108	1.942%
office2	208.074 KB	200.953 KB	7.121 KB	1,643	66	0.723%


Dock windows

The **Project Explorer** and **Project Status** are both dock windows which are on the left section of display by default, you can hide or alter their positions.

- **Hide dock windows**

Click the  icon to hide a dock window; to show it again, put your mouse cursor on the dock window button, then click the  icon again.

- **Close dock windows**

Click the  icon to close a dock window. To recover the display, click the **Explorer** or **Status** icon in the toolbar, or make selection from the **View** menu.

- **Change position**

To change a dock window's position, move your mouse cursor to it's title bar, hold down the mouse button and drag the whole bar to your intended position.

- **Reset**

Double click the title pane, the dock window will be reset to default position.

Performance Optimization

The performance of Colasoft Capsa depends on many factors like network environment, network scale, traffic size, etc. To get the most out of Colasoft Capsa you can take the following measures to optimize its performance.

- **Program configuration**

By default, Colasoft Capsa captures and analyzes all the traffic passing through your network. When you only need to analyze segmental packets, the efficiency will play down if you maintain the default settings.

- **Packet filters**

The packet filters in Colasoft Capsa are flexible and customizable, you can discard undesired packets by setting filters to increase the analysis speed.

- **Logs**

The logs can be disabled in the **Project Setting - Log** page. When you disable a log, Colasoft Capsa will not display the logged data corresponding to it.

- **Packet buffer size**

The packet buffer size is set to 16384 KB by default and should be customized according to your system memory size, it might slow down the system performance if you set a big value.

- **Project settings**

Some project settings may increase the resource occupation of your system, such as resolve host name of captured IP addresses, enable logs, save log file to disk, etc. You can enable such optional functions only when necessary.

- **Analyzer**

The more analyzers are enabled the more system resource and memory will be occupied. You can disable some analyzers in the **Options - Analyzer** dialog.
- **Packet decoders**

The more decoders you enable for packet decoding, the more system resources are occupied. You can disable some packet decoders in the **Options - Decoder** dialog.
- **Multiple projects**

It will increase system's resource occupation when multiple projects are capturing. It would be better not to use multiple projects if a single project can fulfill the monitoring work.
- **Monitoring multiple adapters**

Colasoft Capsa can monitor the traffic passing through different adapters (unique to enterprise edition), but opening multiple adapters simultaneously may play down the program performance. To ensure the capture and analysis efficiency it is recommended to open an adapter at a time.
- **Hardware optimization**

The minimum requirements for Colasoft Capsa are PIII 500 CPU and 256 MB RAM. With the minimum requirements Colasoft Capsa can work well in a small network; however, it may occur such problems as slow analysis speed, unstable system performance or even crash in a big network (e.g. a network with over 1024 hosts). If so, you need to optimize your hardware facilities.

 - **CPU**

CPU is one of the most important symbols for system performance, you can enhance the system and program performance using a CPU with quicker process speed.
 - **System memory**

Another important symbol for system performance is system memory. Sufficient system memory can ensure the speediness of project storage.
 - **Hard disk/NIC**

Such system assistant facilities also may affect the performance of Colasoft Capsa, it is recommended to use high-speed hard disk and 100M - 1000M adapters.
- **Operation system and system services**

The performance of Colasoft Capsa may also be influenced by other running processes, enabled services or defined virtual memory. On the server installed with Colasoft Capsa you should enable as few applications/services as possible, expand virtual memory and do not offer outbound services. In addition, since higher operation system occupies more system resources, it is recommended to adopt the most appropriate operation system in view of different configurations.
- **Network topology optimization**

The network topology is very important for network monitoring and analysis, too many broadcast, multicast or loop-back packets will add the resource occupation. You should check your network topology, avoiding loop-back traffic or improper connections to reduce trash packets in your network.