Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

User Manual

(Enterprise Edition)

Contact Us

Telephone

800-381-6680 (8:00AM - 6:00PM CST)

Sales

sales@colasoft.com

Technical Support

support@colasoft.com

Website

http://www.colasoft.com/

Mailing Address

Colasoft LLC

8177 South Harvard Ave., Suite 101

Tulsa, OK 7413

Contents

Overview

Welcome to Capsa Enterprise, the portable network analyzer from Colasoft.

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

You may install Colasoft Capsa on a laptop and analyze, monitor and diagnose anywhere in your network you want to. Colasoft Capsa analyzes and diagnoses either real-time network traffic or problems in replayed saved packet files. To realize accurate problem location and efficient analysis, you can use application analysis profile to lock down problems in real-time.

Colasoft Capsa 7 adopts new user interface style of Microsoft Office 2007, which intends to display analysis statistics in a more simple-straight and graphical style. The new organized statistics tabs will really help shorten network engineers' time spent on finding useful information to diagnose the network. New Dashboard tab gives you enough choices to customize and create almost any kind of statistics graphs you want.

Based on the second-generation **Colasoft Packet Analysis Engine** (CSPAE) platform, Colasoft Capsa 7 enhances its performance in large traffic network. No matter in 100M or 1000M network, Colasoft Capsa provides you with efficient and complete network analysis solution.

Capsa Enterprise just adopted the support for wireless networks, which enables you to capture, monitor and analyze traffic from any of the 802.11 a, 802.11 b, 802.11 g, 802.11n wireless networks. Conformance to the latest **Network Driver Interface Specification** (NDIS) 6.0 library, Capsa Enterprise will run on almost all popular wireless cards in the market, which means almost every wireless card working under Windows Vista and Windows 7 will work with Capsa Enterprise.

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

- *Network traffic analysis*
- *Network communication monitoring*
- *Network problems diagnosis*
- *Network security analysis*
- *Network performance detecting*
- *Network protocol analysis*

Capsa Enterprise analyzes your wired and wireless networks from the lowest level and all the way up to the application level, so that it finds out all the problems of your network. Colasoft Capsa 7 Enterprise, in cooperation with other network management tools, will maximize your network value.

Deployment

Note that the following parts are only for wired networks. If you just need to analyze wireless networks, you can skip this chapter.

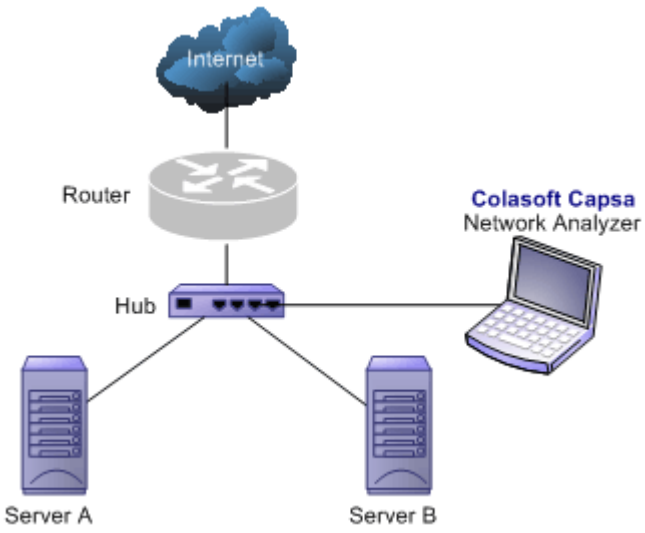
Installation environment

Colasoft Capsa is professional in monitoring and analyzing intranet packets and packets from internet, even packets crossing VLAN. Colasoft Capsa only need to be installed on the management machine, but other managed clients need not. Administrator needs to decide which machine to install Colasoft Capsa. Installation on different nodes, total captured packets number may differ. Therefore, you are recommended that you install or connect Colasoft Capsa to the central switch equipment, so that Colasoft Capsa will capture packets of your entire network to have a comprehensive monitoring and analysis. Of course you can use a TAP* to capture packets and analyze any network segment. Here we introduce you some common topology environments that Colasoft Capsa could have a sufficient monitor and analysis.

Shared network – Hub

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.

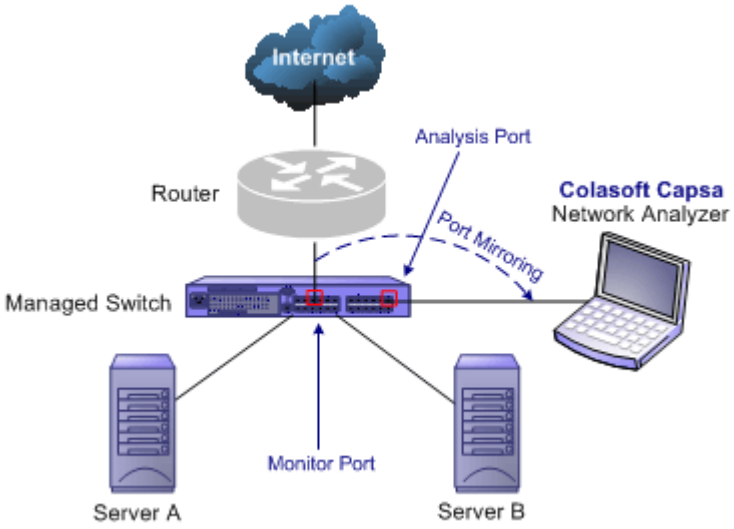


Switched network - managed switches (Port mirroring)

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.

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).

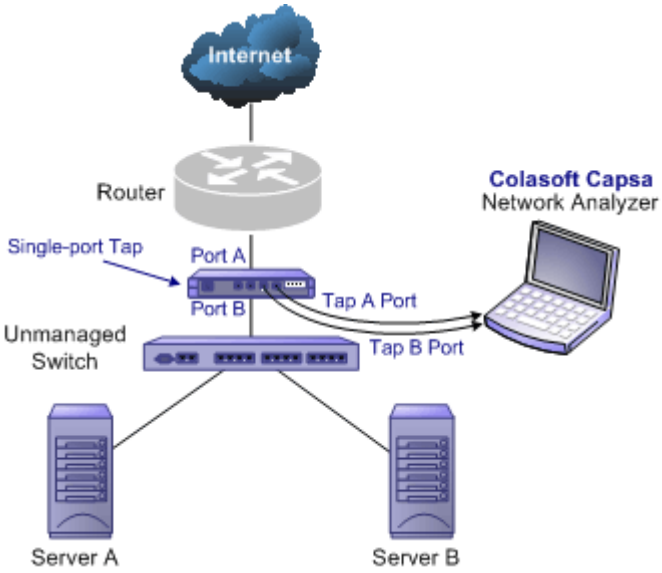


Switched network - unmanaged switches

Some switches do not have the network management function. So there is no mirroring port as well. You can either, in this scenario, use a Hub or a TAP* to monitor and analyze your network with Colasoft Capsa.

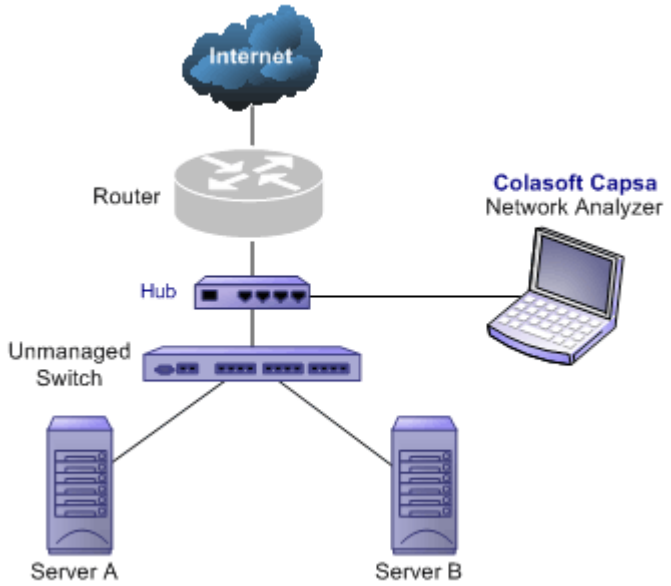
Connect a TAP* with the line to be monitored

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.



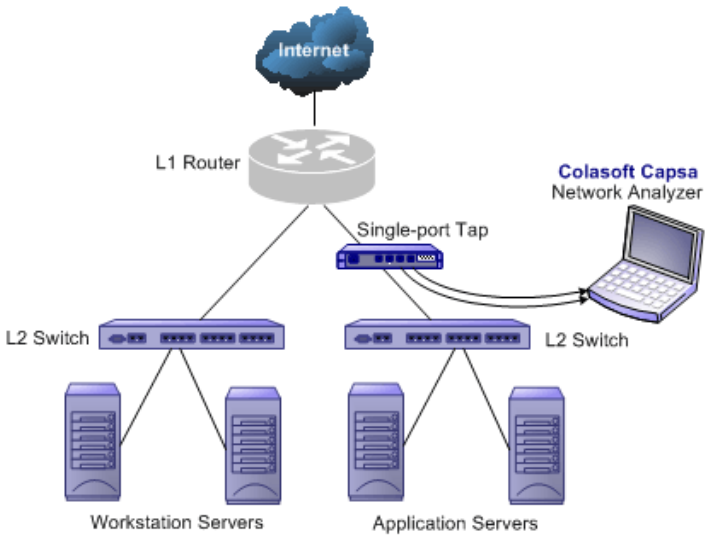
Connect a hub with the line to be monitored

A Hub costs lower than a TAP* but lower performance than a TAP in large traffic network.



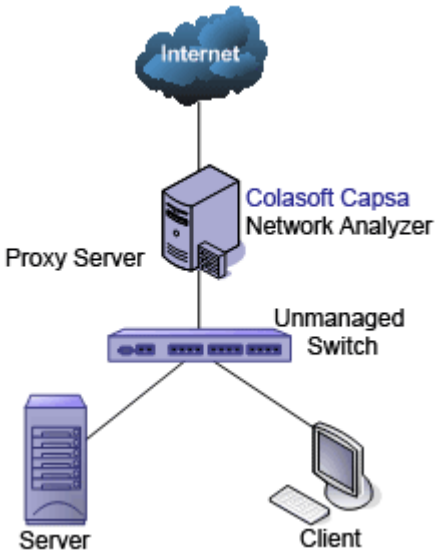
Monitoring a network segment

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 an exchange facility. The exchange facility can be hub, switch or proxy server.



Proxy server

In small network, a proxy server is a reliable choice to deploy a network. Under this circumstance, you can install Colasoft Capsa directly on the proxy server.



Ways of configuring port mirroring would be different from different switches or models. See Switch and Port Mirroring to learn common-used switch port mirroring configurations.

Port mirroring

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 packet analyzer) is limited to capturing packets only from the port the machine connected to and broadcast packets and multicast packets.

However, most modern switches (management switches) support port mirroring, which allows users 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 configuration documents shipped with your switch for 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. Read Installation Environment to know how to deploy Colasoft Capsa.

A list of some managed switches (with port monitoring/spanning) which are commonly used is available on our website, please visit the Switch Management page for references.

System requirements

Colasoft Capsa does not need a high performance machine and can be installed on many Windows operation systems, such as Windows XP, Windows 2003, Windows Vista and x64 Edition and the latest Windows 7. Your system's performance and configuration

will affect the running of Colasoft Capsa. The following minimum requirements are the bottom 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

- P4 2.8GHz CPU
- 2 GB RAM
- Internet Explorer 6.0

Recommended requirements

- Intel Core Duo 2.4GHz CPU
- 4 GB RAM or more
- Internet Explorer 6.0 or higher

Supported windows operating systems

- Windows XP (SP 1 or later) and 64bit Edition*
- Windows Server 2003 and 64bit Edition*
- Windows Vista and 64bit Edition
- Windows 2008 and 64bit Edition*
- Windows 7 and 64bit Edition

**The wireless analysis module is not compatible with this operation system.*

Wireless adapters

- All integrated USB, Express Card and PCI wireless adapters with Network Driver Interface Specification (NDIS) 6.0 driver library.

Installation and Uninstall

Before installation

1. Carefully read Installation Environment and check if your network topology is fit for Colasoft Capsa working environment.
2. Carefully read System Requirements and make sure your machine meets the minimum requirements at least.
3. Close all running applications on your machine.
4. Uninstall any earlier or trial versions of Colasoft Capsa on your machine.

You can skip the uninstall step. Colasoft Capsa will automatically check the older versions and ask you to uninstall them in the installation wizard.

Installation

1. Double-click the installation file, **Welcome** screen appears, telling you that Colasoft Capsa will be installed on your machine. Click **Next** to continue or **Cancel** to exit setup.
2. Read the License Agreement carefully in the next screen to learn our terms and conditions concerning possession and use of Colasoft Capsa. You must accept the terms of the license agreement to continue the installation.
3. The screen presents the important information from the **ReadMe** file.
4. Select **Destination Location** screen. It suggests the default location to install Colasoft Capsa. You may click **Browse...** to choose another installation location. Space requirement display on the bottom of the dialog box; make sure you have enough space for the installation. Click **Next** to continue.
5. Select **Start Menu Folder** screen. Click the **Browse...** button to designate an alternate start menu folder. Click **Next** to continue.
6. Select **Additional Tasks** screen. **Create a Desktop Icon** and **Create a Quick Icon** are checked by default. Uncheck any checkbox if you do not want to create the icon. Click **Next** to continue.
7. Now you are ready to install Colasoft Capsa on your machine. Click Install to start installation or click **Back** to change your settings.
8. When installation is complete, the completing screen appears. Click **Finish** to close the setup wizard. Colasoft Capsa will be started if you checked **Launch Program**.

If no changes on default create desktop icon and shortcut icon check boxes, you will see an icon on the desktop and one in **Quick Start**.

Uninstall

To open Colasoft Capsa Uninstall dialog box, do one of the following:

- To uninstall Colasoft Capsa, choose Start > All Programs > Colasoft Capsa 7 Enterprise > Uninstall Colasoft Capsa 7 Enterprise.
- Open the Control Panel > double-click Add/Remove Programs icon, the Add/Remove Programs window appears > find Colasoft Capsa 7 in the list and click Remove.

The Uninstall dialog box appears. Follow these steps to uninstall Colasoft Capsa:

1. If you want to completely remove Colasoft Capsa 7 and all of its components from your machine, click YES to continue, or click NO to quit uninstall.
2. If you want to delete the license information, click YES, or click NO to remain license information on your machine to continue.

You are recommended to click NO to keep license information on your machine, in case you want to install Colasoft Capsa on your computer again.

3. If you want to delete your customized alias in Name Table and filters in Colasoft Capsa, click YES or NO to remain them on your machine to continue.
4. To finish uninstall, click YES to restart your machine.

Product Activation

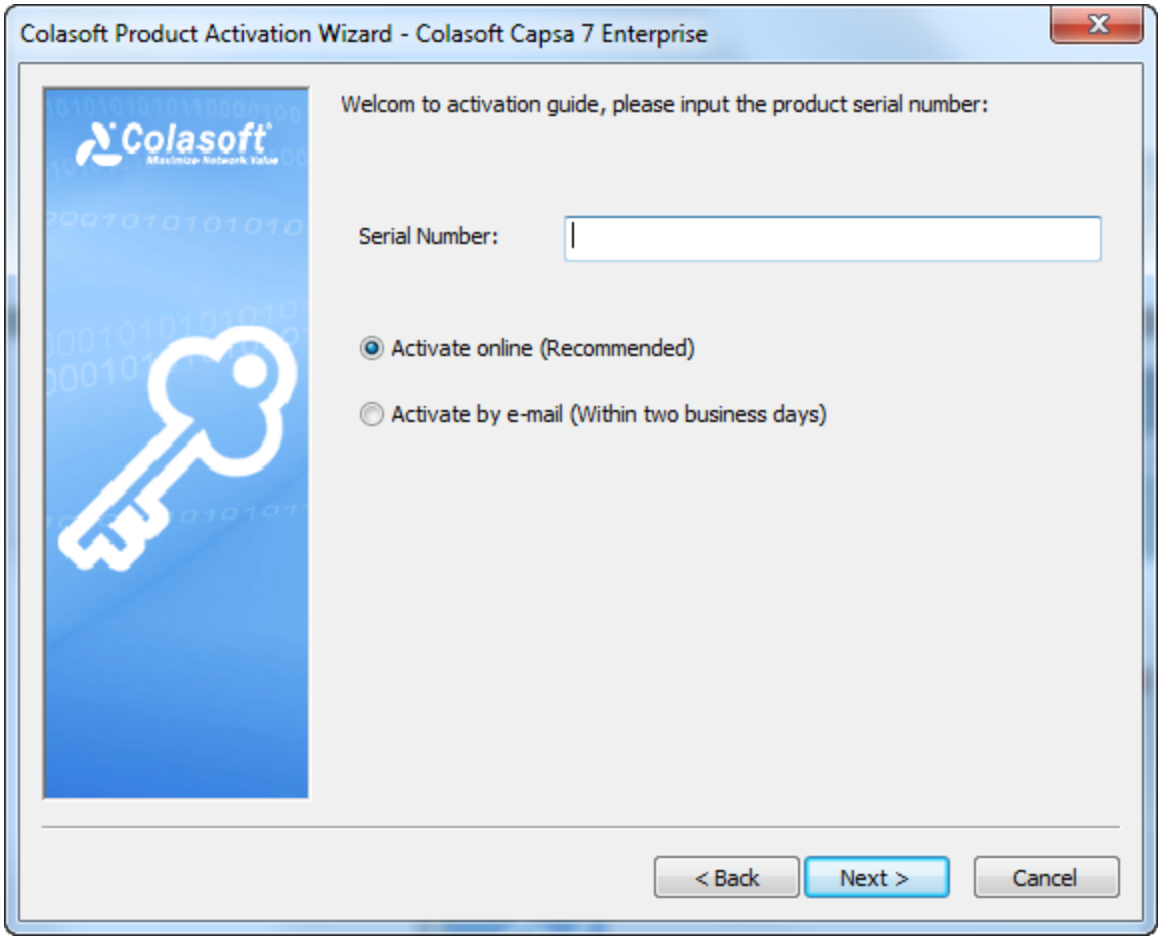
Colasoft Product Activation is an anti-piracy technology designed to verify that software products have been legitimately licensed. This aims to reduce a form of piracy known as casual copying. Activation also helps protect against hard drive cloning. Activation is quick, simple, and unobtrusive, and 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 Activation Number 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 the program. It is allowed to reactivate the program no more than five times per day.

Activation guide

The product activate process is very important to against privacy. To activate Capsa, you need to correctly enter the serial number, and a dialog box will appear to require you to activate your product. You may choose to activate product over the Internet, or by fax or email.



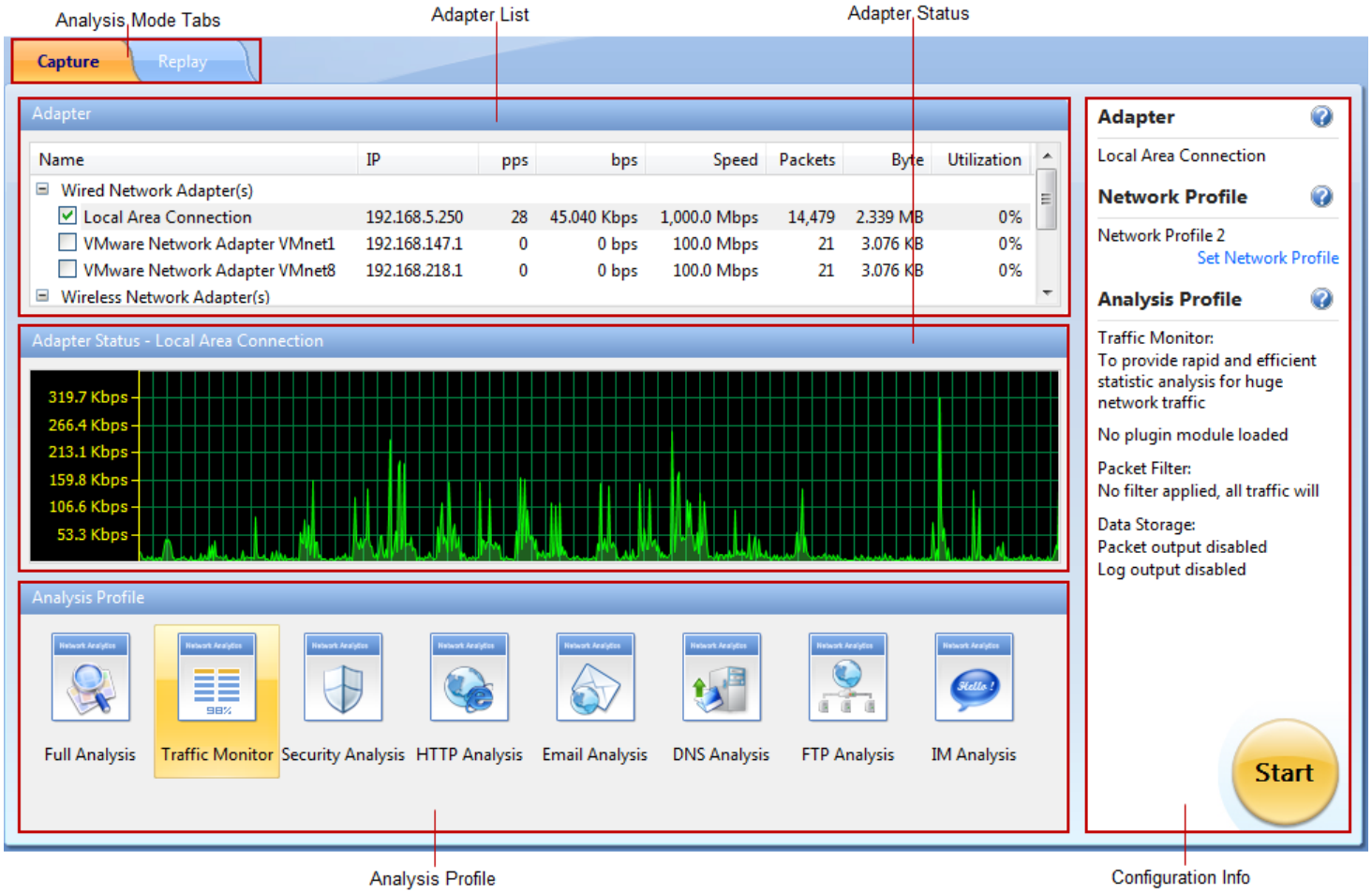
- **Activate online**: It is very quick and easy, the activation process will only take a few seconds with a couple of clicks.
- **Activate by email**: If you select to activate product manually, it will need more time to finish. Please send us via email the

Serial Number and Machine Number. After receiving your request, we will get back to you with a license file. Import the license file, and your product will be activated immediately.

Getting Started

Start Page

The *Start Page* is the first screen you see when starting the program, which guides you to start an analysis project step by step and appears as below.



The *Start Page* includes following parts.

1. **Analysis Mode tabs**: Includes **Capture** tab and **Replay** tab. The **Capture** tab is for capturing live network data. The **Replay** tab is for replaying captured network data (See *Replaying captured packets* for details).
2. **Adapter List section**: Lists all available network adapters, including wired and wireless ones. Data is transmitted over the network via network adapters (also known as Network Interface Card, NIC for short), and network analyzers capture the data through network adapters.
3. **Adapter Status section**:
    - When a wired network adapter on the **Adapter List section** is selected, this section shows the real-time traffic status of the adapter.

- When a wireless network adapter on the **Adapter List section** is selected, this section will be *AP Status section* and lists all available APs.

4. **Analysis Profile section:** Lists all available analysis profiles (See *Analysis Profile* for details).
5. **Configuration Info section**: Displays the configuration info of the analysis project and includes following parts:
   - **Adapter**: Displays the adapter selected on the **Adapter List section**.
   - **Network Profile**: Displays the selected network profile. To edit or change a network profile, click **Set Network Profile** on the right side. See *Network Profile* for details.
   - **Analysis Profile**: Shows some details of the analysis profile selected on the **Analysis Profile section**, including loaded analysis modules, packet filters, and data storage information.

You can click  on the right side to get related tips and introductions.

Starting a capture

This page mainly describes the steps to start a capture with wired network adapters. To start a capture with wireless network adapters, see *Capturing with wireless network adapters* for details, and to replay packet files, see *Replaying captured packets* for details.

To quickly start a live network data capture, select a network adapter and click the **Start** button on the *Start Page*.

To start a capture with user-defined configurations, follow the steps below:

1. Select the **Capture** tab on the **Analysis Mode Tabs**.
2. Select a network adapter on the **Adapter List section**. The **Adapter Status section** shows the traffic status of selected adapter. You can choose one or more wired network adapters at the same time.
3. Click **Set Network Profile** on the **Configuration Info section** to select a network profile. A network profile includes the settings about node group, name table, and alarms (See *Network Profile* for details).
4. Select a proper analysis profile on the **Analysis Profile section**. An analysis profile includes the settings about analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display. Capsa provides six analysis profiles by default, and you also can create new analysis profiles (See *Analysis Profile* for details).
5. Click the **Start** button on the bottom-right to start an analysis project.

Tips

1. You can run up to four analysis projects on the same machine at the same time.
2. If you just want to analyze some specific packets on the network, you should use packet filters. Click *Creating Filters* for details.

Capturing with wireless network adapters

Besides capturing traffic data with wired network adapters, Capsa can capture packets with wireless network adapter. To start a capture with wireless network adapters, follow the steps below.

1. Select the **Capture** tab on the **Analysis Mode Tabs**.
2. Select a wireless network adapter on the **Adapter List section**, and then the **Adapter Status section** will be *AP Status section* and lists all available APs.

3. Select an AP, then you will be asked to type the key if the AP is encrypted. You can also select more than one AP, but the APs must be of the same channel.
4. Click **Set Network Profile** on the **Configuration Info section** to select a network profile. A network profile includes the settings about node group, name table, and alarms (See *Network Profile* for details).
5. Select a proper analysis profile on the **Analysis Profile section**. An analysis profile includes the settings about analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display. Capsa provides six analysis profiles by default, and you also can create new analysis profiles (See *Analysis Profile* for details).
6. Click the **Start** button on the bottom-right to start an analysis project.

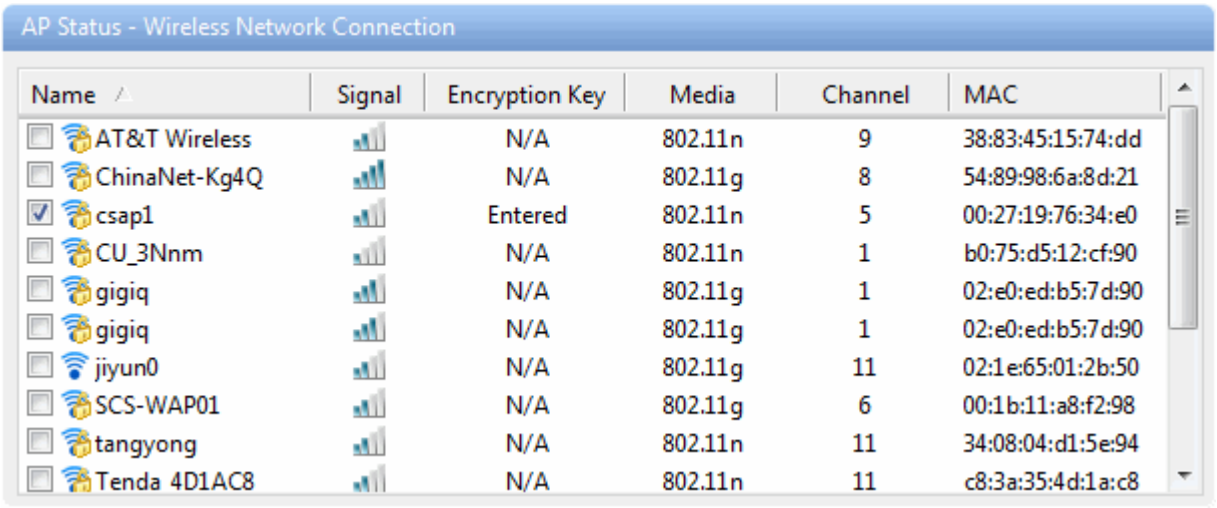
Note

1. It is only available in Windows Vista and Windows 7 to capture packets with wireless network adapters.
2. If you enter the wrong key, the analysis project will run as well but it will not capture packets.
3. One analysis project only captures traffic data from one wireless network adapter. If you have multiple wireless network adapters on your machine, you should create new analysis projects, one wireless network adapter for one analysis project.

AP Status section

Once a wireless network adapter is selected, all detected APs are listed on the **AP Status section** immediately with AP name, signal intensity, encryption keys, media type, AP channel, and MAC address.

This section appears as follows:



To refresh the AP list, right-click and choose **Refresh**.

To edit the properties of an AP, double-click the AP or right-click the AP and choose **Properties** to open a Wireless Network Properties dialog box, which is used to configure the settings of an AP, including alias and encryption keys. You can give the AP an alias to be easily identified. Capsa can identify the encryption type and you should just enter the encryption keys. The program can memory the settings of an AP. If it is not the first time you select an AP, you would just select the AP without enter the keys.

To manage the APs that have been used, right-click and choose **Wireless Network Manager** to open the Wireless Network Manager window in which, you can find a history list for all the wireless APs that have been monitored. You can change their encryption keys and

delete the old entries.

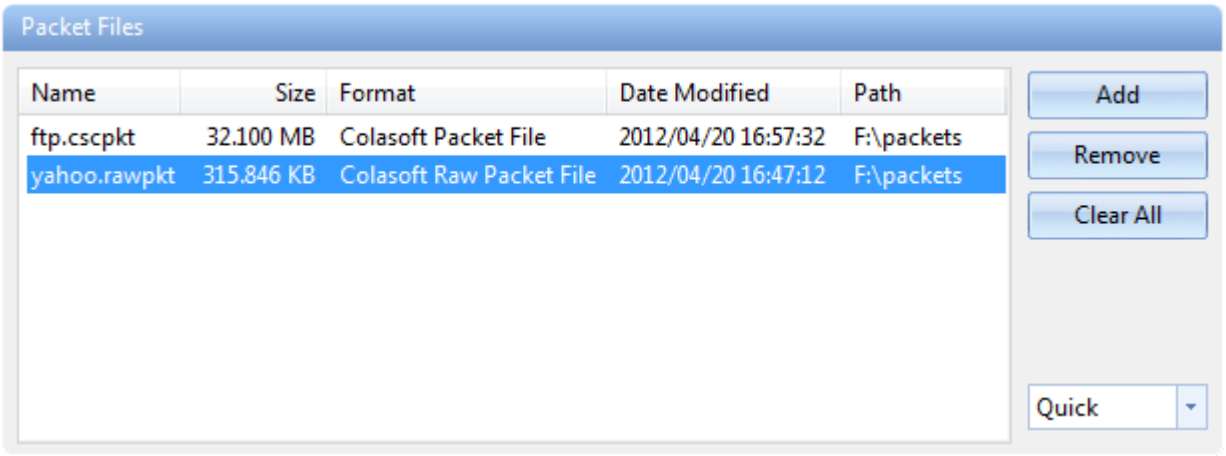
Replaying captured packets

Capsa analyzes not only live network data but also captured packets, including packets captured by Capsa as well as packets captured by other programs, such as, Wireshark, Omnipeek and other packet files.

To replay captured packets, follow the steps below:

1. Select **Replay** tab on the *Start Page*.
2. Add the packet files from **Packet Files** section.
3. Click **Set Network Profile** on the **Configuration info section** to select a network profile. A network profile includes the settings about node group, name table, and alarms (See *Network Profile* for details).
4. Select a proper analysis profile on the **Analysis Profile section**. An analysis profile includes the settings about analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display. Capsa provides six analysis profiles by default, and you also can create new analysis profiles (See *Analysis Profile* for details).
5. Click the **Start** button on the bottom-right to start an analysis project.

The **Packet Files** section appears as below.



- **Add**: Adds the files to be replayed. When multiple packet files are replayed simultaneously, packets will be replayed according to time stamps, instead of file listing order in the packet file list.
- **Remove**: Removes the selected packet file from the list.
- **Clear All**: Empties the packet file list.
- **Replay Speed**: The speed to replay the packets, including:

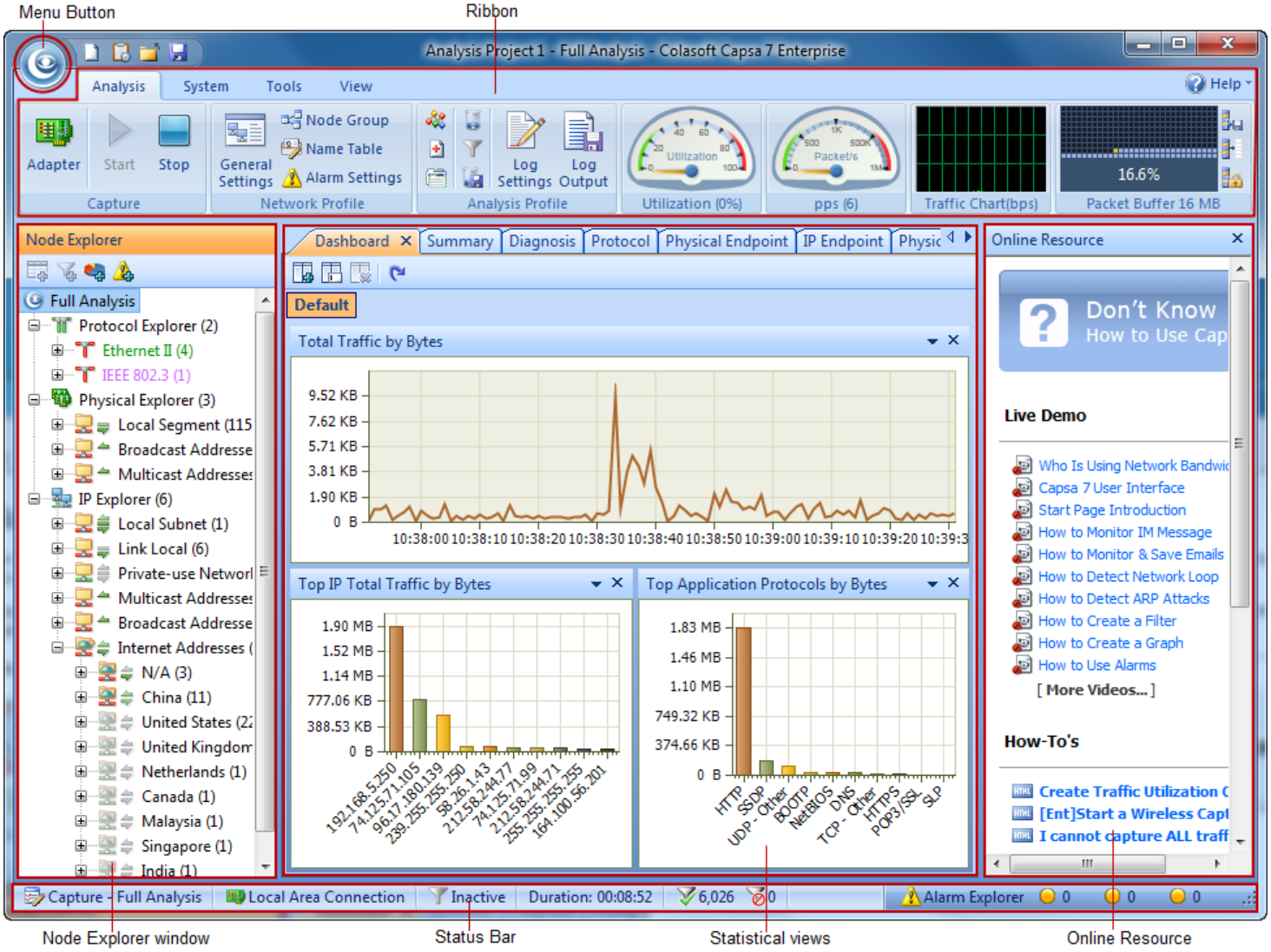
  Quick: Packets will be replayed by ignoring the time intervals. Capsa replays packets with Quick speed by default.

  Normal: Packets will be replayed at capturing speed, which is slow.

Main User Interface

After starting an analysis project, whether real-time capturing or replaying packets, Capsa enters the main user interface in which you still can start a new analysis project, set network profile and analysis profile, and which show you all statistics and the root of network problems. All functions provided at the *Start Page* can be realized on the main user interface.

By adopting new *Microsoft Office UI*, Capsa intends to present statistics and diagnosis data in a simple-straight and graphical style. From the figure below, you can learn that an analysis project window is mainly divided into six sections.



Menu Button

The **Menu** button is on the top-left corner of a project window and appears as  .

Items on the menu button

The following table lists and describes the items on the menu button.

Item	Shortcut	Description
New	Ctrl+N	Creates a new analysis project.
Configurations Backup		Imports or exports global configurations (See *Global configurations* for details). Import: Imports global configurations from a file. Export: Exports current configurations of the program to a file.
Print		Prints current page or sets print configurations. Print: Prints the current window in a format appropriate to its type. Print Settings: Configures printer functions in the **Print Setup** dialog box. Print Preview: Preview the print page.
Resource		Offers Internet information about Colasoft and network analysis. Colasoft Home Page: Opens Colasoft home page. Tech Forum: Opens the technical forum, where you can get help and learn more skills on network analysis.
Product		Provides product information. Product License: Renews your license key. Register: Registers at Colasoft official website to get timely customer services and product information. Check Update: Checks new versions. About: Opens the **About** dialog box where you can find the version, copyright and license information of the product.
Close		Closes current analysis project and goes back to the *Start Page*.
Recent Files		A list of recently opened packet files for you to conveniently select a file to open.
Options		Configures some settings for the analysis project (See *System Options* for details).
Exit		Exits the program.

Quick Access Icons

After starting an analysis project, there are three quick access icons beside the **Menu** button.

Icon	Description
	Creates a new analysis project.
	Calls out *Task Scheduler* to add new task (See *Task Scheduler* for details).
	Closes current project and goes back to the *Start Page*.
	Saves packets in the buffer to disk. You can save packets in twelve formats, including *Colasoft Packet File (*.cscpkt)*, *Colasoft Raw Packet File (*.rawpkt)*, *Colasoft Raw Packet File (v2) (*.rawpkt)*, *Accellent 5Views Packet File (*.5vw)*, *EtherPeek Packet File (V9) (*.pkt)*, *HP Unix Nettl Packet File (*.TRC0; TRC1)*, *libpcap (Wireshark, Ethereal, Tcpdump, etc.) (*.cap; pcap)*, *Microsoft Network Monitor 1.x, 2.x (*.cap)*, *Novell LANalyzer (*.tr1)*, *NetXRay2.0, and Windows Sniffer (*.cap)*, *Sun_Snoop (*.Snoop)*, and *Visual Network Traffic Capture (*.cap)*.

Ribbon

The **Ribbon** section includes four tabs as follows:

Analysis: Configures settings for the analysis project.

System: Contains **Resources** and **Product** sections.

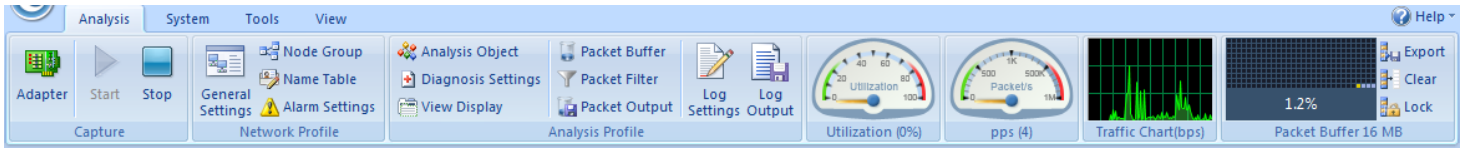
Tools: Provides Colasoft network tools.

View: Configures the display of the program.

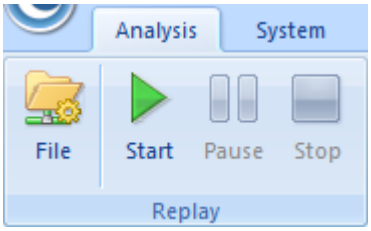
Tips You can use the mouse scroll wheel to navigate from one tab to another when the mouse pointer is over the **Ribbon** section.

Analysis tab

The **Analysis** tab appears as follows:



When the **Replay** analysis mode is selected, the **Capture** part will be **Replay** as follows:



The **Analysis** tab includes the following sections:

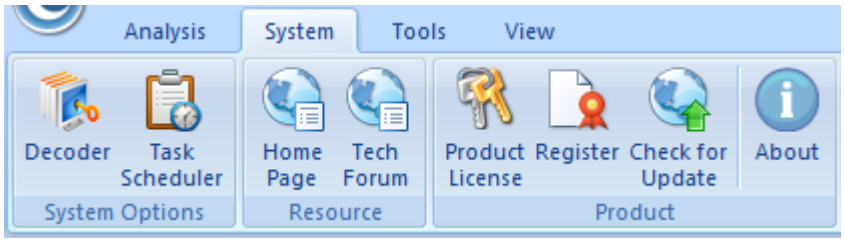
- **Capture**:
  - Adapter: Click to open the **Select Network Adapter** dialog box to view the adapter properties or change the selection on the adapters.
  - Filter: Sets packet filters (See *Creating Filters* for details).
  - Start: Starts capturing packets.
  - Stop: Stops capturing packets.
- **Replay**:
  - File: Opens the **Packet File Management** dialog box which is just the same as the **Packet Files** section on the *Start Page*.
  - Filter: Sets packet filters (See *Creating Filters* for details).
  - Start: Starts the replay.
  - Pause: Pauses the replay.
  - Stop: Stops the replay.
- **Network Profile**: Sets the parameters for network profile. (Read *Network Profile* for more details).
- **Analysis Profile**: Sets the parameters for analysis profile (Read *Analysis Profile* for more details).
- **Gauge**:
  - Utilization (%): Shows network bandwidth utilization in gauge.
  - pps: Shows the number of captured packets in gauge.

- **Traffic Chart (bps)**: Shows the traffic of chosen adapter with refreshing every second. Move your mouse over the chart and you will see the traffic number and specific time.
- **Packet Buffer**:
    - Buffer Map: Shows how much buffer for the analysis project was used with total buffer size below the Buffer Map (See *Packet Buffer* to know how to set buffer size).
    - Export: Saves the packets in packet buffer in a format selected from the *Save as type* drop-down list box.
    - Clear: Clears the data in the packet buffer.
    - Lock: Stops storing packets in the buffer.

Note The program still captures packets upon locking the packet buffer.

System tab

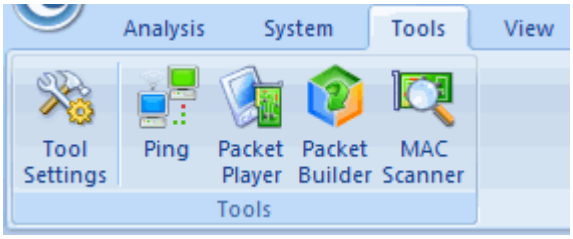
The **System tab** appears as follows:



- **Decoder**: Calls out **Decoder Settings** tab to set decoders.
- **Custom Protocol**: View user-defined protocols.
- **Task Scheduler**: Calls out *Task Scheduler* to add new tasks. Only available in Capsa *Enterprise*.
- **Home Page**: Opens Colasoft home page.
- **Tech Forum**: Opens the technical forum, where you can get help and learn more skills on network analysis.
- **Product License**: Renews the license key.
- **Register**: Registers at Colasoft official website to get timely customer services and product information.
- **Check for Update**: Checks new versions.
- **About**: Opens the **About** dialog box where you can find the version, copyright and license information of the product.

Tools tab

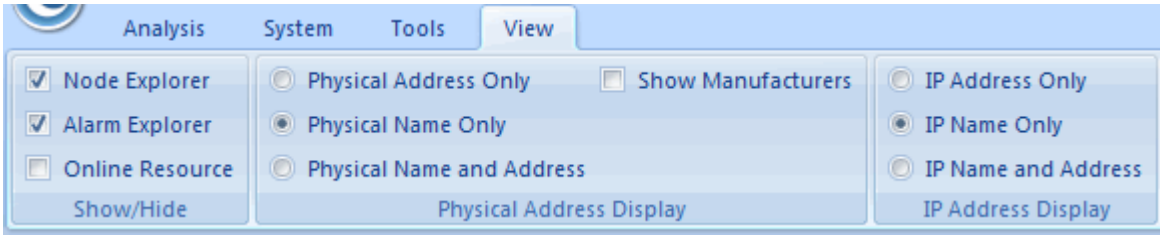
The **Tools tab** appears as follows:



For more information about **Tools** tab, see *Network Tools*.

View tab

The **View** tab appears as follows:



The **View** tab contains the following items:

- **Show/Hide**: Enables the **Node Explorer**, **Alarm Explorer** and **Online Resource** windows to show or hide.
- **Physical Address Display**: Sets the display format of MAC addresses.
    - Physical Address Only: Only shows the MAC addresses in hex, e.g. *AA:BB:CC:33:44:55*.
    - Physical Name Only: Only shows the MAC addresses in alias, e.g. *localhost*.
    - Physical Name and Address: Shows the MAC addresses in hex and alias (if any), e.g. *[localhost]-AA:BB:CC:33:44:55*.
    - Show Manufacturers: Hides or shows the adapter vendor.
- **IP Address Display**: Sets the display format of IP addresses.
    - IP Address Only: Only shows the IP addresses in digits, e.g. *192.168.1.1*.
    - IP Name Only: Only shows the IP addresses in alias, e.g. *Localhost*.
    - IP Name and Address: Shows the IP addresses in digits and alias (if any), e.g. *[Localhost]-192.168.1.1*.

Node Explorer window

The **Node Explorer** window is functionally a display filter, by which you can view various conversation data of a node quickly and accurately. So, when you select different type of nodes in the **Node Explorer** window, the statistical views will show different tabs and the tabs will present different statistics.

Buttons

The **Node Explorer** window includes the following buttons:

 : Adds specific node to name table (See *Name Table* for details).

 : Creates filters using the specific node (See *Creating Filters* for details).

 : Creates graphs using the specific node (See *Creating Graphs* for details).

 : Creating alarms using the specific node (See *Creating Alarms* for details).

Nodes

The **Node Explorer** window includes the name of selected analysis profile which is called as the root node and three node explorers which are called as **Protocol Explorer**, **Physical Explorer**, and **IP Explorer**. Each explorer includes many nodes. The **Protocol Explorer** groups the protocol nodes by protocol layer. The **Physical Explorer** and **IP Explorer** group the address nodes by the node groups. You can group local MAC addresses and local IP addresses. See *Node Group* for details.

Tips You can operate the nodes by keyboard: press **UP** arrow on the keyboard to select the upper node, **Down** to select the lower node, **LEFT** to collapse the node, and **Right** to expand the node.

In the **Node Explorer** window, both a single node and a node group can be called as a node.

Note

1. For the protocols not identified by the program, they will be displayed as **Other**.
2. For wireless network adapter, some IP addresses will not be displayed due to encryption.

Protocol icon

There are three types of icons in front of each protocol node. The red icon  indicates there is data transmission in five seconds, the green icon  indicates there is data transmission in thirty seconds, and the grey icon  indicates there is no data transmission in thirty seconds.

Traffic direction icon

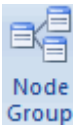
You may have noticed the arrow icons in front of each node with different directions and colors. The upper arrow indicates packets transmitted to the node, the middle line indicates transmission inside the node, and the lower arrow indicates packets transmitted out from the node. Green indicates ongoing transmission and grey indicates completed transmission.

Address type icon

In front of arrow icons, there are icons indicating the address type of the node,  and  both indicating broadcast address,  and  both indicating multicast address, and  indicating Internet address.

Internet address group

By default, Internet IP addresses are hierarchically grouped by countries or areas. To display the Internet IP addresses flat, click **Node**

Group icon 

on the **Analysis** tab of the **Ribbons** section and cancel the selection on **Enable Country Group**.

Statistical views

The statistical views provide huge amount of statistics on the network (See *Viewing Statistics* for more information).

The default visibility status of statistical views changes along with analysis profile. The following table lists the statistical views for each analysis profile.

Analysis profile	Statistical views available	Show status
Full Analysis	Dashboard, Summary, Diagnosis, Protocol, Physical Endpoint, IP Endpoint, Physical Conversation, IP Conversation, TCP Conversation, UDP Conversation, Matrix, Packet, Log, Report	All available statistical views are displayed.
Traffic Monitor	All views in **Full Analysis** with different display order	The views except TCP Conversation, UDP Conversation and Packet are displayed.
Security Analysis*	All views in **Full Analysis** with different display order plus ARP Attack, Worm, DoS Attacking, DoS Attacked, TCP Port Scan, and Suspect Conversation views	The views except Dashboard, Protocol, UDP conversation are displayed.
HTTP Analysis	All views in **Full Analysis** with different display order	The views except Physical Conversation and Packet are displayed.
Email Analysis	All views in **Full Analysis** with different display order	The views except Dashboard, Physical Conversation and Packet are displayed.
DNS Analysis	All views in **Full Analysis** with different display order	The views except Physical Conversation, TCP Conversation and Packet are displayed.
FTP Analysis	All views in **Full Analysis** with different display order	The views except Physical Conversation and Packet are displayed.
IM Analysis	All views in **Full Analysis** with different display order	The views except Dashboard, Packet, and Report are displayed.

* *Security Analysis* is only available in Capsa Enterprise.

You can also show or hide or arrange statistical views.

- To show a view, click **View Display** icon on the **Analysis** tab of the **Ribbon** section and select the view.
- To arrange views, click **View Display** icon on the **Analysis** tab of the **Ribbon** section and click **Move Up** or **Move Down**.

Meanwhile, the statistical view section provides different statistical views when selecting different type of nodes in the Node Explorer window.

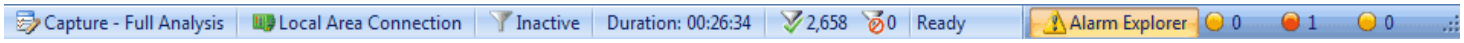
Online Resource window

Online Resource window provides much online resource, including how to use Capsa, live demo, and technical forum.

Online Resource window is displayed on the right section of the main user interface by default. You can close it by clicking the close button on the top right corner. If you do not want to show it when starting analysis projects, click **Menu** button, select **Options**, and on **Basic Settings** tab cancel the selection on **Show Online Resource window on start**.

Status Bar

The *Status Bar* presents you the general information of current project. It is at the bottom of an analysis project and appears as below.



From left to right, the *Status Bar* includes seven parts as below.

Analysis Mode - Analysis Profile

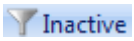
This part shows the analysis mode and the analysis profile you selected. You can click this part to open the **Analysis Profile Settings** dialog box to configure settings. See *Analysis Profile* for more details.

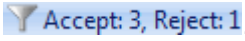
Adapters

In **Capture** analysis mode, this part shows the name or the number of selected wireless AP or wired network adapter. You can click it to view the details.

In **Replay** analysis mode, this part shows the total size of replayed files and the replay status. You can click it to view the details.

Filter

This part shows filter information. It shows **Inactive** as 

when no filters are utilized, or shows the numbers of **Accept** filters and **Reject** filters as 

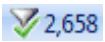
. You can click this part to open the **Filter** dialog box to set filters. See *Creating Filters* for details.

Duration

In **Capture** analysis mode, this part shows duration of current analysis project.

In **Replay** analysis mode, this part shows the time to replay the packet files.

Captured and Filtered Packets

This part shows the number of the packets captured by the program as 

and shows the number of the packets filtered out by the filters as 

.

Button and Menu Tips

This part shows tips of focused items when the mouse pointer moves over an item on the **Menu** or over a button on the **Ribbon** section, and showing *Ready* by default.

Alarm Notification Area

This part includes an **Alarm Explorer** icon and three counters of triggered alarms. See *Alarm Explorer window* for more details.

Viewing Statistics

Capsa provides a wide variety of statistics presented on the statistical views, each focusing on statistics of different types. The table below describes all statistical views briefly and you can click the links to know the details. Please note that different analysis profiles may have different views.

View	Description
Dashboard	Provides various graphs and charts of the statistics.
Summary	Provides general statistical information of the selected node in the Node Explorer window.
Diagnosis	Presents the real-time diagnosis events of global network by groups of protocol layers or security levels.
Protocol	Lists statistics of all protocols used in network transactions hierarchically.
Physical Endpoint	Lists statistics of all MAC addresses that communicate in the network hierarchically.
IP Endpoint	Lists statistics of all IP addresses that communicate in the network hierarchically.
Physical Conversation	Lists the conversations between two MAC addresses.
IP Conversation	Lists the conversations between two IP addresses.
TCP Conversation	Lists TCP conversations.
UDP Conversation	Lists the conversations using UDP protocols.
Matrix	Visually presents the communications among nodes dynamically.
Packet	Provides the details of a packet, by which you can get the original information of conversations.
Log	Provides the logs of DNS, Email communications, FTP transfer, web accesses, etc.
Report	Provides a wide range of statistics reports from global network to a specific node.
ARP Attack	Detects ARP attack activities and provides source MAC addresses to locate the infected hosts.
Worm	Detects suspicious worm activities and provides details including source IP addresses to locate the infected hosts.
DoS Attacking	Detects the hosts which attack a remote site, and provides details of the hosts.
DoS Attacked	Detects the hosts under a DoS attack and provides details of the hosts.
TCP Port Scan	Detects suspicious TCP port scanning activities.
Suspicious Conversation	Detects suspicious conversations of HTTP, FTP, SMTP and POP3.

Dashboard view

The **Dashboard** view is visible only when the root node of the **Node Explorer** window was selected. If it is still invisible, click **View Display** icon on the **Analysis** tab on the **Ribbon** section, and check **Dashboard** in the list (See *View Display* for details).

Capsa provides lots of statistical graphs which are managed by panels on the **Dashboard** view. So, you should first create dashboard panel before you create graphs (See *Creating Graphs* to know how to create a graph).

Toolbar

There are four button icons on the **Dashboard** view.

 : Creates a new dashboard panel.

 : Renames the selected panel.

 : Deletes the selected panel.

: Resets the **Dashboard** view to default settings and all user-defined graphs will be deleted.

By default, Capsa provides a dashboard panel named **Default** which includes three graphs and which can be renamed and be deleted after you have created a new panel.

Note The close icon on the top-right corner of a graph means deleting the graph from the dashboard panel instead of closing it.

Pop-up menu

Right-click charts of **Sample Chart** type to get a pop-up menu with items as follows:

Item	Description
Pause Refresh	Pauses the refresh.
Legend Box	Sets display options: Show Legend Box, Hide Legend Box, and Auto-show Legend Box: Set whether show Legend Box or not Pos: Top, Pos: Bottom, Pos: Left, and Pos: Right: Select the position where Legend Box shows
Line Chart	Displays the graph in line chart.
Area Chart	Displays the graph in area chart.
Titles	Shows the title of the graph, the title of X coordinate, and the title of Y coordinate.
Indicatrix	Shows a horizontal line which moves with mouse pointer and shows the value of Y coordinate where the mouse pointer locates.
Sample Interval	Sets the sample interval.
Save Graph	Saves the current graph to disk. You can save graphs in .png, .emf, and .bmp formats.

Right-click charts of **Top Chart** type to get a pop-up menu with items as follows:

Item	Description
Pause Refresh	Pauses the refresh.
Legend Box	Sets display options: Show Legend Box, Hide Legend Box, and Auto-show Legend Box: Set whether show Legend Box or not Pos: Top, Pos: Bottom, Pos: Left, and Pos: Right: Select the position where Legend Box shows
Bar Chart	Displays the graph in bar chart.
Pie Chart	Displays the graph in pie chart.
Titles	Shows the title of the graph, the title of X coordinate, and the title of Y coordinate.
Top Number	Displays the top number statistical items of the graph. It could be Top 5, Top 10, and Top 20.
Sample Value	Sets the statistic value type. It could be commulative value and last second value.
Refresh Interval	Sets the refresh interval.
Save Graph	Saves the current graph to disk. You can save graphs in .png, .emf, and .bmp formats.

Change graph position

Position of a graph is changeable. You can click and drag the head of a graph to rearrange its position go get a better view.

Summary view

Toolbar

There is only a **Refresh** button on the toolbar of this view to refresh the display. The little triangle is for setting the refresh interval. 1 second is selected by default. If the interval is set to **Manually Refresh**, display will update only when **Refresh** button is clicked.

Statistics item

The **Summary** view provides statistics of the whole network traffic and refreshes automatically. Different selections on the node on **Node Explorer** result in different statistics items.

For all analysis profiles:

Choosing the root node of **Node Explorer**, the **Summary** view provides all available statistics items of selected analysis profile (See *Summary items* for all statistics items).

Choosing a specific node of **Protocol Explorer**, the **Summary** view provides Total Traffic and Packet Size Distribution statistics of the node.

Choosing a specific MAC address of **Physical Explorer**, the **Summary** view provides Traffic statistics, Conversation statistics and TCP statistics of the node (plus ARP Attack statistics in the analysis profile of **Security Analysis**).

Choosing a specific node of **IP Explorer**, the **Summary** view provides:

- For **Full Analysis**: Traffic statistics, Conversation statistics, TCP statistics, DNS Analysis statistics, Email Analysis statistics, FTP Analysis statistics and HTTP Analysis statistics of the node.
- For **Security Analysis**: Security Analysis statistics, Traffic statistics, Conversation statistics, TCP statistics, DNS Analysis statistics, Email Analysis statistics, FTP Analysis statistics and HTTP Analysis statistics of the node.
- For **HTTP Analysis**: Traffic statistics, Conversation statistics, TCP statistics and HTTP Analysis statistics of the node.
- For **Email Analysis**: Traffic statistics, Conversation statistics, TCP statistics, and Email Analysis statistics of the node.
- For **DNS Analysis**: Traffic statistics, Conversation statistics, TCP statistics, and DNS Analysis statistics of the node.
- For **FTP Analysis**: Traffic statistics, Conversation statistics, TCP statistics, and FTP Analysis statistics of the node.

Summary items

The **Summary** view provides statistics changed along with **Analysis Profile** and the node in the **Node Explorer** window.

With **Full Analysis** and choosing the root node on **Node Explorer** window, the statistics items for **Summary** view include:

Item type	Item	Description
Diagnosis	Information Events, Notice Events, Warning Events, Error Events	List the number of each event type (See *Diagnosis* for more information)
Traffic	Total, Broadcast, Multicast, Average Packet Size	List byte, packet number, utilization, bps, packets per second of each traffic type Over **50%** of total traffic utilization: network may be overloaded Over **20%** of broadcast or multicast traffic utilization: broadcast/multicast storm and ARP attack
Packet Size Distribution	<=64, 65-127, 128-255, 256-511, 512-1023,1024-1517, >=1518	List byte, packet number, utilization, bps, packets per second of each packet size type Large portion of traffic at <=64 or >=1518: fragment attack or flood attack
Address	MAC Address, IP Address, Local IP Address, Remote IP address	List the number of each address type Too large number: MAC flooding attack, TCP

		flooding attack, etc.
Protocol	Total Protocols, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer	List the number of total protocols and protocols of six layers
Conversation	Physical Conversations, IP Conversations, TCP Conversations, UDP Conversations	List the number of four types of conversation
TCP	TCP SYN Sent, TCP SYNACK Sent, TCP FIN Sent, TCP Reset Sent (plus TCP SYN Received, TCP SYNACK Sent, TCP FIN Received and TCP Reset Received when a specific node of IP Explorer is selected)	List the number of each flag of TCP conversation Large number of TCP SYN packets: port scanning (TCP SYN flooding attack)
Alarm	Security Alarms, Performance Alarms, Fault Alarms	List the number of each alarm type
DNS Analysis	DNS Queries, DNS Responses	List the number of DNS query and response This type of statistics will not display in the analysis profiles of Email Analysis, FTP Analysis and HTTP Analysis.
Email Analysis	SMTP Connections, POP3 Connections	List the number of SMTP and POP3 connections This type of statistics will not display in the analysis profiles of DNS Analysis, FTP Analysis and HTTP Analysis.
FTP Analysis	FTP Upload, FTP Download	List the number of FTP upload and download This type of statistics will not display in the analysis profiles of DNS Analysis, Email Analysis and HTTP Analysis.
HTTP Analysis	HTTP Request Sent, HTTP Request Received, HTTP Connections	List the number of HTTP application This type of statistics will not display in the analysis profiles of DNS Analysis, Email Analysis and FTP Analysis.
Security Analysis	Worm, DoS Attacking, DoS Attacked, Suspect Conversation, TCP Port Scan, ARP Attack	List the number of each attack Security Analysis statistics are only available in the analysis profile of Security Analysis.

Diagnosis view

The **Diagnosis** view presents the real-time network events of the entire network down to a specific node via analyzing captured packets. The network events were defined by Capsa according to large amount of network data and can be defined by users through defining diagnosis settings (See *Diagnosis settings* for details).

The **Diagnosis** view contains three panes:

- *Diagnosis Item*
- *Diagnosis Address*
- *Diagnosis Events*

To change the size of the panes, move the mouse pointer on the border between panes, and when the pointer becomes a double-headed arrow, drag the pointer to move the split line.

Diagnosis Item pane

This pane lists the name and the count of all diagnosis events according to layers which the events belong to. All events are grouped into four types on the basis of security levels as follows:

Severity level	Icon	Description

Information		Indicates a normal message and no network problem.
Notice		Indicates normal but significant conditions.
Warning		Indicates an error that requires attention and should be solved soon.
Error		Indicates requiring immediate intervention by administrators to prevent serious problem to the network.

You can change the severity level and the trigger condition of diagnosis events in *Diagnosis Settings*.

When selecting a specific node in the **Node Explorer** window, this pane will only show the events related to the node.

Different analysis profiles may have different event items. See *Application layer events*, *Transport layer events*, *Network layer events* and *Data link layer events* for all available events.

Tips You can click **Name** and **Count** to sort the items. Note that only father nodes and number on the father nodes, such as **Transport Layer**, **Application Layer**, **Network Layer** and **Data Link Layer**, can be sorted.

Toolbar

The buttons of the toolbar are listed in the following table.

Item	Description
	Displays the settings of selected event. You can also view the settings of an event by double-clicking the event.
	Saves the current list of diagnosis events as a .csv file.
	Hides or shows the **Diagnosis Address** pane and show it by default.
	Hides or shows the **Diagnosis Events** pane and show it by default.
	Refreshes the event list or set the display refresh interval. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	The count of the rows of current list. Not the diagnosis event count. The name changes along with the selection in the **Node Explorer** window.

You can expand/collapse the event list by clicking the plus/minus sign.

Tips If you want to save all events in .csv format, you should first expand all and then click **Save as**, or else you only save the current event list, which means the specific events that were collapsed will not be saved.

Diagnosis Address pane

This pane displays the address of the event that is selected in the **Diagnosis Item** pane.

Note that the column **IP Address** is not available for events on data link layer.

The buttons of the toolbar are listed in the following table:

Item	Description
	Saves the address list as a .csv file.
	Makes a packet filter based on the IP address or MAC address of selected item on the address list. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for the IP address or MAC address of selected item on the address list. See *Name Table* for details.

	Refreshes the address list or set display refresh interval. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.

Right-click the address list to get a pop-up menu with items as follows:

Item	Description
Find	Calls out **Find** dialog box to search only on the **Diagnosis Address** pane.
Copy	Copies the selection and the header row in original format to the clipboard.
Save Log	Saves current address list as a .csv file.
Resolve Address	Only available when the address is IP address. Resolves the IP address of selected address item.
Make Filter	Makes a packet filter based on the IP address or MAC address of selected item on the address list. See *Creating Filters* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item on the address list. See *Name Table* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the IP address or MAC address of selected item on the address list. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the IP address or MAC address of selected item on the address list. See *Creating Alarms* for details.
Locate in Node Explorer	Locates the IP address or MAC address of selected item on the address list in the **Node Explorer** window.
Select All	Selects all items on the address list.
Refresh	Refreshes the address list.

Diagnosis Events pane

This pane lists the detailed information of diagnosis events. The list of this pane changes according to the selections on the **Diagnosis Item** pane and the **Diagnosis Address** pane. When you select a specific item on the **Diagnosis Address** pane, the **Diagnosis Events** pane will only display the events of selected address in detail.

The buttons of toolbar are listed in the following table:

Item	Description
	Saves the list of this pane as a .csv file.
	Makes a packet filter based on the IP address or MAC address of selected item in the list. See *Creating Filters* for details.
	Locates the IP address or MAC address of selected item in the list in the **Node Explorer** window.
	Refreshes the list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.

Diagnosis Events columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and set the position, the alignment and the width of the column.

The following table lists and describes the columns of this pane.

Column	Description
Time	The date and time the event occurred.

Severity	The severity of the event, including  ,  ,  ,  .
Type	The type of the event, including performance, security and fault.
Layer	The network layer that the event belongs to.
Event Description	The description of the event, including event reason and packet number, etc.
Source IP Address	The source IP address for the packet. The node is identified by its IP address or by the alias for the IP address if it exists in the Name Table.
Source MAC Address	The source MAC address for the packet. The node is identified by its MAC address or by the alias for the MAC address if it exists in the Name Table.
Destination IP Address	The destination IP address for the packet. The node is identified by its IP address or by the alias for the IP address if it exists in the Name Table.
Destination MAC Address	The destination MAC address for the packet. The node is identified by its MAC address or by the alias for the MAC address if it exists in the Name Table.
Source Port	The source port for the packet.
Destination Port	The destination port for the packet.

Tips You can double-click an item to view detailed packet information in the **Packet** window (You can also right-click an item and select **Display Packet in New Window**). The window will be named with a prefix just the same as **Event Description** and a postfix of **Data Stream of Diagnosis Information**, and the window is just the same as the Packet view (See *Packet view* for more information).

Application layer events

Capsa can diagnoses application layer events as below.

Event	Description	Severity	Possible causes	Solutions
DNS Server Slow Response	The response time from the DNS server is equal to or higher than the threshold.	Performance	Network congestion. The route between client and DNS server is slow. The DNS server is overloaded. Poor DNS server performance.	Check the application services running on the network. Use other DNS server addresses. Check the security and the working status of DNS server. Upgrade the DNS server.
DNS Non-existent Host or Domain	Requested host or domain name cannot be found.	Fault	The IP address or domain name is invalid. The DNS server has incomplete DNS table. Reverse DNS lookup is disabled.	Ensure the IP address or domain name is listed on the DNS table. Check the IP address or domain name is typed correctly. Change DNS server address.
DNS Server Returned Error	DNS server returns an error other than an invalid name.	Fault	Query format error. Query failure. DNS server returns *Not Implemented*, *Refused*, or *Reserved*.	Check if the DNS query is correct. Change DNS server address.
SMTP Server Slow Response	The response time is equal to or higher than the threshold.	Performance	Network congestion. The connection between client and SMTP server is slow. The SMTP server is overloaded. Poor SMTP server performance.	Check the application services running on the network. Update the configurations of route. Check the security and the working status of SMTP server. Upgrade SMTP server.
Suspicious SMTP Conversation	A connection uses TCP port 25 to transmit non-SMTP data.	Security	An application running on TCP port 25 produces non-SMTP traffic.	Check the applications that are using port 25. Check the traffic content of source port and destination port.
SMTP Server Returned Error	An SMTP connection or request is rejected by an SMTP server after a TCP	Fault	The client program executes invalid commands. The client application configures incorrect user name and password. SMTP server is overloaded.	Ensure the client executes correct commands. Check user name and password on the client application. Look for attempted spam.

	connection has already been established.		Incorrect configurations of SMTP server software.	Check the configurations of SMTP server software.
POP3 Server Slow Response	The average response time is equal to or higher than the threshold.	Performance	Network congestion. The connection between client and POP3 server is slow. The POP3 server is overloaded. Poor POP3 server performance.	Check the application services running on the network. Update the configurations of route. Check the security and the working status of POP3 server. Upgrade POP3 server.
Suspicious POP3 Conversation	A connection uses TCP port 110 to transmit non-POP3 traffic.	Security	An application running on TCP port 110 produces non-POP3 traffic.	Check the applications using port 110. Check the traffic content of source port and destination port.
POP3 Server Returned Error	A POP3 connection or request is rejected by a POP3 server after a TCP connection has already been established.	Fault	The client executes invalid commands. The client application configures incorrect user name and password. POP3 server is overloaded. Incorrect configurations of POP3 server software.	Ensure the client executes correct commands. Check user name and password on the client application. Check if POP3 server is attacked. Check the configurations of POP3 server software.
FTP Server Slow Response	The response time is equal to or higher than the threshold.	Performance	Network congestion. The connection between client and FTP server is slow. The FTP server is overloaded. Poor FTP server performance.	Check the application services running on the network. Update the configurations of route. Check the security and the working status of FTP server. Upgrade FTP server.
Suspicious FTP Conversation	A connection uses TCP port 21 to transmit non-FTP traffic.	Security	An application running on TCP port 21 produces non-FTP traffic.	Check the applications using port 21. Check the traffic content of source port and destination port.
FTP Server Returned Error	An FTP connection or request is rejected by an FTP server after a TCP connection has already been established.	Fault	The client executes invalid commands. The client application configures incorrect user name and password. POP3 server is overloaded. The client has a work mode unmatched with the server. Incorrect configurations of FTP server software.	Ensure the client executes correct commands. Check user name and password on the client application. Check if POP3 server is attacked. Ensure the client works in a mode supported by the server. Check the configurations of POP3 server software.
HTTP Client Error	HTTP server returns a 4xx error code other than 404 (Request Not Found) to indicate a client error.	Fault	The request could not be understood by the server due to malformed syntax. Unauthorized request. The access is forbidden. The request method is not allowed. The request times out. The requested URL is too long. Unsupported media type.	Check the syntax in the original request packet that generated the error. Change the request. Change the request or use authorized account. Change the request method. The client repeats the request. Change the requested URL. Modify the media type.
Suspicious HTTP Conversation	A connection uses TCP port 80 to transmit non-HTTP traffic.	Security	An application running on TCP port 80 produces non-HTTP traffic.	Check the applications using port 80. Check the traffic content of source port and destination port.
HTTP Request Not Found	HTTP server returns this error when the requested URL was not found.	Fault	Invalid URL. DNS server table does not contain the map relationship between the entered domain name and mapped IP address.	Check if the URL is valid. Change DNS server address.
HTTP Server Returned Error	HTTP server returns a 5xx error code to indicate a server error; usually the	Fault	Internal server error, not implemented, gateway timeout, or unavailable service. HTTP version is not supported.	Update the configurations of HTTP server. Upgrade the HTTP server to support the version type.

	client's request is valid.			
HTTP Server Slow Response	The average response time is equal to or higher than the threshold.	Performance	Network congestion. The connection between client and HTTP server is slow. The HTTP server is overloaded. Poor HTTP server performance.	Check the application services running on the network. Update the configurations of routes. Check the security and the working status of HTTP server. Upgrade HTTP server.

Tips What diagnosis events will display in the **Diagnosis** view depend on the **Diagnosis Settings** (See *Diagnosis settings* for details).

Transport layer events

Capsa can diagnoses transport layer events as below.

Event	Description	Severity	Possible causes	Solutions
TCP Connection Refused	A client's initial TCP connection attempt is rejected by the host.	Fault	A client is requesting a service that the host does not offer. There are no more available resources on the host to handle the request.	Check for service availability at the host. Check for the maximum number of incoming connections that a host can handle.
TCP Repeated Connect Attempt	A client is attempting multiple times to establish a TCP connection.	Fault	The server does not exist or is not powered on. A client requests a service that is not available on the server. The SYN packet from a client or the ACK packet from a server is lost or damaged. The SYN packet from a client or the ACK packet from a server is blocked by a firewall.	Make sure the server is existent and is powered on. Open the port for the service on the server. Make sure the SYN packet is reaching the server. If the server ACKs, make sure the ACK packet reaches the client. Open the access control policy on the firewall.
TCP Retransmission	The source host is sending another TCP packet with the sequence number identical to or less than that of a previously sent TCP packet to the same destination IP address and TCP port number.	Performance	Network congestion. A packet from a client or the ACK packet from the server is lost because the switch or the router is overloaded. The connection between a client and the server is slow. The buffer of server side overflows. The TCP packet is lost or damaged during transmission. A segment of a segmented TCP packet is lost or damaged during transmission.	Check the application services running on the network. Check the working status of switches and routers. Update the configurations of routes. Check the working status of the host at the receiving side.
TCP Invalid Checksum	The destination host calculates TCP checksum of received packet, which is not identical to the value of TCP checksum field in the received packet.	Fault	The packet is damaged during transmission. Calculating TCP checksum may be disabled if TCP checksum of all packets is wrong. The source stack does not calculate TCP checksum.	Check if there are electromagnetic interference devices on the transmission line or if there is faulty transmission device. Check if it is necessary to enable calculating checksum. Disable TCP Checksum Offload.
TCP Slow Response	The response time for ACK packet is higher than the threshold.	Performance	Network congestion. The connection between the sending host and the receiving host is slow.	Check the application services running on the network. Update the configurations of routes. Check if the ACK packet is lost or

			The ACK packet is lost or damaged during transmission. A router between the sending host and the receiving host is overloaded.	damaged. Upgrade the router.
TCP Duplicated Acknowledgement	There are at least three packets have identical ACK number and SEQ number.	Performance	TCP segment is lost due to network congestion. Packets are lost due to other network problems. The other side of TCP connection is unresponsive	Check if there is network congestion. Check if packets are lost due to other network problems. Check if the hosts of TCP connection are working regularly.
TCY SYN Storm	A lot of TCP SYN packets are being sent at a speed higher than the threshold.	Security	There is DOS or DDOS attack.	Check if there is DOS or DDOS attack.
TCP Header Offset Error	TCP header offset is less than 5.	Security	The source host is sending faulty TCP packets.	Check if there is attack on the source host. Check if the progresses are regular.
TCP Port Scan	A local or remote host scans TCP ports, the number of which is higher than the threshold.	Security	A local host infects worm to automatically scan TCP ports. Scan software scans TCP ports.	Check if the host is infected with worm. Check if there is manual scanning on the source host.

Network layer events

Capsa can diagnoses network layer events as below.

Event	Description	Severity	Possible causes	Solutions
IP Invalid Checksum	The destination host calculates IP checksum of received packet, which is not identical to the value of IP checksum field in the received packet.	Fault	The packet is damaged during transmission. Calculating IP checksum may be disabled if IP checksum of all packets is wrong. The source stack does not calculate IP checksum.	Check if there are electromagnetic interference devices on the transmission line or if there is faulty transmission device. Check if it is necessary to enable calculating checksum. Disable IP Checksum Offload.
IP Too Low TTL	The IP Time-To-Live (TTL) is equal to or less than the threshold indicating that the packet can only traverse that many routers before it is discarded.	Fault	Network loop. The originating IP host transmitted the packet with a low TTL.	Check for routing table information. There is something wrong on the source host.
IP Address Conflict	A host detects that another device is trying to use its IP address and notifies the device by ARP information.	Security	A device tries to use an IP address which has been used.	Assign an IP address to the device.
ICMP Destination Unreachable	A router is reporting to the source host unreachable messages, except network unreachable, host unreachable and	Fault	The transport protocol used by source host is unavailable on the destination host or on the router. Segmenting is disabled on the router. The routing is failed. The router cannon forward the	Change the transport protocol on the source host or add transport protocols supported by the router and the destination host. Check and update the configurations of the router.

	port unreachable messages.		packets with specified Type of Service (ToS). Limited by the communication management rules on the router.	
ICMP Network Unreachable	A router is reporting to the source host that a network is unavailable or the path for destination network is unavailable.	Fault	The router is not configured with a default route. The destination network does not exist. The router cannot find the path to the destination network. The number of hops to destination network exceeds the maximum hop limit specified by the routing protocol on the router.	Add a default route for the router. Add a route for the destination network to the router, or add a default route. Add a default route to the router. Change the routing protocol on the router.
ICMP Host Unreachable	A router is reporting to the source host that the destination host is unavailable.	Fault	The destination host does not exist. The destination host is not powered on.	Check the existence of the destination host. Check if the destination host is powered on.
ICMP Port Unreachable	The destination host or a router is reporting to the source host that the requested port is inactive.	Fault	The service for the requested port is not enabled. The service for the requested port is in error. A firewall blocks the access to the port.	Enable the service for the requested port. Check the configurations for the service. Enable the access control policy on the firewall or the router for the port.
ICMP Host Redirect	A router is reporting to the source host that it should use an alternate route for the destination host.	Performance	A host in LAN uses an external domain to access internal server after port mapping configuration. There is an ICMP attack.	Access the server using an internal IP address. Look for the attack source address according to the packet.
ICMP Network Redirect	A router is reporting to the source host that it should use an alternate route for the destination network.	Performance	A host in LAN uses an external domain to access internal server after port mapping configuration. There is an ICMP attack.	Access the server using an internal IP address. Look for the attack source address according to the packet.
ICMP Source Quench	A router or the destination host sends an ICMP source quench packet to the source host.	Fault	Network congestion. The destination host has inadequate space or the service is not available. The router has inadequate cache space. There is DOS or DDOS attack.	Check the application services running on the network. Check the destination host and close unnecessary services. Enlarge the size of route cache. Check if there are malicious attacks from the source host.

Data link layer events

Capsa can diagnoses data link layer events as below.

Event	Description	Severity	Possible causes	Solutions
Invalid ARP Format	Unable to operate correctly on the Ethernet, and violate the frame format defined by RFC. For example, source MAC address is multicast address, or the address information in ARP header does not match that in	Security	The address information in ARP header is falsified or forged for attack.	Check if there is ARP attack.

	Ethernet MAC header.			
ARP Request Storm	In a predetermined sampling duration, the number of ARP request packets per second is higher than the threshold.	Security	Check if the source host sends a lot of ARP requests. The host infects virus which is automatically performing ARP scan. A scan application is performing ARP scan. The port for capturing traffic is not mirrored or the machine with the program is not connected with the mirrored port.	Use antivirus software to scan the host which sends a lot of ARP requests. Close the application which performs ARP scan. Mirror the port which is for capturing traffic and install the program on the machine which is connected with the mirrored port.
ARP Scan	In a predetermined sampling duration, the percentage of unresponsive ARP request packets is equal to or higher than the threshold.	Security	The source host sending ARP packets has a program performing scan. There is monitor application on the network. The host infects virus which is automatically performing ARP scan. A scan application is performing ARP scan.	Check if the source host has a program performing scan. End the monitor process. Use antivirus software to scan the host which performs ARP scan. Close the scan application.
ARP Too Many Unrequested Responses	In a predetermined sampling duration, the number of unrequested ARP response packets of a host is equal to or higher than the threshold.	Security	There is ARP spoofing on the network. The program is installed on a central switching device and ARP request packets are isolated.	Check if there is ARP spoofing on the host which sends a lot of ARP response packets.

Protocol view

The **Protocol** view visually provides statistics of the network traffic on the basis of protocols. By default, protocols are displayed in an expanded hierarchical structure. Each protocol has its own color that you can easily find out your target protocol in the list by color. You can click any column header to sort the list.

The items on the protocol list changes along with the selection in the **Node Explorer** window. When you select the root node, **Protocol Explorer** node, **Physical Explorer** node or **IP Explorer** node, the **Protocol** view will present all protocols on the network and their statistical information. When you select a specific node in the Node Explorer window, the Protocol view will only present the protocols relating to the node and their statistical information.

When you select a specific item on the protocol list, the lower pane tabs will provide detailed information about the item. See *Protocol lower pane tabs* for details. You can also double-click a protocol to view detailed packet information in the **Packet** window which is named with the protocol and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar:

Item	Description
	Exports all of the protocol statistics as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected protocol. See *Creating Filters* for details.

	Locates the selected protocol in the **Node Explorer** window.
	Refreshes the protocol list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the protocol number in the list. The name changes along with the selection in the **Node Explorer** window.

Protocol columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Protocol columns* for details.

The following table lists and describes the columns of **Protocol** view.

Pop-up menu

Right-click the protocol list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the protocol type in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Protocol Statistics	Saves current list of the protocol statistics as a .csv file.
Find	Calls out **Find** dialog box to search only on the protocol list.
Make Filter	Makes a packet filter based on the selected protocol. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected protocol. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected protocol. See *Creating Alarms* for details.
Locate in Node Explorer	Locates the selected protocol in the **Node Explorer** window.
Select All	Selects all items on the protocol list.
Refresh	Refreshes the protocol list.

Protocol lower pane tabs

The **Protocol** lower pane tabs display the details of the protocol selected on the **Protocol** view. By default, the protocol lower pane is visible. You can click **Details** button on the **Protocol** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The tabs showing on the lower pane are different with different selection in the **Node Explorer** window:

- Choosing the root node or any nodes on the **Protocol Explorer**, the lower pane includes **Physical Endpoint** tab and **IP Endpoint** tab.
    - The **Physical Endpoint** tab lists all MAC address nodes and their traffic information using the protocol selected on the

Protocol view. The toolbar and columns are just the same as those on **Physical Endpoint** view. See *Physical Endpoint* for details.

- The **IP Endpoint tab** lists all IP address nodes and their traffic information about the protocol selected on the **Protocol** view. The toolbar and columns are just the same as those on **IP Endpoint** view. See *IP Endpoint* for details.
- You can double-click any item on the node list to view detailed packet information in the **Packet** window which is named with the protocol and the node name and is just the same as the **Packet** view (See *Packet view* for more information).

- Choosing any nodes except MAC address and IP address nodes on the **Physical Explorer**, the lower pane includes **Physical Endpoint** tab and **Physical Conversation** tab.
  - The **Physical Conversation** tab lists all MAC address conversations about the protocol selected on the **Protocol** view. The toolbar and columns are just the same as those on **Physical Conversation** view. See *Physical Conversation* for details.
  - You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the protocol and the conversation and is just the same as the **Packet** view (See *Packet view* for more information).
- Choosing MAC address nodes on the **Physical Explorer**, the lower pane includes **Physical Conversation** tab and **IP Conversation** tab.
  - The **IP Conversation** tab lists all IP address conversations using the protocol selected on the **Protocol** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
  - You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the protocol and the conversation and is just the same as the **Packet** view (See *Packet view* for more information).
  - Note The **IP Conversation** tab will have statistics only when there is IP address node under the MAC address node on the **Physical Explorer**, or else there are no items on this tab.
- Choosing any nodes except IP address nodes on the **IP Explorer**, the lower pane includes **IP Endpoint** tab and **IP Conversation** tab.
- Choosing IP address nodes on the **Physical Explorer** or **IP Explorer**, the lower pane includes **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.
  - The **TCP Conversation** tab lists the conversations using TCP protocol. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
  - The **UDP Conversation** tab lists the conversations using UDP protocol. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.
  - You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the protocol and the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

In combination with **Node Explorer**, you can conveniently view the statistics that you are care about.

Protocol columns

The following table lists and describes the columns of **Protocol** view.

Column	Description
Name	Protocol name.
Bytes	Total bytes of the packets using this protocol.
Packets	The number of packets using this protocol.
Bps	Total Bytes per second.
bps	Total Bits per second.
pps	The number of packets per second.
Bytes%	Percentage of total bytes of this protocol type.
Packets%	Percentage of packets of this protocol type.
Bps%	Percentage of bytes per second.
pps%	Percentage of packets per second.

Physical Endpoint view

The **Physical Endpoint** view hierarchically shows statistics of the network traffic on the basis of MAC addresses or node groups of MAC address, to help you find useful information on MAC addresses. For example, you can find the physical endpoints with the largest traffic volume or check if there is any broadcast storm or multicast storm on the network.

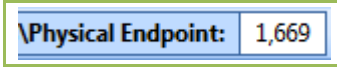
Note The **Physical Endpoint** view will not be available when you select IP address nodes on the **Physical Explorer** or any nodes on the **IP Explorer**.

When you select a specific item in the node list on the **Physical Endpoint** view, the lower pane tabs will provide detailed information about the item. See *Physical Endpoint lower pane tabs* for details. You can double-click an item on the MAC address list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Shows the node list in hierarchical type or in flat type.
	Exports current MAC address statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.

	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the nodes in the list. The name changes along with the selection in the **Node Explorer** window.

Physical Endpoint columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the MAC address list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Ping	Only available with right-clicking IP address node. Calls out the build-in **Ping Tool** to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

Physical Endpoint lower pane tabs

The **Physical Endpoint** lower pane tabs display the details of the node selected on the **Physical Endpoint** view. By default, the lower pane is visible. You can click **Details** button on the **Physical Endpoint** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

By default, there is only a **Physical Conversation** tab on the lower pane.

- The **Physical Conversation** tab lists all MAC address conversations of the node selected on the **Physical Endpoint** view. The toolbar and columns are just the same as those on **Physical Conversation** view. See *Physical Conversation* for details.
    - You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

When an IP address node under an MAC address node is selected on the **Physical Endpoint** view, the lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **Physical Endpoint** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **Physical Endpoint** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **Physical Endpoint** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.
    - You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Endpoint columns

The following table lists and describes the columns for endpoint views, including **Physical Endpoint** view, **IP Endpoint** view, **ARP Attack** view, **Worm** view, **DoS Attacking** view, **DoS Attacked** view, and **TCP Port Scan** view.

Column	Description
Name	The name of the node. The node may be MAC addresses, IP addresses, node groups or resolved names.
Bytes	Total bytes sent and received by the node.
Packets	The number of packets sent and received by the node.
Internal Bytes	Only available for node group items. Total bytes transmitted inside the node group (See *Node Group* for more information).
Internal Packets	Only available for node group items. Total packets transmitted inside the node group.
Broadcast Bytes	Total broadcast bytes sent and received by the node.
Broadcast Packets	Total broadcast packets sent and received by the node.
Multicast Bytes	Total multicast bytes sent and received by the node.
Multicast Packets	Total multicast packets sent and received by the node.
bps	Bits per second.
Bytes/s	Bytes per second.
Packets/s	Packets per second.
Bytes In	Received bytes.
Packets In	Received packets.
Bytes Out	Sent bytes.
Packets Out	Sent packets.
Bytes Out/In (%)	The ratio of sent bytes to received bytes.
Packets Out/In (%)	The ratio of sent packets to received packets.
IP Count	The number of IP addresses. Only available for node group items and MAC address items in the list.
Physical Conversation	The number of physical conversations.
IP Conversation	The number of IP conversations.
TCP Conversation	The number of TCP conversations.
UDP Conversation	The number of UDP conversations.
TCP SYN Sent	The number of sent packets with SYN flag set to be 1.
TCP SYN Received	The number of received packets with SYN flag set to be 1.
TCP SYNACK Sent	The number of sent packets with ACK and SYN flags both set to be 1. The value of this item should be equal to that of **TCP SYN Received** for a normal TCP connection establishment.
TCP SYNACK	The number of received packets with ACK and SYN flags both set to be 1. The value of this item should be

Received	equal to that of **TCP SYN Sent** for a normal TCP connection establishment.
Location	Country or Area that the node belongs to.
TCP FIN Sent	The number of sent packets with FIN flag set to be 1.
TCP FIN Received	The number of received packets with FIN flag set to be 1. The value of this item should be equal to that of **TCP FIN Sent** for a normal TCP connection close.
TCP Reset Sent	The number of sent packets with RST flag set to be 1.
TCP Reset Received	The number of received packets with RST flag set to be 1.
Bytes%	Percentage of total bytes sent and received by the node.
Packets%	Percentage of packets sent and received by the node.
Internal Bytes%	Percentage of bytes sent and received inside the node group.
Internal Packets%	Percentage of packets sent and received inside the node group.
Broadcast Bytes%	Percentage of broadcast bytes.
Broadcast Packets%	Percentage of broadcast packets.
Multicast Bytes%	Percentage of multicast bytes.
Multicast Packets%	Percentage of multicast packets.
Bytes In%	Percentage of received bytes.
Packets In%	Percentage of received packets.
Bytes Out%	Percentage of sent bytes.
Packets Out%	Percentage of sent packets.
bps%	Percentage of bits per second.
Bps%	Percentage of bytes per second.
pps%	Percentage of packets per second.
Broadcast packets/s Peak	The peak value of broadcast packets per second.
Multicast packets/s Peak	The peak value of multicast packets per second.
Bytes In/s Peak	The peak value of bytes received per second.
Packets In/s Peak	The peak value of packets received per second.
Bytes Out/s Peak	The peak value of bytes sent per second.
Packets Out/s Peak	The peak value of packets sent per second.
TCP SYN Sent/s Peak	The peak value of packets with SYN flag set to be 1 sent per second.
TCP SYN Received/s Peak	The peak value of packets with SYN flag set to be 1 received per second.

IP Endpoint view

The **IP Endpoint** view hierarchically shows statistics of the network traffic on the basis of IP addresses or node groups of IP address, to help you find useful information on IP addresses. For example, you can find the IP address with the largest traffic volume on a local network.

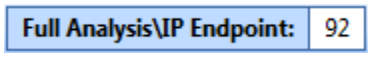
Note The **IP Endpoint** view will not be available when you select node group or MAC address on the **Physical Explorer**.

When you select a specific item in the node list on the **IP Endpoint** view, the lower pane tabs will provide detailed information about the item. See *IP Endpoint lower pane tabs* for details. You can double-click an item in the node list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description

	Shows the node list in hierarchical type or in flat type.
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the Name Table for selected node. See *Name Table* for details.
	Locates the selected node in the Node Explorer window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to Manually Refresh, display will update only when the Refresh button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the nodes in the list. The name changes along with the selection in the Node Explorer window.

IP Endpoint columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Exports current statistical list as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address in the node list. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Ping	Only available with right-clicking IP address node. Calls out the build-in **Ping Tool** to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

IP Endpoint lower pane tabs

The **IP Endpoint** lower pane tabs display the details of the node selected on the **IP Endpoint** view. By default, the lower pane is visible.

You can click **Details** button on the **IP Endpoint** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **IP Endpoint** lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **IP Endpoint** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **IP Endpoint** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **IP Endpoint** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.

  You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Physical Conversation view

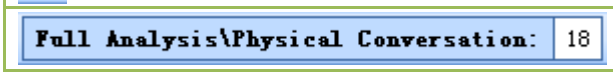
The **Physical Conversation** view shows statistics of the network traffic on the basis of MAC address conversations, to help you know the traffic status between MAC addresses of the network.

Note The **Physical Conversation** view will not be available when you select IP address nodes on the **Physical Explorer** or any nodes on the **IP Explorer**.

You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current conversation list as a .csv file.
	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
	Refreshes the conversation list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the conversations in the list. The name changes along with the selection in the **Node Explorer** window.

Physical Conversation columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Conversation columns* for details.

Pop-up menu

Right-click the conversation list on this view to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the conversation in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Conversation Statistics	Saves current list as a .csv file.
Find	Calls out **Find** dialog box to search only in the conversation list.
Make Filter	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
Resolve Address	Not available in this view.
Add to Name Table	Adds an alias to the **Name Table** for the node of selected conversation. See *Name Table* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the node of selected conversation. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the node of selected conversation. See *Creating Alarms* for details.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Select All	Selects all items in the conversation list.
Refresh	Refreshes the conversation list.

Conversation columns

The following table lists and describes the columns of **Conversation** view, including **Physical Conversation** view, **IP Conversation** view, **TCP Conversation** view, **UDP Conversation** view, and **Suspicious Conversation** view.

Column	Description
Node 1 ->	The source address of the first packet in the conversation.
<- Node 2	The destination address of the first packet in the conversation.
Duration	Duration of the conversation, that is, from the timestamp of the first packet to the timestamp of the last packet in the conversation.
Bytes	Total bytes sent and received in this conversation.
Bytes ->	Bytes sent from node 1 to node 2.
<- Bytes	Bytes sent from node 2 to node 1.
Packets	The number of packets sent and received in this conversation.
Packets ->	The number of packets sent from node 1 to node 2.
<- Packets	The number of packets sent from node 2 to node 1.
Start Time	The timestamp of the first packet in the conversation.
Start Time ->	The timestamp of the first packet that is sent from node 1 to node 2.
<- Start Time	The timestamp of the first packet that is sent from node 2 to node 1.
End Time	The timestamp of the last packet in the conversation.
End Time ->	The timestamp of the last packet that is sent from node 1 to node 2.
<- End Time	The timestamp of the last packet that is sent from node 2 to node 1.
Protocol	The protocol for the conversation.

IP Conversation view

The **IP Conversation** view shows statistics of the network traffic on the basis of IP address conversations, to help you know the traffic status between IP addresses of the network.

Note The **IP Conversation** view will not be available when you select node group or MAC address on the **Physical Explorer** or some protocol nodes on the **Protocol Explorer**.

When you select a specific item in the conversation list on the **IP Conversation** view, the lower pane tabs will provide detailed information about the item. See *IP Conversation lower pane tabs* for details. You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
	Refreshes the conversation list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the conversations in the list. The name changes along with the selection in the **Node Explorer** window.

IP Conversation columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Conversation columns* for details.

Pop-up menu

Right-click the conversation list on this view to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the conversation in the Packet window which is just the same as the Packet view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Conversation Statistics	Exports current statistical list as a .csv file.
Find	Calls out Find dialog box to search only in the conversation list.
Make Filter	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
Make Graph	Makes a graph in the Dashboard view on the basis of the node of selected conversation. See *Creating*

	Graphs for details.
Make Alarm	Makes an alarm on the basis of the node of selected conversation. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the Name Table for the node of the selected conversation. See *Name Table* for details.
Resolve Address	Resolves the host name of the node of selected conversation.
Locate in Node Explorer	Locates the node of selected conversation in the Node Explorer window.
Ping	Calls out the build-in Ping Tool to ping the node of selected conversation.
Select All	Selects all items in the conversation list.
Refresh	Refreshes the conversation list.

IP Conversation lower pane tabs

The **IP Conversation** lower pane tabs display the details of the conversation selected on the **IP Conversation** view. By default, the lower pane is visible. You can click **Details** button on the **IP Conversation** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **IP Conversation** lower pane provides **TCP Conversation** tab and **UDP Conversation** tab.

- The **TCP Conversation** tab lists the conversations using TCP protocol of the conversation selected on the **IP Conversation** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the conversation selected on the **IP Conversation** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.
    - You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

TCP Conversation view

The **TCP Conversation** view shows statistics of the network traffic on the basis of TCP conversations. TCP conversation is identified by the flag fields set to be 1 or the load length of greater than 0.

Note The **TCP Conversation** view will not be available when you select node group or MAC address on the **Physical Explorer** or protocol nodes not belonging to TCP protocol on the **Protocol Explorer**.

When you select a specific item in the conversation list on the **TCP Conversation** view, the lower pane tabs will provide detailed information about the item. See *TCP Conversation lower pane tabs* for details. You can double-click any item in the conversation list to open **TCP Flow Analysis** window to view detailed conversation information. See *TCP Flow Analysis window* for details.

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.

	Refreshes the conversation list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the conversations in the list. The name changes along with the selection in the **Node Explorer** window.

TCP Conversation columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Conversation columns* for details.

Pop-up menu

Right-click the conversation list on this view to get a pop-up menu with items as follows:

Item	Description
Packet/TCP Flow Details	To open TCP Flow Analysis window. See *TCP Flow Analysis window* for details.
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Conversation Statistics	Exports current statistical list as a .csv file.
Find	Calls out Find dialog box to search only in the conversation list.
Make Filter	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
Make Graph	Makes a graph in the Dashboard view on the basis of the node of selected conversation. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the node of selected conversation. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the Name Table for the node of the selected conversation. See *Name Table* for details.
Resolve Address	Resolves the host name of the node of selected conversation.
Locate in Node Explorer	Locates the node of selected conversation in the Node Explorer window.
Ping	Calls out the build-in Ping Tool to ping the node of selected conversation.
Select All	Selects all items in the conversation list.
Refresh	Refreshes the conversation list.

Lower pane tabs

When you select a specific item in the conversation list on the **TCP Conversation** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **TCP Conversation** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

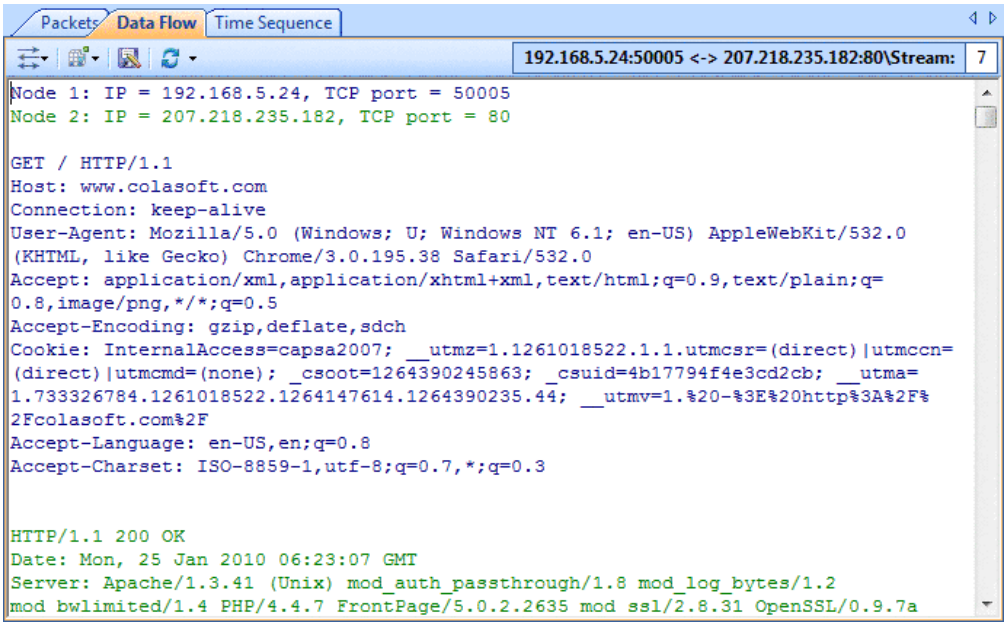
The **TCP Conversation** lower pane includes **Packets** tab, **Data Flow** tab and **Time Sequence** tab.

- The **Packets** tab lists all packets for the TCP conversation selected in the **TCP Conversation** view. The toolbar and columns are just the same as those on **Packet** view. See *Packet view* for details.
- The **Data Flow** tab provides reassembled data flow for the TCP conversation selected in the **TCP Conversation** view. See *Data Flow tab* for details.

- The **Time Sequence** tab displays TCP conversation in time-sequential order. See *Time Sequence tab* for details.

Data Flow tab

This tab presents original information of the conversation selected on the **TCP Conversation** view. A TCP conversation realized on the network may be sliced into multiple packets, and the packets are transmitted over the network out of order. Capsa organizes these packets in correct orders and reconstructs these packets into a TCP flow. The conversations using TCP protocol, including Web (HTTP), Email (SMTP/POP3), FTP and MSN and so on, can be reconstructed. The **Data Flow** tab appears as follows:

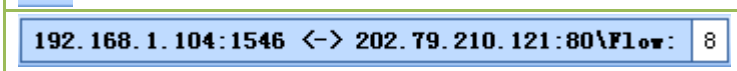


Note You may get unreadable symbols because some data are encrypted in transmission.

By default, the **Data Flow** tab presents the whole data flow between two nodes. You can distinguish the data of different nodes by colors, blue is for data from node 1 to node 2 and green is for data from node 2 to node 1.

Toolbar

The following table lists and describes the items on the toolbar:

Item	Description
	To choose flow direction for displaying the data flow: Bidirectional: Displays the whole data flow. Node 1 to Node 2: Only displays the data from node 1 to node 2. Node 2 to Node 1: Only displays the data from node 2 to node 1.
	Limits the first number of packets in the conversation to display on the **Data Flow** tab.
	Saves the data flow as a .txt file.
	Refreshes the data flow. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	The number of packets displayed in the flow.

Pop-up menu

Right-click the conversation list on this view to get a pop-up menu with items as follows:

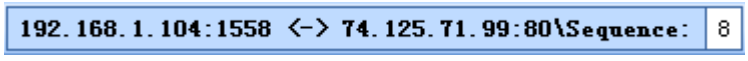
Item	Description
Copy	Copies the selected content to the clipboard.
Line Wrap	Auto-wraps.
Decoding	Chooses a decoding format to view the data flow.
Find	Calls out **Find** dialog box to search only on this tab.
Find Next	Finds next search result.
Select All	Selects all content of the data flow.
Refresh	Refreshes the data flow.

Time Sequence tab

The **Time Sequence** tab provides a time sequence diagram of the TCP conversation selected on the **TCP Conversation** view. You can view the diagram to understand the packet transmission mechanism in a TCP conversation. Grey is for packet from node 1 to node 2 and yellow is for packet from node 2 to node 1.

Toolbar

There are only three items on the toolbar of this tab, described as below:

Item	Description
	The type to display the sequence number of the byte flow in data transmission, including: Show Absolute Seq: Shows the real sequence number in the packet. Show Relative Seq: Shows relative sequence number with the first packet of the conversation being 0.
	Refreshes the diagram. If the interval is set to Manually Refresh, display will update only when the Refresh button is clicked.
	The number of packets of the conversation.

Time sequence diagram

The time sequence diagram is organized by six columns which are described as below.

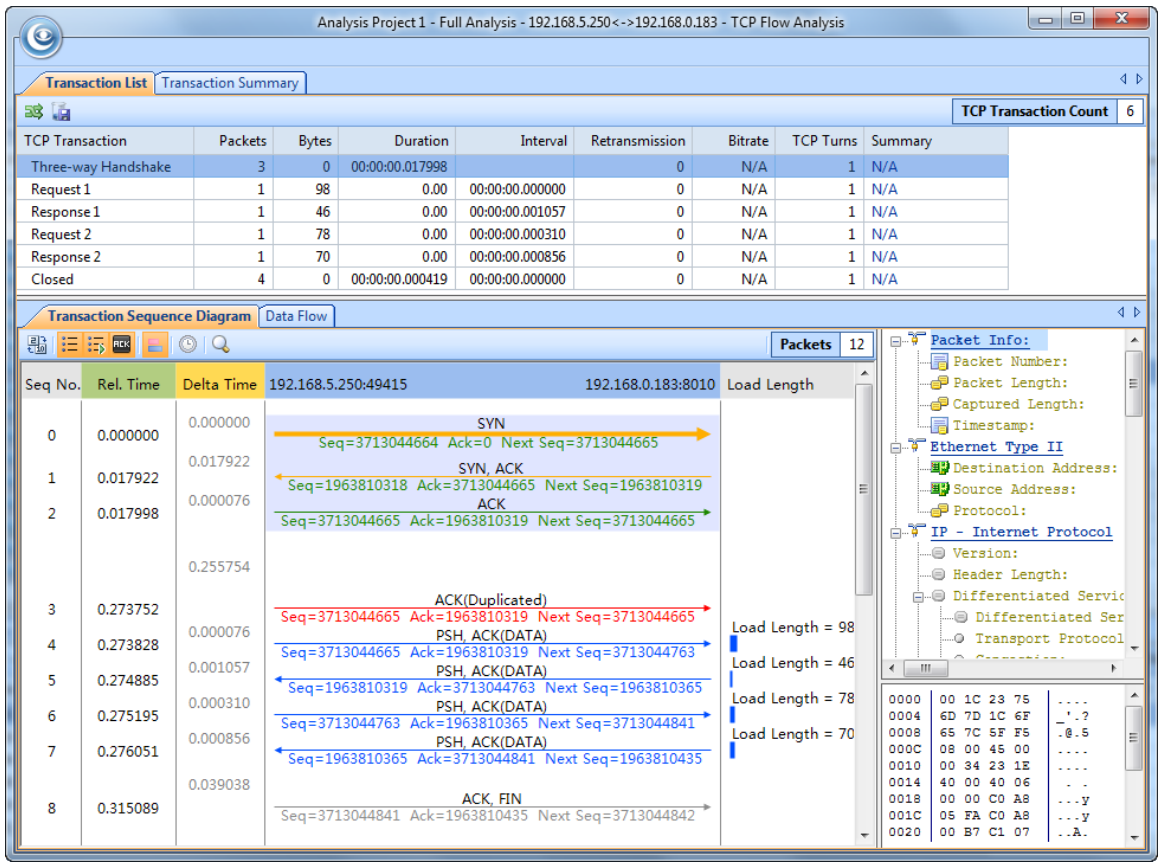
Column	Description
Relative Time	The time from the timestamp of selected packet to that of the first packet in the conversation, with the first packet of the conversation being set as the reference object.
Summary->	The information about sequence number, acknowledgement number, next sequence number of the packet sent by node 1.
Node 1->	The window size information of node 1. A window size of 0 indicates that Node 2 should stop transmitting.
Flag and Load Length	Flags that are control flags in TCP segment header and load length which is the size of the data portion of TCP segment.
<- Node 2	The window size information of node 2. A window size of 0 indicates that Node 1 should stop transmitting.
<-Summary	The information about sequence number, acknowledgement number, next sequence number of the packet sent by node 2.

You can double-click the conversation selected on the **TCP Conversation** view to open *TCP Flow Analysis window* to know the details of the conversation.

TCP Flow Analysis window

To open **TCP Flow Analysis** window, double-click any item in the conversation list on the **TCP Conversation** view or right-click any item and select **Packet/TCP Flow Details**.

The **TCP Flow Analysis** window appears as below.



The **TCP Flow Analysis** window provides detailed transaction information, packet information, and data flow information of the conversation selected on the **TCP Conversation** view, including two views:

- *Transaction List*
- *Transaction Summary*

Transaction List

The **Transaction List** view includes an upper pane which provides transaction list information about the conversation selected on the **TCP Conversation** view and a lower pane which contains **Transaction Sequence Diagram** tab and **Data Flow** tab.

Transaction List toolbar

There are only three items on the toolbar of this tab, described as below

Item	Description
	Reverses the transaction list to reverse between requests and responses.
	Saves the packets of selected transaction in the transaction list. You can save packets in any format selected from the *Save as type* drop-down list box.

TCP Transaction Count 8	Shows the number of the transactions.

Transaction List columns

The following table lists and describes the columns of **Transaction List**.

Column	Description
TCP Transaction	Lists the name of a transaction, including **Three-way Handshake**, **Request** count, **Response** count, and **Closed**.
Source	The source of the transaction, including IP address and port number.
Destination	The destination of the transaction, including IP address and port number.
Packets	The number of packets for the transaction.
Bytes	Total bytes of load length which is the size of the data portion of TCP segment.
Duration	Duration of the transaction.
Interval	The interval between two adjacent transactions.
Retransmission	The retransmission times for the transaction.
Bitrate	The bitrate of the transaction. Only available when the packet number is greater than or equal to 10.
TCP Turns	The times of TCP turns. TCP turn means the number of paired ACKnowledgement packet and packet with data portion, plus1 when there is a packet with data portion at the tail of a transaction. TCP turn will be 1 when there is only one pair of adjacent ACKnowledgement packets. There are at least one TCP turn in one transaction.
Start Time	The time when the transaction started.
End Time	The time when the transaction ended.
Summary	Summary for the transaction.

When a specific transaction is selected, the Transaction Sequence Diagram tab will auto-scroll to display corresponding transaction information in diagram type.

Transaction Sequence Diagram

When a transaction item is selected on the transaction list, the Transaction Sequence Diagram will display corresponding packet information for the transaction with a background color of grey.

On the diagram, one horizontal line with arrow represents one packet and the arrow represented the direction of the packet. The green lines represents packets of Three-way Handshake, the blue ones represent packets with application data, the yellow ones represent ACKnowledgement packet, and the red ones represent packets with something wrong, lick retransmission, repeated ACKnowledgement and so on.

Click an arrow, the arrow becomes thick yellow and the right section will display the decoding information of the packet.

The following table lists and describes the buttons on the toolbar of this tab:

Item	Description
	Displays relative packet number from 0 to n or displays real packet number in the project buffer.
	Displays Sequence Number of the packet.
	Displays Next Sequence Number of the packet.
	Displays Ack Number of the packet.
	Displays load length information of the packet.

	Sets relative time for the packets.
	Calls out **Find** dialog box to search in the packet decoding section on the right. When finding the result, the horizontal line for the packet will be highlighted.

Data Flow tab

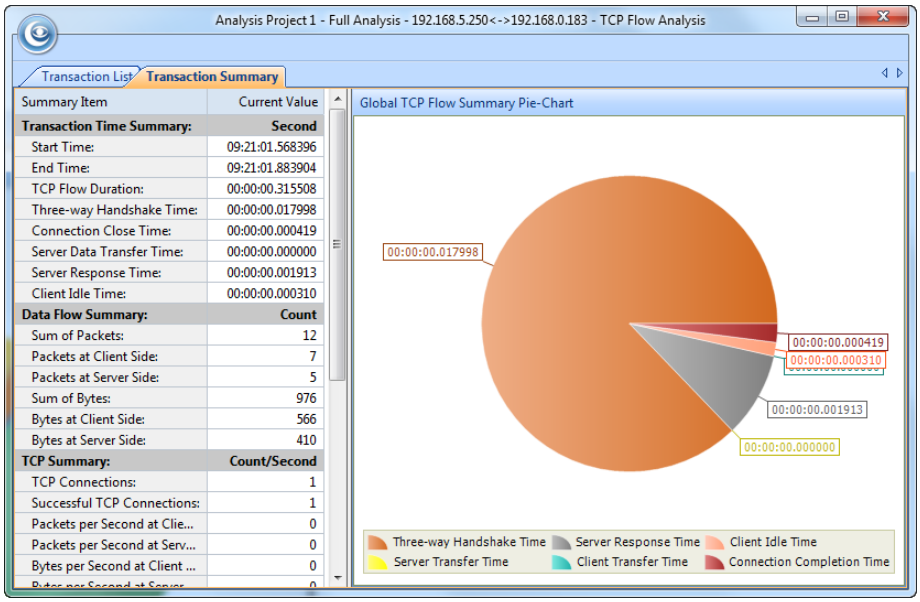
This tab presents original information of the transaction selected on the transaction list. See *Data Flow tab* for more information.

Note You may get unreadable symbols because some data are encrypted in transmission.

Transaction Summary

The **Transaction Summary** view displays TCP transaction statistics on the left pane and related metrics with pie chart on the right pane.

The **Transaction Summary** view appears as below.



The left pane provides statistical items listed as below:

- Transaction Time Summary: Includes Start Time, End Time, TCP Flow Duration, Three-way Handshake Time, Connection Close Time, Server Data Transfer Time, Server Response Time, Client Idle Time
- Data Flow Summary: Includes Sum of Packets, Packets at Client Side, Packets at Server Side, Sum of Bytes, Bytes at Client Side, Bytes at Server Side
- TCP Summary: Includes TCP Connections, Successful TCP Connections, Packets per Second at Client Side, Packets per Second at Server Side, Bytes per Second at Client Side, Bytes per Second at Server Side, Sum of Client Retransmissions, Sum of Server Retransmissions, Lost TCP Segments at Client Side, Lost TCP Segments at Server Side, Max Ack Time, Min Ack Time, Average Ack Time at Client Side, Average Ack Time at Server Side
- TCP Transaction Summary: Includes Sum of Transactions, Transaction Processing Time, Average Transaction Processing Time, Max Transaction Processing Time, Min Transaction Processing Time

The right pane prevents a pie chart of global TCP flow statistics, including six items on the pie chart: Three-way Handshake Time, Server Response Time, Client Idle Time, Server Transfer Time, Client Transfer Time, and Connection Completion Time, and visually showing

the TCP flow time information of the TCP conversation selected on the TCP Conversation view.

UDP Conversation view

The **UDP Conversation** view provides you with all UDP conversation statistics of the network.

Note The **UDP Conversation** view will not be available when you select node group or MAC address on the **Physical Explorer** or the protocol nodes other than UDP on the **Protocol Explorer**.

When you select a specific item in the conversation list on the **UDP Conversation** view, the lower pane tabs will provide detailed information about the item. See *UDP Conversation lower pane tabs* for details. You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
	Refreshes the conversation list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of the conversations in the list. The name changes along with the selection in the **Node Explorer** window.

UDP Conversation columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Conversation columns* for details.

Pop-up menu

Right-click the conversation list on this view to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the conversation in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Conversation Statistics	Exports current statistical list as a .csv file.
Find	Calls out **Find** dialog box to search only in the conversation list.
Make Filter	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.

Make Graph	Makes a graph in the **Dashboard** view on the basis of the node of selected conversation. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the node of selected conversation. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the node of the selected conversation. See *Name Table* for details.
Resolve Address	Resolves the host name of the node of selected conversation.
Locate in Node Explorer	Locates the node of selected conversation in the **Node Explorer** window.
Ping	Calls out the build-in **Ping Tool** to ping the node of selected conversation.
Select All	Selects all items in the conversation list.
Refresh	Refreshes the conversation list.

UDP Conversation Lower pane tabs

When you select a specific item in the conversation list on the **UDP Conversation** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **TCP Conversation** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **UDP Conversation** lower pane includes **Packets** tab and **Data** tab.

- The **Packets** tab lists all packets for the UDP conversation selected in the **UDP Conversation** view. The toolbar and columns are just the same as those on **Packet** view. See *Packet view* for details.
- The **Data** tab provides original data for the UDP conversation selected in the **UDP Conversation** view. The toolbar and columns are just the same as those on **Data Flow** tab on the **TCP Conversation** view. See *Data Flow tab* for details.

Matrix view

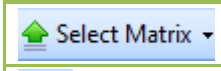
The **Matrix** view dynamically shows the network traffic status in graph. The graph consists of nodes and lines, the nodes representing the nodes on the network and the lines representing the conversations on the network. The number after the node represents the number of peer hosts. Move your mouse over a node, the nodes and the lines connected with the node will be yellow highlighted, and traffic statistical information about the node will be displayed. Move your mouse over a line, the line and two nodes connected by the line will be yellow highlighted, and traffic statistical information about the conversations will be displayed.

When there are too many nodes on the graph, you can drag the node to another position to view the traffic status clearly and you can also hide unnecessary nodes.

You can also select other types of matrix or create a new matrix through the left pane. See *Matrix left pane* for details.

Toolbar

The following table lists the items on the toolbar:

Item	Description
	Click the little triangle to choose a matrix type in the list. Simply click the button to hide or show the matrix left pane.
	Sets the font size of the nodes in the matrix graph.
	Sets the color for the items of the matrix graph.
	Refreshes the matrix graph or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.

Show Nodes/Total Nodes: 71/147	Shows the count of nodes in the matrix graph. The first number is the count of showed nodes and the second number is the count of total nodes.

Pop-up menu

Right-click a selected node on the matrix graph to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the conversation in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Re-arrange Nodes	Rearranges the position of nodes.
Hide	Hides selected node, selected node and its peer nodes, or other nodes.
Resolve Address	Resolves the host name of the selected node or the selected node and its peer nodes.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Display All Hidden Nodes	Shows all user-hidden nodes.

Matrix left pane

The matrix left pane contains three sections as follows:

- *Matrix type*
- *User Hidden Nodes*
- *Invisible Nodes*

Matrix type

There are four types of matrix by default:

- Top 100 Physical Conversation
- Top 100 Physical Node
- Top 100 IPv4 Conversation
- Top 100 IPv4 Node

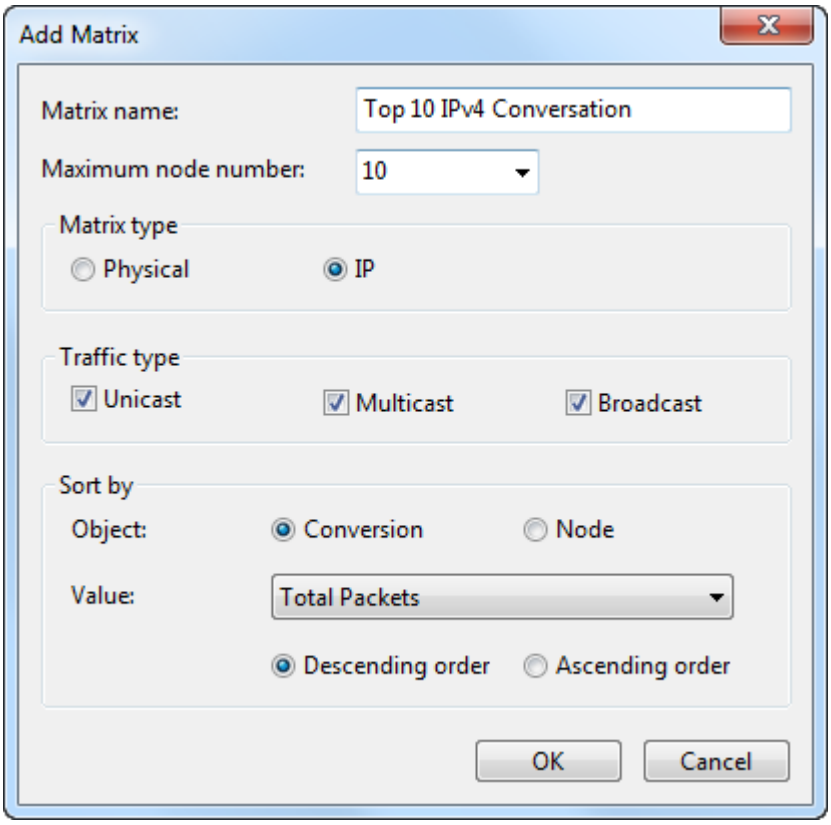
You can edit default matrixes or create a new matrix by the icons on the toolbar:

 : Opens **Add Matrix** dialog box to create a new matrix.

 : Opens **Modify Matrix** dialog box to edit the selected matrix.

 : Deletes the selected matrix.

The **Add Matrix** dialog box appears as follows:



The **Add Matrix** dialog box includes items as follows:

- Matrix name: The name of the matrix.
- Maximum node number: The maximum number of the nodes. You can type any integer between 1 and 1000.
- Matrix type: **Physical** means that the statistics are based on MAC addresses and **IP** means that the statistics are based on IP addresses.
- Traffic type: The traffic type for statistics.
- Object: The statistical object for the matrix.
- Value: The value type of the statistical object.
- Descending order: The matrix will display the top number of statistics.
- Ascending order: The matrix will display the bottom number of statistics.

User Hidden Nodes

This section lists the nodes which have been hidden by user. The number in the bracket on this section shows the number of hidden nodes.

To display user hidden nodes, right-click this section and choose **Display Selected Nodes** to display selected nodes or choose **Display All Nodes** to display all user hidden nodes. You can also right-click the matrix graph and choose **Display All Hidden Nodes** to display all user hidden nodes.

Invisible Nodes

The section lists the nodes which have been temporarily hidden in the matrix because they do not match the settings of the matrix. The number in the bracket on the **Invisible Nodes** pane head shows the number of invisible nodes.

Packet view

The **Packet** view displays captured packets and provides packet decoding information. This view includes three panes as follows:

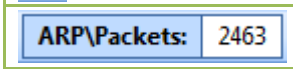
- *Packet List pane*
- *Field Decode pane*
- *HEX Decode pane*

Packet List pane

This pane lists captured packets by number and the list changes aong with the selection in the **Node Explorer** window. The packet list only displays the packets for the node selected in the **Node Explorer** window.

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Saves selected packets or exports all packets in the packet list. You can save packets in any format selected from the *Save as type* drop-down list box.
	Selects the previous packet in the list.
	Selects the next packet in the list.
	Shows the **Packet List** pane.
	Shows the **Field Decode** pane.
	Shows the **Hex Decode** pane.
	Selects a layout style for **Packet List** pane, **Field Decode** pane, and **Hex Decode** pane.
	Makes a packet filter based on the node or port number of selected packet. See *Creating Filters* for details.
	Automatically scrolls down to display the newest packets. Note that this button will be invalid when an item on the packet list is selected.
	Refreshes the packet list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Separates particular packet. See *Display Filter* for details.
	Shows the number of packets in the list. The name changes along with the selection in the **Node Explorer** window.

Packet columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Packet columns* for details.

Pop-up menu

Right-click the packet list on this pane to get a pop-up menu with items as follows:

Item	Description
Decode in New Window	Opens a new window to show packet decode information; alternatively, you can double-click the packet.
Copy (Ctrl+C)	Copies the selection in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns.
Packet Summary	Shows the packet summary. Automatic: Shows the uppermost protocol summary IP Summary: Shows the packet summary of IP protocols; if no IP protocols, show the uppermost protocol summary TCP/UDP Summary: Shows the packet summary of TCP/UDP protocols; if no TCP/UDP protocols, show the uppermost protocol summary
Export Packets	Saves selected packets or exports all packets in the packet list. You can save packets in any format selected from the *Save as type* drop-down list box.
Find	Finds an item in the list.
Set Relative Time	Makes your selected item as the reference time point and recalculates the relative time based on the selected item.
Make Filter	Opens a new dialog box to make a packet filter based on the selection.
Resolve Address	Resolves the host name of your selected item. With the resolved name, you can easily find the machine in your network.
Add to Name Table	Add an alias for the selected node to the **Name Table**.
Make Graph	Generates a new graph item in **Graph** tab based on the selected item.
Make Alarm	Generates a new alarm item in **Alarm Explorer** window to alert you anomalies, based on the selected item.
Locate in Node Explorer	Locates the current node in the **Explorer**.
Ping	Invokes the build-in **Ping Tool** to ping the endpoints.
Send to Packet Builder	Sends the selected packets to the build-in tool Packet Builder.
Select Relative Packets	Highlights the related packets by source, destination, source and destination, conversation or protocol.
Hide Selected Packets	Hides the highlighted packets.
Hide Unselected Packets	Hides all the packets in the list except the highlighted ones.
Unhide All Packets	Shows all hidden packets back to list.
Select All	Selects all items in the list.
Notes	Makes notes for selected packet.
Highlight	Highlights the selected packet.
Refresh	Refreshes the current list.

Field Decode pane

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

The **Filed Decode** pane presents information based on the protocol used in packet transmission, click the minus or plus signs in the margin to collapse or expand the hierarchy of any header section.

The following table lists and describes all the items on the pop-up menu from right-clicking the **Field Decode** pane.

Item	Description
Copy	Copies the selection and puts it on the clipboard.
Copy Tree	Copies the packet decode tree and puts it on the clipboard. Only available when a father node is selected.
Make Filter	Opens a new dialog box to make a packet filter based on the selection.
Add to Name Table	Add an alias for the selected node to the Name Table.
Expand All	Expands all items of the display.
Collapse All	Collapses all items of the display.
Select All	Selects all rows in the Field Decode pane.
Refresh	Refreshes the current pane.

Hex Decode pane

This pane interworks with the **Field Decode** pane, and when you select a portion of packet content in the **Field Decode** pane, Capsa highlights the selected portion and the corresponding Hex data and ASCII or EBCDIC data in this pane.

The following table lists and describes all the items on the pop-up menu from right-clicking the **Hex Decode** pane.

Item	Description
Copy	Copies the data and puts it on the clipboard.
Copy HEX	Copies the HEX digits and puts it on the clipboard.
Copy Text	Copies selected text in ASCII/EBCDIC decode area.
Display in ASCII Code	Shows the decoded information as ASCII.
Display in EBCDIC Code	Shows the decoded information as EBCDIC.
Select All	Selects all Hex digits.
Refresh	Refreshes the current pane.

Packet columns

The following table lists and describes the columns of **Packet** view.

Column	Description
No.	The number of the packet.
Date	The date of the operating system when the packet is captured.
Absolute Time	The time of the operating system when the packet is captured.
Delta Time	The time difference between selected packet and the previous packet.
Relative Time	The relative time when the packet is captured. To set relative time, right-click an item on the packet list and choose **Set Relative Time**.
Notes	The note about the selected packet. To make notes of a packet, right-click an item on the packet list and choose **Note->Edit Note**.
Source	The source of the packet.
Destination	The destination of the packet.
Protocol	The name of the highest layer protocol of the packet.
Size	The size of the packet.
Source MAC	The source MAC address of the packet.
Destination MAC	The destination MAC address of the packet.
Source IP	The source IP address of the packet.
Destination IP	The destination IP address of the packet.
Source Port	The source port number of the packet.
Destination	The destination port number of the packet.

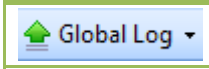
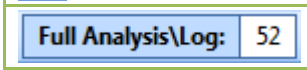
Port	
Decode	The decoding information of selected field on the **Field Decode** pane.
Summary	The summary information of the packet.

Log view

Logs are provided by different analysis modules which focus on recording different sorts of operations in detail by analyzing the captured packets. The program automatically analyzes the commands in the captured packets and recognizes the application type. If logging function of the application is activated, the commands and actions will be recorded to the corresponding log.

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Click the little triangle to choose a log type in the list and simply click the button to hide or show the log type pane.
	Exports the log list of selected log type as a .csv file.
	Makes a packet filter based on the node in the selected log. See *Creating Filters* for details.
	Locates the node in the selected log in the **Node Explorer** window
	Automatically scrolls down to display the newest logs.
	Refreshes the log list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Views particular logs. See *Display Filter* for details.
	Shows the log count of selected log type. The name changes along with the selection in the **Node Explorer** window.

Log left pane

This section lists all the log types of current analysis profile. Click one log type, the Log List section on the right will lists the detailed log information. See *Log Types* for more information.

You can save the log list of current log type by clicking the export icon on the toolbar, and you can also automatically save all logs. See *Log Output* for more information.

Note The logs will be displayed only when the log type is selected in the Log Settings. See *Log Settings* for more information.

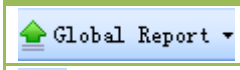
Report view

The **Report** view provides the real-time statistics of the whole network by reports.

By default, the program provides a **Global Report** which includes all report items of the analysis project (See *Report items* for details). You can also create new reports (See *Creating Reports* for details).

Toolbar

The following table lists and describes the items on the toolbar of this view:

Item	Description
	Click the little triangle to choose a report and simply click the button to hide or show the Report left pane.
	Saves the report as .html, .pdf or .mht file.
	Opens *Report Settings* dialog box to set reports properties.
	Refreshes the report.

Report left pane

This section lists all reports, including the default one and the reports created by users.

There are four icon buttons on the report list pane:

Item	Description
	Opens the **New Report** dialog box.
	Opens the **Edit Report** dialog box.
	Deletes selected report.
	Resets the report list to default.

 Default report cannot be deleted but can be edited.

Report content

The **Report view** presents report items in different tables with statistic numbers and some with bar charts. The **Report view** has the following three parts.

1. Report Head

   The **Report head** has four components:

   - **Name**: Shows the prefix of the report name and the name you specified when creating the report.
   - **Create Time**: Displays the time for creating the report.
   - **Logo**: Shows the logo image of the company.
   - **Company Name**: Shows the name of the company.

   All the four components can be edited on the *Report Settings*.

2. Report Body

   The Report Body is the main part of the report. It consists of multiple tables, statistics and bar charts. Some report items contain many sub report items. With the bar charts, the report viewer can have a clear understanding of the percentage comparison. All selected items for creating reports will be listed here, with sort by Item, Statistical Value and Reference Value which can be modified by editing a report.

3. Report Footer

This part displays the name of the creator, which can be edited on the *Report Settings*.

ARP Attack view

The **ARP Attack** view is only available when you are using the analysis profile of **Security Analysis**.

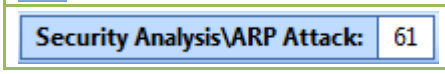
The ARP attack analysis is able to detect ARP scanning, ARP spoofing, ARP request storm. All these ARP problems will be identified according to default setting values, and you can also customize these values to let the program find out the problems more accurately (See *ARP Attack settings* for details).

Note The **ARP Attack** view will not be available when you select any nodes on the **Protocol Explorer** and the **IP Explorer** or IP address nodes on the **Physical Explorer**.

This view lists all MAC addresses and their traffic information of the hosts which may be subject to ARP attack. You can double-click any item on the list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current MAC address statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of ARP attacks in the list. The name changes along with the selection in the **Node Explorer** window.

ARP Attack columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the MAC address list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.

Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

ARP Attack lower pane

When you select a specific item in the node list on the **ARP Attack** view, the lower pane tab will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **ARP Attack** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

There is only a **Physical Conversation** tab on the lower pane. The **Physical Conversation** tab lists all MAC address conversations of the node selected on the **ARP Attack** view. The toolbar and columns are just the same as those on **Physical Conversation** view. See *Physical Conversation* for details.

You can double-click any item in the conversation list to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Worm view

The **Worm** view is only available when you are using the analysis profile of **Security Analysis**.

A computer worm is a self-replicating malware computer program. It uses the computer network to send copies of itself to other nodes and it may do so without any user intervention. To spread itself, it always needs network, either directly affecting others computers or sending out by emails. Worm attacks will be identified according to default setting values, and you can also customize these values to let the program find out the attacks more accurately (See *Worm attack settings* for details).

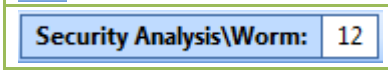
Note The **Worm** view will not be available when you select any nodes on the **Protocol Explorer** and all nodes except IP address nodes on the **Physical Explorer**.

This view lists the IP addresses and their traffic information of the hosts which may be affected with worm. You can double-click any item on the list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description

	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of worm attacks in the list. The name changes along with the selection in the **Node Explorer** window.

Worm columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Ping	Only available with right-clicking IP address node. Calls out the build-in **Ping Tool** to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

Worm lower pane

When you select a specific item in the node list on the **Worm** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **Worm** view to close it, and you can also click **Details** button to

show the lower pane when it is invisible.

The **Worm** lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.

You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

DoS Attacking view

The **DoS Attacking** view is only available when you are using the analysis profile of **Security Analysis**.

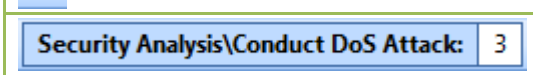
If there is an item on this view, it means that the listed computers has been compromised and been manipulated to join in an attack of some remote or local sites. A compromised machine like this is called a *botnet*. A botnet consumes the network bandwidth dramatically. DoS attackings are identified according to default setting values, and you can also customize these values to let the program find out the root of the problem more accurately (See *DoS attacking settings* for details).

Note The **DoS Attacking** view will not be available when you select any nodes on the **Protocol Explorer** and all nodes except IP address nodes on the **Physical Explorer**.

This view lists the IP addresses and their traffic information of the hosts which may perform DoS attack. You can double-click any item on the list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of worm attacks in the list. The name changes along with the selection in the **Node Explorer** window.

DoS Attacking columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Ping	Only available with right-clicking IP address node. Calls out the build-in **Ping Tool** to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

DoS Attacking lower pane

When you select a specific item in the node list on the **DoS Attacking** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **DoS Attacking** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **DoS Attacking** lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.

You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the

conversation and is just the same as the **Packet** view (See *Packet view* for more information).

DoS Attacked view

The **DoS Attacked** view is only available when you are using the analysis profile of **Security Analysis**.

DoS Attacked means that a host in your network has been under a DoS or DDoS attack. A denial-of-service (DoS) attack or distributed denial-of-service (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

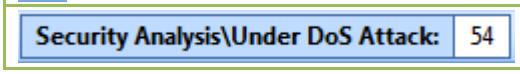
DoS attacked problems are identified according to default setting values, and you can also customize these values to let the program find out the root of the problem more accurately (See *DoS attacked settings* for details).

Note The **DoS Attacked** view will not be available when you select any nodes on the **Protocol Explorer** and all nodes except IP address nodes on the **Physical Explorer**.

This view lists the IP addresses and their traffic information of the hosts which may be under a DoS or DDoS attack. You can double-click any item on the list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of worm attacks in the list. The name changes along with the selection in the **Node Explorer** window.

DoS Attacked columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the Packet window which is just the same as the Packet view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out Find dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the Dashboard view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the Name Table for the IP address or MAC address of selected item. See *Name Table* for details.
Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the Node Explorer window.
Ping	Only available with right-clicking IP address node. Calls out the build-in Ping Tool to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

DoS Attacked lower pane

When you select a specific item in the node list on the **DoS Attacked** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **DoS Attacked** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **DoS Attacked** lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.

You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

TCP Port Scan view

The **TCP Port Scan** view is only available when you are using the analysis profile of **Security Analysis**.

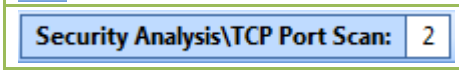
A scanning is always the first step of a malware to infect other hosts, or of a hacker to intrude your system. Network administrators should also pay attention to the port scanning. If a host send a group of TCP SYN packets to a target host continuously in a short time, it is identified as a TCP port scan. TCP Port Scan attacks are identified according to default setting values, and you can also customize these values to let the program find out the root of the problem more accurately (See *TCP Port Scan settings* for details).

Note The **TCP Port Scan** view will not be available when you select any nodes on the **Protocol Explorer** and all nodes except IP address nodes on the **Physical Explorer**.

This view lists the IP addresses and their traffic information of the hosts which may be under TCP Port Scan attacks. You can double-click any item on the list to view detailed packet information in the **Packet** window which is named with the node and is just the same as the **Packet** view (See *Packet view* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.
	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Adds an alias to the **Name Table** for selected node. See *Name Table* for details.
	Locates the selected node in the **Node Explorer** window.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of worm attacks in the list. The name changes along with the selection in the **Node Explorer** window.

TCP Port Scan columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Endpoint columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet Details	Views the decoding information of the packets of the node in the **Packet** window which is just the same as the **Packet** view (See *Packet view* for more information).
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Node Statistics	Saves current list of the node statistics as a .csv file.
Find	Calls out **Find** dialog box to search only in the node list.
Make Filter	Makes a packet filter based on the selected node. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the selected node. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the selected node. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the IP address or MAC address of selected item. See *Name Table* for details.

Resolve Address	Only available when an IP address node is selected. Resolves the host name of selected node.
Locate in Node Explorer	Locates the selected node in the **Node Explorer** window.
Ping	Only available with right-clicking IP address node. Calls out the build-in **Ping Tool** to ping selected node.
Select All	Selects all items in the node list.
Refresh	Refreshes the node list.

TCP Port Scan lower pane

When you select a specific item in the node list on the **TCP Port Scan** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **TCP Port Scan** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **TCP Port Scan** lower pane provides **IP Conversation** tab, **TCP Conversation** tab, and **UDP Conversation** tab.

- The **IP Conversation** tab lists all IP address conversations of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **IP Conversation** view. See *IP Conversation* for details.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **TCP Conversation** view. See *TCP Conversation* for details.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **Worm** view. The toolbar and columns are just the same as those on **UDP Conversation** view. See *UDP Conversation* for details.

You can double-click any item in the conversation lists to view detailed packet information in the **Packet** window which is named with the conversation and is just the same as the **Packet** view (See *Packet view* for more information).

Suspicious Conversation view

The **Suspicious Conversation** view is only available when you are using the analysis profile of **Security Analysis**.

The conversations with TCP port connected and without corresponding data traffic are identified as suspicious conversations. The program identifies suspicious HTTP conversations, suspicious POP3 conversations, suspicious SMTP conversations and suspicious FTP conversations. Suspicious conversations are identified according to default setting values configured by the program, and you can also choose not to detect suspicious conversations (See *Suspicious Conversation settings* for details).

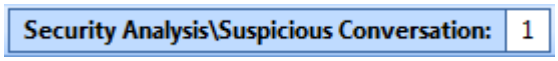
Note The **Suspicious Conversation** view will not be available when you select any nodes on the **Protocol Explorer** and all nodes except IP address nodes on the **Physical Explorer**.

This view lists the traffic statistical information of suspicious conversations. You can double-click any item on the list to view detailed conversation information in the **TCP Flow Analysis** window (See *TCP Flow Analysis window* for more information).

Toolbar

The following table lists and describes the items on the toolbar of this view.

Item	Description
	Exports current statistical list as a .csv file.
	Shows or hides the lower pane.

	Makes a packet filter based on the selected node. See *Creating Filters* for details.
	Refreshes the node list or sets display refresh interval by clicking the little triangle. If the interval is set to **Manually Refresh**, display will update only when the **Refresh** button is clicked.
	Displays particular items of the list. See *Display Filter* for details.
	Shows the number of worm attacks in the list. The name changes along with the selection in the **Node Explorer** window.

Suspicious Conversation columns

By right-clicking the column header, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column. See *Conversation columns* for details.

Pop-up menu

Right-click the node list to get a pop-up menu with items as follows:

Item	Description
Packet/TCP Flow Details	To open **TCP Flow Analysis** window. See *TCP Flow Analysis window* for details.
Copy	Copies the selection and the header row in original format to the clipboard.
Copy Column	Copies the selected column in original format to the clipboard.
Display Column	Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
Export Conversation Statistics	Exports current statistical list as a .csv file.
Find	Calls out **Find** dialog box to search only in the conversation list.
Make Filter	Makes a packet filter based on the node of selected conversation. See *Creating Filters* for details.
Make Graph	Makes a graph in the **Dashboard** view on the basis of the node of selected conversation. See *Creating Graphs* for details.
Make Alarm	Makes an alarm on the basis of the node of selected conversation. See *Creating Alarms* for details.
Add to Name Table	Adds an alias to the **Name Table** for the node of the selected conversation. See *Name Table* for details.
Resolve Address	Resolves the host name of the node of selected conversation.
Locate in Node Explorer	Locates the node of selected conversation in the **Node Explorer** window.
Ping	Calls out the build-in **Ping Tool** to ping the node of selected conversation.
Select All	Selects all items in the conversation list.
Refresh	Refreshes the conversation list.

Lower pane tabs

When you select a specific item in the conversation list on the **Suspicious Conversation** view, the lower pane tabs will provide detailed information about the item. By default, the lower pane is visible. You can click **Details** button on the **Suspicious Conversation** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **Suspicious Conversation** lower pane includes **Packets** tab, **Data Flow** tab and **Time Sequence** tab.

- The **Packets** tab lists all packets for the conversation selected in the **Suspicious Conversation** view. The toolbar and columns are just the same as those on **Packet** view. See *Packet view* for details.
- The **Data Flow** tab provides reassembled data flow for the TCP conversation selected in the **TCP Conversation** view. See

Data Flow tab for details.

- The **Time Sequence** tab displays TCP conversation in time-sequential order. See *Time Sequence tab* for details.

Network Profile

Network Profile is designed to store general properties of different networks. Different network segments may have their own environment. Colasoft Capsa lets you save the most common-used properties, including bandwidth, network structure, name table and alarms. By default, a network profile is not applied, but when you make changes to network group, name table or alarms, you are required to create a network profile first.

When you installed Colasoft Capsa on a laptop and need to move it between different network segments, you are recommended to save the network properties in a network profile and recall the profile when you come to the network again.

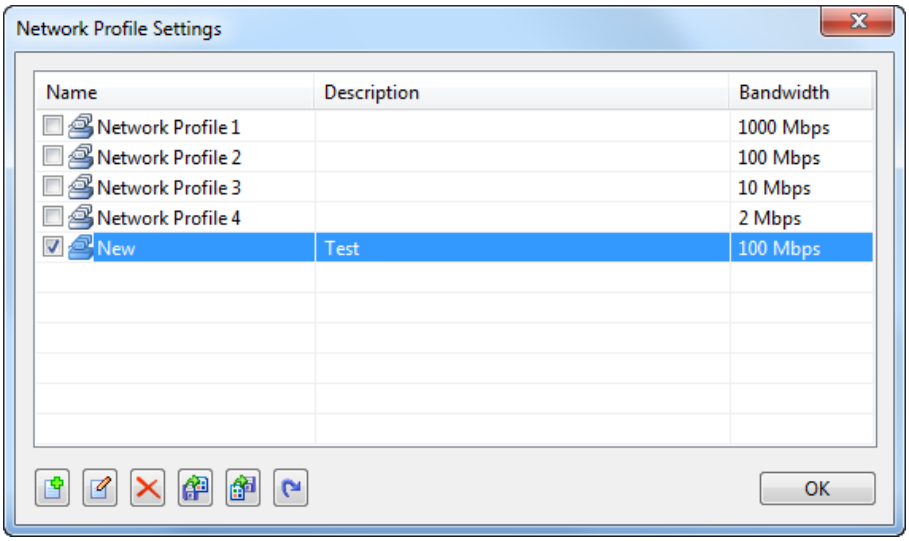
You can open the **Network Profile** dialog box by one of the following:

- On the *Start Page*: Click *Set Network Profile* link on the **Configuration info section** to open the **Network Profile Settings** dialog box. Double-click the network profile you need to edit.
- In an analysis project: Click any icon on the **Network Profile** group on the **Analysis** tab of the **Ribbon**.

The **Network Profile** dialog box contains the following tabs:

- *General Settings*
- *Node Group*
- *Name Table*
- *Alarm Settings*

The **Network Profile Settings** dialog box appears as follows:



The **Network Profile Settings** dialog box includes all available network profiles. You can use the buttons on the bottom of the dialog box to add, edit and delete a network profile, or import/export a network profile file.

General Settings

The **General Settings** tab contains following options:

- **Profile Name**: The name of the network profile.
- **Profile Description**: The description about the network profile.
- **Bandwidth**: The real bandwidth of current network.

Note The bandwidth is very important. It is the benchmark of calculating the network utilization. By default this value is calculated from the properties of the adapter.

Node Group

In Capsa, all IP address nodes and MAC address nodes on the network can be divided into different node groups so that it will be easy to identify local traffic from internet traffic and broadcast traffic from multicast traffic.

For MAC addresses, there are three node groups: Local Segment, Broadcast Addresses and Multicast Addresses. For IP addresses, there are six node groups: Local Subnet, Private-use Networks, Multicast Addresses, Broadcast Addresses, Internet Addresses and Link Local. All these node groups will be displayed in the **Node Explorer** window when available.

The **Node Group** tab is utilized to manage local MAC and IP addresses of the network and contains an upper pane called as node group list which lists all node groups, a lower pane called as node list which lists all nodes for the node group selected in the node group List, and multiple buttons described as follows:

- Add: Adds a new node group which belongs to the node group selected in the node group List.
- Edit: Edits the name of selected node group in the node group list.
- Delete: Deletes the selected node group from the node group list.
- Move Up: Moves the selected node group up.
- Move Down: Moves the selected node group up.
- Import: Imports current node group list from .cscnp file.
- Export: Exports current node group list as .cscnp file.
- Auto Detect: Detects and groups local MAC addresses and IP addresses of current network.
- Enable Country Group: Groups the node group **Internet Addresses** by countries or areas.

In the node group list, the node **Local Segment** manages the node groups of local MAC addresses and the node **Local Subnet** manages the node groups of local IP addresses. By default, there are automatically generated node groups which are detected through the network adapter. You can also get the same result by clicking **Auto Detect**.

- To add a node group of MAC addresses, select **Local Segment** in the node group list, click **Add**, type the name for the new node group and click **OK** on the pop-up dialog box, and type MAC addresses for the new node group on the node list with one MAC address one line.
- To add a node group of IP addresses, select **Local Subnet** in the node group list, click **Add**, type the name for the new node group and click **OK** on the pop-up dialog box, and type IP addresses for the new node group on the node list with one IP address one line, one IP address range one line, or one IP address mask one line.

Note The new node group will be the sub node group of the selected node group.

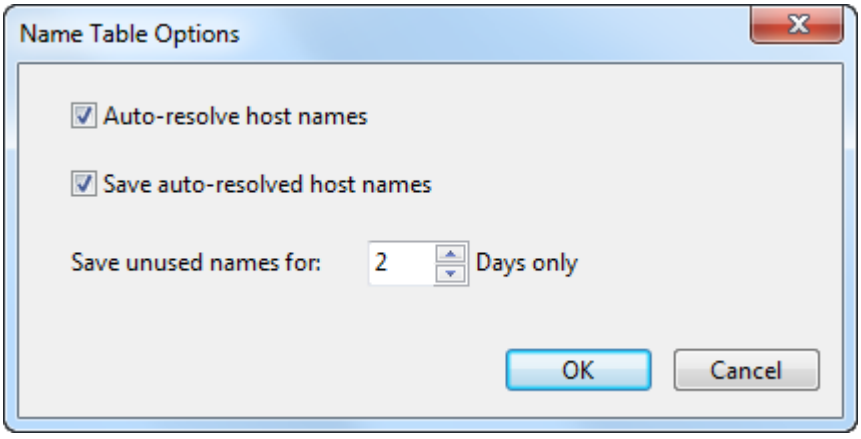
Name Table

The **Name Table** tab manages symbolic names for all MAC addresses and IP addresses. You can use the **Select name table** to select between MAC name table and IP name table. If you have too many items in the list, you can type a key word in the **Search** textbox to find your item.

The buttons on this tab are described as follows:

- Add: Adds a name for an address (See *Adding to Name Table* for details).
- Modify: Edits the selected alias item.
- Delete: Deletes the selected alias item.
- Import: Reads the filters from a .csccont file or .cscntab file.
- Export: Saves the filters to a .csccont file.
- Options: Sets Name Table options.

Click the **Options** button, the **Name Table Options** dialog box appears.



- Auto-resolve host names: Enabled by default to automatically resolve the names for the hosts.
- Save auto-resolved host names: Enabled by default to save auto-resolved host names.
- Save unused names: Specifies the days to save unused names, and 2 days by default.

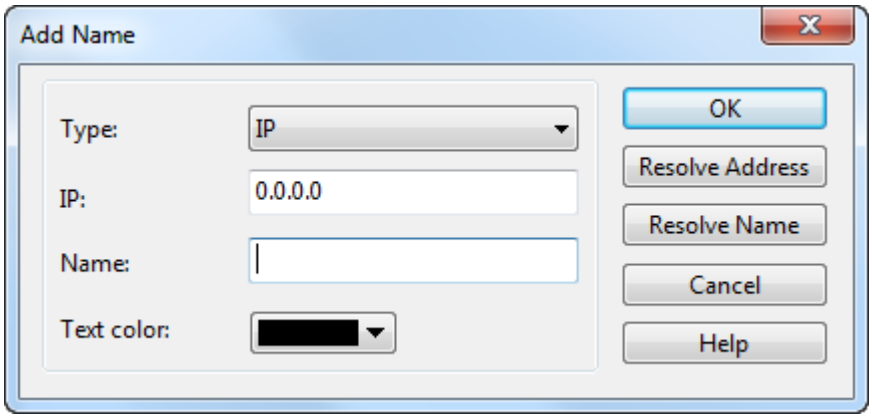
The host will be displayed with the resolved names instead of IP addresses.

Note The function of automatically resolving will only be valid when a network profile is applied.

Adding to Name Table

To add a name for an address, follow the steps below:

1. Click **Name Table** button on the **Analysis** tab of **Ribbon** section, select a name table, and click **Add** button to open the **Add Name** dialog box which appears below.



2. Type the address, and the name for the address.
3. Click **OK** on the dialog box, and click **OK** on the **Name Table** tab.

When you do not know the name for the address, you can use **Resolve address** button to automatically resolve the address; or, when you do not know the address for a name, you can use **Resolve name** button to automatically resolve the name. See *Address resolution* for details.

To add a name for a specified address, follow the steps below:

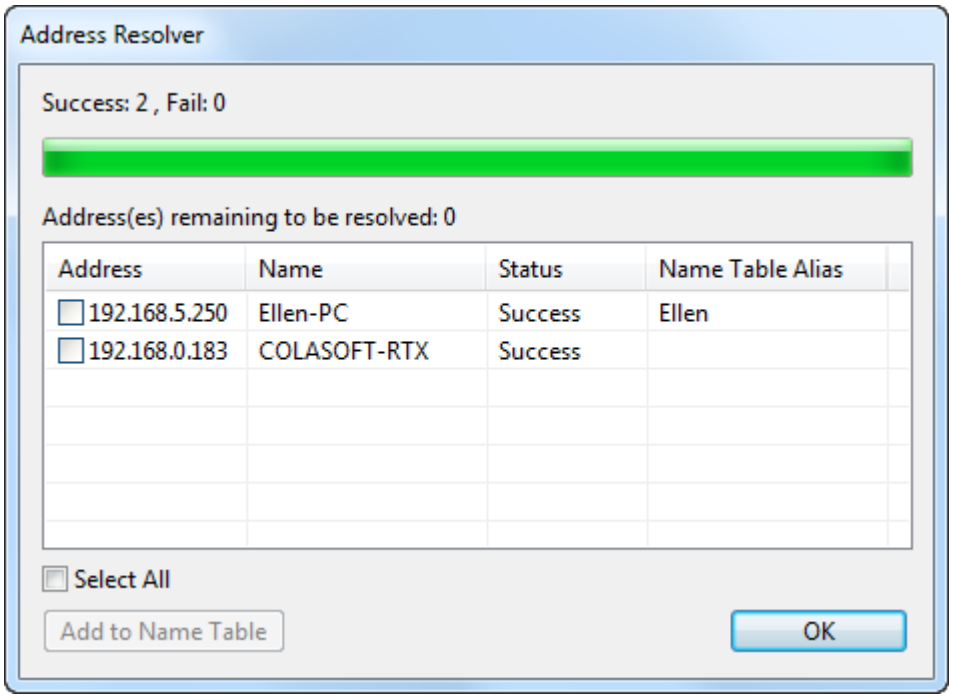
1. Select an address node, and click  on the toolbar of **Node Explorer** window or on the toolbar of some statistical views to open the **Add Name** dialog box.

   Tips You can also right-click the selected address node, and select **Add to Name Table** to open the **Add Name** dialog box.
2. Type the name for the address and click **OK** on the dialog box.

For auto-resolved address, you can also add the name to **Name Table** by right-click the auto-resolved name and select **Add to Name Table**.

Address resolution

You not only can add names to Name Table, but can use *Address Resolver* to auto-resolve addresses and names. The *Address Resolver* appears as below.



The *Address Resolver* contains four columns.

- Address: The address to be resolved.
- Name: The resolved name for the address.
- Status: The resolution status.
- Name Table Alias: The alias of the address on the name table.

Add to Name Table: Adds selected items to Name Table and removes them from the *Address Resolver.*

To use *Address Resolver*, right-click an IP address node and select **Address Resolve**.

Note Only IP addresses can be resolved by *Address Resolver.*

Alarm Settings

The **Alarm Settings** tab manages all alarms available in a network profile and lists these alarms hierarchically according to alarm type.

The buttons on the **Alarm Settings** tab are described as follows:

- Add: Creates a new alarm (See *Creating Alarms* for details).
- Delete: Deletes the selected alarm.
- Properties: Views or modifies the properties of the selected alarm.
- Import: Loads the alarm settings from an .csalam file.
- Export: Saves the alarm settings as an .csalam file.
- Enable all: Enables all the alarms in the list.
- Disable all: Disables all the alarms in the list.

- Invert: Inverts the selection on the alarms in the list.

Save alarm logs: Saves triggered alarm records as a .txt file. Enable this option and click  to specify the path and the file name for the log file.

Alarm Notification

This tab is for setting alarm notification options. The alarms will be notified with emails and/or sound when they are triggered.

Email notification

To notify alarms with emails, follow the steps below.

1. Select the checkbox Email notification on the Alarm Notification tab.
2. At the textbox Email server, type the email server address by which the emails are sent; and then type the port number that the email server applies.
3. Type the sender address and the password of the sender address.
4. Type the recipient address.

Tips

- You can click Send Test Email to test if the configurations are correct.
- You can type multiple recipient addresses and use semicolon to separate them.

Sound notification

To notify alarms with sound, follow the steps below.

1. Select the checkbox Sound notification on the Alarm Notification tab.
2. Click  to select the sound file.

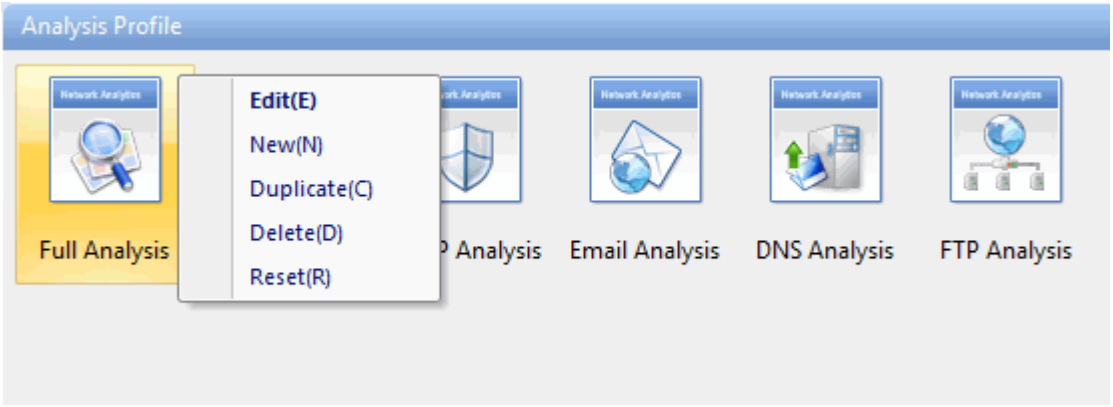
Analysis Profile

Analysis Profile is just like the container for containing the settings for an analysis project, to provide flexible, extensible and effective analysis performance. All settings in analysis profile are memorized by the program when the program or even the operating system is shut down, and can be applied to other analysis projects.

On the **Analysis Profile** section on the *Start Page*, there are eight built-in analysis profiles as follows:

Analysis profile	Description
Full Analysis	Provides comprehensive analysis of all the applications and network problems.
Traffic Monitor	Provides traffic statistics and high efficient analysis of main objects, including MAC addresses, IP addresses and protocol.
Security Analysis	Provides dedicated analysis of potential network security risk.
HTTP Analysis	Analyzes Web applications (based on HTTP) and record clients' web activities and web communication logs.
Email Analysis	Analyzes Email applications (based on POP3 and SMTP) and monitor Email content and attachments and log Email transactions.
DNS Analysis	Analyzes DNS applications, diagnose DNS applications errors and record DNS application logs.
FTP Analysis	Analyzes FTP applications (based on TCP port 21 and 20) and FTP transaction logs.
IM Analysis	Provides instant messenger analysis.

Different analysis profiles load different analysis modules and have different packet filters to analyze specific network traffic. You can also create, edit, duplicate, and delete an analysis profile by right-clicking any analysis profile on the **Analysis Profile** section:



- Edit: Opens the **Analysis Profile Settings** dialog box to edit the selected analysis profile.
- New: Opens the **Analysis Profile Settings** dialog box to create a new analysis profile.
- Duplicate: Duplicates the selected analysis profile and make changes on the copy.
- Delete: Deletes the selected analysis profile.
- Reset: Resets the **Analysis Profile**.

The **Analysis Profile Settings** dialog box includes following tabs:

- *Analysis Settings*: Configures the basic settings of an analysis profile.

- *Analysis Object*: Sets which objects to be analyzed and the maximum number of each object.
- *Diagnosis Settings*: Sets the thresholds for diagnosis events.
- *View Display*: Shows/hides the statistical views and rearranges the order of those views.
- *Packet Buffer*: Configures the buffer size, buffer mode and configure how to save packets in the buffer to disk.
- *Packet Filter*: Sets filters for capture.
- *Packet Output*: Automatically saves packets.
- *Log Settings*: Customizes all available log settings to get useful log records.
- *Log Output*: Automatically saves logs.
- *Security Analysis*: Sets the conditions to detect the hidden security problems. Only available when the analysis profile of **Security Analysis** is applied.

Note

1. You can also configure the analysis profile settings when the analysis project is running.
2. The **Analysis Settings** tab is only available when the **Analysis Profile Settings** dialog box is opened from the *Start Page*.

Analysis Settings

The **Analysis Settings** tab contains options for an analysis profile. It includes following items:

- **Name**: The name for the analysis profile.
- **Description**: Description about the analysis profile to make it identified.
- **Profile Icon**: Click the **Change** button to select an image for the analysis profile.
- **Analysis Module**: To choose the analysis modules to analyze the specific traffic over the network.

Analysis Object

The **Analysis Object** settings are used to customize the objects to be analyzed, such as protocols, addresses, conversations and the maximum number of the objects.

There are three columns on this tab:

- **Analysis Object**: Includes Network Protocol, Physical Address, Local IP Address, Remote IP Address, Physical Group, IP Group, Physical Conversation, IP Conversation, TCP Conversation, and UDP Conversation. All analysis objects on the list are selected by default. The program will not analyze the analysis object if it is not selected.

  For example, if analysis object **Local IP Address** is not selected, all statistical information based on local IP address will not be available, including local IP addresses on the **IP Explorer** and all statistics about local IP address on the statistical views.

- **Protocol Details**: Sets the display of detailed traffic information for the **Protocol** view. The table below lists the function of this column when it is enabled.

Analysis object	Function

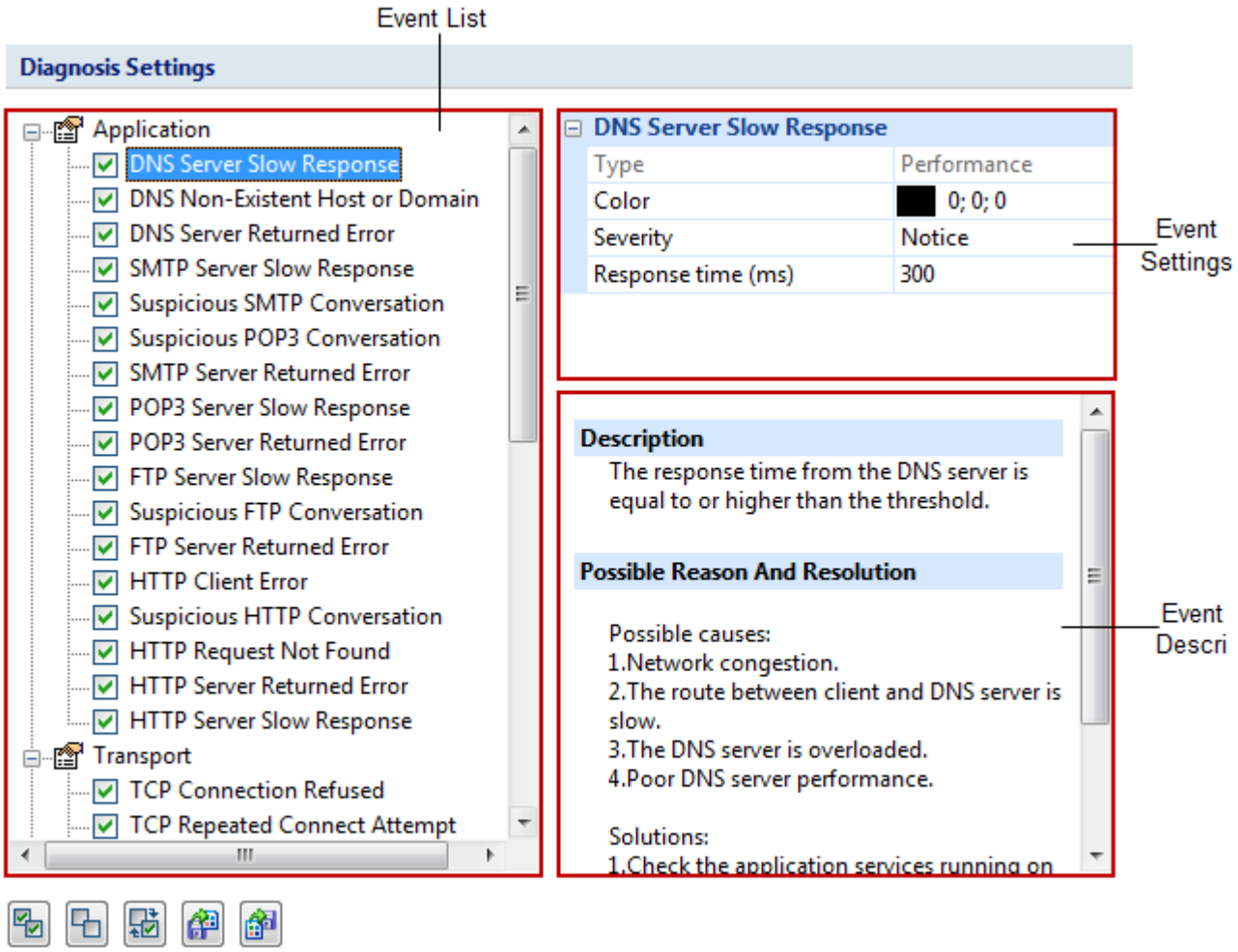
MAC Address	The **Protocol** view will display detailed protocol statistics information when a specific MAC address on the **Physical Explorer** is selected, and the **Physical Endpoint** tab on the **Protocol** view will display the detailed traffic information of a single MAC address; or else, said information will not be available.
Local IP Address	The column **Protocol Details** is selected, the **Protocol** view will display detailed protocol statistics information when a specific local IP address on the **IP Explorer** is selected, and the **IP Endpoint** tab on the **Protocol** view will display the detailed traffic information of a single local IP address.
Remote IP Address	The **Protocol** view will display detailed protocol statistics information when a specific remote IP address on the **IP Explorer** is selected, and the **IP Endpoint** tab on the **Protocol** view will display the detailed traffic information of a single remote IP address.
MAC Address Group	The **Protocol** view will display detailed protocol statistics information when an MAC address group on the **Physical Explorer** is selected, and the **Physical Endpoint** tab on the **Protocol** view will display the detailed traffic information of an MAC address group.
IP Group	The **Protocol** view will display detailed protocol statistics information when an IP address group on the **IP Explorer** is selected, and the **IP Endpoint** tab on the **Protocol** view will display the detailed traffic information of an IP address group.
Physical Conversation	The **Physical Conversation** tab on the **Protocol** view will display the detailed traffic information of the MAC address conversation when any node except IP address node on the **Physical Explorer** is selected.
IP Conversation	The **IP Conversation** tab on the **Protocol** view will display the detailed traffic information of the IP address conversation when any node on the **IP Explorer** or IP address node on the **Physical Explorer** is selected.

- **Max Object Count**: The maximum analysis object count for each analysis object and 10,000 is set by default. You can click the number to set it. The value for the number is from 1 to 10,000.

Reset: Resets the settings on this tab.

Diagnosis Settings

This tab lists all available diagnosis events of the loaded analysis module of the current analysis project. All diagnosis events are hierarchically grouped in protocol layers: *Application layer events*, *Transport layer events*, *Network layer events* and *Data link Layer events*. You can easily find which layer a network problem belongs to. The **Diagnosis Settings** tab appears as follows:



The **Diagnosis Settings** tab includes three sections.

- Event List: Lists all available diagnosis events of current analysis profile. The occurred diagnosis events will display on the **Diagnosis** view only when they are selected on the Event List section.
- Event Setting: Allows you to edit the options of a specific event selected on the Event List section just by clicking the options. The options include color, severity type and other available parameters which depend on the event.
- Event Description: Provides the event description and possible reasons and resolutions for you to quickly throubleshoot the network when there are network problems.

There are five buttons on the bottom of this window to help you manage all your diagnosis events.

Item	Description
	Selects all the diagnosis events in the list.
	Clears the selection on all the diagnosis events in the list.
	Inverts the selection on the diagnosis events in the list.
	Reads the diagnosis event settings from a .cscdiag file.
	Saves the diagnosis event settings to a .cscdiag file.

View Display

This tab is utilized to specify which statistical views to be shown or hidden, and the order to show the views.

For **Full Analysis**, all statistical views are shown by default.

To hide a statistical view, cancel the selection on the **Show** column of the view.

To rearrange the display order of the statistical views, click **Move Up** or **Move Down**.

Packet Buffer

Capsa captures traffic on the network and stores the analyzed packets into the buffer. All packets displayed on the **Packet** view are stored in the **Packet Buffer**. Therefore, the buffer size decides how many packets you can see on the **Packet** view.

Enable packet buffer

Packet buffer is enabled to store packet information. If this function is disabled, all statistical information based on packet will not be available, including detailed packet decoding information on the **Packet** view, the statistics on the **Packet** tab, the **Data Flow** tab, the **Time sequence** tab on the **TCP Conversation** view, the **Packet** window and the **TCP Flow Analysis** window.

Buffer size

By default the packet buffer size is set to be 16 MB. You can change the value, but you should take the size of your system memory into consideration.

Tips You are recommended to set the packet buffer size to be less than half of the available physical memory of the operating system.

When buffer is full

When the **Packet Buffer** is full with captured packets, you can choose to:

- **Discard oldest packets (circulative buffer)**
  It is recommended to discard the oldest packets to store the latest packets.
- **Discard new packets after analyzing**
  All new captured packets will be discarded after being analyzed and will not be saved to the packet buffer.
- **Discard all old packets**
  The program will empty the packet buffer and then store new packets to it.
- **Stop capture or replay**
  Stop the current capture or replay.

Note If you do not want to miss any packets during the capture, read *Packet Output* to learn how to save all packets.

Packet Filter

Packet Filter is utilized to set the conditions for capturing the traffic on the network.

You can click filter icon 

to open **Packet Filter Settings** dialog box which includes a right pane and a left pane.

The left pane lists all available filters including built-in filters and user-defined filters. For each filter, there are two options, **Accept** and **Reject**. **Accept** means only packets matching the filter will be captured by Capsa, while **Reject** means only packets unmatched will be captured by Capsa. All selected filters are in OR relationship.

The right pane is filter flow chart which shows all selected filter items on the filter list, including **Accept** ones and **Reject** ones. It refreshes upon any changes on the filters. You can double-click a filter on the flow chart to edit it.

Buttons

There are six buttons for setting packet filters.

-  : Creates a new filter.
-  : Edits the selected filter.
-  : Deletes the selected filter.
-  : Imports saved filter files to current filter list. When a filter file was imported, all the filters in current list will be replaced.
-  : Saves all filters in current filter list to disk.
-  : Resets the filter to default.

As how to create a packet filter, read *Creating Filters* for details.

Packet Output

When you need to automatically save all packets on the **Packet** view, you can enable **Packet Output**.

Save Packets to disk

This function is enabled to automatically save all packets as .rawpkt file.

- **Limit each packet to**: Limits the size of each single packet. When this function is enabled, the **Packet** view will only decode the packet of specified size. It is recommended to you to disable this function when you want to view the detailed decoding information of the packets.
- **Single file**: All packets are saved as one file.
- **Multiple files**: Packets are saved as multiple files split by time or size. To reduce the total size, you may choose to only keep the latest files.
    - **Save into folder**: The path to store the multiple packet files.
    - **Prefix name**: The prefix of the file name. Click the button  to view an example.

- **Split file every**: The rule for splitting the packet file when the file size is too big. You can split files by time or file size.
- **Save all files**: Saves all split packet files.
- **Save the latest**: Saves the latest number of split files.

Log Settings

Capsa can analyze and log the application layer traffic, e.g. DNS, HTTP, Email, FTP traffics, and also monitors MSN and Yahoo Messenger chatting messages. This tab allows you to configure log settings to get more useful logs of these traffics and save the logs to disk.

This page contains two parts:

- **Log Settings**: To specify which types of log to be displayed on the **Log** view, and to set the display buffer for each type of log. You can click the number to change the value. The maximum value of each log buffer is 16MB.
  Tips **Diagnosis Log** is selected to display the detailed information of diagnosis events on the **Diagnosis Events** pane of the **Diagnosis** view, or else, there will be no item on the **Diagnosis Events** pane.
- **Output Settings**: To specify which types of log to be saved when the **Log Output** function is enabled. The column **Folder** shows the folder name for saving the logs of the type and the column **File Prefix** shows the prefix of the log file name.

Note The **Email Copy** is for saving copies of monitored emails on your network. If you don't want to save email copies, just cancel the selection on this item.

Log Output

When you need to automatically save the log records on the **Log** view, you can enable **Log Output**.

Save log to disk

This function is enabled to automatically save the log records on the **Log** view.

- **File Path**: Specifies a folder to save the log files.
- **Save as**: The file format for storing the logs.
- **Split file every**: The rule for splitting the log file when the file size is too big. You can split files by time or file size.
- **Save all files**: Saves all log files.
- **Save the latest**: Saves the latest number of log files.

Note Not all logs will be saved when this function is enabled. See *Log Settings* for more information.

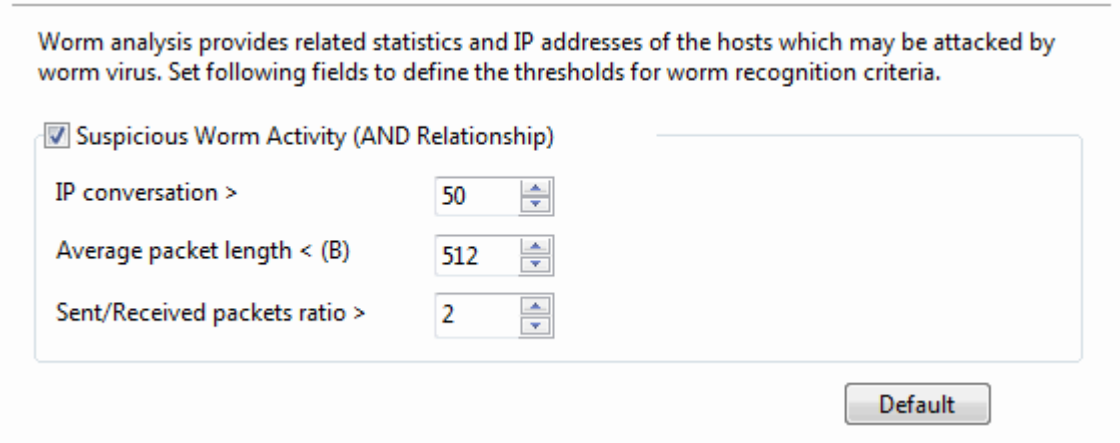
Tips All logs are saved into different folders according to the log type. See *Log Settings* for more information.

Security Analysis

This tab is only available when the analysis profile of **Security Analysis** is selected. It includes six types of malicious activities.

Worm attack settings

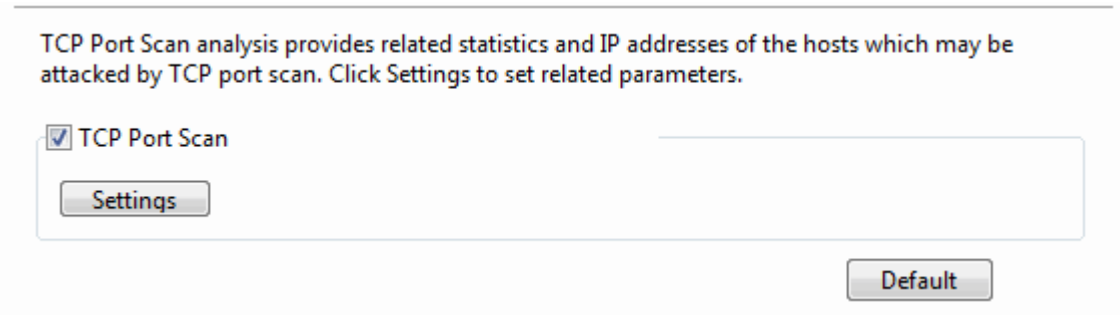
The worm analysis detects suspicious worm activities and the settings part appears as follows:



- **Suspicious Worm Activity**: Enables worm analysis, or else there will be no item to show on the **Worm** view. **AND Relationship** means the three conditions below should all be met to define the worm activity.
- **IP conversation**: Sets the IP conversation count of a host. If the IP conversation count of a host is greater than the setting value, it is supposed that the host may be attacked by worm virus. The value is an integer between 1 and 1,000, and 50 is set by default.
- **Average packet length**: The unit is byte. If the average packet length of a host is less than the setting value, it is supposed that the host may be attacked by worm virus. The value is an integer between 64 and 1,514, and 512 is set by default.
- **Sent/Received packets ratio**: The ratio of sent packets to received packets. If the ratio is greater than the setting value, it is supposed that the host may be attacked by worm virus. The value is an integer between 1 and 100, and 2 is set by default.

TCP Port Scan settings

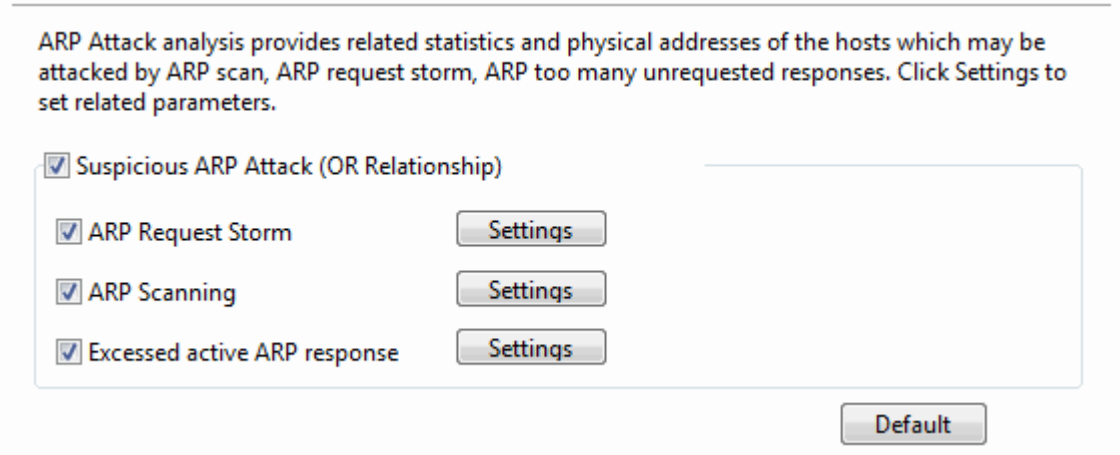
The TCP port scan analysis detects the TCP port scanning activities and the settings part appears as follows:



- **TCP Port Scan**: Enables TCP port scan analysis, or else there will be no item to show on the **TCP Port Scan** view.
- **Settings**: Locates to the **TCP Port Scan** diagnosis event on the **Diagnosis Settings** tab. The count on the Event setting pane means the count of TCP port connected by a local or a remote host. If the count is greater than the setting value, it is supposed that the host is performing TCP port scan. The value is an integer between 5 and 50, and 6 is set by default.

ARP Attack settings

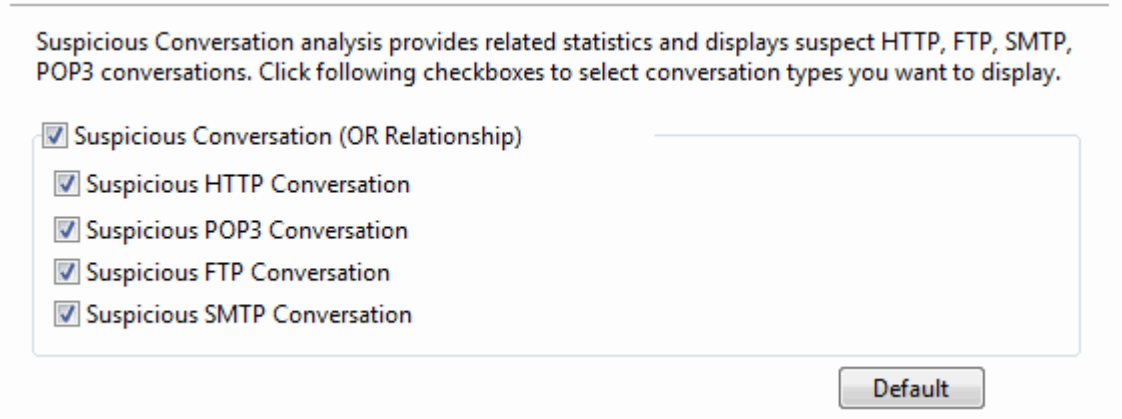
The ARP attack analysis detects ARP attack activities and the settings part appears as follows:



- **Suspicious ARP Attack**: Enables ARP attack analysis, or else there will be no item to show on the **ARP Attack** view. **OR Relationship** means one of the three conditions below is met to define the ARP attack activity.
- **ARP Request Storm**: Enables ARP request storm analysis. Click **Settings** to locate the **ARP Request Storm** diagnosis event on the **Diagnosis Settings** tab. There are two main parameters for this event.
    - **Sampling Duration**: The sampling time with the unit of second. The value is an integer between 1 and 3,600, and 20 is set by default.
    - **Request Times**: The times of ARP Request. If the time is greater than the setting value in the sampling duration, it is supposed that there is ARP request storm attack on the network. The value is an integer between 1 and 10,000, and 10 is set by default.
- **ARP Scanning**: Enables ARP scanning analysis. Click **Settings** to locate the **ARP Scanning** diagnosis event on the **Diagnosis Settings** tab. There are two main parameters for this event.
    - **Scan sampling duration**: The sampling time with the unit of second. The value is an integer between 15 and 180, and 60 is set by default.
    - **No response packet percentage (%)**: The percentage of no response packets. If the percentage is greater than the setting value in the scan sampling duration, it is supposed that there is ARP scanning attack on the network. The value is an integer between 1 and 100, and 20 is set by default.
- **Excessed active ARP response**: Enables excessed active ARP response analysis. Click **Settings** to locate the **ARP Too Many Active Response** diagnosis event on the **Diagnosis Settings** tab. There are two main parameters for this event.
    - **Unit Time**: The sampling time with the unit of second. The value is an integer between 30 and 3,600, and 60 is set by default.
    - **Number of Sent Response**: The number of sent response. If the number is greater than the setting value in the unit time, it is supposed that there is excessed active ARP response on the network. The value is an integer between 30 and 20,000, and 300 is set by default.

Suspicious Conversation settings

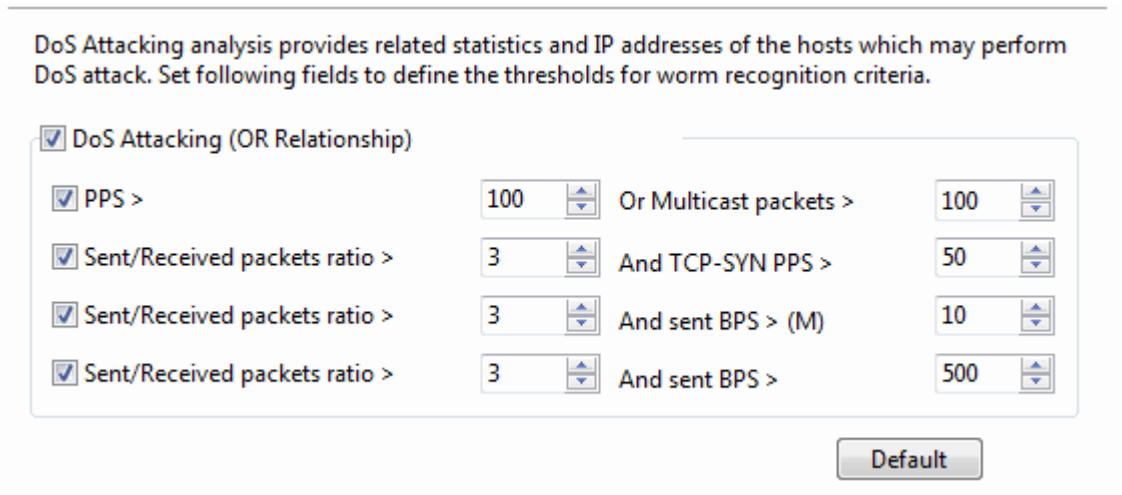
This function detects the suspicious conversations of HTTP, FTP, SMTP and POP3 and the settings part appears as follows:



- **Suspicious Conversation**: Enables suspicious conversation analysis, or else there will be no item to show on the **Suspicious Conversation** view. **OR Relationship** means one of the four conditions below is met to define the suspicious conversation attack activity.
- **Suspicious HTTP Conversation**: Enables suspicious HTTP conversation analysis which is set by the program on the **Diagnosis Settings** tab. It is supposed that there is suspicious HTTP conversation on the network when port 80 is connected without HTTP data.
- **Suspicious POP3 Conversation**: Enables suspicious POP3 conversation analysis which is set by the program on the **Diagnosis Settings** tab. It is supposed that there is suspicious POP3 conversation on the network when port 110 is connected without POP3 data.
- **Suspicious FTP Conversation**: Enables suspicious FTP conversation analysis which is set by the program on the **Diagnosis Settings** tab. It is supposed that there is suspicious FTP conversation on the network when port 21 is connected without FTP data.
- **Suspicious SMTP Conversation**: Enables suspicious SMTP conversation analysis which is set by the program on the **Diagnosis Settings** tab. It is supposed that there is suspicious SMTP conversation on the network when port 25 is connected without SMTP data.

DoS Attacking settings

The DoS attacking analysis detects the hosts which perform DoS attack and the settings part appears as follows:



- **DoS Attacking**: Enables DoS attacking analysis, or else there will be no item to show on the **DoS Attacking** view. **OR Relationship** means one of the four conditions below is met to define the DoS attacking activity.

    1. It is supposed to be DoS Attacking when broadcast packet per second is greater than its setting value or multicast packet per second is greater than its setting value. Both the setting values are an integer between 10 and 500 and 100 is set by default.

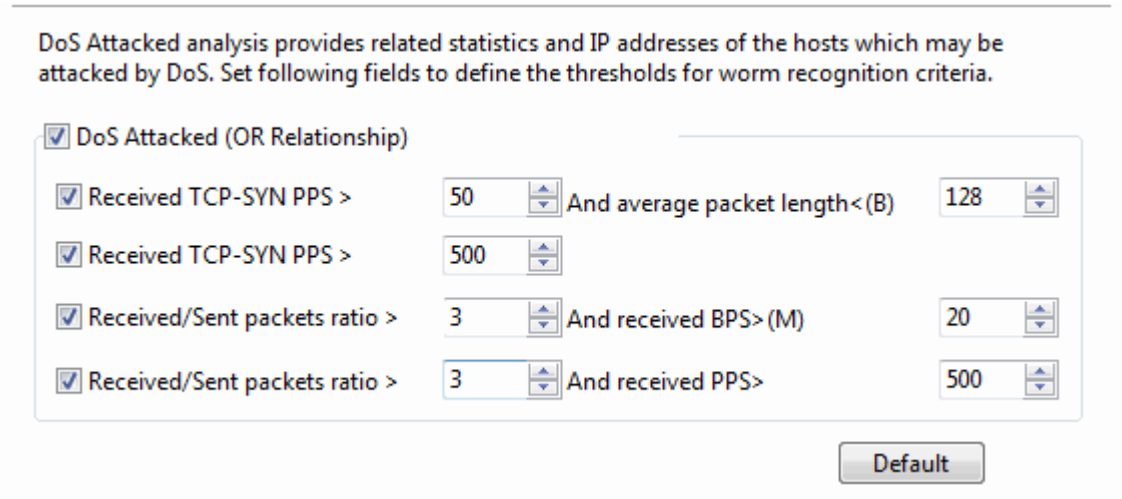
    2. It is supposed to be DoS Attacking when the ratio of sent packets to received packets is greater than its setting value and sent TCP SYN packet per second is greater than its setting value. The first setting value is an integer between 1 and 5 and 3 is set by default. The second value is an integer between 3 and 200, and 50 is set by default.

    3. It is supposed to be DoS Attacking when the ratio of sent packets to received packets is greater than its setting value and sent bytes per second is greater than its setting value. The first setting value is an integer between 1 and 5 and 3 is set by default. The second value is an integer between 1 and 100, and 10 is set by default.

    4. It is supposed to be DoS Attacking when the ratio of sent packets to received packets is greater than its setting value and sent packet per second is greater than its setting value. The first setting value is an integer between 1 and 5 and 3 is set by default. The second value is an integer between 100 and 1,000, and 500 is set by default.

DoS Attacked settings

The DoS attacked analysis detects the hosts which are under DoS attack and the settings part appears as follows:



- **DoS Attacked**: Enables DoS attacked analysis, or else there will be no item to show on the **DoS Attacked** view. **OR Relationship** means one of the four conditions below is met to define the DoS attacked activity.

    1. It is supposed to be DoS Attacked when received TCP SYN packet per second is greater than its setting value and the average packet length is less than its setting value. The first setting value is an integer between 5 and 500 and 50 is set by default. The second setting value is an integer between 64 and 1518 and 128 is set by default.

    2. It is supposed to be DoS Attacked when received TCP SYN packet per second is greater than its setting value. The setting value is an integer between 5 and 1000, and 500 is set by default.

    3. It is supposed to be DoS Attacked when the ratio of received packets to sent packets is greater than its setting value and the received bytes per second is greater than its setting value. The first setting value is an integer between 1 and 5

and 3 is set by default. The second setting value is an integer between 1 and 100, and 20 is set by default.

4. It is supposed to be DoS Attacked when the ratio of received packets to sent packets is greater than its setting value and the received packets per second is greater than its setting value. The first setting value is an integer between 1 and 5 and 3 is set by default. The second setting value is an integer between 50 and 1000, and 500 is set by default.

Default: Resets the setting of that type of security analysis to default.

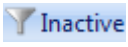
Creating Filters

Filters are utilized to separate particular packets. If no filter was enabled, Capsa will capture and analyze all the packets transmitted over the adapter. Once a filter was created, you can apply it to any analysis projects.

To create a filter, follow the steps below:

1. Click filter icon 

on the **Analysis** tab of the **Ribbon** section to open the **Packet Filter Settings** dialog box (See *Packet Filter* for details).

   Tips You can also click filter icon 

on the *Status Bar* to open the **Packet Filter Settings** dialog box.

2. Click  on the **Packet Filter Settings** dialog box to open the **Packet Filter** dialog box.

3. Select a simple filter or an advanced filter and set the filter, including the filter name, filter description, and filter rules (See *Simple filter* and *Advanced filter* for details).

4. Click **OK** on the **Packet Filter** dialog box, and click **OK** on the **Packet Filter Settings** dialog box.

To create a filter based on a selected object, which could be an address node, a port number or a protocol, follow the steps below:

1. Select an object and click  on the toolbar or right-click an object and select **Make Filter** to open the **Packet Filter** dialog box.

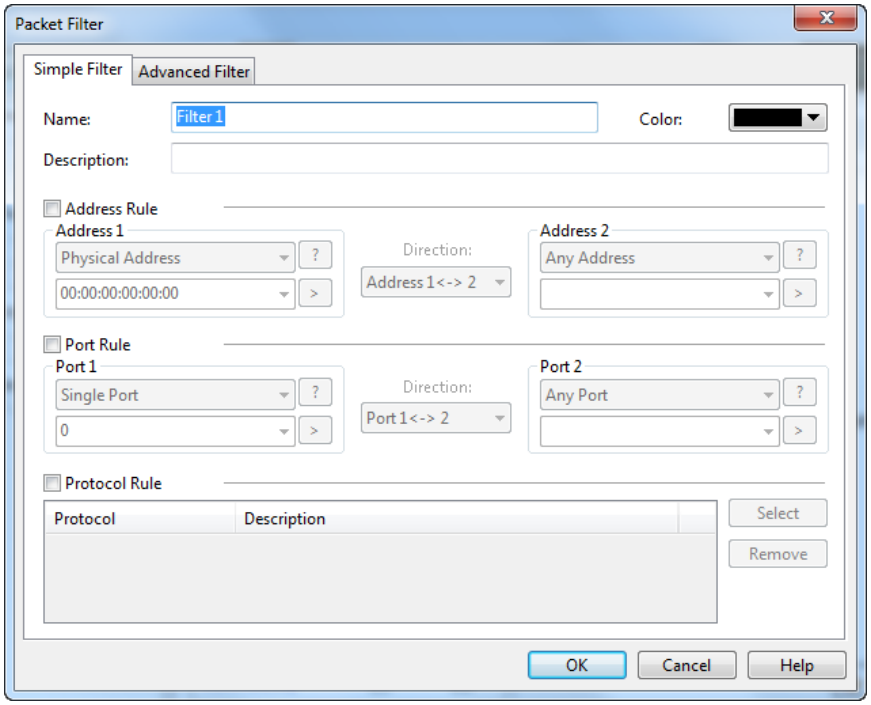
2. Select a simple filter or an advanced filter and set the filter, including the filter name, filter description, and filter rules.

3. Click **OK** on the **Packet Filter** dialog box, and click **OK** on the **Packet Filter Settings** dialog box.

Note After creating a filter, if you want to apply the filter, you should select the **Accept** or **Reject** checkbox to enable the filter.

Simple filters

When creating a filter, you can choose to create a simple filter or an advanced filter. The Simple Filter tab appears as below.



The **Simple Filter** tab allows you to create simple filters by address, port and protocol. When multiple parameters are set, they are connected by logical AND statements. That is, packets must match all of the conditions to match the filter.

For distinction and readability, you can define filters by specifying the name, the color, and the description about them.

In order to capture packets precisely, you can specify packet transmission direction (address 1 -> address 2, address 2 -> address 1 and address 1 <-> address 2) in IP address rule, MAC address rule and port rule. In simple filter, you can customize filters by combining conditions among address, port and protocol rules.

Tips You can further define simple filters in **Advanced Filter** tab.

Defining address rule

To set an address rule, follow the steps below:

1. Select the **Address Rule** checkbox.
2. Select an address type from **Address 1**. You can select MAC address, IP address, IP range or IP subnet.
3. Click the text box below the address type and type the address.
4. Click the direction drop-down list box and select packet transmission direction between the two addresses.
5. Select an address type from **Address 2**.
6. Click **OK** on the **Packet Filter** dialog box.

Tips Click the icon to get references if you are not familiar with address format. Click the icon to delete all items typed before.

Defining port rule

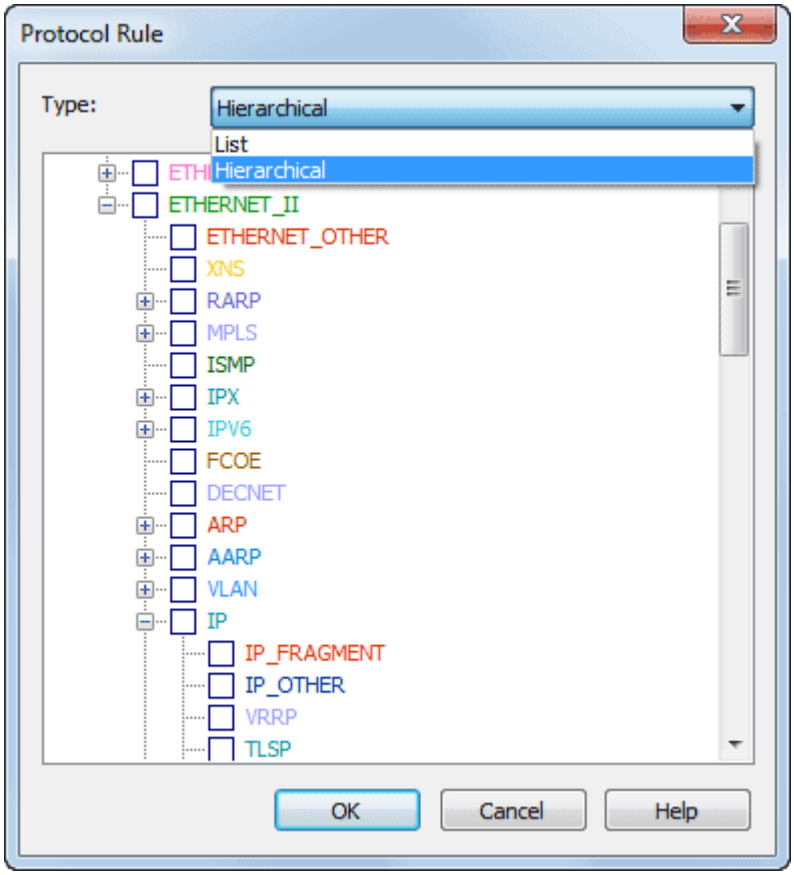
To set a port rule, follow the steps below:

1. Select the **Port Rule** checkbox.
2. Select a port type from **Port 1**. You can select single port, port range or multiple port.
3. Click the text box below the port type and type the port number.
4. Click the direction drop-down list box and select packet transmission direction between the two ports.
5. Select a port type from **Port 2**.
6. Click **OK** on the **Packet Filter** dialog box.

Defining protocol rule

To define a protocol rule, follow the steps below:

1. Select the **Protocol Rule** checkbox.
2. Click **Select** to open the Protocol Rule dialog box which appears as below.

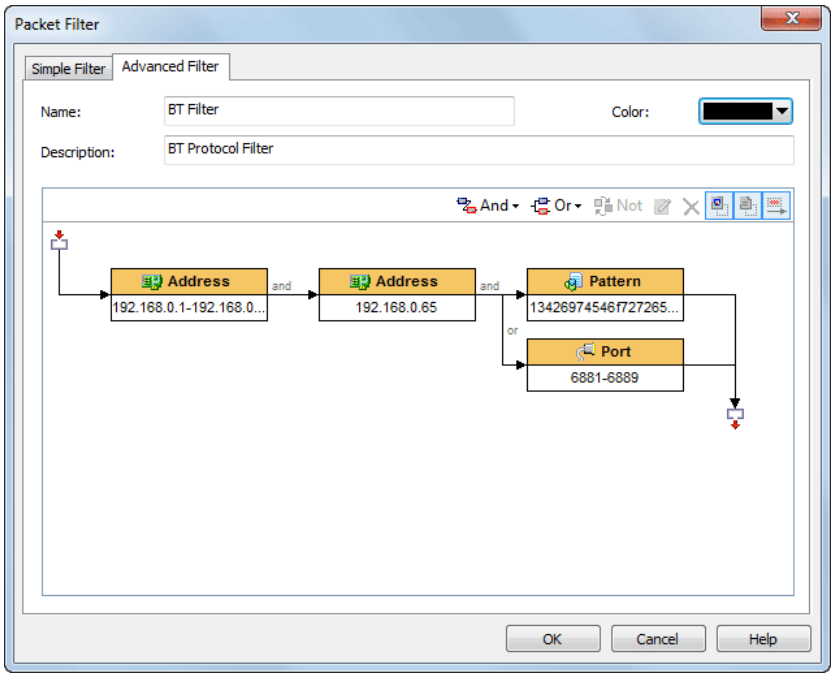


3. Choose the protocols you want to define the rule and click **OK**.
4. Click **OK** on the **Packet Filter** dialog box.

The chosen protocols are listed in **Protocol Rule** section. You can delete a protocol item from the list with the **Remove** button.

Advanced filters

When creating a filter, you can choose to create a simple filter or an advanced filter. The Advanced Filter tab appears as below.



The filter rules are arranged in a filter relation map. The map shows the logical relations among the rules from adapter to an analysis project. You can double-click the rule to edit it.

Toolbar

The toolbar contains the following items:

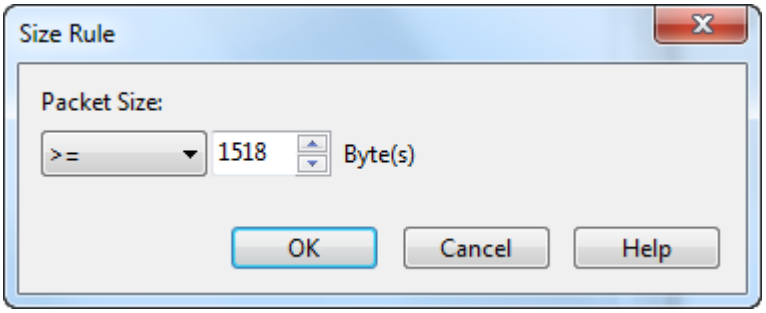
- And: The rules connected by "and" are in logical and relationship.
- Or: The rules connected by "or" are in logical or relationship.
- Not: Only packets unmatched the condition will be captured. The Not rules are marked as red ones.
- : Edits the selected rule.
- : Deletes the selected rule.
- : Shows the icon for each rule.
- : Shows the details of the rules.
- : Shows the logical relationships of the rules.

For advanced filters, there are six kinds of rules, including Address, Port, Protocol, Size, Value and Pattern. The Address, Port and Protocol rules are the same to those in simple filters (See *Simple filters* for details).

Defining size rule

Size rule is for defining the rule on packet size. Only packets of the size satisfying the rule will be captured.

To define a size rule, click **And** or **Or** on the toolbar and select **Size** to open the **Size Rule** dialog box which appears as below.

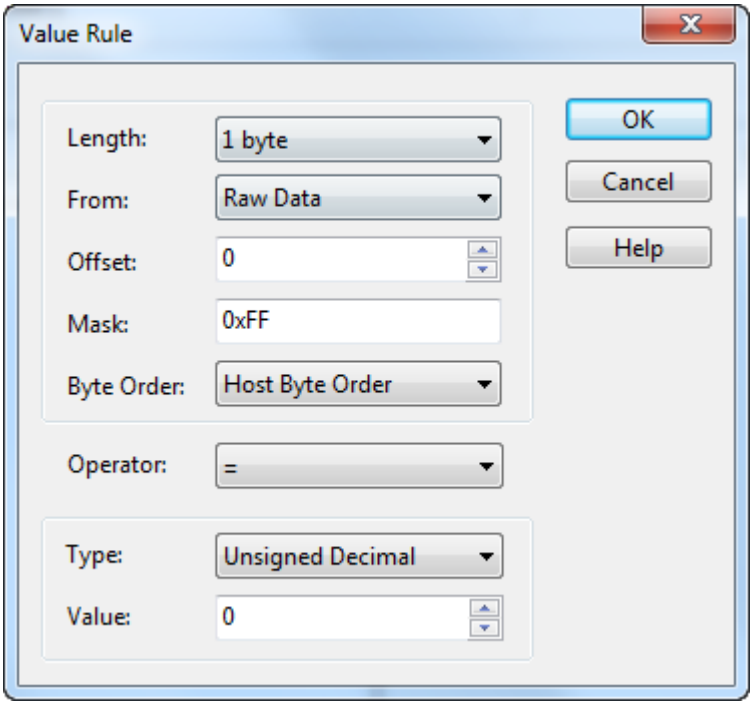


You can choose < (less than), <= (less than or equal to), > (greater than), >= (greater than or equal to), = (equal to), != (not equal to), Between (size range) to define the size rule.

Defining value rule

Value rule is for defining the rule on the value of decoded field of a packet.

To define a value rule, click **And** or **Or** on the toolbar and select **Value** to open the **Value Rule** dialog box which appears as below.



- Length: Specifies the length of the mask, and the length of the value for the rule. It could be 1 byte, 2 bytes and 4 bytes.
- From: Specifies where to offset in a packet. It could be Raw data, IP Header, ARP Header, TCP Header, and UDP Header.
- Offset: Specifies the bytes to be offset. The unit is byte.
- Mask: The hexadecimal mask of the value.
- Byte order: The order of the bytes. It could be network byte order and host byte order.
- Operator: It could be = (equal to), != (not equal to), < (less than), <= (less than or equal to), > (greater than), >= (greater than or equal to).

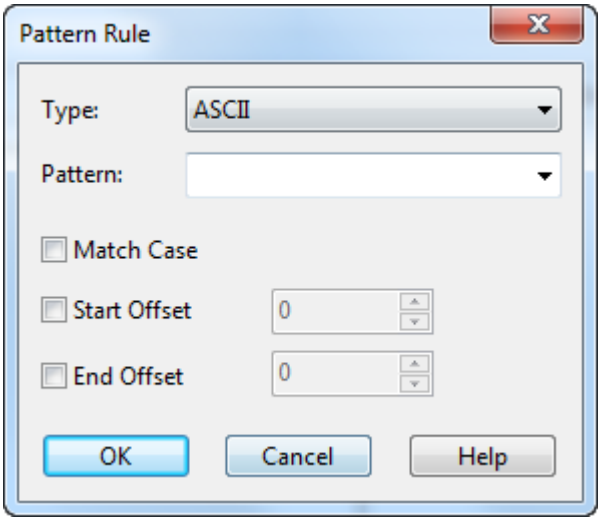
- Type: The type of the value. It could be binary, octal, unsigned decimal and hex.
- Value: The value for the rule.

When a value rule is enabled, do logical AND operation between the specified bytes in a packet and the mask, and compare the operation result with the value for the rule. If the compare result is consonant, the packet will be captured; or else, the packet will be filtered out.

Defining pattern rule

Content rule is for defining the rule on the content of a packet.

To define a content rule, click **And** or **Or** on the toolbar, select **Pattern** to open the **Pattern Rule** dialog box which appears as below, select the type for the content, type the content, set the offset options, and click **OK**.

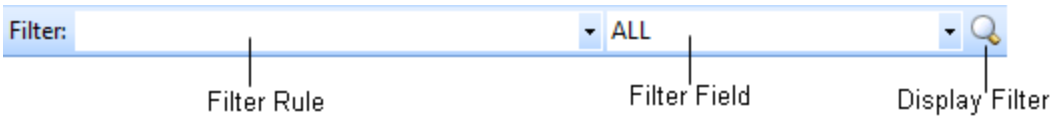


The unit for offset is byte.

Note Advanced filters can also be converted into simple filters, but some filter rules will be lost because advanced filters have more filter conditions than simple filters.

Display Filter

Filters are utilized to separate particular packets. The packet filters are utilized to restrict the packets into the buffer of a capture. However, the **Display Filter** is utilized only to isolate particular some of the captured packets to display. The **Display Filter** is available on many statistical views and shows as follows:



- The text box **Filter Rule** is for you to type filter rule. You can use =, !, >, <, >= and <= to set the filter rule.
- The drop-down list **Filter Field** is the columns of each view or tab and the field changes due to different views or tabs.

Creating Alarms

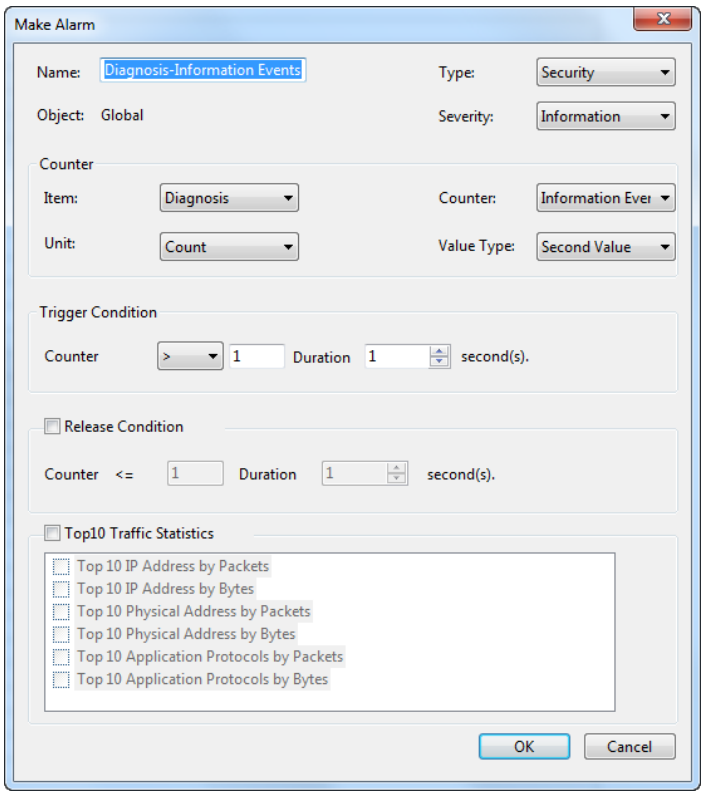
To open the **Make Alarm** dialog box to create a new alarm, you can perform one of the following operations:

- Click **Add Alarm** button on the **Alarm Explorer** window.
- Open **Network Profile Settings** dialog box, select **Alarm Settings** tab, and click **Add** button (Read *Network Profile* to know how to open the **Network Profile Settings** dialog box).
- Click icon  in the **Node Explorer** window.
- Choose **Make Alarm** on the pop-up menu from the **Node Explorer** window and statistical views.

Tips

1. Alarms created by the first two methods above will be triggered or dismissed according to the statistics of all packets captured by the analysis project.
2. Alarms created by the last two methods above will be trigged or dismissed according to the statistics about the node which you right-clicked or which you selected in the **Node Explorer** window.
3. You can get pop-up menu with **Make Alarm** on it by right-clicking in the **Node Explorer** window and on all statistical views except the **Dashboard**, the **Summary**, the **Matrix** and the **Report** views.

The **Make Alarm** dialog box shows as follows:



The **Make Alarm** dialog box has the following parts:

- **General Information**
  Sets the general information of the alarm, including alarm name, alarm type, object and alarm severity, wherein the object option is set by the program automatically.
- **Counter**
  Sets the statistic items of the alarm, with different alarm object having different statistics items.
- **Trigger Condition**
  Sets the trigger conditions for the alarm.
- **Release Condition**
  Sets the release conditions for the alarm.
- **Top 10 Traffic Statistics**
  This functionality enabled, top 10 traffic statistics will be recorded in the alarm log when the alarm was triggered. Different alarm object have different traffic statistic items.

Note Each alarm has its unique name and you cannot create an alarm with a name that already exists in the list.

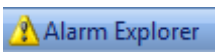
Edit Alarm

You can double-click any alarm to open the **Edit Alarm** dialog box to edit the alarm. The **Edit Alarm** dialog box is just the same as the **Make Alarm** dialog box.

You can only edit **Alarm Name and Type**, **Value Type of Counter**, **Trigger Condition** and **Release Condition** in the **Edit Alarm** dialog box. If you need to edit other options, you should delete it first and then create a new one.

Alarm Explorer window

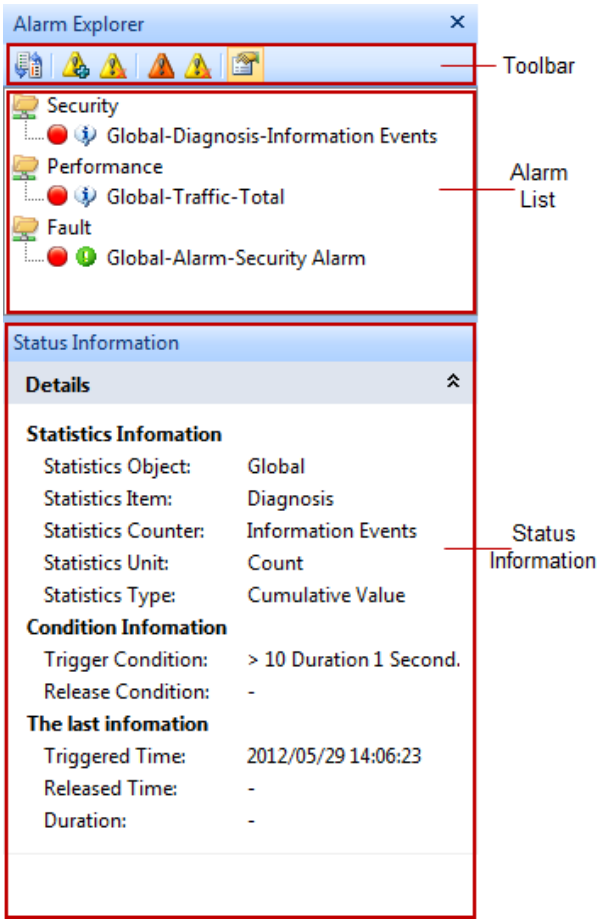
When you view the statistics of the network, you may want a tool to alert you some specific statistics or traffic status of the network. The alarm function is the tool.
For your convenience, Capsa provides an **Alarm Explorer** window to manage alarms, in which you can create, edit and view alarms. You can also get triggered alarm info in the alarm notification area on the right side of the *Status Bar*. Read *Creating Alarms* to learn how to create and edit an alarm.

To open the **Alarm Explorer** window, click 

in the alarm notifications area on the right side of the *Status Bar*.

If you want to show the **Alarm Explorer** window when starting analysis projects, click **View** tab of the **Ribbon** section and select **Alarm Explorer**.

The **Alarm Explorer** window appears as below.



Toolbar

The toolbar includes six items as follows:

Item	Description
	Switches the alarm layout between hierarchical and flat.
	Opens the **Create Alarms** dialog box to create a new alarm.
	Deletes the selected alarm.
	Only shows triggered alarms.
	Releases a triggered alarm.
	Views the properties of the alarm or edit the alarm.

Alarm List

All created alarms are hierarchically grouped in three types: **Security**, **Performance** and **Fault**. You can double-click an alarm item to open the **Edit Alarms** dialog box to edit it.

Click an alarm item, and the **Status Information** panel will display the details of the alarm.

Status Information

The **Status Information** pane displays the properties of the selected alarm in detail.

Tips You can click to collapse the details.

Alarm Pop-ups

When an alarm is triggered or dismissed, a pop-up fades in to inform you the alarm information even when the program window is not active.

You can click the link: **Click here to view alarms' log** to view alarm log (Read *Alarm Settings* to know how to set alarm logs).

Tips The corresponding alarm bubble on the right side of the *Status Bar* starts flashing when an alarm was triggered.

Note

1. Pop-up shows and keeps for only one second and then fades away.
2. There is no link of **Click here to view alarms' log** if you didn't save alarm log.

Alarm Notification Area

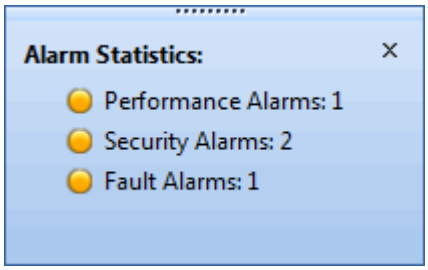
The **Alarm Notification Area** is utilized to display the real-time triggered alarm information. The **Alarm Notification Area** appears as follows:

You can click the **Alarm Explorer** icon to open or close the **Alarm Explorer** window.

The three bubbles represent three alarm types: **Security**, **Performance** and **Fault**.

The numbers following the bubbles represent the number of triggered alarms of every alarm types.

Click the bubbles, and you will get an Alarm Statistics pop-up showing the details of the alarm types as follows:



Creating Graphs

You may want to view specific statistics graphically, and Capsa provides you two types of graphs (See *Graph types* for details).

You can customize statistical graphs based on from global network to a specific node, including an MAC address, an IP address and a protocol.

To open the **Make Graph** dialog box to create a graph, you can perform one of the following operations:

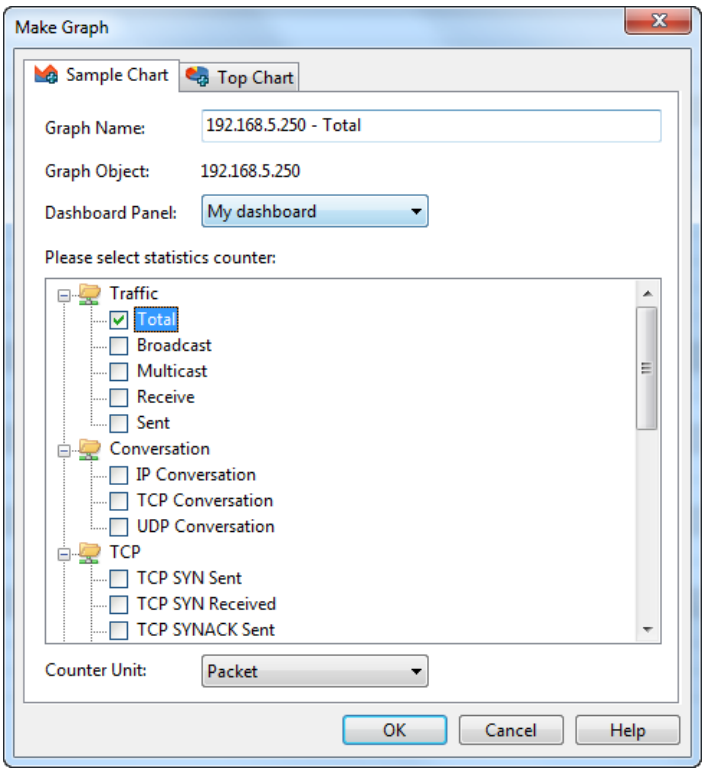
- Click  on the top-right corner of every dashboard panel.
- Click the link **Click here to add a new chart** on the dashboard panel.
- Click  icon in the **Node Explorer** window.
- Choose **Make Graph** on **Pop-up menu** which are available for the **Node Explorer** window and all statistical views except **Dashboard**, **Summary**, **Matrix**, and **Report** views.

Tips

1. Graphs that are created by the first two methods above show the statistics of all packets captured by the analysis project.
2. Graphs that are created by the last two methods above show the statistics of the packets about the node which you right-clicked or which you selected in the **Node Explorer** window.

For example, when you want to view the total traffic status of a specific network segment in a graph, you should first locate the segment in the **Node Explorer** window, right-click the segment and choose **Make Graph**, and then check **Total** in the **Traffic** list.

The **Make Graph** dialog box appears as follows:



The **Make Graph** dialog box contains two tabs: Sample Chart and Top Chart, both including the following items:

- **Graph Name**: The name of the graph, which can be automatically generated or defined by users.
- **Graph Object**: Show the statistical object of the graph, which is defined by the program.
- **Dashboard Panel**: For you to choose the dashboard panel for managing the graph and listing all created dashboard panels on the combo box.
- **Statistics Counters**: Showing all available statistical items, which are changed along with the **Graph Object**.
- **Counter Unit**: Showing the unit for the **Statistics Counters**.

Graph types

Capsa provides a wide range of statistics items for you to create graphs, generalizing as two types:

- *Sample chart*
- *Top chart*

Sample chart

Sample Chart includes statistics items as follows:

- **Diagnosis Statistics**: Information Diagnosis, Notice Diagnosis, Alarm Diagnosis and Error Diagnosis
- **Wireless Analysis**: Noise Traffic, Control Frame Traffic, Management Frame Traffic, Decrypted Data Frame Traffic, Unencrypted Data Frame Traffic and Undecrypted Data Frame Traffic
- **Traffic**: Total, Broadcast, Multicast, Average Packet Size and Utilization

- **Packet Size Distribution**: <=64, 65-127, 128-255, 256-511, 512-1023, 1024-1517 and >=1518
- **Address**: Physical Address Count, IP Address Count, Local IP Address Count and Remote IP Address Count
- **Protocol**: Total Protocols, Data Link Layer Protocols, Network Layer Protocols, Transport Layer Protocols, Session Layer Protocols, Presentation Layer Protocols and Application Layer Protocols
- **Conversation**: Physical Conversation, IP Conversation, TCP Conversation and UDP Conversation
- **TCP**:TCP SYN Sent, TCP SYNACK Sent, TCP FIN Sent and TCP Reset Sent
- **Alarm**: Security, Performance and Fault
- **DNS Analysis**: DNS Query and DNS Response
- **Email Analysis**: SMTP Connection and POP3 Connection
- **FTP Analysis**: FTP Upload and FTP Download
- **HTTP Analysis**: HTTP Request, HTTP Requested and HTTP Connection

Top chart

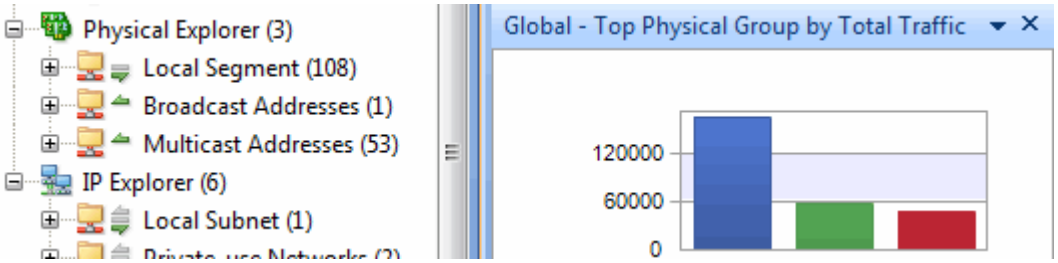
Top Chart includes statistics items as follows:

- **Top Physical Group by Total Traffic**
- **Top Physical Group by Received Traffic**
- **Top Physical Group by Sent Traffic**
- **Top IP Group by Total Traffic**
- **Top IP Group by Received Traffic**
- **Top IP Group by Sent Traffic**
- **Top Physical Address by Total Traffic**
- **Top Physical Address by Received Traffic**
- **Top Physical Address by Sent Traffic**
- **Top IP Address by Total Traffic**
- **Top Local IP Address by Total Traffic**
- **Top Remote IP Address by Total Traffic**
- **Top IP Address by Received Traffic**
- **Top IP Address by Sent Traffic**
- **Top Local IP Address by Received Traffic**
- **Top Local IP Address by Sent Traffic**

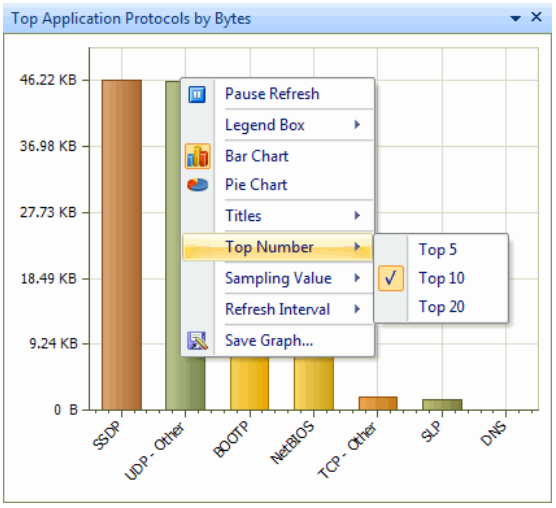
- **Top Remote IP Address by Received Traffic**
- **Top Remote IP Address by Sent Traffic**
- **Top Application Protocols**
- **Packet Size Distribution**

Tips

1. The **Physical Group/IP Group** means the node group of **Physical Explorer/IP Explorer** in the **Node Explorer** window.
2. Different **Top** items have different **Top** numbers, e.g. the top item **Top Physical Group by Total Traffic** will have only Top 3 if the **Physical Explorer** has only 3 groups (Fig below).



3. You can change the **Top** number by right-clicking the chart (Fig below) and selecting **Top Number** on the pop-up menu.



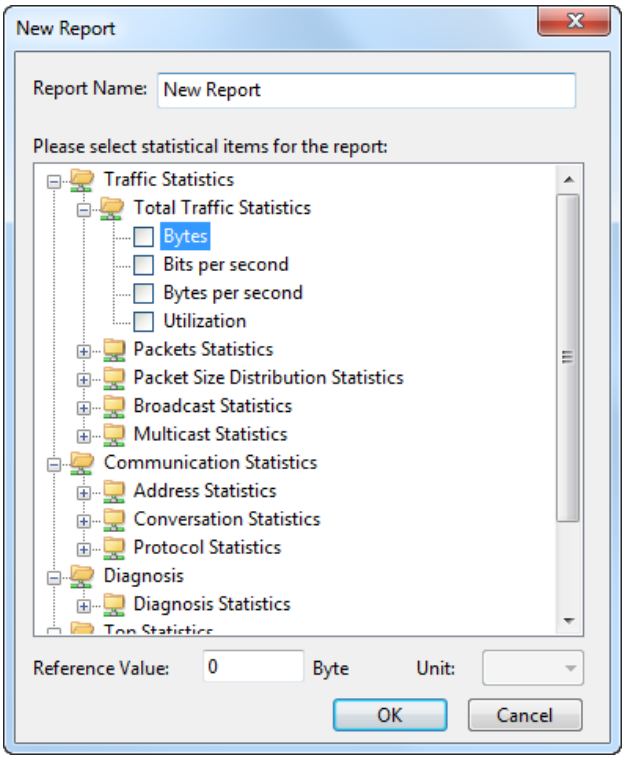
4. You can change the sampling value of **TOP Chart** by right-clicking the chart and selecting **Sampling value** on the pop-up menu.

Creating Reports

Besides the default **Global Report**, you can create new reports according to the need.

To create a report, follow the steps below:

1. Click  on the **Report view** to pop-up the **New Report** dialog box which appears as below.



2. Specify a name for the report.
3. Select the statistical items for the report, type the reference value and specify the unit for each statistical item (See *Report items* for all report items).
4. Click **OK** on the dialog box.

Tips

1. The items of **Diagnosis Statistics** as well as **Top Statistics** have no reference value.
2. Only statistical items of **Top Address and Host** as well as **TOP Application** have counter unit.

After creating the report, you can click  on the toolbar of the **Report view** to set the name of the company, the prefix of the report name, the creator of the report, the logo of the company, whether or not to show the created time (See *Report Settings* for more details).

Report items

The following table lists all available report items:

Statistical type	Statistical item	Report item
Traffic Statistics	Total Traffic Statistics	Bytes, Bits per second, Bytes per second, Utilization
	Packets Statistics	Total packets, Packets per second, Average packet size
	Packet Size Distribution Statistics	<=64, 65-127, 128-255, 256-511, 512-1023, 1024-1517, >=1518
	Broadcast Statistics	Broadcast bytes, Broadcast packets, Broadcast bytes per second, Broadcast packets
	Multicast Statistics	Multicast bytes, Multicast packets, Multicast bytes per second, Multicast packets
Communication Statistics	Address Statistics	MAC address count, IP address count, Local IP address count, Remote IP address count
	Conversation Statistics	Physical conversation count, IP conversation count, TCP conversation count, UDP conversation count
	Protocol Statistics	Total protocol count, Data link layer protocol count, Network layer protocol count, Transport layer protocol count, Session layer protocol count, Presentation layer protocol count, Application layer protocol count
Diagnosis	Diagnosis Statistics	Information events, Notice events, Warning events, Error events
Top Statistics	Top Address and Host	Top MAC Address by Total Traffic, Top MAC Address by Received Traffic, Top MAC Address by Sent Traffic, Top IP Address by Total Traffic, Top IP Address by Received Traffic, Top IP Address by Sent Traffic, Top IP Address Connection Count, Top Local IP Address by Total Traffic, Top Local IP Address by Received Traffic, Top Local IP Address by Sent Traffic, Top Local IP Address Connection Count, Top Remote IP Address by Total Traffic, Top Remote IP Address by Received Traffic, Top Remote IP Address by Sent Traffic
	Top Conversation	Top Physical Conversation, Top IP Conversation, Top TCP Conversation, Top UDP Conversation
	Top Application	Top Application Protocol

Log Types

Capsa provides eight types of log in total. Click following links to view the detailed information of each log type.

- *Global Log*
- *DNS Log*
- *Email Log*
- *FTP Log*
- *HTTP Log*
- *ICQ Log*
- *MSN Log*
- *YAHOO Log*

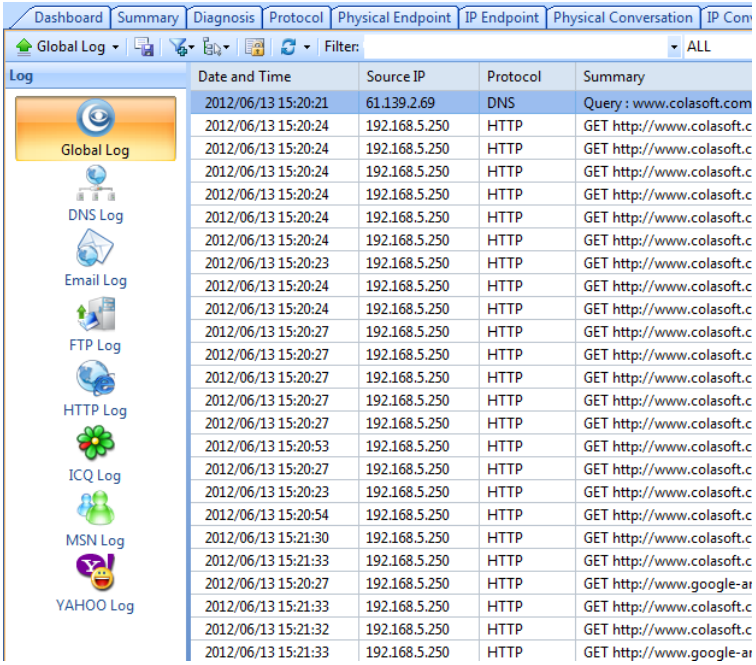
Not every analysis project has all log types. What log types will display in an analysis project depends on the analysis modules selected. Different analysis profiles have different log types. The following table lists the log types for every analysis profile.

Analysis profile	Log types
Full Analysis	Global Log, DNS Log, Email Log, FTP Log, HTTP Log, MSN Log, YAHOO Log
Traffic Monitor	Global Log
Security Analysis*	Global Log, DNS Log, Email Log, FTP Log, HTPP Log
HTTP Analysis	Global Log, HTTP Log
Email Analysis	Global Log, Email Log
DNS Analysis	Global Log, DNS Log
FTP Analysis	Global Log, FTP Log
IM Analysis	Global Log, ICQ Log, MSN Log, YAHOO Log

* *Security Analysis* is only available in Capsa Enterprise.

Global Log

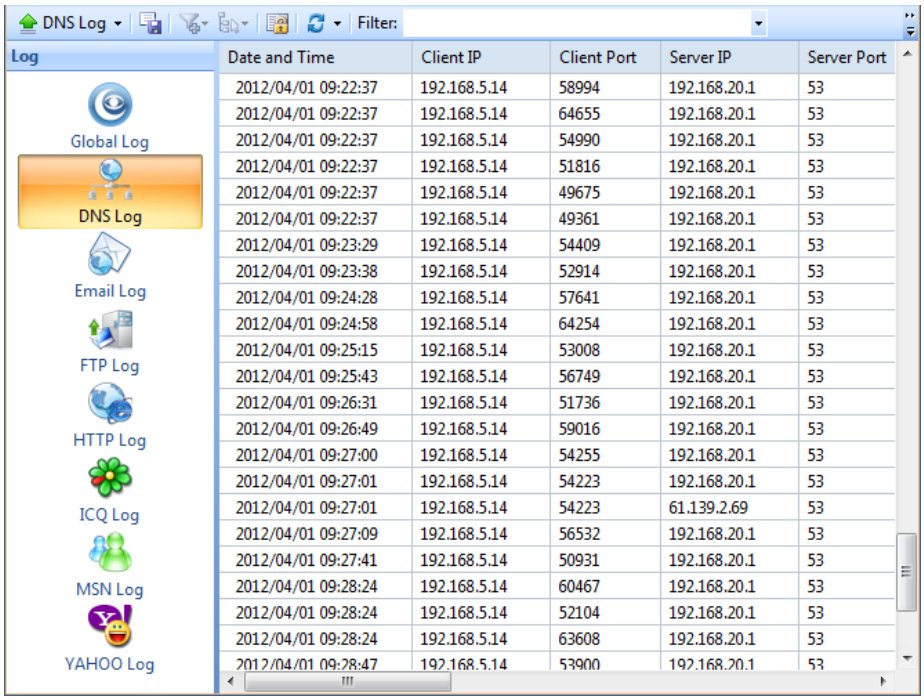
The **Global Log** collects the logs of other seven log types and displays the log information based on date and time. It appears as below.



The **Global Log** includes columns **Date and Time**, **Source MAC**, **Source IP**, **Destination MAC**, **Destination IP**, **Protocol**, and **Summary**. To show a column, right-click the column header and select the column.

DNS Log

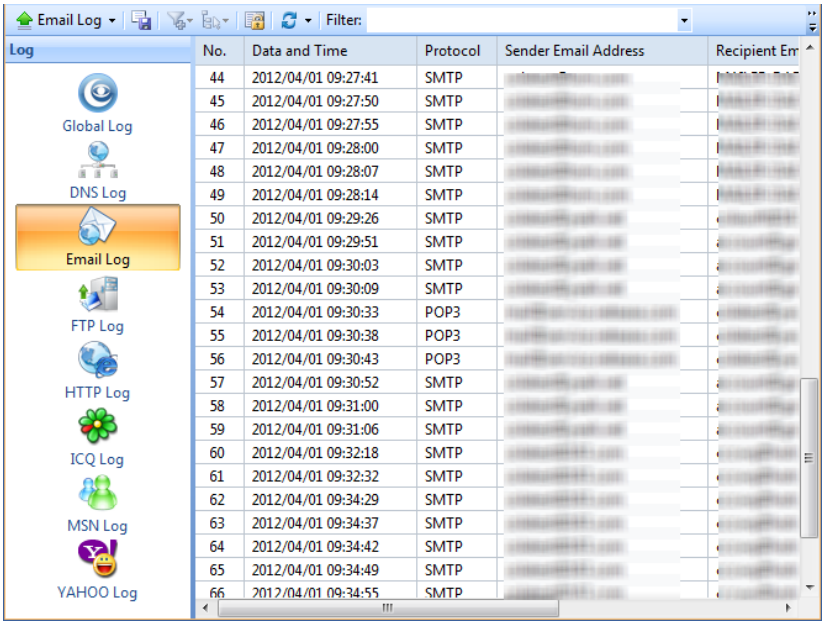
The **DNS Log** records DNS query application. It appears as below.



The **DNS Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Query**, **Status** and **Summary**. To show a column, right-click the column header and select the column.

Email Log

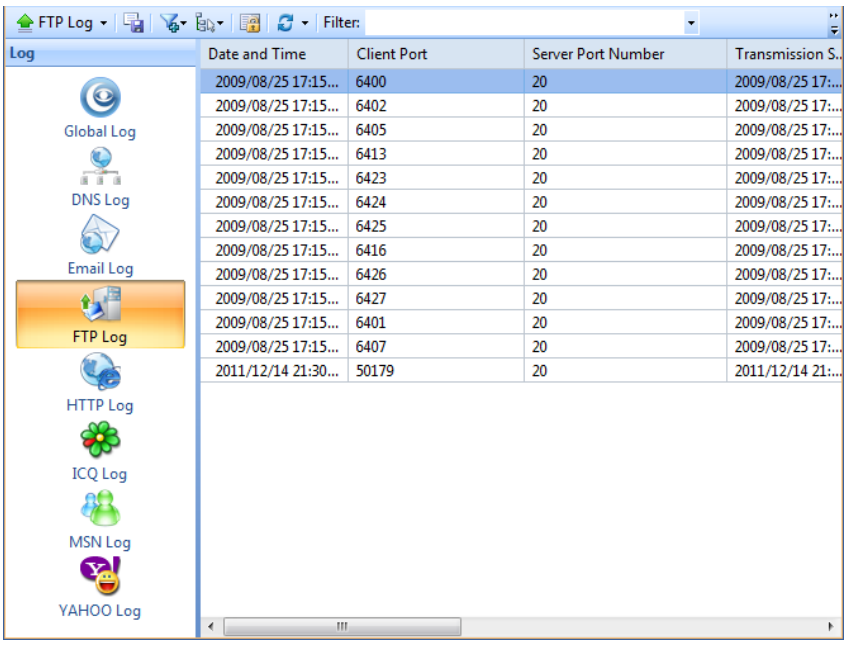
The **Email Log** records the information about the emails sent and received using SMTP and POP3 protocols. Double-click any item of the email log list, the email will be opened. It appears as below.



The Email Log includes columns **No.**, **Date and Time**, **Protocol**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Server**, **Client**, **Sender**, **Sender Email Address**, **Recipient**, **Recipient Email Address**, **Cc**, **Subject**, **Send Time**, **Client Software**, **Account**, **Attachment**, **File Size (Byte)**, **Duration (s)**, **Average Speed (Bps)**, **and Path for Email Copy**. To show a column, right-click the column header and select the column.

FTP Log

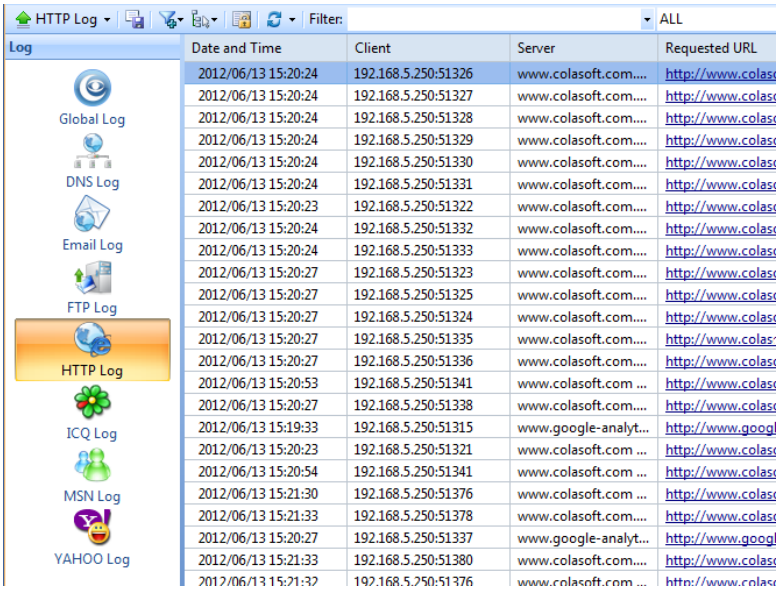
The **FTP Log** records the uploading and downloading from FTP server. It appears as below.



The **FTP Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Server**, **Client**, **Start Time**, **End Time**, **Duration (s)**, **Account**, **Operation Type**, **File**, **Transmission Mode**, **Total Bytes**, **Server Bytes**, **Client Bytes**, **Total Packets**, **Server Packets**, **Client Packets** and **Average Speed (Bps)**. To show a column, right-click the column header and select the column.

HTTP Log

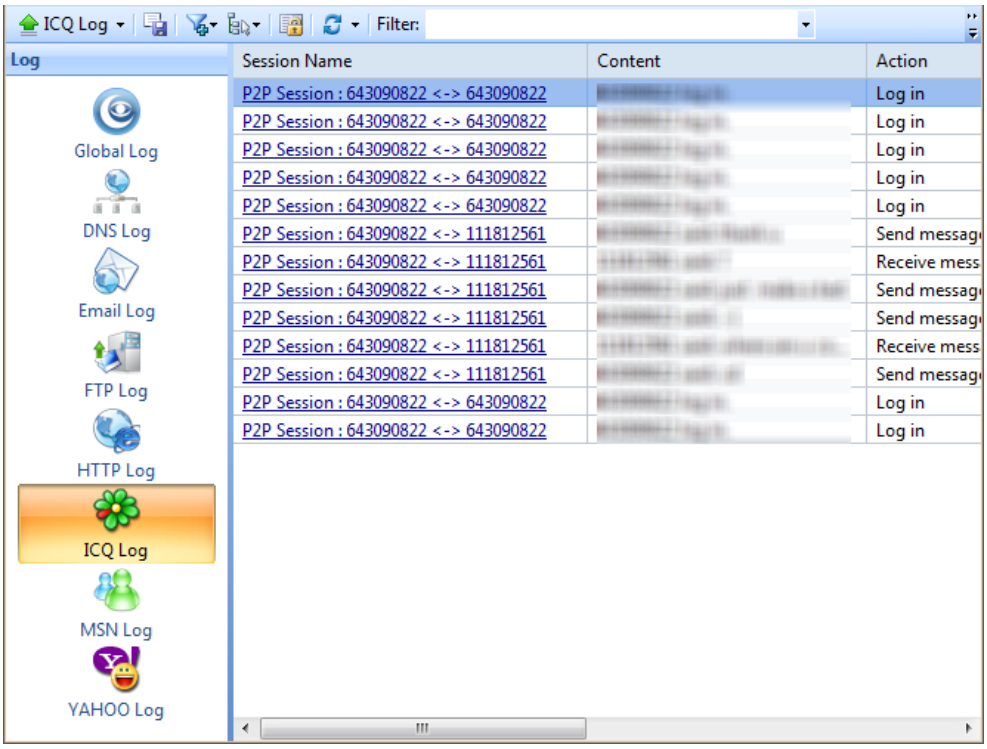
The **HTTP Log** records all web activities and provides log information including time, client and server addresses, requested URL, content length, content type. It appears as below.



The **HTTP Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Client**, **Server**, **Requested URL**, **Method**, **User Agent**, **Quote**, **Content Length**, **Content Type**, **Authentication**, **Client HTTP Version**, **Duration**, **Average Speed (Bps)**, **Status Code** and **Server Response**. To show a column, right-click the column header and select the column.

ICQ Log

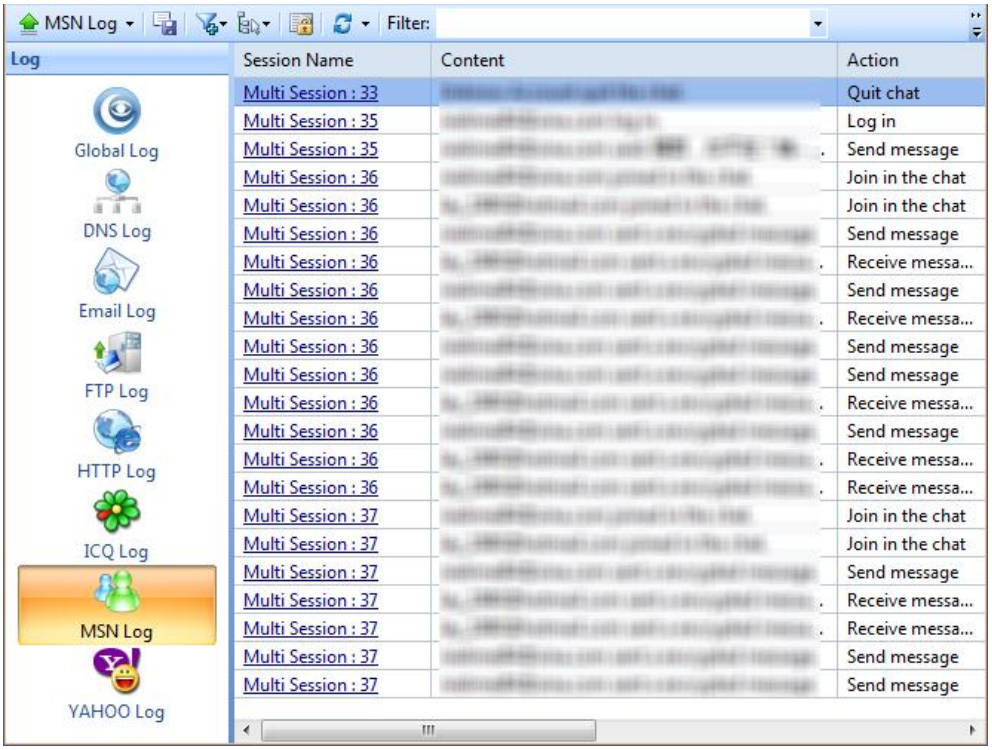
The **ICQ Log** records ICQ conversations automatically in real time, and exports all intercepted messages to files for later processing and analyzing. It appears as below.



The **ICQ Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Session Name**, **Content**, **Action**, **Sender Account**, **Receiver Account**, and **IM Type**. To show a column, right-click the column header and select the column.

MSN Log

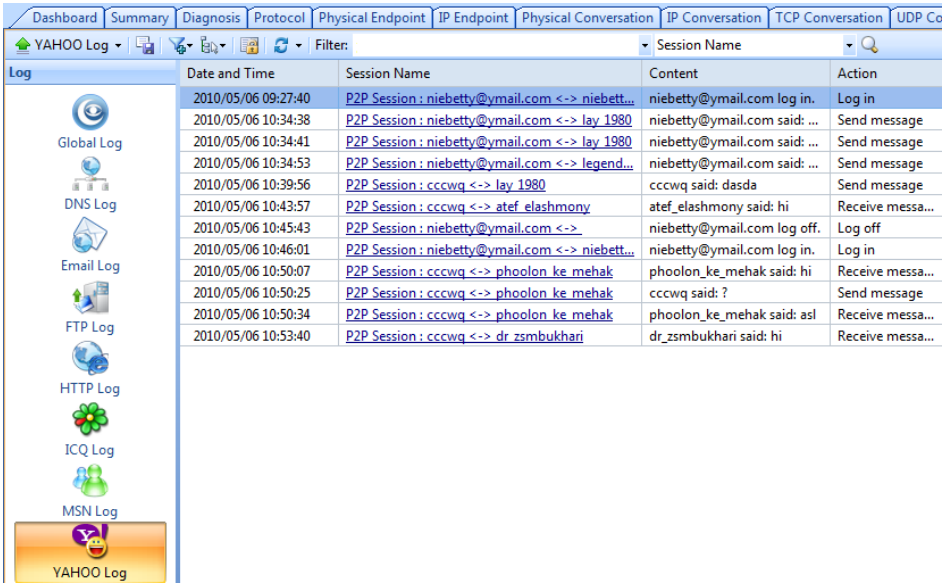
The **MSN Log** records MSN communications over the network, including communication date and time, session name, message content, action status, and the communication accounts. You can read the messages in plain text and login and logout status records. It appears as below.



The **MSN Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Session Name**, **Content**, **Action**, **Sender Account**, **Receiver Account**, and **IM Type**. To show a column, right-click the column header and select the column.

YAHOO Log

The **YAHOO Log** records YAHOO communications over the network, including communication date and time, session name, message content, action status, and the communication accounts. It appears as below.



You can click the session name or double-click the items to open the Notepad to view the detailed communication of the session name.

The **YAHOO Log** includes columns **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Server IP**, **Server Port**, **Session**

Name, **Content**, **Action**, **Sender Account**, **Receiver Account**, and **IM Type**. To show a column, right-click the column header and select the column.

Configurations in Capsa

Before using Capsa to capture network traffic, you may do some configurations about the program, like configurations for system options, network profile settings and analysis profile settings; and after starting an analysis project, you may also do some configurations about the project, like settings for address display format, settings for the columns of statistical views, operations on graphs and reports, and other settings for the program.

All of said settings can be memorized by Capsa, so there is no need for you to do the configurations every time when launching the program. For example, you can specify the arrangement order and the width for the columns of **IP Endpoint** view for an analysis project. The **IP Endpoint** view will display the columns with specified order and width the next time you launch the program.

The configurations that can be memorized by Capsa and need no repeated operations include:

- The selection on network adapters, the selection on network profile, and the selection on analysis profile.
- The keys for APs.
- All settings for network profile.
- All settings for analysis profile.
- The show status and width for the columns of all statistical views.
- All dashboard panels and all charts on the panels.
- All matrices and the settings for each matrix.
- All reports and the settings for each report.
- All settings for system options.
- The settings for address display format.
- All settings from toolbars and pop-up menus of all statistical views.

Note The selection on network adapters, the selection on network profile, and the selection on analysis profile will be memorized only when these selections are applied to an analysis project.

If you want the programs installed on different machines have the same analysis settings, you should use global configurations. See *Global configurations* for details.

Global configurations

Global configurations mean the configurations for the program. Global configurations contain configurations as follows:

- Network profile settings, including default network profiles, user-defined network profiles, the selection on the network profile, General Settings, Node Group, Name Table, and Alarm Settings.
- Analysis profile settings, including default analysis profiles, user-defined analysis profiles, Basic Settings of the analysis profiles, Analysis Object, Packets Buffer, Packet Filter, Log Output, Log settings, Diagnosis Settings, Packets Output, and View Display.
- Dashboard, including default dashboard panel and user-defined dashboard panels, and the charts on the panels.

- Matrix, including default matrix and user-defined matrices.
- Report, including default report and user-defined reports.

This function is very useful when you want Capsa on different machines to have the same configurations, or when you configure Capsa after reinstalling the operating system. Just by some simple clicks, you can achieve said purposes.

- To export global configurations, click **Menu Button**  , point **Global Configurations** and select **Export global configurations** to export the global configurations as .csbak file.
- To import global configurations, click **Menu Button**  , point **Global Configurations** and select **Import global configurations**.

System Options

To open the **System Options** dialog box, click the **Menu** button and select **Options** on the bottom-right corner of the menu.

The **System Options** dialog box includes six tabs as below:

- *Basic Settings*
- *Decoder Settings*
- *Protocol Settings*
- *Task Scheduler*
- *Report Settings*
- *Display Format*

Basic Settings

This tab includes six options:

- **Always maximize the window when starting the program:** Always maximizes the program window when launching the program.
- **Disable windows from suspending during capture:** The power option schema in your system control panel will be ignored. You cannot standby or hibernate your system without stop Capsa from capturing.
- **Disable list smooth scrolling:** Instant scrolling will be enabled if you select this option.
- **Disable list sorting if item count reaches:** If the item count reaches the limitation, the columns of the statistical views cannot be automatically sorted by clicking the column headers.
- **Show Save Packet dialog box on exit:** The program will pop-up a dialog box to remind you to save the packets in the buffer when exiting the program.
- **Show Online Resource window on start:** The **Online Resource** window will be shown on the right side of the program when launching the program.
- **Show wireless network disconnection message on starting wireless analysis**: Shows wireless network disconnection message when starting a wireless analysis project using the wireless network adapter.

Default: Click to reset all settings on this tab.

Decoder Settings

This tab lists all decoding modules of Capsa. All decoders are modularized and you can enable or disable them by the check boxes. By default, all decoders are enabled.

There are only two buttons

 : Enables all decoders.

 : Disables all decoders.

Protocol Settings

This tab is used to manage default protocols and user-defined protocols.

Note that you cannot make any changes to the protocols or create a new one when there is a capture running (You need to stop all captures and go back to the *Start Page*). In a capture, you can only view the existing protocols.

Protocol List

You can click any of the column headers to rearrange the protocols in descending order or in ascending order.

You can double-click a protocol item to edit it. You are not allowed to modify the color of the pre-specified protocols.

Display Filter

There are two protocol filters on the top for you to locate a certain type of protocol.

- **Select protocol**: Displays the selected type of protocol in the list and hide the rest, e.g. **Ethernet II**, **IP**, **TCP** and **UDP**.
- **Filter display**: Displays the protocols by their status, e.g. **All Protocols**, **built-in Protocols**, **Customized Protocols** and **Modified Protocols**.

Buttons

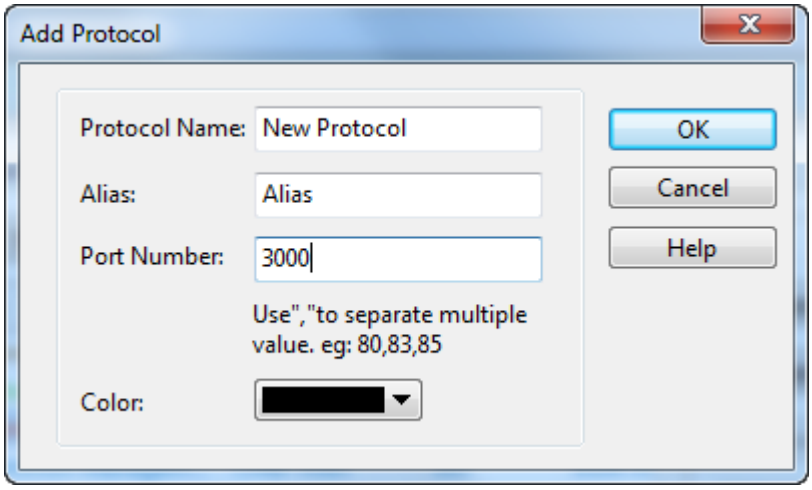
- **Add**: Creates a new rule to identify a new protocol.
- **Edit**: Edits a highlighted protocol item.
- **Delete**: Deletes a highlighted protocol item.
- **Import**: Reads the protocol list from a *.cscpro* file.
- **Export**: Saves the protocol list to a *.cscpro* file.
- **Default**: Resets the protocol list. All user-defined protocols will be deleted and built-in protocols will be reset. You should be careful of clicking this button.

You cannot delete any built-in protocols and when you are running a capture, the buttons above will be disabled. You need to stop all the captures and go back to the *Start Page*, then the buttons will be enabled again.

Adding protocols

To add a protocol, click **Add** to open the **Add Protocol** dialog box in which you can specify the protocol name, the alias, and the port number for the protocol. You can add up to forty protocols.

The **Add Protocol** dialog box appears as below.



Task Scheduler

To capture network packets of a specific period of time, you can utilize the function of scheduling project, which makes the program run a new project to capture packets at the specified time.

To schedule a project:

1. Click menu button  , click **Options**, and then click the **Task Scheduler** tab.
2. Click **Add**, and then type the name of the project, set the frequency for running the project and select appropriate analysis profile, network profile and network adapter.
3. Click **OK** to close the **Schedule Project** dialog box.

The **Task Scheduler** tab provides a list of all scheduled projects you created and five buttons, wherein the list contains: **Name** which means the name of the project, **Create Time** which indicates the time when the scheduled project was created, **Schedule** which shows times that the scheduled project runs, and **Start Time** showing the specific time to run the scheduled project. The five buttons on the right includes:

- **Add**: Schedules a new analysis project.
- **Edit**: Edits the selected project.
- **Delete**: Deletes the selected project.
- **Import**: Removes existing projects in the list and imports new scheduled tasks.
- **Export**: Exports existing projects in the list as a.dat file.

The **New Task** dialog box includes following parts:

- **Name**: Shows the name of the scheduled project, named with time by default.
- **Schedule**: Sets the schedule to run a task. You can choose to schedule the task at one time, or on a daily or weekly schedule. The time you set is relative to the time zone that is set on the computer that runs the task.
    - If you select the **One time** radio button, you set a start date and time to start the task and an end date and time to end

the task.

- If you select the **Daily** radio button, you set a start time to start the task and an end time to end the task. The task will run at the start time every day as long as the program is on.
- If you select the **Weekly** radio button, you set a start time to start the task, an end time to end the task, and the days of the week in which to start the task. The task will run at the specified time on each of the specified days.

- **Options**: Sets analysis profile, network profile and network adapter for the scheduled task.

Report Settings

You can configure the following options listed below:

Company Name: Enable this item (disabled by default), enter your company name into the textbox. It will be displayed on the top left corner of **Report** tab.

Prefix: Enable this item (disabled by default), enter a name into the textbox, which will be added before all report title as a prefix. You can find it on the top left corner of a report in title area.

Author: Enable this item (disabled by default), enter the name of whoever generate the reports, which will be displayed on the bottom right corner of reports.

Show Create Time: This item enabled, the time when a report is generated will be displayed on the top left corner of the report. This item is disabled by default with nothing shown in that area.

Company logo: Enable this item (disabled by default), select a picture file on your machine or shared network folder as the logo of your company, which will be displayed on the top right corner of **Report** tab.

Display Format

The **Display Format** tab lets you customize the format of decimals and measures. 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.

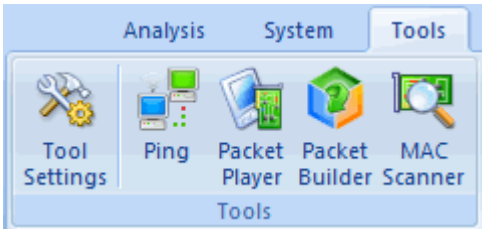
The items on this tab are described as below.

- **Precision after decimal:** The display precision of a number. You can customize the decimal places though the thousandth in default.
- **Precision behind percentage decimal:** The display precision of a percentage. You can customize the decimal places though the thousandth in default.
- **Byte measure:** By default, the program 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.
- **Bit measure:** By default, the program 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.
- **Byte/second measure:** The measure of bytes per second. It could be Bps, KBps, MBps, GBps, and TBps. which means bytes per second, kilobytes per second, megabytes per second, gigabytes per second, and terabytes per second respectively.

- **Bit/second measure:** The measure of bits per second. It could be bps, Kbps, Mbps, Gbps, and Tbps. which means bits per second, kilobits per second, megabits per second, gigabits per second, and terabits per second respectively.
- **Default**: Resets all the settings on this tab to default.

Network Tools

For your convenience on network management, Capsa provides four network tools on the **Tools** tab which appears as follows:



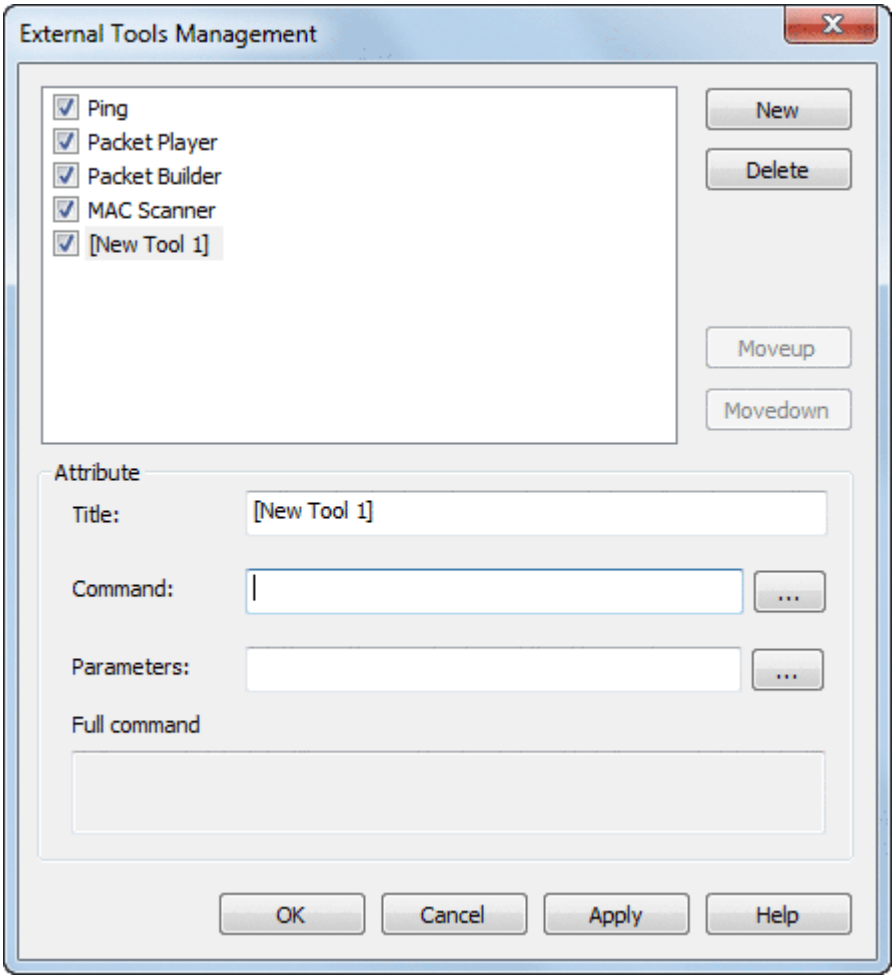
- *Tool Settings*: Opens the **External Tools Management** dialog box to manage the external tools.
- *Ping*: Launches Colasoft Ping Tool.
- *MAC Scanner*: Launches Colasoft MAC Scanner.
- *Packet Player*: Launches Colasoft Packet Player.
- *Packet Builder*: Launches Colasoft Packet Builder.

Tool Settings

In addition to the four tools provided by default, users can add other *Windows* applications and tools into Colasoft Capsa with the **External Tools Management** dialog box. You cannot only invoke but also execute the added applications and tools via Colasoft Capsa.

To open **External Tools Management** dialog box, click **Tool Settings** in **Tools** tab of the **Ribbon**.

The **External Tools Management** dialog box appears.



You can click **New** to attach new tools, **Delete** to delete your selected Tool in Left pane. And also you can rearrange the listed items order by **Move up** and **Move Down**.

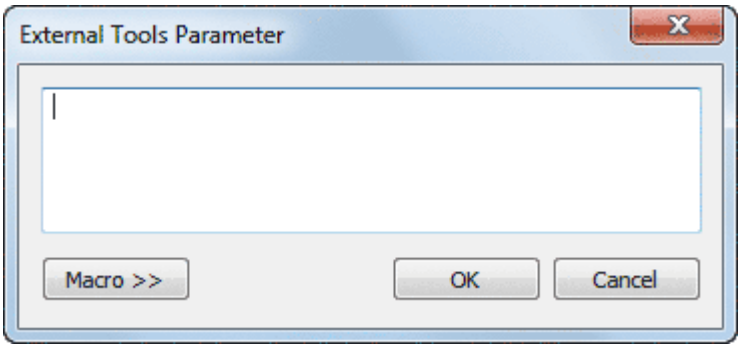
To demonstrate, you can follow the steps below to attach the **Tracert** command of Windows into Colasoft Capsa.

1. Click the **New** button, the **Attribute** pane appears.

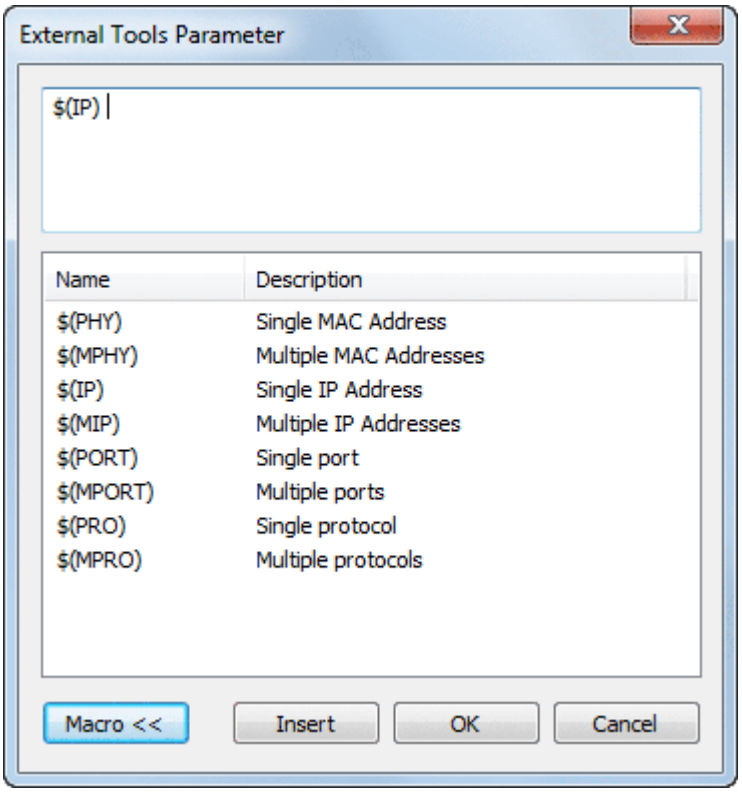
2. Enter *Tracert* in **Title** textbox as its name.

3. Enter the path of the program in Command: *C:\WINDOWS\system32\tracert.exe*, or click ... to choose the path.

4. Click ... after Parameters textbox. The **External Tools Parameter** dialog box appears.



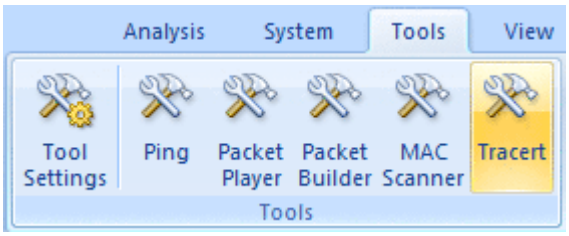
5. Click the **Macro >>** button to view the details.



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 are 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.

6. Choose the IP Address and click **Insert** and then click **OK** to save the settings and back to the **External Tools Management** dialog box.

Now you can find **Tracert** icon in **Tools** tab of the **Ribbon**. Click it to open tracert command.



Appendices

FAQ

Q: What can I do with Capsa?

A:

Network administrators: Diagnose network faults, detect the PC infected virus, monitor network traffic, analyze network protocols, and detect network vulnerability.

Company IT administrators: Monitor the overall network health and infrastructure health, and view the statistics and reports.

Security managers: Monitor all network activities to detect any violations of the company security policy with forensic analysis.

Consultants: Analyze network troubleshoots, solve network problems for customers, and optimize network capability.

Network application developers: Debug network applications, optimize program capability, test the content sent/received, and examine network protocols.

Q: Can I set up my own traffic filter?

A: Yes, in Capsa, setting up a set of rules can help you filter the traffic you are interested in. The filters help user to speed up analyzing and displaying packets, enabling you to focus on what you are really interested in. Capsa has two kinds of filters: global filters and project filters. Global filters are some commonly used protocols filters, which can be applied to the current project. Project filters are only applied to the current project.

Q: Can Capsa monitor the traffic utilization in the network?

A: Yes, Capsa provides users with detailed network statistics information of the overall network or each network segment, traffic utilization status, top talkers, congestion, MAC/IP address or protocol, bitrate, and TCP transaction statistic etc..

Q: Our LAN is connected with a hub, but I can only detect my own traffic.

A: Generally, if a NIC supports promiscuous mode it can work well with Capsa, a possible reason is your hub actually acts as a switch though labeled as a hub (e.g. Linksys hubs). Another possible reason is you are using a multi-speed hub, in which case you can't see the traffic from the stations operating at the speed that is different from your NIC's speed (e.g. if you have a 10 Mbit NIC, you can't see the traffic generated by 100 Mbit NICs).

Q: How to configure port mirroring?

A: Please read your switch's manual or visit its website to learn how to setup port mirroring. Or you may ask their technicians for help.

Q: Does Colasoft Capsa enable me as a network administrator to easily see who is listening to the radio and downloading music online?

A: Yes. The standard ports for media protocols are: RTSP - port 554 PNM - port 7070 (also known as PNA port) MMS - port 1755 By setting port filters in the "Project Settings - Filter" dialog box you can easily find out who is visiting media resources; to monitor the downloads of media files (e.g. .rm), you can set a URL filter for HTTP analysis in the "Project Settings - Advanced Analyzer" dialog box.

Q: Why don't I see the Dashboard tab sometimes?

A: The Dashboard is visible only when you select the root node in the Node Explorer. That's because the Dashboard is global, which doesn't belong to any specific node in the Node Explorer. When a node selected in the Node Explorer, only the tabs relating to the

selected is visible.

Q: After I entered the serial number and license key, they didn't work.

A: Please copy and paste the serial number and license key you received from us to the fields required, it may include unnecessary blank or input error if you type in the numbers.

If you are Free edition user, you need to apply for a serial number first at: *Apply License*, and the serial number will be sent to your mailbox in a minute.

Q: Can I export packets captured, log, reports and graphs in different formats?

A: Yes. Capsa can export packets in many formats, and export log, reports, and graphs in many file and image formats. Please check the relative section to get the details.

Q: Does Capsa support RADIUS protocols?

A: Yes. Capsa can capture and analyze RADIUS packets and protocols.

We keep updating more FAQs on our official website. Please visit *Colasoft.com* to learn more.

Ethernet Type Codes

Ethernet		Exp. Ethernet		Description
decimal	Hex	decimal	octal	
0000	0000-05DC			IEEE802.3LengthField
0257	0101-01FF	-	-	Experimental
0512	0200	512	1000	XEROX PUP (see 0A00)
0513	0201	-	-	PUP Addr Trans (see 0A01)
	0400	-	-	Nixdorf
1536	0600	1536	3000	XEROX NS IDP
	0660	-	-	DLOG
	0661	-	-	DLOG
2048	0800	513	1001	Internet IP (IPv4)
2049	0801	-	-	X.75 Internet
2050	0802	-	-	NBS Internet
2051	0803	-	-	ECMA Internet
2052	0804	-	-	Chaosnet
2053	0805	-	-	X.25 Level 3
2054	0806	-	-	ARP
2055	0807	-	-	XNS Compatability
2056	0808	-	-	Frame Relay ARP
2076	081C	-	-	Symbolics Private
2184	0888-088A	-	-	Xyplex
2304	0900	-	-	Ungermann-Bass net debugr
2560	0A00	-	-	Xerox IEEE802.3 PUP
2561	0A01	-	-	PUP Addr Trans
2989	0BAD	-	-	Banyan VINES
2990	0BAE	-	-	VINES Loopback
2991	0BAF	-	-	VINES Echo
4096	1000	-	-	Berkeley Trailer nego
4097	1001-100F	-	-	Berkeley Trailer encap/IP
5632	1600	-	-	Valid Systems

16962	4242	-	-	PCS Basic Block Protocol
21000	5208	-	-	BBN Simnet
24576	6000	-	-	DEC Unassigned (Exp.)
24577	6001	-	-	DEC MOP Dump/Load
24578	6002	-	-	DEC MOP Remote Console
24579	6003	-	-	DEC DECNET Phase IV Route
24580	6004	-	-	DEC LAT
24581	6005	-	-	DEC Diagnostic Protocol
24582	6006	-	-	DEC Customer Protocol
24583	6007	-	-	DEC LAVC, SCA
24584	6008-6009	-	-	DEC Unassigned
24586	6010-6014	-	-	3Com Corporation
25944	6558	-	-	Trans Ether Bridging
25945	6559	-	-	Raw Frame Relay
28672	7000	-	-	Ungermann-Bass download
28674	7002	-	-	Ungermann-Bass dia/loop
28704	7020-7029	-	-	LRT
28720	7030	-	-	Proteon
28724	7034	-	-	Cabletron
32771	8003	-	-	Cronus VLN
32772	8004	-	-	Cronus Direct
32773	8005	-	-	HP Probe
32774	8006	-	-	Nestar
32776	8008	-	-	AT&T
32784	8010	-	-	Excelan
32787	8013	-	-	SGI diagnostics
32788	8014	-	-	SGI network games
32789	8015	-	-	SGI reserved
32790	8016	-	-	SGI bounce server
32793	8019	-	-	Apollo Domain
32815	802E	-	-	Tymshare
32816	802F	-	-	Tigan, Inc.
32821	8035	-	-	Reverse ARP
32822	8036	-	-	Aeonic Systems
32824	8038	-	-	DEC LANBridge
32825	8039-803C	-	-	DEC Unassigned
32829	803D	-	-	DEC Ethernet Encryption
32830	803E	-	-	DEC Unassigned
32831	803F	-	-	DEC LAN Traffic Monitor
32832	8040-8042	-	-	DEC Unassigned
32836	8044	-	-	Planning Research Corp.
32838	8046	-	-	AT&T
32839	8047	-	-	AT&T
32841	8049	-	-	ExperData
32859	805B	-	-	Stanford V Kernel exp.
32860	805C	-	-	Stanford V Kernel prod.
32861	805D	-	-	Evans & Sutherland
32864	8060	-	-	Little Machines
32866	8062	-	-	Counterpoint Computers
32869	8065	-	-	Univ. of Mass. @A mherst
32870	8066	-	-	Univ. of Mass. @ Amherst
32871	8067	-	-	Veeco Integrated Auto.

32872	8068	-	-	General Dynamics
32873	8069	-	-	AT&T
32874	806A	-	-	Autophon
32876	806C	-	-	ComDesign
32877	806D	-	-	Computgraphic Corp.
32878	806E-8077	-	-	Landmark Graphics Corp.
32890	807A	-	-	Matra
32891	807B	-	-	Dansk Data Elektronik
32892	807C	-	-	Merit Internodal
32893	807D-807F	-	-	Vitalink Communications
32896	8080	-	-	Vitalink TransLAN III
32897	8081-8083	-	-	Counterpoint Computers
32923	809B	-	-	Appletalk
32924	809C-809E	-	-	Datability
32927	809F	-	-	Spider Systems Ltd.
32931	80A3	-	-	Nixdorf Computers
32932	80A4-80B3	-	-	Siemens Gammasonics Inc.
32960	80C0-80C3	-	-	DCA Data Exchange Cluster
32964	80C4	-	-	Banyan Systems
32965	80C5	-	-	Banyan Systems
32966	80C6	-	-	Pacer Software
32967	80C7	-	-	Applitek Corporation
32968	80C8-80CC	-	-	Intergraph Corporation
32973	80CD-80CE	-	-	Harris Corporation
32975	80CF-80D2	-	-	Taylor Instrument
32979	80D3-80D4	-	-	Rosemount Corporation
32981	80D5	-	-	IBM SNA Service on Ether
32989	80DD	-	-	Varian Associates
32990	80DE-80DF	-	-	Integrated Solutions TRFS
32992	80E0-80E3	-	-	Allen-Bradley
32996	80E4-80F0	-	-	Datability
33010	80F2	-	-	Retix
33011	80F3	-	-	AppleTalk AARP (Kinetics)
33012	80F4-80F5	-	-	Kinetics
33015	80F7	-	-	Apollo Computer
33023	80FF-8103	-	-	Wellfleet Communications
33031	8107-8109	-	-	Symbolics Private
33072	8130	-	-	Hayes Microcomputers
33073	8131	-	-	VG Laboratory Systems
33074	8132-8136	-	-	Bridge Communications
33079	8137-8138	-	-	Novell, Inc.
33081	8139-813D	-	-	KTI
	8148	-	-	Logicraft
	8149	-	-	Network Computing Devices
	814A	-	-	Alpha Micro
33100	814C	-	-	- SNMP
	814D	-	-	BIIN
	814E	-	-	BIIN
	814F	-	-	Technically Elite Concept
	8150	-	-	Rational Corp
	8151-8153	-	-	Qualcomm
	815C-815E	-	-	Computer Protocol Pty Ltd

	8164-8166	-	-	Charles River Data System
	817D	-	-	XTP
	817E	-	-	SGI/Time Warner prop.
	8180	-	-	HIPPI-FP encapsulation
	8181	-	-	STP, HIPPI-ST
	8182	-	-	Reserved for HIPPI-6400
	8183	-	-	Reserved for HIPPI-6400
	8184-818C	-	-	Silicon Graphics prop.
	818D	-	-	Motorola Computer
	819A-81A3	-	-	Qualcomm
	81A4	-	-	ARAI Bunkichi
	81A5-81AE	-	-	RAD Network Devices
	81B7-81B9	-	-	Xyplex
	81CC-81D5	-	-	Apricot Computers
	81D6-81DD	-	-	Artisoft
	81E6-81EF	-	-	Polygon
	81F0-81F2	-	-	Comsat Labs
	81F3-81F5	-	-	SAIC
	81F6-81F8	-	-	VG Analytical
	8203-8205	-	-	Quantum Software
	8221-8222	-	-	Ascom Banking Systems
	823E-8240	-	-	Advanced Encryption Syste
	827F-8282	-	-	Athena Programming
	8263-826A	-	-	Charles River Data System
	829A-829B	-	-	Inst Ind Info Tech
	829C-82AB	-	-	Taurus Controls
	82AC-8693	-	-	Walker Richer & Quinn
	8694-869D	-	-	Idea Courier
	869E-86A1	-	-	Computer Network Tech
	86A3-86AC	-	-	Gateway Communications
	86DB	-	-	SECTRA
	86DE	-	-	Delta Controls
	86DD	-	-	IPv6
34543	86DF	-	-	ATOMIC
	86E0-86EF	-	-	Landis & Gyr Powers
	8700-8710	-	-	Motorola
34667	876B	-	-	TCP/IP Compression
34668	876C	-	-	IP Autonomous Systems
34669	876D	-	-	Secure Data
	880B	-	-	PPP
	8847	-	-	MPLS Unicast
	8848	-	-	MPLS Multicast
	8A96-8A97	-	-	Invisible Software
36864	9000	-	-	Loopback
36865	9001	-	-	3Com(Bridge) XNS Sys Mgmt
36866	9002	-	-	3Com(Bridge) TCP-IP Sys
36867	9003	-	-	3Com(Bridge) loop detect
65280	FF00	-	-	BBN VITAL-LanBridge cache
	FF00-FF0F	-	-	ISC Bunker Ramo
65535	FFFF	-	-	Reserved

HTTP Status Codes

Status code	Description
100	Continue--the request can be continued.
101	Switch protocols--the server has switched protocols in an upgrade header.
200	OK-- the request was fulfilled.
201	Created--the request successful and a new resource was created.
202	Accepted--the request has been accepted for processing, but processing is not completed.
203	Non-Authoritative Information--the returned information is only partial.
204	No Content--the request received but no information exists to send back.
205	Reset Content--the request was successful but the User-Agent should reset the document view that caused the request.
206	Partial Content--the partial GET request has been successful.
300	Multiple Choices--the request resource has multiple possibilities, each with different locations.
301	Moved Permanently--the data requested has a new location and the change is permanent.
302	Found--the data requested has a different URL temporarily.
303	See Other--the requested response is at a different URI and should be accessed using a GET command at the given URI.
304	Not Modified--the document has not been modified as expected.
305	Use Proxy--the requested resource can only be accessed through the proxy specified in the location field.
306	No Longer Used--reserved for future use.
307	Redirect Keep Verb--the redirected request keeps the same HTTP verb. HTTP/1.1 behavior.
400	Bad request--syntax problem in the request or it could not be satisfied.
401	Unauthorized--the client is not authorized to access data.
402	Payment required--indicates a charging scheme is in effect.
403	Forbidden--access not required even with authorization.
404	Not found--server could not find the given resource.
405	Method Not Allowed--the HTTP verb is not allowed.
406	Not Acceptable--no responses acceptable to the client were found.
407	Proxy Auth Req--the request first requires authentication with the proxy.
408	Request Timeout--the client filed to sent a request in the time allowed by the server.
409	Conflict--the request was unsuccessful due to a conflict in the state of the resource.
410	Gone--the resource requested is no longer available and o forwarding address is available.
411	Length Required--the server cannot accept the request without a defined content length.
412	Precondition Failed--a precondition specified in one or more Request-Header fields returned false.
413	Request Entity Too Large--the request was unsuccessful because the request entity is larger than the server will allow.
414	Request URI Too Long--the server cannot service the request because the request URI is longer than the server can interpret.
415	Unsupported Media Type--a server refuses a request because the message body is in an inappropriate format.
416	Requested Range Not Satisfiable--the server could not process the client's partial GET request.
417	Expectation Failed--the expectation given in the Expect request-header could not be fulfilled by the server.
449	Retry With--the request should be retried after doing the appropriate action.
500	Internal Error--the server could not fulfill the request because of an unexpected condition.
501	Not implemented--the sever does not support the facility requested.
502	Bad Gateway--the server received an invalid response from the upstream server while trying to fulfill the request.
503	Service Unavailable--the request was unsuccessful to the server being down or overloaded.
504	Gateway timeout--server waited for another service that did not complete in time.
505	HTTP Version Not Supported--the server does not support or is not allowing the HTTP protocol version specified in the request.