Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

User Guide

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

Contact Us

Sales

sales@colasoft.com

Technical Support

support@colasoft.com

Website

http://www.colasoft.com/

Contents

Introduction

Thanks for choosing Capsa, the portable network analyzer from Colasoft.

Trusted by both Fortune 500 as well as small and medium-sized companies as their management solution, Colasoft Capsa offers an easy, yet powerful way for network monitoring, analysis and troubleshooting. By providing vivid graphs, information-rich statistics and real-time alarms via a well-designed GUI, Capsa allows IT administrators to identify, diagnose, and solve both wired and wireless network problems in real time, monitor user activities on their networks, and ensure the safety of network communications.

Overview

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

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

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

Colasoft Capsa supports monitoring multiple adapters, letting you view the traffic passing through your network via different adapters.

Advanced analysis modules provide detailed information about network traffic, allowing you to view the analysis statistics of Email messages, FTP transfers, HTTP requests and DNS analysis and other logs.

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

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

The featured expert diagnosis lists network diagnosis events and provides possible reasons and solutions. Matrix dynamically shows you mapped network traffic between network nodes. Reports provide real-time statistic reports of global network or specific groups.

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

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

Capsa 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 on your network. Colasoft Capsa, in cooperation with other network management tools, will maximize your network value.

Technical Support

For common questions, you can find answers in our Knowledge Base.

If you meet a problem when using the program and cannot solve it after referring to this manual and other material on Colasoft website, you may enquire local agent for more advice or contact Colasoft support team.

Note Licensed users are entitled to obtain higher priority of technical supports from Colasoft and we also offer supports to free users.

1. Website support

   In addition to up-to-date FAQ and Glossary, there is version upgrade information and public resources relevant to Colasoft Capsa available at http://www.colasoft.com.

2. Email support

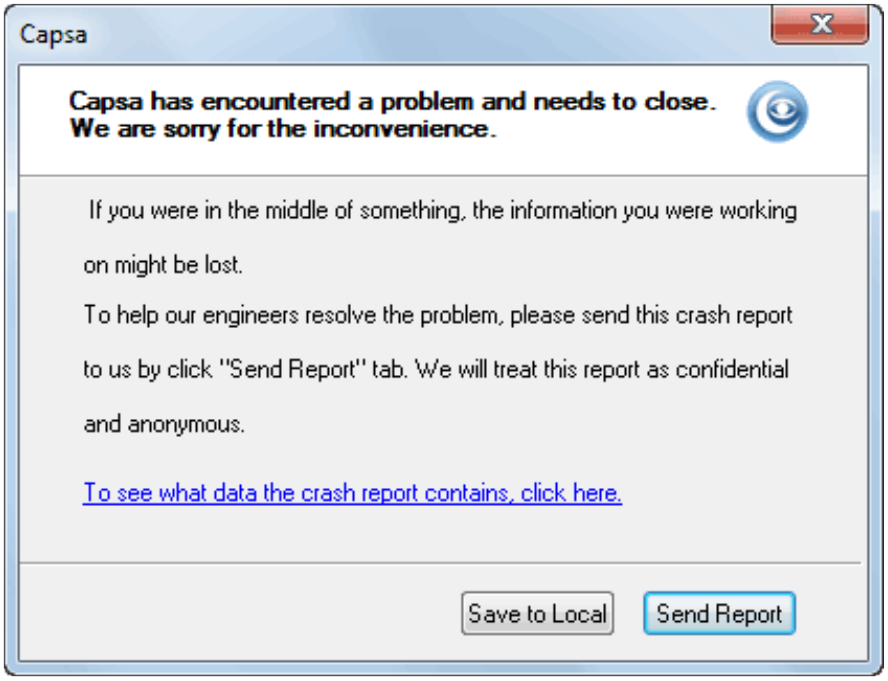
   You are welcome to contact us at support@colasoft.com with technical questions at any time; we will reply you as quickly as possible. In your email please include the serial number, product version and edition, Windows' OS, detailed problem description and other relevant information.

3. Forum support

   We have a large group of Free edition users and we don't directly provide support for free uses via email. If you are using the Free edition, please post your questions at our Support Forum for help, where you can get help and assist from other Free users quickly. Join our support forum to provide your suggestions and discuss our products with other users.

Crash report

When program crashes, Capsa generates a dump file which contains the import information of the causes of the problem, and shows a crash report message box. The dump file tells us where the problem comes from and helps us improve our product. Please click **Send Report** to send the dump file to us. Or, if you have no access to internet, please click **Save to Local** to save the report and send the dump file to us via email. The following figure is a crash report message box:



Error reporting

If you do not see the crash report message box, or you want to report other problems to us, please include the following information:

1. Is the problem reproducible? If so, how?
2. What version of Windows are you running (Windows XP, Windows 7, etc.)?
3. What version of Capsa are you running (to check the version, choose **About** from the **Product** menu)? Please include the entire "version" line in your problem report.
4. If a dialog box with an error message was displayed, please include the full text of the dialog box and the text in title bar.

Tips You can press **F1** for context-sensitive help at any time when the program is active.

Conventions

There are three types of conventions in this user guide document.

Icon conventions

The table below describes the icon conventions used in this user guide document.

Icon	Descriptions
Advice	This icon provides some advice, suggestions, and recommended operations.
Note	You should pay more attention to the descriptions following this icon.
Tips	This icon provides alternative operations which may be more practical.

Description conventions

The table below describes the description conventions used in this user guide document.

Item	Descriptions
Bold font	Indicates the menus, labels, commands, tabs and other elements from the program interface.
Italic font	Indicates reference, cross-reference, or the terms from the glossary.
>	Indicates step-by-step procedures. You can follow these instructions to complete a task.

Mouse action conventions

Action	Description
Click	Press and release the left mouse button once, without moving the mouse.
Right-click	Press and release the right mouse button once, without moving the mouse.
Double-click	Press and release the left mouse button twice within 1 second or less, without moving the mouse.
Drag	Press the left mouse button, hold it down and move the mouse simultaneously.

Editions Comparison

The following table lists the main differences among Capsa Enterprise and Capsa Free.

Key Feature	Capsa Enterprise	Capsa Free
Capture WiFi traffic	YES	NO
Local IP nodes monitored	Unlimited	10
Session timeout length	Unlimited	4 hour
Max packet buffer size	Unlimited	16MB
Customizable dashboards	16	NO
Customizable protocols	40	1
Customizable alarms	40	5
Run multiple projects	YES	NO
Packet auto-output function	YES	NO

Key Feature	Capsa Enterprise	Capsa Free
Replay multiple trace files	YES	NO
Network tap support	YES	NO
Printing	YES	NO
Log output	YES	NO
Multiple adapters support	YES	NO
Auto-scheduling	YES	NO
Email notification upon alarms	YES	NO
Save report	YES	NO
Expert diagnosis	YES	NO
Security analysis setting	YES	NO
Customizing report	YES	NO
ARP Attack view	YES	NO
Worm view	YES	NO
DoS Attacking view	YES	NO
DoS Attacked view	YES	NO
TCP Port Scan view	YES	NO
Suspicious Conversation view	YES	NO
VoIP analysis	YES	NO
Advanced display filter	YES	NO
Analyze IMAP4 emails	YES	NO

Deployment and Installation

This chapter describes how to deploy, install, uninstall and activate Capsa, and describes the system requirements of Capsa.

Deployment Environment

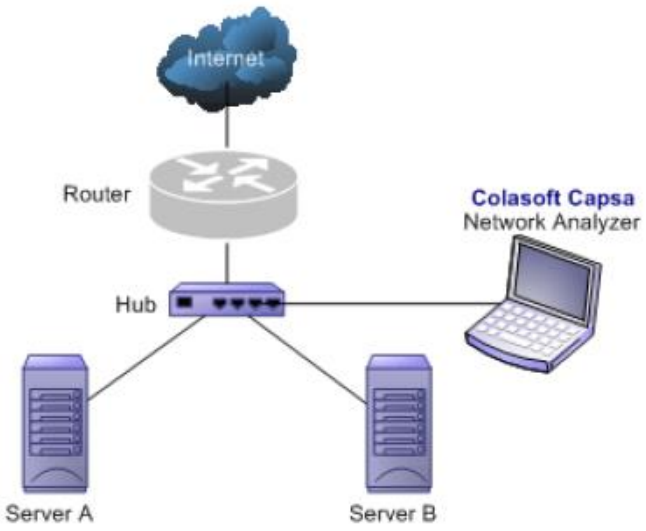
Colasoft Capsa is professional in monitoring and analyzing intranet packets and packets from internet, even packets crossing VLAN. Colasoft Capsa only needs to be installed on the management machine, but other managed clients need not. Administrator needs to decide which machine to install Colasoft Capsa. 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.

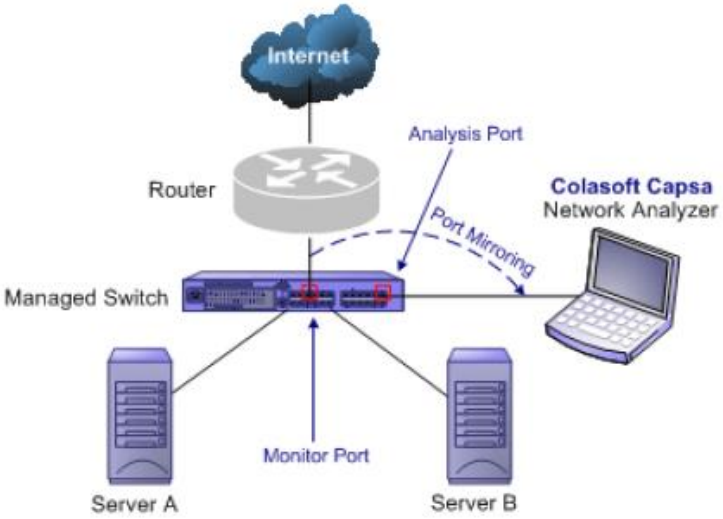
With a shared environment, Colasoft Capsa can be installed on any host in LAN. The entire network data transmitted through the hub will be captured, including the communication between any two hosts in LAN.



Switched network - managed switches (Port mirroring)

Switch is a network device working on the Data Link Layer of OSI. Switch can learn the MAC 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).

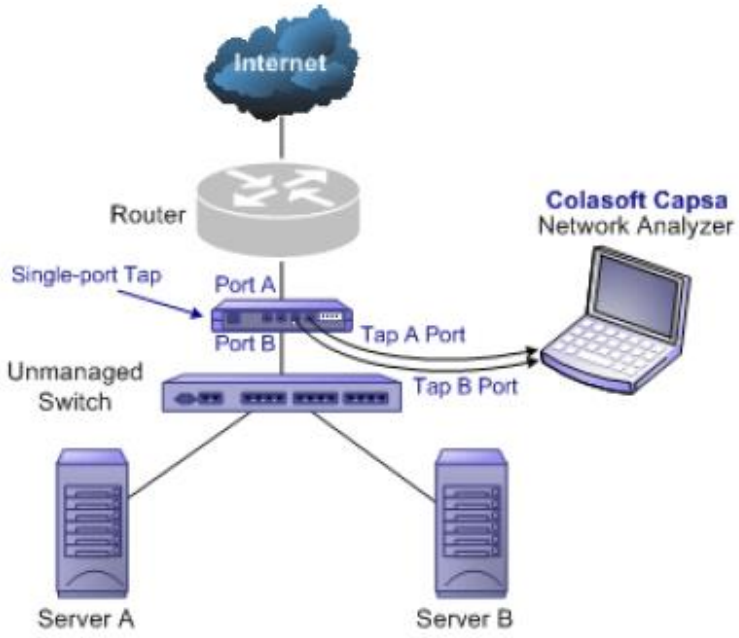


Switched network - unmanaged switches

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.

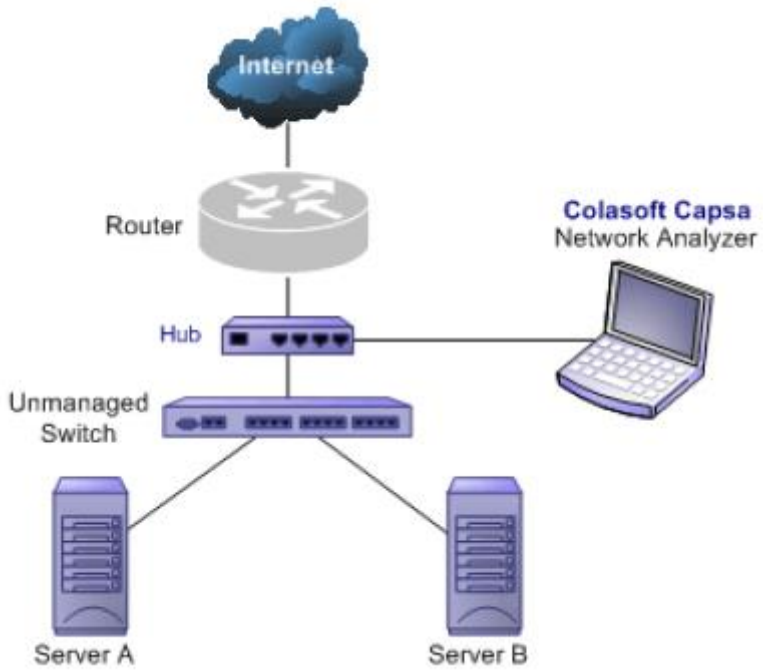
Connect a tap with the line to be monitored

Taps can be flexibly placed on any line in the network. When the requirement for network performance is very high, you can add a tap to connect your network.



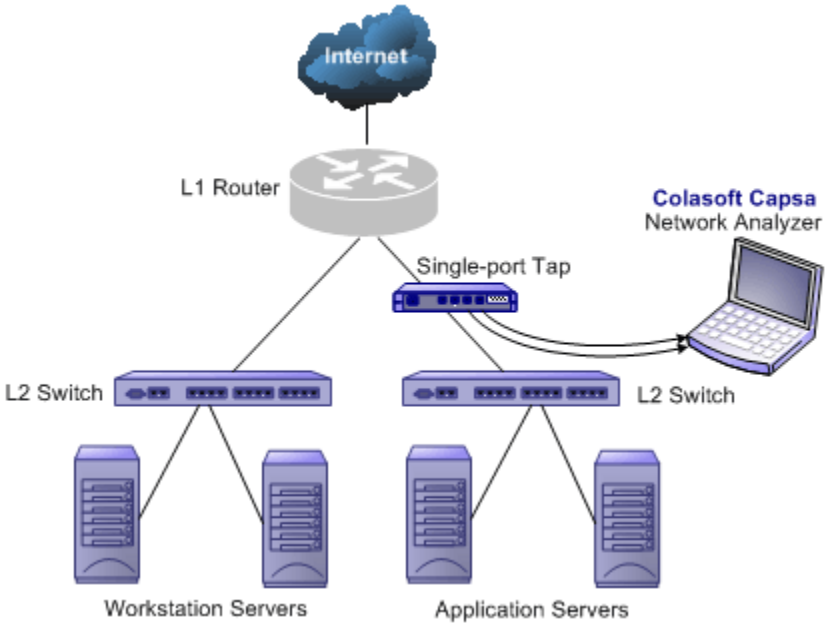
Connect a hub with the line to be monitored

A hub costs lower than a tap but lower performance than a tap in large traffic network.



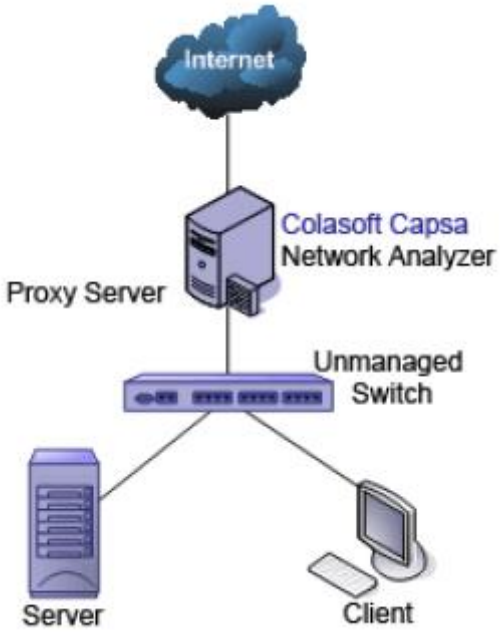
Monitoring a network segment

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.



Hub vs. Tap vs. Switch

Hub	Switch (Mirror Port)	Tap

Positive	• Low cost • No need configuration and settings • No need to change original network topology	• No additional facility required • No need to change original network topology	• No influence to network transmission performance • No interference with data stream and raw data • Does not occupy IP address, free from network attacks • No need to change network topology
Negative	• Additional facility (hub) required • Interference to network transmission performance when meeting huge traffic • Not applicable for big networks	• Occupies a switch port • Possible influence to network transmission performance when meeting huge traffic.	• High cost • Additional facility (tap) required • Requires dual adapters • Cannot connect Internet
Comments	A hub works in a shared network and is common equipment used in early days of network deployment. It has been replaced by simple switches nowadays. A hub is mostly used in a small network.	A management switch has port mirroring function which allows administrator to manage the network. Port mirroring is very applicable which mirrors 1 to 1 or 1 to all ports. Port mirroring is the most common management way at present.	A tap is very applicable to be installed at any place of a network. Under large traffic, a tap should be a reasonable choice if its high cost is ignored.

Tips 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.

Note Tap is not supported by the **Free** Edition.

Switch and 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 Deployment 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. 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 Vista, Windows 7, Windows 8/8.1, Windows 10 Professional. (All are 64-bit version.) 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 2.8 GHz CPU
- 4 GB RAM
- Internet Explorer 6.0

Recommended requirements

- Intel Dual-Core 3.2 GHz CPU
- 8 GB RAM or more
- Internet Explorer 8.0 or higher

Supported Windows Operating Systems

- Windows Server 2008 (64-bit) *
- Windows Server 2012 (64-bit) **
- Windows Vista (64-bit)
- Windows 7 (64-bit)
- Windows 8/8.1 (64-bit)
- Windows 10 Professional (64-bit)

* indicates that wireless analysis module is not compatible with this operating system.

** indicates that Colasoft Packet Builder is not compatible with this operating system.

Supported wireless network adapters

Colasoft Capsa Enterprise supports following wireless network adapters:

- Atheros AR7015, AR6004, AR9380, AR9382, AR9390, AR9485, AR9462, AR958x
- Intel 1000, 4965, 5100, 5150, 5300, 5350, 6200, 6250, 6300, 6350, AC 7260, 82579LM
- Realtek RTL8188CU, RTL8192CU, RTL8187
- Broadcom 4313GN 802.11 b/g/n
- TP-Link TL-WDN3200(5.1.7.5014), TL-822N v2
- D-Link DWA-160 B2(5.1.7.5014)

Note Capturing with wireless network adapters is only available for Capsa Enterprise.

Installation and Uninstall

Before installation:

1. Carefully read Deployment 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/demo/free versions of Colasoft Capsa on your machine.

Installation

1. Double-click the installation file, and the **Welcome** screen appears, telling you that Colasoft Capsa will be installed on your machine. Click **Next** to continue.
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 pops up. 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 pops up. Click the **Browse** button to designate an alternate start menu folder. Click **Next** to continue.
6. **Select Additional Tasks** screen pops up. **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**.

Tips If no changes are made 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 followings:

- To uninstall Colasoft Capsa, choose **Start** > **All Programs** > **Colasoft Capsa** > **Uninstall Colasoft Capsa**.
- Open **Control Panel** > double-click **Programs and Features**, the **Uninstall or change a program** window appears > find Capsa in the list and right-click to **Uninstall**.

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

1. If you want to completely remove Colasoft Capsa 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.

Advice 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.

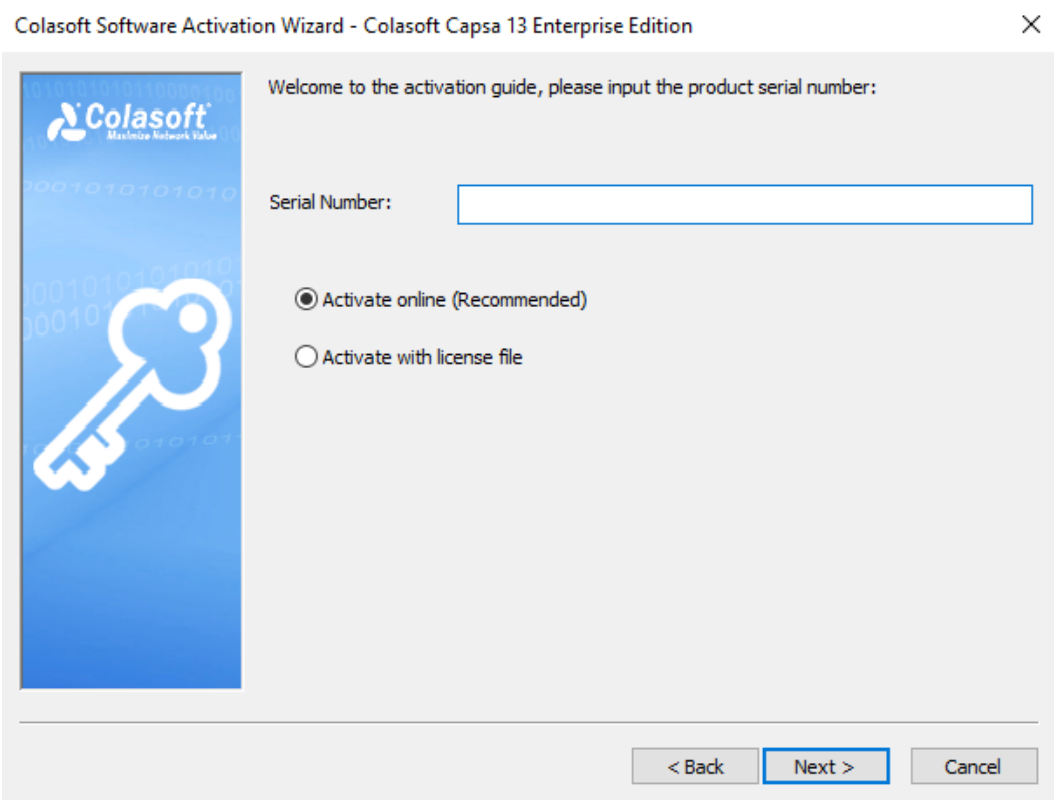
3. To finish uninstall, click **YES** to restart your machine.

Product Activation

After the installation, the Activation Wizard pops up automatically to guide the activation. There are two methods to activate Colasoft Capsa: **Activate online** and **Activate with license file**.

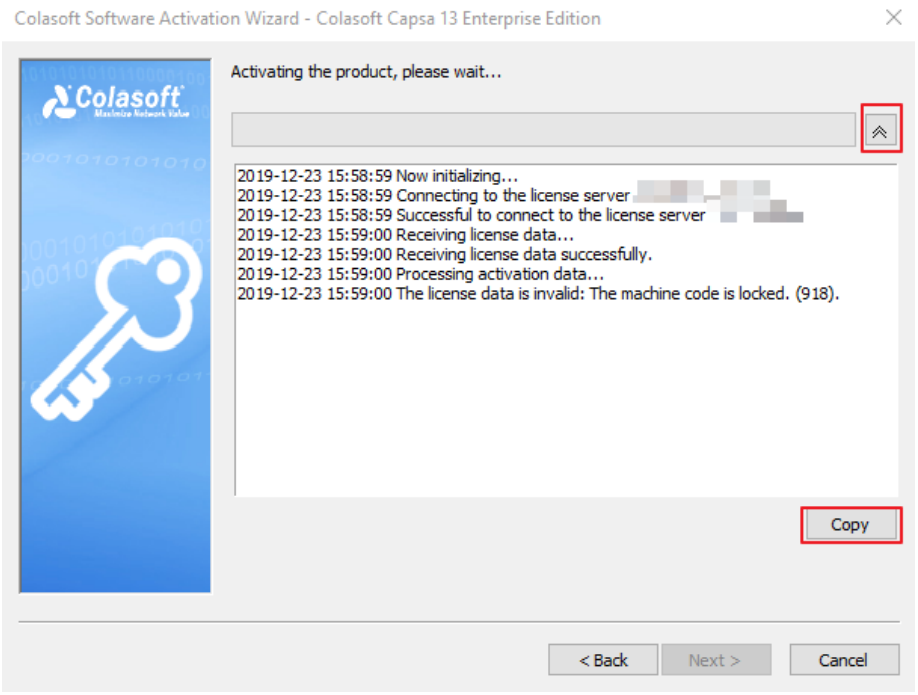
Activate online

To activate Capsa online, just enter the Serial Number and then click **Next** to complete the activation. This method is very quick and easy, and the activation process will only take a few seconds.



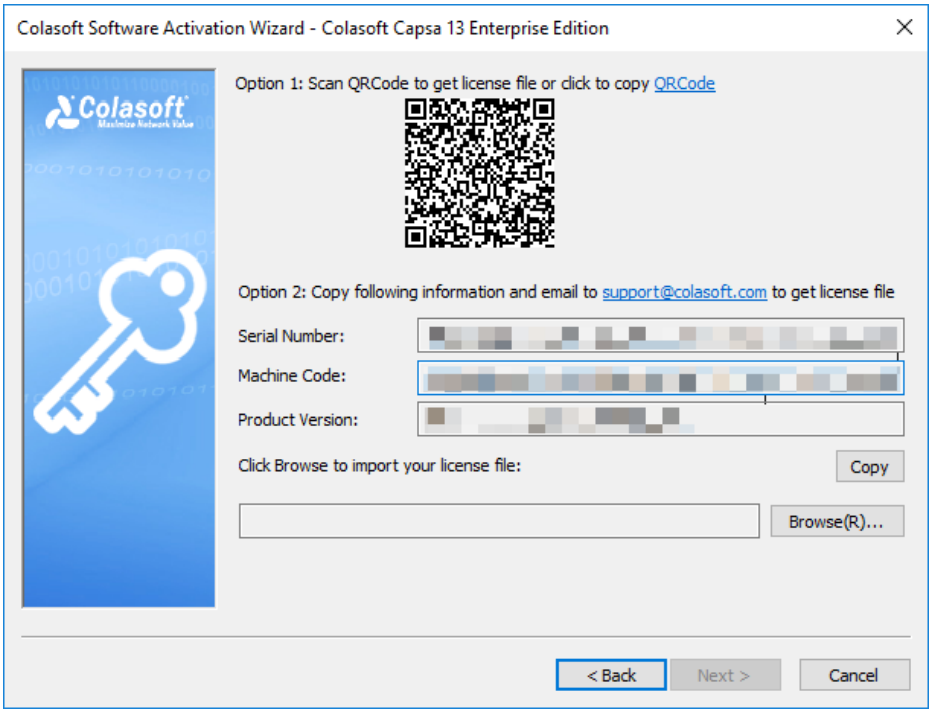
If it fails to activate online,

1. Click **Activate with license file** to activate the program with license file.
2. Click the down double-arrow button on the right of the activation progress bar to show the details and click **Copy**, then send the copied information to support@colasoft.com.



Activate with license file

When you don't have Internet access or failed to activate online, you can choose this method to activate Capsa. If you select this method, the activation interface shows as below:

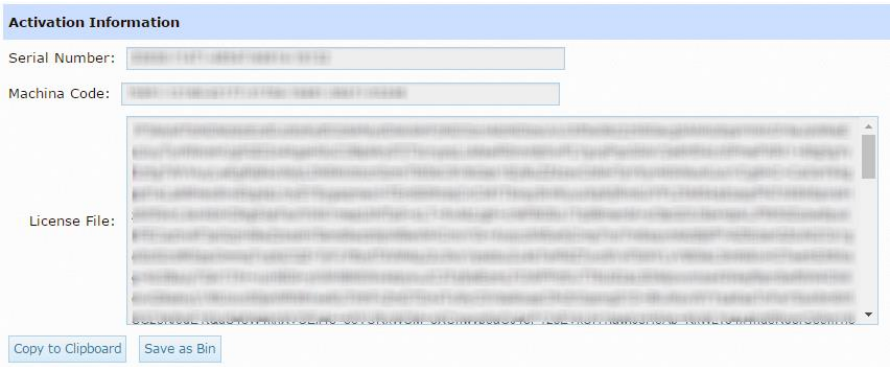


The license file can be obtained by two ways: via Colasoft Webpage and via Colasoft Support.

Via Colasoft Webpage

Follow steps below to obtain license file via Colasoft Webpage:

1. Scan QR Code or click **QRCode** to copy the link to the browser to access Colasoft Webpage
2. On the activation interface, click the link in Option 1, and then Colasoft Activation Webpage pops up:



3. Click **Save as Bin** to save the license file.
4. On the activation interface, import the license file, and then click **Next**.

Via Colasoft Support

Follow steps below to obtain license file via Colasoft Support:

1. Click the button **Copy**. The Activation Wizard will copy Serial Number, Machine code, Product Version, and if you have tried online activation, Online Activation Log will be copied together.
2. Send the copied information to support@colasoft.com.

Getting Started

After the activation, you can start to capture network traffic. Click following links to know details.

- Starting a Capture
- Capturing with Wireless Network Adapters
- Replaying Captured Packets

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. Double-click **Default** analysis settings on the **Analysis Settings** section to edit the analysis settings. In Analysis Settings, the settings about analysis modules, node group, name table, alarms, analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display are included.
4. Click the **Start** button on the bottom to start an analysis project.

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** tab.
2. Select a wireless network adapter on the **Adapter List** section, and then the **Adapter Status** section will be shown, which 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. Double-click **Default** analysis settings on the **Analysis Settings** section to edit the analysis settings. In Analysis Settings, the settings about analysis modules, node group, name table, alarms, analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display are included.
5. Click the **Start** button on the bottom to start an analysis project.

Note

- Capturing with wireless network adapters is only available for Capsa Enterprise. Capsa Free

don't provide such feature.

- It is only available for Windows Vista and higher version to capture packets with wireless network adapters.
- If you enter the wrong key for an AP, the analysis project will run as well but it will not decode any packets.
- 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.
- One analysis project can monitor multiple APs at a time.

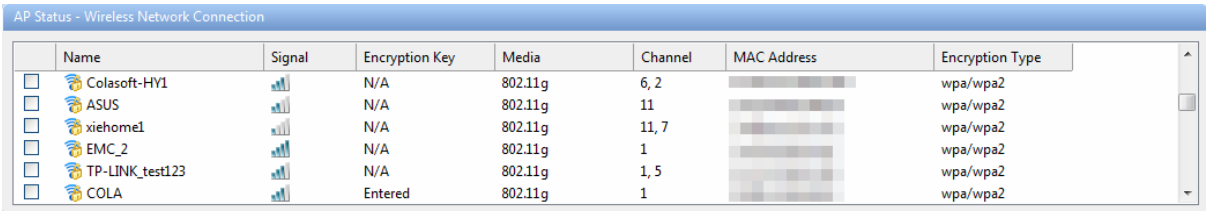
Advice To decode and analyze Wi-Fi traffic, you are recommended to:

- make sure the password for monitored AP is correct.
- be close enough to the wireless router (signal source) to thereby capture all packets.
- monitor the AP before other hosts access the network to thereby capture EAPOL handshake packets.

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 key, media type, AP channel, MAC address and encryption type.

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.

Capsa supports analyzing the traffic of 2-channel wireless AP.

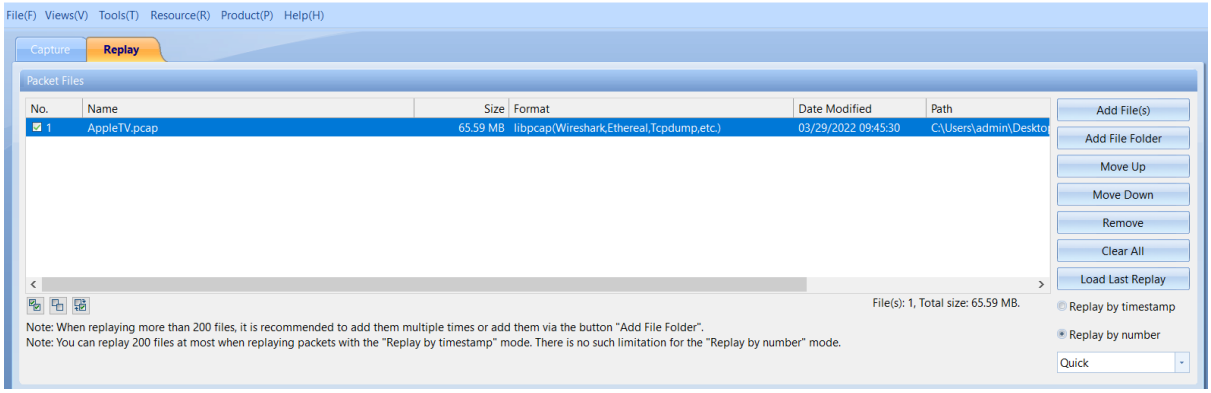
Replaying Captured Packets

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.

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. Double-click **Default** analysis settings on the **Analysis Settings** section to edit the analysis settings. In Analysis Settings, the settings about analysis modules, node group, name table, alarms, analysis modules, analysis objects, packet buffer, packet filters, logs, diagnosis events, packet output, and view display are included.
4. Click the **Start** button on the bottom to start an analysis project.

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



- **Add File(s)**: Adds the files to be replayed. When multiple packet files are replayed simultaneously, users can choose to replay them by timestamp or by number.
- **Add File Folder**: Adds all the packet files in the selected folders.
- **Remove**: Removes the selected packet file from the list.
- **Clear All**: Empties the packet file list.
- **Load Last Replay**: The latest replayed packet file will display on Packet Files box.
- **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.

The formats of the packet files which can be replayed by Capsa are shown as below:

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (*.cscpkt; *rapkt; *.rawpkt; *.cacproj)
- EtherPeek Packet File (V7/V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)

- Novell LANalyer (*.tr1)
- Network Instruments Observer V9.0 (*.bfr)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)

Visual Network Traffic Capture (*.cap)

And for captured packet, it can be exported as one of the following formats:

- Accellent 5Views Packet File (*.5vw)
- Colasoft Packet File (V3) (*.rapkt)
- Colasoft Packet File (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt）
- Colasoft Raw Packet File (V2) (*.rawpkt）
- EtherPeek Packet File (V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO; *.TRC1)
- Libpcap (Wireshark, Tcpdump, Ethereal, etc.) (*.cap; *pcap)
- Wireshark (Wireshark, etc.) (*.pcapang; *pcapang.gz; *.ntar; *.ntar.gz)
- Microsoft Network Monitor 1.x 2.x (*.cap)
- Novell LANalyer (*.tr1)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

Main User Interface

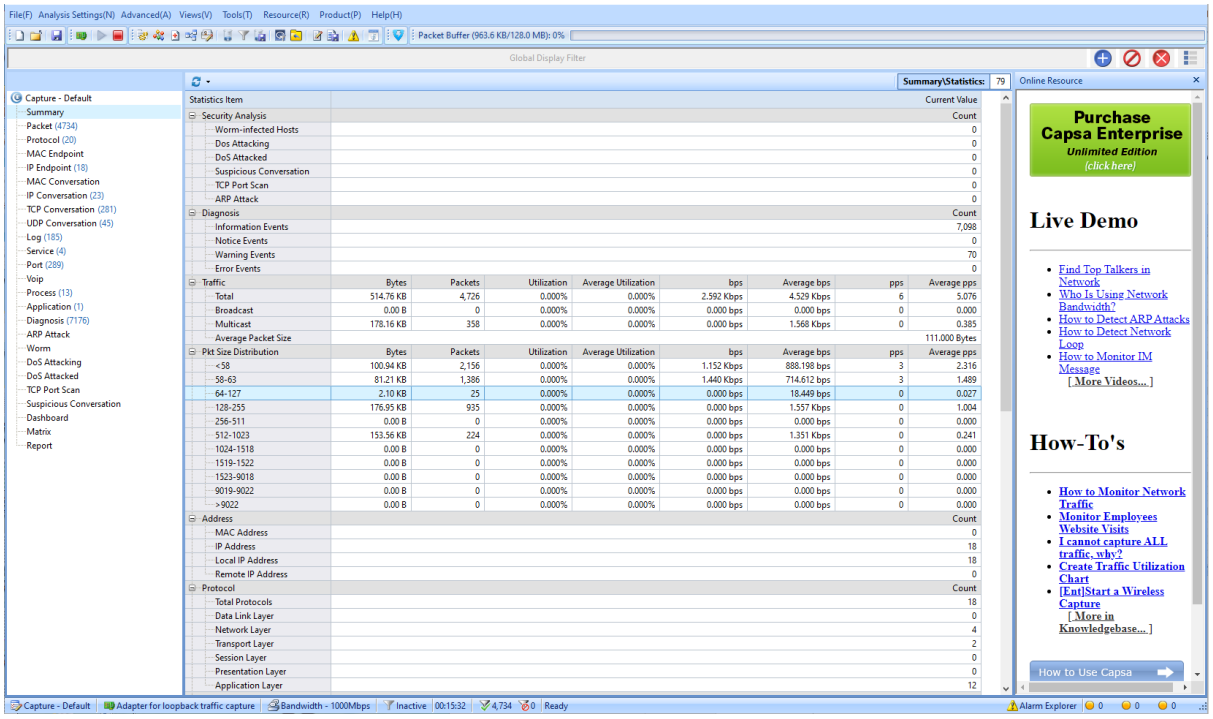
After starting an analysis project, whether real-time capturing or replaying packets, Capsa enters the main user interface, which shows you all statistics and the root of network problems. The main user interface is mainly divided into six sections.

- System Main Interface
- Global Function Area
- Node Explorer window
- Statistical views
- Online Resources window
- Status Bar

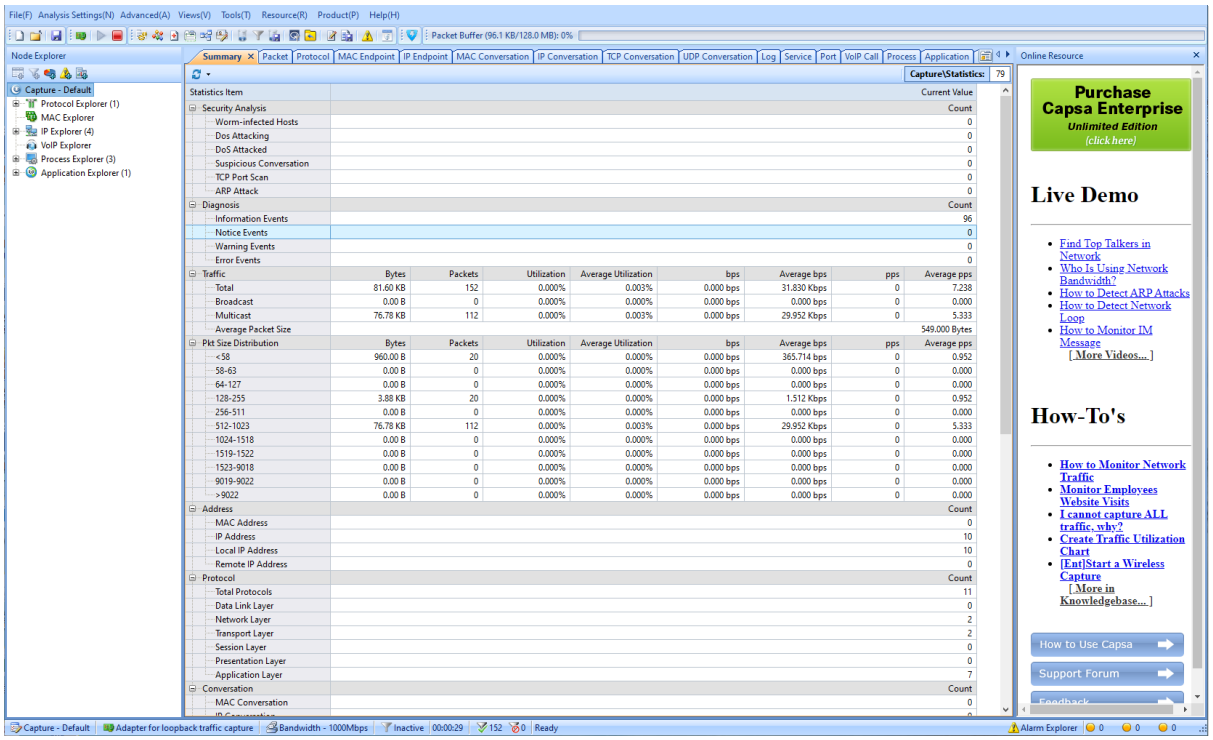
System Main Interface

There are two main interfaces, one is the interface with the global filtering function, and the other is the interface without the global filtering function, as shown below:

Interface with Global Filtering Function:



Interface without Global Filtering Function:



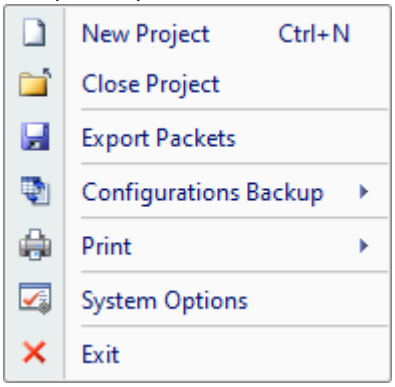
Global Function Area

The global function area is composed of three parts: menu, toolbar and global filter. The menu bar is mainly used to change some common settings. The toolbar is used to quickly enable a function or quickly open the corresponding configuration interface. The global filter is used in all views Filter condition settings.

Menu

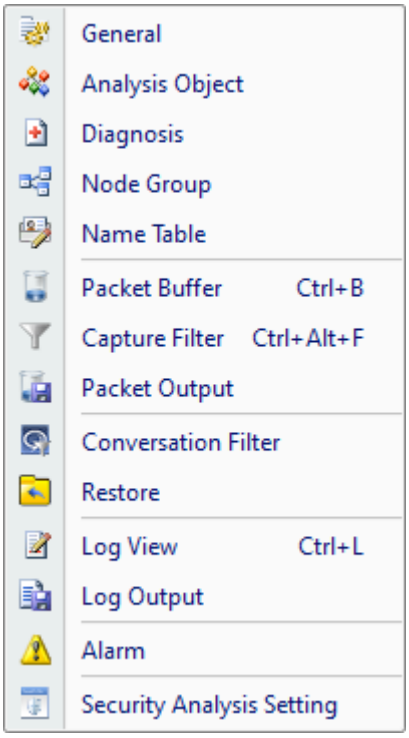
The menu bar is composed of file, analysis settings, advanced, interface, tools, resources, products, and help. The specific menu items are as follows:

1. File (Alt + F)



- New: Creates a new analysis project.
- Close: Close the project.
- Export Packets: Export the packets from the cache and save them locally.
- Configurations Backup: Imports or exports global configurations (see Configurations backup for details).
- Print: Prints current page or sets print configurations.
- System Options: Configures some settings for the analysis project (see System Options for details).
- Exit: Exits the program.

2. Analysis Settings (Alt+N)

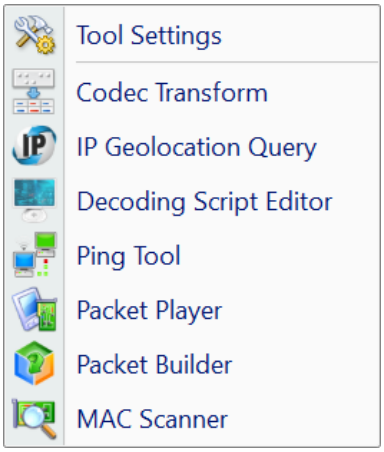


- Basic Settings: Open general analysis settings interface, go to General for more information.
- Analysis Object: Open analysis object settings interface, go to Analysis Object for more information.
- Diagnosis: Open diagnosis settings interface, go to Diagnosis for more information.
- Node Group: Open node group settings interface, go to Node Group for more information.
- Name Table: Open name table settings interface, go to Name Table for more information.
- Packet Buffer: Open packet buffer settings interface, go to Packet Buffer for more information.
- Capture Filter: Open filter settings interface, go to Packet Analysis Filter for more information.
- Packet Output: Open packet output settings interface, go to Packet Output for more information.
- Conversation Filter: Open conversation filter settings interface, go to Conversation Filter for more information.
- Restore: Open restore settings interface, go to Reconstruct Settings for more information.
- Log View: Open log view settings interface, go to Log View for more information.
- Log Output: Open log output settings interface, go to Log Output for more information.
- Alarm: Open alarm settings interface, go to Alarm Settings for more information.
- Security Analysis Setting: Open security analysis settings interface, go to Security Analysis for more information.

3. Views (Alt + V)

- Online Resource: Open or close online resource window.
- Window Size: Set window size.

4. Tools (Alt + T)

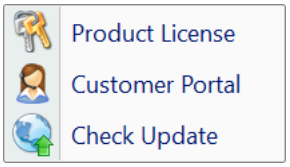


In tools menu, uses can use built-in network tools, codec transform, IP geolocation query, decoding script editor, ping tool, packet player, packet builder and MAC scanner are included. Go to Network Tools for more information.

5. Resource (Alt +R)

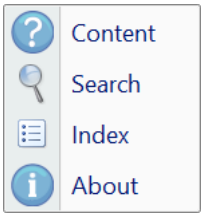
Users can access Colasoft home page and forum quickly.

6. Product (Alt + P)



Users can enter a new serial number and activate here, register new user information, check whether there is a new version released, and view related information about the software.

7. Help (Alt + H)



Users can quickly view the help content they want to view.

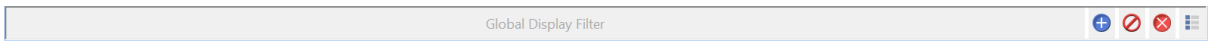
Toolbar

Without global filter, the toolbar is as shown below:

With global filter, the tool bar is as shown below:

Global Display Filter

The global display filter is a display filter for all analysis views. Once a global display filter is set, all views will preferentially use the filter conditions of the global display filter for display filtering. The global display filter interface is as follows:



 Add global display filter.

 Delete global display filter.

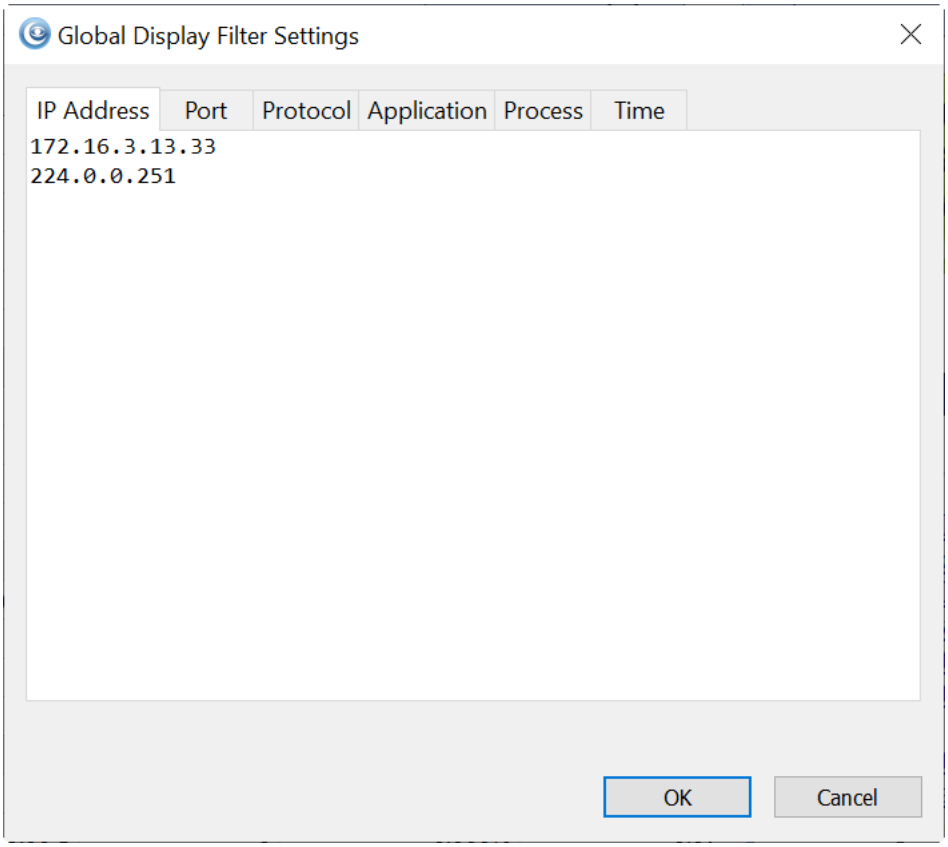
 Disable global display filter.

 View global display filter list.

Add a Global Display Filter

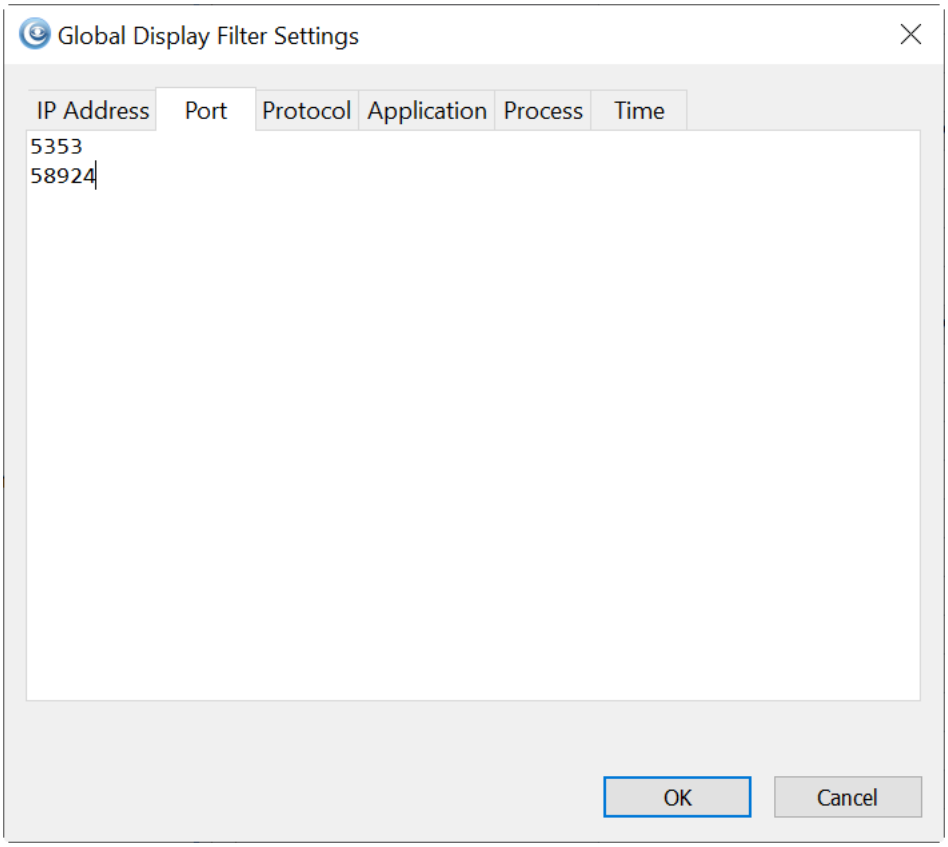
User can add a global display filter quickly by shortcut Alt + G or click button  .

Click the IP Address tab on the filter editing interface, and enter the IP addresses to be filtered in the edit box, one IP address per line. The configuration interface is as follows:



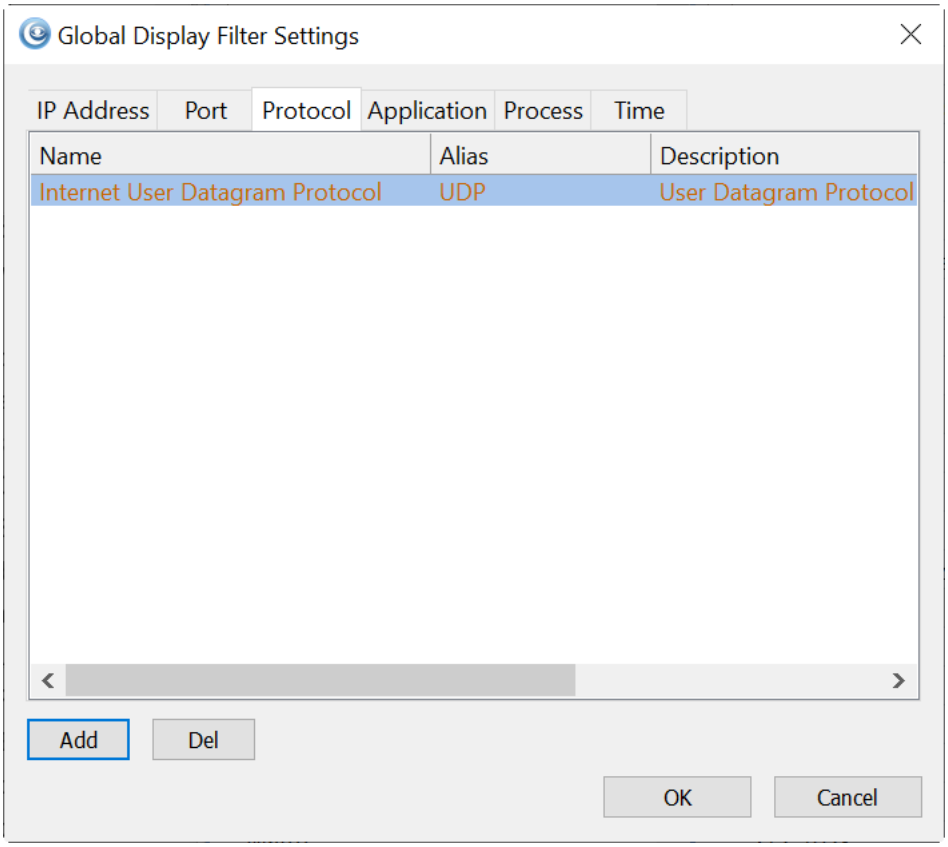
Add Ports

Click the port tab on the filter editing interface, and enter the ports to be filtered in the edit box, one port per line. The configuration interface is as follows:



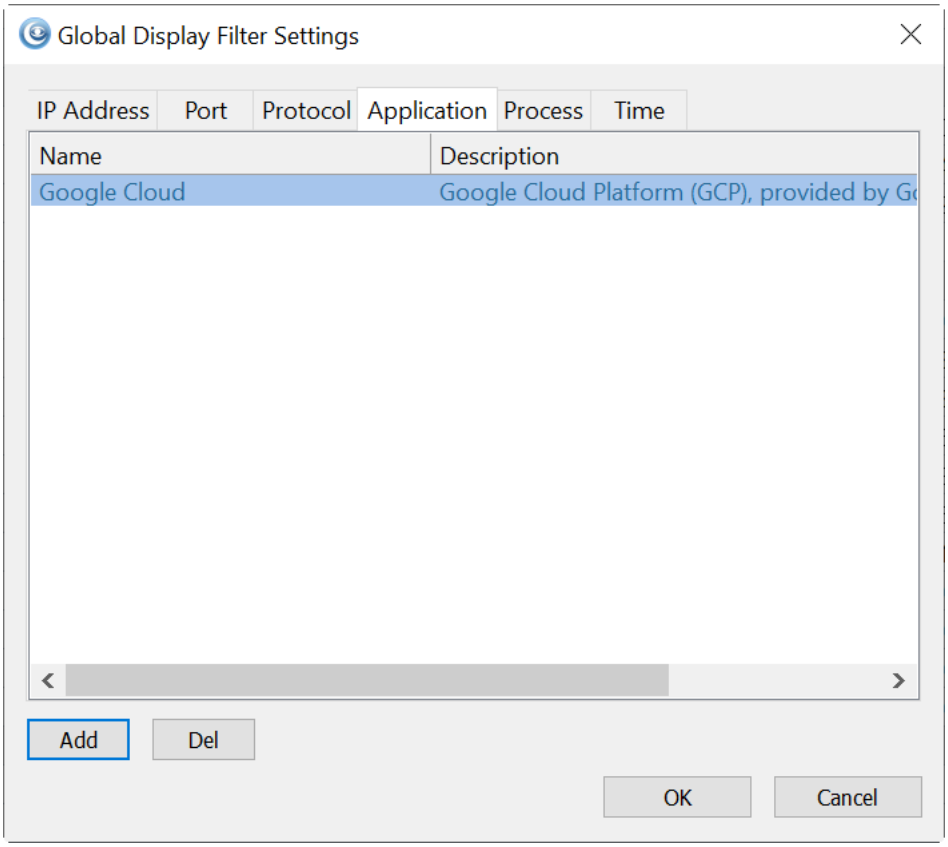
Add Protocols

Click the protocol tab on the filter editing interface, and enter the protocols to be filtered in the edit box. If a protocol is not needed, select the protocol and click the delete button. The configuration interface is as follows:



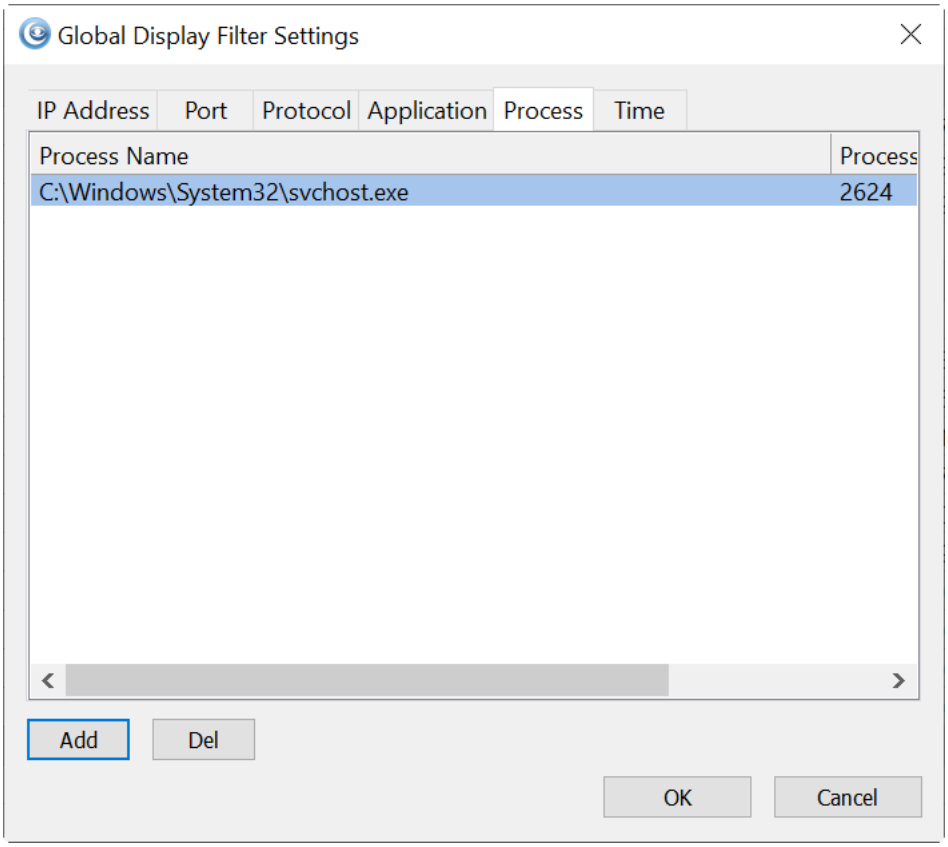
Add Applications

Click the application tab on the filter editing interface, and enter the protocols to be filtered in the edit box. If an application is not needed, select the application and click the delete button. The configuration interface is as follows:



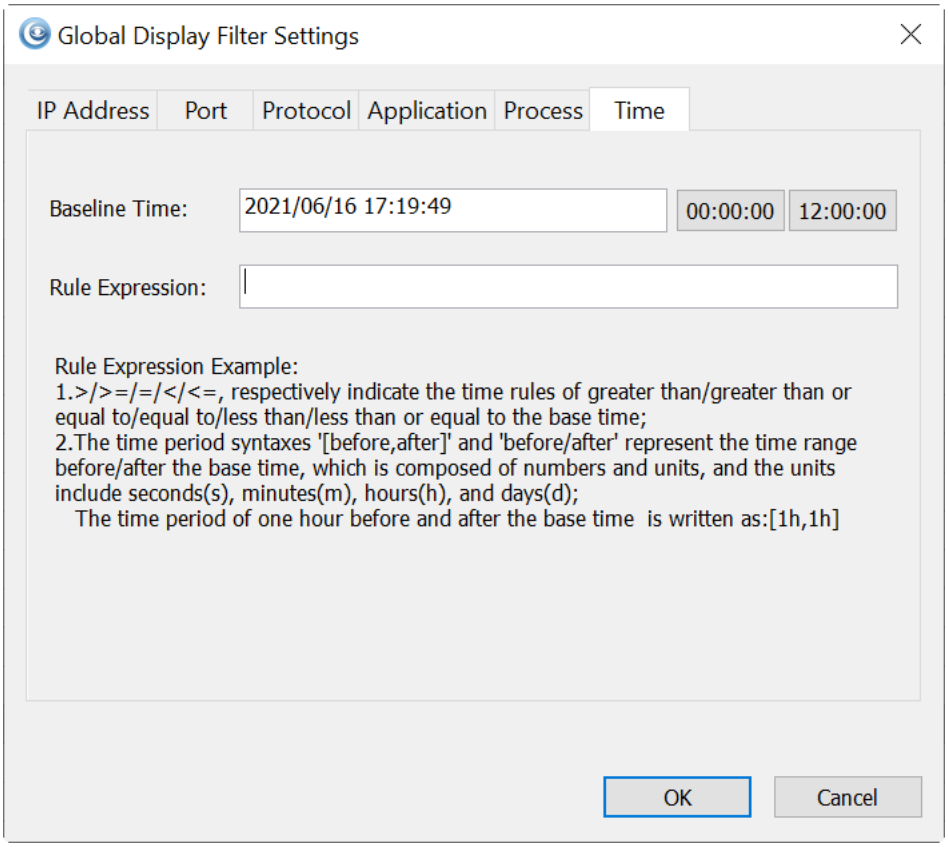
Add Processes

Click the process tab on the filter editing interface, and enter the processes to be filtered in the edit box. If a process is not needed, select the process and click the delete button. The configuration interface is as follows:



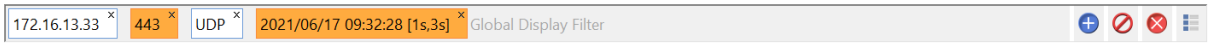
Add Timestamp

Click the time tab on the filter editing interface, and enter the base timestamps in the edit box, and write the specific rules in the regular expression (refer to the example below for the way of writing the rules). The configuration interface is as follows:



In the right-click menu of each analysis view, if the current view has global display filter conditions that can be added, the following icons will appear:  . The icons in the toolbar respectively represent source IP address, destination IP address, source IP address and destination IP address, source port, destination port, source port and destination port, protocol, application, process, and timestamp. Click the corresponding icon on the toolbar to quickly add the data in the currently selected item as a global display filter.

After configuring the filter conditions, the global display filter interface will display all filter labels. Select a label to perform filtering. If you need to select multiple filters, use Ctrl + left mouse. The selected filter labels are highlighted, as shown in the figure below:



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.

Note If user checks global display filter option in the Analysis Settings, the node explorer will not display.

Buttons

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

 : Adds the selected node to Name Table.

 : Creates filters based on the selected node.

 : Creates graphs based on the selected node.

 : Creates alarms based on the selected node.

 : Makes report based on the selected node.

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.

For more information about Node Explorer, please refer to Node Explorer.

Statistical views

The statistical views provide huge amount of analysis statistics (see Statistics for more information), dashboard, reports, logs, and other information.

The default visibility status of statistical views changes along with the settings of chosen analysis setting.

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**.

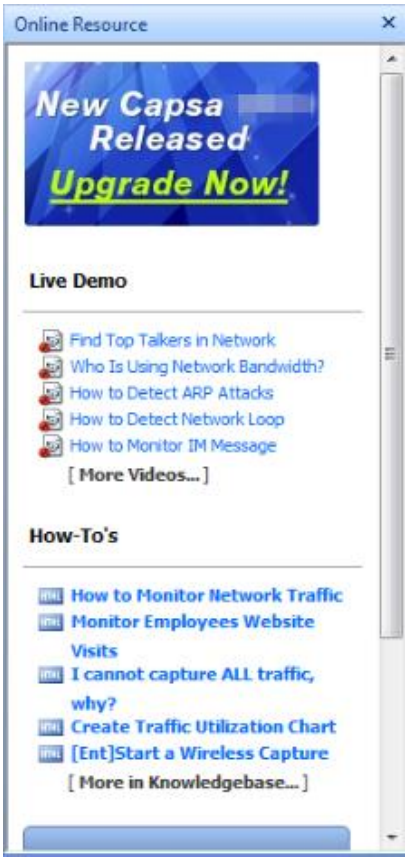
Meanwhile, the statistical view section provides different statistical views when selecting different type of nodes in the Node Explorer window.

Security Analysis and VoIP Analysis are only available for Capsa Enterprise.

Online Resource window

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

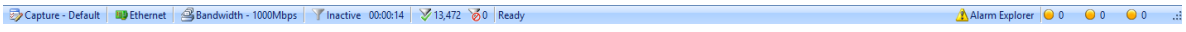
Online Resource window is displayed on the right section of the main user interface by default. You can close it by clicking the close button on the top right corner. If you do not want to show it when starting analysis projects, click **Menu** button, select **Options**, and on **Basic Settings** tab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



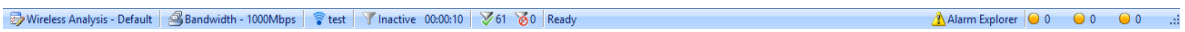
Note The Online Resource window cannot be hidden for Capsa Free.

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.



If the analysis is based on wireless network, the status bar appears as below.



From left to right, the status bar includes seven parts as below.

Analysis Mode

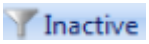
This part shows the analysis mode and the analysis settings. You can click this part to open the **Analysis Settings** dialog box.

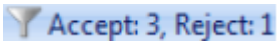
Adapters

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** 

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.

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.

System Options

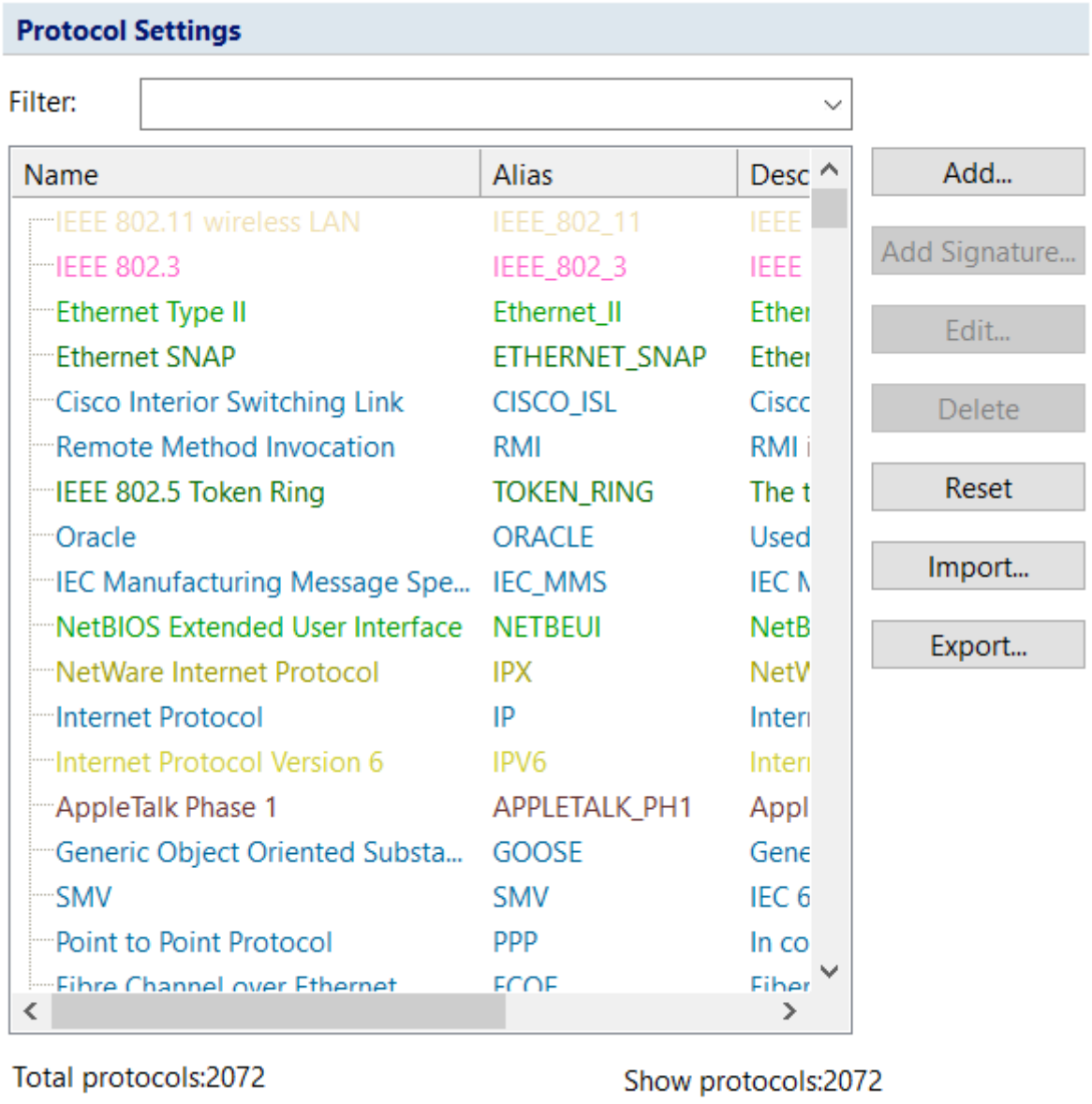
To open the **System Options** dialog box, click the **Menu** button and select System **Options** on the bottom-right corner of the menu.

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

- Basic Settings
- Decoder Settings
- Advanced Protocol Settings

Protocol Settings

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



Note 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.

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

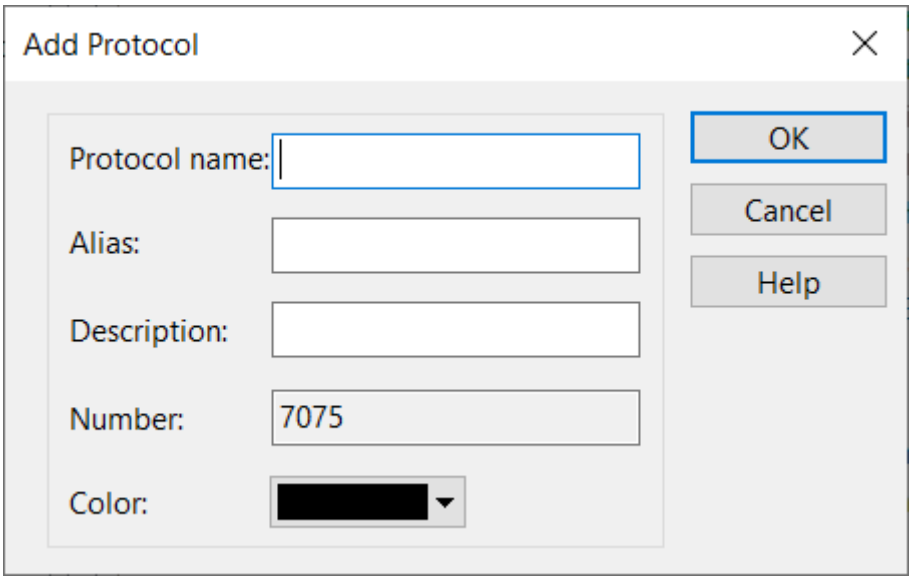
- **Add Protocol**: Create a new protocol.
- **Add Signature:** Create a new rule to identify a new protocol.
- **Edit**: Edit a highlighted protocol item.
- **Delete**: Delete a highlighted protocol item.
- **Reset:** Reset built-in protocols. User-defined protocols will not be deleted or modified.
- **Import**: Read the protocol list from a *.cscpro* file.
- **Export**: Save the protocol list to a *.cscpro* file.

Note 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 S*tart Page*, and then the buttons will be enabled again.

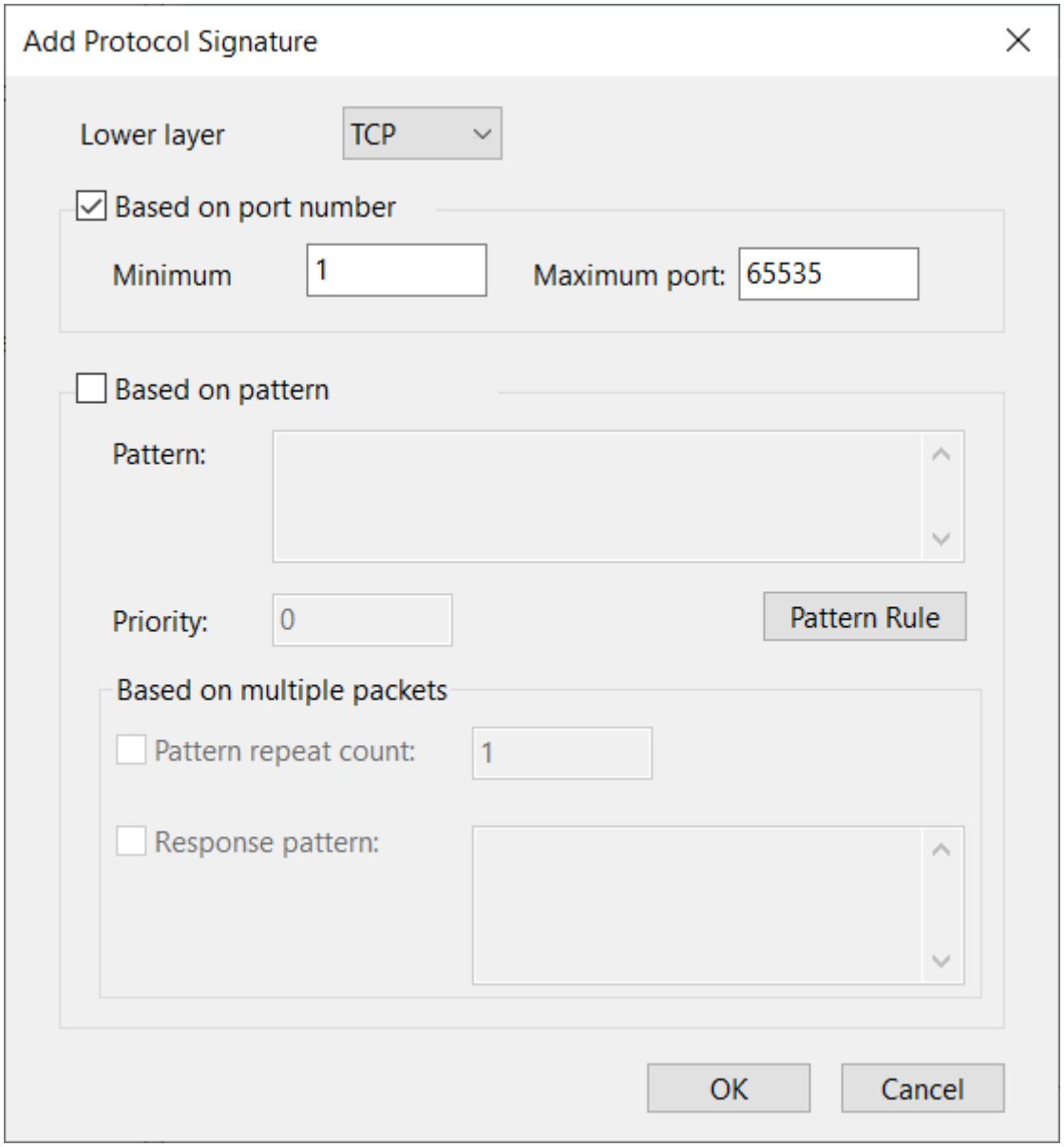
Adding protocols

To add a protocol, click **Add** to open the **Add Protocol** dialog box in which you can specify the name, alias, maker, description, port number and color of the protocol. **Number** is auto-generated by the system and users can edit it.

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



Select the new-added protocol in protocol list, click **Add Signature**, the **Add Protocol Signature** dialog box appears as below.



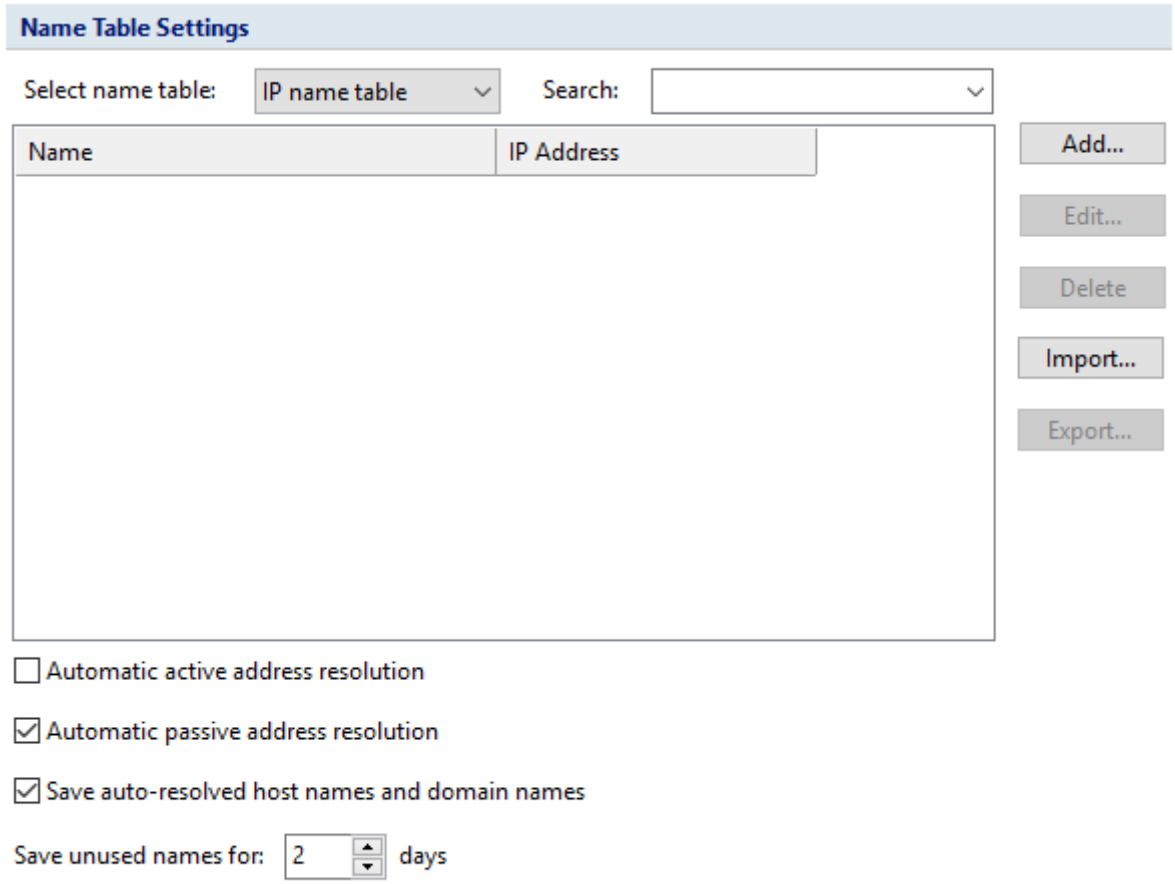
Set detailed signature of the protocol in the dialog box. System recognizes the protocol according to the signature.

Protocol signature is port number or content signature.

- Application Settings
- Protocol Settings
- Name Table

Name Table

The **Name Table** tab manages symbolic names for all MAC addresses and IP addresses. You can use **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:

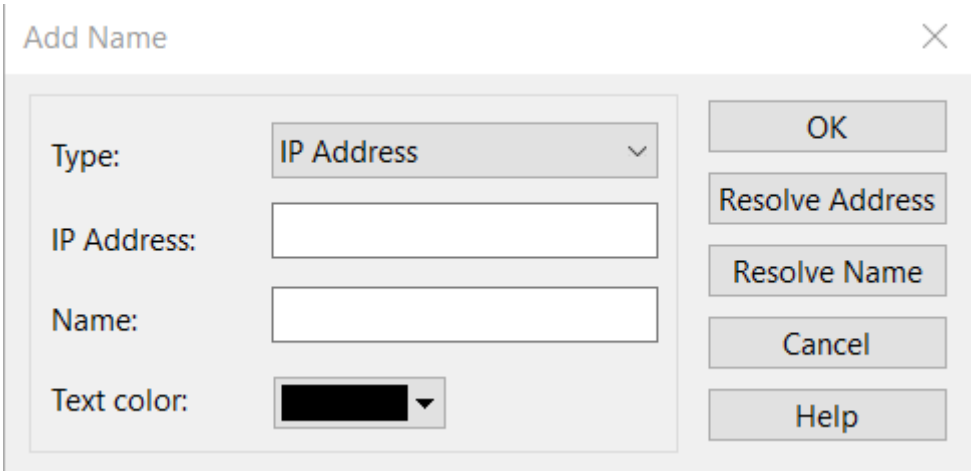
- **Add**: Adds a name for an address (see Adding to Name Table for details).
- **Edit**: Edits the selected alias item.
- **Delete**: Deletes the selected alias item.
- **Import**: Imports name table from a "*.csv", "*.xml", "*.cscont", or "*.cscntab" file.
- **Export**: Saves the current name table to a "*.csv", "*.xml", or "*.cscont" file.

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

Adding to Name Table

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

1. Click **Name Table** button on the **System Options** tab, 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.

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

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

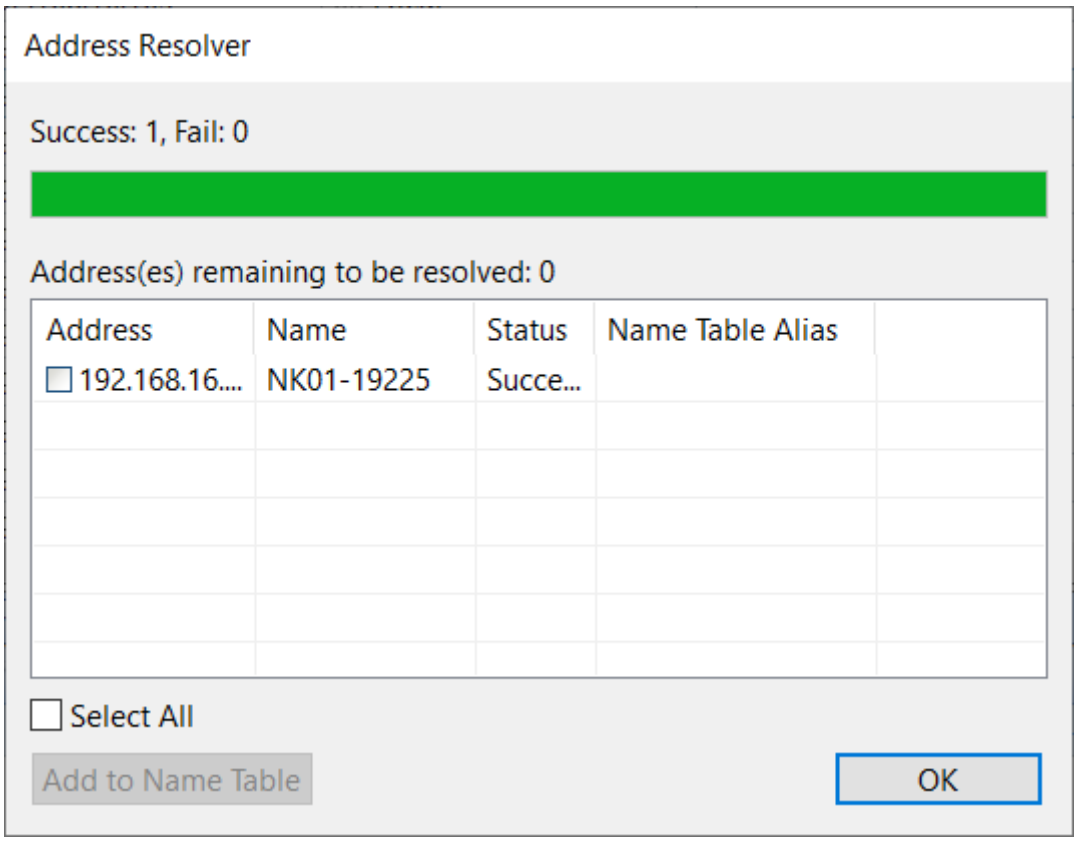
   Tips You can also right-click the selected address node, and select **Add to Name Table** to open the **Add Name** dialog box.

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.

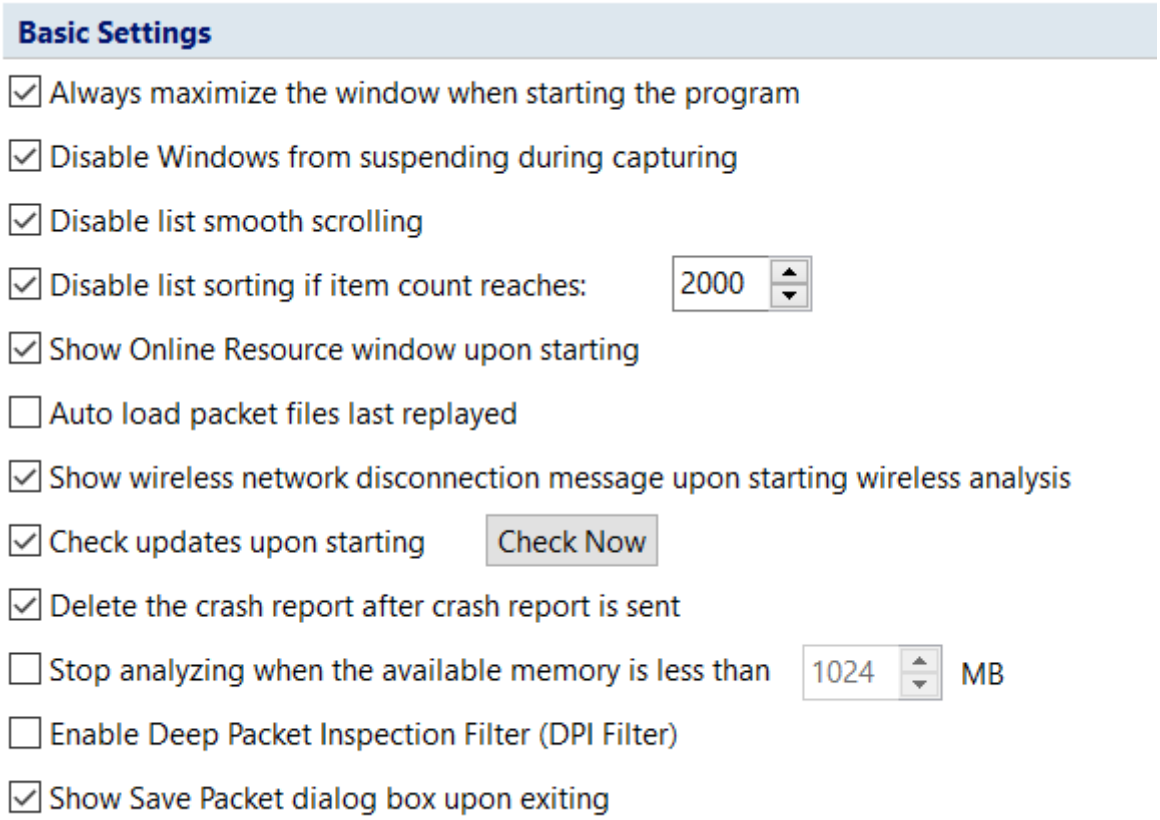
Add to Name Table: Adds selected items to Name Table and removes them from the *Address Resolver.*

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

Note Only IP addresses can be resolved by Address Resolver.

- Task Scheduler
- Report Settings
- Display Format

Basic Settings



This tab includes twelve options:

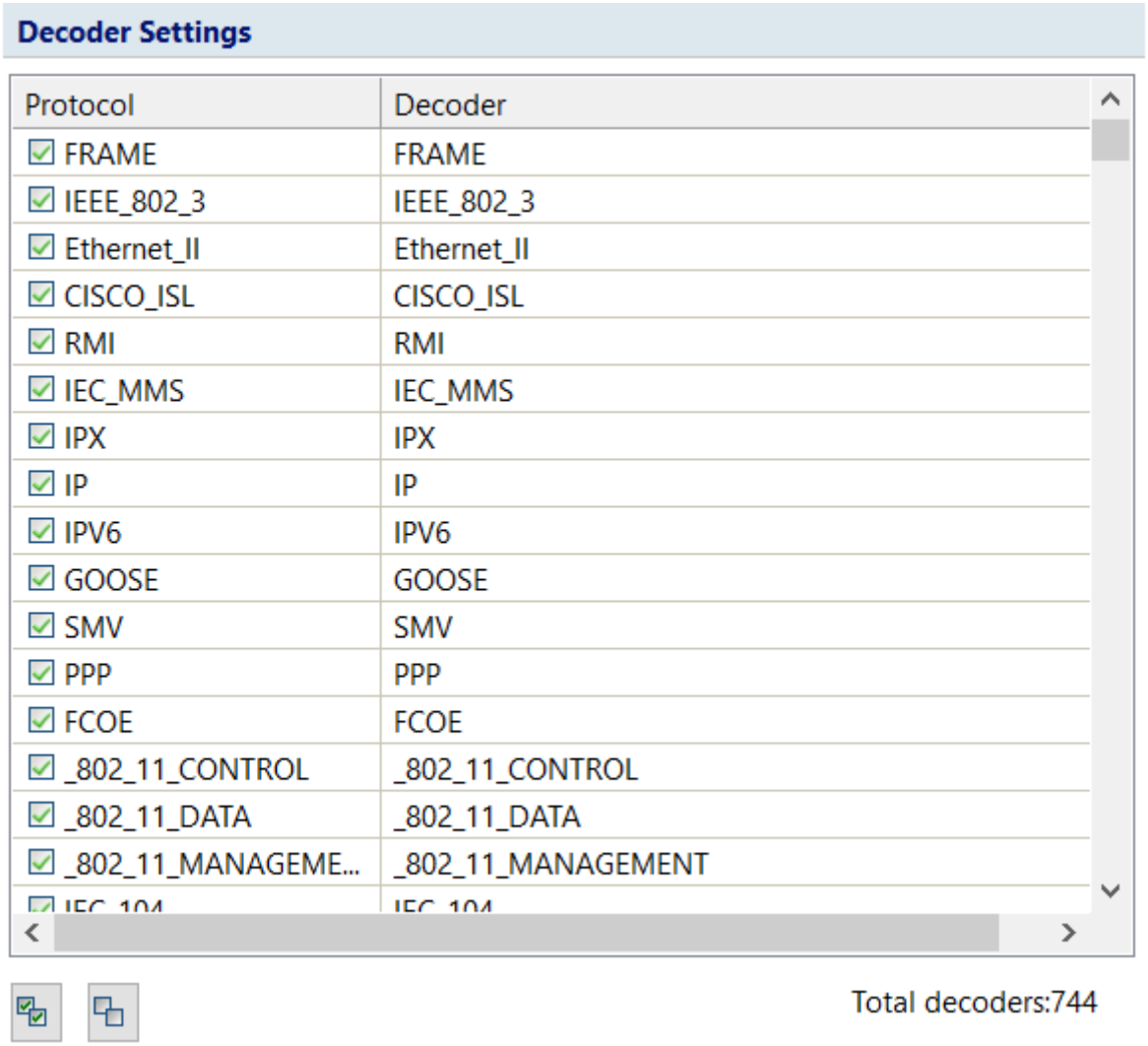
- **Always maximize the window when starting the program**: Always maximize the program window when launching the program.
- **Disable Windows from suspending during capturing**: The power option schema in your system control panel will be ignored. You cannot make your system standby or hibernated without stopping 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 upon exiting**: 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 upon starting**: The **Online Resource** window will be shown on the right side of the program when launching the program.
- **Auto load packet files last replayed**: Load the packet files last replayed when opening Capsa.
- **Show wireless network disconnection message upon starting wireless analysis**: Shows wireless network disconnection message when starting a wireless analysis project using the wireless network adapter. This option is only available in Capsa Enterprise.
- **Check updates upon starting**: Automatically check product updates when Capsa starts. You

can click **Check Now** to check updates immediately.

- **Delete the file of crash report after sending crash report**: Delete the file of crash report after sending crash report if you select this option. It is enabled by default.
- **Stop analyzing when the available memory is less than xx MB**: When the available memory of the machine is less than a specific value, analysis will stop.
- **Enable Deep Packet Inspection Filter (DPI Filter)**: The new filter method (DPI filter) to filter out packets. If you need enable it, please select DPI filter on the Start Page.
- **Show Save Packet dialog box upon exiting**: Ask users if they want to save the packets in buffer when clicking close button.
- **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:

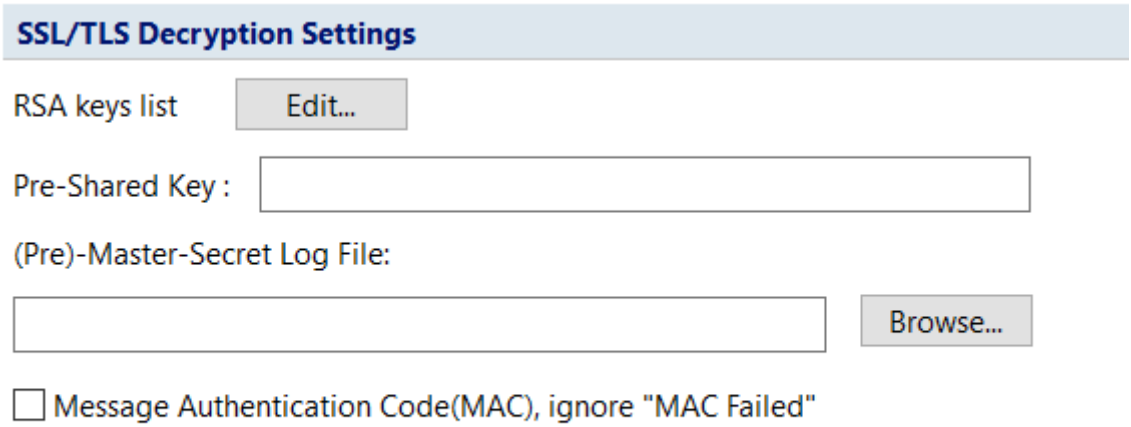
 : Enables all decoders.

 : Disables all decoders.

Advanced Protocol Settings

SSL/TLS Decryption Settings

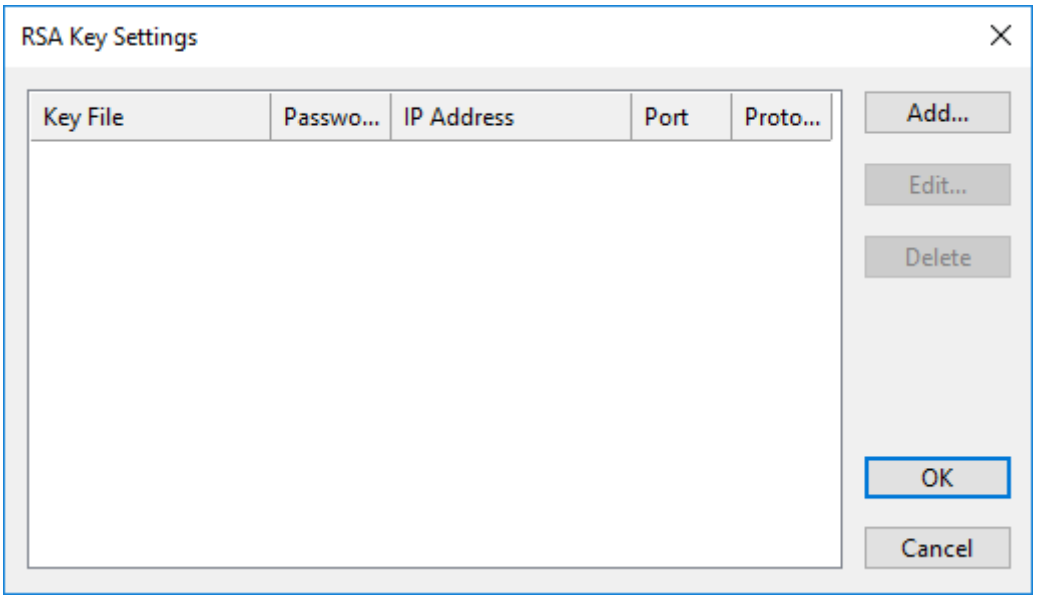
To decrypt the HTTPS packets, you need first configure HTTPS Decryption Settings. You could use different ways to configure your HTTPS decryption settings according to the different encryption method. With the right configuration, Capsa is able to use the key to decrypt the HTTPS Packets.



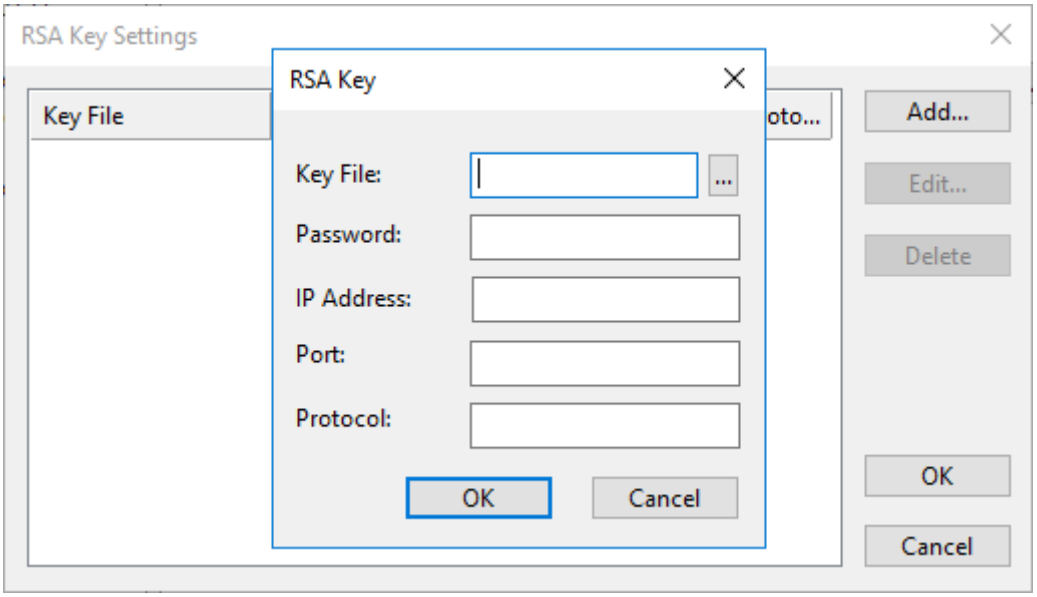
SSL/TLS encryption method mainly includes: RSA, PSK, DH

- RSA

  If the packet used RSA method for encryption, you could click the “Edit” button behind “RSA keys list”. The RSA Key Settings view is as the screenshot shows as below.



Click the “Add” button to upload the key file.



- Key File (Required): Upload RAS key file. After the uploading, Capsa will use the key file to decrypt the HTTPS packets which were encrypted with this key file.
- Password (Not Required): If the key file has been encrypted again, you need to put the password for decryption; otherwise Capsa is not able to use the key file to decrypt HTTPS packets.
- IP Address (Not Required): The IP address of the server which is using this key file.
- Port (Not Required): The number of HTTPS service port on the server.
- Protocol (Not Required): The protocol format after decryption. Now, only HTTP protocol is supported.

- PSK

  If the packet used PSK method for encryption, you could put the HEX code for Pre-Shared Key to decrypt the packet.

- DH

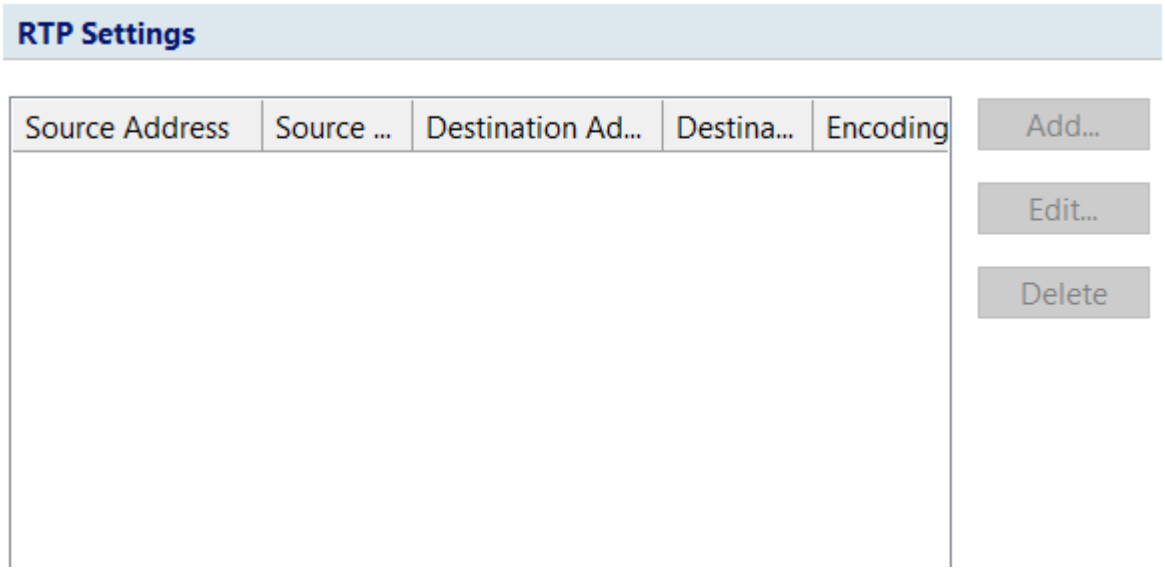
  If the packet used DH method for encryption, you could click the “Browse” button to upload the PMS key log file.

After allowing Capsa to ignore “MAC Failed” the Capsa will continue decryption when the “MAC Failed” message appears. Without checking this box, the Capsa will skip decrypting this part and continue decrypting the following parts.

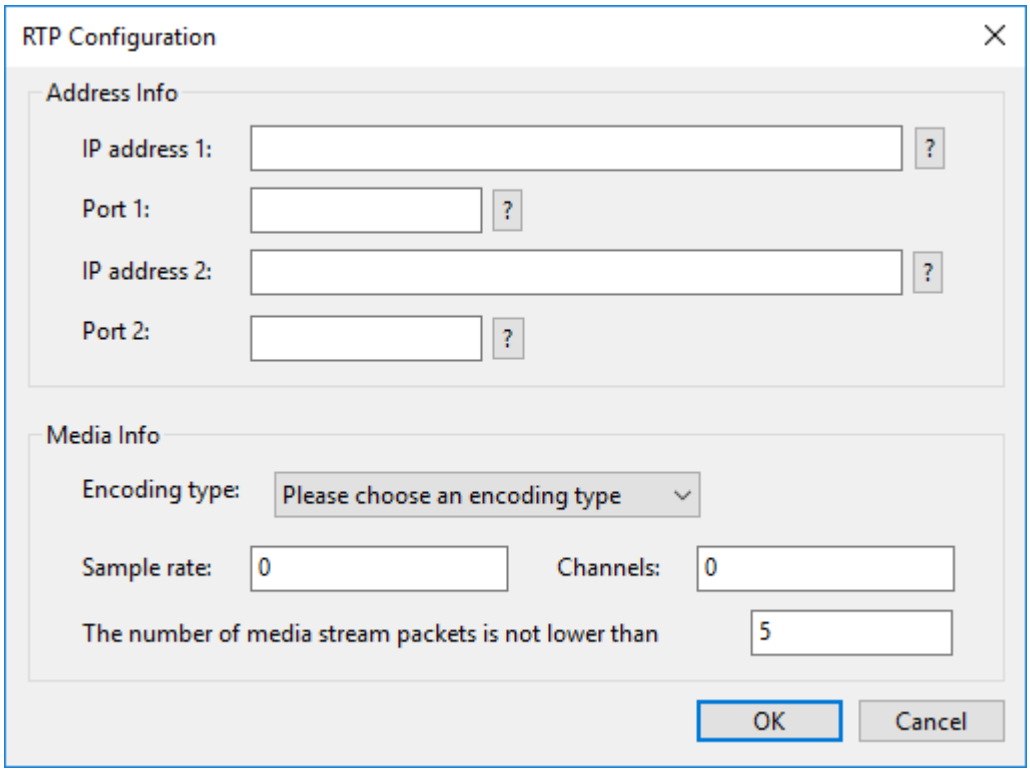
After the configuration, you could go to the View Packets to check the HTTPS packets after the decryption.

RTP Settings

Signaling packets contain the encoding methods for audio and video. If there is no signaling, the decoding method to reconstruct RTP flow cannot be determined. It means that audio and video files cannot be reconstructed. Therefore, to reconstruct the audio and video in RTP packets without signaling, it is required to configure RTP information, as the screenshot below:



You can configure RTP information by clicking the “Add” button.

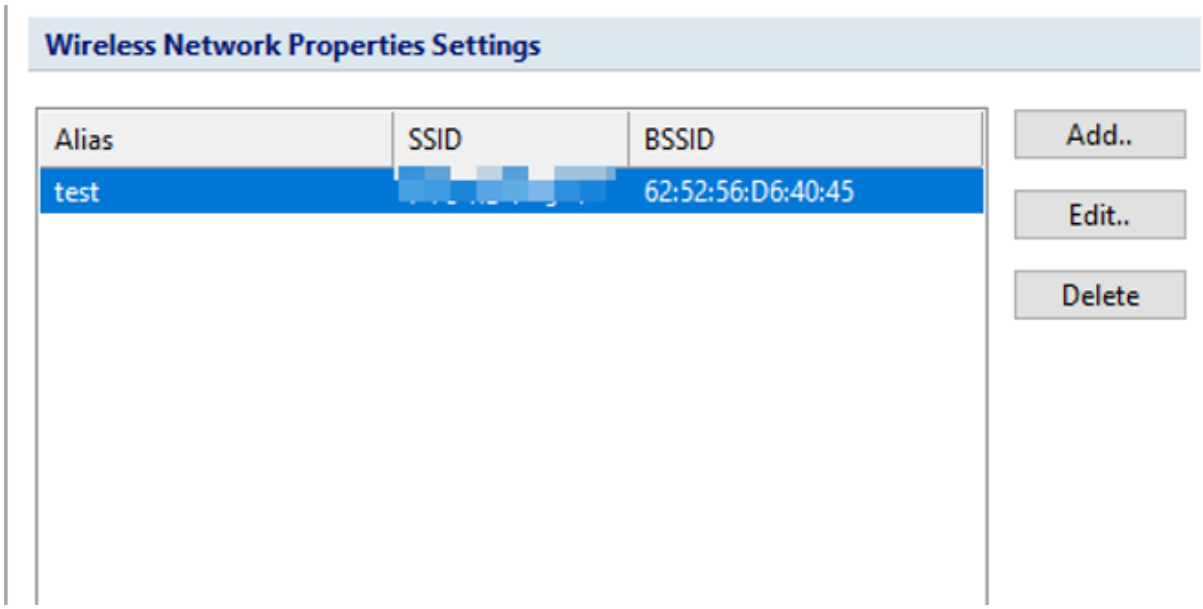


If the source and the destination are determined, input them, and then specify the encoding type, sample rate and channels.

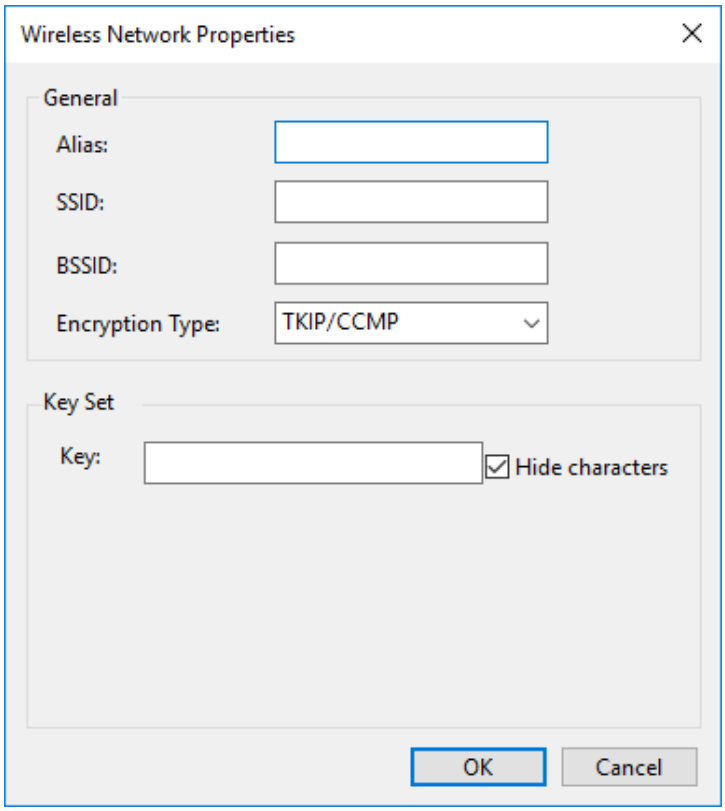
If the source and the destination are not determined, input one side of them, and the other side will match all.

IEEE 802.11 Settings

IEEE 802.11 configuration is used to configure the wireless network keys. You can configure the corresponding key according to the encryption type of the wireless network. After the configuration, the corresponding wireless packet can be decrypted when the packet is replayed for analysis.



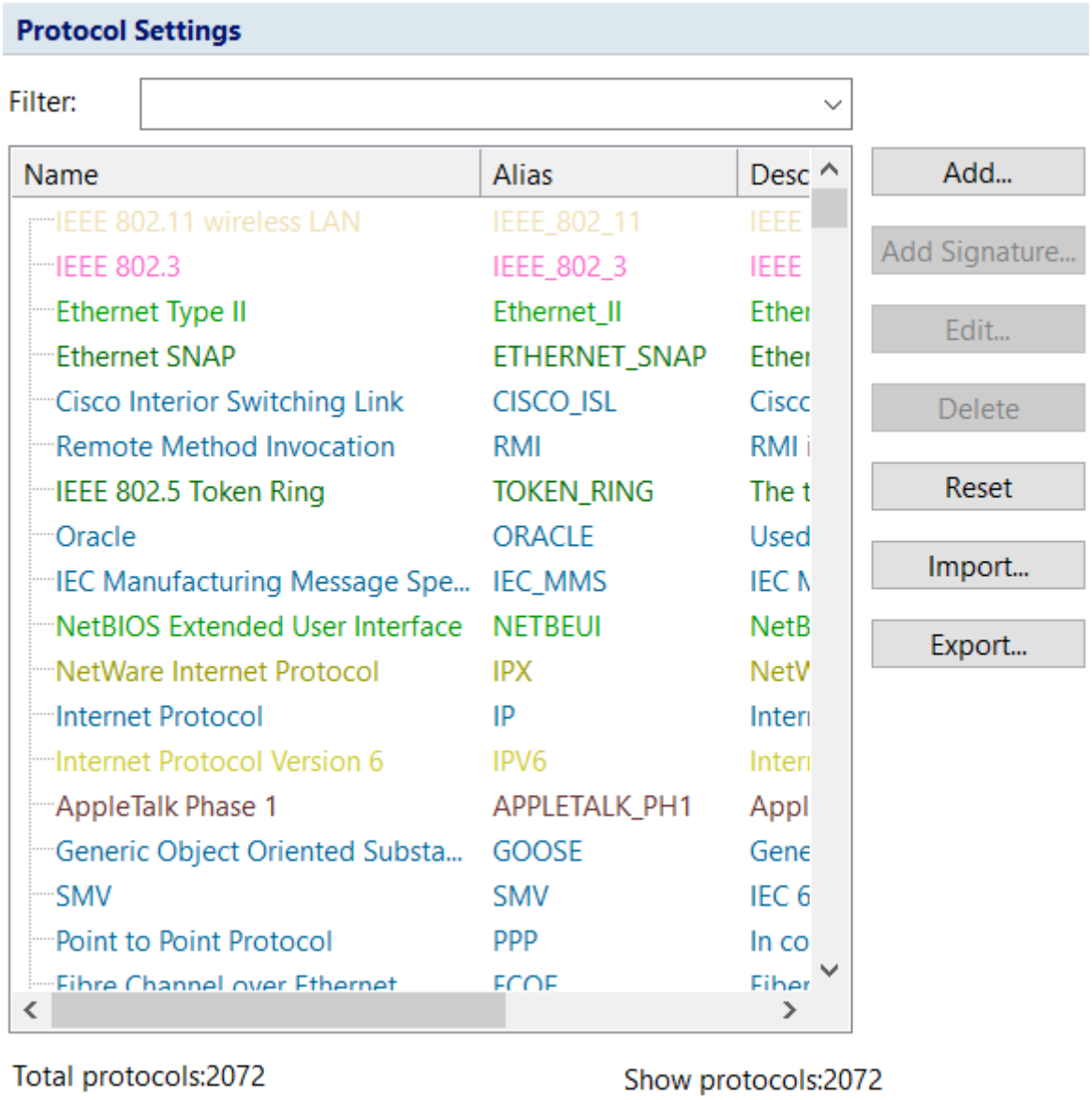
Click the “Add” button to configure the properties.



- Alias: The wireless network alias.
- SSID: The wireless network name.
- BSSID: The wireless network MAC address.
- Encryption Type: Encryption types include TKIP/CCMP and WEP.
- Key: For TKIP/CCMP type, only one key can be set. For WEP type, multiple keys can be set.

Protocol Settings

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



Note 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.

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

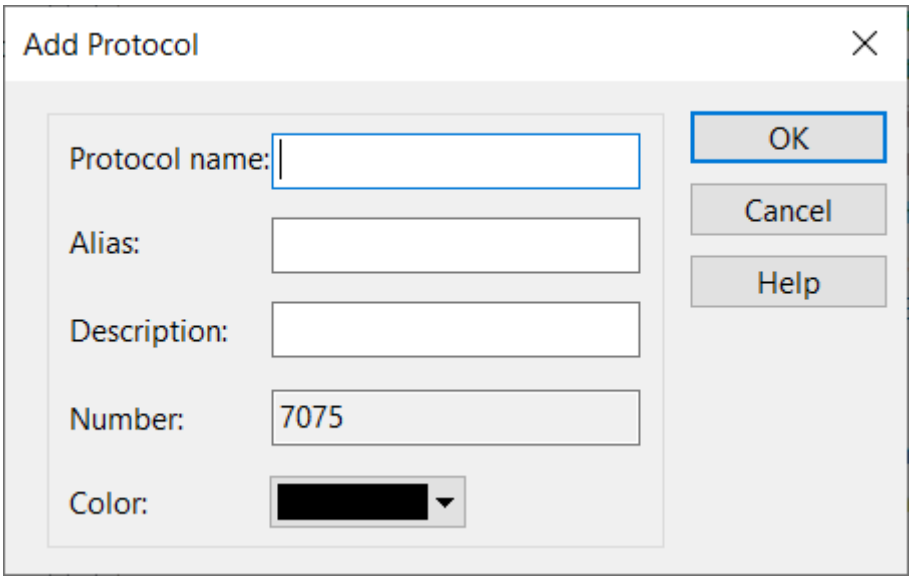
- **Add Protocol**: Create a new protocol.
- **Add Signature:** Create a new rule to identify a new protocol.
- **Edit**: Edit a highlighted protocol item.
- **Delete**: Delete a highlighted protocol item.
- **Reset:** Reset built-in protocols. User-defined protocols will not be deleted or modified.
- **Import**: Read the protocol list from a *.cscpro* file.
- **Export**: Save the protocol list to a *.cscpro* file.

Note 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*, and then the buttons will be enabled again.

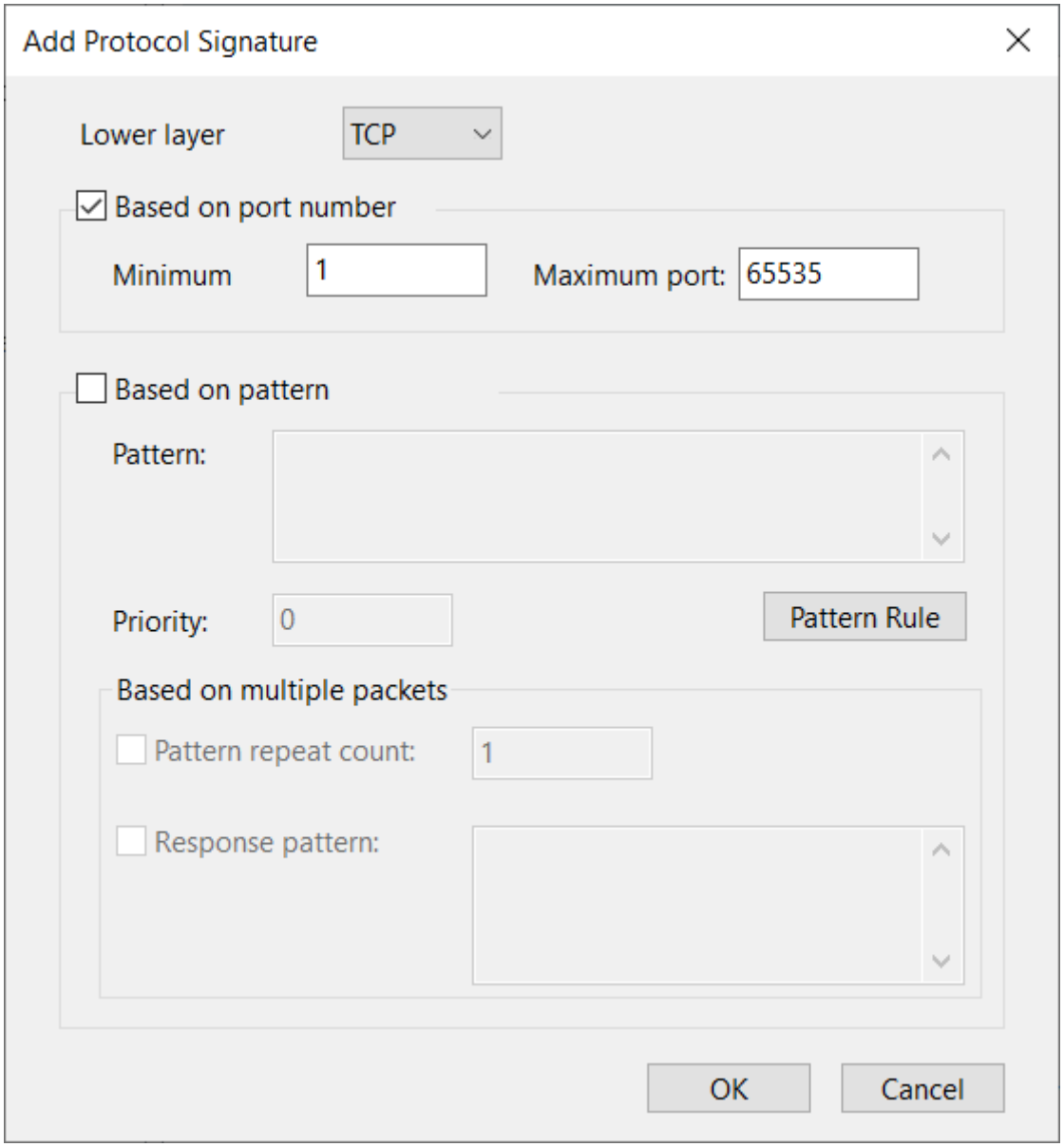
Adding protocols

To add a protocol, click **Add** to open the **Add Protocol** dialog box in which you can specify the name, alias, maker, description, port number and color of the protocol. **Number** is auto-generated by the system and users can edit it.

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



Select the new-added protocol in protocol list, click **Add Signature**, the **Add Protocol Signature** dialog box appears as below.



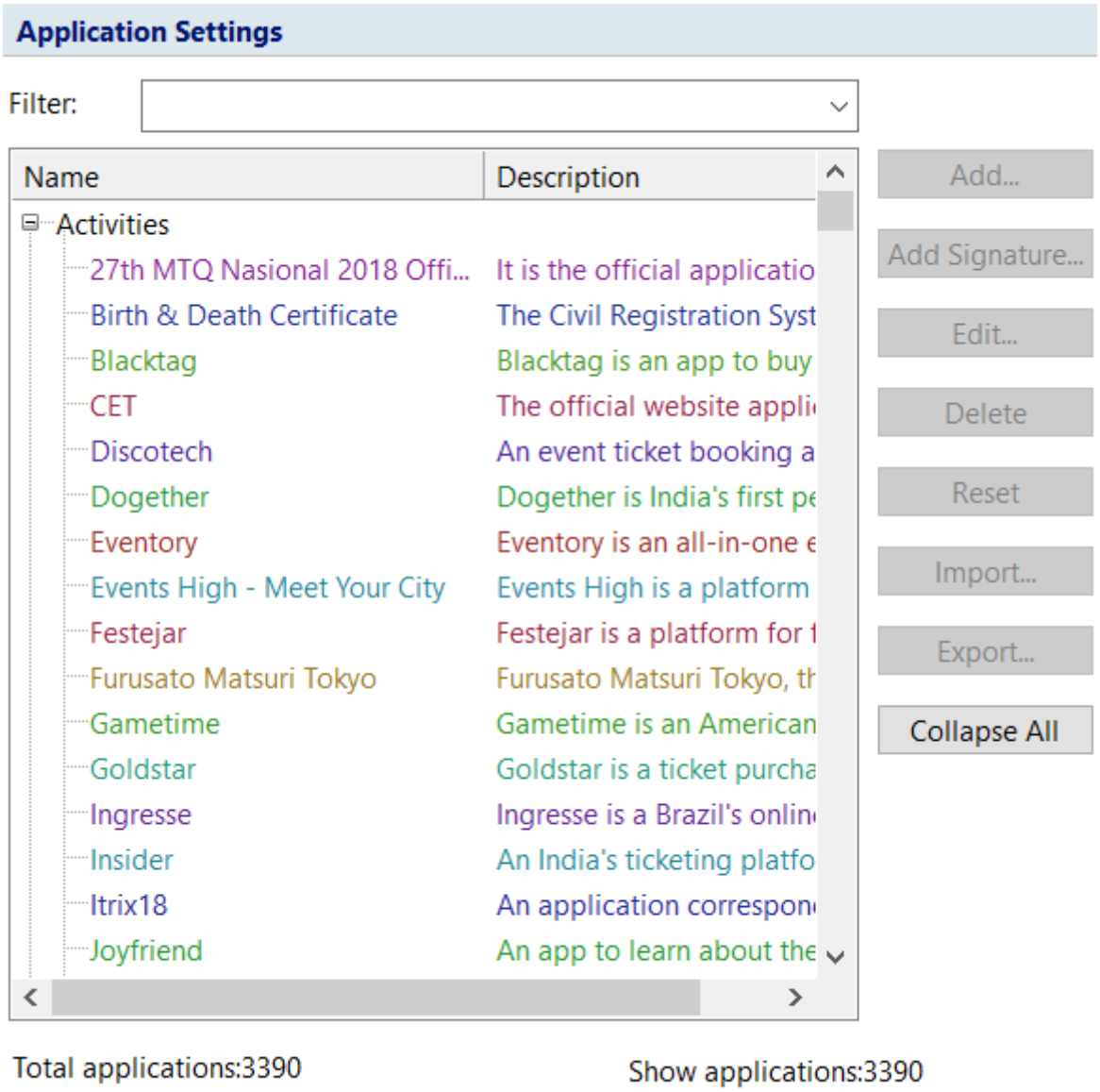
Set detailed signature of the protocol in the dialog box. System recognizes the protocol according to the signature.

Protocol signature is port number or content signature.

Application Settings

User could define the special applications in application settings according to their need.

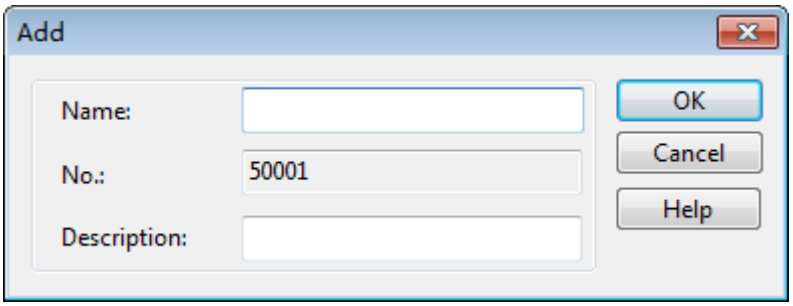
Both systematic application and customized application can be presented in the statistics view.



Note To configure the application sittings, you could only have one project opened and you must stop the capturing before making any change.

Add Application

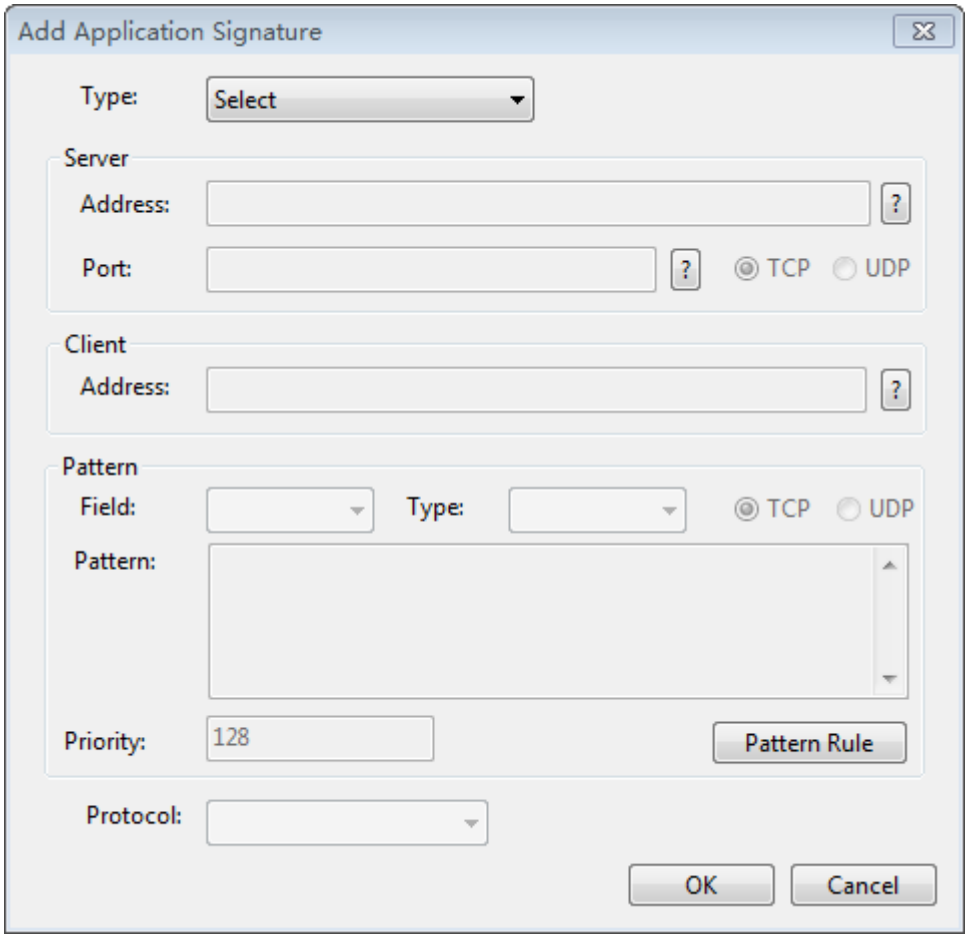
Click “Add” button to add an application.



You could set name, number, and description for an application. You could only input integer as No. and you cannot edit the No. after clicking OK.

Add Signature

Click “Add Signature” button to add a signature for the application.



According to your signature configuration for the application, Capsa will recognize the application from the traffic flow.

You could define the signature based on the protocol, port, IP address, pattern, IP address + protocol, IP address + port, IP address pair, server + client, IP address + Port + Pattern of the application.

An application can have multiple signatures, and the relationship between signatures is “or”, which means the application will be recognized by Capsa as long as one of all the signatures meets.

By using pattern to define a signature, the user could set the priority for the signature. If an application includes many signature patterns, the pattern with higher priority will be recognized. The smaller the number is, the higher the priority will be. If two patterns have the same priority, then Capsa will follow the sequence for recognition.

Import/Export Application

Capsa allows user to import and export the application settings.

- Export:

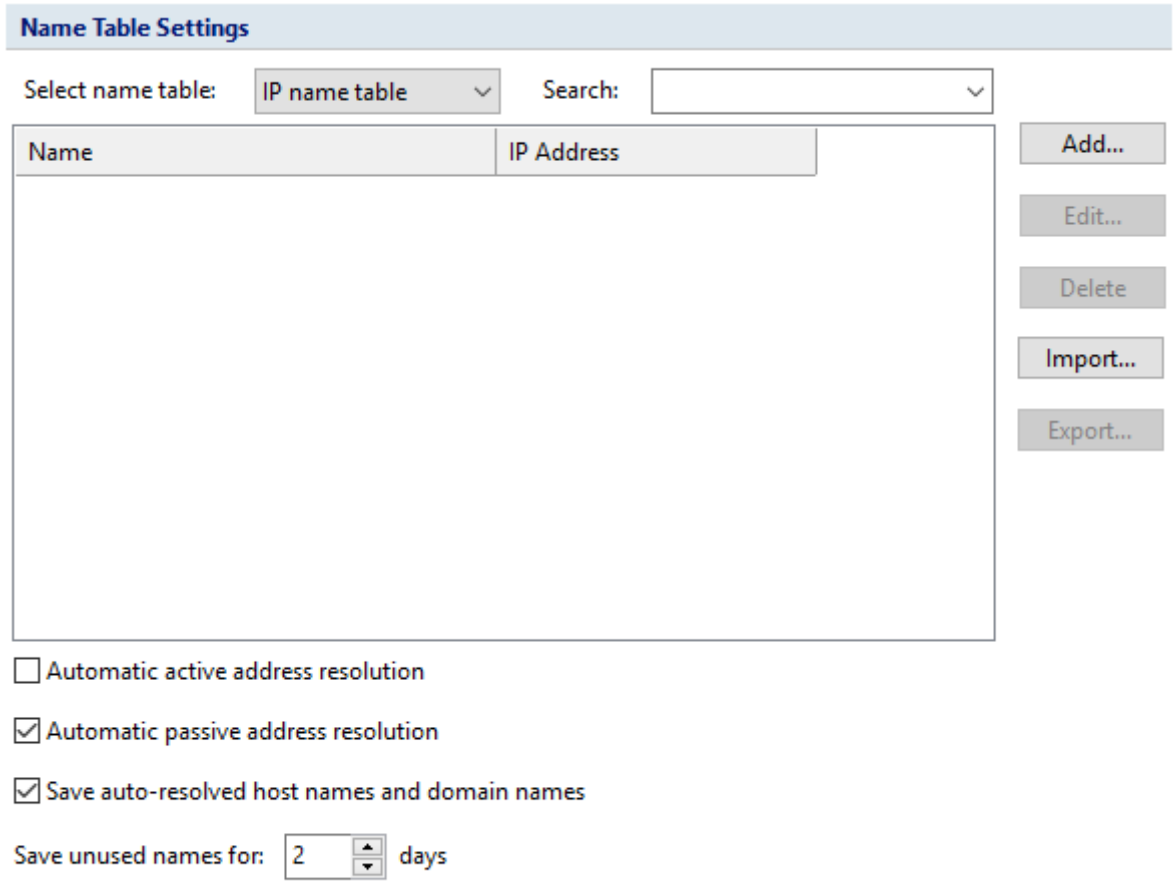
  Click “Export” button to export the application settings. Capsa will create two files, "CustomApp.cscapp" and "CustomApp.cscappsig", when the exportation, is success.

- Import:

  Click “Import” button to import the application settings. For import, you only need to import "CustomApp.cscapp" file, but both "CustomApp.cscapp" and "CustomApp.cscappsig" must be under the same path, otherwise, the application setting import cannot succeed.

Name Table

The **Name Table** tab manages symbolic names for all MAC addresses and IP addresses. You can use **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:

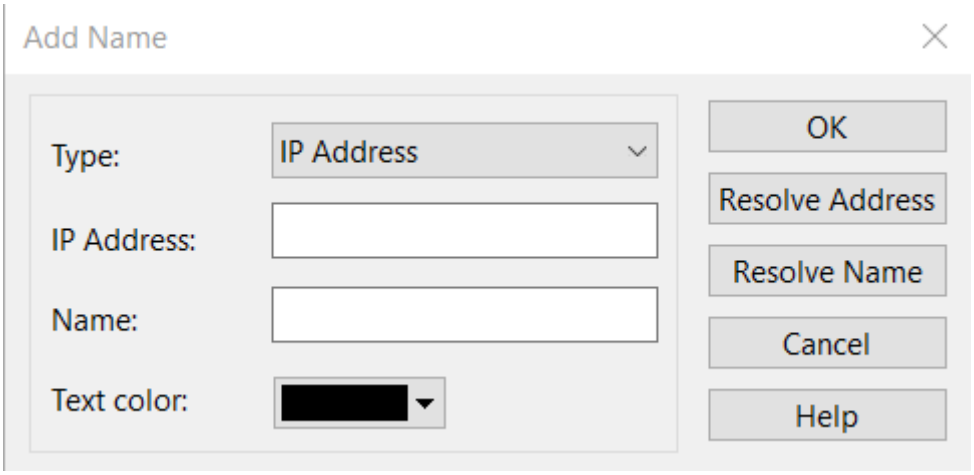
- **Add**: Adds a name for an address (see Adding to Name Table for details).
- **Edit**: Edits the selected alias item.
- **Delete**: Deletes the selected alias item.
- **Import**: Imports name table from a "*.csv", "*.xml", "*.cscont", or "*.cscntab" file.
- **Export**: Saves the current name table to a "*.csv", "*.xml", or "*.cscont" file.

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

Adding to Name Table

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

3. Click **Name Table** button on the **System Options** tab, click **Add** button to open the **Add Name** dialog box which appears below.



4. Type the address, and the name for the address.
5. 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.

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

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

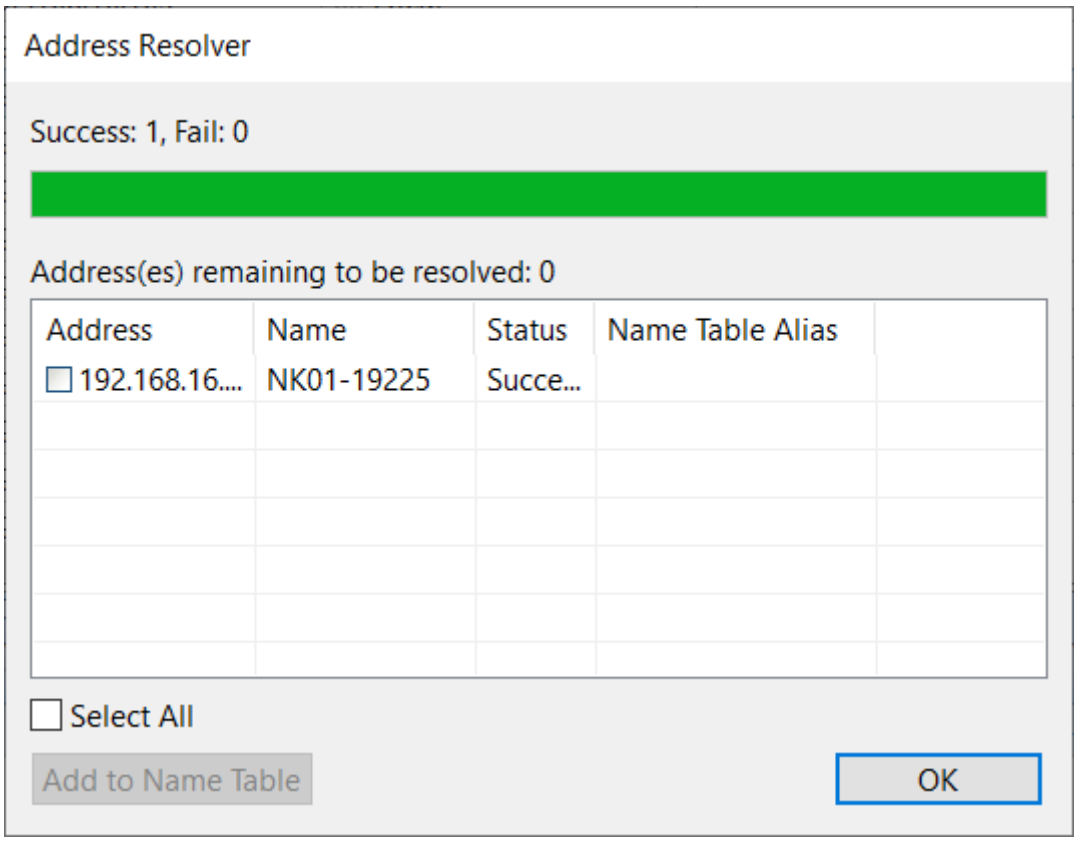
   Tips You can also right-click the selected address node, and select **Add to Name Table** to open the **Add Name** dialog box.

7. 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**.

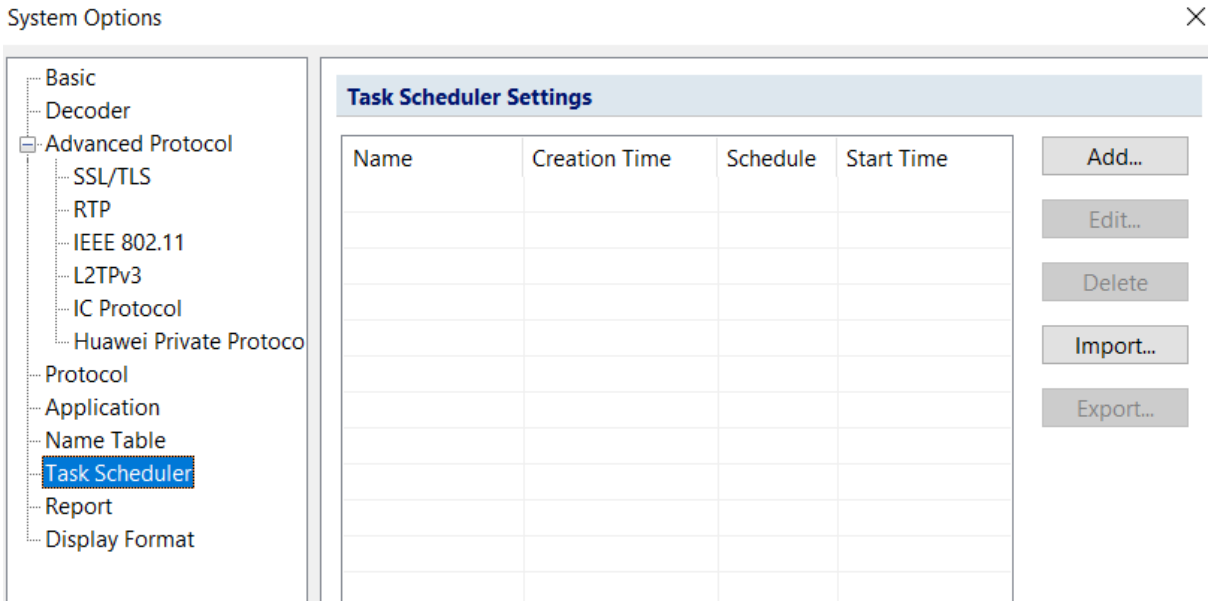
Note Only IP addresses can be resolved by Address Resolver.

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 System Options button, then click the **Task Scheduler** tab.

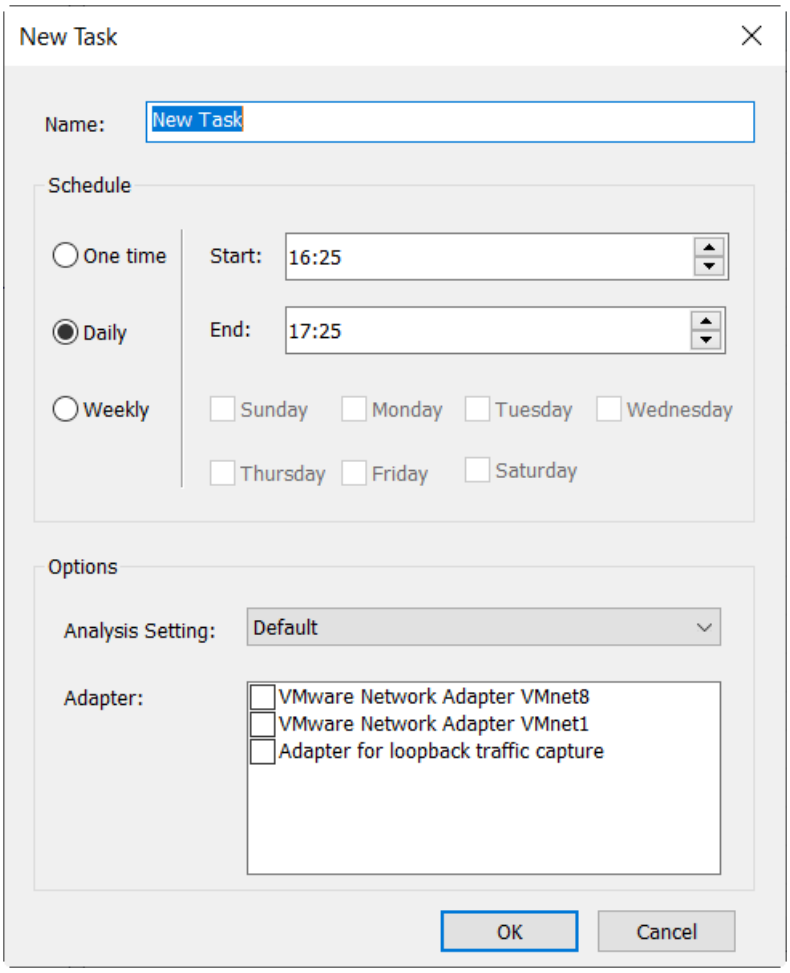


2. Click **Add**, and then type the name of the project, set the frequency for running the project and select appropriate analysis setting and network adapter.
3. Click **OK** to close the **Schedule Project** dialog box.

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:

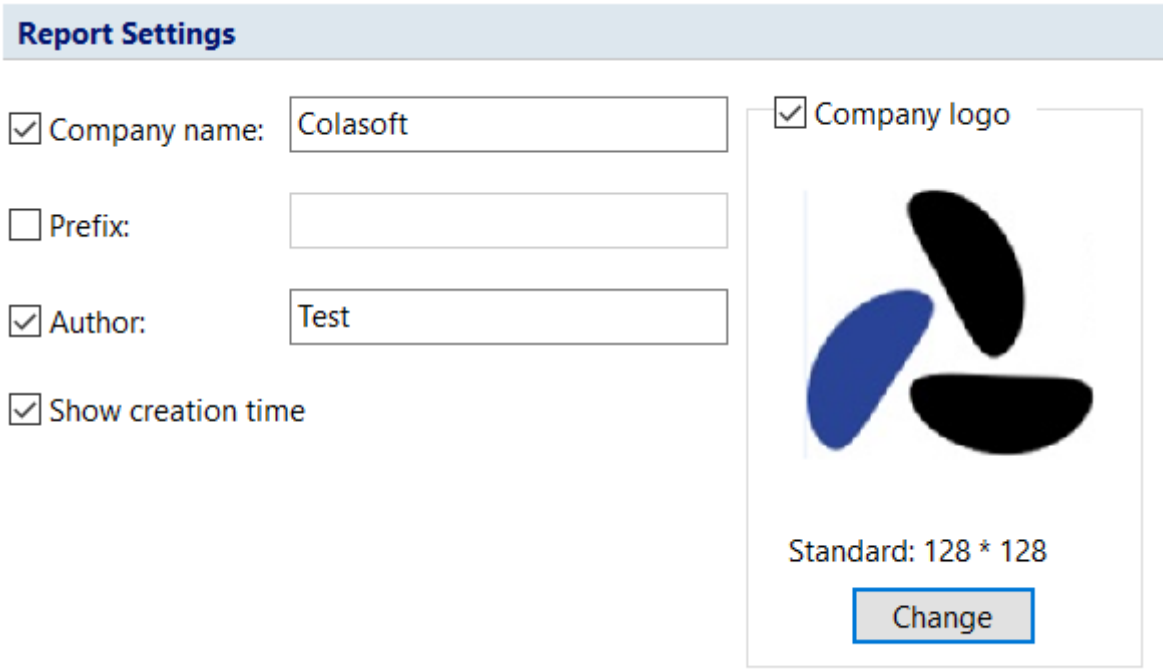
- **Add**: Schedules a new analysis project.
- **Edit**: Edits the selected project.
- **Delete**: Deletes the selected project.
- **Import**: Removes existing projects in the list and imports new scheduled tasks.
- **Export**: Exports existing projects in the list as a.dat file.

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 setting and network adapter for the scheduled task.

Report Settings

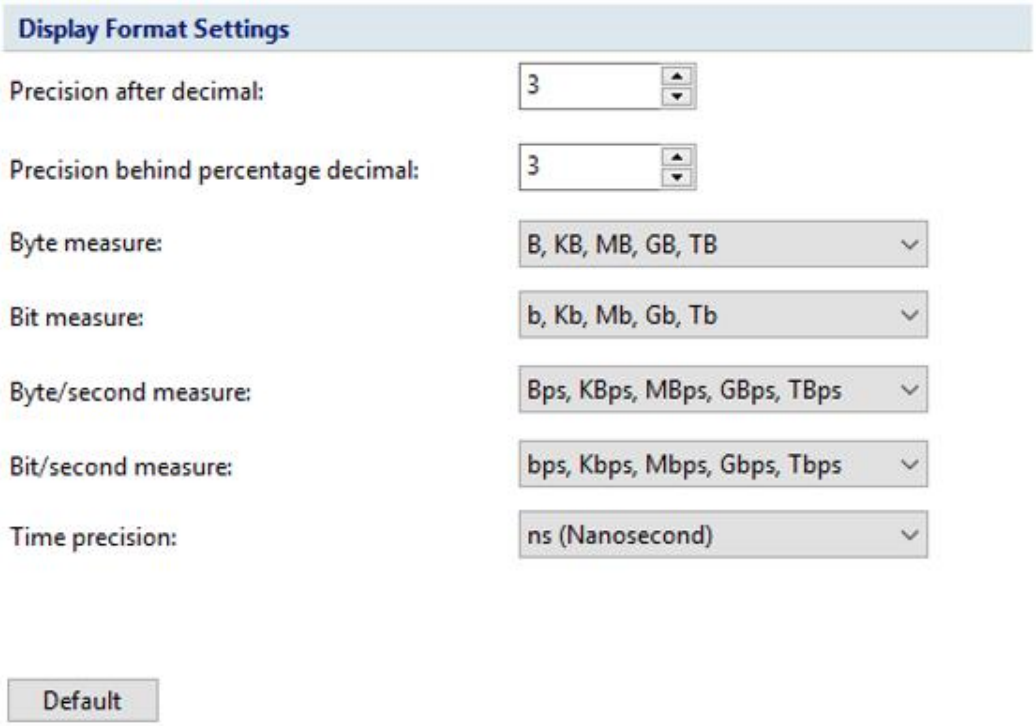


You can configure the following options listed below:

- **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, bytes and bits per second format, etc.



The items on this tab are described as below.

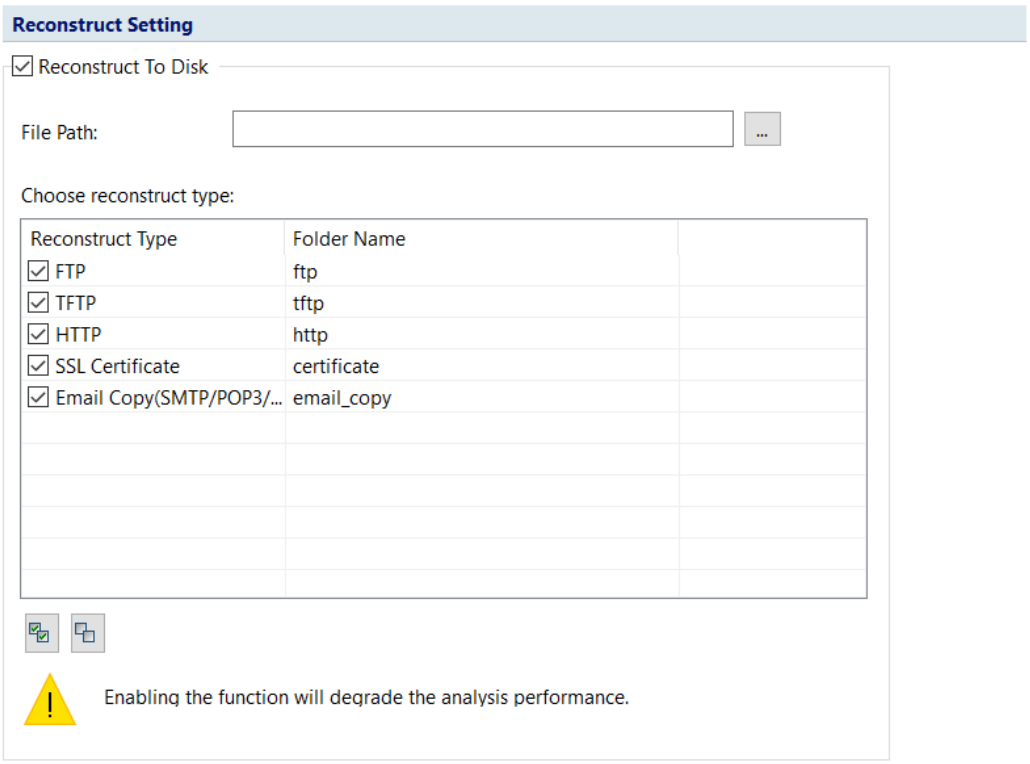
- **Precision after decimal:** The display precision of a value. The number of decimal places is 3 by default, and you can enter a numeric value between 1 and 6.
- **Precision behind percentage decimal:** The display precision of a percentage value. The number of decimal places is 3 by default, and you can enter a numeric value between 1 and 6.
- **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. When you specify a fixed display unit, then all bytes will be displayed in that format.
- **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. When you specify a fixed display unit, then all bits will be displayed in that format.
- **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. When you specify a fixed display unit, then all bytes/second will be displayed in that format.
- **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. When you specify a fixed display unit, then all bits/second will be displayed in that format.
- **Time precision:** The time precision displayed by the system. By default, it's set to nanosecond (ns). Seconds (s), milliseconds (ms) and microseconds (us) also supported.
- **Default**: Resets all the settings on this tab to default.

Analysis Settings

Reconstruct Settings

Capsa is able to extract and fully reconstruct the files transmitted over FTP, TFTP, and HTTP, as well as SSL certificates.

To reconstruct files, enable the checkbox **Reconstruct To Disk** as the screenshot below, set the path to store the files to be reconstructed, and the reconstruct types.



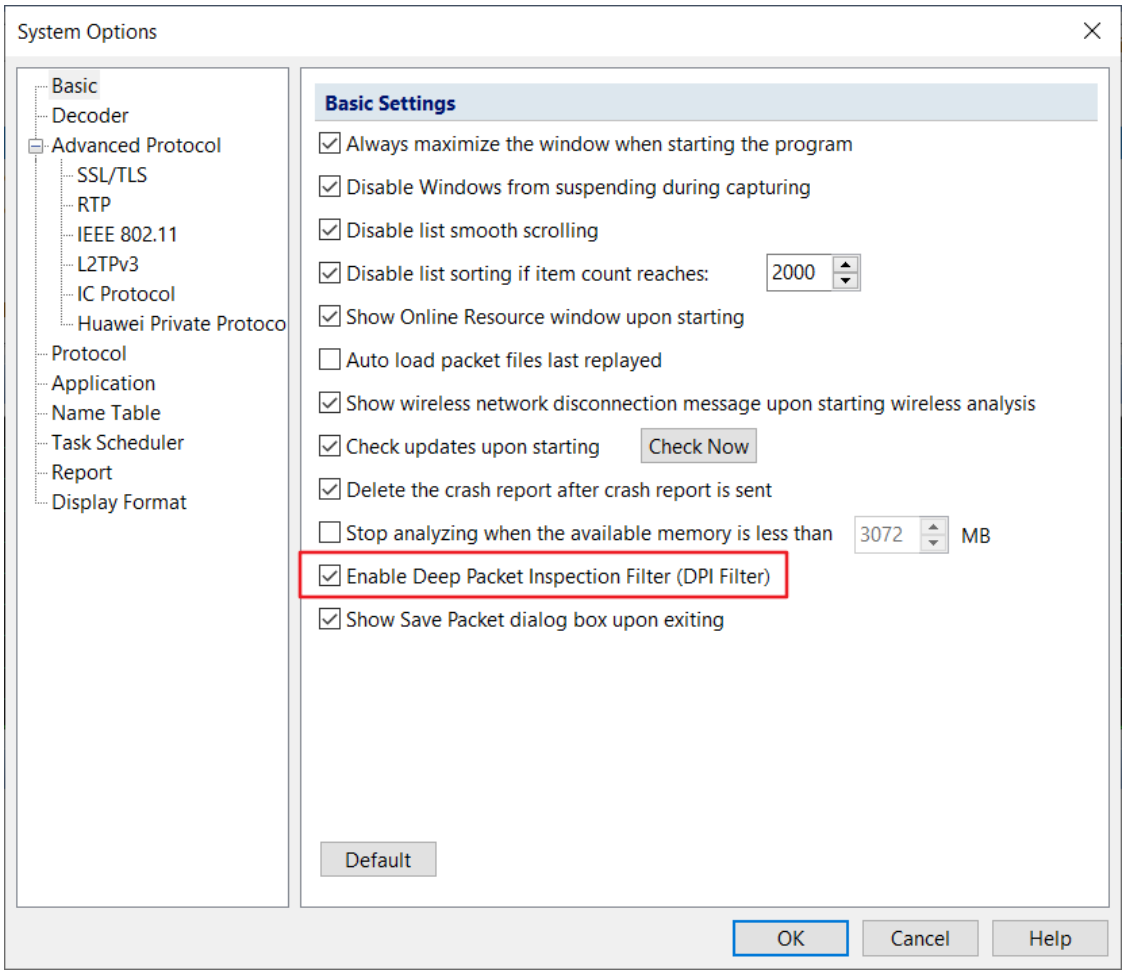
Note Enabling the reconstruction function will affect the system analysis performance a lot.

- Log View
- Log Output
- DPI Filters

Filter settings are the important method for you to change the scope of captured data. If no filters are set, the system will capture and analyze all packets.

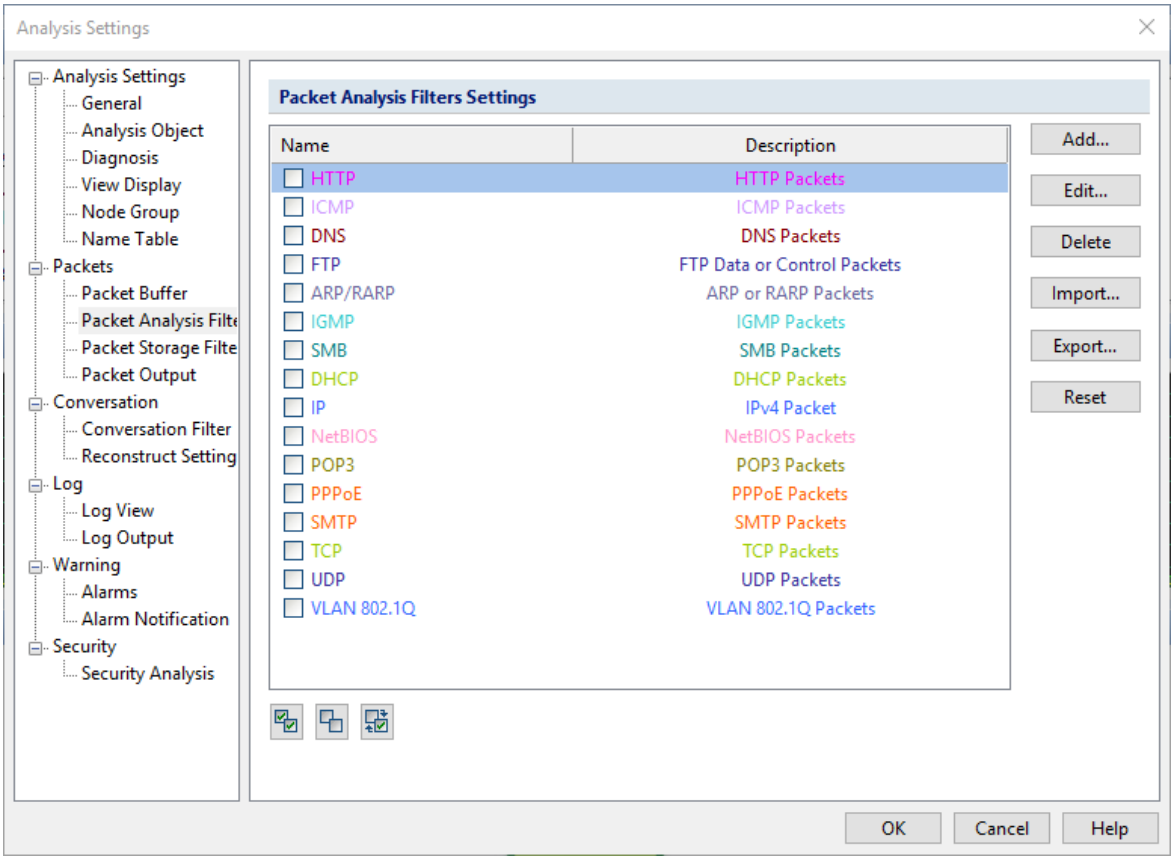
By setting up filters, we can capture only the specific packets, separate important data, and filter out unnecessary data. In this way, you can focus on only the data information of network failure or network attack, instead of looking for it in a large amount of data, reducing the trouble and complexity of finding data in a large amount of data. Colasoft Network Analysis System also provides you with a default list of protocol filters, where you can easily customize filters and manage all filters. In DPI filters, you can input the filter expression to filter packets, so that the results will be more precise.

To enable the DPI Filter, check the option **Enable Deep Packet Inspection Filter (DPI Filter)** on System Options.



In addition to setting the filter in the analysis plan, you can also click the filter icon in the system ribbon to enter the filter settings dialog box, as shown below:

The filter settings interface is shown below.



Filter List

The filter condition in the filter list are all filters that you customize. You can check the filter by checking the corresponding filter. The relationship between different filters exists in logic OR. You can also select multiple filters to combine and customize the capture range of the packets you need. Double click any filter to enter the filter editing interface. You can set the filter condition as you want to add or delete in "DPI Filter Setting", then separate the packets by writing expression conditions.

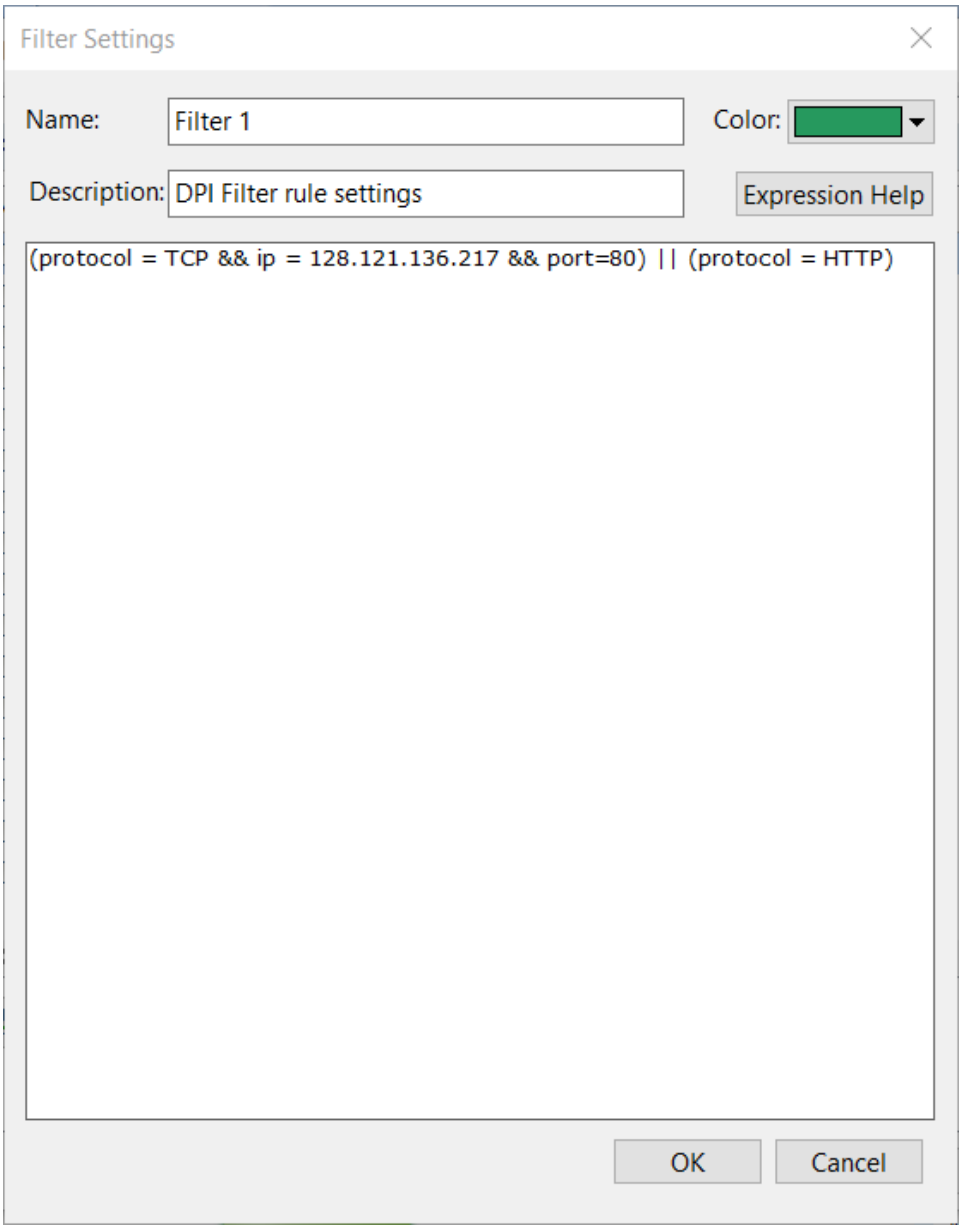
Tips When you create a new filter, the system automatically saves the newly created filter to the filter list. Next time when you reboot the system, you can easily call the previously set filter.

Note The small toolbar on the bottom  , can help you manage the filter list conveniently. The specific functions are: enabled all, disabled all, and reversed.

Note Dpi filter suitable range: Dpi filter is only suitable for 64-bit operating system currently and supports AVX instruction sets. In addition, use the old version of "Filter" to configure the filtering conditions.

DPI Filter Settings

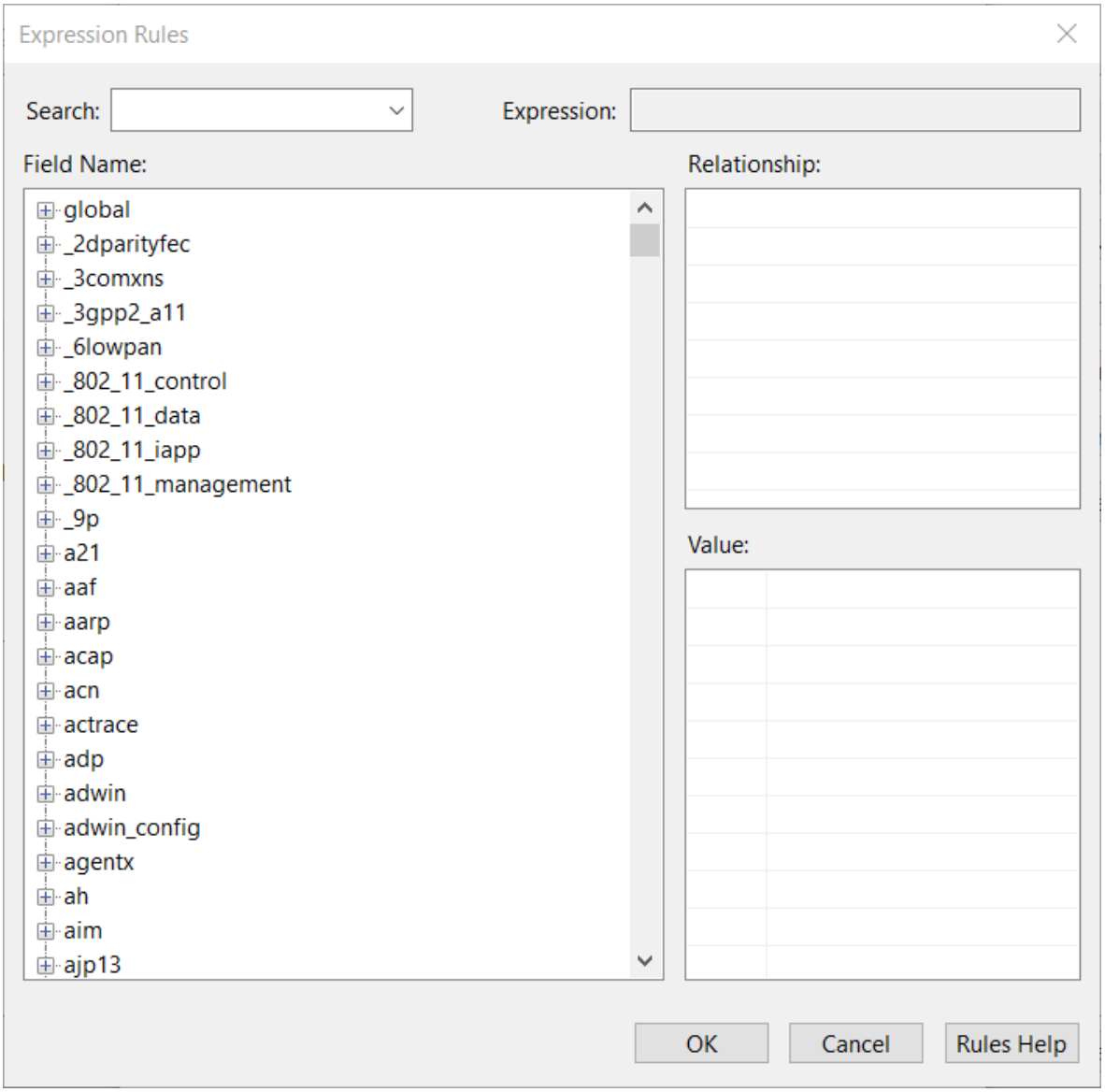
DPI Filter can use expressions to show your filter condition. The interface for DPI Filter settings is shown in the following figure:



Tips Expressions are composed of field names, operators, values, and logical operators. For a detailed description of the expression, please refer to "Help For Expressions".

DPI Filter Help

The help for expression interface lists all currently supported protocols and fields, the operators corresponding to the fields, the value types of the fields, and the writing way for some specific field values. The expression help interface is shown below:

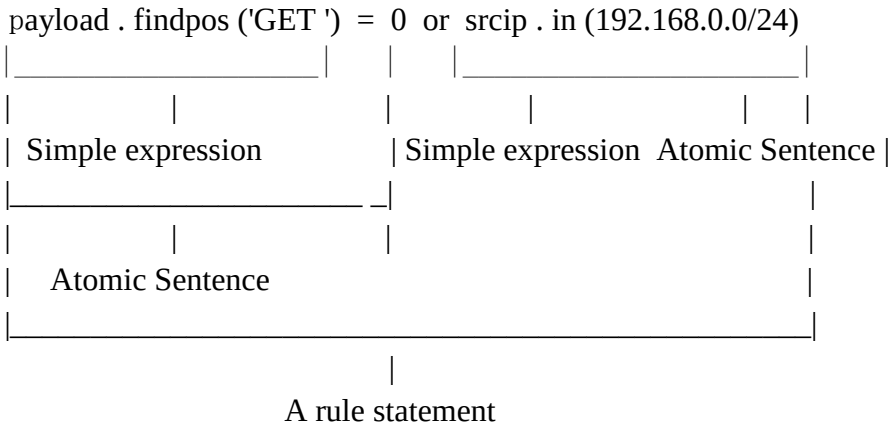


Note If you want to know a certain field, you can search this field with full field name. Or by expanding the tree structure in the field tree, the field-supported operators, type, value will be displayed on the right.

Description of Expression Rule

Rules and Rules Group

1. DPI filtering rules consist of logical expressions; each logical statement consists of a simple expression. For example:



2. A rule group consists of multiple rule statements.

The following rules are composed of 3 rules, here is the ID = 0, 1, 2(There is logical OR between each one of them):

payloadlength <= 30 && payload[0,6].find('https:')

!(payload[3,20].find(HEX'00 00 00 0A 00 00 00 00')) || dstport >=1000

payload[0,4] = HEX'03 00 00 00' and (payload.find(HEX'10 00 00 0C 0A 83 86 7C') or packetlength <= 2000)

Representation Rules of Types

1. Representation Rules of String Type

String	Rules
Single quotes”	Escape characters is not supported. Sets: All ASC|| characters except single quotes”.
Hexadecimal String	Add HEX prefix in front of single quotes, for example:HEX’00 0A’

2. Representation Rules of DateTime Type

DateTime has two longitude types: DTSec and DTNanoSec. Leap second is supported, e.g.: DT'2019-01-01 07:59:60+0800'.

Format	Notes
DT 'year month mday hour min sec'	Second level DT type without time zone, local-host time zone.
DT 'year month mday hour min sec .nanosec'	Nanosecond level DT type without time zone, local-host time zone.
DT 'year month mday hour min sec ±timezone'	Second level DT type with time-zone.

DT 'year month mday hour min sec .nanosec ±timezone'	Nanosecond level DT type with time-zone.

The following constraints should be complied:

- Literal value must contain DT 'and ';
- year Year, consisting of four consecutive numeric characters, the number cannot be less than 1970.
- month Month, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [01,12];
- mday day of the month, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [01, 31];
- hour Hour, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 23];
- min Minute, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 59];
- sec Second, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 60], support leap second.
- nanosec Nanosecond, consisting of 9 consecutive numeric characters, if the number is less than night digits must be padded by zero; It must use the profix '.', And no other characters can be mixed between the nanosecond and the prefix. The presence or absence of nanoseconds is a unique identifier for determining the accuracy of a DT type: No nanosecond is of the DTSec type; there are nanoseconds of the DTNanoSec type;
- timezone Time zone correction, time difference from GMT/UTC, consisting of 4 consecutive numbers of characters, the first two digits stand for hour and two digits after is minute. Less than four digits must be padded by zero; it must appear with the prefix + or - and must not be mixed with any other characters, + means earlier than UTC, - means later than UTC
- Other
  1. DT Literal value will ignore all white space characters such as ' ', '\t','\n' etc.
  2. year, month, mday Only one valid non-white character can be used to divide year/mouth/mday.
  3. hour, min, sec Only one valid non-white character can be used to divide hour/min/sec.
  4. Valid non-white partitioning characters include (including but not limited to)!"#$%&* +,./:;@^_|~.

Examples of valid format:

Type	Example
Without time zone suffix: the default is the time zone of local time	DT'2019-09-26 11:02:59' DT'2019/09/26 11:02:59' DT'2019-09-26 11:02:59.981815000' DT'2019/09/26 11:02:59.981815000'
UTC	DT'2019-09-26 11:02:59+0000' DT'2019/09/26 11:02:59+0000' DT'2019-09-26 11:02:59.981815000+0000' DT'2019/09/26 11:02:59.981815000+0000'

Chinese Standard Time CST	DT'2019-09-26 11:02:59+0800' DT'2019/09/26 11:02:59+0800' DT'2019-09-26 11:02:59.981815000+0800' DT'2019/09/26 11:02:59.981815000+0800'
Pacific Standard Time PST	DT'2019-09-26 11:02:59-0800' DT'2019/09/26 11:02:59-0800' DT'2019-09-26 11:02:59.981815000-0800' DT'2019/09/26 11:02:59.981815000-0800'
Other Valid Format	DT'20190926 11:02:59-0800' DT'20190926110259' DT'20190926110259+0800' DT'2019/09/26 110259-0800' DT'2019 09 26 11 02 59 +0800' DT'2019-09-26 110259-0800' DT'20190926110259.055000000+0800'

3. Representation Rules of Regular Expression Type

Regular expressions are only used in the find () function. The regular expression syntax consists of two parts: pattern and modifiers. Writing format: /pattern/modifiers; modifiers can be used by default.

Pattern: Perl/POSIX style regular expressions.

Single slash '\' in pattern means character escaping.
When \ and / as special character exist in pattern, they need to be escaped into: \\ and \/

modifiers: Matching method (pattern modifiers)

One modifiers consists of zero or multiple modifiers: I, m, s, V
Related function is not enable until the specific modifiers is configured.
modifiers can be superimposed.
Multiple modifiers must be connected, no other characters can be mixed in between. For example, there is a space between modifiers in /abc/i m, which is the wrong writing style.

Description of modifiers

Modifier	Paraphrase
i	Case insensitive
m	^ can match the beginning of a line; $ can match the end of a line Note: The first byte of the payload is not at the beginning of the line.
s	. can match any character, including newlines.
v	Allow empty strings, such as (a|).

Note Regular expression rules are not fully supported. Some advanced usages are shown below:

Advanced	Support or not	Example
(?:pattern)	Support	/(?:45|56)123/
Zero-width assertions	Support	Zero width assertion: /(?!abc)def/
Back-references	Not support	nChronos reference:/.*?<\/[hH]\1/s
Conditional references	Not support.	/(?(1)foo|bar)/

4. Int Integer type, sets: 8 bytes signed integer
5. IP type. **Only supports IPv4 currently**. Use the String type to set IPv6 rules.

1) IPv4 literal-value writing supports dotted decimal and dotted hexadecimal, and their mixed style(wiki-IPv4). Decimal and hexadecimal IPs are also limitedly supported. Such as a valid IPv4 literal value:

Format	Value	Whether can be used to write IP range (segment/subnet)
Dotted Decimal	192.0.2.235	Support
Dotted Hexadecimal	0xC0.0x00.0x2.0xeB	Support
Mixed	192.0.0x2.235	Support
Hexadecimal	0xC00002EB	Not support
Decimal	3221226219	Not support

2) IP Range (Segment/Subnet)

IP Range (Segment/Subnet) represents a closed IP interval.

All Valid Format	Notes
192.168.1.0-192.168.1.255	IPv4 range, commonly used
192.168.1.0/24	IPv4 subnet, commonly used
192.168.0x01.0-192.168.1.255	
192.168.0x01.0-192.168.1.0xff	
192.168.0x01.0/24	
192.168.0x01.0/0x18	

Member function of types

String type member function

Function Name	Example	Description
find	payload.find('HTTP 1.')	The matching method of fixed feature string. If the feature string exists in

		parent string, the value of the expression is true; if not, then false.
find	payload.find(/ [hc]at<\/tag>/i)	The matching method of the regular expression version. Specially, payload[2, 10].find(/a[0-9]*c/) will search the whole packet for a[0-9]*c, only to guarantee the drop point of 'c' in [2,10] in payload, even if 'a' doesn't appear in payload.

Int type member function

Function Name	Example	Description
findpos	payload.findpos('ABC')	Returns the offset value in parent string payload to feature string 'ABC'. Offset value starts from zero. If this feature string does not exist in the parent string, the value of its logical expression is abnormal. The contrast value of findpos() should not be less than zero.
N2H16	payload.N2H16()	Returns the positive integer from network byte order converts to little-endian order of the first two bytes for payload.
N2H32	payload[30,100].N2H32()	Returns the positive integer from network byte order converts to little-endian order of the first four bytes for string.
N2H64	payload.N2H64()	Returns the positive integer from network byte order converts to little-endian order of the first eight bytes for string.

IP type number function

Function Name	Example	Description
in	srcip.in(192.168.1.0-192.168.1.30)	Judge the srcip belongs to a continuous IP range or not.
in	dstip.in(192.168.1.1/24)	Judge the dstip belongs to a IP subnet or not.

Operators (operators, modifiers, etc.)

No arithmetic operators like '+' or '-' are currently provided yet.

Type of Operators	Paraphrase
Relation	Relational operators
Logic	Logical Operators
Grouping	Grouping operators
Modifier	Modifiers

Priority: Grouping > Modifier > Relation > Logic

1. Relational Operators

Relation Operators	Paraphrase
=	Equal
<	Less than
>	Greater than
!=	Not equal to
>=	greater or equal to
<=	Less or equal to

2. Logical Operators

Relation Operators	Paraphrase	Priority	Direction
! not	NOT	High	From right to left.
&& and	AND	Medium	From right to left.
|| or	OR	Low	From right to left.

3. Grouping Operators

Grouping Operators	Paraphrase	Priority	Example
()	Group	Highest	such as:!(bool_expr1||bool_expr2);(bool_expr1||bool_expr2) && bool_expr3 etc.

4. Modifiers

Modifiers	Paraphrase	Description/Examples
()	Function call	find()

[a, b]	String endpoint modifiers. a, b is used to indicate the expected maximum endpoint, both of which are integer type.	Used for String expression to get a SubString. Endpoints is disable in SubString.
.	Member access	HTTP.url ; payload.find('str')
.	Used for literal value of IP type	192.168.0.1
''	String literal value modifiers	Empty literal-value String '' is not allowed, also escape is not allowed.
HEX''	Profix modifier for hexadecimal string, and only single quotes are supported. No other characters are allowed between HEX and the first single quote.	Both uppercase and lowercase letter can be used in single quotes, and letter in mixed case is allowed. Between byte and byte there must be separated by a white space characters. The width limit for each single byte is 2 bytes and it should be filled with zero (0) if the width is not enough. Allow multiple consecutive whitespace characters as a split.
/pattern/modifiers	Regular expression	Modifiers can be default; regular expressions are only available for find()

Additional notes for the boundary modifier [a, b]:

- a is for the expected left-endpoint, b is for the expected right-endpoint. [a, b] stands for an interval which is greater than or equal to a and less than b.
- Range: a, b ∈ { -2147483648, ..., -2, -1, 0, 1, 2, ..., 2147483647}
- a < b and a × b >= 0 is strictly true.
  There are only two cases, for example, as for the parent string 'helloworld':
  1) 0 <= a < b :

	0	1	2	3	4	5	6	7	8	9	10
	h	e	l	l	o	w	o	r	l	d	

  2) a < b <= 0 :

-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0

  In the example, [1,4] will get 'ell' and [-4,0] will get 'orld'.
  Because of the expected endpoints, [1,200 will get 'elloworld'.
  In the example, if someone modify 'helloword' with [200,300], then will get an exception-string null
- Strategy for value: between the same modifying range of a string, if there is intersection, this

intersection will be taken; and if no intersection exists, then return an exception-string nullstr.
Modifying a 0 long empty string will obtain an exception sting.
Modifying an exception string will still obtain an exception string.

- Endpoint a default: the left boundary; b default: the right boundary; an and b are not allowed to be default in the same time. [0,] is equal to [, 0], and they can be used to show parent string.
- The following writing is legitimate:
  [1, 2], [1,], [, -20], [-10, -1], [-10,], [0,], [, 0], [, -1], [, 10]

Metadata Field

Two writing styles for metadata field

1. Common form: data source.field

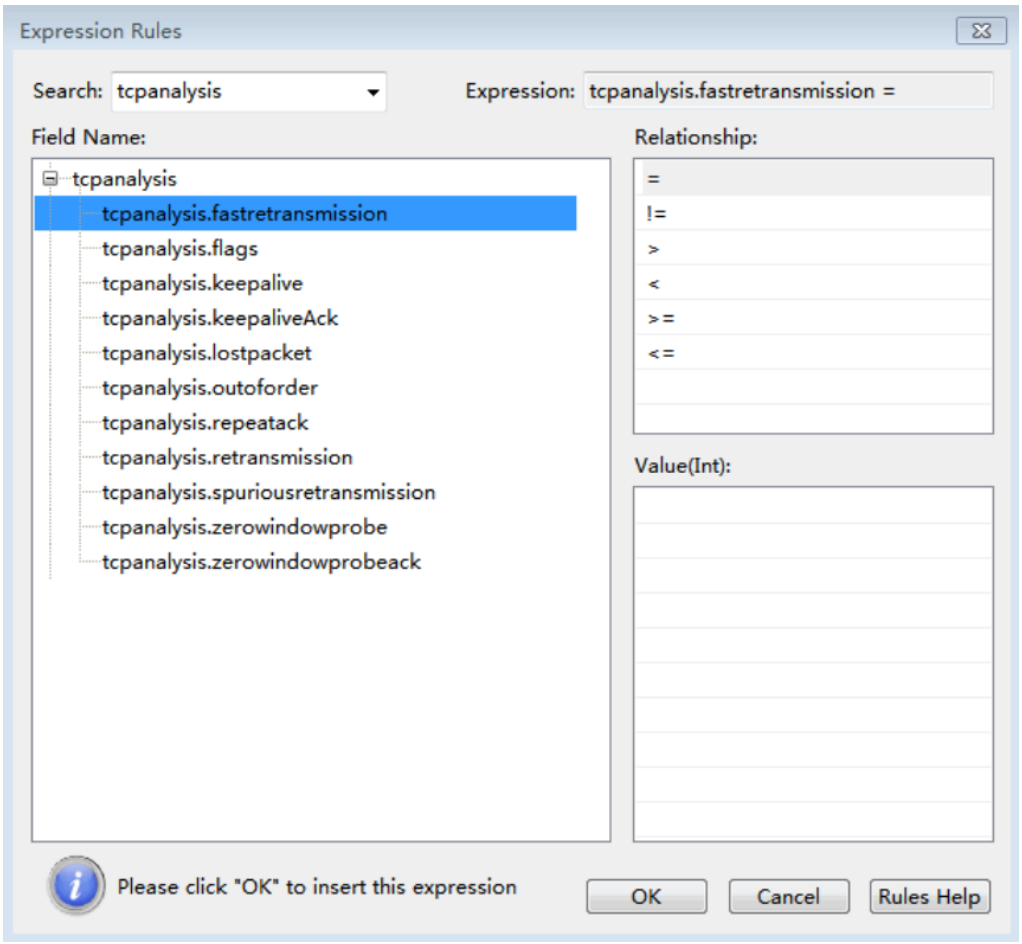
2. Built-in global field writing style

Built-in Metadata Field	Paraphrase
packet	Packet
capturelength	Packet captured length
packetlength	Packet length
payload	Payload of TCP or UDP
payloadlength	Payload length
ip	IP address
srcip	Source IP
dstip	Destination IP
port	Port
srcport	Source port
dstport	Destination port
timestamp	Timestamp

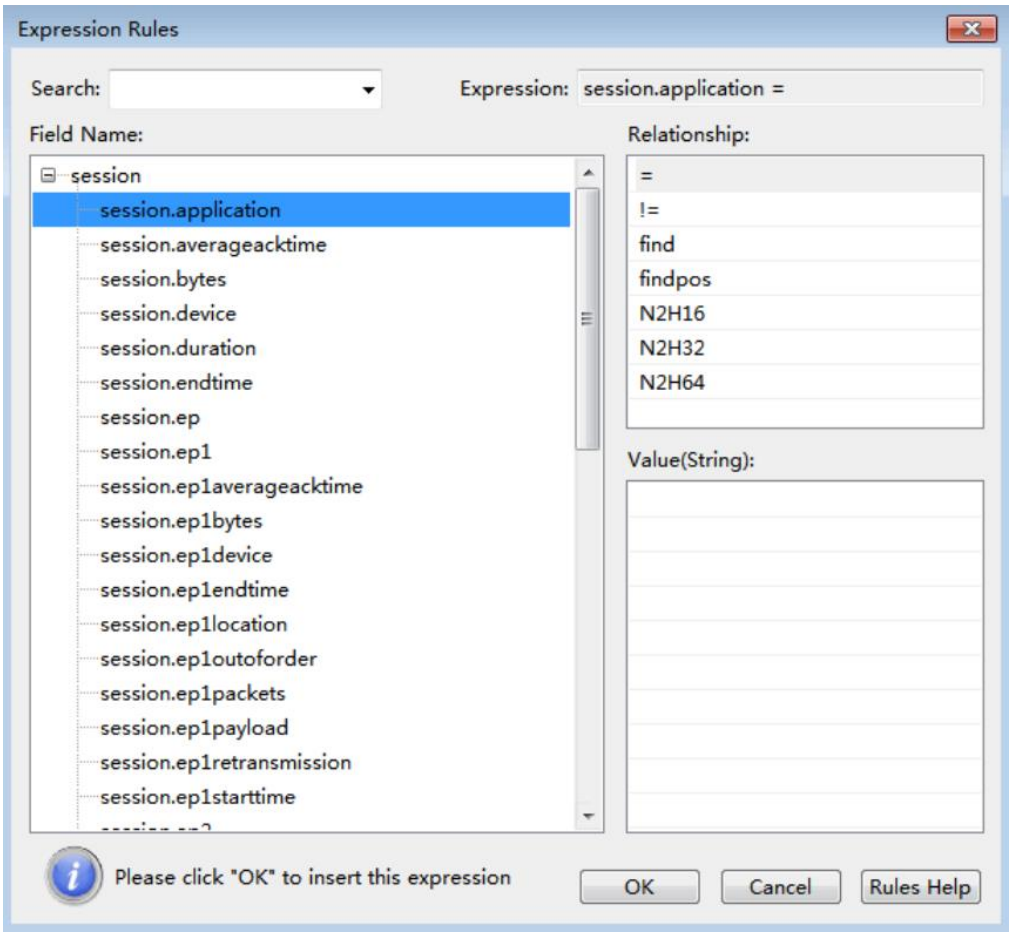
Operators supported by built-in fields

Fields	Data Type	Supported Operators
packet / payload	String	[a, b] . = !=
capturelength / payloadlength / srcport / dstport / port / timestamp	Int	All relational operators
srcip / dstip / ip	IP	= != .

In Packet view, TCP analysis fields (*tcpanalysis*) are added in display filter. The fields are applied after packet analysis.



In Conversation view, there are only session fields (*session*) in display filter. The fields are applied for conversation statistics only.



Note The fields related to the number of bytes and time in the session field support filtering of different precisions, and these fields are all int type fields, and do not support floating-point number writing.

1. Byte count related fields: **session.bytes, session.ep1bytes, session.ep2bytes**.
   The unit of byte size is b(byte) by default, and k(kb), m(mb), g(gb), t(tb) are also supported. ex: session.bytes > 1024k can also be written as session.bytes > 1mb.

2. Time related fields: **session.duration, session.averaggeacktime, session.ep1averageacktime, session.ep2averageacktime, session.maxacktime**.
   The unit of time size is nanoseconds(ns) by default. and microseconds(us), millisecond(ms), second(s), minute(m), hour(h). ex: session.duration > 60s can also be written as session.duration > 1m.

3. String type field: **session.payload, session.uncompressedpayload, session.decryptedpayload** is written according to the expression of the String type field, where **session.payload** represents TCP or UDP session content filtering, **session.uncompressedpayload** represents HTTP session data decompression content filtering, and **session.decryptedpayload** represents the decrypted SSL/TLS session data content filtering.

Abnormalities Occurring During the Calculation

If an exception occurs during the calculation of a logical expression, the value of the logical expression will also be an exception. The abnormal state is the third state which is not true or false, and it is not just true or false in multi-valued logic. The calculated range of an atomic logic expression is: {true, false, abnormal}.

The rules for predicate calculus and logical operations with abnormal participation are as follows (tristate booleans, here the third state is assumed to be abnormal):

1. The result of logic expression with any predicate calculus involving abnormal operand is abnormal. Contains all relationship comparisons: =! = > >= < <=.
2. Logic OR operation (||) with abnormal operand, if the result is true, then it is true, other results are abnormal.
3. Logic AND operation (&&) with abnormal operand, if the result is false, then it is false, other results are abnormal.
4. Logic NOT operation(!) with abnormal operand, the results would be abnormal.

Our definition of an atomic logical expression hit means that the atomic logical expression has a value of true; the definition of a rule hit is that the value of the rule is true.

Examples of situations that may cause anomalies:

1. Range modification of String is no intersection out of bounds, which will cause the operand to be an exception-string nullstr.
2. There is a special field payload in the global data source. if the length of payload is zero (payloadlength = 0), then payload is an exception-string nullstr. Its intuitive semantics is "no load." But not all String fields which length is zero are exception string, it depends on the registration strategy of the field.
3. The built-in findpos function throws an exception when no signature string is found. That is the rule: StringOperand.findpos('abc') < 20 ||! (StringOperand.findpos('abc') < 20), If 'abc' isn't found in StringOperand, then the rule won't hit.
4. Other conditions that may cause an abnormal.

Multi-valued "Existing Quantifiers" and "Full Quantifiers"

Mathematically, existential quantifier means that there is at least one exist, and full quantifiers means all. A statement modified by an existing quantifier, the multi-value is logic OR expression, and a statement modified by full quantifiers, the multi-value is logic AND expression.

For example, a multivalued Int type operand var, its value is [1,3,10}, As the rule set, for var > 11, if modified with an existing quantifier, the value of the expression is true as long as there is any value greater than 11. In the meanwhile, if it was modified with full quantifiers, then the value of the expression would be true only if all values are greater than 11.

The current engine (v3.2.2) does not implement the explicit specification of the existing quantifiers and the full quantifiers. In the case of no specified quantifier, it will always be existing quantifiers. That is to say, the existing quantifiers are implemented in the current engine version.

The application of existing quantifiers:

- port > 80 is equal to srcport > 80 || dstport > 80
- ! (port > 80) is equal to! (srcport > 80 || dstport > 80) and equal to srcport <= 80 && dstport <= 80

DPI Filter Expression Example

- String Expression
- DateTime Expression
- Regular Expression
- Int Expression
- IP Expression
- Multi-value Expression

String Expression

- Match the string "abcd" in the payload: payload.find('abcd')
- Use hexadecimal to match the string "abcd" in the payload: payload.find(HEX'61 62 63 64')
- Use the boundary modifier to find the content and match the string "abcd" in the payload:
  payload[2,50].find('abcd'), which means to find "abcd" in the data at offset 2 to offset 50 in the payload
  payload[,50].find('abcd'), which means to find "abcd" in the data at offset 0 to offset 50 in the payload
  payload[10,].find('abcd'), which means to find "abcd" in the data starting at offset 10 in the payload
  payload[-10,-1].find('abcd'), which means to find "abcd" in the data offset from the 10th to the 1st in the payload
- Match the offset of the string "abcd" in the payload greater than 10:
  payload.findpos('abcd')> 10
- Match data packets where the http.url field does not exist: http.url.isnull()
- Match the payload length greater than 100: payload.length()> 100
- Match the first byte in the payload greater than 10: payload.U8()> 10

DateTime Expression

- timestamp = DT'2021-9-10 13:00:10', indicating that the matching timestamp is "2021-9-10 13:00:10"
- timestamp = DT'2021-9-10 13:00:10.981815000', indicating that the timestamp matches in nanoseconds
- timestamp = DT'2020-09-26 11:02:59+0800', which means to match the second-level timestamp with time zone; +0800 means East Eighth District time, that is, Beijing time; -0800 means West Eighth District time; 0000 means UTC time

Regular Expression

- Match the string "aBCd" in the payload, and is case sensitive: payload.find(/aBCd/i)

- Match the string "ab\c\d" in the payload, and is case sensitive: payload.find(/ab\\c\\d/i)
- Match the string "ab[any single character]d" in the payload: payload.find(/ab.d/s)
- Match the string "ab[any multiple characters]d" in the payload: payload.find(/ab.*d/s)
- Match the string "ab[any single character]D" in the payload, and is case sensitive: payload.find(/ab.D/is)

Int Expression

payloadlength = 100; payloadlength> 100; payloadlength <100; respectively indicate that the matching payloadlength is equal to 100, greater than 100, and less than 100

IP Expression

- Match a single ip: ip = 192.168.9.12
- Match IP range: ip.in (192.168.9.1-192.168.9.15)
- Match IP subnet: ip.in(192.168.1.1/24)
- Match the IP in the set, the elements in the set can be a single ip, ip range, ip subnet: ip.in(192.168.9.20,192.168.9.1-192.168.9.15,192.168.1.1/24)

Multi-value Expression

When matching multi-value types, the results of "!=" and "!" are different, for example:

ip != 192.168.9.12 is equivalent to (srcip != 192.168.9.12 || dstip != 192.168.9.12);

!(ip=192.168.9.12) is equivalent to (srcip != 192.168.9.12 && dstip != 192.168.9.12);

protocol != TCP is not equivalent to !(protocol = TCP) ;

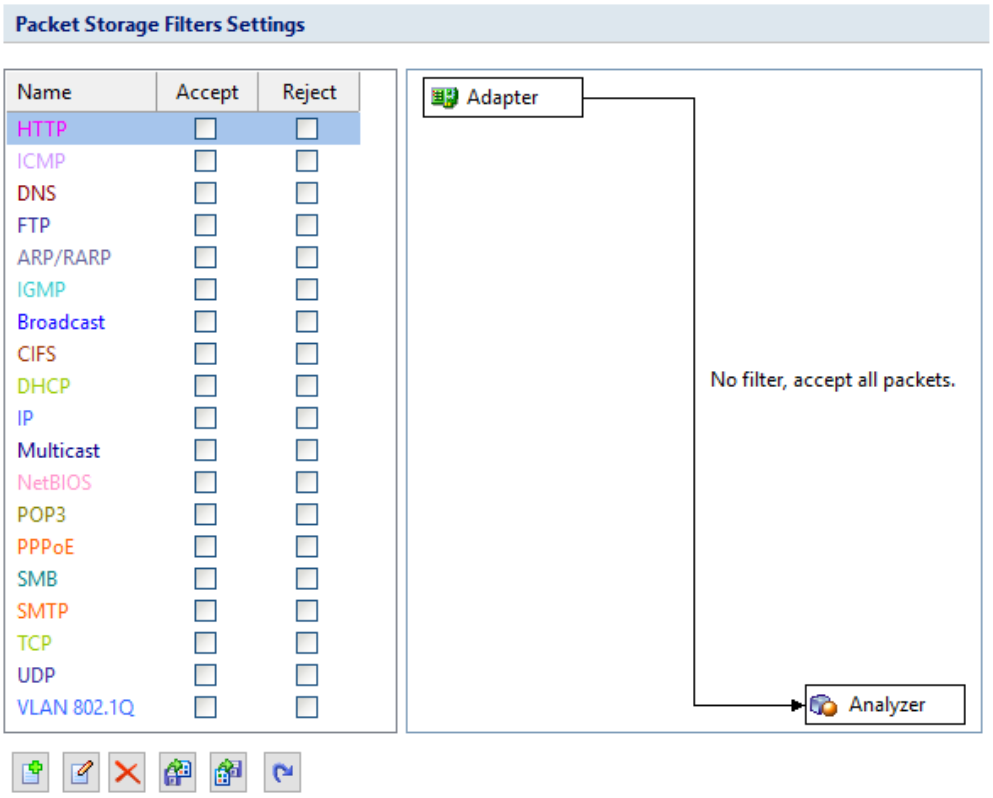
port != 80 is not equivalent to ! (port = 80).

This is because in the packet, ip represents the source IP and destination IP; port represents the source port and destination port; protocol represents the data link layer, transport layer, application layer and other different levels of protocols.

Currently, the multi-value types in Filter include ip, port, protocol, and all fields under all protocols.

Packet Storage Filters

This tab is for containing, setting up, and applying storage filters. Storage filters are utilized to storage particular packets. If no filter was enabled, Capsa will storage all the packets that are analyzed. Unlike the analysis filters, the filtered packets in the storage filters are still analyzed and counted, but are not placed in the display cache. The filter conditions only apply to storage (display cache, packet cache). Packet storage filters can improve the storage performance of the system.



This tab 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 stored by Capsa, while **Reject** means only packets unmatched will be stored 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.

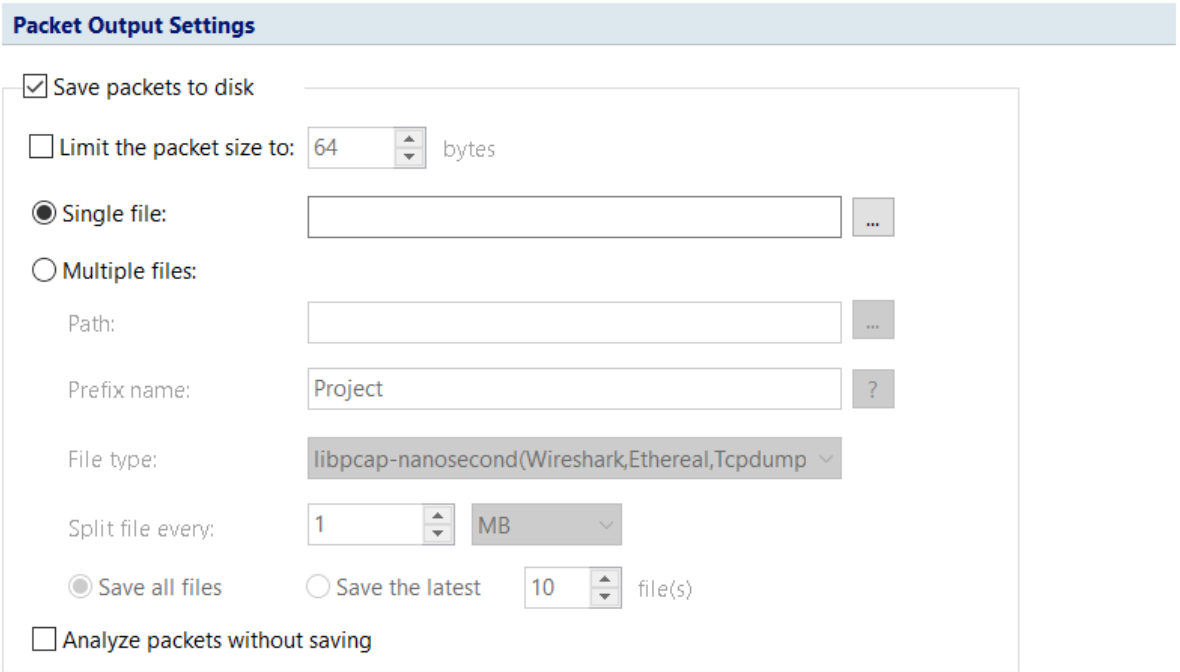
To create a storage filter.

1. On the Storage Filter tab of the **Analysis Settings** dialog box, click  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 (see Creating Simple Filter and Creating Advanced Filter for details).
3. Click **OK** on the **Packet Filter** dialog box, and click **OK** on the **Packet Filter Settings** dialog box.

Note After creating a filter, you should select the **Accept** or **Reject** checkbox to make the filter take effect.

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.

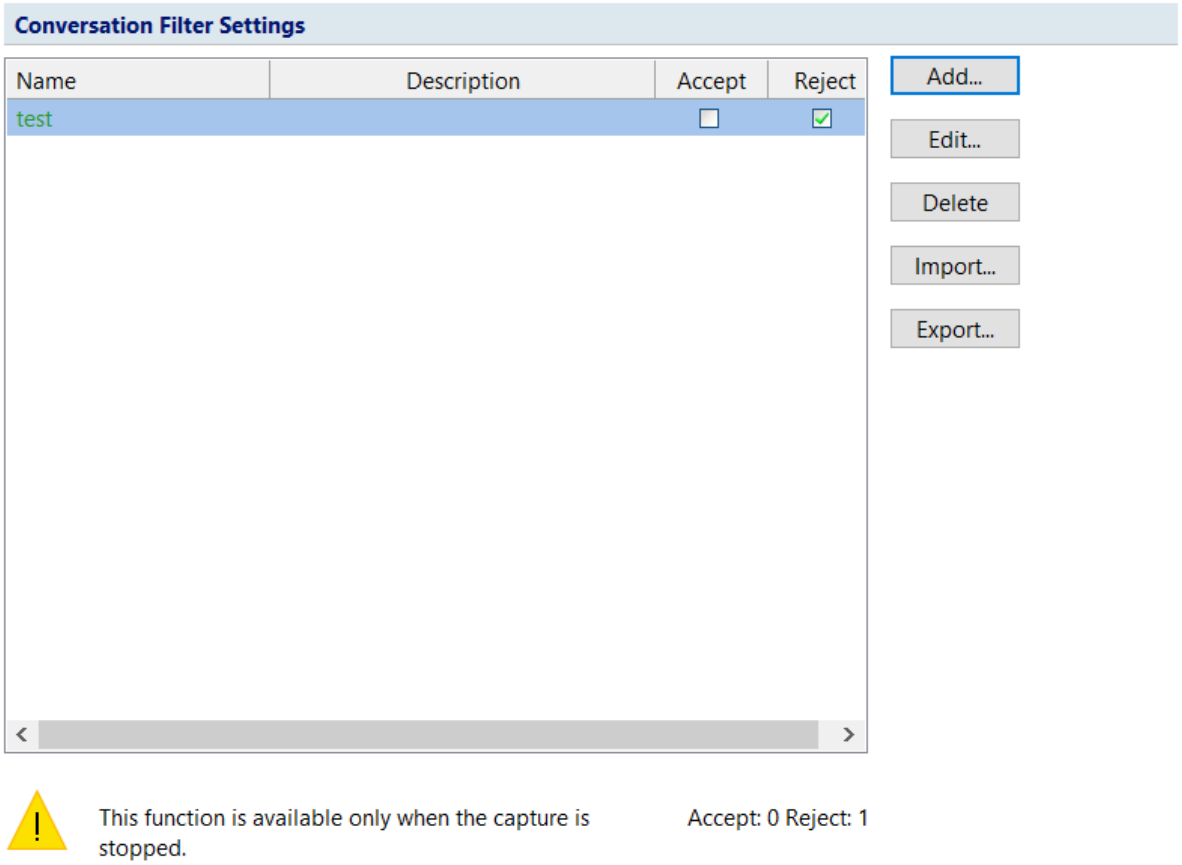
Difference between Packet Buffer and Packet Output

Packet Buffer is for buffering the packets on the Packet view. For example, when you capture a traffic of 30M and you set up a Packet Buffer of 16MB, the Packet view will only display packets of 16MB, the other 14MB of packets are discarded due to not enough packet buffer; all 30MB packets are analyzed by Capsa, but 14MB packets cannot be displayed. In other words, the size of Packet Buffer only impact the number of packets displayed on the Packet view.

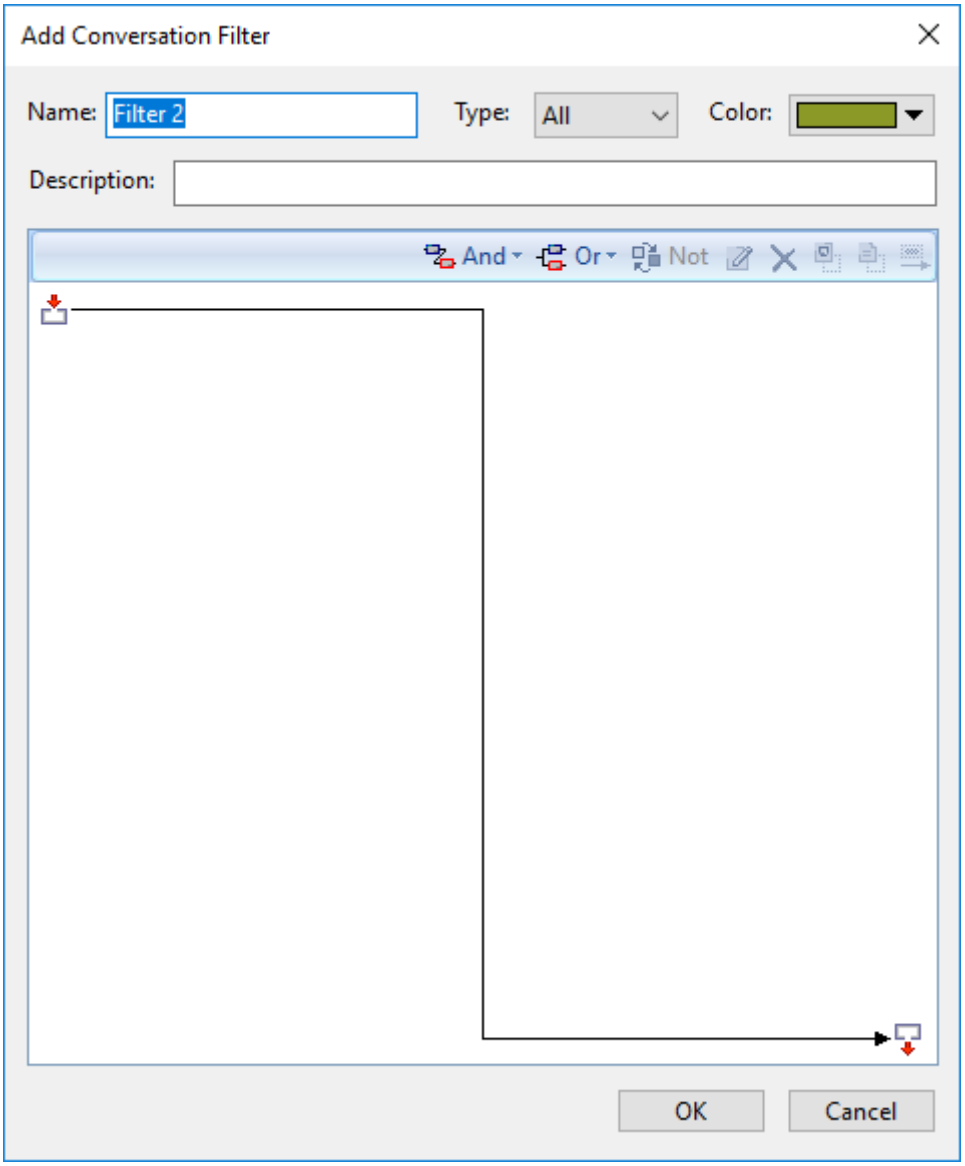
Packet Output feature is for automatically saving all the packets, the packets from the start to the end of a capture. It has nothing to do with Packet Buffer. No matter the size of the Packet Buffer, Capsa will save all packets once the Packet Output feature is enabled.

Conversation Filter

You can configure the conversation filter when the capturing is stopped. By configuring the conversation filter, Capsa will be able to provide a certain kind of conversation data.



You can add a conversation filter by clicking the add button.



You can configure the following fields to set up the conversation filter:

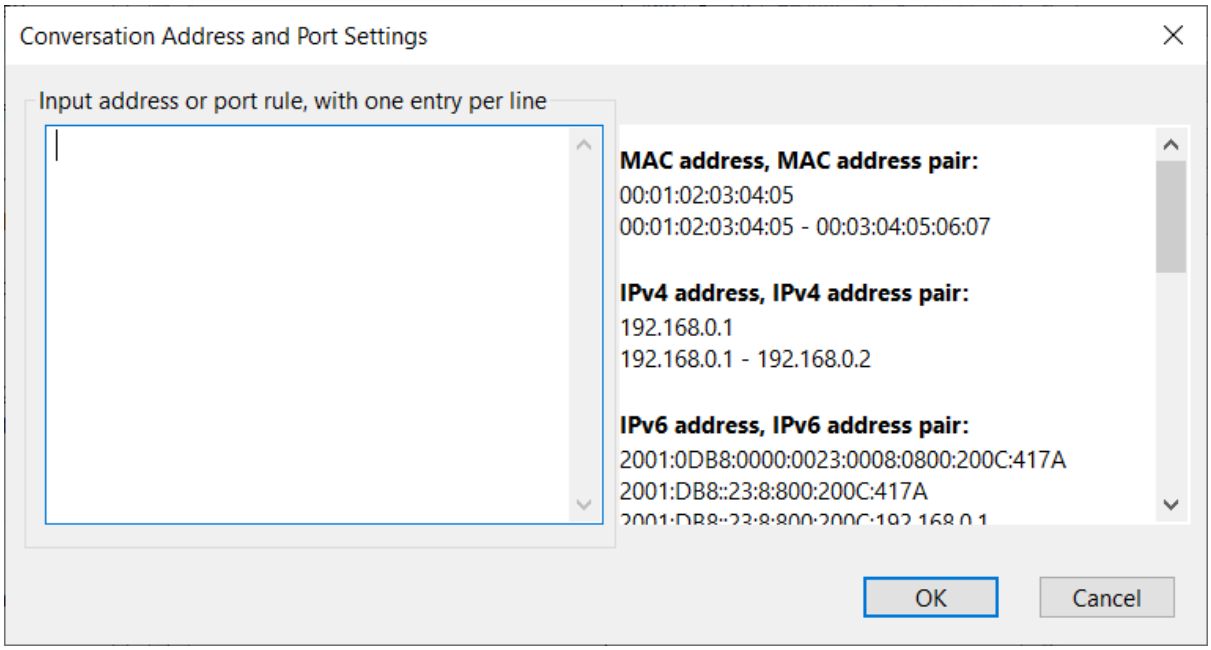
Field	Explanation
Name	The name for this filter.
Type	Capsa supports filter on MAC conversation, IP conversation, TCP conversation, UDP conversation. You can set a filter on one of them, or you can also set a filter on all of them.
Color	Set the color for the filter's name.
Description	You can put a brief description for you filter.
Rule	1. Capsa supports having multiple rules in one filter. The "and", "or" relationship between rules is supported. 2. Each rule supports to filter according to the address and port, location,

conversation protocol, conversation packet, conversation content, and conversation option.
For the configurations please refer to the instruction of each Rule.

Rule

- **Address and Port**

  This feature allows you to filter conversations according to the address or the port.

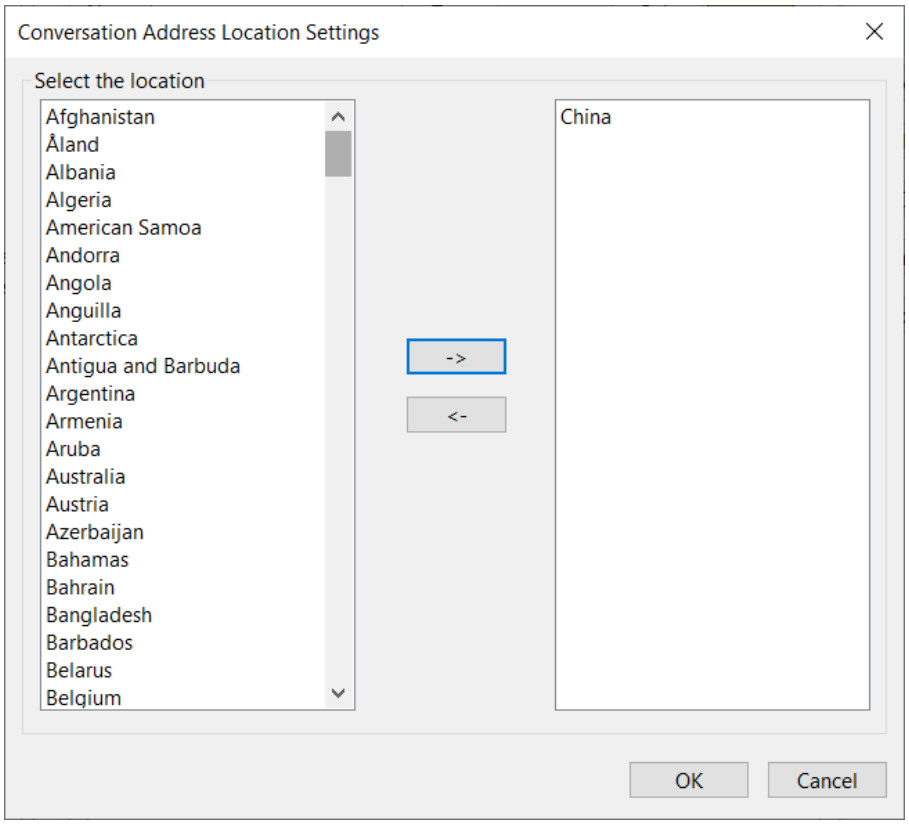


  As it is shown in the figure, Capsa supports multiple ways to configure the filter to fit all kinds of conversations:

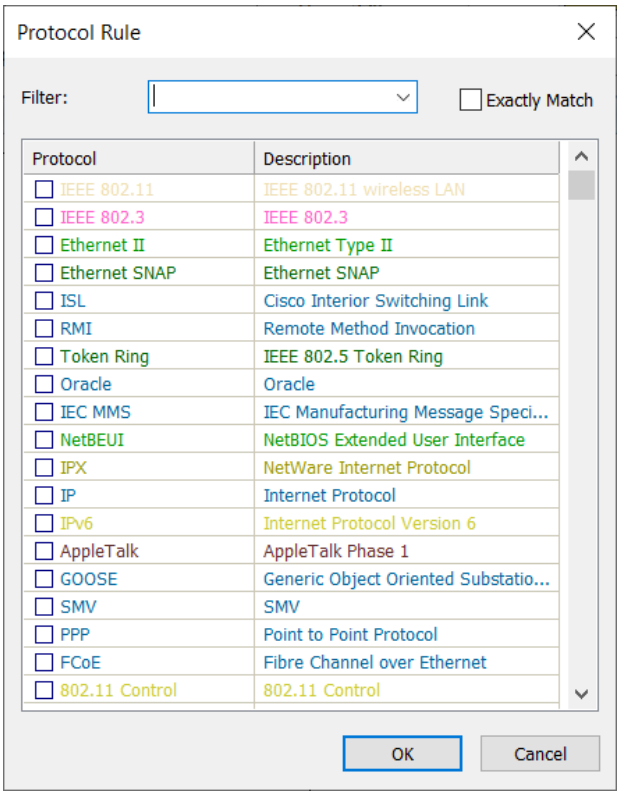
  - MAC address, MAC address pair: filters conversations according to MAC addresses.
  - IP address, IP address pair: fits for IP conversations, TCP conversations, and UDP conversations.
  - IP address, IP address pair: for the TCP conversation and the UDP conversation, Capsa can filter conversations according to the IP address port/IP address port pair; but for IP conversation, Capsa filters according to the IP address/IP address port.
  - Port, port pair: only works for the TCP conversation and the UDP conversation.

- **Location**

  Only the IP conversation can be filtered by locations. This feature does not apply to MAC conversations.



- **Conversation Protocol**
  After selecting one or multiple protocols, Capsa will filter conversations according to the protocol.



- **Conversation Packet**

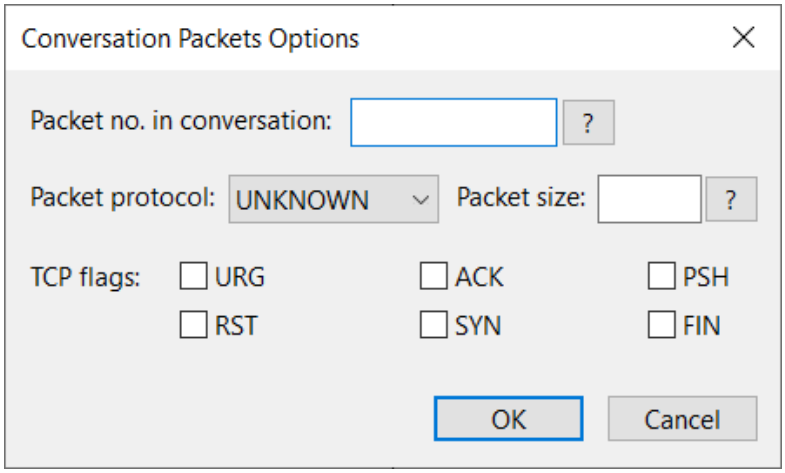
  Packet no. in conversation: set the sequence number of the packet in a conversation.

  Packet protocol: select a packet protocol.

  Packet size: set the size for this packet.

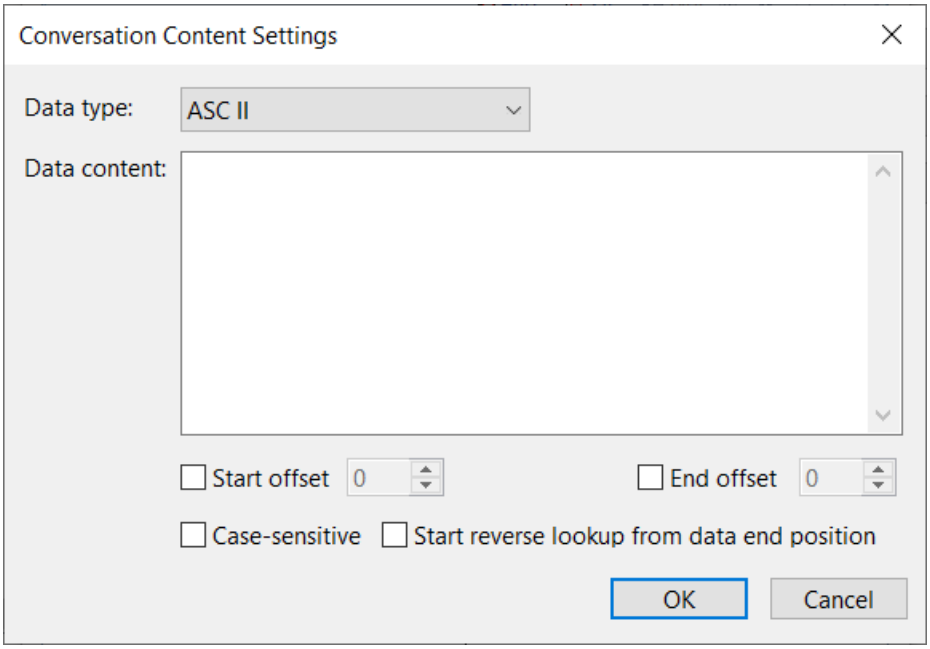
  TCP flags: select the TCP flag for this packet. This setting only applies to TCP conversations.

  Note The option Packet no. in conversation is required.

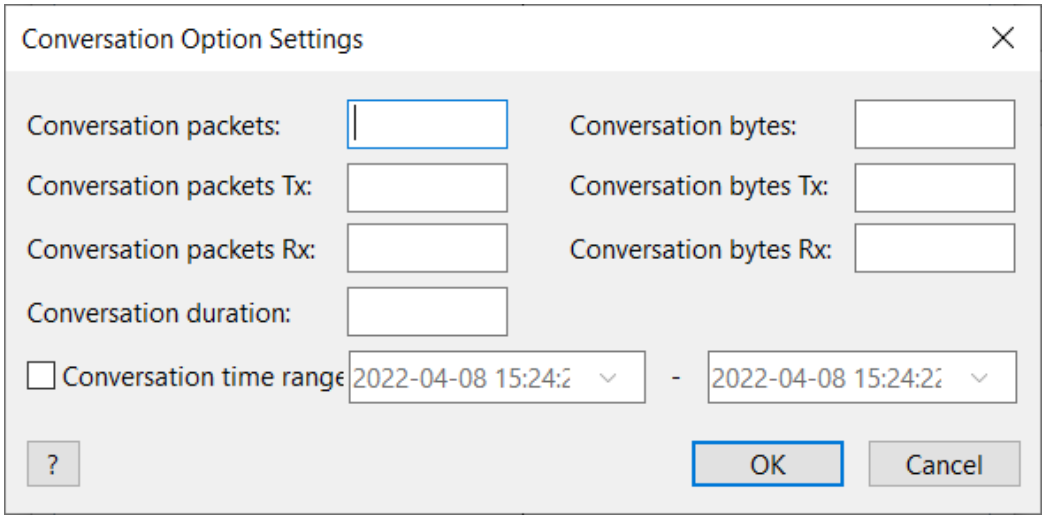


- **Conversation Content**

  Capsa supports to filter conversations according to the conversation content. When configuring the data content, you can select a data type, such as: ASCII, HEX, UTF-8, UTF-16. You can also set the start/end offset and case-sensitive.



- **Conversation Option**
  Capsa supports filtering conversations according to the key property.
  - Conversation packets: the total packets count of this conversation.
  - Conversation bytes: the total bytes of this conversation.
  - Conversation bytes Tx: sent bytes in this conversation.
  - Conversation bytes Rx: received bytes in this conversation.
  - Conversation packets Tx: sent packets count of this conversation.
  - Conversation packets Rx: received packets count of this conversation.
  - Conversation duration: for how long the conversation lasts.
  - Conversation time range: the time range for the conversation.



Start the filter

After configuring a filter, you can choose to accept it or reject it.

- Accept: Only show conversations that meet the filter requirement.
- Reject: Do not show conversations that meet the filter requirement.

Import/Export

You can click "Export" button to save the filter configuration as ".csconvflt" to the local disk. You can also click "Import" button to import ".csconvflt" files from the local disk to the Capsa, as a quick configuration for the filter.

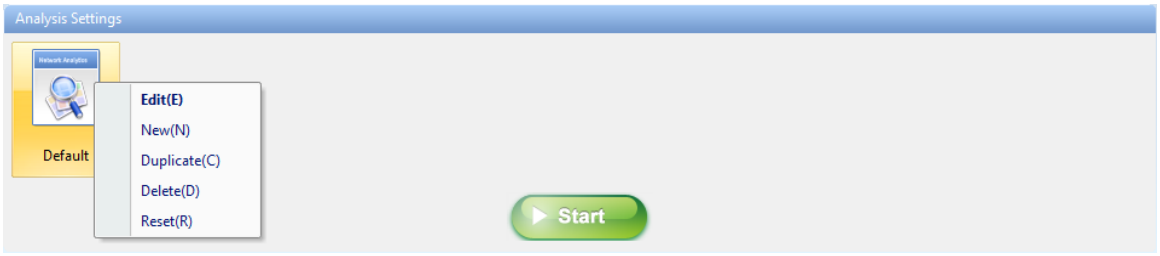
- Alarm Settings
- Alarm
- Security Analysis

About Analysis Settings

Analysis Settings section on the *Start Page* contains the settings for an analysis project, to provide flexible, extensible and effective analysis performance. On **Analysis Settings**, you can configure the settings about node group, name table, alarms, analysis modules, analysis objects and so on. All settings are memorized by the program when the program or even the operating system is shut down, and can be applied to other analysis projects.

Different analysis settings are set for different objects. On **Analysis Settings**, there are analysis settings named **Default**, which provides comprehensive analysis of all the applications and network problems.

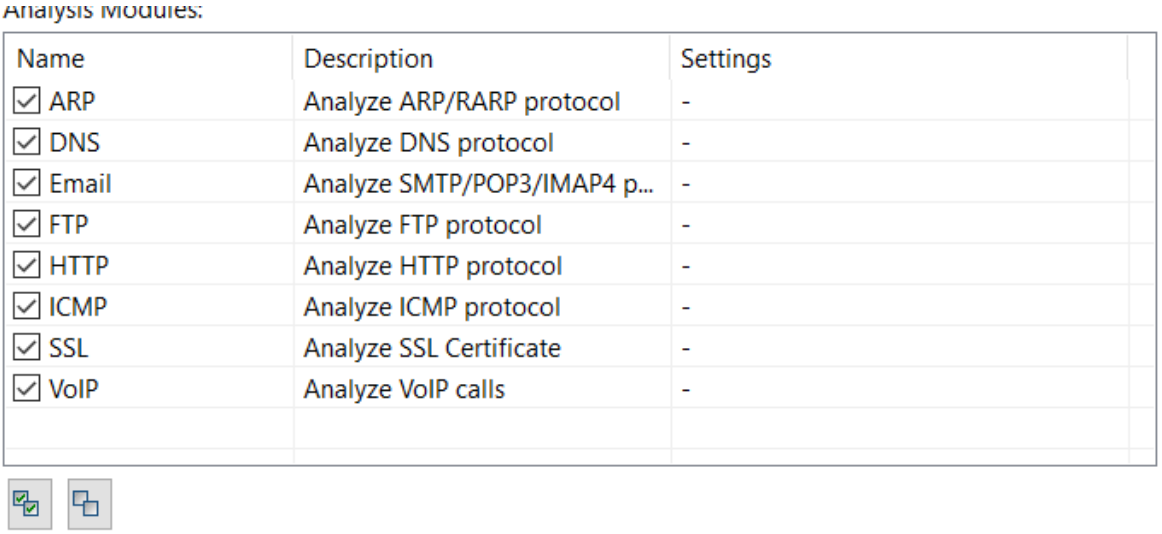
You can also create, edit, duplicate, and delete analysis settings by right-clicking anywhere on **Analysis Settings** section:



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

Add new analysis settings

For example, for adding HTTP Analysis Settings, you need check the **DNS** module and the **HTTP** module on **Analysis Modules** section.

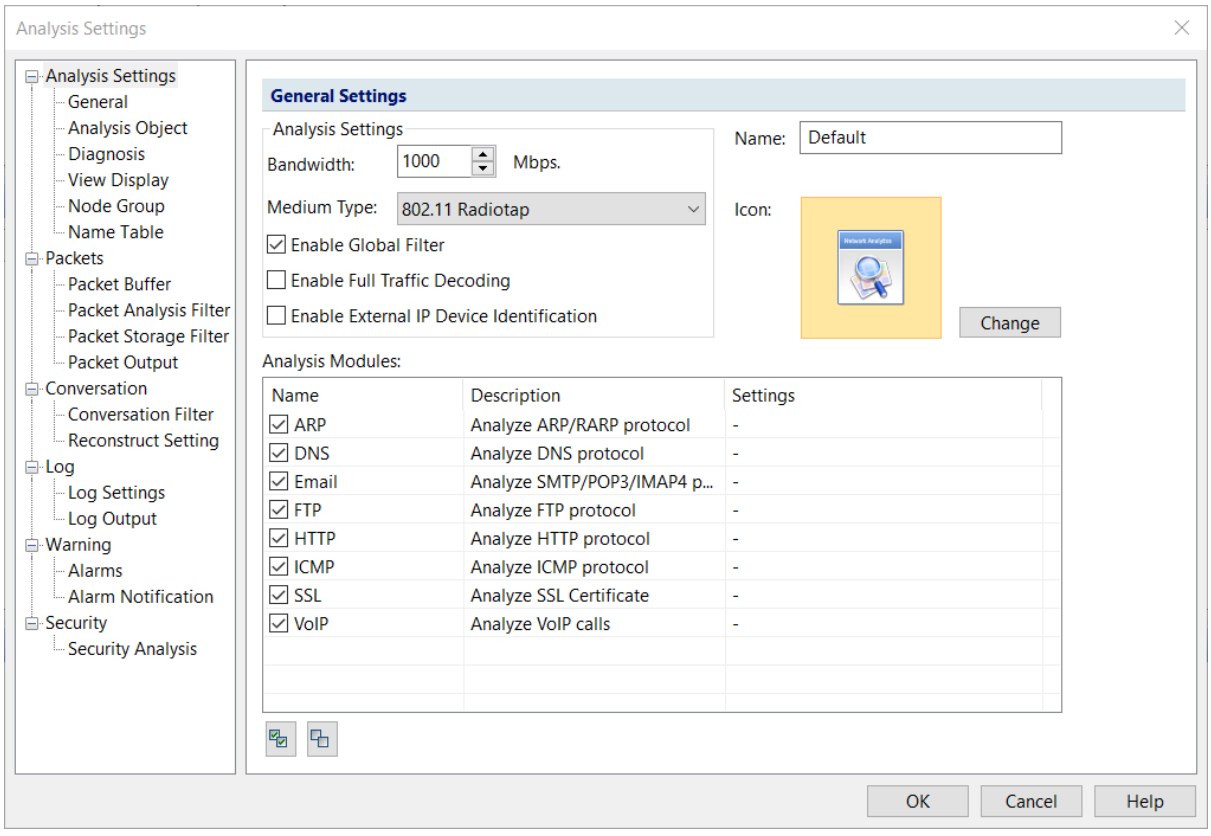


As for adding other settings, there are some configurations for reference.

Name	Description	Modules Needed
Traffic Monitor	Provides traffic statistics and high efficient analysis of main objects, including MAC.	DNS

Security Analysis	Provides dedicated analysis of potential network security risk.	ARP, DNS, Email, FTP, HTTP, ICMP
HTTP Analysis	Analyzes Web applications (based on HTTP) and record clients' web activities and web communication logs.	DNS, HTTP
Email Analysis	Analyzes Email applications (based on POP3 and SMTP) and monitor Email content and attachments and log Email transactions.	DNS, Email
DNS Analysis	Analyzes DNS applications, diagnose DNS applications errors and record DNS application logs.	DNS
FTP Analysis	Analyzes FTP applications (based on TCP port 21 and 20) and FTP transaction logs.	DNS, FTP
VoIP Analysis	Provides analysis and troubleshooting for VoIP calls.	ARP, DNS, ICMP, VoIP
Process Analysis	Provides network traffic analysis and statistics for all local processes.	ARP, NDS, Email, FTP, HTTP, ICMP

General



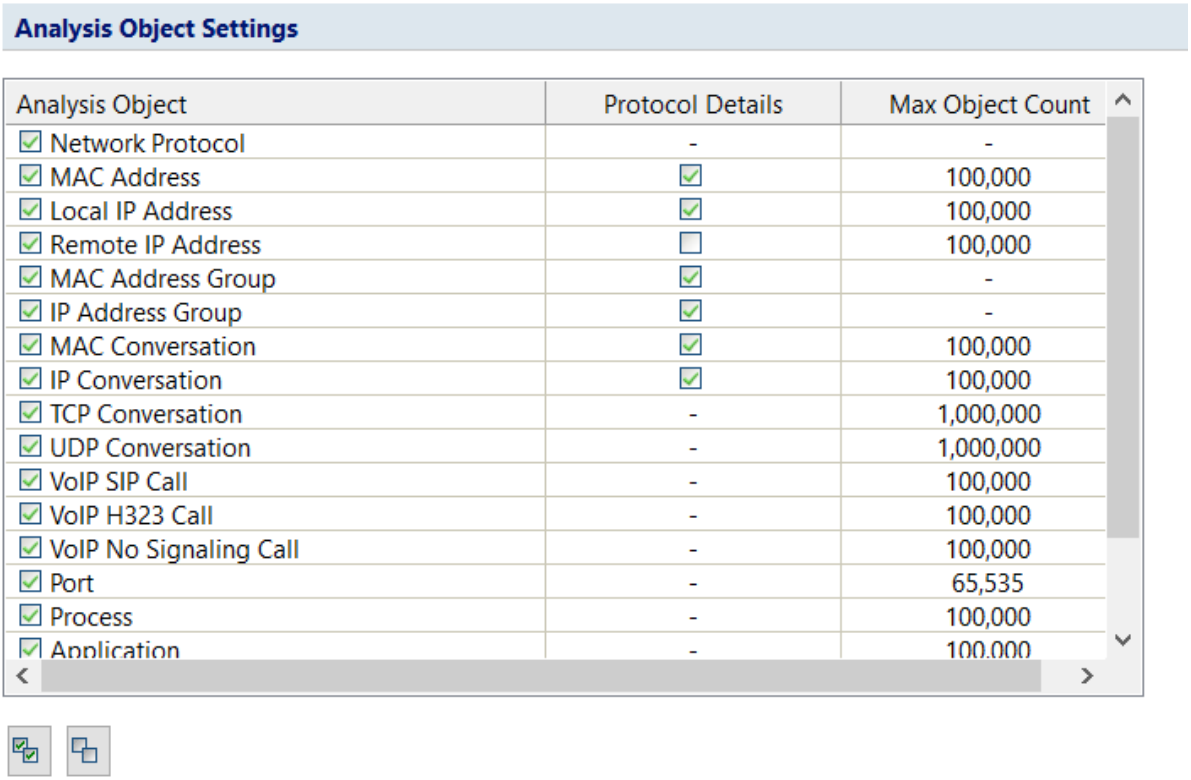
The analysis setting is composed of multiple different analysis modules, and different analysis modules analyze different objects. Users can customize the analysis settings according needs.

The general settings can be configured before starting analysis. When the analysis is going, the settings will not be available.

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.

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, MAC Address, Local IP Address, Remote IP Address, MAC Group, IP Group, MAC 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 in **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 in **MAC Explorer** is selected, and the **MAC Endpoint** tab on

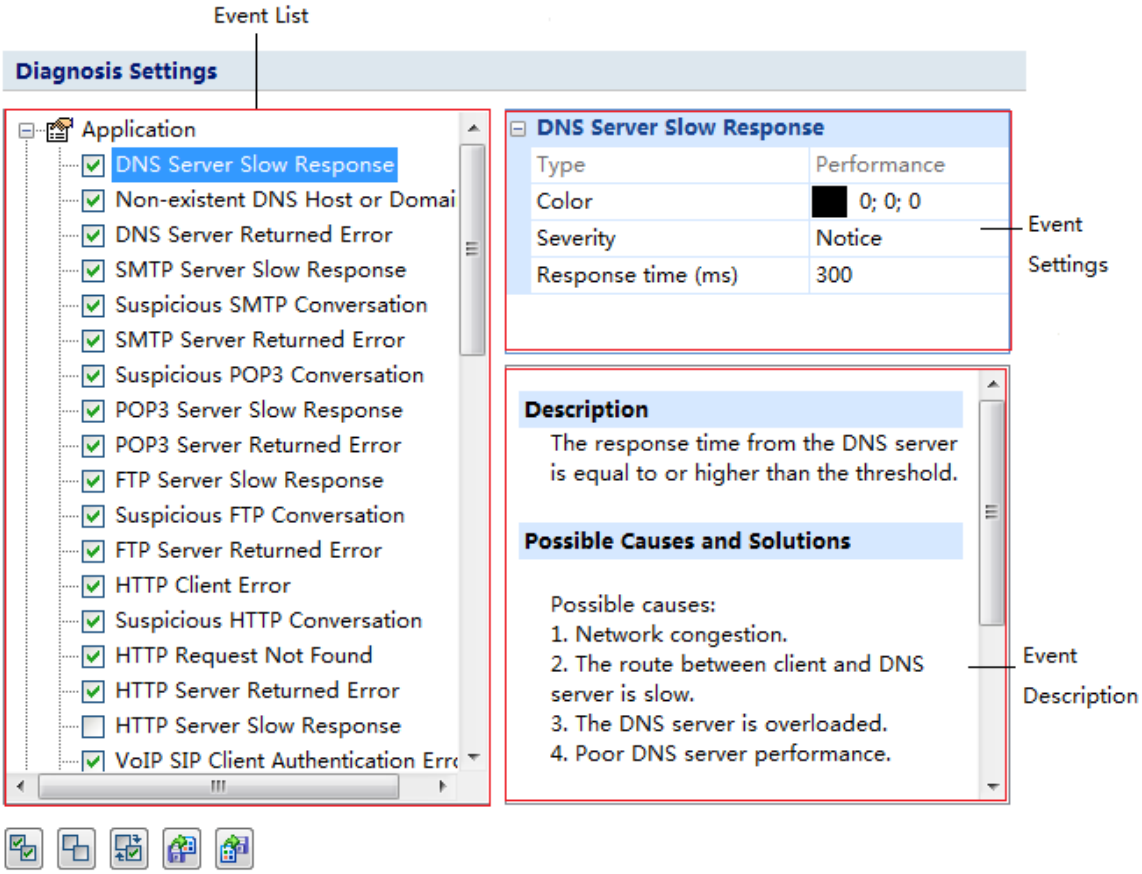
	the **Protocol** view will display the detailed traffic information of a single MAC address; or else, said information will not be available.
Local IP Address	The column **Protocol Details** is selected, the **Protocol** view will display detailed protocol statistics information when a specific local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

- **Max Object Count**: The maximum analysis object count for each analysis object. 10,000 is set by default. You can click the number to set it. The value for the number is from 1 to 10,0000.

Reset: Resets the settings on this tab.

Diagnosis

This tab lists all available diagnosis events of the loaded analysis module of the current analysis project. All diagnosis events are hierarchically grouped in the protocol layer. Therefore, you can easily know which layer a network problem belongs to. The **Diagnosis** tab appears as follows:



This tab includes three sections.

- **Event List**: Lists all available diagnosis events of current analysis settings. 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 troubleshoot the network when there are network problems.

The following list describes the buttons on the bottom of this tab.

 : Selects all the diagnosis events in the list.

 : Clears the selection on all the diagnosis events in the list.

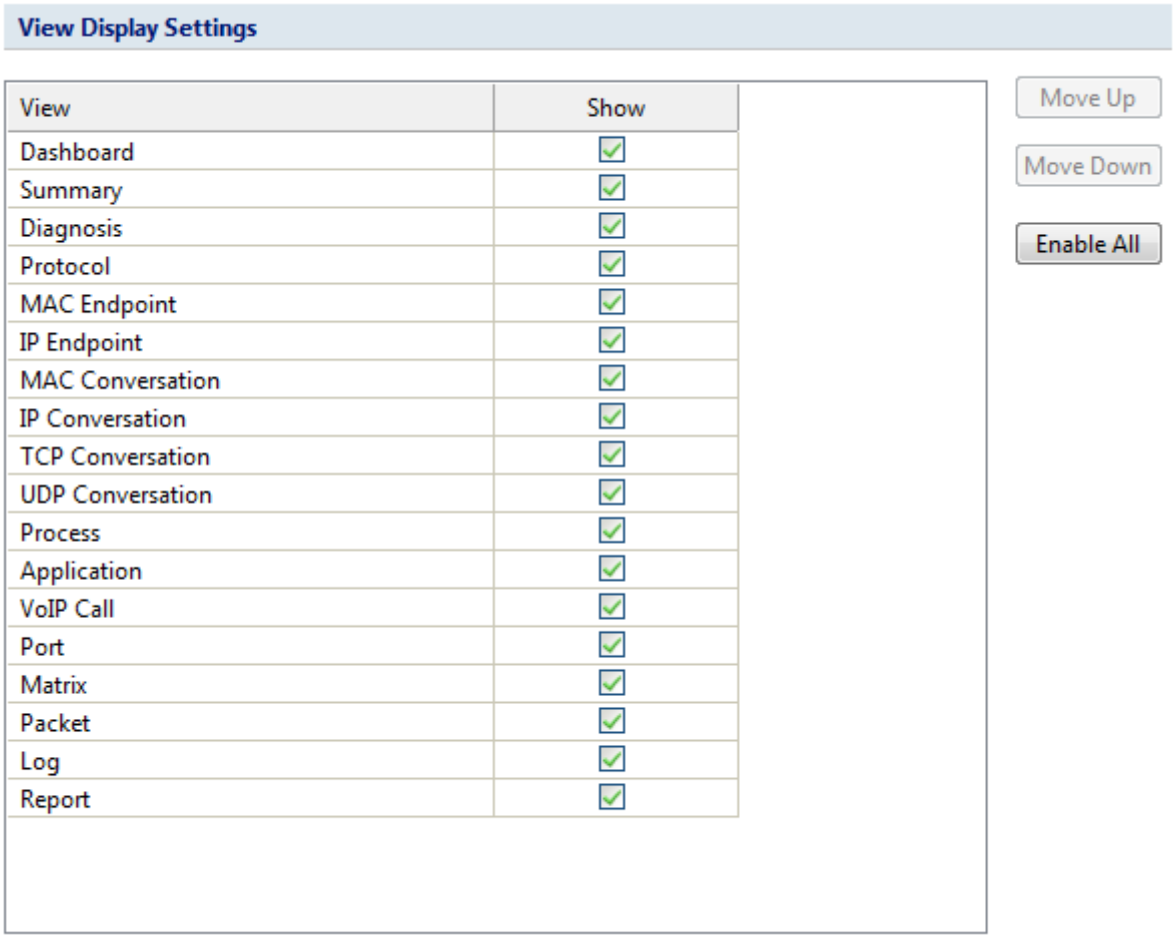
 : Inverts the selection on the diagnosis events in the list.

 : 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.

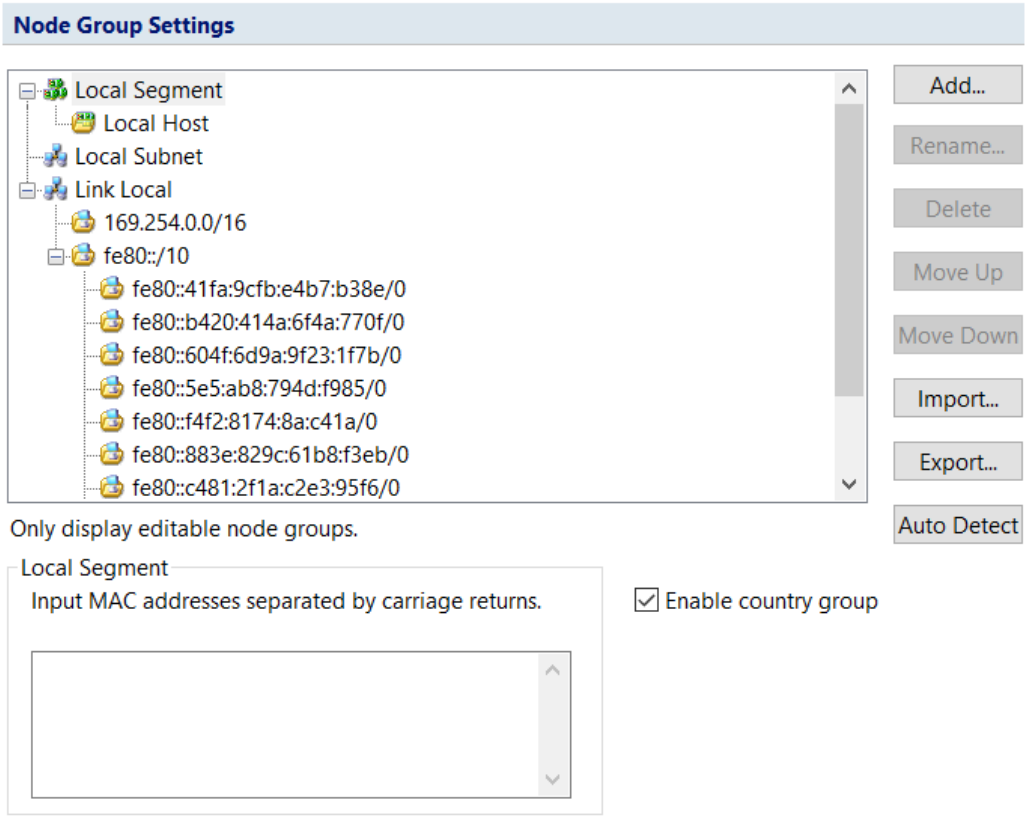
To rearrange the display order of the statistical views, click **Move Up** or **Move Down**.

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.
- **Rename**: 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 .cscng file.
- **Export**: Exports current node group list as .cscng 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

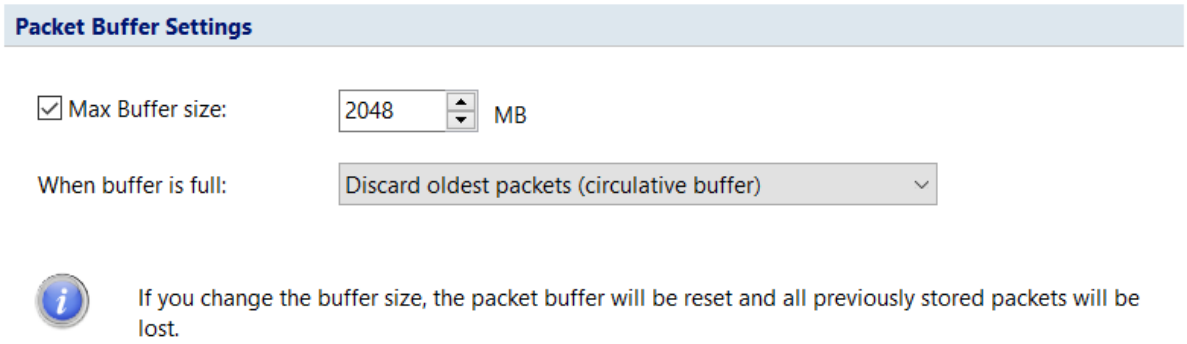
automatically generated node groups which are detected through the network adapter. You can also get the same result by clicking **Auto Detect**.

- 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.

Packet 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

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:

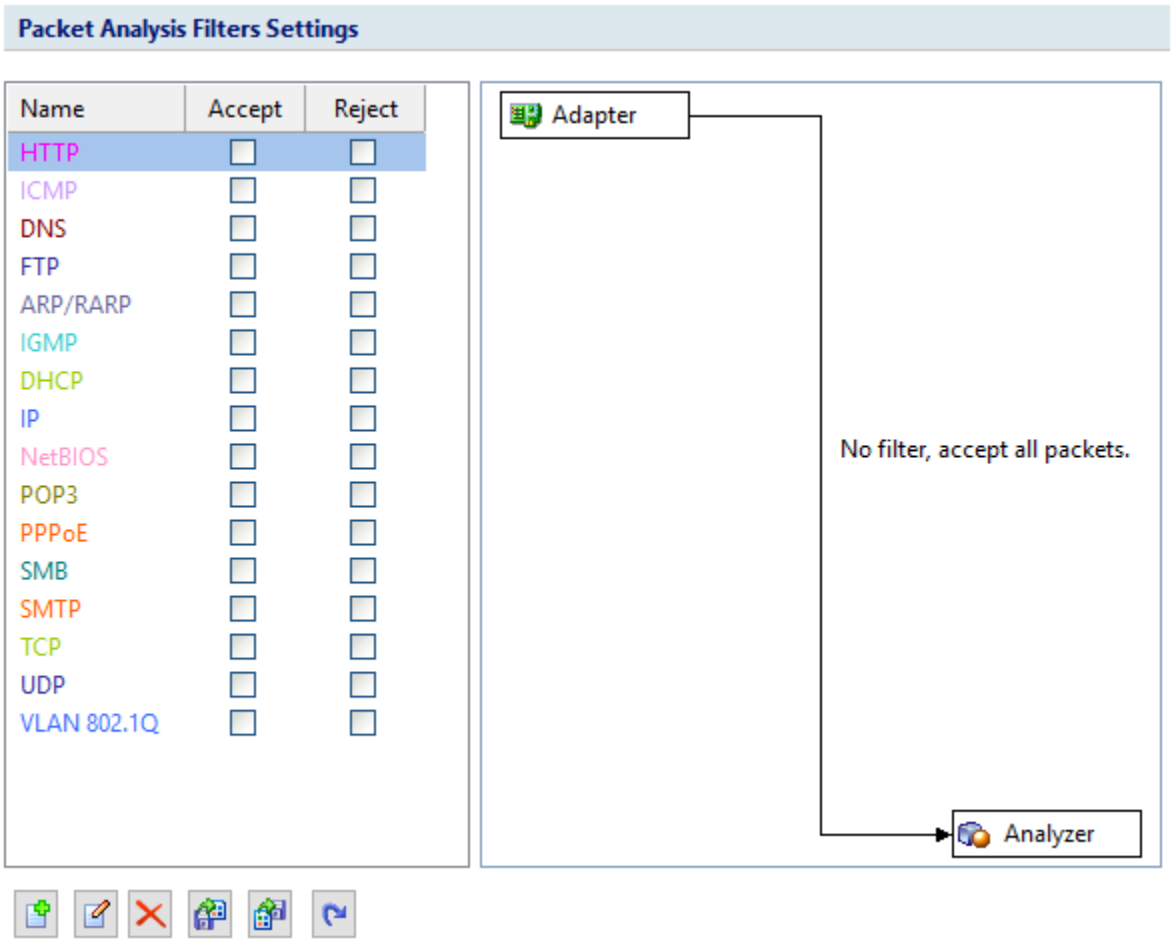
- **Discard oldest packets (circulative buffer)**
  It is recommended to discard the oldest packets to store the latest packets.
- **Discard new packets after analyzing**
  All new captured packets will be discarded after being analyzed and will not be saved to the packet buffer.
- **Discard all old 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 Analysis Filter

This tab is for containing, setting up, and applying capture filters. Capture 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.

Without DPI, this tab 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.

To create a capture filter,

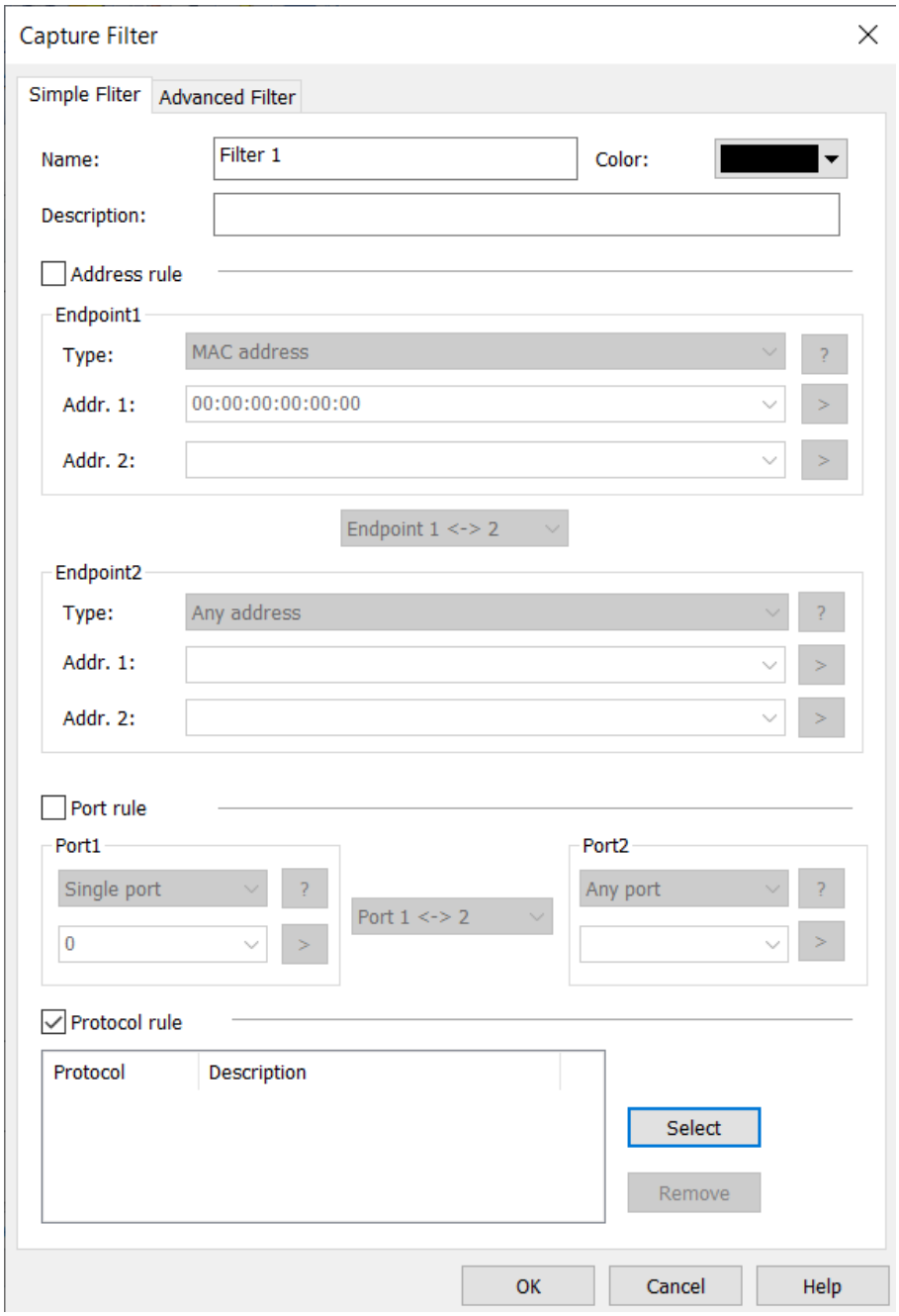
1. On the Capture Filter tab of the Analysis Settings dialog box, click  to open the **Packet Filter** dialog box.
2. Select a simple filter or an advanced filter and set the filter, including the filter name, filter description, and filter rules (see Creating Simple Filter and Creating Advanced Filter for details).
3. Click **OK** on the **Packet Filter** dialog box, and click **OK** on the **Packet Filter Settings** dialog box.

Note After creating a filter, you should select the **Accept** or **Reject** checkbox to make the filter take effect.

During a capture, you can still create a capture filter based on the selected object.

Creating Simple Filter

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 of them.

In order to capture packets precisely, you can specify packet transmission direction (for example Endpoint 1 -> 2, Endpoint 2 -> 1 and Endpoint 1 <-> 2) in 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 filter in **Advanced Filter** tab.

Defining address rule

To set an address rule, follow the steps below:

1. Select the **Address rule** checkbox.
2. Select a **Type** for **Addr.1** and **Addr.2** in **Endpoint 1** and **Endpoint 2**. You can select MAC address, IP address, IP range or IP subnet. Only when you choose IP range, **Addr.2** is available.
3. Input the addresses for **Addr.1** and **Addr.2** in **Endpoint 1** and **Endpoint 2**.
4. Click the direction drop-down list box and select packet transmission direction between **Endpoint 1** and **Endpoint 2**.
5. Click **OK** on the **Capture 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.

Tips If you have multiple addresses to set up, you can go to **Advanced Filter** tab, where batch is supported.

Defining port rule

To set a port rule, follow the steps below:

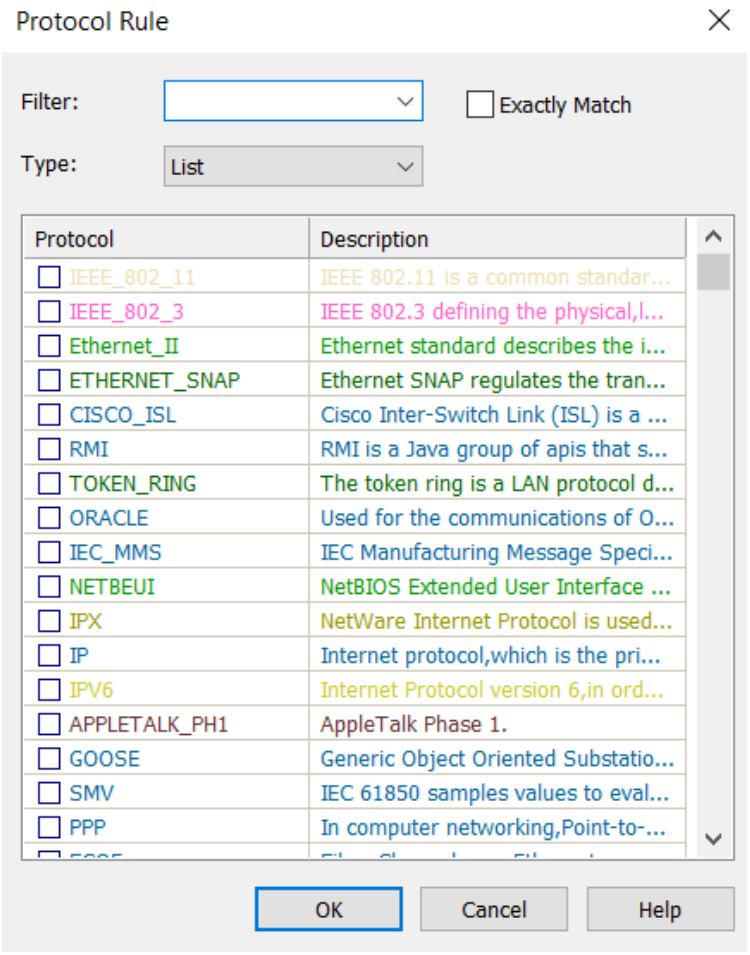
1. Select the **Port Rule** checkbox.
2. Select a port type from **Port 1**. You can select single port, port range or multiple port.
3. Click the text box below the port type and type the port number.
4. Click the direction drop-down list box and select packet transmission direction between the two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

Tips If you have multiple ports to set up, you can go to **Advanced Filter** tab, where batch is supported.

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**. You can type the protocol name in the Filter box to display-filter the protocol.
4. Click **OK** on the **Packet Filter** dialog box.

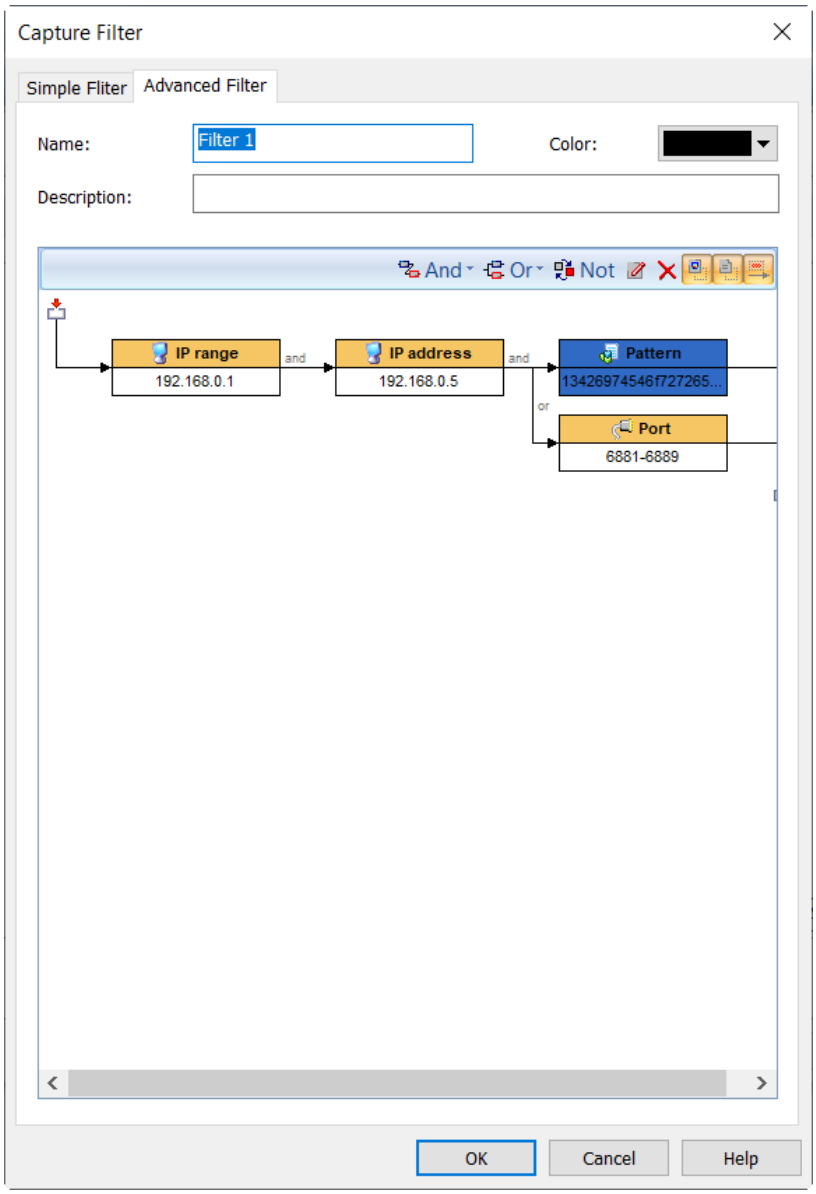
The chosen protocols are listed in **Protocol Rule** section. You can delete a protocol item from the list with the **Remove** button.

Defining conversation filter

Conversation filter can filter captured packets at conversation-level, only the packets which meet the filter condition will be displayed in the statistics view. Conversation filter is based on protocol filter, so users must select the **Protocol Rule** box, and select the **Only for Conversation** box at the same time when setting conversation filter.

Creating Advanced Filter

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.

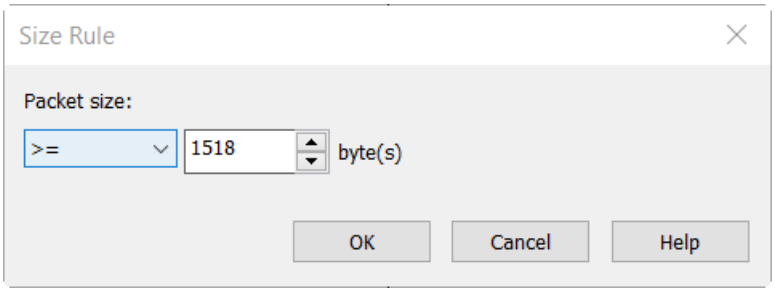
- : Deletes the selected rule.
- : Shows the icon for each rule.
- : Shows the details of the rules.
- : Shows the logical relationships of the rules.

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 Creating Simple Filter 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.

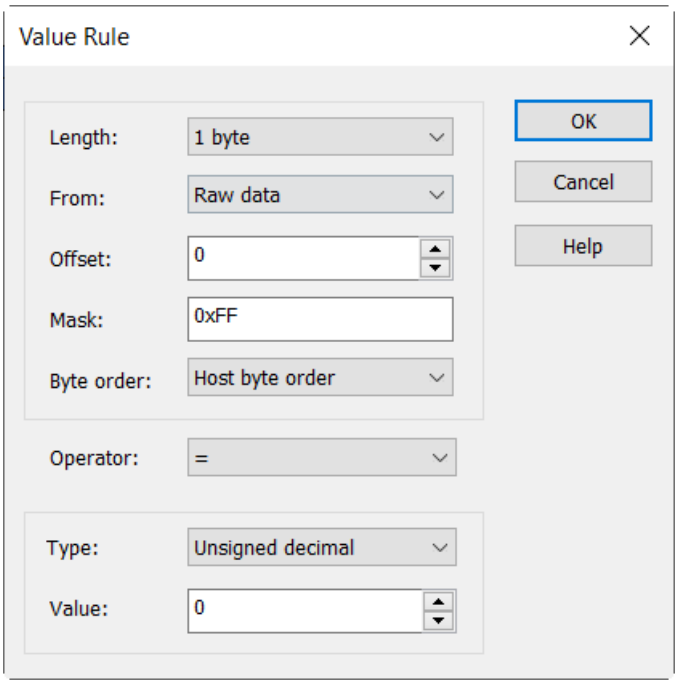


You can choose < (less than), <= (less than or equal to), > (greater than), >= (greater than or equal to), = (equal to), != (not equal to), Between (size range) to define the size rule.

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.



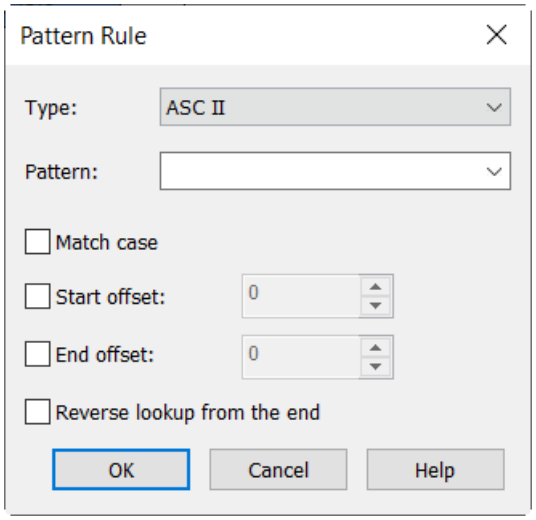
- Length: Specifies the length of the mask, and the length of the value for the rule. It could be 1 byte, 2 bytes and 4 bytes.
- From: Specifies where to offset in a packet. It could be Raw data, IP Header, ARP Header, TCP Header, and UDP Header.
- Offset: Specifies the bytes to be offset. The unit is 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**.

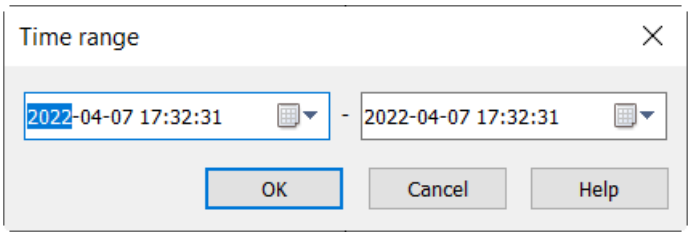


The unit for offset is byte.

Defining time range

Time range is for filtering the packets in a certain time range.

To define a Time range, click **And** or **Or** on the toolbar, select **Time** to open the **Time range** dialog box which appears as below, select the start time and the end time, and click **OK**.



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.

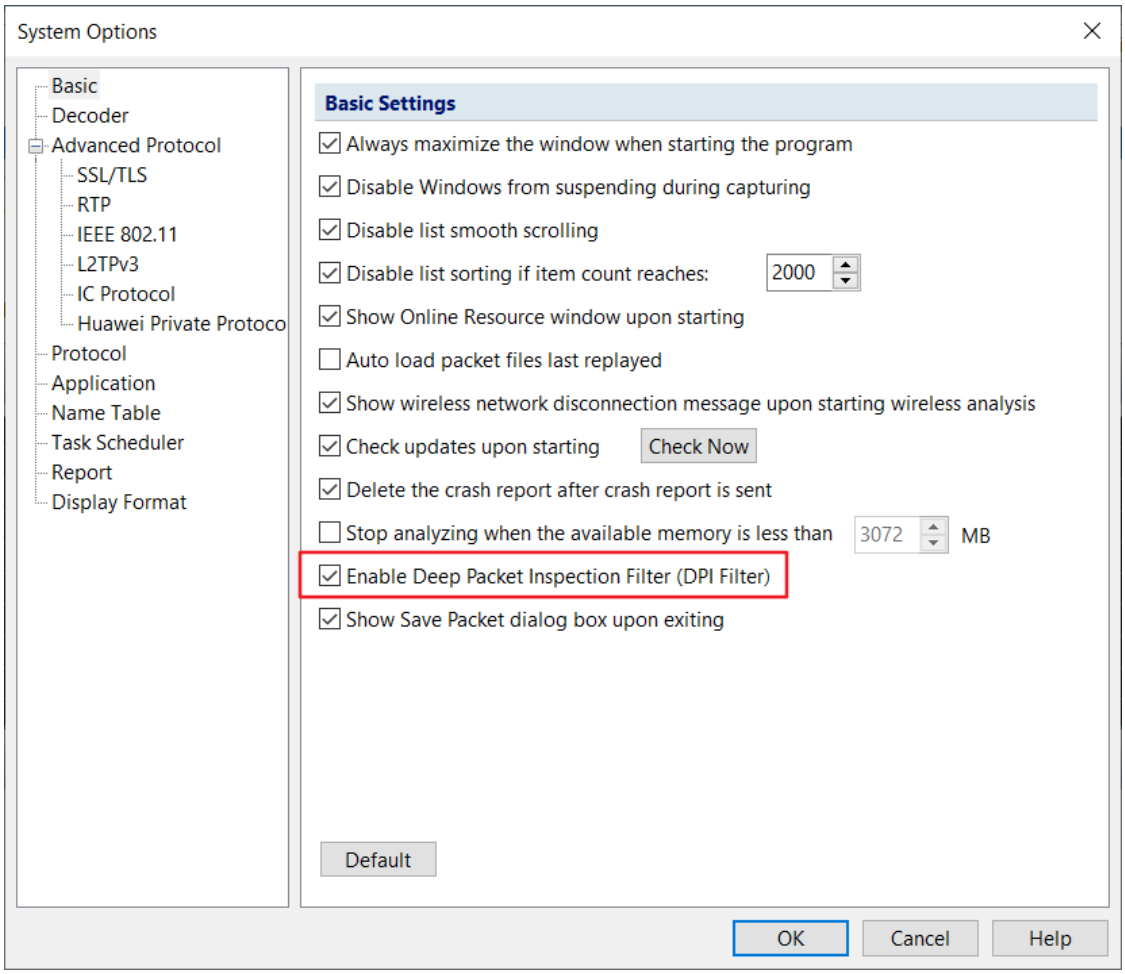
DPI Filters

Filter settings are the important method for you to change the scope of captured data. If no filters are set, the system will capture and analyze all packets.

By setting up filters, we can capture only the specific packets, separate important data, and filter out unnecessary data. In this way, you can focus on only the data information of network failure or network attack, instead of looking for it in a large amount of data, reducing the trouble and complexity of finding data in a large amount of data. Colasoft Network Analysis System also provides you with a default list of protocol filters, where you can easily customize filters and manage all

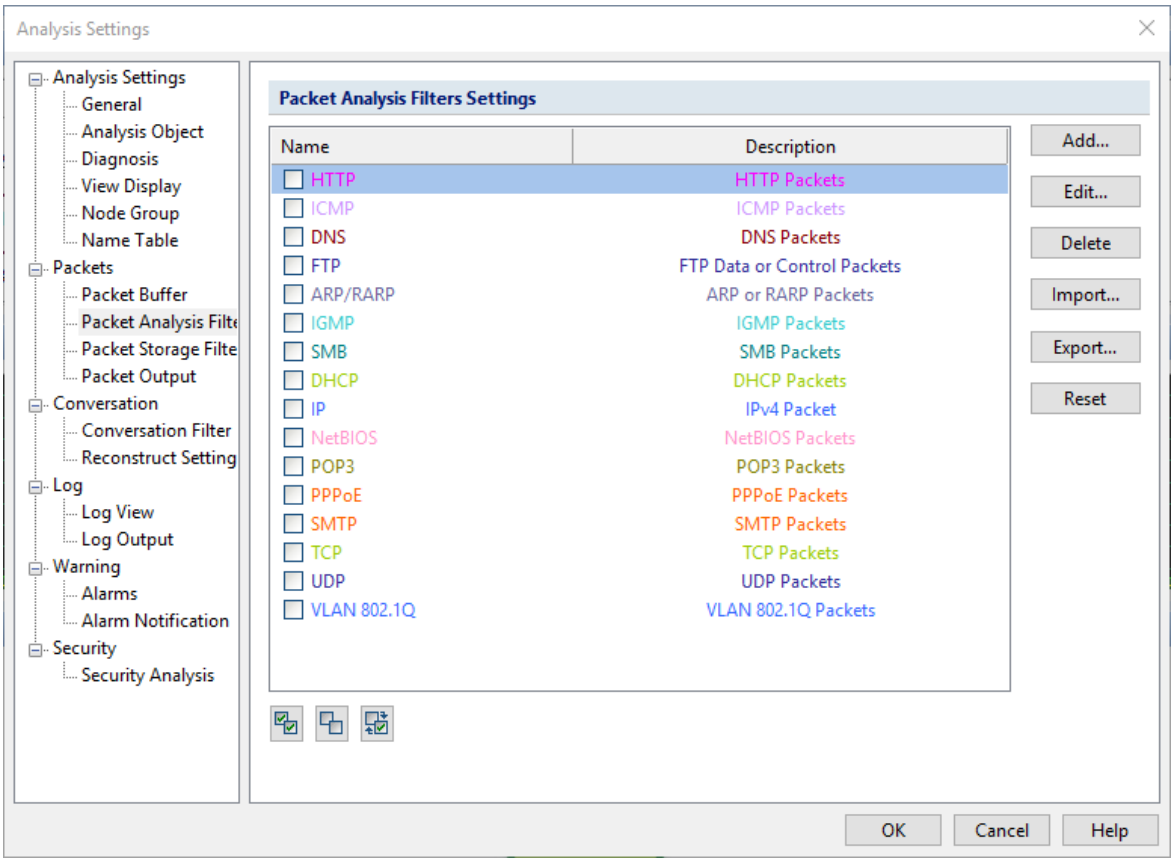
filters. In DPI filters, you can input the filter expression to filter packets, so that the results will be more precise.

To enable the DPI Filter, check the option **Enable Deep Packet Inspection Filter (DPI Filter)** on System Options.



In addition to setting the filter in the analysis plan, you can also click the filter icon in the system ribbon to enter the filter settings dialog box, as shown below:

The filter settings interface is shown below.



Filter List

The filter condition in the filter list are all filters that you customize. You can check the filter by checking the corresponding filter. The relationship between different filters exists in logic OR. You can also select multiple filters to combine and customize the capture range of the packets you need. Double click any filter to enter the filter editing interface. You can set the filter condition as you want to add or delete in "DPI Filter Setting", then separate the packets by writing expression conditions.

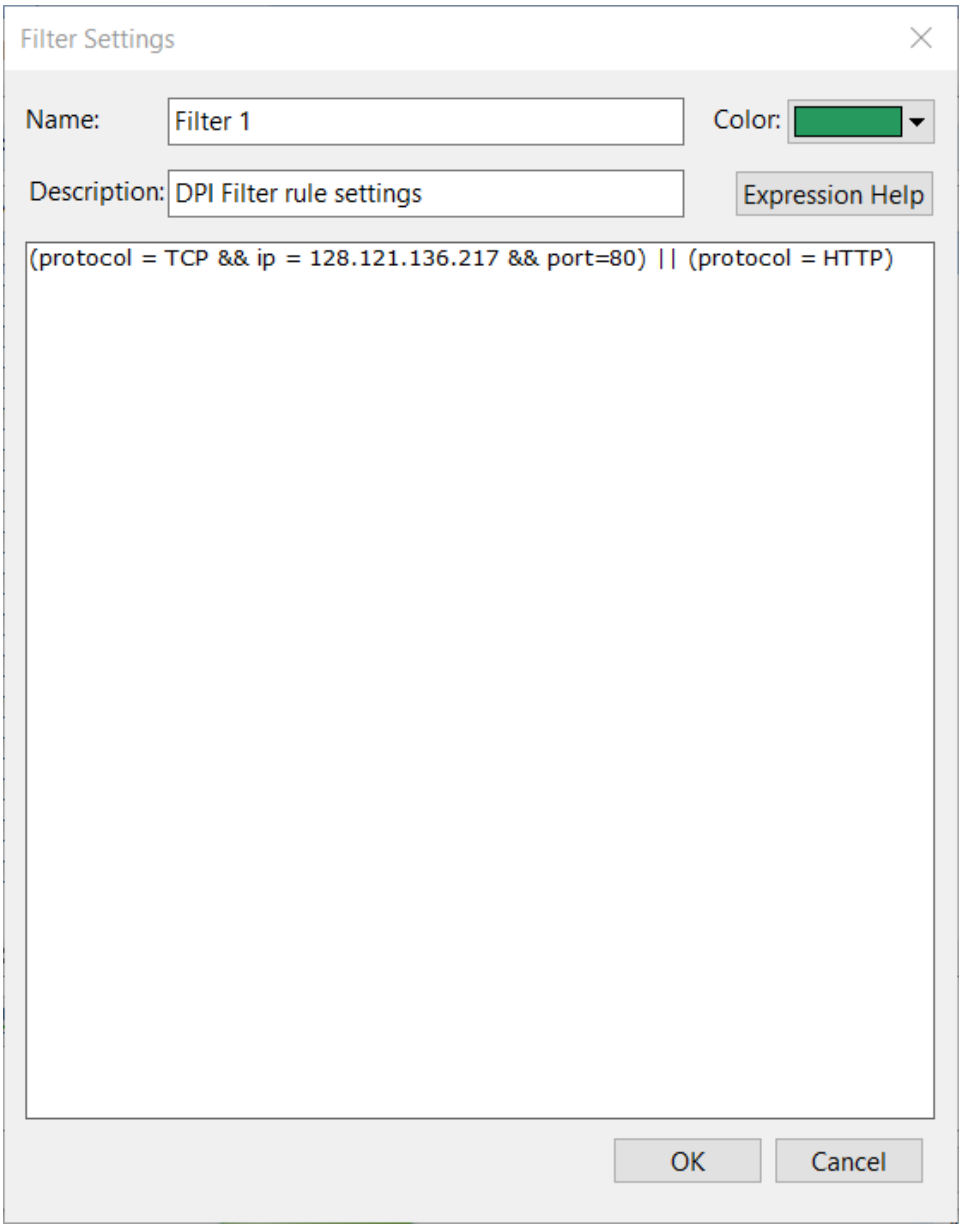
Tips When you create a new filter, the system automatically saves the newly created filter to the filter list. Next time when you reboot the system, you can easily call the previously set filter.

Note The small toolbar on the bottom  , can help you manage the filter list conveniently. The specific functions are: enabled all, disabled all, and reversed.

Note Dpi filter suitable range: Dpi filter is only suitable for 64-bit operating system currently and supports AVX instruction sets. In addition, use the old version of "Filter" to configure the filtering conditions.

DPI Filter Settings

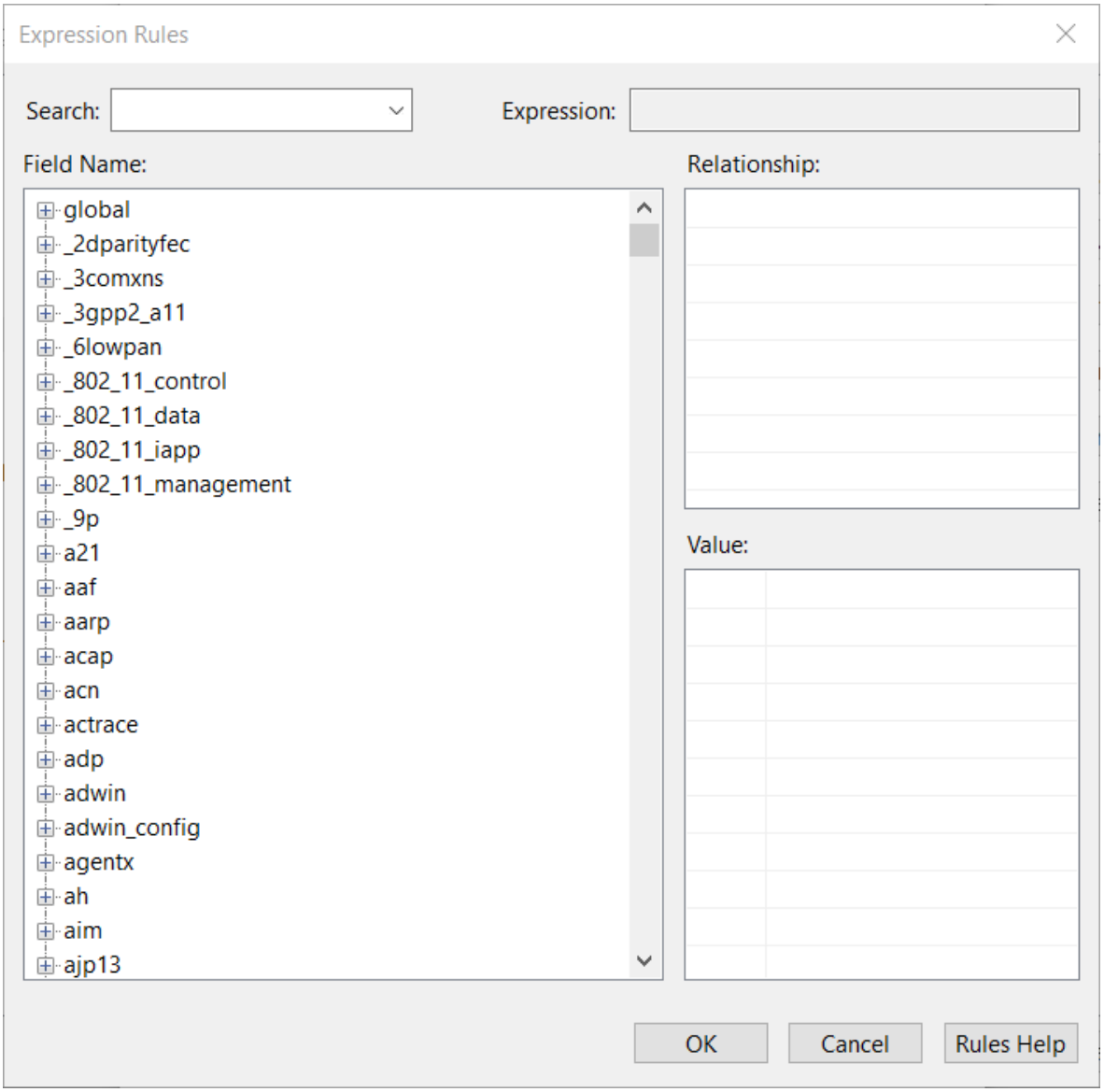
DPI Filter can use expressions to show your filter condition. The interface for DPI Filter settings is shown in the following figure:



Tips Expressions are composed of field names, operators, values, and logical operators. For a detailed description of the expression, please refer to "Help For Expressions".

DPI Filter Help

The help for expression interface lists all currently supported protocols and fields, the operators corresponding to the fields, the value types of the fields, and the writing way for some specific field values. The expression help interface is shown below:

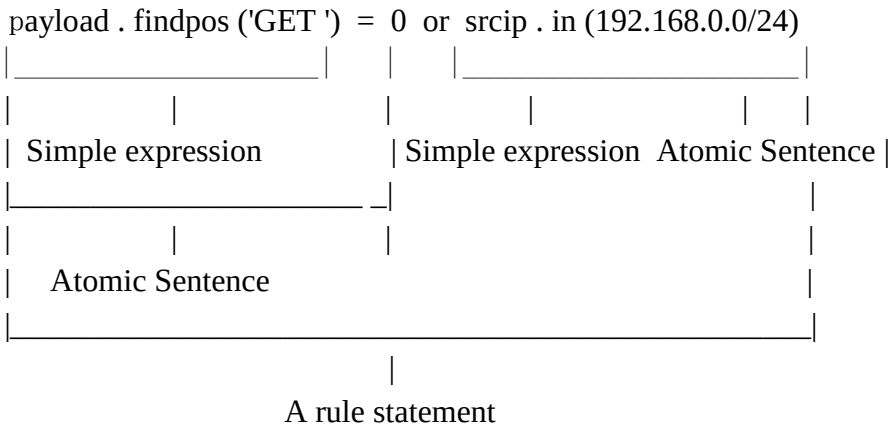


Note If you want to know a certain field, you can search this field with full field name. Or by expanding the tree structure in the field tree, the field-supported operators, type, value will be displayed on the right.

Description of Expression Rule

Rules and Rules Group

3. DPI filtering rules consist of logical expressions; each logical statement consists of a simple expression. For example:



4. A rule group consists of multiple rule statements.

The following rules are composed of 3 rules, here is the ID = 0, 1, 2(There is logical OR between each one of them):

payloadlength <= 30 && payload[0,6].find('https:')

!(payload[3,20].find(HEX'00 00 00 0A 00 00 00 00')) || dstport >=1000

payload[0,4] = HEX'03 00 00 00' and (payload.find(HEX'10 00 00 0C 0A 83 86 7C') or packetlength <= 2000)

Representation Rules of Types

6. Representation Rules of String Type

String	Rules
Single quotes”	Escape characters is not supported. Sets: All ASC|| characters except single quotes”.
Hexadecimal String	Add HEX prefix in front of single quotes, for example:HEX’00 0A’

7. Representation Rules of DateTime Type

DateTime has two longitude types: DTSec and DTNanoSec. Leap second is supported, e.g.: DT'2019-01-01 07:59:60+0800'.

Format	Notes
DT 'year month mday hour min sec'	Second level DT type without time zone, local-host time zone.
DT 'year month mday hour min sec .nanosec'	Nanosecond level DT type without time zone, local-host time zone.
DT 'year month mday hour min sec ±timezone'	Second level DT type with time-zone.
DT 'year month mday hour min sec .nanosec ±timezone'	Nanosecond level DT type with time-zone.

The following constraints should be complied:

- Literal value must contain DT 'and ';

- year Year, consisting of four consecutive numeric characters, the number cannot be less than 1970.
- month Month, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [01,12];
- mday day of the month, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [01, 31];
- hour Hour, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 23];
- min Minute, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 59];
- sec Second, consisting of 2 consecutive numeric characters, if the number is less than double digit must be padded by zero, the reasonable range is [00, 60], support leap second.
- nanosec Nanosecond, consisting of 9 consecutive numeric characters, if the number is less than night digits must be padded by zero; It must use the profix '.', And no other characters can be mixed between the nanosecond and the prefix. The presence or absence of nanoseconds is a unique identifier for determining the accuracy of a DT type: No nanosecond is of the DTSec type; there are nanoseconds of the DTNanoSec type;
- timezone Time zone correction, time difference from GMT/UTC, consisting of 4 consecutive numbers of characters, the first two digits stand for hour and two digits after is minute. Less than four digits must be padded by zero; it must appear with the prefix + or - and must not be mixed with any other characters, + means earlier than UTC, - means later than UTC
- Other

  1. DT Literal value will ignore all white space characters such as ' ', '\t','\n' etc.
  2. year, month, mday Only one valid non-white character can be used to divide year/mouth/mday.
  3. hour, min, sec Only one valid non-white character can be used to divide hour/min/sec.
  4. Valid non-white partitioning characters include (including but not limited to)!"#$%&* +,./:;@^_|~.

Examples of valid format:

Type	Example
Without time zone suffix: the default is the time zone of local time	DT'2019-09-26 11:02:59' DT'2019/09/26 11:02:59' DT'2019-09-26 11:02:59.981815000' DT'2019/09/26 11:02:59.981815000'
UTC	DT'2019-09-26 11:02:59+0000' DT'2019/09/26 11:02:59+0000' DT'2019-09-26 11:02:59.981815000+0000' DT'2019/09/26 11:02:59.981815000+0000'
Chinese Standard Time CST	DT'2019-09-26 11:02:59+0800' DT'2019/09/26 11:02:59+0800' DT'2019-09-26 11:02:59.981815000+0800' DT'2019/09/26 11:02:59.981815000+0800'
Pacific Standard Time PST	DT'2019-09-26 11:02:59-0800' DT'2019/09/26 11:02:59-0800' DT'2019-09-26 11:02:59.981815000-0800' DT'2019/09/26 11:02:59.981815000-0800'

Other Valid Format	DT'20190926 11:02:59-0800' DT'20190926110259' DT'20190926110259+0800' DT'2019/09/26 110259-0800' DT'2019 09 26 11 02 59 +0800' DT'2019-09-26 110259-0800' DT'20190926110259.055000000+0800'

8. Representation Rules of Regular Expression Type

Regular expressions are only used in the find () function. The regular expression syntax consists of two parts: pattern and modifiers. Writing format: /pattern/modifiers; modifiers can be used by default.

Pattern: Perl/POSIX style regular expressions.

Single slash '\' in pattern means character escaping.
When \ and / as special character exist in pattern, they need to be escaped into: \\ and \/

modifiers: Matching method (pattern modifiers)

One modifiers consists of zero or multiple modifiers: I, m, s, V
Related function is not enable until the specific modifiers is configured.
modifiers can be superimposed.
Multiple modifiers must be connected, no other characters can be mixed in between. For example, there is a space between modifiers in /abc/i m, which is the wrong writing style.

Description of modifiers

Modifier	Paraphrase
i	Case insensitive
m	^ can match the beginning of a line; $ can match the end of a line Note: The first byte of the payload is not at the beginning of the line.
s	. can match any character, including newlines.
v	Allow empty strings, such as (a|).

Note Regular expression rules are not fully supported. Some advanced usages are shown below:

Advanced	Support or not	Example
(?:pattern)	Support	/(?:45|56)123/

Zero-width assertions	Support	Zero width assertion: /(?!abc)def/
Back-references	Not support	nChronos reference:/.*?<\/[hH]\1/s
Conditional references	Not support.	/(?(1)foo|bar)/

9. Int Integer type, sets: 8 bytes signed integer
10. IP type. **Only supports IPv4 currently**. Use the String type to set IPv6 rules.

3) IPv4 literal-value writing supports dotted decimal and dotted hexadecimal, and their mixed style(wiki-IPv4). Decimal and hexadecimal IPs are also limitedly supported. Such as a valid IPv4 literal value:

Format	Value	Whether can be used to write IP range (segment/subnet)
Dotted Decimal	192.0.2.235	Support
Dotted Hexadecimal	0xC0.0x00.0x2.0xeB	Support
Mixed	192.0.0x2.235	Support
Hexadecimal	0xC00002EB	Not support
Decimal	3221226219	Not support

4) IP Range (Segment/Subnet)

IP Range (Segment/Subnet) represents a closed IP interval.

All Valid Format	Notes
192.168.1.0-192.168.1.255	IPv4 range, commonly used
192.168.1.0/24	IPv4 subnet, commonly used
192.168.0x01.0-192.168.1.255	
192.168.0x01.0-192.168.1.0xff	
192.168.0x01.0/24	
192.168.0x01.0/0x18	

Member function of types

String type member function

Function Name	Example	Description
find	payload.find('HTTP 1.')	The matching method of fixed feature string. If the feature string exists in parent string, the value of the expression is true; if not, then false.
find	payload.find(/ [hc]at<\/tag>/i)	The matching method of the regular expression version. Specially, payload[2, 10].find(/a[0-9]*c/) will

	search the whole packet for a[0-9]*c, only to guarantee the drop point of 'c' in [2,10] in payload, even if 'a' doesn't appear in payload.

Int type member function

Function Name	Example	Description
findpos	payload.findpos('ABC')	Returns the offset value in parent string payload to feature string 'ABC'. Offset value starts from zero. If this feature string does not exist in the parent string, the value of its logical expression is abnormal. The contrast value of findpos() should not be less than zero.
N2H16	payload.N2H16()	Returns the positive integer from network byte order converts to little-endian order of the first two bytes for payload.
N2H32	payload[30,100].N2H32()	Returns the positive integer from network byte order converts to little-endian order of the first four bytes for string.
N2H64	payload.N2H64()	Returns the positive integer from network byte order converts to little-endian order of the first eight bytes for string.

IP type number function

Function Name	Example	Description
in	srcip.in(192.168.1.0-192.168.1.30)	Judge the srcip belongs to a continuous IP range or not.
in	dstip.in(192.168.1.1/24)	Judge the dstip belongs to a IP subnet or not.

Operators (operators, modifiers, etc.)

No arithmetic operators like '+' or '-' are currently provided yet.

Type of Operators	Paraphrase
Relation	Relational operators

Logic	Logical Operators
Grouping	Grouping operators
Modifier	Modifiers

Priority: Grouping > Modifier > Relation > Logic

5. Relational Operators

Relation Operators	Paraphrase
=	Equal
<	Less than
>	Greater than
!=	Not equal to
>=	greater or equal to
<=	Less or equal to

6. Logical Operators

Relation Operators	Paraphrase	Priority	Direction
! not	NOT	High	From right to left.
&& and	AND	Medium	From right to left.
|| or	OR	Low	From right to left.

7. Grouping Operators

Grouping Operators	Paraphrase	Priority	Example
()	Group	Highest	such as:!(bool_expr1||bool_expr2);(bool_expr1||bool_expr2) && bool_expr3 etc.

8. Modifiers

Modifiers	Paraphrase	Description/Examples
()	Function call	find()
[a, b]	String endpoint modifiers. a, b is used to indicate the expected maximum endpoint, both of which are integer type.	Used for String expression to get a SubString. Endpoints is disable in SubString.
.	Member access	HTTP.url ; payload.find('str')
.	Used for literal value of IP type	192.168.0.1

''	String literal value modifiers	Empty literal-value String '' is not allowed, also escape is not allowed.
HEX''	Profix modifier for hexadecimal string, and only single quotes are supported. No other characters are allowed between HEX and the first single quote.	Both uppercase and lowercase letter can be used in single quotes, and letter in mixed case is allowed. Between byte and byte there must be separated by a white space characters. The width limit for each single byte is 2 bytes and it should be filled with zero (0) if the width is not enough. Allow multiple consecutive whitespace characters as a split.
/pattern/modifiers	Regular expression	Modifiers can be default; regular expressions are only available for find()

Additional notes for the boundary modifier [a, b]:

- a is for the expected left-endpoint, b is for the expected right-endpoint. [a, b] stands for an interval which is greater than or equal to a and less than b.
- Range: a, b ∈ { -2147483648, ..., -2, -1, 0, 1, 2, ..., 2147483647}
- a < b and a × b >= 0 is strictly true.
  There are only two cases, for example, as for the parent string 'helloworld':
  1) 0 <= a < b : | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10|
  |-----|----|----|----|----|----|----|----|----|----|----|
  | h | e | l | l | o | w | o | r | l | d |
  |-----|----|----|----|----|----|----|----|----|----|----|
  2) a < b <= 0 : |-10 |-9 | -8 |-7 | -6 | -5| -4 | -3| -2 | -1 | 0 |
  In the example, [1,4] will get 'ell' and [-4,0] will get 'orld'.
  Because of the expected endpoints, [1,200 will get 'elloworld'.
  In the example, if someone modify 'helloword' with [200,300], then will get an exception-string null
- Strategy for value: between the same modifying range of a string, if there is intersection, this intersection will be taken; and if no intersection exists, then return an exception-string nullstr.
  Modifying a 0 long empty string will obtain an exception sting.
  Modifying an exception string will still obtain an exception string.
- Endpoint a default: the left boundary; b default: the right boundary; an and b are not allowed to be default in the same time. [0,] is equal to [, 0], and they can be used to show parent string.

- The following writing is legitimate:
  [1, 2], [1,], [, -20], [-10, -1], [-10,], [0,], [, 0], [, -1], [, 10]

Metadata Field

Two writing styles for metadata field

3. Common form: data source.field

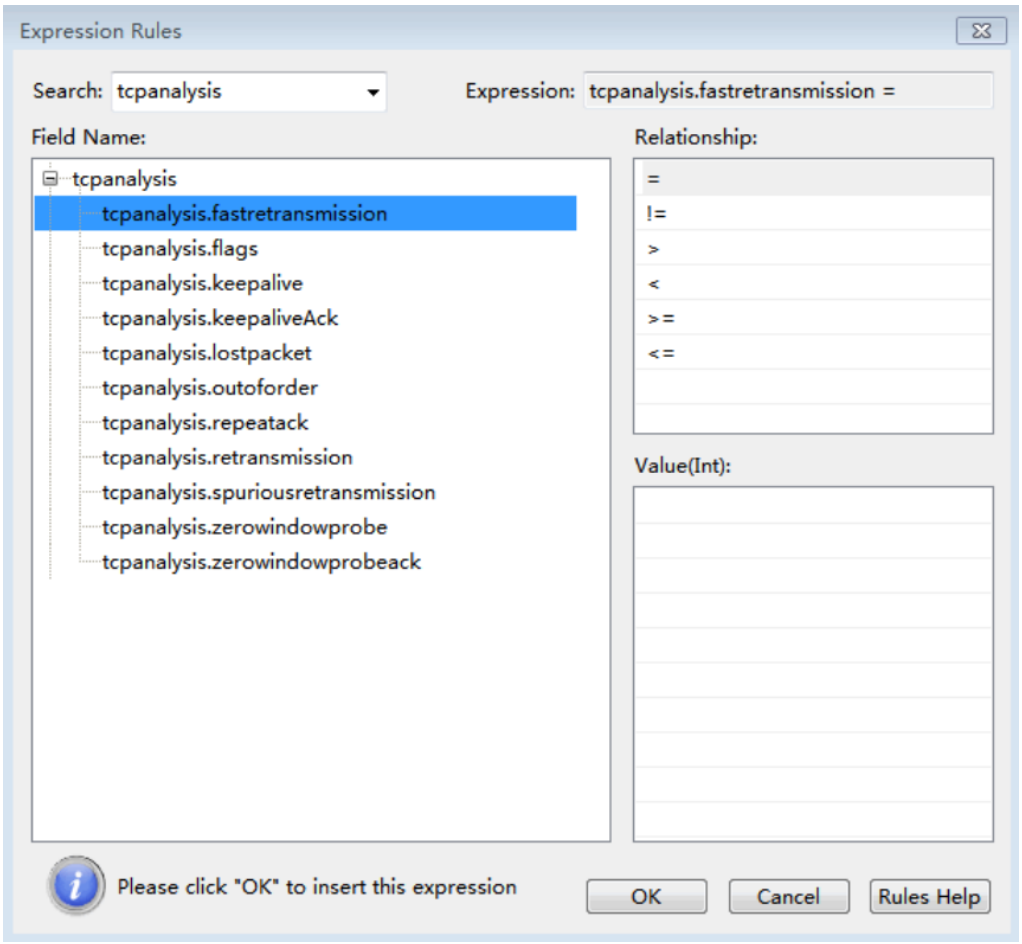
4. Built-in global field writing style

Built-in Metadata Field	Paraphrase
packet	Packet
capturelength	Packet captured length
packetlength	Packet length
payload	Payload of TCP or UDP
payloadlength	Payload length
ip	IP address
srcip	Source IP
dstip	Destination IP
port	Port
srcport	Source port
dstport	Destination port
timestamp	Timestamp

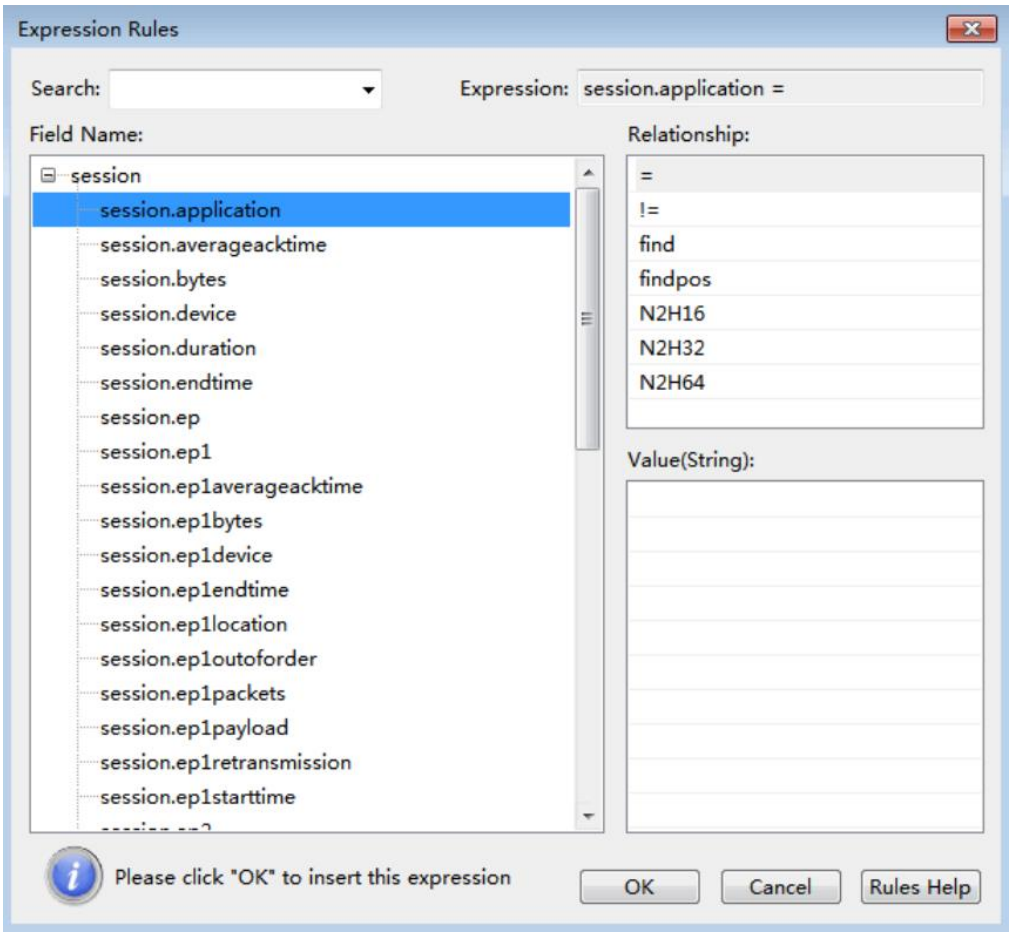
Operators supported by built-in fields

Fields	Data Type	Supported Operators
packet / payload	String	[a, b] . = !=
capturelength / payloadlength / srcport / dstport / port / timestamp	Int	All relational operators
srcip / dstip / ip	IP	= != .

In Packet view, TCP analysis fields (*tcpanalysis*) are added in display filter. The fields are applied after packet analysis.



In Conversation view, there are only session fields (*session*) in display filter. The fields are applied for conversation statistics only.



Note The fields related to the number of bytes and time in the session field support filtering of different precisions, and these fields are all int type fields, and do not support floating-point number writing.

4. Byte count related fields: **session.bytes, session.ep1bytes, session.ep2bytes**.
   The unit of byte size is b(byte) by default, and k(kb), m(mb), g(gb), t(tb) are also supported. ex: session.bytes > 1024k can also be written as session.bytes > 1mb.

5. Time related fields: **session.duration, session.averaggeacktime, session.ep1averageacktime, session.ep2averageacktime, session.maxacktime**.
   The unit of time size is nanoseconds(ns) by default. and microseconds(us), millisecond(ms), second(s), minute(m), hour(h). ex: session.duration > 60s can also be written as session.duration > 1m.

6. String type field: **session.payload, session.uncompressedpayload, session.decryptedpayload** is written according to the expression of the String type field, where **session.payload** represents TCP or UDP session content filtering, **session.uncompressedpayload** represents HTTP session data decompression content filtering, and **session.decryptedpayload** represents the decrypted SSL/TLS session data content filtering.

Abnormalities Occurring During the Calculation

If an exception occurs during the calculation of a logical expression, the value of the logical expression will also be an exception. The abnormal state is the third state which is not true or false, and it is not just true or false in multi-valued logic. The calculated range of an atomic logic expression is: {true, false, abnormal}.

The rules for predicate calculus and logical operations with abnormal participation are as follows (tristate booleans, here the third state is assumed to be abnormal):

5. The result of logic expression with any predicate calculus involving abnormal operand is abnormal. Contains all relationship comparisons: =! = > >= < <=.
6. Logic OR operation (||) with abnormal operand, if the result is true, then it is true, other results are abnormal.
7. Logic AND operation (&&) with abnormal operand, if the result is false, then it is false, other results are abnormal.
8. Logic NOT operation(!) with abnormal operand, the results would be abnormal.

Our definition of an atomic logical expression hit means that the atomic logical expression has a value of true; the definition of a rule hit is that the value of the rule is true.

Examples of situations that may cause anomalies:

5. Range modification of String is no intersection out of bounds, which will cause the operand to be an exception-string nullstr.
6. There is a special field payload in the global data source. if the length of payload is zero (payloadlength = 0), then payload is an exception-string nullstr. Its intuitive semantics is "no load." But not all String fields which length is zero are exception string, it depends on the registration strategy of the field.
7. The built-in findpos function throws an exception when no signature string is found. That is the rule: StringOperand.findpos('abc') < 20 ||! (StringOperand.findpos('abc') < 20), If 'abc' isn't found in StringOperand, then the rule won't hit.
8. Other conditions that may cause an abnormal.

Multi-valued "Existing Quantifiers" and "Full Quantifiers"

Mathematically, existential quantifier means that there is at least one exist, and full quantifiers means all. A statement modified by an existing quantifier, the multi-value is logic OR expression, and a statement modified by full quantifiers, the multi-value is logic AND expression.

For example, a multivalued Int type operand var, its value is [1,3,10}, As the rule set, for var > 11, if modified with an existing quantifier, the value of the expression is true as long as there is any value greater than 11. In the meanwhile, if it was modified with full quantifiers, then the value of the expression would be true only if all values are greater than 11.

The current engine (v3.2.2) does not implement the explicit specification of the existing quantifiers and the full quantifiers. In the case of no specified quantifier, it will always be existing quantifiers. That is to say, the existing quantifiers are implemented in the current engine version.

The application of existing quantifiers:

- port > 80 is equal to srcport > 80 || dstport > 80
- ! (port > 80) is equal to! (srcport > 80 || dstport > 80) and equal to srcport <= 80 && dstport <= 80

DPI Filter Expression Example

String Expression

- Match the string "abcd" in the payload: payload.find('abcd')
- Use hexadecimal to match the string "abcd" in the payload: payload.find(HEX'61 62 63 64')
- Use the boundary modifier to find the content and match the string "abcd" in the payload:
  payload[2,50].find('abcd'), which means to find "abcd" in the data at offset 2 to offset 50 in the payload
  payload[,50].find('abcd'), which means to find "abcd" in the data at offset 0 to offset 50 in the payload
  payload[10,].find('abcd'), which means to find "abcd" in the data starting at offset 10 in the payload
  payload[-10,-1].find('abcd'), which means to find "abcd" in the data offset from the 10th to the 1st in the payload
- Match the offset of the string "abcd" in the payload greater than 10:
  payload.findpos('abcd')> 10
- Match data packets where the http.url field does not exist: http.url.isnull()
- Match the payload length greater than 100: payload.length()> 100
- Match the first byte in the payload greater than 10: payload.U8()> 10

DateTime Expression

- timestamp = DT'2021-9-10 13:00:10', indicating that the matching timestamp is "2021-9-10 13:00:10"
- timestamp = DT'2021-9-10 13:00:10.981815000', indicating that the timestamp matches in nanoseconds
- timestamp = DT'2020-09-26 11:02:59+0800', which means to match the second-level timestamp with time zone; +0800 means East Eighth District time, that is, Beijing time; -0800 means West Eighth District time; 0000 means UTC time

Regular Expression

- Match the string "aBCd" in the payload, and is case sensitive: payload.find(/aBCd/i)

- Match the string "ab\c\d" in the payload, and is case sensitive: payload.find(/ab\\c\\d/i)
- Match the string "ab[any single character]d" in the payload: payload.find(/ab.d/s)
- Match the string "ab[any multiple characters]d" in the payload: payload.find(/ab.*d/s)
- Match the string "ab[any single character]D" in the payload, and is case sensitive: payload.find(/ab.D/is)

Int Expression

payloadlength = 100; payloadlength> 100; payloadlength <100; respectively indicate that the matching payloadlength is equal to 100, greater than 100, and less than 100

IP Expression

- Match a single ip: ip = 192.168.9.12
- Match IP range: ip.in (192.168.9.1-192.168.9.15)
- Match IP subnet: ip.in(192.168.1.1/24)
- Match the IP in the set, the elements in the set can be a single ip, ip range, ip subnet: ip.in(192.168.9.20,192.168.9.1-192.168.9.15,192.168.1.1/24)

Multi-value Expression

When matching multi-value types, the results of "!=" and "!" are different, for example:

ip != 192.168.9.12 is equivalent to (srcip != 192.168.9.12 || dstip != 192.168.9.12);

!(ip=192.168.9.12) is equivalent to (srcip != 192.168.9.12 && dstip != 192.168.9.12);

protocol != TCP is not equivalent to !(protocol = TCP) ;

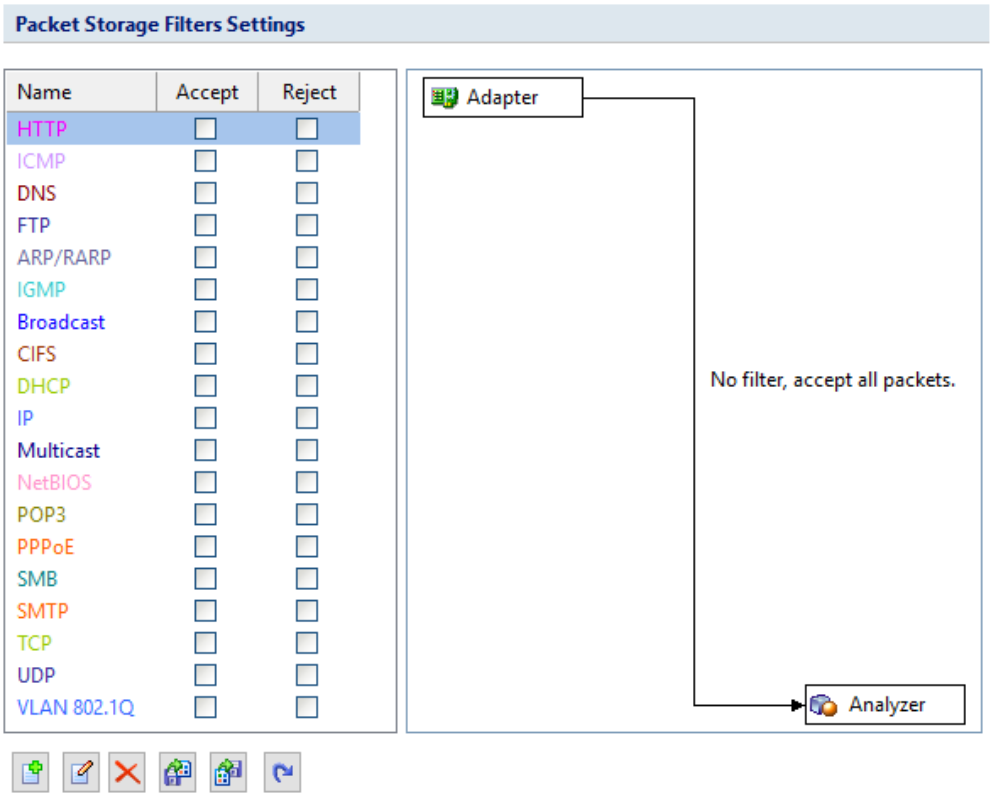
port != 80 is not equivalent to ! (port = 80).

This is because in the packet, ip represents the source IP and destination IP; port represents the source port and destination port; protocol represents the data link layer, transport layer, application layer and other different levels of protocols.

Currently, the multi-value types in Filter include ip, port, protocol, and all fields under all protocols.

Packet Storage Filters

This tab is for containing, setting up, and applying storage filters. Storage filters are utilized to storage particular packets. If no filter was enabled, Capsa will storage all the packets that are analyzed. Unlike the analysis filters, the filtered packets in the storage filters are still analyzed and counted, but are not placed in the display cache. The filter conditions only apply to storage (display cache, packet cache). Packet storage filters can improve the storage performance of the system.



This tab 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 stored by Capsa, while **Reject** means only packets unmatched will be stored 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.

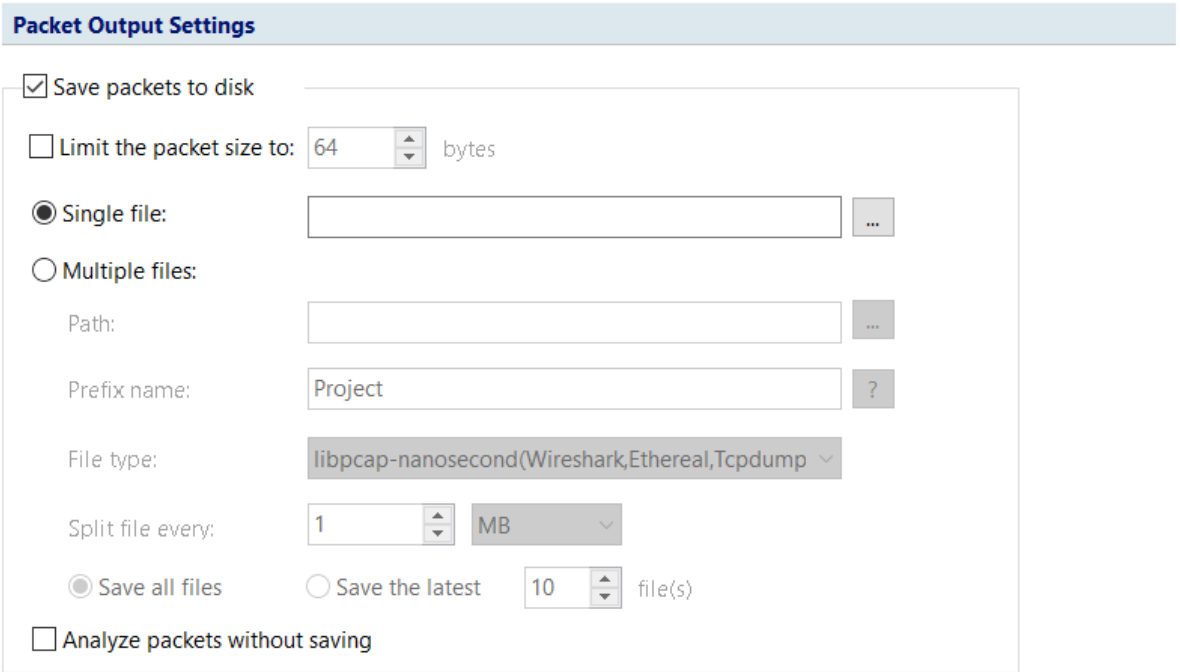
To create a storage filter.

4. On the Storage Filter tab of the **Analysis Settings** dialog box, click  to open the **Packet Filter** dialog box.
5. Select a simple filter or an advanced filter and set the filter, including the filter name, filter description, and filter rules (see Creating Simple Filter and Creating Advanced Filter for details).
6. Click **OK** on the **Packet Filter** dialog box, and click **OK** on the **Packet Filter Settings** dialog box.

Note After creating a filter, you should select the **Accept** or **Reject** checkbox to make the filter take effect.

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.

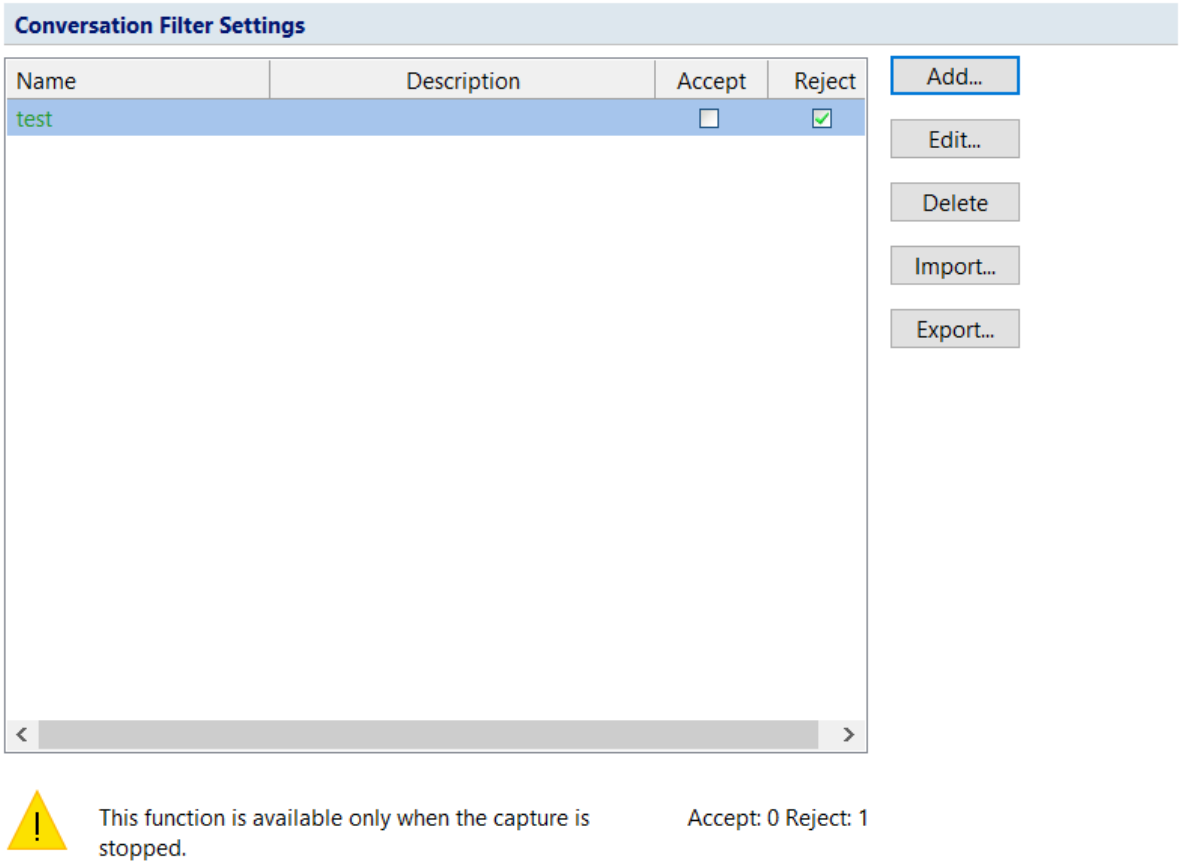
Difference between Packet Buffer and Packet Output

Packet Buffer is for buffering the packets on the Packet view. For example, when you capture a traffic of 30M and you set up a Packet Buffer of 16MB, the Packet view will only display packets of 16MB, the other 14MB of packets are discarded due to not enough packet buffer; all 30MB packets are analyzed by Capsa, but 14MB packets cannot be displayed. In other words, the size of Packet Buffer only impact the number of packets displayed on the Packet view.

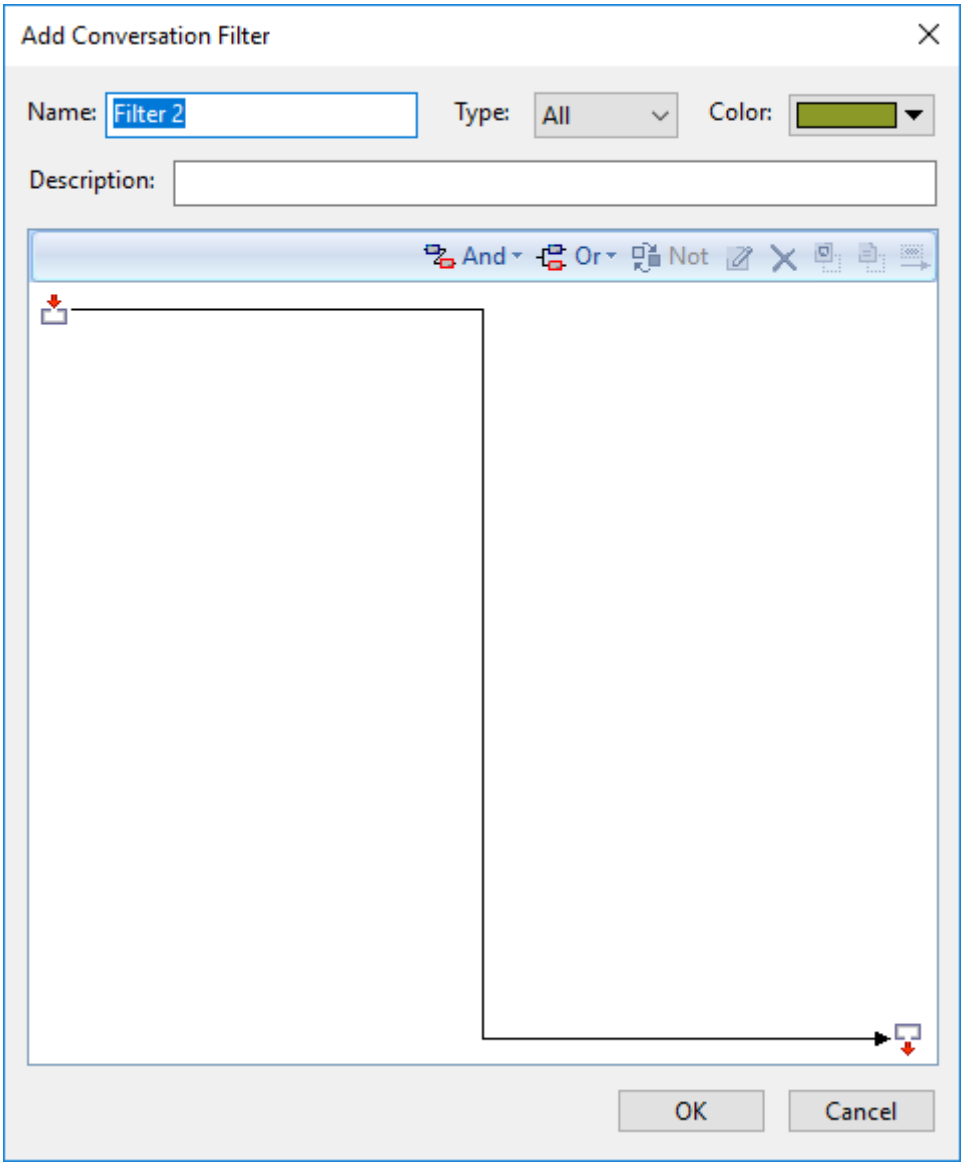
Packet Output feature is for automatically saving all the packets, the packets from the start to the end of a capture. It has nothing to do with Packet Buffer. No matter the size of the Packet Buffer, Capsa will save all packets once the Packet Output feature is enabled.

Conversation Filter

You can configure the conversation filter when the capturing is stopped. By configuring the conversation filter, Capsa will be able to provide a certain kind of conversation data.



You can add a conversation filter by clicking the add button.



You can configure the following fields to set up the conversation filter:

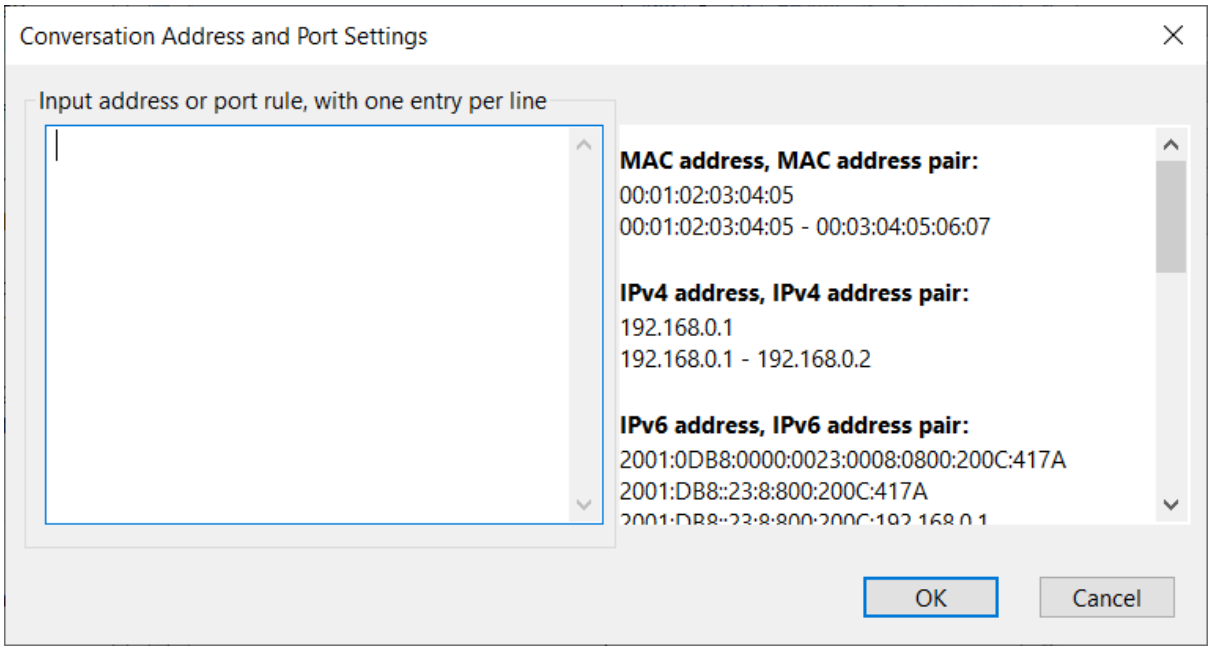
Field	Explanation
Name	The name for this filter.
Type	Capsa supports filter on MAC conversation, IP conversation, TCP conversation, UDP conversation. You can set a filter on one of them, or you can also set a filter on all of them.
Color	Set the color for the filter's name.
Description	You can put a brief description for you filter.
Rule	1. Capsa supports having multiple rules in one filter. The "and", "or" relationship between rules is supported. 2. Each rule supports to filter according to the address and port, location,

conversation protocol, conversation packet, conversation content, and conversation option.
For the configurations please refer to the instruction of each Rule.

Rule

- **Address and Port**

  This feature allows you to filter conversations according to the address or the port.

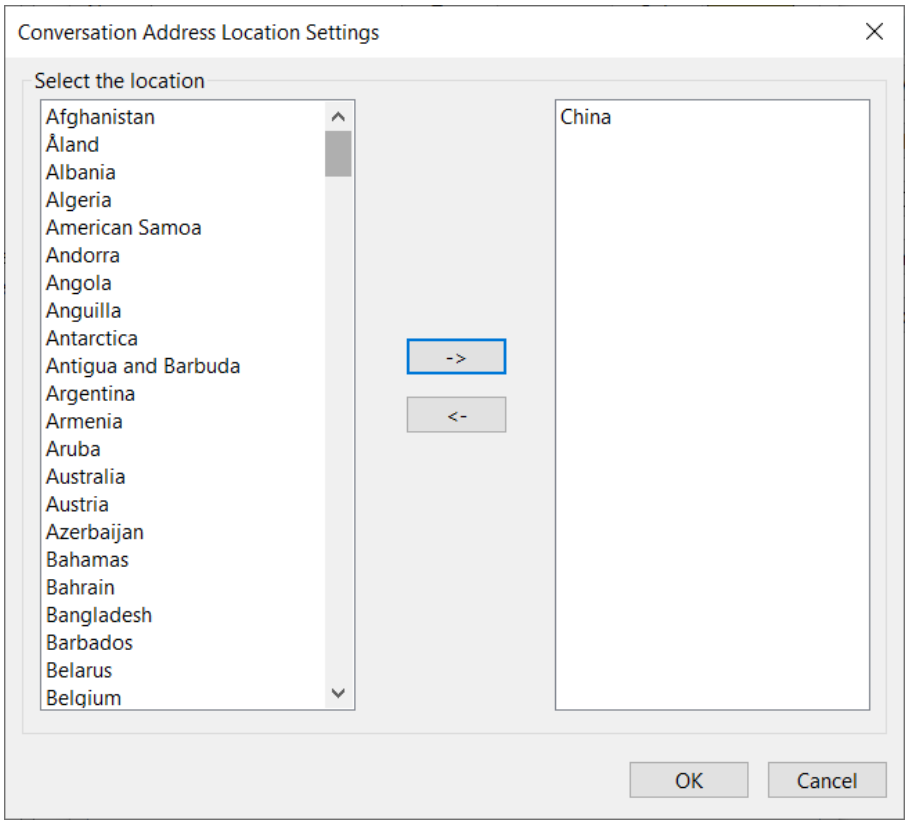


  As it is shown in the figure, Capsa supports multiple ways to configure the filter to fit all kinds of conversations:

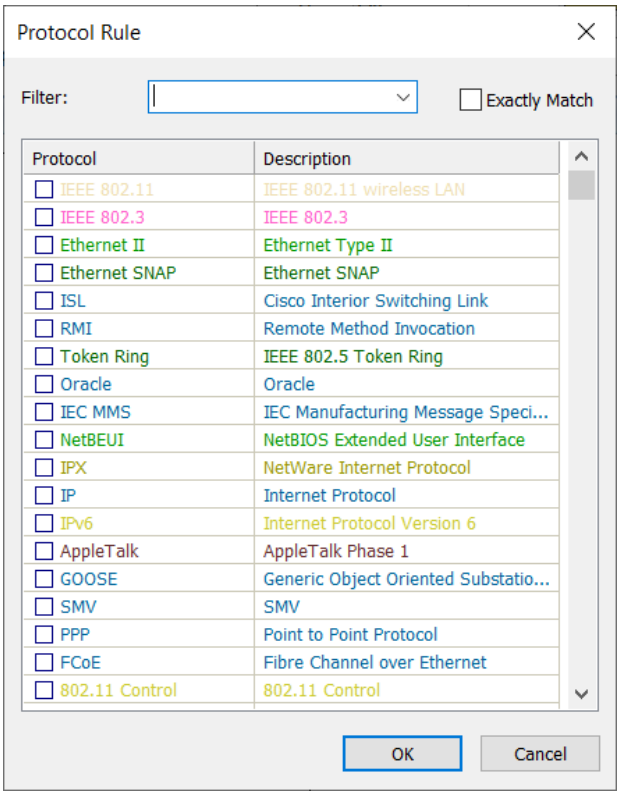
  - MAC address, MAC address pair: filters conversations according to MAC addresses.
  - IP address, IP address pair: fits for IP conversations, TCP conversations, and UDP conversations.
  - IP address, IP address pair: for the TCP conversation and the UDP conversation, Capsa can filter conversations according to the IP address port/IP address port pair; but for IP conversation, Capsa filters according to the IP address/IP address port.
  - Port, port pair: only works for the TCP conversation and the UDP conversation.

- **Location**

  Only the IP conversation can be filtered by locations. This feature does not apply to MAC conversations.



- **Conversation Protocol**
  After selecting one or multiple protocols, Capsa will filter conversations according to the protocol.



- **Conversation Packet**

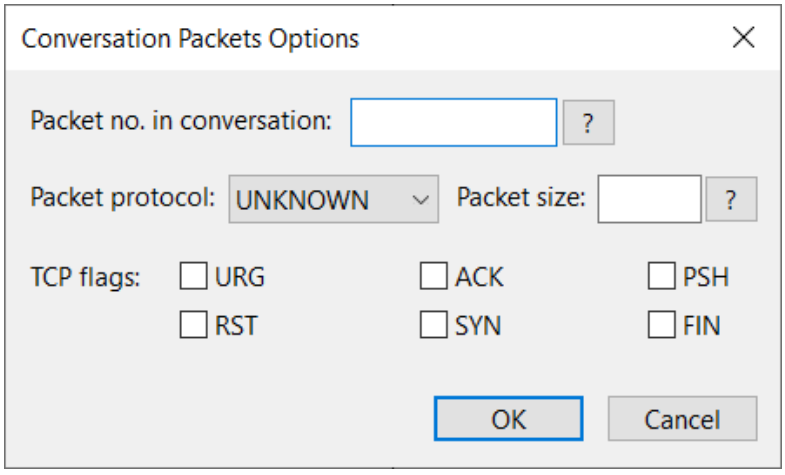
  Packet no. in conversation: set the sequence number of the packet in a conversation.

  Packet protocol: select a packet protocol.

  Packet size: set the size for this packet.

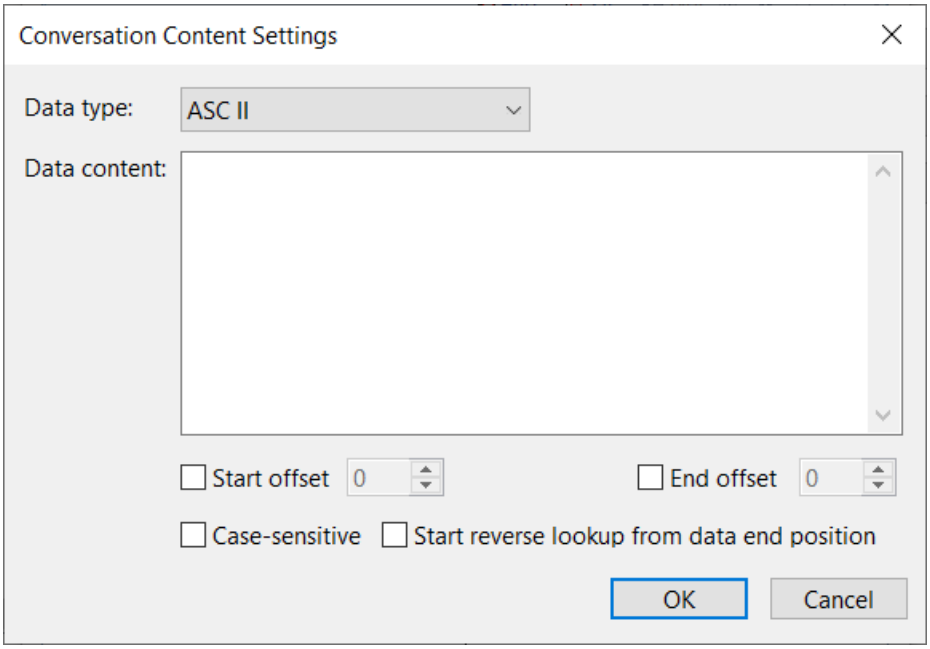
  TCP flags: select the TCP flag for this packet. This setting only applies to TCP conversations.

  Note The option Packet no. in conversation is required.



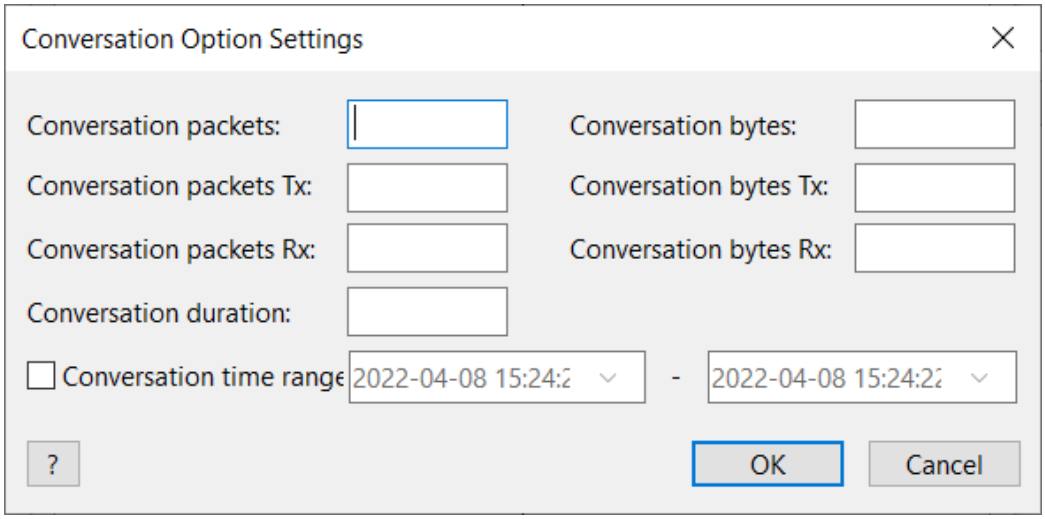
- **Conversation Content**

  Capsa supports to filter conversations according to the conversation content. When configuring the data content, you can select a data type, such as: ASCII, HEX, UTF-8, UTF-16. You can also set the start/end offset and case-sensitive.



- **Conversation Option**

  Capsa supports filtering conversations according to the key property.
  - Conversation packets: the total packets count of this conversation.
  - Conversation bytes: the total bytes of this conversation.
  - Conversation bytes Tx: sent bytes in this conversation.
  - Conversation bytes Rx: received bytes in this conversation.
  - Conversation packets Tx: sent packets count of this conversation.
  - Conversation packets Rx: received packets count of this conversation.
  - Conversation duration: for how long the conversation lasts.
  - Conversation time range: the time range for the conversation.



Start the filter

After configuring a filter, you can choose to accept it or reject it.

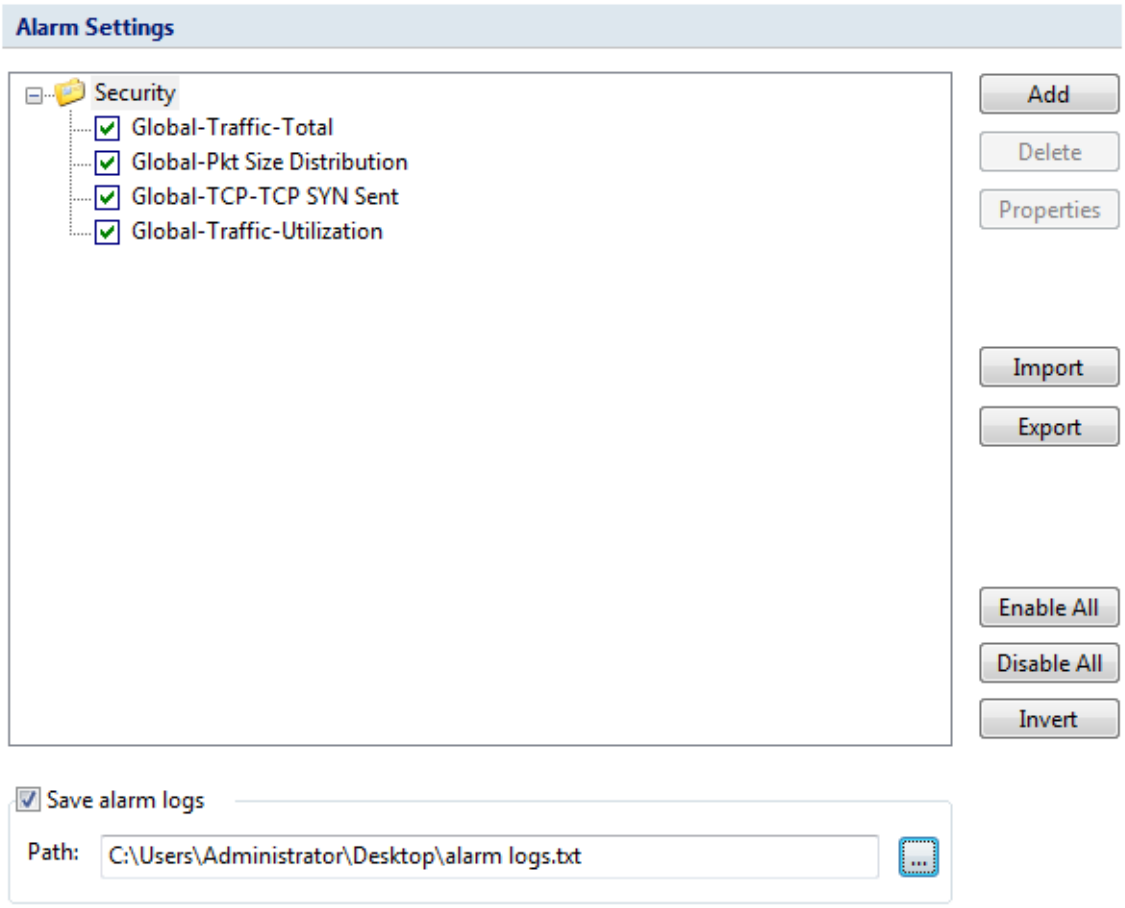
- Accept: Only show conversations that meet the filter requirement.
- Reject: Do not show conversations that meet the filter requirement.

Import/Export

You can click "Export" button to save the filter configuration as ".csconvflt" to the local disk. You can also click "Import" button to import ".csconvflt" files from the local disk to the Capsa, as a quick configuration for the filter.

Alarm Settings

The **Alarm Settings** tab manages all alarms available in analysis settings 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 Alarm for details).
- **Delete**: Deletes the selected alarm.
- **Properties**: Views or modifies the properties of the selected alarm.
- **Import**: Loads the alarm settings from a .csalarm file.
- **Export**: Saves the alarm settings as a .csalarm 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.

Creating Alarm

To create an alarm, do one of the following to open the **Make Alarm** dialog box and then complete the **Make Alarm** dialog box:

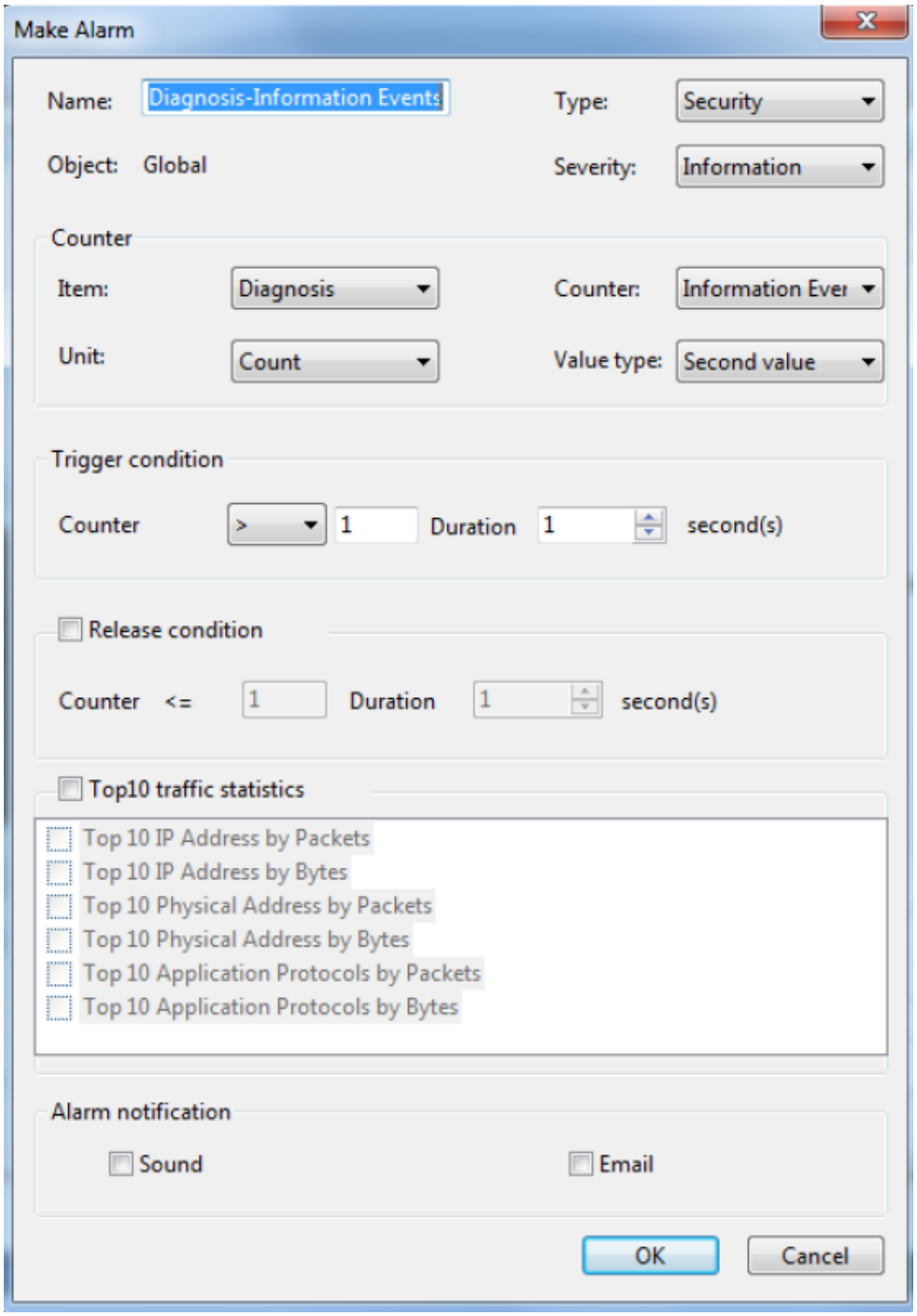
- Click **Add Alarm** button on the **Alarm Explorer** window.
- Open **Analysis Settings** dialog box, select **Alarms** tab, and click **Add** button.
- Click icon in the **Node Explorer** window.

- 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-click or which you select in the **Node Explorer** window.

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**
  When this option is enabled, top 10 traffic statistics will be recorded in the alarm log when the alarm was triggered. Different alarm object has different traffic statistic items.
- **Alarm notification**
  This function is only available for Capsa Enterprise. You can set how to notify the alarm messages when they are triggered. To notify with a sound, select the **Sound** checkbox, and to notify with an email, select the **Email** checkbox.

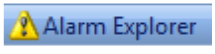
Edit Alarm

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

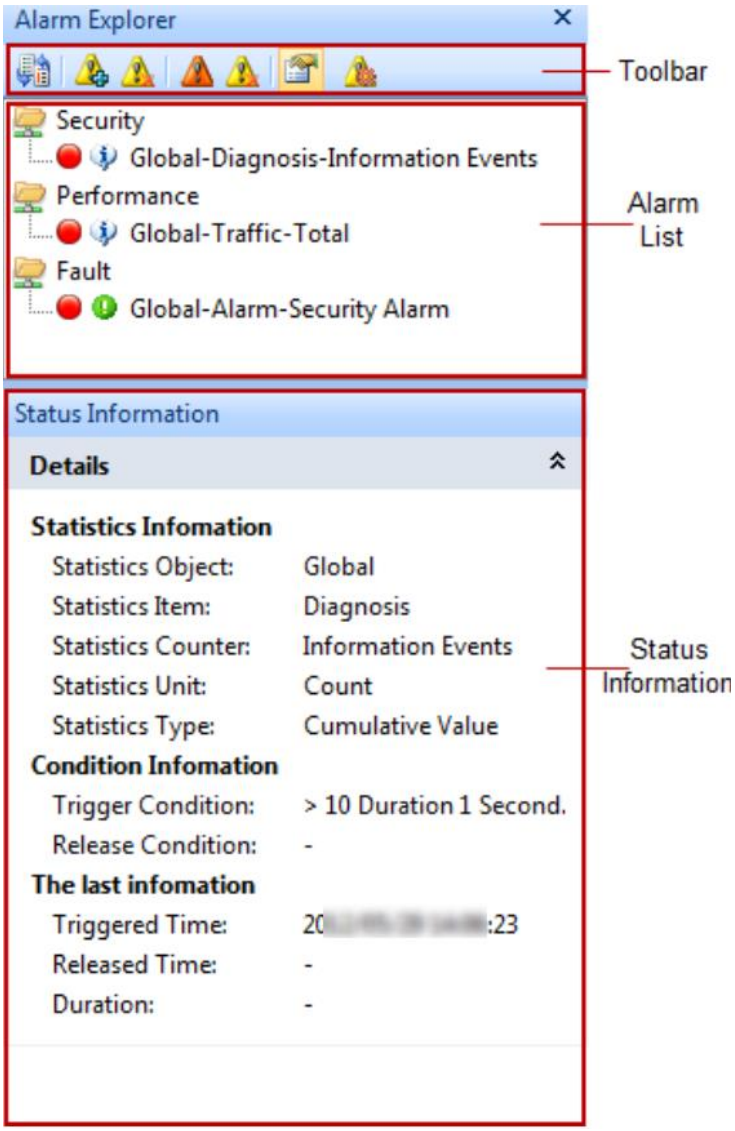
When you view the statistics of the network, you may want a tool to alert you some specific statistics or traffic status of the network. The alarm function is the tool.
For your convenience, Capsa provides an **Alarm Explorer** window to manage alarms, in which you can create, edit and view alarms. You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

: 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.

: Opens the **Alarms** tab of the **Analysis Settings** dialog box to manage alarms.

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

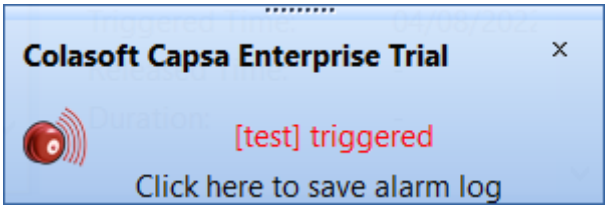
The **Status Information** pane displays the properties of the selected alarm in detail.

Tips You can click to collapse the details.

When an alarm is triggered, a box pops up to inform you.

Alarm Notification

When an alarm is triggered or dismissed, a pop-up fade in at the bottom of the Alarm Explorer window to inform you the alarm information even when the program window is not active.



You can click the link: **Click here to view alarm log** to view alarm log.

Tips The corresponding alarm bubble on the right side of the status bar starts flashing when an alarm was triggered.

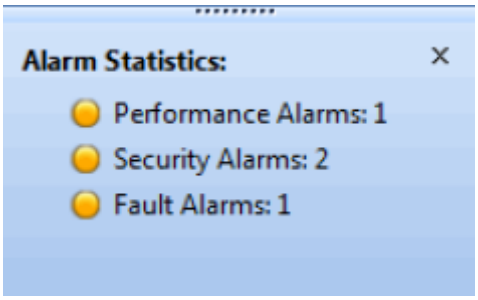
Note

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.

There are three bubbles under the Alarm Explorer window, to 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:

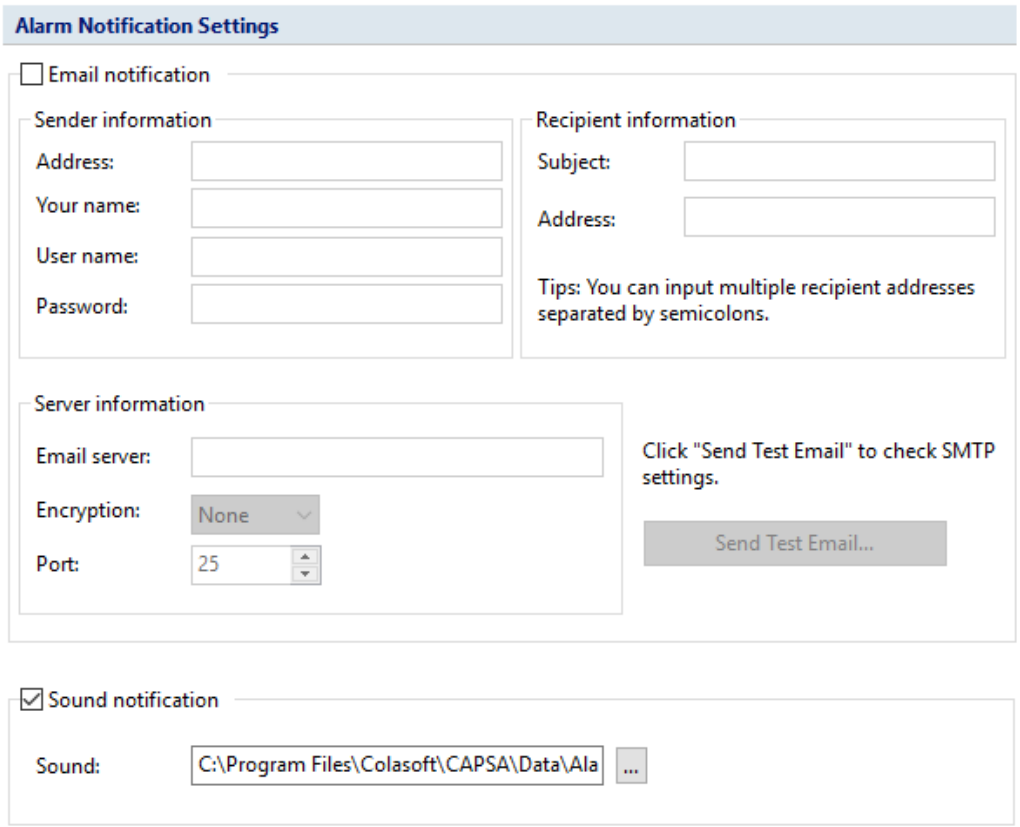


Furthermore, if you enabled "Sound" and "Email" alarm notification settings when defining an alarm, you will hear a sound and receive an email when the alarm is triggered.

Alarm Notification

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

Note Alarm notification feature is only available for Capsa Enterprise. Capsa Standard and Capsa Free don't provide such feature.



Email notification

To notify alarms with emails, follow the steps below.

1. Select the checkbox Email notification on the Alarm Notification tab.
2. In the Sender information group box, enter sender information:
    - **Address**: The email address of the sender.
    - **Your name**: The name of the sender.
    - **User name**: The user name of the sender to logon the email server.
    - **Password**: The password for the sender to logon the email server.
3. In the **Recipient information** group box, enter recipient information:
    - **Subject**: The subject of the alarm notification emails.
    - **Address**: The recipient address of the alarm notification emails. Users can enter multiple recipients with semicolon to separate.
4. In the **Server information** group box, enter email server information:
    - **Email server**: The address of the email server.
    - **Encryption**: The encryption connection type of email server.
    - **Port**: The port number for the connection to the email server.
5. Click **Send Test Email** to check the settings. If the settings are correct, you should receive an email at your email inbox.
6. Click **OK** to save the settings.

Note At present, Capsa only supports following authentication types: AUTH LOGIN, AUTH PLAIN, AUTH NTLM, ANONYMOUS login.

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.

Security Analysis

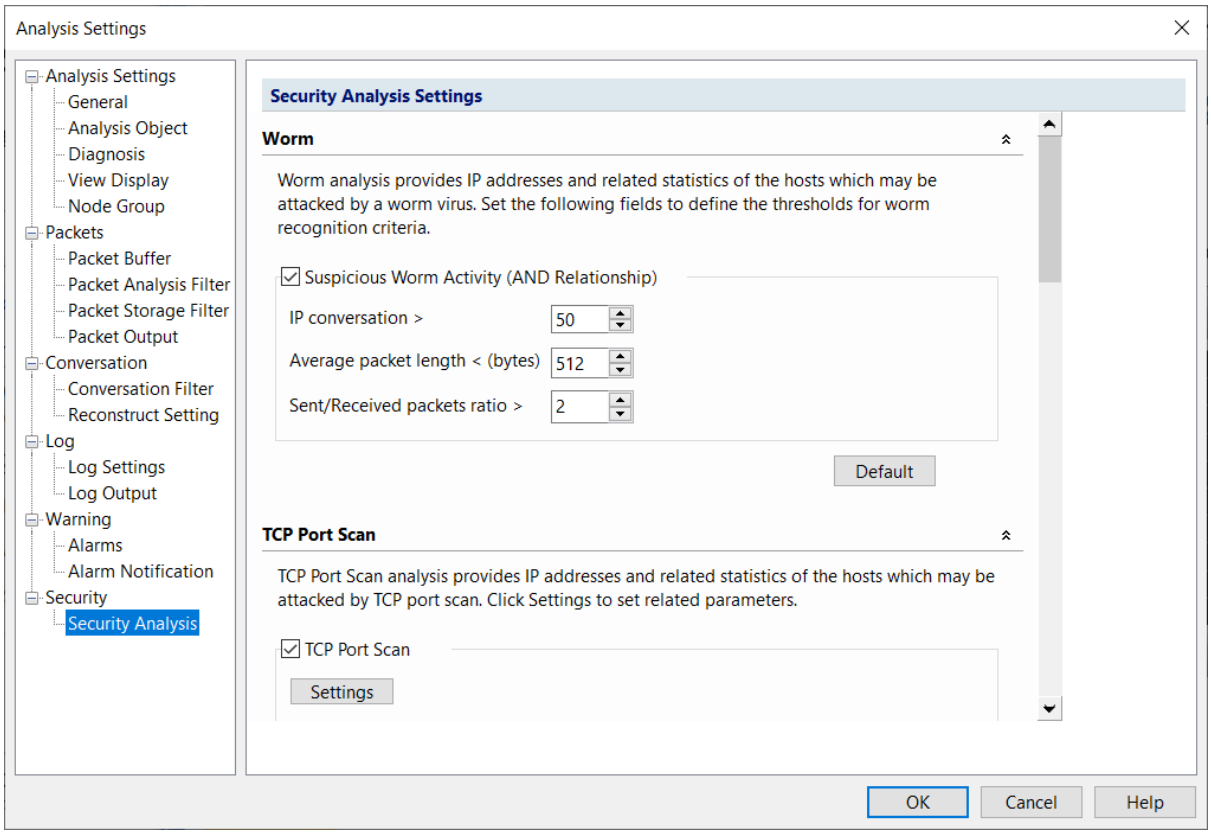
Security analysis is designed to detect worm activities, TCP port scanning, ARP attacks, DoS attacks and suspicious conversations on the network.

- Security Analysis Settings
- Security Analysis views

Note Security analysis is only available for Capsa Enterprise.

Security Analysis Settings

To view/modify the settings, just double-click the analysis settings and then go to the Security Analysis tab.



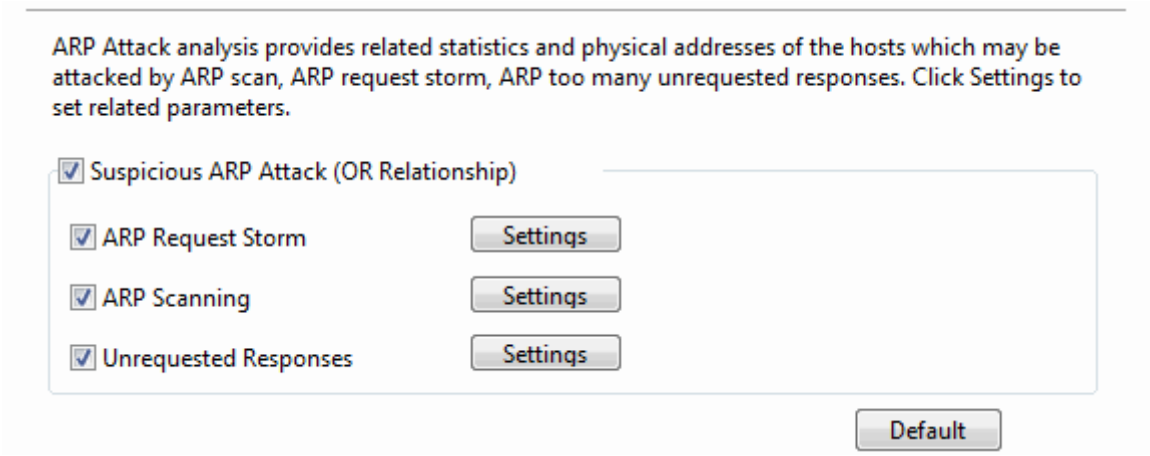
Security Analysis settings have all setting tabs that default analysis settings include and has a plus Security Analysis tab to configure related settings. To modify other setting tabs, please refer to Analysis Settings.

The Security Analysis tab includes following settings:

- ARP Attack Settings
- Worm Settings
- DoS Attacking Settings
- DoS Attacked Settings
- TCP Port Scan Settings
- Suspicious Conversation Settings

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.

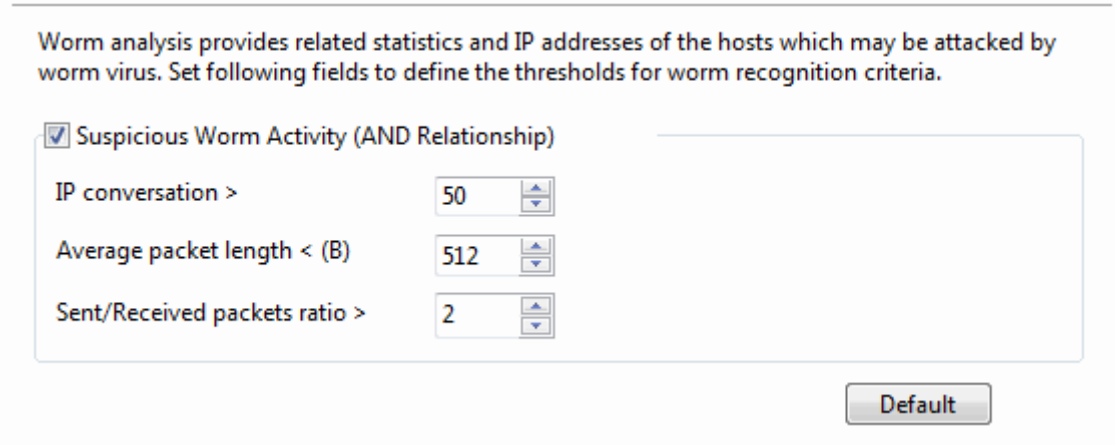
- **ARP Request Storm**: Enables ARP request storm analysis. Click **Settings** to locate the **ARP Request Storm** diagnosis event on the **Diagnosis** tab. There are two main parameters for this event.
    - **Sampling Duration**: The sampling time with the unit of second. The value is an integer between 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** 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** 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.

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

Worm Settings

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



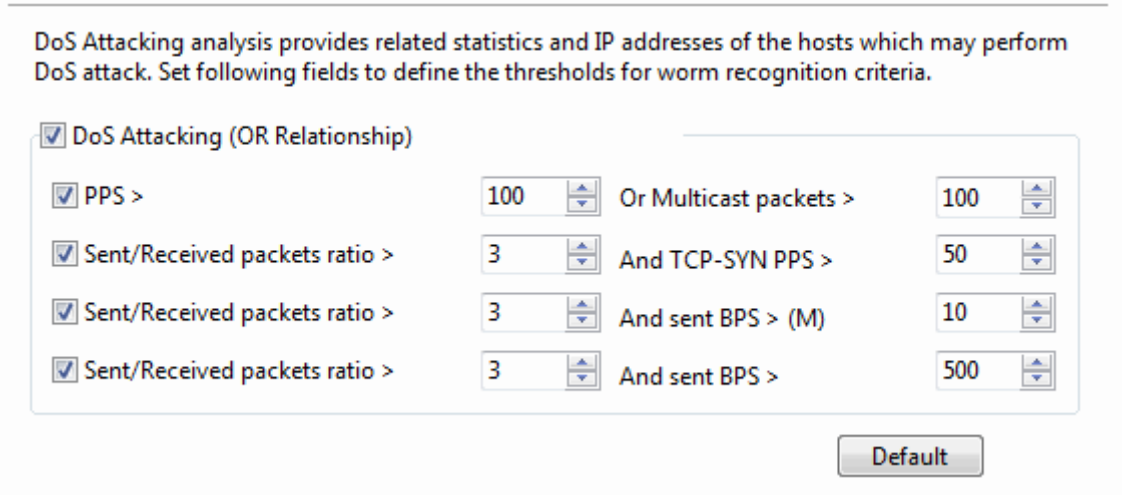
Suspicious Worm Activity: Enables worm analysis, or else there will be no item to show on the **Worm** view. **AND Relationship** means the three conditions below should all be met to define the worm activity.

- **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.

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

DoS Attacking Settings

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



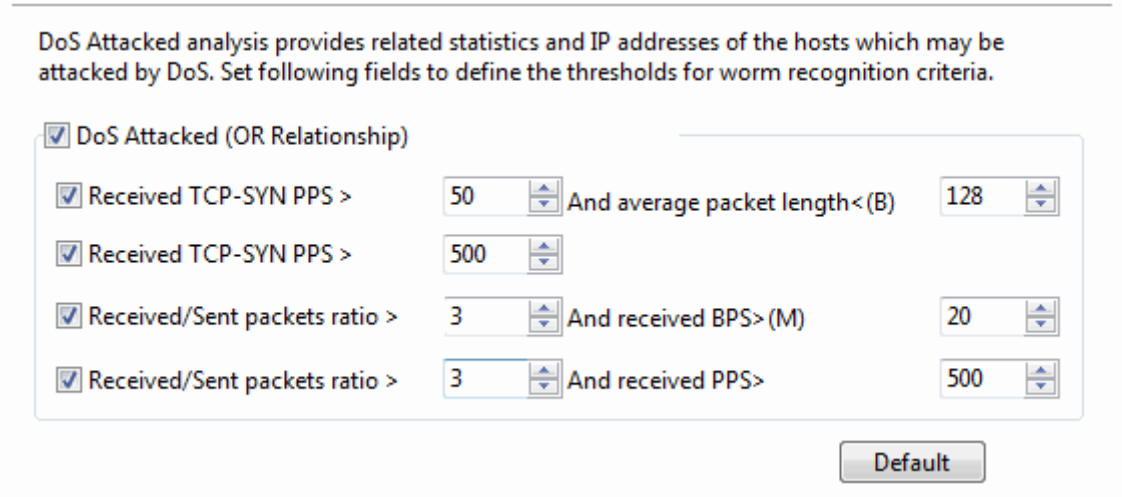
DoS Attacking: Enables DoS attacking analysis, or else there will be no item to show on the **DoS Attacking** view. **OR Relationship** means one of the four conditions below is met to define the DoS attacking activity.

- 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.
- 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.
- 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.
- 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.

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

DoS Attacked Settings

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



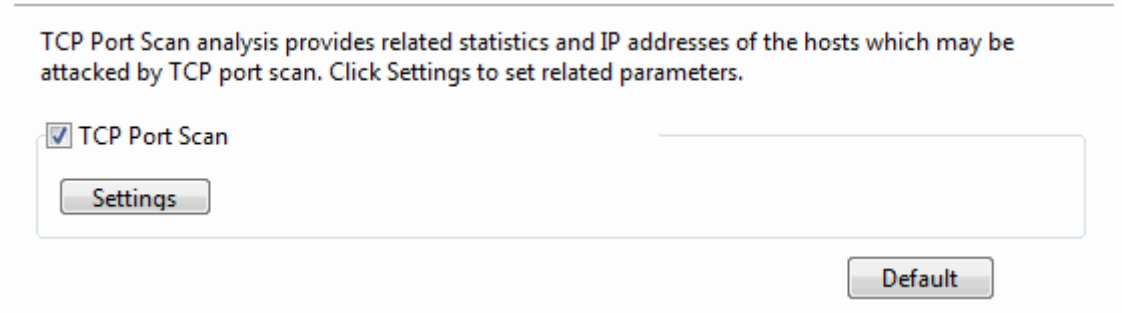
DoS Attacked: Enables DoS attacked analysis, or else there will be no item to show on the **DoS Attacked** view. **OR Relationship** means one of the four conditions below is met to define the DoS attacked activity.

- 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.
- 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.
- It is supposed to be DoS Attacked when the ratio of received packets to send 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.
- It is supposed to be DoS Attacked when the ratio of received packets to send 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.

TCP Port Scan Settings

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



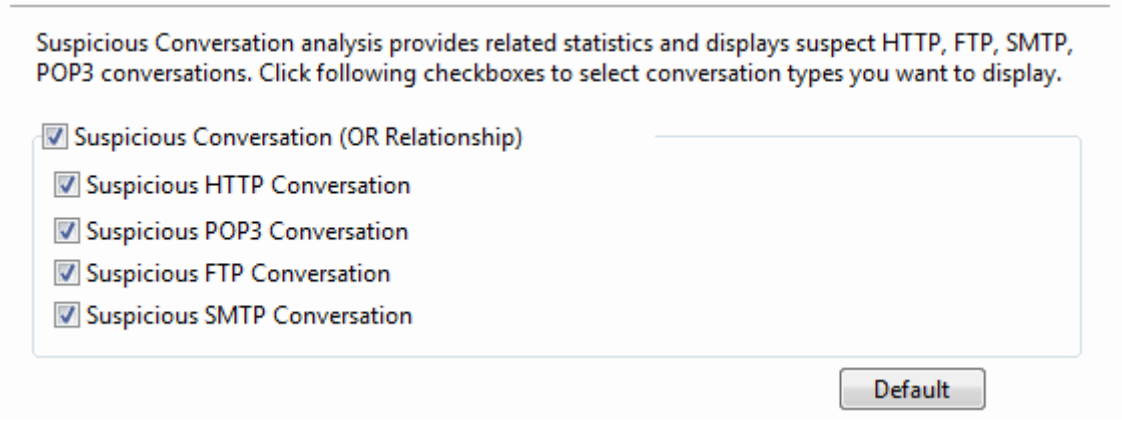
TCP Port Scan: Enables TCP port scan analysis, or else there will be no item to show on the **TCP Port Scan** view.

Settings: Locates to the **TCP Port Scan** diagnosis event on the **Diagnosis** 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.

Default: Resets the setting of that type of security analysis to 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** tab. It is supposed that there is suspicious HTTP conversation on the network when port 80 is connected without HTTP data.

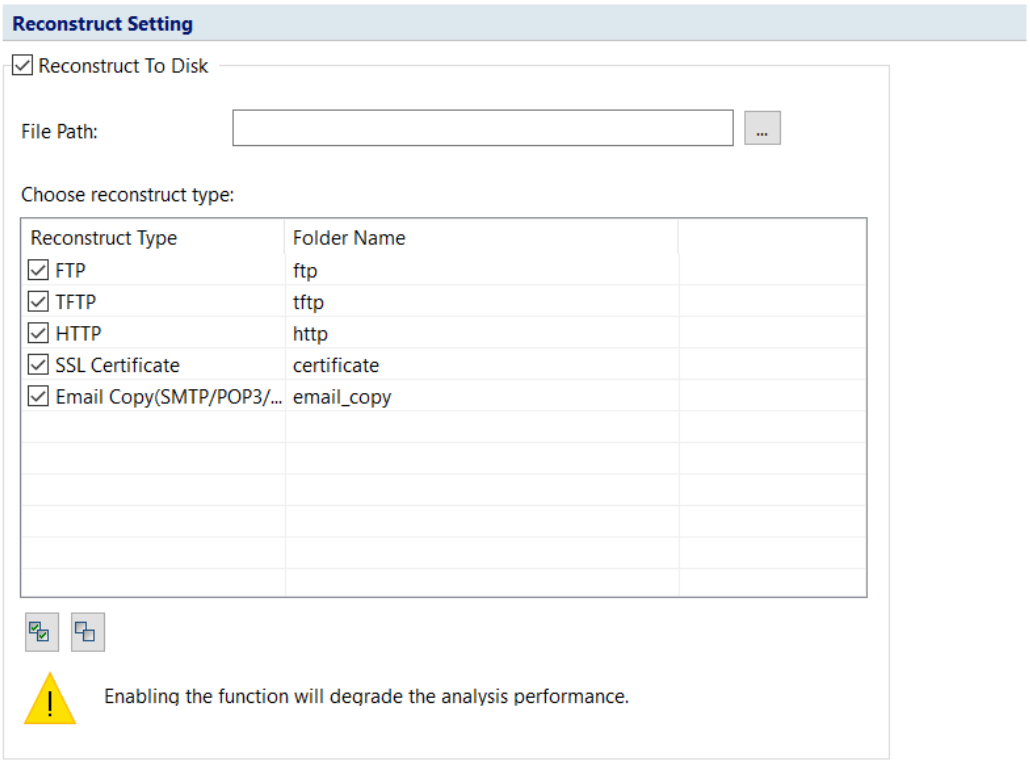
- **Suspicious POP3 Conversation**: Enables suspicious POP3 conversation analysis which is set by the program on the **Diagnosis** tab. It is supposed that there is suspicious POP3 conversation on the network when port 110 is connected without POP3 data.
- **Suspicious FTP Conversation**: Enables suspicious FTP conversation analysis which is set by the program on the **Diagnosis** 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** tab. It is supposed that there is suspicious SMTP conversation on the network when port 25 is connected without SMTP data.

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

Reconstruct Settings

Capsa is able to extract and fully reconstruct the files transmitted over FTP, TFTP, and HTTP, as well as SSL certificates.

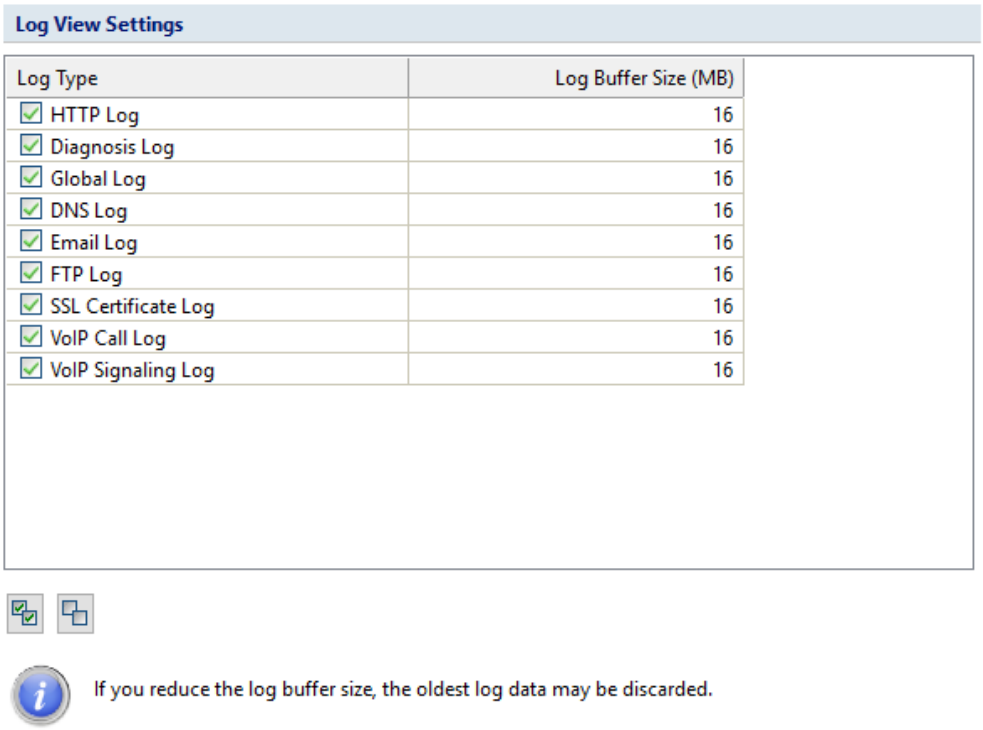
To reconstruct files, enable the checkbox **Reconstruct To Disk** as the screenshot below, set the path to store the files to be reconstructed, and the reconstruct types.



Note Enabling the reconstruction function will affect the system analysis performance a lot.

Log View

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



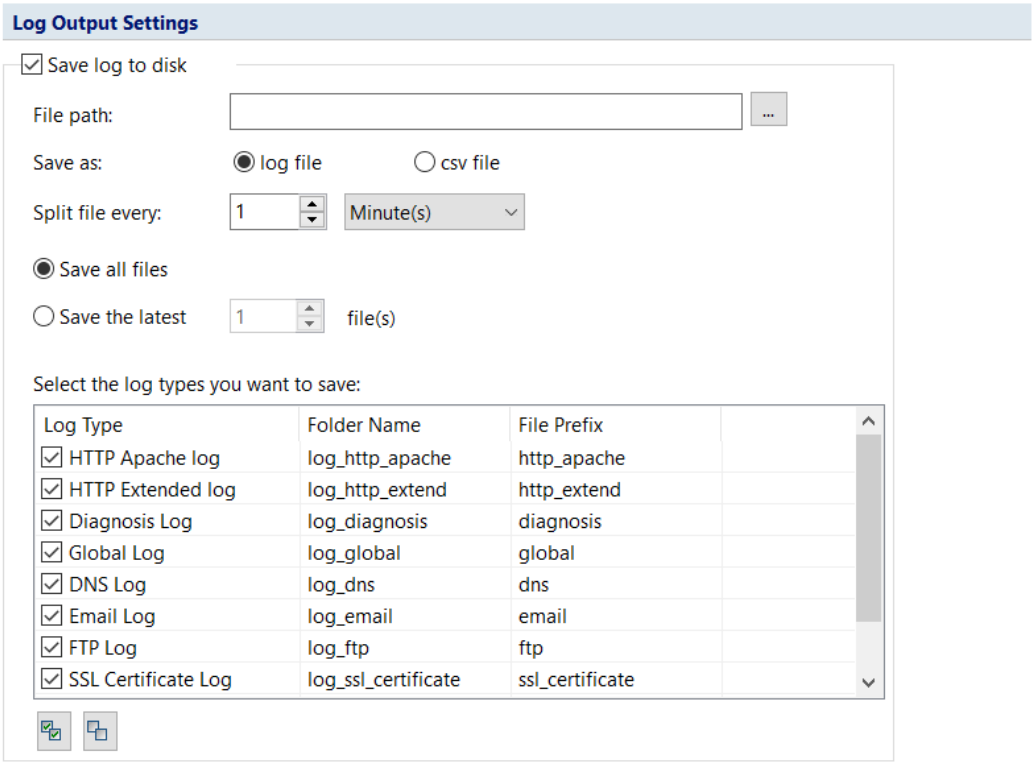
This tab contains two columns:

- **Log Type**: To specify which types of log to be displayed on the **Log** view.
  Tips **Diagnosis Log** is selected to display the detailed information of diagnosis events on the **Details** pane of the **Diagnosis** view, or else, there will be no item on the **Details** pane.
- **Log Buffer Size**: 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.

Note If you reduce the log buffer size, the oldest log data may be discarded.

Log Output

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



The following list describes the options on this tab:

- **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.
- **Select the log types you want to save**: This option is for specifying which log types to be saved.

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.

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.

Node Explorer

Colasoft Capsa provides innovative Node Explorer, which functions like a display filter. The node could be a protocol, a MAC address, and an IP address. Once a node is chosen, the analysis views displays data only related to this node.

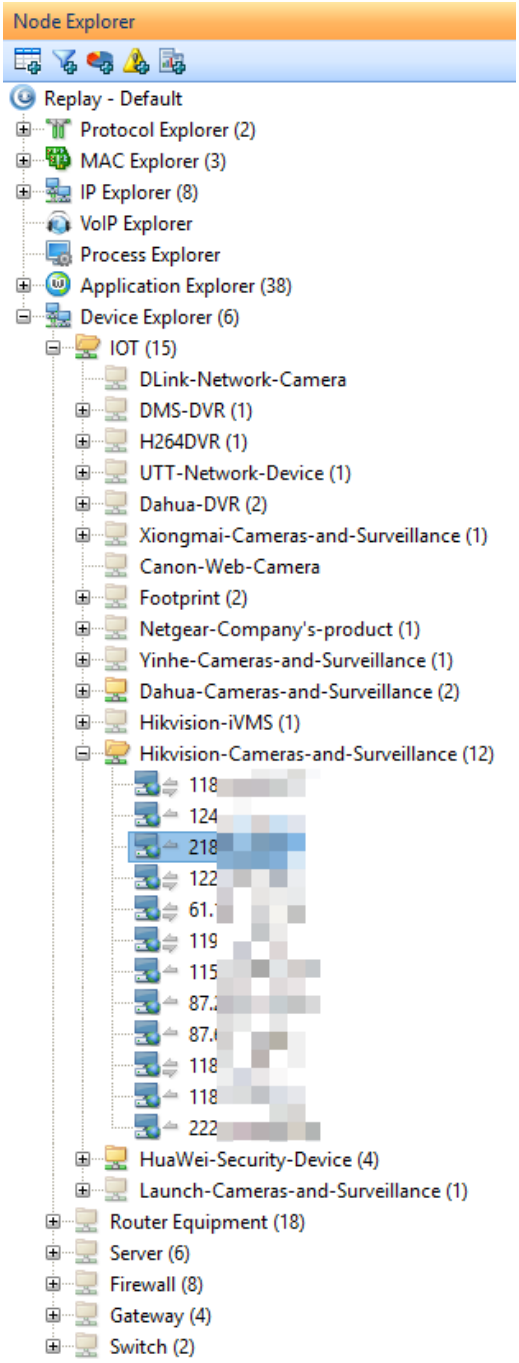
- Protocol Explorer
- MAC Explorer
- IP Explorer
- Process Explorer
- Application Explorer
- Device Explorer

Device Explorer

The **Device Explorer** groups all devices according device type or device name. All identified devices are displayed on the Device Explorer.

When a device is chosen on Node Explorer, the analysis views display analysis results only related to the chosen device.

Below is a screenshot of **Device Explorer**:



You can click a specific IP address, and the right pane displays statistics views only related to the IP.

Note Only when the Device IP Identification feature is enabled will there be Device Explorer in the Node Explorer window.

- Troubleshooting with Node Explorer

Note If user checks global display filter option in the Analysis Settings, the node explorer will not display.

Protocol Explorer

Protocol Explorer groups protocol nodes by protocol layer. All captured protocols are displayed in Protocol Explorer. You can right-click a father protocol node or a sub protocol node to make filter, graph, alarm, and report based on the protocol.

When a protocol node is chosen in Node Explorer, the analysis views display analysis results only related to the chosen protocol, and analysis views change along with different protocol selection. For example, when the protocol node "TCP" is chosen, the TCP Conversation view is available, but the UDP Conversation view is unavailable; when the protocol node "UDP" is chosen, the UDP Conversation view is available, but the TCP Conversation view is unavailable.

Tips The protocols that cannot be identified by Capsa will be displayed as *Other*.

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.

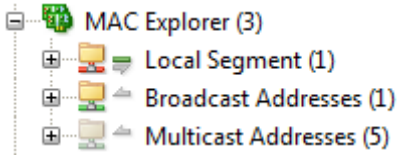
There are three types of icons in front of each protocol node. The red icon indicates there is data transmission in five seconds, the green icon indicates there is data transmission in thirty seconds, and the grey icon indicates there is no data transmission in thirty seconds.

MAC Explorer

MAC Explorer groups all MAC addresses. All captured MAC addresses are displayed in MAC Explorer. You can right-click a MAC node to make filter, graph, alarm, and report based on the MAC address, and to add it to Name Table.

When a MAC node is chosen in Node Explorer, the analysis views display analysis results only related to the chosen MAC.

Below is a screenshot of MAC Explorer:



There are three types of nodes in MAC Explorer: Local Segment, Broadcast Addresses and Multicast Addresses.

- Node "Local Segment" contains local MAC addresses. Sub-node "Local Host" contains MAC addresses that are defined in Node Group (see Node Group for details).
- Node "Multicast Addresses" contains multicast MAC addresses.
- Node "Broadcast Addresses" contains broadcast MAC addresses.

The number after each MAC address indicates the number of corresponding IP addresses.

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.

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.

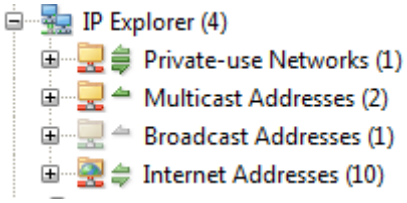
In front of arrow icons, there are icons indicating the address type of the node, indicating broadcast IP address, and indicating multicast IP address.

IP Explorer

IP Explorer groups all IP addresses. All captured IP addresses are displayed in IP Explorer. You can right-click an IP node to make filter, graph, alarm, and report based on the IP, and to resolve it or to add it to Name Table.

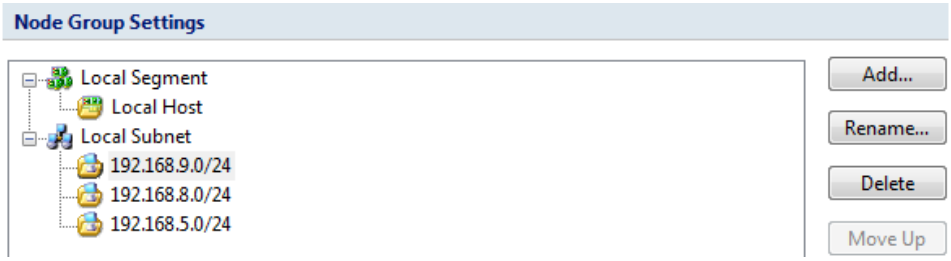
When an IP node is chosen in Node Explorer, the analysis views display analysis results only related to the chosen IP.

Below is a screenshot of IP Explorer:



In general, there are five types of nodes in IP Explorer: Local Subnet, Private-use Networks, Multicast Addresses, Broadcast Addresses, and Internet Addresses.

- Node "Local Subnet" contains IP addresses according to node group rules (see Node Group for details).



- Node "Private-use Networks" contains the private-use IP addresses that don't belong to any pre-defined node groups.
- Node "Multicast Addresses" contains multicast IP addresses.
- Node "Broadcast Addresses" contains broadcast IP addresses.
- Node "Internet Addresses" contains Internet IP addresses, which will be grouped by country if the option "Enable country group" is enabled.

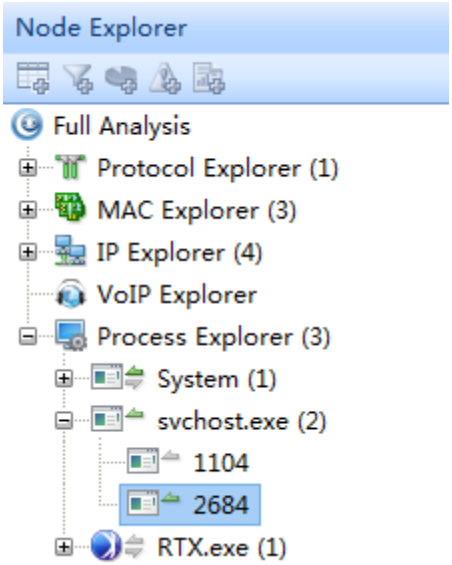
You can operate the nodes by keyboard: press UP arrow on the keyboard to select the upper node, down to select the lower node, LEFT to collapse the node, and Right to expand the node.

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.

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

Process Explorer

The **Process Explorer** groups all processes, listing the process name, process ID in a tree-like structure.

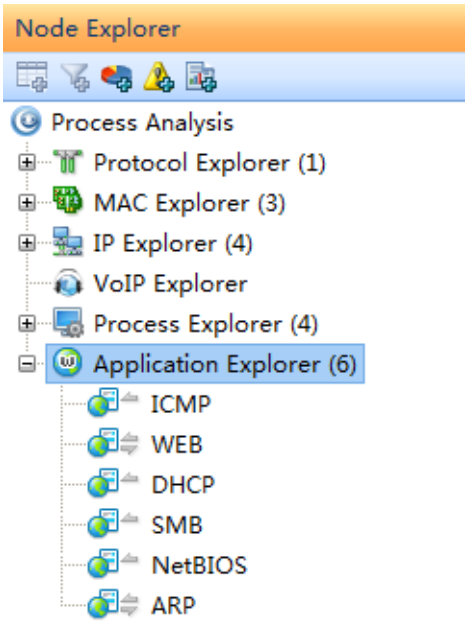


Selecting a specific node, a process name or a process ID, the statistical views on the right will display data only related to that node.

You can right-click a process name or a process ID to open the file location of that process.

Application Explorer

The **Application Explorer** groups all applications and listing the application name in a tree-like structure.



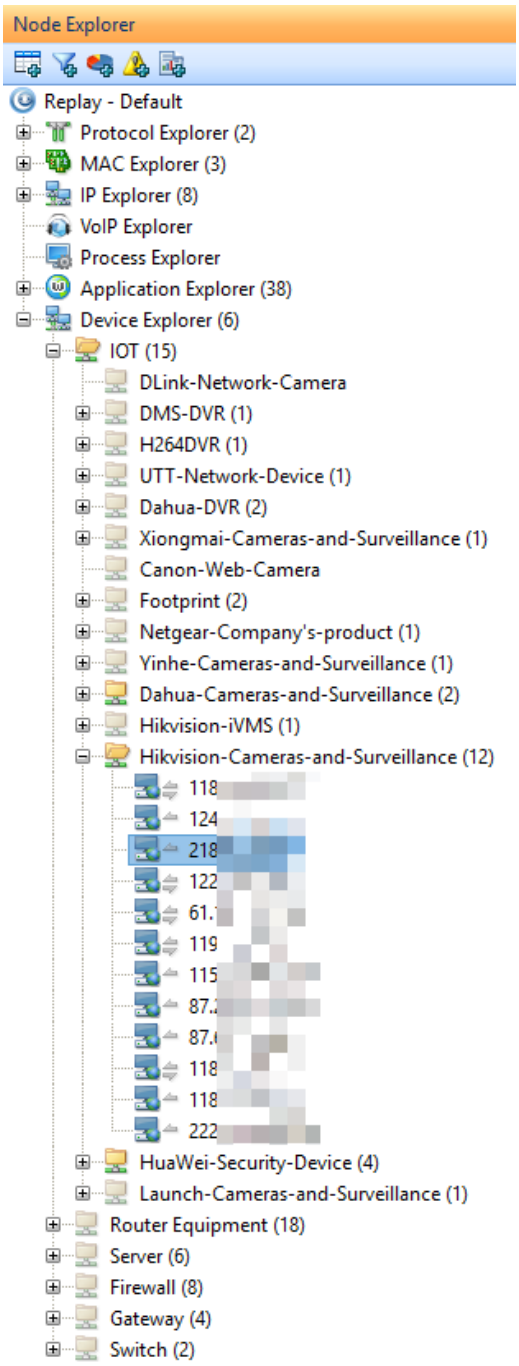
Selecting a specific node, an application name, the statistical views on the right will display data only related to that node.

Device Explorer

The **Device Explorer** groups all devices according device type or device name. All identified devices are displayed on the Device Explorer.

When a device is chosen on Node Explorer, the analysis views display analysis results only related to the chosen device.

Below is a screenshot of **Device Explorer**:



You can click a specific IP address, and the right pane displays statistics views only related to the IP.

Note Only when the Device IP Identification feature is enabled will there be Device Explorer in the Node Explorer window.

Troubleshooting with Node Explorer

Since Node Explorer functions as a display filter, it is helpful to use it for network troubleshooting.

Here is an example for using Node Explorer.

There are two top graphs on the Dashboard: Top IP by total traffic, and Top Protocols by bytes.

Double-click the largest item on the Top IP graph, you can locate the IP in Node Explorer, and in this way the analysis views display analysis results only for that IP. Then you can go to the Protocol view to see the top protocols for that IP.

In another way, double-click the largest item on the Top Protocols graph, you can locate the protocol in Node Explorer, and in this way the analysis views display analysis results only for that protocol. Then you can go to the IP Endpoint view to see the top IPs for that protocol.

Together with other features by Capsa, it is very convenient for network troubleshooting.

Statistics

Capsa provides a wide variety of statistics presented on the statistical views, each focusing on statistics of different types. Click following links to know details.

- Toolbar and pop-up menu
- Summary statistics
- Protocol statistics
- Port statistics
- Address statistics
- Conversation statistics
- Service statistics

In the toolbar, click the "Behaviour Analysis" button to open the application-related subview, which details the Behaviour, TCP conversation, UDP conversation, log and packets information of the selected service.

- Process statistics
- Application statistics
- Top domain statistics
- Viewing and saving statistics

Note In this chapter, all reference screenshots are from analysis interface without global displaying filter.

Toolbar and pop-up menu

The statistical views provide toolbars and pop-up menus to assist viewing and analysis. The items on toolbars and pop-up menus change along with the switch of statistical views, but toolbar and menu items of same icons/commands from different views function the same.

Toolbar items

The following list details all toolbar items for statistical views:

: Creates a new dashboard panel on the Dashboard view, or opens the **New Report** dialog box on the Report view.

: Renames a selected panel on the Dashboard view, or edits a selected report on the Report view.

: Deletes the selected item.

: Resets to default settings.

: Refreshes the display 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 the settings of selected diagnosis event. You can also view the settings of an event

by double-clicking the event.

 : Saves current statistical results.

 : Hides or shows the **Addresses** pane of the Diagnosis view.

 : Hides or shows the **Details** pane of the Diagnosis view.

 : Makes a packet filter based on the selected item.

 : Adds an alias to the **Name Table** for selected address.

 : Locates the selected item in the **Node Explorer** window.

 : Shows or hides the lower pane.

 : Shows the display in hierarchical type or in flat type.

 : Sets the font size of the nodes in the matrix graph.

 : To choose flow direction for displaying the data flow. **Bidirectional** indicates to display the whole data flow, **Node 1 to Node 2** indicates to display the data from node 1 to node 2, and **Node 2 to Node 1** indicates to display the data from node 2 to node 1.

 : Limits the first number of packets in the conversation to display on the **Data Flow** tab.

 : Configures the settings for the display.

 : **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.

 : Saves the data flow as a .txt file.

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

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

 : Deletes the selected matrix.

 : Resets the Matrix view to default settings.

 : 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.

 : Automatically scrolls down to display the newest data.

 : Displays items with specified filter.

At the top right corner of each statistical view, there is a statistical box which shows the statistical results of current view. The name of the statistical box changes along with the selection in the **Node Explorer** window.

Pop-up menus

When you right-click the statistical views, there is a pop-up menu. The pop-up menus from different views may include different command items. The following list describes all of the items.

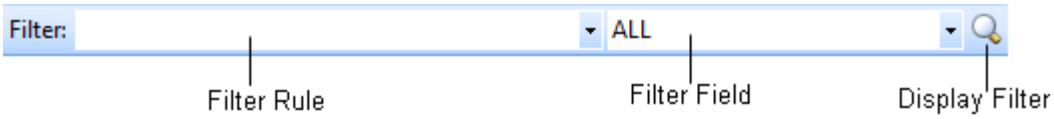
- **Copy**: Copies currently selected rows as well as the header row to the clipboard, or just copies current selection.
- **Copy Column**: Copies the selected column in original format to the clipboard.
- **Display Column**: Shows or hides columns or changes the position of columns. This command is just the same as right-clicking the column header.
- **Export Statistics**: Saves the statistical results of current view as a .csv file.
- **Find**: Calls out Find dialog box.
- **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 selected item.
- **Add to Name Table**: Adds an alias to the **Name Table** for selected address.
- **Make Graph**: Makes a graph in the **Dashboard** view on the basis of selected item.
- **Make Alarm**: Makes an alarm on the basis of selected item.
- **Locate in Node Explorer**: Locates the selected item in the **Node Explorer** window.
- **Select All**: Selects all items on the view.
- **Refresh**: Refreshes current view.
- **Packet Details**: Views the decoding information of the packets for selected item in the **Packet** window which is just the same as the **Packet** view.
- **Ping**: Calls out the build-in **Ping Tool** to ping the selected node.

Display Filter

Filters are utilized to separate particular packets. **Capture Filters** are utilized to restrict the packets into the buffer of a capture. However, **Display Filter** is utilized only to isolate particular records on the view to display. It matches the display keyword with the records on the list. Only matched records are displayed, and unmatched recorded are hidden until the display keyword is removed.

Capsa provides global display filter and classical display filter. For global display filter, please refer to Global Display Filter.

The classical **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.

To apply a display filter, just enter the filter rule, specify the filter field, and then click the Display Filter button.

For information about Capture Filter, please refer to Packet Analysis Filter.

Summary statistics

The Summary view provides summary statistics of current capture or replay. You can click the **Refresh** button to refresh current statistical results.

Different node selections in Node Explorer result in different statistics items. The Summary view displays statistical results only related to the node selected in Node Explorer.

- When the root node is selected, the Summary view provides all available statistics items for selected analysis settings.
- When a protocol node is selected, the Summary view provides Total Traffic and Packet Size Distribution statistics of the node.
- When a MAC address node is selected, the Summary view provides Traffic statistics, Conversation statistics and TCP statistics of the node, plus ARP Attack statistics when the Security Analysis be used.
- When an IP address node is selected, the Summary view provides statistics items changed along with the analysis settings.

When you monitor wireless network, statistics items of Wireless Analysis will be provided.

Furthermore, different analysis settings provide different statistics items. The following list describes all statistics items:

- Diagnosis
  Triggered event count of each diagnosis event type: Information Events, Notice Events, Warning Events, Error Events

- Wireless Analysis
  Wireless analysis traffic: Noise Traffic, Control Frame Traffic, Management Frame Traffic, Decrypted Data Frame Traffic, Unencrypted Data Frame Traffic, Encrypted Data Frame Traffic
  Noise Traffic means the traffic from other APs that using the same channel.
  Decrypted Data Frame Traffic means data frame traffic that is decrypted by Capsa.

Unencrypted Data Frame Traffic means data frame traffic that is not encrypted during the communication.
Encrypted Data Frame Traffic means data frame traffic that is not decrypted by Capsa.
Total traffic of monitored AP = Control Frame traffic + Management Frame Traffic + Data Frame Traffic

- Traffic
  List bytes, packets, utilization, average utilization, bps, average bps, pps (packets per second), and average pps of each traffic type: Total, Broadcast, Multicast, Average Packet Size.
  Over 50% of total traffic utilization: network may be overloaded
  Over 20% of broadcast or multicast traffic utilization: there is maybe broadcast/multicast storm and ARP attack
- Packet Size Distribution
  List byte, packet number, utilization, bps, packets per second of each packet size type: <58, 58-63, 64-127, 128-255, 256-511, 512-1023,1024-1518, 1519-1522, 1523-9018, 9019-9022, >9022
  Large portion of traffic at <=64 or >=1518: fragment attack or flood attack
- Address
  List the number of each address type: MAC Address, IP Address, Local IP Address, Remote IP address
  Abnormal large number: MAC flooding attack, TCP flooding attack, etc.
- Protocol
  List the number of total protocols and protocols of six layers: Total Protocols, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer
- Conversation
  List the number of four types of conversation: MAC Conversations, IP Conversations, TCP Conversations, UDP Conversations
- TCP
  List the number of TCP connection packets: TCP SYN Sent, TCP SYNACK Sent, TCP FIN Sent, TCP Reset Sent, and plus TCP SYN Received, TCP SYNACK Sent, TCP FIN Received and TCP Reset Received when an IP address node is selected in Node Explorer
  TCP SYN packets far more than TCP SYNACK packets: port scanning (TCP SYN flooding attack).
- Process
  Count of processes
- Application
  Count of application
- Alarm
  Triggered alarm count of each alarm type: Security Alarms, Performance Alarms, Fault Alarms
- DNS Analysis

Count of DNS queries and responses

- Email Analysis
  Count of SMTP and POP3 connections
- FTP Analysis
  Count of FTP upload and download activities
- HTTP Analysis
  Count of sent HTTP requests, received HTTP requests, and HTTP connections
- Security Analysis
  Count of each security attack: Worm, DoS Attacking, DoS Attacked, Suspect Conversation, TCP Port Scan, ARP Attack
- VoIP Call Statistics
  Count of each type of VoIP calls: SIP Calls, H.323 Calls, No Signaling Calls.

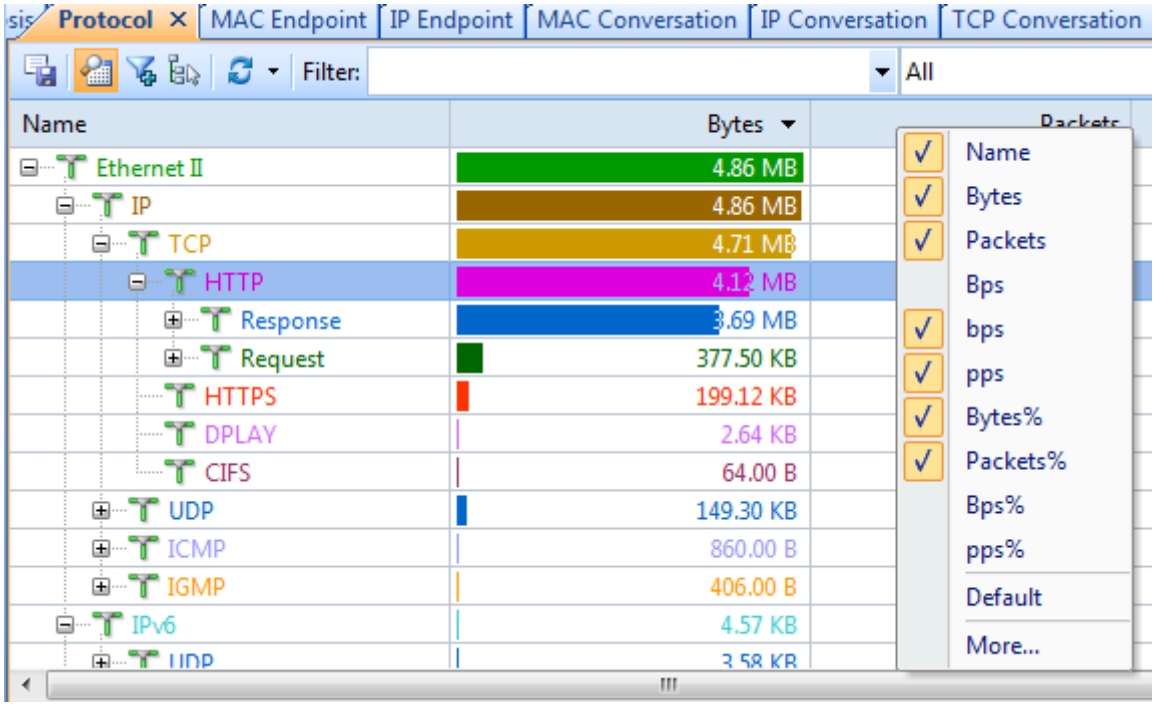
Note Wireless Analysis and Diagnosis Analysis are only available for Capsa Enterprise. Capsa Standard and Capsa Free do not provide such statistics.

Protocol statistics

The **Protocol** view visually provides statistics of the network traffic on the basis of protocols. Each protocol has its own color that you can easily find out your target protocol in the list by color.

By default, protocols are displayed in an expanded hierarchical structure. You can click the collapse/expand icon in front of a protocol to collapse/expand it.

You can click the column header to sort the list based on interested statistical field. Right-click 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 view columns for more information about the statistical fields for protocols.



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, **MAC 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 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 provide detailed information about the item. See Protocol view lower pane tabs for details. If the lower pane is invisible, you can click  to show it.

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.

Protocol view lower pane tabs

The Protocol view 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 hide it, and you can also click **Details** button to show the lower pane when it is invisible.

The tabs showing on the lower pane change along with the selection in the **Node Explorer** window:

- Choosing the root node or any nodes in **Protocol Explorer**, the lower pane includes **MAC Endpoint** tab, **IP Endpoint** tab and **Log** tab.
- Choosing any group nodes in **MAC Explorer**, the lower pane includes **MAC Endpoint** tab,

MAC Conversation tab and **Log** tab.

- Choosing MAC address nodes in **MAC Explorer**, the lower pane includes **MAC Conversation** tab, **IP Conversation** tab and **Log** tab.
- Choosing any nodes except IP address nodes in **IP Explorer**, the lower pane includes **IP Endpoint** tab, **IP Conversation** tab and **Log** tab.
- Choosing IP address nodes in **MAC Explorer** or **IP Explorer**, the lower pane includes **IP Conversation** tab, **TCP Conversation** tab, **UDP Conversation** tab and **Log** tab.

You can double-click any item on the lower pane tabs to view detailed packet information in the **Packet** window which is just the same as the **Packet** view.

Following list describes the lower tabs whatever the selection in Node Explorer is:

- The **MAC 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 **MAC Endpoint** view.
- 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.
- The **MAC 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 **MAC Conversation** view.
- 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.
- The **TCP Conversation** tab lists the conversations using TCP protocol. The toolbar and columns are just the same as those on **TCP Conversation** view.
- The **UDP Conversation** tab lists the conversations using UDP protocol. The toolbar and columns are just the same as those on **UDP Conversation** view.
- The **Log** tab list all the log information about the selected protocol on the **Protocol** view. The toolbar and columns are just the same as those on **Log** view.

In combination with Node Explorer, you can conveniently view the statistics that you are interested in.

Protocol view columns

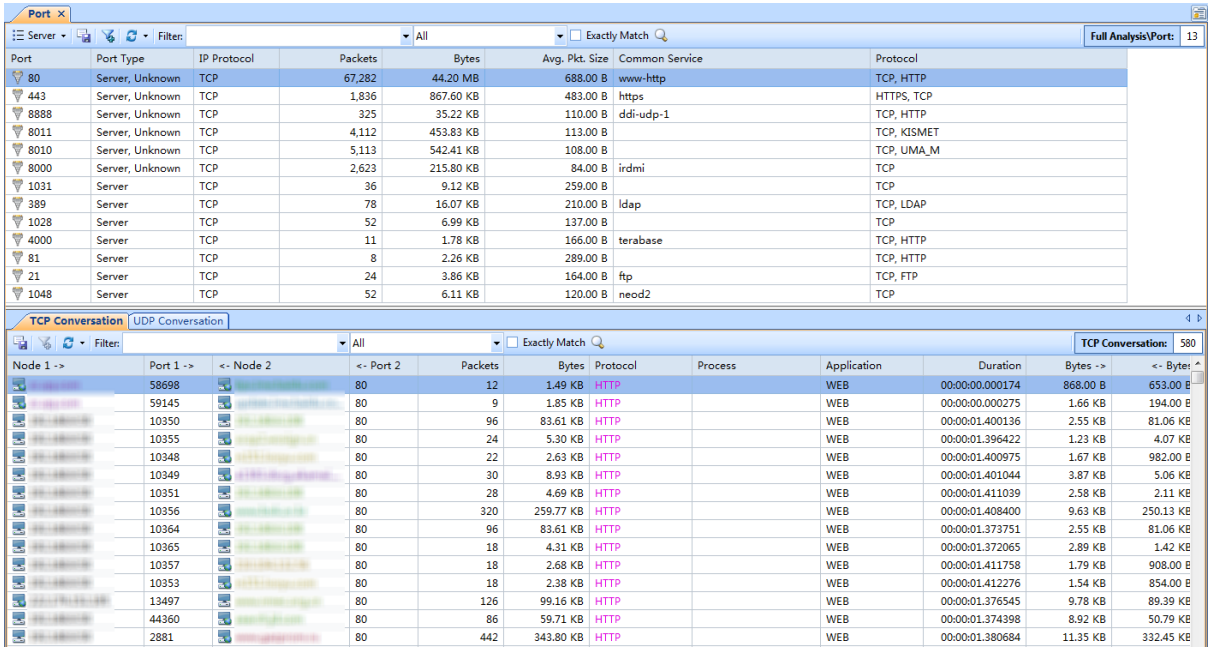
The following table lists and describes the columns of **Protocol** view.

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.

Port statistics

Capsa provides a **Port** view to display port statistics based on TCP/UDP protocols.



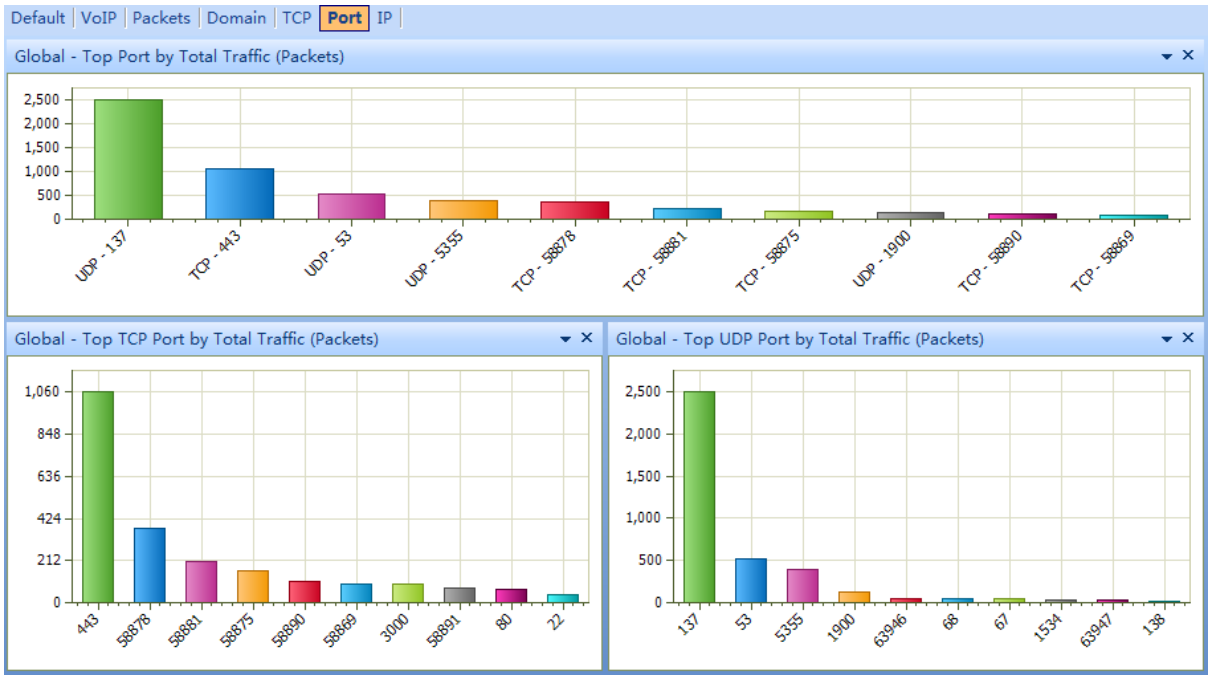
The Port view includes an upper pane to display port number records and a lower pane to display conversation information for the record selected on the upper pane.

You can click the column **Port** to display the statistics based on top ports. You can also click another column header to sort the list based on interested statistical field. To know details about each columns, see Protocol view columns.

When a specific record on the Port view is selected, the lower pane provides detailed information about the record. The lower pane includes two tabs: TCP Conversation and UDP Conversation, which are respectively the same to TCP Conversation view and UDP Conversation view.

If the IP protocol for a port is TCP, there will be TCP conversations on the lower pane, and you can double-click the TCP conversations to view analyze the TCP flow; if the IP protocol for a port is UDP, there will be UDP conversations on the lower pane. If a port adopts both UDP and TCP protocols, there will be two records on the Port view.

Besides the Port view, Colasoft provides three top charts on the Dashboard view for port statistics: Top Port by Total Traffic, Top TCP Port by Total traffic, Top UDP Port by Total traffic. The statistical unit could be Packets or Bytes.



Top port charts could be top 5, top 10 and top 20, just as other top charts.

Port view columns

The following table lists and describes the columns for the Port view.

Column	Description
Port	The port number for communication.
IP Protocol	The protocol that is adopted by the port for communication. It could be UDP or TCP.
Packets	The number of packets for the port.
Bytes	The traffic for the port.
Avg. Pkt. Size	The average packet length of the packets for the port.

Common Application	Common applications that use the port for communication. If no common application, it displays "Unknown".
Protocol	The protocol that is adopted by the port for communication on the transport and application layer.

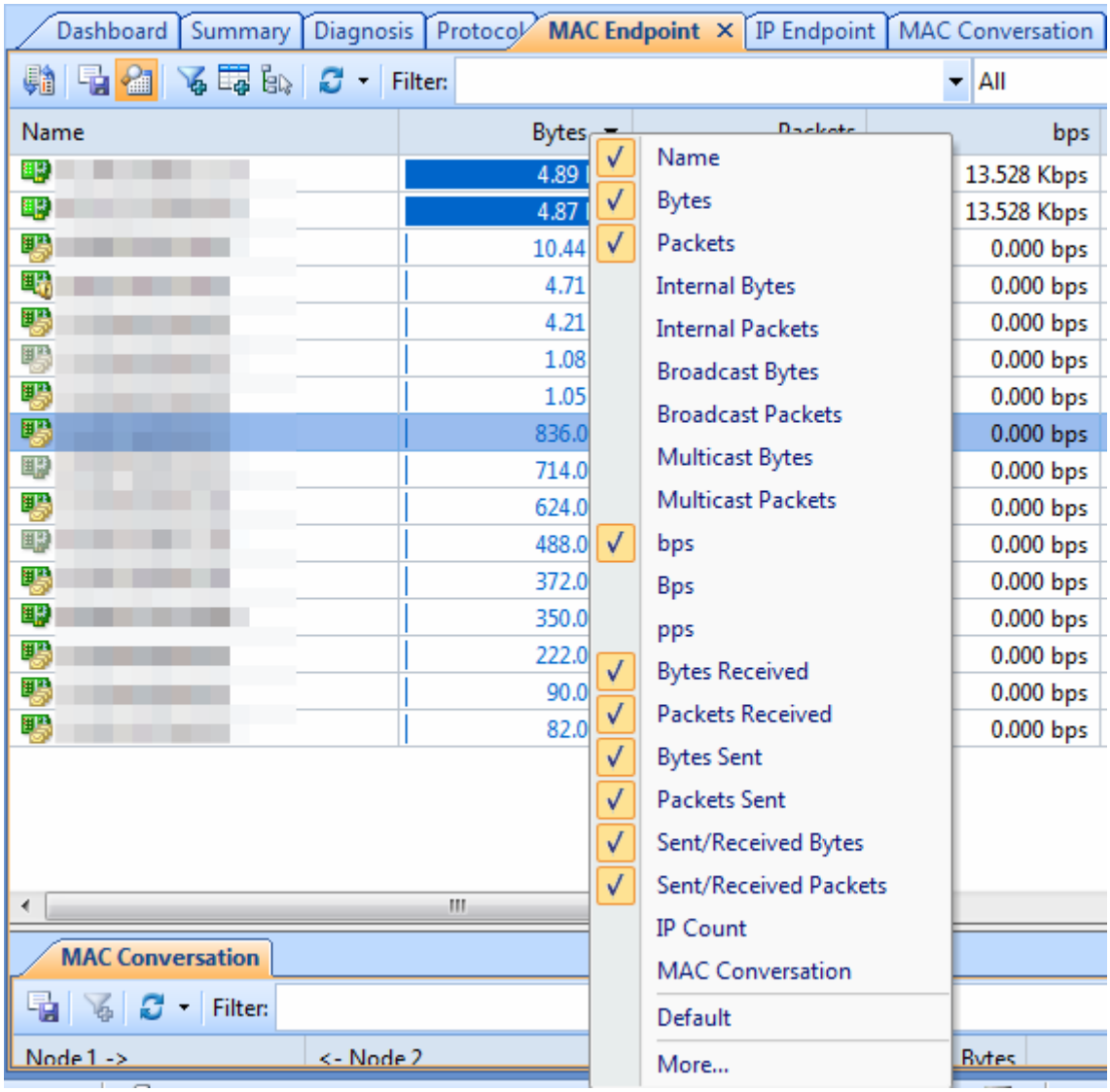
Address statistics

There are two types of address statistics: MAC address statistics and IP address statistics, which are respectively available from the MAC Endpoint view and IP Endpoint view.

Note The **MAC Endpoint** view will not be available when you select IP address nodes in **MAC Explorer** or any nodes in **IP Explorer**. The **IP Endpoint** view will not be available when you select node group or MAC address in **MAC Explorer**.

By default, addresses are displayed in an expanded hierarchical structure. You can click the button  to display them in flat/hierarchical type.

You can click any column header to sort the list based on interested statistical field. Right-click 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 view columns for more information about the statistical fields for addresses.



When you select a specific item in endpoint views, the lower pane tabs will provide detailed information about the item. See MAC Endpoint view lower pane tabs and IP Endpoint view lower pane tabs for details. If the lower pane is invisible, you can click  to show it.

You can double-click an item in the endpoint views to view detailed packet information in the Packet window which is named with the node and is just the same as the Packet view.

MAC Endpoint view lower pane tab

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

The **MAC Endpoint** lower pane contains MAC Conversation tab and **Log** tab.

The **MAC Conversation** tab lists all MAC conversations of the node selected on the **MAC Endpoint** view. The toolbar and columns are just the same as those on **Log** view.

The **Log** tab list all the log information of the node selected no the MAC Endpoint view. The toolbar and columns are just the same as those on **Log** view.

You can double-click any item on the lower pane tabs to view detailed packet information in the **Packet** window which is just the same as the **Packet** view.

IP Endpoint view lower pane tabs

The **IP Endpoint** view 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 contains **IP Conversation** tab, **TCP Conversation** tab, **UDP Conversation** tab and **Log** 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.
- 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.
- 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.
- The **Log** tab lists the log information of the node selected on the **IP Endpoint** view. The toolbar and columns are just the same as those on **Log** view.

You can double-click any item on the lower pane tabs to view detailed packet information in the **Packet** window which is just the same as the **Packet** view.

Endpoint view columns

The following table lists and describes the columns for endpoint views, including **MAC 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.

Column	Description
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.
Average bps	Average bits per second. Average bps = Bytes *8 /the time interval from the last packet to the first packet of that endpoint.
Bps	Bytes per second.
Average Bps	Average bytes per second. Average Bps = Bytes /the time interval from the last packet to the first packet of that endpoint.
pps	Packets per second.
Average pps	Average packets per second. Average pps = Packets /the time interval from the last packet to the first packet of that endpoint.
Bytes Received	Received bytes.
Packets Received	Received packets.
Bytes Sent	Sent bytes.
Packets Sent	Sent packets.

Column	Description
Sent / Received Bytes	The ratio of sent bytes to received bytes.
Sent / Received Packets	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.
MAC Conversation	The number of MAC 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 Received	The number of received packets with ACK and SYN flags both set to be 1. The value of this item should be 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 RST Sent	The number of sent packets with RST flag set to be 1.

Column	Description
TCP RST 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 Received %	Percentage of received bytes.
Packets Received %	Percentage of received packets.
Bytes Sent %	Percentage of sent bytes.
Packets Sent %	Percentage of sent packets.
bps%	Percentage of bits per second.
Bps%	Percentage of bytes per second.
pps%	Percentage of packets per second.
Broadcast pps	Broadcast packets per second.
Multicast pps	Multicast packets per second.
Received Bps	Bytes received per second.

Column	Description
Received pps	Packets received per second.
Sent Bps	Bytes sent per second.
Sent pps	Packets sent per second.
TCP SYN Sent pps	Packets with SYN flag set to be 1 send per second.
TCP SYN Received pps	Packets with SYN flag set to be 1 received per second.

Conversation statistics

There are four types of conversation statistics: MAC conversation, IP conversation, TCP conversation, and UDP conversation, which are respectively available on the MAC Conversation view, IP Conversation view, TCP Conversation view, and UDP Conversation view.

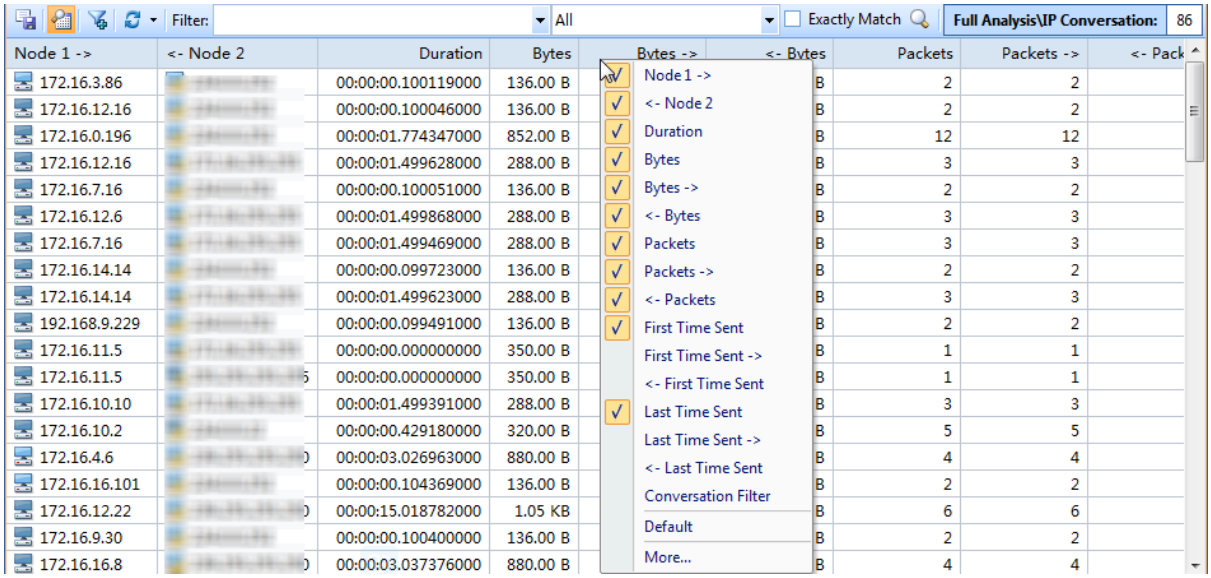
The MAC Conversation view shows statistics of network communication between two MAC addresses.

The IP Conversation view shows statistics of network communication between two IP addresses.

The TCP Conversation view shows statistics of network communication based on TCP protocols.

The UDP Conversation view shows statistics of network communication based on UDP protocols.

You can click any column header to sort the list based on interested statistical field. Right-click 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 view columns for details.



When you are viewing statistics in the MAC Conversation view, IP Conversation view and UDP Conversation view, you can double-click an item to view detailed packet information for selected conversation.

When you are viewing statistics in the TCP Conversation view, you can double-click an item to make further analysis. See TCP Flow Analysis window for details.

When you select a specific item in the IP Conversation view, the lower pane displays detailed information about the selected item. See IP Conversation view lower pane tabs for details. If the lower pane is invisible, you can click  to show it.

When you select a specific item in the TCP Conversation view, the lower pane displays three tabs for the selected TCP flow. For more information, please refer to TCP Flow Analysis.

When you select a specific item in the UDP Conversation view, the lower pane displays detailed information about the selected item. See UDP Conversation view lower pane tabs for details.

IP Conversation view lower pane tabs

The **IP Conversation** view 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, **UDP Conversation** and **Log** 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.

- 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.
- The Log tab list all the log information of the node selected no the MAC Endpoint view. The toolbar and columns are just the same as those on **Log** view.

You can double-click any item on the lower pane tabs to view detailed packet information in the **Packet** window which is just the same as the **Packet** view.

UDP Conversation view 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 **UDP Conversation** view to close it, and you can also click **Details** button to show the lower pane when it is invisible.

The **UDP Conversation** view lower pane includes **Packets** tab, **Data Flow** tab, **Time Sequence** tab and **Log** 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. You can double-click any item on the lower pane tabs to view detailed packet information.
- The **Data** tab provides original data for the UDP conversation selected in the **UDP Conversation** view.
- The **Time Sequence** tab provides the time sequence chart about the **UDP conversation** which is using DNS Protocol.
- The **Log** tab list all the log information of the node selected no the **UDP Conversation** view. The toolbar and columns are just the same as those on **Log** view.

By default, the **Data** tab shows the whole data 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.

You can also click the button  to show only data from node 1 to node 2 or from node 2 to node 1.

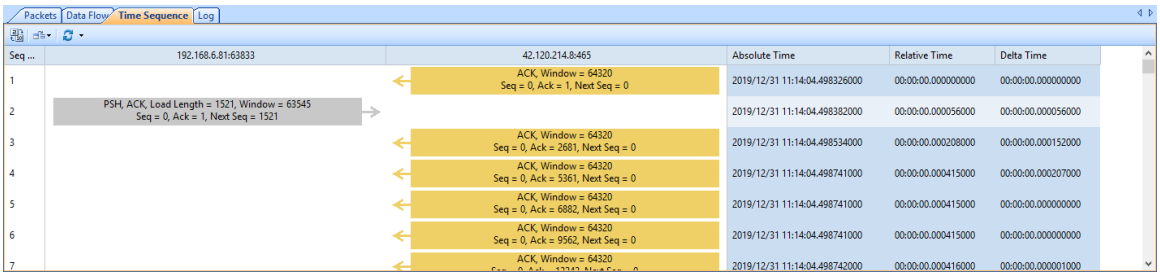
When there are a lot of packets for a UDP conversation, you can click  to just show the data of the first 50, or 100 packets.

If you are interested in the data flow, you can click  to save the data.

If you want to display the data flow in other formats, you can right-click, select **Decoding**, and then click the interested format.

DNS Time Sequence

For the UDP conversation which is using DNS protocol, according to the communication sequence, Capsa can print out the time sequence chart as following:



Conversation view columns

The following table lists and describes the columns of **Conversation** view, including **MAC 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.

First Time Sent	The timestamp of the first packet in the conversation.
First Time Sent ->	The timestamp of the first packet that is sent from node 1 to node 2.
<- First Time Sent	The timestamp of the first packet that is sent from node 2 to node 1.
Last Time Sent	The timestamp of the last packet in the conversation.
Last Time Sent ->	The timestamp of the last packet that is sent from node 1 to node 2.
<- Last Time Sent	The timestamp of the last packet that is sent from node 2 to node 1.
Protocol	The protocol for the conversation.
Process	The process for the conversation.
Application	The application for the conversation. This column is only available for TCP Conversation view and UDP Conversation view.
Port 1 ->	The port number of the conversation for node 1.
<- Port 2	The port number of the conversation for node 2.
Payload	The total payload length of the conversation.
Payload ->	The payload length sent from node 1.
<- Payload	The payload length sent from node 2.
Interaction Diagram	The TCP interaction diagram of the conversation.
Transport Layer Max ACK Time	The maximum one of all the ACK time of the conversation.
Conversation Filter	The name of the conversation filter enabled.

Service statistics

The service view counts and analyzes the communication status of each service according to various parameters such as IP address, port, geographic location, data packet, number of bytes, and load. You can learn the communication status of each service in detail.

1.Toolbar

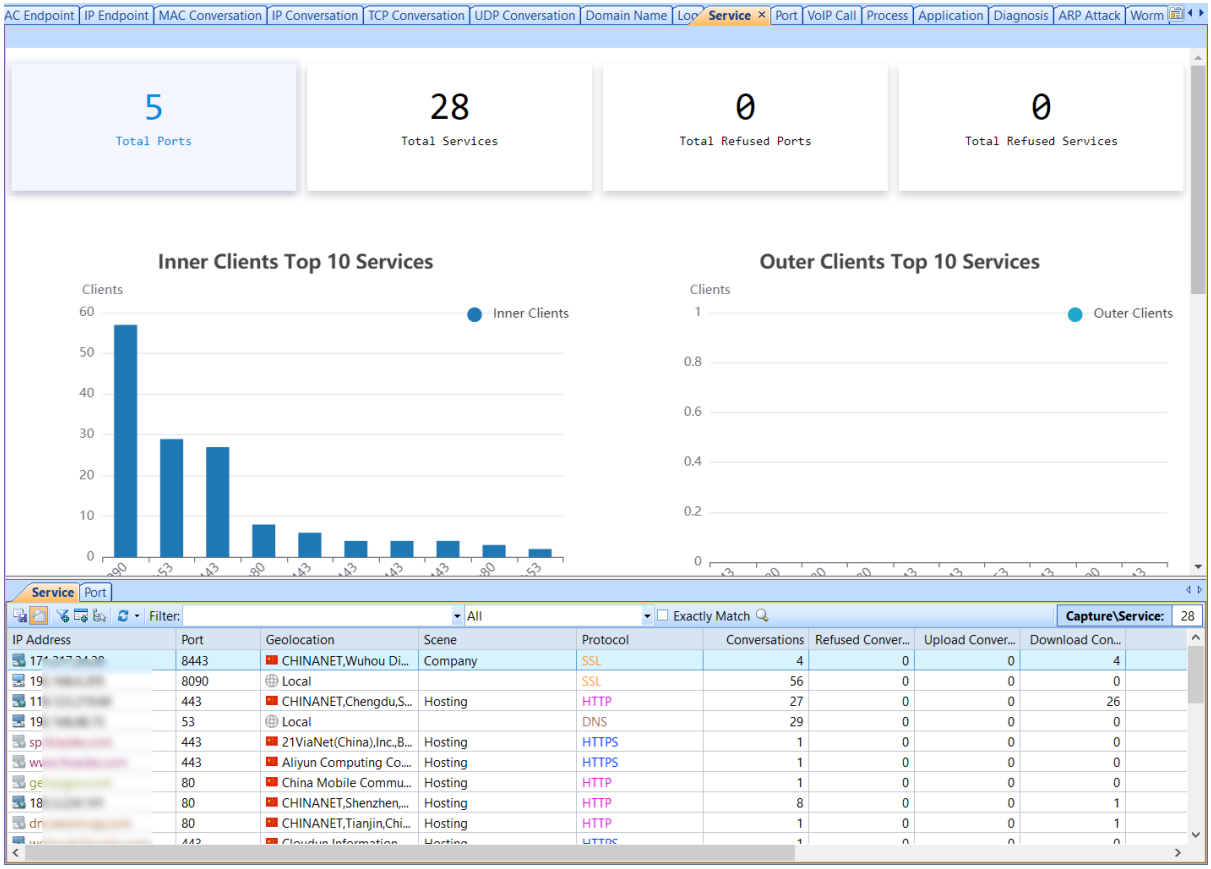
The application view toolbar is shown below:

The toolbar's functions are shown from left to right in the following table:

Function Name	Description
Export	Export all the data in the display area and save it to local disk in CSV format for viewing and saving as history record.
Details	Hide or display application-related protocols, TCP, UDP windows.
Make Filter	Select a specific node to add it to the filter to generate a new filter.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.
Locate in Node Explorer	Select a specific node, click this button, directly locate the node in the node browser, and view other details of the node.
Flash	Set the view refresh interval.
Filter	Filter the condition input, you can enter any condition to quickly find the data.
All	Specific parameters can be specified in this drop-down menu to help you find data faster and improve search efficiency.
Exactly Match	A full-word match means that the search result will be displayed more accurately when it encounters a word that exactly matches the search criteria. The system does not enable full word matching by default.

2.Service statistics list

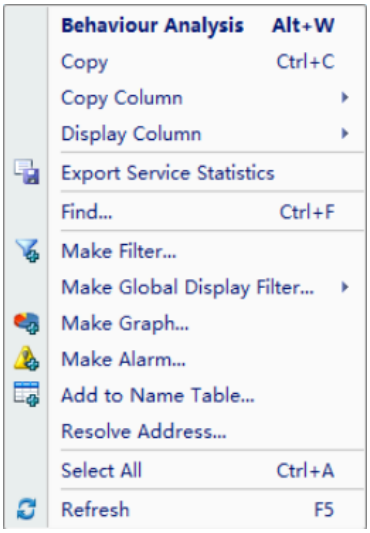
The service statistics list view is shown below:



The service view details the communication status of each service. In the sub-window of the view, the association displays the TCP and UDP session information included in the currently selected service.

Tips Select the field column and right-click or directly click on the custom column in the context menu. You can select more fields you want to view and select Reset to return to the default settings.

Service statistics support the right-click menu function, as shown below:



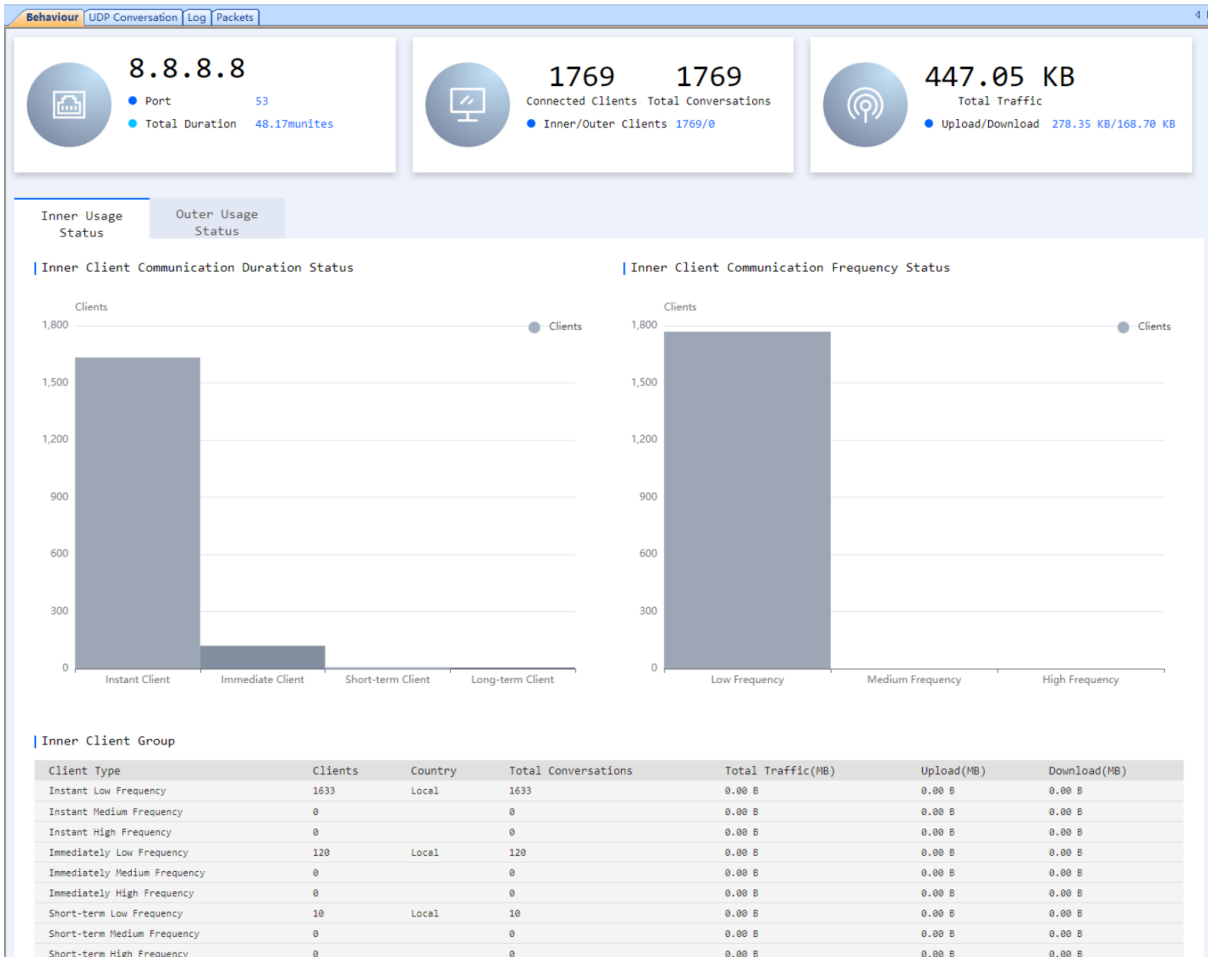
The specific functions are as follows:

Function Name	Description
Behavior Analysis	View Behavior, TCP conversation, UDP conversation, log and packets information in a new window.
Copy	Copy the information in a selected session list.
Copy column	Select to copy a field, such as Node1, Node2, Packet Number, etc.
Display column	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Export Service Statistics	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Find	Enter to search the session you want. Support Fuzzy Search and Search Statistics.
Make filter	Select a specific node to add it to the filter to generate a new filter.
Make Graph	Select a specific node or segment to add it to the chart view and generate a new chart to help view the analysis.
Make Alarm	Select a specific node or network segment to add it to the Alerts view to generate new alerts to help you discover new issues in your network in a timely manner.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.
Resolve address	By proactively parsing the session you selected, you can get the IP address of the node to accurately determine which host on the network this IP node is.
Locate in Node Explorer	After clicking, the system automatically selects the current application in the application node browser.
Select All	Check all apps in the statistics list.

Refresh	Refresh the session statistics list.

3. Pop-up window display area

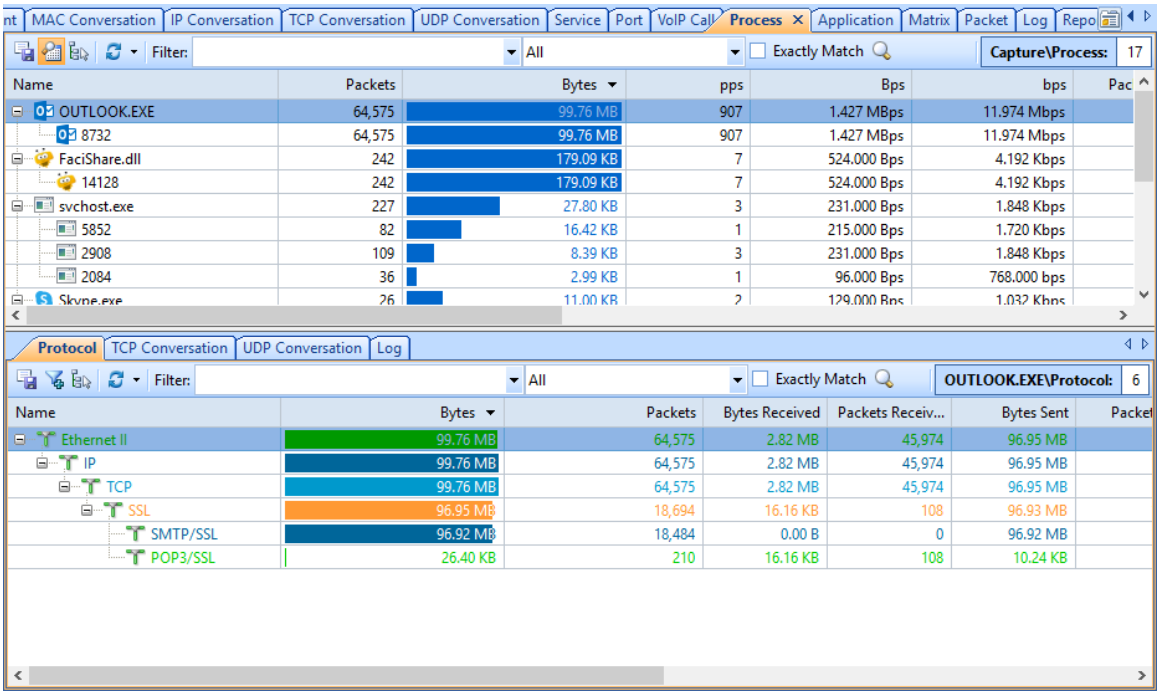
The pop-up window display area interface is shown below:



In the toolbar, click the "Behaviour Analysis" button to open the application-related subview, which details the Behaviour, TCP conversation, UDP conversation, log and packets information of the selected service.

Process statistics

The Process view provides traffic statistics for local processes, including total bytes, packets, Bps, bps, pps, path, etc. The screenshot below shows the Process view:

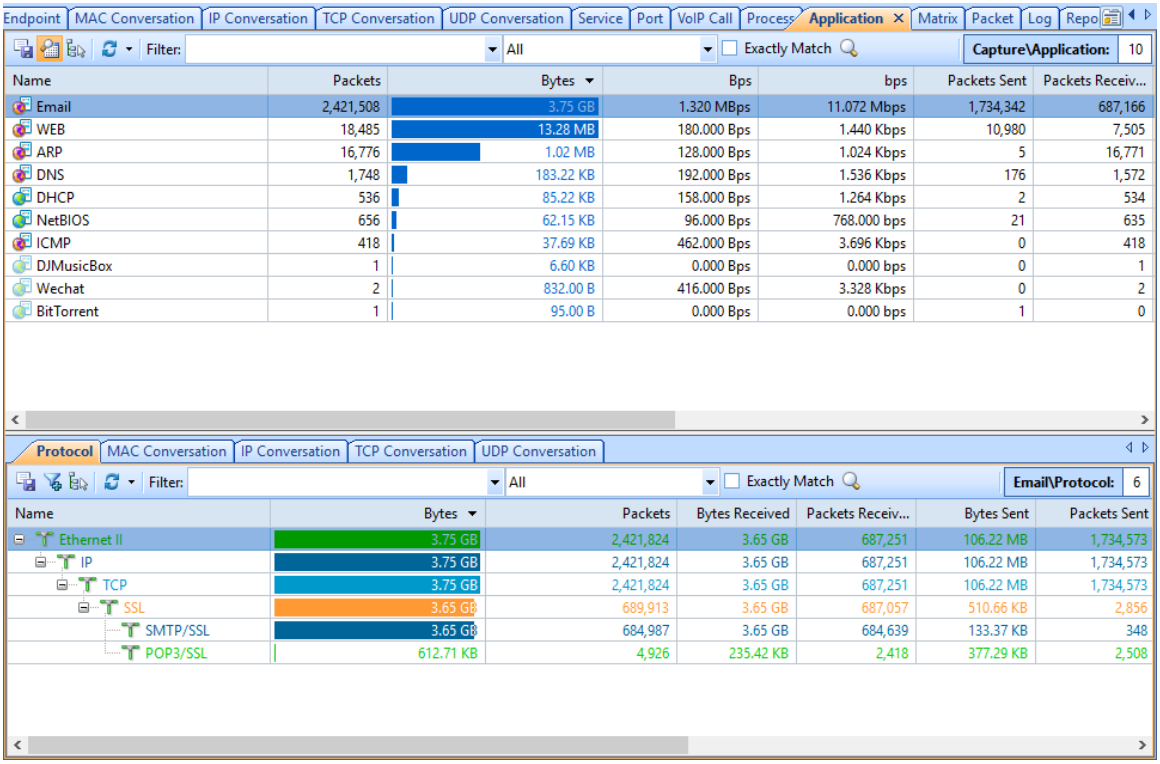


You can double-click an item to show all packets for that process.

When selecting a specific item, the lower tabs will show related protocol, related conversation information and related log information for that item. Furthermore, a Process column is provided for TCP Conversation view and UDP Conversation view to show the process name of that TCP/UDP conversation, which helps users troubleshoot quickly. You can also go the Dashboard view to see the top processes based on network traffic.

Application statistics

The Application view provides traffic statistics for applications, including total bytes, packets, Bps, bps, pps, etc. The screenshot below shows the Application view:



You can double-click an item to show all packets for that application.

When selecting a specific item, the lower tabs will show the related protocol or conversation information for that item. Furthermore, an Application column is provided for TCP Conversation view and UDP Conversation view to show the application name of that TCP/UDP conversation, which helps users troubleshoot quickly. You can also go the Dashboard view to see the top applications based on network traffic.

Top domain statistics

Capsa provides a Top Domain Name chart to display top domain statistics. The Top Domain Name chart displays the most visited domain names. It could be Top 5, Top 10, or Top 20.

If the Top Domain Name chart is invisible or you want to show it to another dashboard panel, you can add it manually. First select a proper dashboard panel (you can create a new panel or select an existing panel), and then add the domain chart (see Creating graph to know how to create a chart).

Domain name

The domain name view analyzes and displays the communication information of the IP addresses corresponding to the domain names in the network. For the IP address under each domain name, statistical parameters such as the number of IP conversations, the number of TCP conversations, the number of UDP conversations, the number of packets, the packets sent and received, and the size of the packets can be counted. At the same time, the IP conversations, TCP conversations and UDP conversations associated with the currently selected domain name will be displayed in the sub-window below. Through these conversation information, users can quickly understand the status of domain name conversations in the current network.

The domain name view toolbar is as shown below:

The functions on the toolbar of the domain name view are shown in the following table:

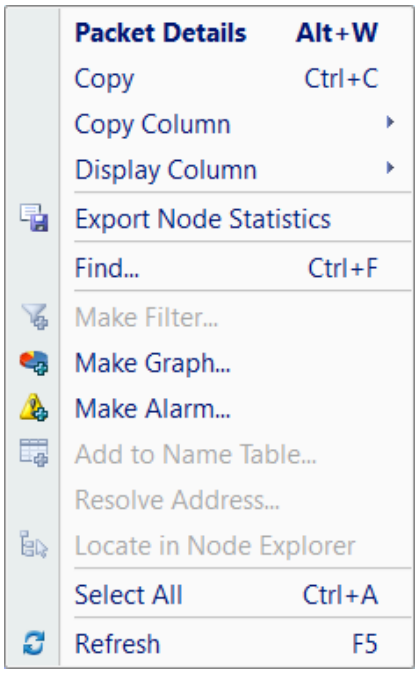
Function Name	Description
Export	Export all the data in the display area and save it to local disk in CSV format for viewing and saving as history record.
Details	Hide or display domain name-related protocols, TCP, UDP windows.
Make Filter	Select a specific node to add it to the filter to generate a new filter.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.
Expand All	All expand/contract all nodes in the domain name view.
Refresh	Set the view refresh interval.
Filter	Filter the condition input, you can enter any condition to quickly find the data.
All	Specific parameters can be specified in this drop-down menu to help you find data faster and improve search efficiency.
Exactly Match	A full-word match means that the search result will be displayed more accurately when it encounters a word that exactly matches the search criteria. The system does not enable full word matching by default.

The domain name statistics view is shown in the figure below:

Name	IP Count	Geolocation	IP Conversation	TCP Conversati...	UDP Conversati...	Packets
googleads.g.doubleclick.net	1					
12	-	Local	1	1	0	37
ss1.b	1					
18	-	Chengdu,Sichuan,China	-	-	-	-
hm.b	1					
11	-	Local	1	1	0	18
static kypeasset...	1					
19	-	Local	1	1	0	5
dss1.l	2					
11	-	Nanchong,Sichuan,Chi...	-	-	-	-
18	-	Chengdu,Sichuan,China	-	-	-	-
www	2					
39	-	Local	1	3	0	130
39	-	Local	1	1	0	27
hectc com	3					
11	-	Local	1	1	0	19
11	-	Chengdu,Sichuan,China	-	-	-	-
11	-	Luzhou,Sichuan,China	-	-	-	-
sp0.b	2					
39	-	Local	1	3	0	130
39	-	Local	1	1	0	27
sp1.b	2					
39	-	Local	1	3	0	130

The domain name view counts the communication status of the IP address corresponding to the domain name in the network. In the sub-window of the view, the IP conversation, TCP conversation and other information corresponding to the currently selected domain name are displayed. Through this information, we can determine the communication status of the domain name in the current network.

Domain name statistics support the right-click menu function, as shown in the figure below:



The specific functions are shown in the following table:

Function Name	Description
Behavior Analysis	View Behavior, TCP conversation, UDP conversation, log and packets information in a new window.
Copy	Copy the information in a selected session list.
Copy column	Select to copy a field, such as Node1, Node2, Packet Number, etc.
Display column	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Export Service Statistics	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Find	Enter to search the session you want. Support Fuzzy Search and Search Statistics.
Make Filter	Select a specific node to add it to the filter to generate a new filter.
Make Global Display Filter	Select a specific IP address to add it to the global display filter to generate a new global display filter.
Make Graph	Select a specific node or segment to add it to the chart view and generate a new chart to help view the analysis.
Make Alarm	Select a specific node or network segment to add it to the Alerts view to generate new alerts to help you discover new issues in your network in a timely manner.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.

Resolve address	By proactively parsing the session you selected, you can get the IP address of the node to accurately determine which host on the network this IP node is.
Select All	Check all apps in the statistics list.
Refresh	Refresh the session statistics list.

Viewing and saving statistics

There are some tips for you to view statistics:

- You can click interested statistical field on the column header to sort the statistical results according to that field.
- Right-clicking on the column header allows you to show/hide statistical fields.
- Double-clicking an item usually will bring up the Packet view to show packet details for the selected item.
- Right-click an item, you can make a filter, make a graph, and make an alarm based on the selected item, and locate the item in Node Explorer.

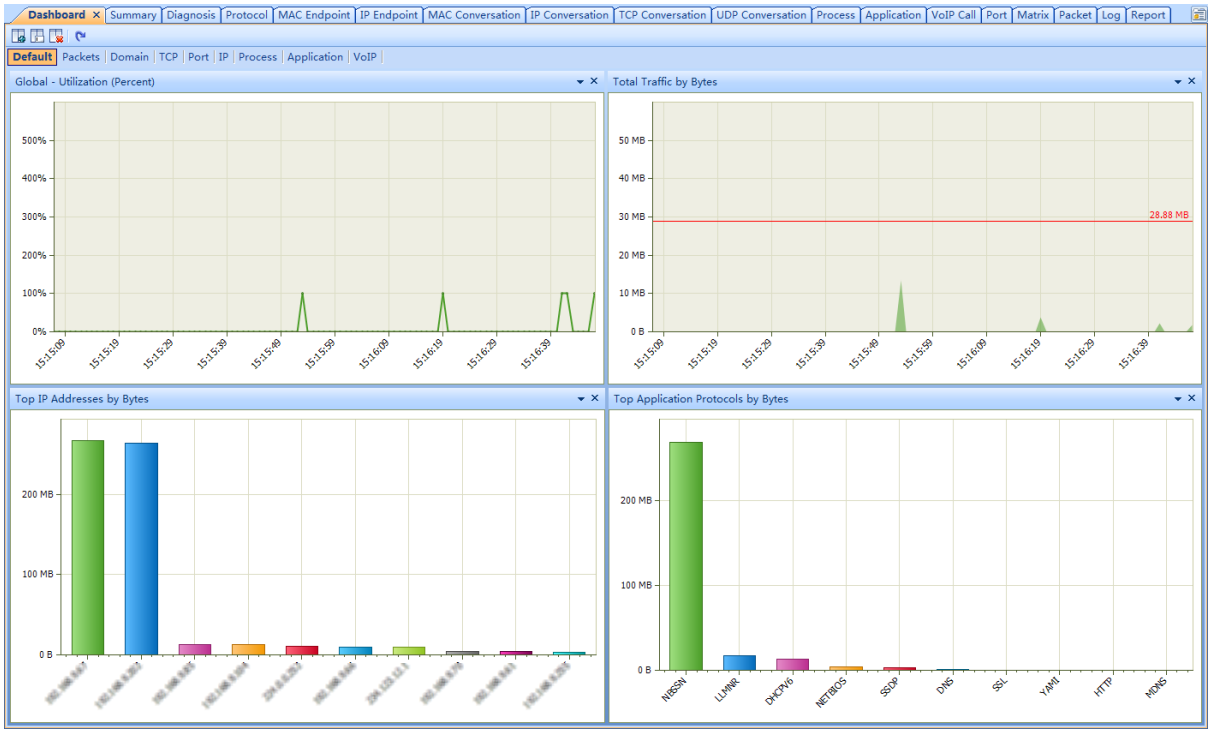
To save the statistics, just click the save button  . All statistics views except the Summary view are provided with the save button for you to save the statistics of current display.

Dashboard

The Dashboard view

The Dashboard view dynamically displays statistics with various charts.

By default, the Dashboard view provides eight dashboard panels, as the figure below:



If the dashboard panel "Wireless" is invisible, please click to show it.

Please note that the dashboard panel "Wireless" is only available when you monitor a WiFi network, and the "VoIP" panel is only available when the VoIP analysis module is enabled.

You can click the dashboard panel name to view other graphs and charts.

Besides the default dashboard panels, you can click to add new dashboard panels. Each dashboard contains one to four charts. If you want to view more charts, you can add new ones (see Creating graph to learn how to create a chart).

The Dashboard view is visible only when the root node of the **Node Explorer** window is 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).

The charts on the Dashboard view dynamically refresh according to sample interval or refresh interval. There are two types of charts in Capsa: Sample Chart and Top Chart. Sample charts automatically refresh according to sample interval, and top charts automatically refresh according to refresh interval. The intervals can be defined by users. Just right-click the chart and choose the proper interval.

Right-click sample charts to get a pop-up menu with items as follows:

- **Pause Refresh**: Pauses the display refresh of the chart.
- **Legend Box**: Whether and where to show legend box
- **Line Chart**: Displays the chart in line chart.
- **Area Chart**: Displays the chart in area chart.
- **Titles**: Shows the title of the chart, the title of X axis, and the title of Y axis.
- **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 of the chart.
- **Save Graph**: Saves the current graph to disk. You can save graphs in .png, .emf, and .bmp formats.

Right-click top charts to get a pop-up menu with items as follows:

- **Pause Refresh**: Pauses the display refresh of the chart.
- **Legend Box**: Whether and where to show legend box
- **Bar Chart**: Displays the chart in bar chart.
- **Pie Chart**: Displays the chart in pie chart.
- **Titles**: Shows the title of the chart, the title of X axis, and the title of Y axis.
- **Top Number**: Displays the top number of statistical items on the chart. It could be Top 5, Top 10, and Top 20.
- **Sample Value**: Sets the statistic value type. **Cumulative Value** means the statistics for chart items are calculated from the start of the capture and **Last Second Value** means the statistics are calculated for last second.
- **Refresh Interval**: Sets the refresh interval of the chart.
- **Save Graph**: Saves the current graph to disk. You can save graphs in .png, .emf, and .bmp formats.

Position of a chart is changeable. You can click and drag chart title bar to rearrange its position to get a better view.

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

Creating graph

Before creating a graph, you need to specify which dashboard panel to contain the graphs. To create a new dashboard panel, click  .

You can customize statistical graphs based on from global network to a specific node, including a 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:

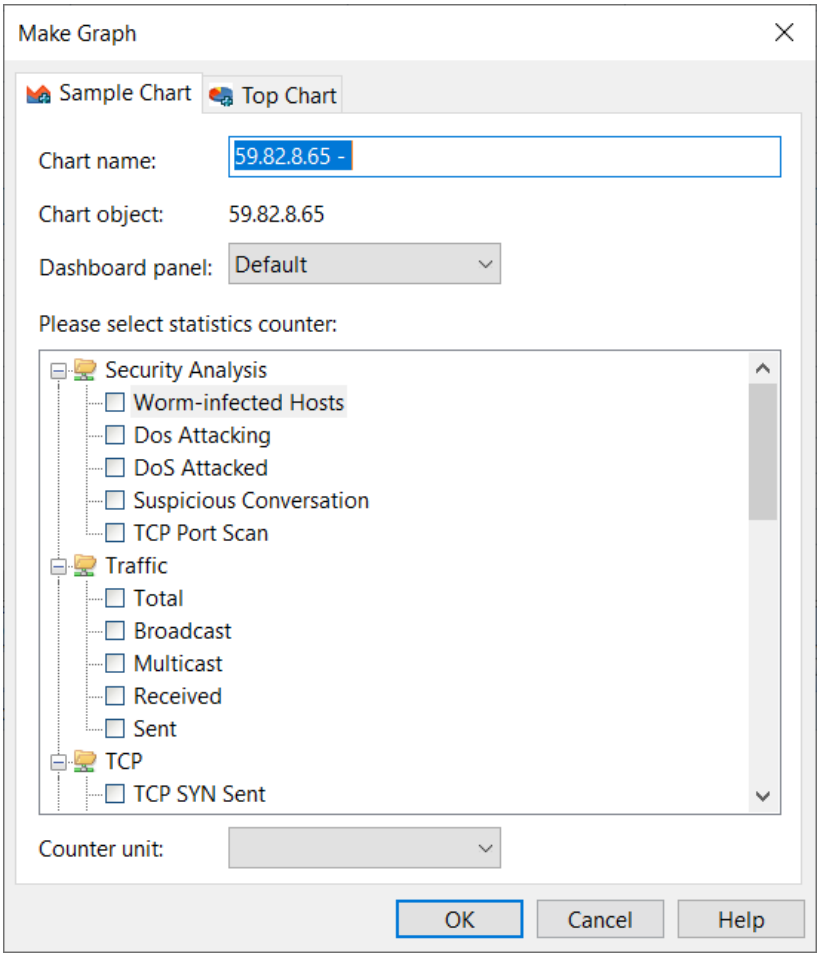
- Click  on the top-right corner of every dashboard panel.
- Click the link **Click here to add a new chart** on the dashboard panel.
- Click  icon in the **Node Explorer** window.
- Choose **Make Graph** on **Pop-up menu** which are available for the **Node Explorer** window and all statistical views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

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:

- **Chart name**: The name of the graph, which can be automatically generated or defined by users.
- **Chart object**: Shows the statistical object of the graph, which is defined by the program.
- **Dashboard panel**: Specify which dashboard panel to contain the graph to be created.
- **Statistics counters**: Shows all available statistical items, which are changed along with chart object.
- **Counter unit**: Specify 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 Unencrypted 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**: MAC 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**: MAC 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

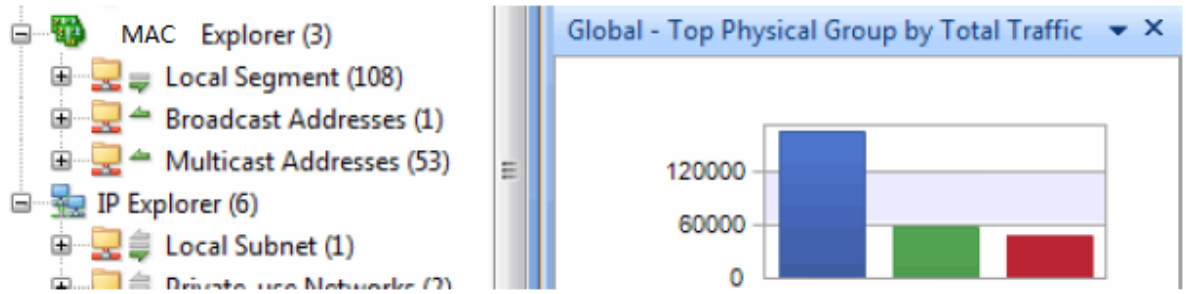
Top Chart includes statistics items as follows:

- Top MAC Group by Total Traffic
- Top MAC Group by Received Traffic
- Top MAC Group by Sent Traffic
- Top IP Group by Total Traffic
- Top IP Group by Received Traffic
- Top IP Group by Sent Traffic
- 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 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

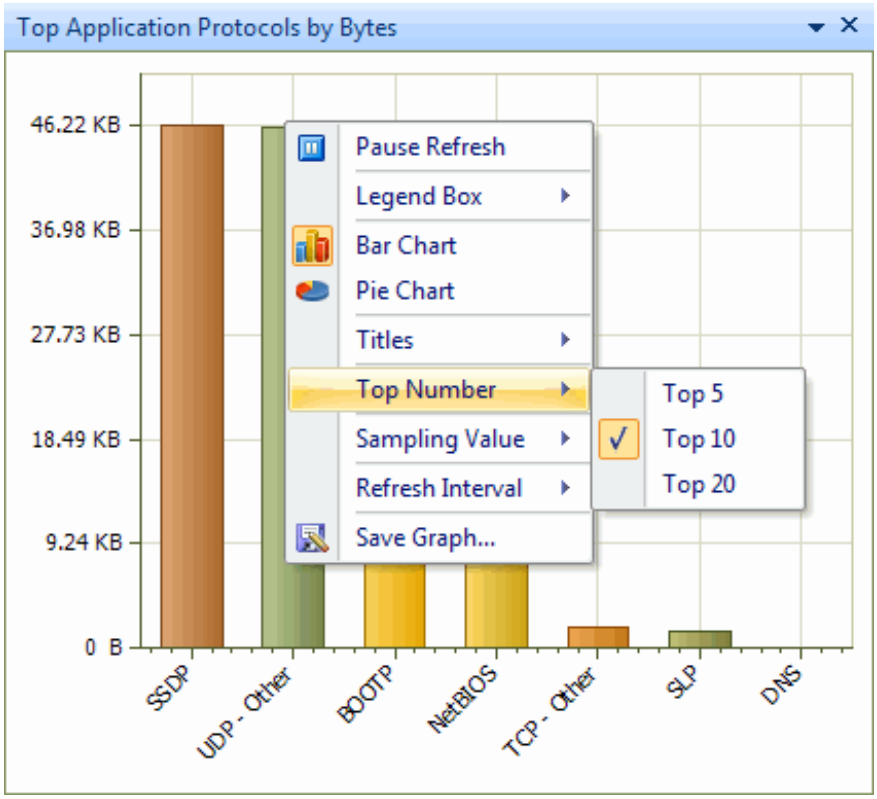
- Top Remote IP Address by Sent Traffic
- Top Application Protocols
- Packet Size Distribution
- VoIP Call Status Distribution
- VoIP Call MOS Distribution
- Top IP by Call Frequency
- Top IP by Call Duration
- Top IP by Call Traffic
- Top Port by Total Traffic
- Top TCP Port by Total Traffic
- Top UDP Port by Total Traffic
- Top Process by Total Traffic
- Top Process by TCP Conversations
- Top Process by UDP Conversations
- Top Applications by Total Traffic
- Top Domain Name
- Top Call by Error Packets Ratio

Tips

1. The MAC Group/IP Group means the node group of MAC Explorer/IP Explorer in the Node Explorer window.
2. Different Top items have different Top numbers, e.g. the top item Top MAC Group by Total Traffic will have only Top 3 if MAC 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.



Expert Diagnosis

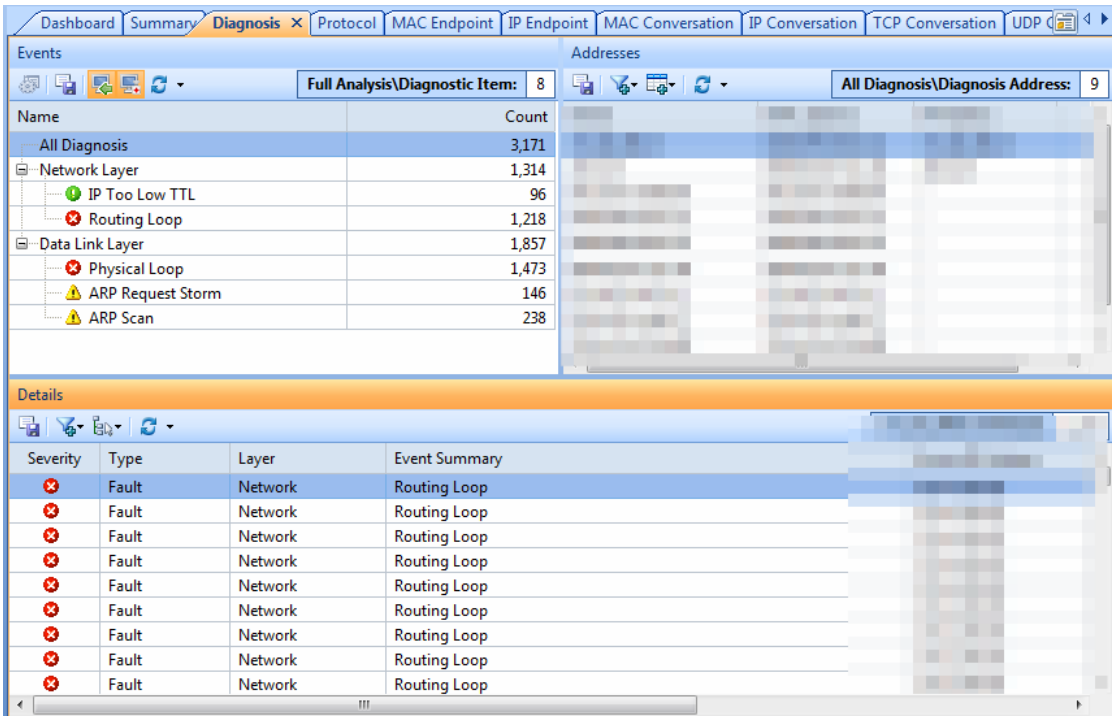
Capsa provides an expert diagnosis feature, which is built in with dozens of diagnosis events. Once the diagnosis events are triggered, they will be displayed on the Diagnosis view with details.

- The Diagnosis view
- Analyzing Diagnosis Events

Note Expert diagnosis feature is only available for Capsa Enterprise.

The 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 are defined by Capsa according to large amount of network data and can be defined by users through defining diagnosis settings.



The **Diagnosis** view contains three panes:

- Events pane
- Addresses pane
- Details pane

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.

Events 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.

Double-click a diagnosis event, you can view the definition and trigger settings of the event.

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

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.

The number in the top right corner indicates the count of the rows of current list, instead of 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.

Addresses pane

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

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

You can click column header to sort the items.

Tips When you select "All Diagnosis" on the Events pane, and on the Addresses pane click the column **Count**, you will get the top addresses according to event counts.

To save the diagnosis address logs, click the save button.

Right-click an item, you can locate it in Node Explorer, resolve address, add it to Name Table, make graph, make alarm, and make filter.

Details pane

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

Details 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 list 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.
Source MAC Address	The source MAC address for the packet.
Destination IP Address	The destination IP address for the packet.
Destination MAC Address	The destination MAC address for the packet.
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.

Analyzing Diagnosis Events

When there are diagnosis events triggered, you may want to know what happened on earth. Here are some tips for it.

When viewing a triggered event, select it on the Events pane, then the Addresses lists the addresses for the event; click the interested address, and then the Details pane shows the detailed information for the event of that address. The Event Summary on the Details pane provides the summary information of the event, and you can double-click it to view packet decoding information.

If you want to view other traffic data of the event address, right-click the address and locate it in Node Explorer, then the views show data only related to that address. You can go to the Protocol view to see the top applications. You can go to the Log view to see the activity logs of the address. You can go to the Matrix view to view its communication status.

If you want to know how the event happens and how to resolve it, you can double-click the event on the Events panel to open the settings box, which provides possible causes and solutions for the network event.

The following list describes the possible causes and solutions for all diagnosis events:

- Application layer diagnosis events
- Transport layer diagnosis events
- Network layer diagnosis events
- Data Link layer diagnosis events

Application layer diagnosis events

The table below describes the diagnosis events on application layer.

Event	Description	Type	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 working status of the DNS server. Upgrade the DNS server.
Non-existent DNS Host or Domain	Requested host or domain name cannot be found.	Fault	The IP address or domain name is invalid. The DNS server has an incomplete DNS table. Reverse DNS lookup is disabled.	Ensure the IP address or domain name is listed on the DNS table. Ensure the IP address or domain name is typed correctly. Change the DNS server address.
DNS Server Returned Error	DNS server returns an error other	Fault	Query format error. Query failure. DNS server returns Not Implemented,	Ensure the DNS query is correct. Change the DNS server address.

Event	Description	Type	Possible causes	Solutions
	than an invalid name.		Refused, or Reserved.	
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 the SMTP server. Upgrade the 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 the source port and destination port.
SMTP Server Returned Error	An SMTP connection or request is rejected by an SMTP server after a TCP connection has already been established.	Fault	The client program executes invalid commands. The client application configures an incorrect user name and password. SMTP server is overloaded. Incorrect configurations of SMTP server software.	Ensure the client executes correct commands. Check user name and password on the client application. Look for attempted spam. Check the configurations of the 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 the POP3 server. Upgrade the 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	Fault	The client executes invalid commands.	Ensure the client executes correct commands.

Event	Description	Type	Possible causes	Solutions
	rejected by a POP3 server after a TCP connection has already been established.		The client application configures incorrect user name and password. POP3 server is overloaded. Incorrect configurations of POP3 server software.	Check user name and password on the client application. Check for POP3 server attack. Check the configurations of the 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 the FTP server. Upgrade the 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 the 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 for POP3 server attack. Ensure the client works in a mode supported by the server. Check the configurations of the 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.	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.

Event	Description	Type	Possible causes	Solutions
			The request method is not allowed. The request times out. The requested URL is too long. Unsupported media type.	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 the 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 the validity of the URL. Change the DNS server address.
HTTP Server Returned Error	HTTP server returns a 5xx error code to indicate a server error; usually the client's request is valid.	Fault	Internal server error, not implemented, gateway timeout, or unavailable service. HTTP version is not supported.	Update the configurations of the HTTP server. Upgrade the HTTP server to support the version type.
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 route configurations. Check the security and working status of the HTTP server. Upgrade the HTTP server.
VoIP SIP Client Authentication Error	A client's request results in a 407-Proxy Authentication Required response from a server.	Fault	The client has not authenticated itself before sending a request that requires authentication.	The client sends correct authentication information.

Event	Description	Type	Possible causes	Solutions
VoIP RTP Packet Out of Sequence	An RTP packet doesn't arrive according to the sending sequence, but arrives ahead of a previously sent RTP packet.	Performance	Too long transmission distance or too slow transmission speed between the sending side and receiving side.	Modify router configurations or optimize network environment.
VoIP RTP Packet Loss	There will be RTP packet loss when RTP packets have incomplete sequence numbers.	Performance	Network congestion or network is overloaded. Too long transmission distance or too slow transmission speed between the sending side and receiving side. The buffer on the receiving side overflows.	Check the application services running on the network; check and upgrade the software and hardware configurations. Modify router configurations or optimize network environment. Check the working status of the host at the receiving side.
SDP Info Deficient or Format Error	SIP packets are deficient in SDP data or SDP info has incorrect format.	Performance	Packets have oversized MTU. Something wrong happened to the packets during transmission. The packets are tampered.	Check MTU settings on network devices. Check or upgrade software and hardware configures on the network. Improve network security.

Transport layer diagnosis events

The table below describes the diagnosis events on transport layer.

Event	Description	Type	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.	Make sure the server exists and is powered on. Open the port for the service on the server. Make sure the SYN packet is reaching the

Event	Description	Type	Possible causes	Solutions
			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.	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 on the 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 route configurations. 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 is wrong for all packets. The source stack does not calculate TCP checksum.	Check for electromagnetic interference devices on the transmission line or for a faulty transmission device. Check if it is necessary to enable calculating checksum. Disable TCP Checksum Offload.
TCP Slow Response	The response time for	Performance	Network congestion. The connection between the sending	Check the application services running on the network.

Event	Description	Type	Possible causes	Solutions
	ACK packet is higher than the threshold.		host and the receiving host is slow. The ACK packet is lost or damaged during transmission. A router between the sending host and the receiving host is overloaded.	Update the route configurations. Check if the ACK packet is lost or damaged. Upgrade the router.
TCP Duplicated Acknowledgement	There are at least three packets that have identical ACK number and SEQ numbers.	Performance	TCP segment is lost due to network congestion. Packets are lost due to other network problems. The other side of the 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 the 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 a DoS or DDoS attack.	Check if there is a 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 an attack on the source host. Check if the progresses are normal.
TCP Port Scan	The number of TCP ports scanned by a local or remote host is higher than the threshold.	Security	A local host has a worm infection that automatically scans TCP ports. Scan software scans TCP ports.	Check if the host is infected with a worm. Check if there is manual scanning on the source host.

Network layer diagnosis events

The table below describes the diagnosis events on network layer.

Event	Description	Type	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 is wrong for all packets. The source stack does not calculate IP checksum.	Check for electromagnetic interference devices on the transmission line or for a 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,	Fault	The transport protocol used by source host is unavailable on the destination host or on the router.	Change the transport protocol on the source host or add transport protocols supported by the router and the destination host.

Event	Description	Type	Possible causes	Solutions
	except the Network Unreachable message, the Host Unreachable message, and the Port Unreachable message.		Segmenting is disabled on the router. The routing has failed. The router cannot forward the packets with specified Type of Service (ToS). Limited by the communication management rules on the router.	Check and update the configurations of 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	Performance	After configuring port mapping, a host in LAN uses an external domain to access internal server. There is an ICMP attack.	Access the server using an internal IP address. Look for the attack source address according to the packet.

Event	Description	Type	Possible causes	Solutions
	destination host.			
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 a 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 for malicious attacks from the source host.
Routing Loop	Due to improper routing protocol, even if there is no redundant link, there may be a routing loop.	Fault	Improper static routing setting. Improper dynamic routing setting. Regular broadcast led to this problem.	Check whether the static routing setting is correct. Check whether the dynamic routing setting is correct.

Data Link layer diagnosis events

The table below describes the diagnosis events on data link layer.

Event	Description	Type	Possible causes	Solutions
Invalid ARP Format	Unable to operate correctly on the Ethernet, and violates the frame format defined by RFC. For example, source MAC address is a multicast	Security	The address information in ARP header is falsified or forged for attack.	Check if there is an ARP attack.

Event	Description	Type	Possible causes	Solutions
	address, or the address information in the ARP header does not match that in the 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 is infecting with a virus that is automatically performing the ARP scan. A scan application is performing the 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 that performs the 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 is infecting with a virus that is automatically performing the ARP scan. A scan application is performing the 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 the 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	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.

Event	Description	Type	Possible causes	Solutions
	than the threshold.			

VoIP Analysis

- VoIP Analysis Settings
- VoIP Call view
- VoIP Explorer
- VoIP Dashboard
- VoIP Diagnosis
- VoIP Logs
- VoIP Reports

VoIP Analysis Settings

If you just need to analyze VoIP traffic, you have two choices, configure the analysis settings for VoIP analysis only or start analyzing directly with default analysis settings.

The default analysis settings cover all analysis modules that VoIP analysis settings need Besides analysis module settings, VoIP Analysis settings also include settings for analysis object, diagnosis, view display, packet buffer, capture filter, packet output, log view, and log output. To know more about these settings, see Analysis Settings.

For VoIP analysis, there are other 18 diagnosis events added. To know more details, see VoIP Diagnosis. And there are two log typed added: VoIP Signaling Log, and VoIP Call Log.

VoIP Call view

The VoIP Call view displays the analysis statistics for VoIP calls.

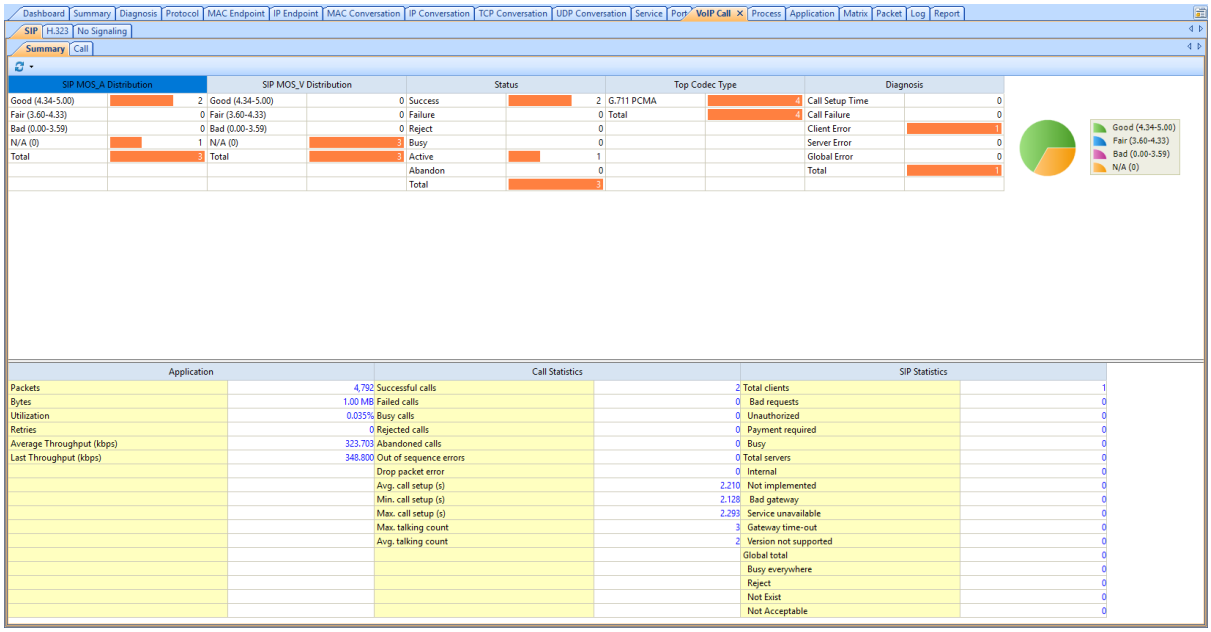
There are two tabs for VoIP Call view, the SIP tab and the H.323 tab, which display the analysis statistics for VoIP calls based on SIP protocol and H.323 protocol, respectively.

The SIP tab and the H.323 tab are almost the same, both containing a Summary tab and a Call tab.

- VoIP Summary tab
- VoIP Call tab

VoIP Summary tab

The VoIP Summary tab shows as below:



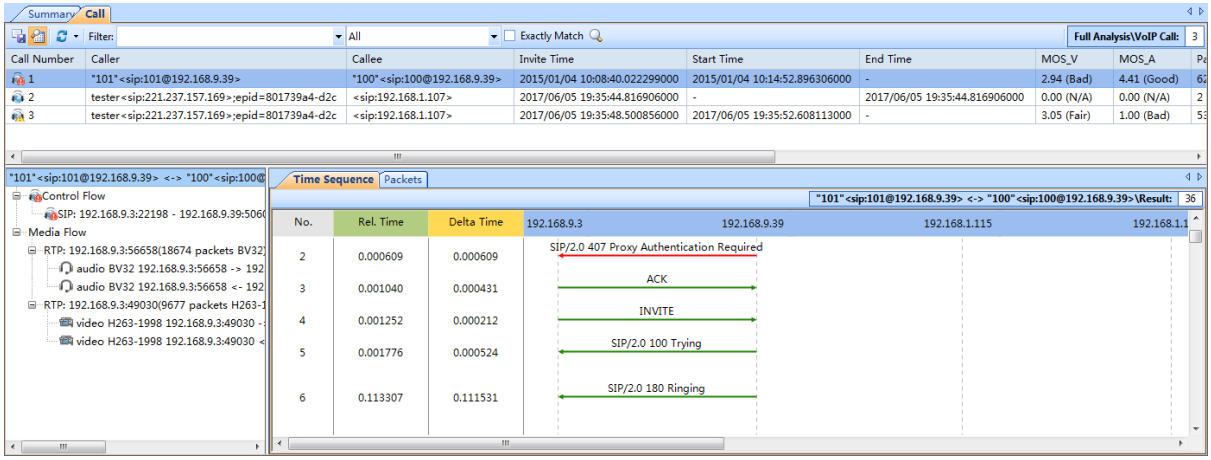
The VoIP Summary tab includes an upper pane and a lower pane.

The upper pane displays the MOS_A distribution, MOS-V distribution, call status distribution, call codec types, and call event distribution, for SIP calls or for H.323 calls.

The lower pane displays network traffic statistics, call statistics, and SIP statistics for SIP calls or H.323 statistics for H.323 calls.

VoIP Call tab

The VoIP Call tab contains an upper pane and a lower pane. You can click  to show or hide the lower pane.



The upper pane lists VoIP call records. The buttons on the toolbar and the pop-up menus are just the same as other views (see Toolbar and pop-up menu).

By default, the VoIP Call tab displays VoIP calls based on VoIP call number. You can click other column field to display them based on that field. For example, you can click the column header "Duration" to sort the calls based on call duration.

The following table lists and describes the columns for the VoIP Call tab.

Column	Description
Call Number	The number of a VoIP call, starting from 1.
Start Time	Start time of the call. The timestamp of the first packet in the call or media flow, accurate to millisecond.
End Time	End time of the call. The timestamp of the last packet in the call or media flow, accurate to millisecond.
Duration	Call duration. Duration = End - Start.
Invite Time	The time when the call sends invitation.
Caller	The side that initiates the call.
Callee	The side that receives the call.
Call ID	If the protocol is H.248, there is no call ID and it displays as "N/A". If the protocol is SIP, it displays the actual ID.
Status	Call Status could be: Success, Failure, Reject, Busy, Active, Abandon.
MOS-V	The MOS score calculated for the video stream of a call.
MOS-A	The MOS score calculated for the audio stream of a call.
Packets	The number of packets for a call, including media flow and control flow.
Bytes	The bytes for all packets for a call, not the payload length.
Diagnosis	The number of diagnosis events for the call. For SIP calls, the diagnosis events include: long call setup time, call failure, client error, server error, global error. For H.323 calls, the diagnosis events include: long call setup time, call failure, gatekeeper reject, registration reject, unregister reject, admission reject, bandwidth reject, location reject, disengage reject
Codec	The code type for the call.
Jitter (ms)	The jitter for the call. The smaller the value, the better the signal.
Packet Loss	The number of lost packets for the call.
Max. Latency	The maximum one of network latency of the call.
Avg. Throughput (kbps)	The average throughput for the call.

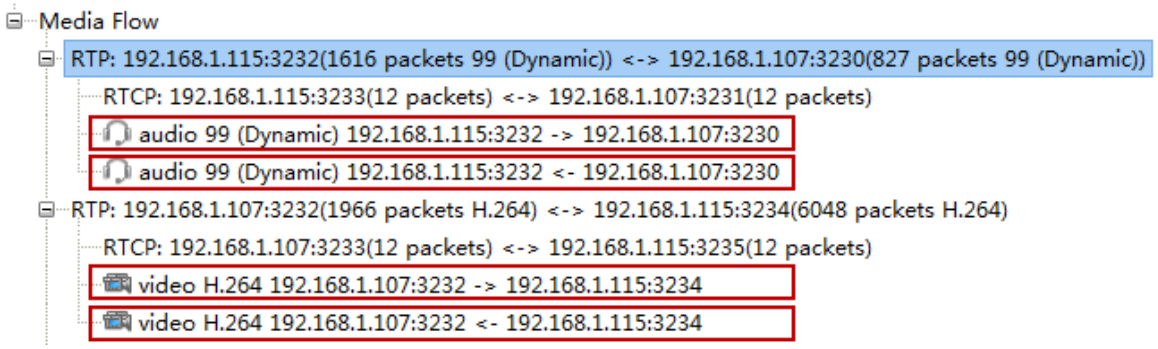
The lower pane displays information for the VoIP call selected on the upper pane, and includes two parts: the left part and the right part.

The left part displays a VoIP call hierarchically, including the control flow and media flow information for the selected call on the upper pane, and the right part shows Time Sequence tab, Packets tab, and Statistics tab for the selected flow on the left part.

Pay audio/video

Capsa is able to play audio and video in the VoIP calls.

Double-click the audio/video flow (marked with red rectangle in following screenshot), the audio/video flow will be played automatically.



For SIP calls, audio based on following codecs can be played: G.711/a, G.711/u, GSM, BV32, Speex, PCM.

For SIP calls, video based on following codecs can be played: H.264 (unencrypted), H.263(unencrypted), Mp4v-es.

For H.323 calls, audio based on following codecs can be played: G.711/a, G.711/u, GSM.

For H.323 calls, video based on following codecs can be played: H.264 (unencrypted), H.263(unencrypted).

The audio for playing is .wav, and the video for playing is .avi. To play the audio/video, please make sure the machine is installed with the player supporting the formats.

Call Time Sequence

The Time Sequence tab displays time sequence for selected call or flow.

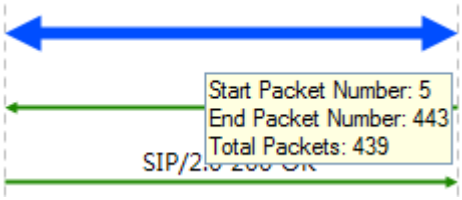
The following list describes the columns for the Time Sequence tab:

- **No.**: The number of packets or media flow for a VoIP call, starting with "0".
- **Rel. Time**: The time from the timestamp of selected packet to that of the first packet in the flow.
- **Delta Time**: The time difference between selected packet and the previous packet.
- **Caller IP**: IP address of the caller.
- **Callee IP**: IP address of the callee.

The Time Sequence tab provides a line with arrows to display the packet direction. A left arrow indicates a packet from callee to caller, a right arrow indicates a packet from caller to callee, and a two-way arrow indicates packets between caller and callee.

Control flow and media flow have different line color to distinguish. Green arrows indicate packets for control flow and blue arrows indicate packets for media flow.

When a mouse hovers a line on the Time Sequence tab, the line will be thickened and displays tips. If the line is for a control flow, the tips are packet number for the control flow packet; if the line is for media flow, the tips include Start Packet Number, End Packet Number, and Total Packets, like the figure below:



- Start Packet Number: The packet number of the first packet for the media flow.
- End Packet Number: The packet number of the last packet for the media flow.
- Total Packets: The count of packets for the media flow.

Packets

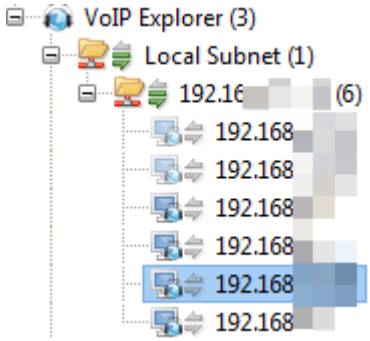
The Packets tab displays all the packets for selected control flow or media flow.

Statistics

The Statistics tab displays the VoIP statistics for the selected control flow/RTP/RTCP data. The statistical items vary according to the selected item on the left part.

VoIP Explorer

A VoIP Explorer is added for VoIP analysis, functioning as IP Explorer, VoIP Explorer contains the IP addresses that related to VoIP calls, and the IP addresses are sorted according to the rules for IP Explorer.



When a specific node is selected, the right pane displays statistical views only related to the node.

For more information, see IP Explorer.

VoIP Dashboard

On the Dashboard view, there is an SIP dashboard panel to display the default VoIP charts for SIP calls, and an H.323 dashboard panel to display the default VoIP charts for H.323 calls.

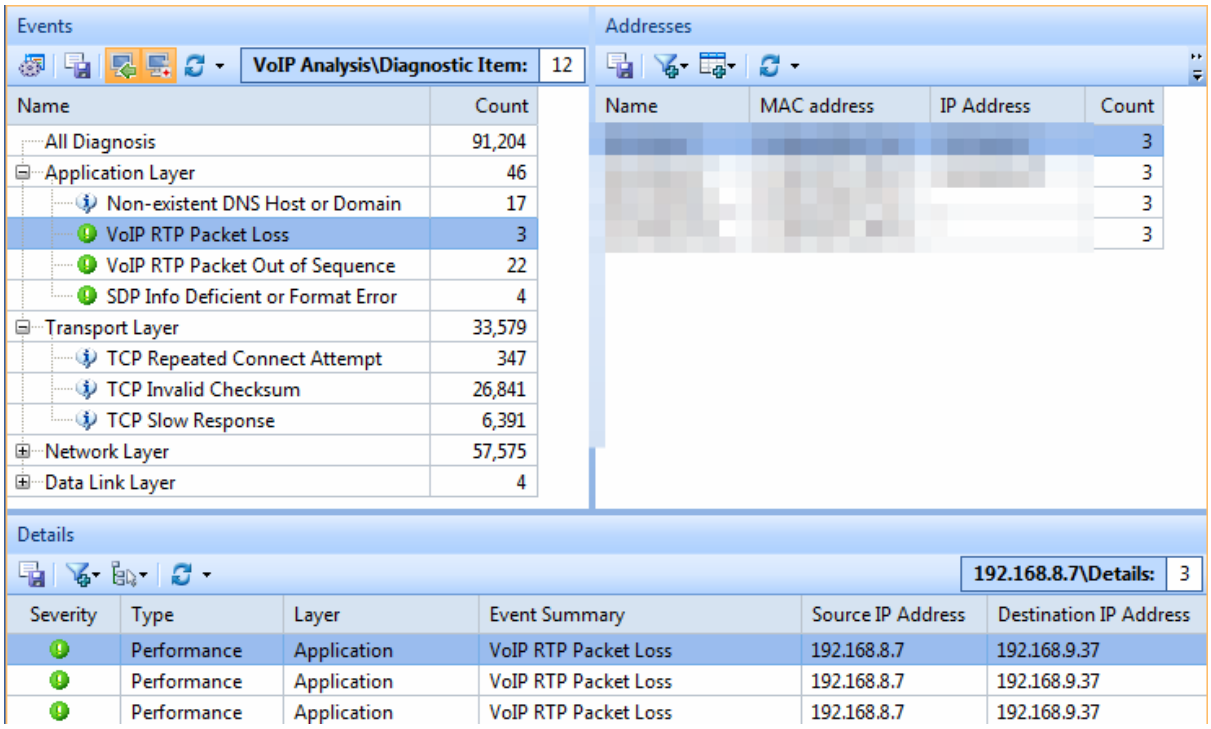
Besides the default VoIP charts, users are allowed to customize new VoIP graphs. All VoIP chart modules include:

- SIP Call MOS_A Distribution
- SIP Call MOS_V Distribution
- SIP Call Codec Distribution
- SIP Call Event Distribution
- SIP Call Status Distribution
- H.323 Call MOS_A Distribution
- H.323 Call MOS_V Distribution
- H.323 Call Codec Distribution
- H.323 Call Event Distribution
- H.323 Call Status Distribution
- No signaling MOS_A distribution
- No signaling MOS_V distribution
- No signaling coding distribution

To know how to add a chart, see Creating graph.

VoIP Diagnosis

Besides the diagnosis events for the whole network, Capsa adds some diagnosis events for VoIP analysis, as the screenshot below:



Capsa is able to diagnose following VoIP events:

- SIP Client Authentication Error
- RTP Packet Loss
- RTP Packet Out of Sequence
- SDP Info Deficient or Format Error
- SIP Call Setup Time
- SIP Call Failure
- SIP Client Error
- SIP Server Error
- SIP Global Error
- H.323 Call Setup Time
- H.323 Call Failure
- H.323 Gatekeeper Reject
- H.323 Registration Reject
- H.323 Unregister Reject
- H.323 Admission Reject
- H.323 Bandwidth Reject
- H.323 Location Reject
- H.323 Disengage Reject

Once the events are triggered, they will display on the Diagnosis view. You can get related information to the events from the Diagnosis view, including the trigger source address, destination address, summary information, port number. See The Diagnosis view.

VoIP Logs

On the Log view, there are two types of VoIP logs: VoIP Signaling Log and VoIP Call Log.

VoIP Signaling Log displays all VoIP calls and the details, including timestamp, source and destination addresses, call ID, summary information. See VoIP Signaling Log.

VoIP Call Log displays all VoIP calls. One VoIP call is recorded as one VoIP Call Log. See VoIP Call Log.

VoIP Reports

On the Report view, a VoIP Report is added for reporting VoIP analysis statistics. Users are able to customize VoIP reports.

The report items include:

- SIP Call MOS_A Distribution
- SIP Call MOS_V Distribution
- SIP Call Codec Distribution
- SIP Call Event Distribution
- SIP Call Status Distribution
- H.323 Call MOS_A Distribution
- H.323 Call MOS_V Distribution
- H.323 Call Codec Distribution
- H.323 Call Event Distribution
- H.323 Call Status Distribution

Besides the VoIP Report, you can create a new report with VoIP statistics. To know how to create a report, see Creating report.

TCP Flow Analysis

The separately transmitted packets for a TCP conversation flow can be reconstructed by Capsa to display the original conversation content. Just by a glance, you can know if there is packet loss, retransmission, or out of order on the network. Capsa provides a TCP Conversation view and a TCP Flow Analysis window to display the analysis results and assist you with further analysis.

- TCP Conversation view
- TCP Flow Analysis window

TCP Conversation view

The **TCP Conversation** view shows statistics of the network communication traffic based on TCP protocol. TCP conversation is identified by TCP SYN flag 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 in **MAC Explorer** or protocol nodes not belonging to TCP protocol in **Protocol Explorer**.

You can click a column header to sort the view based on the header field. This function is very useful for making analysis. For example, you can click the column "Duration" to view the top communications based on communication duration. You can click the column "Bytes" to view the top communication based on the traffic transmitted.

The column Interaction Diagram displays the packets interaction status for each TCP conversation. On the Interaction Diagram, the scales indicate the number of payload packets, green indicates request packets, blue indicates response packets, and red indicates retransmission packets.

When you want to view the details of a TCP conversation, you can double-click it to open the TCP Flow Analysis window to view TCP transaction process and time. See TCP Flow Analysis window for details. You can also view the transaction process through the lower pane tabs.

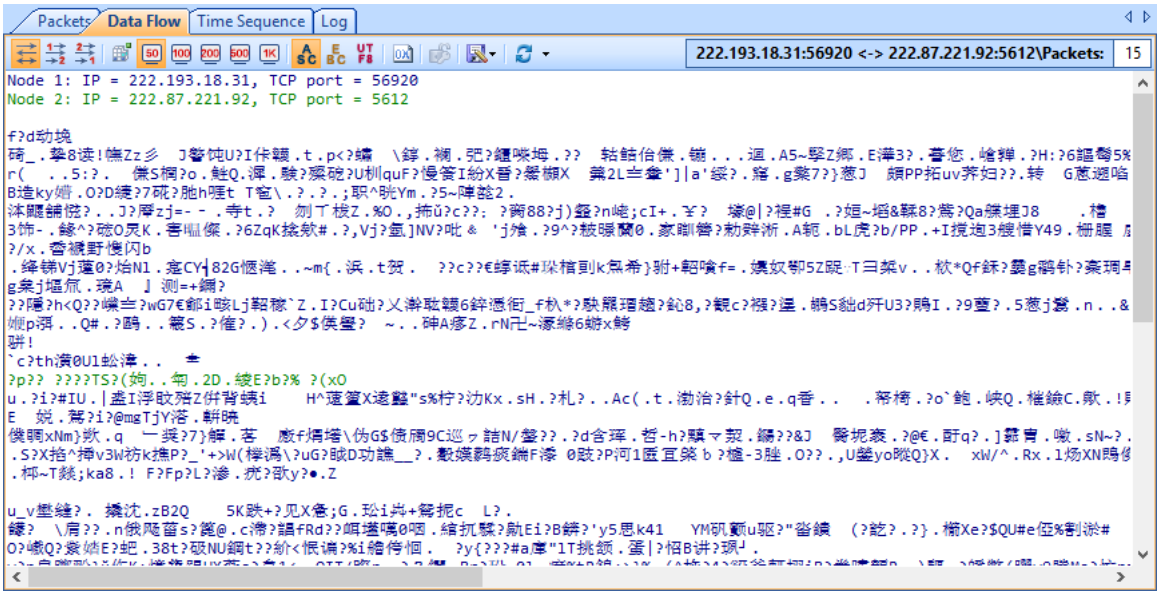
The TCP Conversation view lower pane includes three tabs: Packet, Data Flow, Time Sequence.

- The Packet tab lists the packets only related to the selected TCP conversation. You can click the buttons on it to view the packet decoding information. See Decoding packets for more information.
- The Data Flow tab shows the original flow information of the TCP conversation. See Data Flow tab for more information.
- The Time Sequence tab diagrammatically displays the conversation process. See Time Sequence tab for more information.

If the lower pane is invisible, you can click  to show it.

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 below:



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

By default, the **Data Flow** tab shows 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.

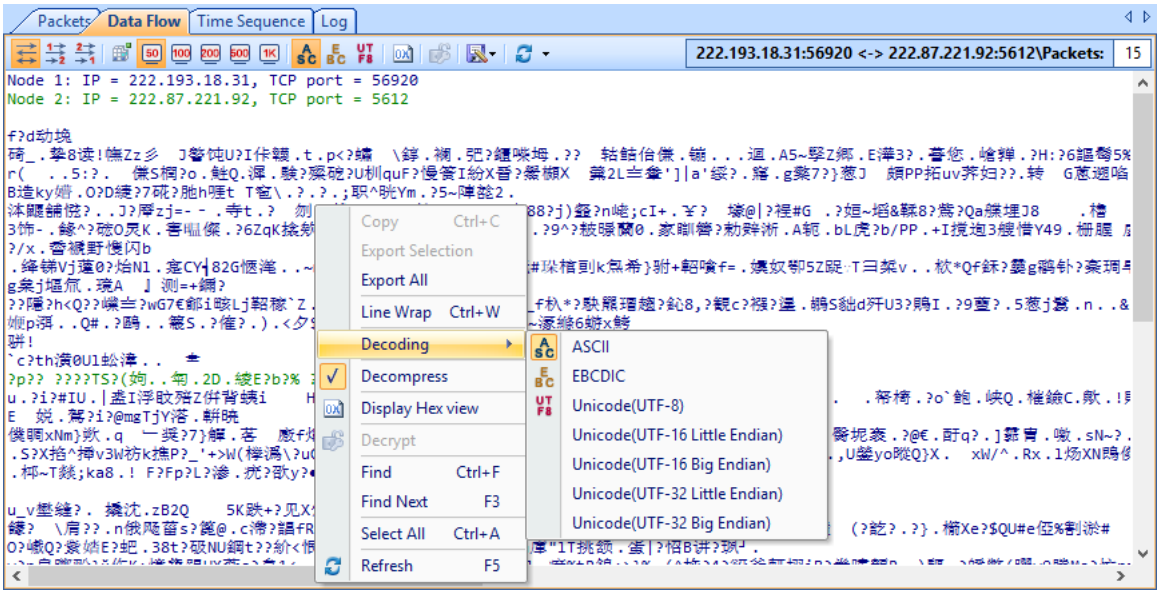
You can also click the button  to show only data from node 1 to node 2 or from node 2 to node 1.

When there are a lot of packets for a TCP conversation, you can click  to just show the data of the first 50, or 100 packets.

You can click  to display the data in hex.

If you are interested in the data flow, you can click  to save the data.

If you want to display the data flow in other formats, you can right-click, select **Decoding**, and then click the interested format.



Time Sequence tab

The **Time Sequence** tab provides a time sequence diagram for 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.

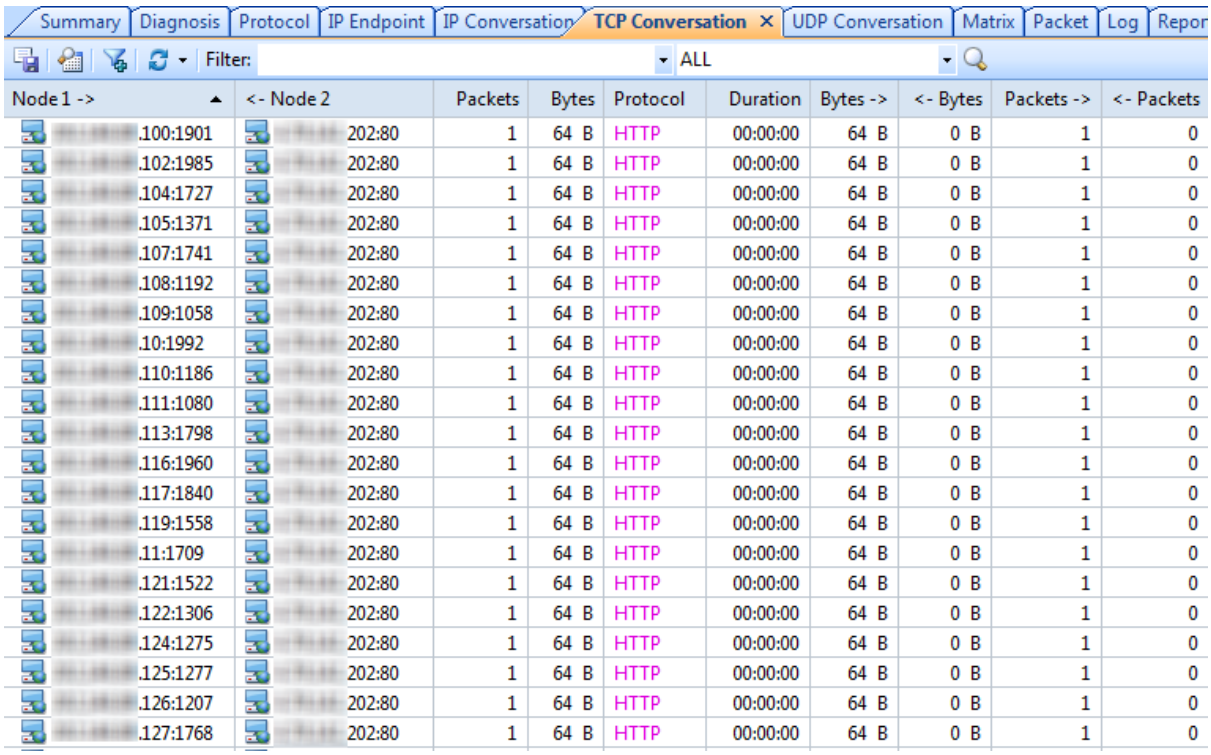
You can click the button  to show the real sequence number or relative sequence number in a TCP flow.

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

- **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

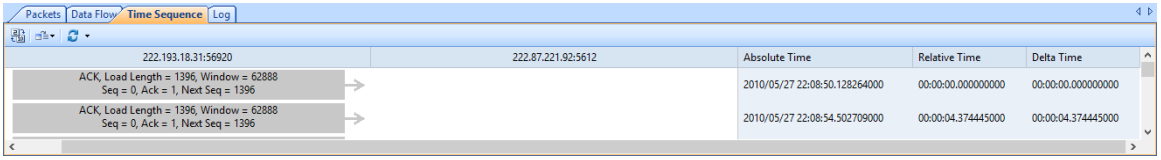
sequence number of the packet sent by node 2.

The time sequence diagram is very useful to understand the whole TCP flow process, and it is helpful to find some network problems. For example, below is a screenshot of the TCP Conversation view of some capture:



Node 1 ->	<- Node 2	Packets	Bytes	Protocol	Duration	Bytes ->	<- Bytes	Packets ->	<- Packets
[redacted].100:1901	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].102:1985	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].104:1727	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].105:1371	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].107:1741	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].108:1192	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].109:1058	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].10:1992	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].110:1186	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].111:1080	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].113:1798	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].116:1960	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].117:1840	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].119:1558	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].11:1709	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].121:1522	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].122:1306	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].124:1275	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].125:1277	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].126:1207	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0
[redacted].127:1768	[redacted]202:80	1	64 B	HTTP	00:00:00	64 B	0 B	1	0

Just by a glance, we can know that it seems that something abnormal is happening. Normal network is very unlikely to have such kind of traffic. Therefore, we click  to show the lower pane, and go to the Time Sequence tab, and we get this:

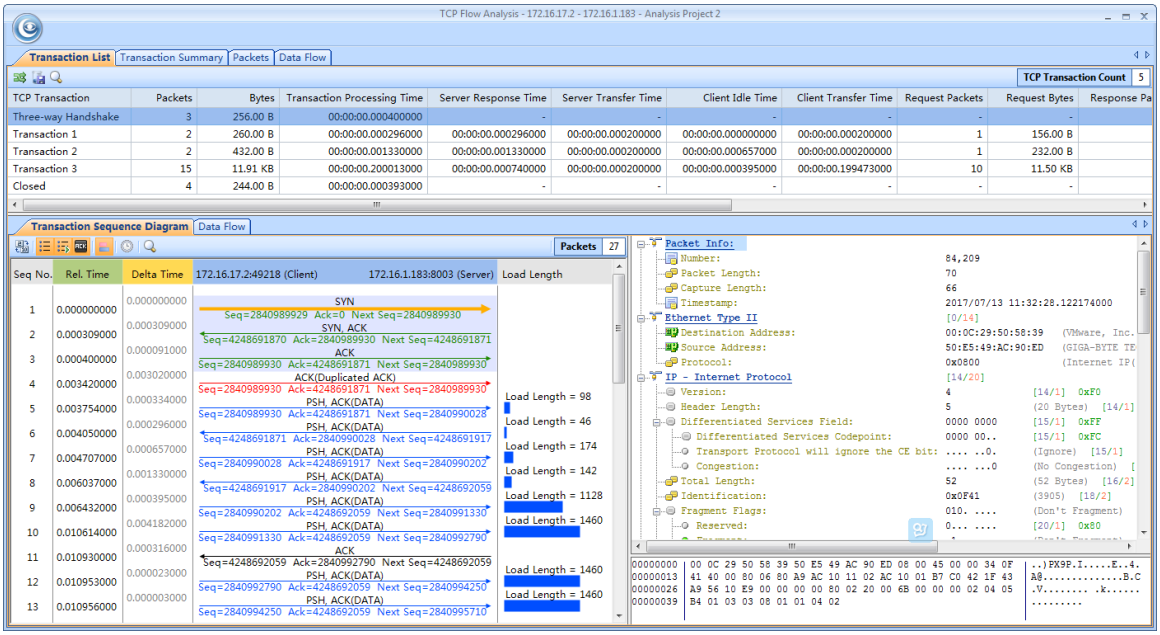


We checked the Time Sequence tab for each TCP conversation, and found they are all the same. Together with other proofs, we finally found that there was DoS attack on the network.

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 four views:

- Transaction List view
- Transaction Summary view
- Packet view
- Data Flow view

Transaction List view

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

Transaction List

The items on the toolbar of the upper pane are described as below:

: 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.

You can right-click the column header of the Transaction list to show/hide columns. All columns for Transaction List are described as below:

- **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.
- **Transaction Processing Time**: Transaction processing time is the time interval from the last packet to the first packet of a transaction.
- **Server Response Time**: Server response time is the time interval from the first packet of a transaction response to the last packet of a transaction request.
- **Server Transfer Time**: Server transfer time is the time interval from the last packet to the first packet of a transaction response.
- **Client Idle Time**: Client idle time is the time interval from the first packet of current transaction to the last packet of previous transaction.
- **Client Transfer Time**: Client transfer time is the time interval from the last packet to the first packet of a transaction request.
- **Request Packets**: The number of payload packets sent from client to server.
- **Request Bytes**: The total bytes of the packets sent from client to server.
- **Response Packets**: The number of payload packets sent from server to client.
- **Response Bytes**: The total bytes of the packets sent from server to client.
- **Retransmission**: The retransmission times for the transaction.
- **Segment Loss**: The times of segment loss.
- **Bitrate**: The bitrate of the transaction. Only available when the packet number is greater than or equal to 10.
- **Start Time**: The time when the transaction starts.
- **End Time**: The time when the transaction ends.
- **Summary**: Summary information 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 displays 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 represent 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, like 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 list describes the buttons on the toolbar of this tab:

 : 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.

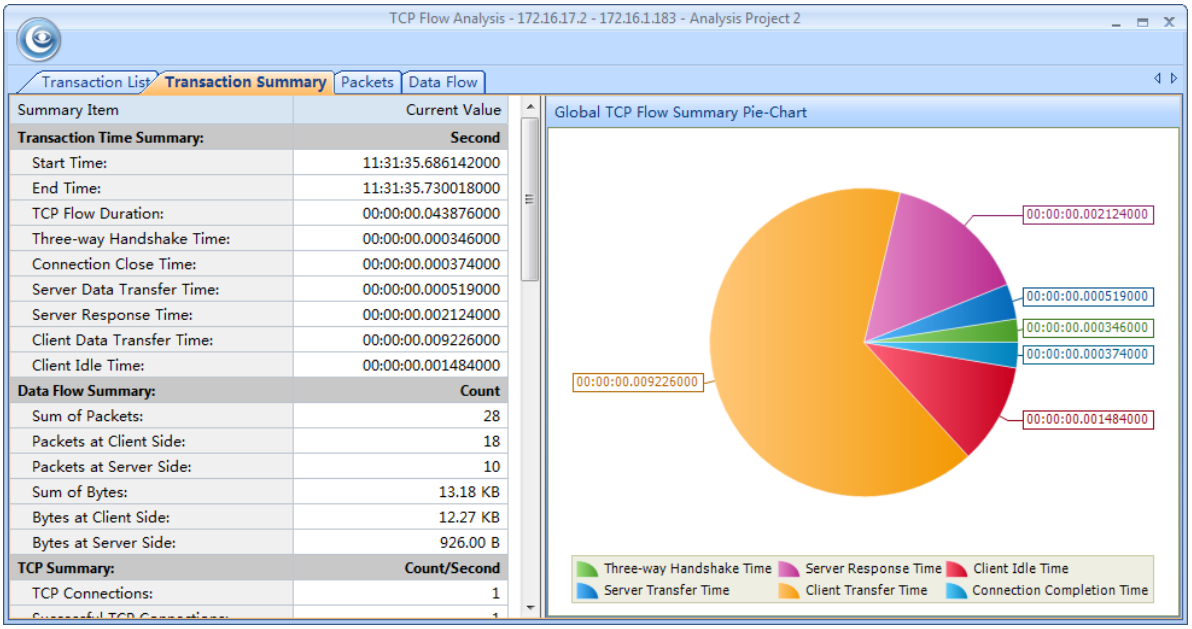
: Calls out **Find** dialog box to search in the packet decoding section on the right. When finding the result, the horizontal line for the packet will be highlighted.

Data Flow tab

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

Transaction Summary view

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

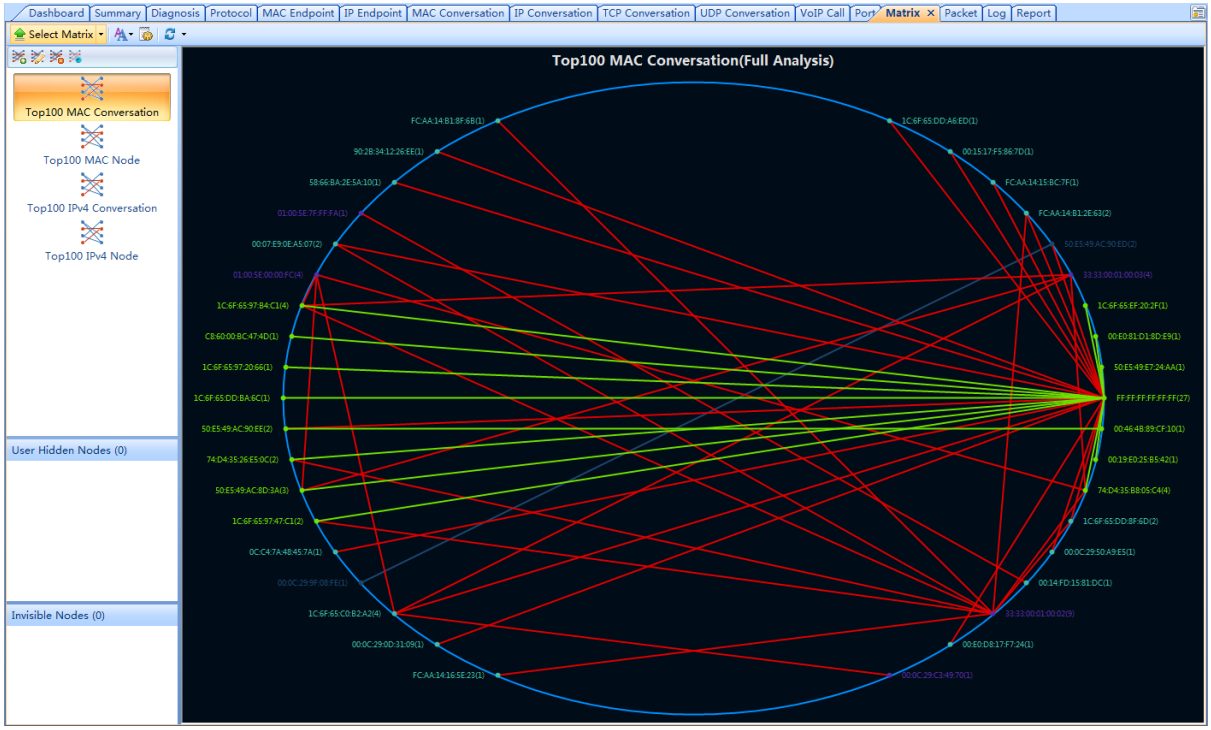
The right pane prevents a pie chart of global TCP flow statistics, including six items on the pie chart: Three-way Handshake Time, Server Response Time, Client Idle Time, Server Transfer Time, Client Transfer Time, and Connection Completion Time, and visually showing the TCP flow time information of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

Using Matrix

Matrix is provided by a Matrix view to dynamically display network traffic with nodes and lines in peer map, the nodes representing network nodes and the lines representing network communication.

The Matrix view

The **Matrix** view consists of a left pane and a matrix which is an ellipse docked with nodes and lines connecting the nodes, the nodes are MAC/IP addresses and the lines indicate communication between the addresses. The number after the node represents the number of peer hosts.



You can click **Select Matrix** on the left top of the Matrix view to hide/show the left pane, and click the little triangle to choose a matrix type to show in the view.

You can click the refresh button  to refresh the matrix view or to set a refresh interval.

On the top of the left pane, it lists the four default matrixes, you can make modifications on them or to add new matrix. See Creating matrix for details.

The color and the font size of the matrix can be defined by users. See Customizing matrix for details.

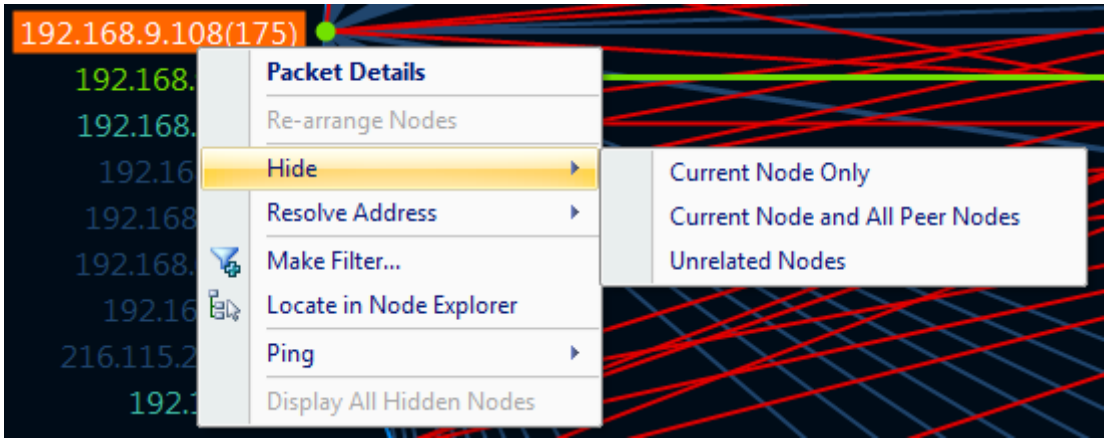
Move your mouse over a node, the nodes and the lines connected with the node will be yellow highlighted, and traffic statistical information about the node will be displayed. Move your mouse over a line, the line and two nodes connected by the line will be yellow highlighted, and traffic statistical information about the conversations will be displayed.

When viewing the matrix, you can double-click a node or a line to open the Packet window, which lists and decodes the packets related to the node or to the nodes connecting the line.

User Hidden Nodes

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

To hide a node, right-click a node and then choose which nodes to hide, like the figure below:



- **Current Node Only**: Only hides the selected node.
- **Current Node and All Peer Nodes**: Hides the selected node and its peer nodes.
- **Unrelated Nodes**: Only shows the selected node and its peer nodes.

When nodes are hidden, they are displayed on the User Hidden Nodes section. 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

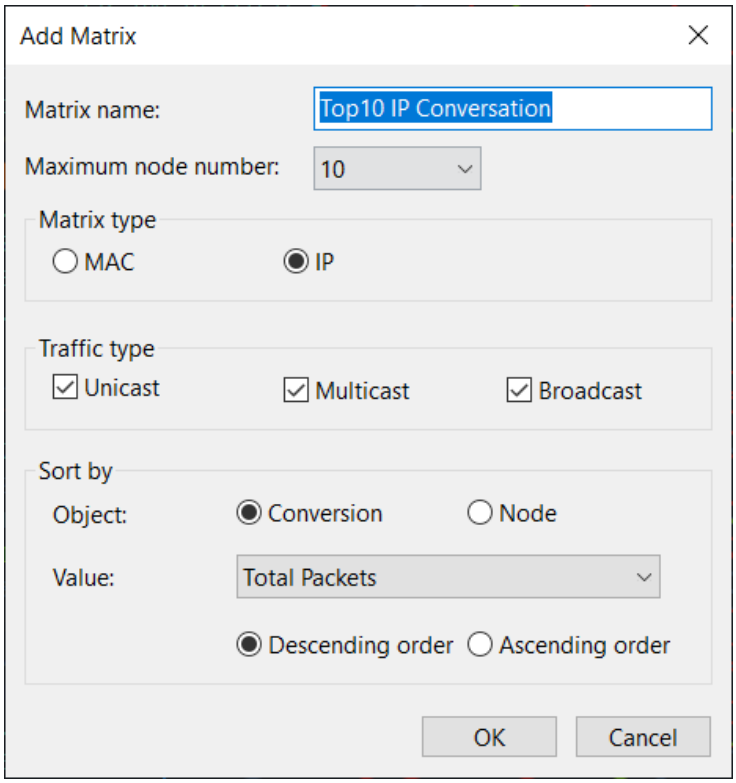
The section lists the nodes which have been temporarily hidden in the matrix because they do not match the settings of the matrix. The number in the bracket on the **Invisible Nodes** pane head shows the number of invisible nodes.

For example, if the matrix is a top100 IP node one, the matrix will only display the top 100 IP addresses on the graph, and if the matrix is a top100 IP conversation one, the matrix will only display the top 100 IP conversations; the remaining nodes will be grouped to Invisible Nodes.

Creating matrix

By default, Capsa provides four matrixes: Top 100 MAC Conversation, Top 100 MAC Node, Top 100 IPv4 Conversation, and Top 100 IPv4 Node.

To add a new matrix, click  to open the **Add Matrix** dialog box and then finishes the box:



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

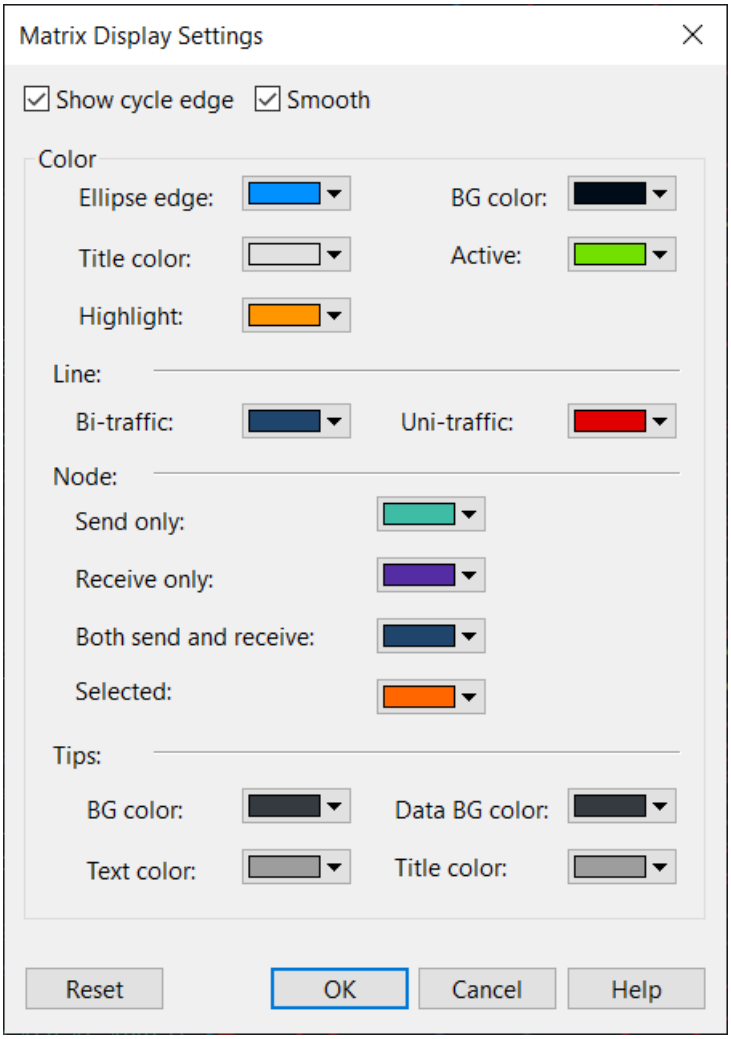
- Matrix name: The name of the matrix.
- Maximum node number: The maximum number of the nodes.
- Matrix type: **MAC** means that the statistics are based on MAC addresses and **IP** means that the statistics are based on IP addresses.
- Traffic type: The traffic type for statistics.
- Object: The statistical 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.

For existing matrixes, you can click  to make modifications.

Customizing matrix

By default, Capsa provides a set of color schemes for the Matrix view. Users can define new color schemes.

To change the display color, click  to open the **Matrix Display Settings** dialog box:



- **Show cycle edge**: Shows the ellipse.
- **Smooth**: Smoothens the ellipse, the lines, and the nodes.
- **Color**: The color for displaying the ellipse, the background, the title of the matrix, active nodes and lines, and highlighted nodes and lines.
- **Line**: The color for displaying bidirectional traffic and unidirectional traffic.
- **Node**: The color for displaying nodes only sending packets, only receiving packets, sending and receiving packets, and selected nodes.
- **Tips**: The color for displaying tips when a node or a line is highlighted.

You can also change the font size for the Matrix view. Just click  and choose a proper one.

Security Analysis views

Security analysis is designed to detect worm activities, TCP port scanning, ARP attacks, DoS attacks and suspicious conversations. Once there are such attacks on the network, the attacks will be shown on corresponding security analysis views.

- ARP Attack view
- Worm view
- DoS Attacking view
- DoS Attacked view
- TCP Port Scan view
- Suspicious Conversation view

Note Security analysis views are only available for Capsa Enterprise.

ARP Attack view

The **ARP Attack** view is only available when you are using the analysis settings 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.

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

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 view columns for details.

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 **MAC Conversation** tab on the lower pane. The **MAC 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 **MAC Conversation** view.

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.

Worm view

The **Worm** view is only available when you are using the analysis settings 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.

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

Worm view 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 view columns for details.

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** view 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.
- 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.
- 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.

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.

DoS Attacking view

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

If there is an item on this view, it means that the listed computers have 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 attacking is identified according to default setting values, and you can also customize this value to let the program find out the root of the problem more accurately.

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

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. Endpoint view columns for details.

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** view 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 **DoS Attacking** view. The toolbar and columns are just the same as those on **IP Conversation** view.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **DoS Attacking** view. The toolbar and columns are just the same as those on **TCP Conversation** view.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **DoS Attacking** view. The toolbar and columns are just the same as those on **UDP Conversation** view.

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.

DoS Attacked view

The **DoS Attacked** view is only available when you are using the analysis settings 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.

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

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 view columns for details.

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 view 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 **DoS Attacked** view. The toolbar and columns are just the same as those on **IP Conversation** view.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **DoS Attacked** view. The toolbar and columns are just the same as those on **TCP Conversation** view.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **DoS Attacked** view. The toolbar and columns are just the same as those on **UDP Conversation** view.

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.

TCP Port Scan view

The **TCP Port Scan** view is only available when you are using the analysis settings 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.

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

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 view columns for details.

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 view 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 **TCP Port Scan** view. The toolbar and columns are just the same as those on **IP Conversation** view.
- The **TCP Conversation** tab lists the conversations using TCP protocol of the node selected on the **TCP Port Scan** view. The toolbar and columns are just the same as those on **TCP Conversation** view.
- The **UDP Conversation** tab lists the conversations using UDP protocol of the node selected on the **TCP Port Scan** view. The toolbar and columns are just the same as those on **UDP Conversation** view.

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.

Suspicious Conversation view

The **Suspicious Conversation** view is only available when you are using the analysis settings 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.

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

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 view columns for details.

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.
- 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.

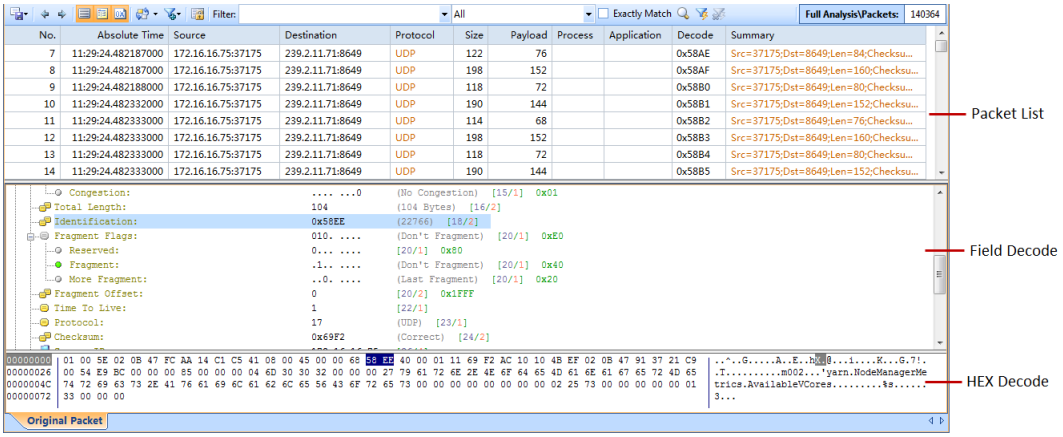
Viewing Packets

Colasoft Capsa can decode every single captured packet. All packets are displayed on the Packet view.

- The Packet view
- Decoding packets

The Packet view

The **Packet** view displays captured packets and provides packet decoding information. This view includes three panes from top to down:



- Packet List pane: Lists captured packets. All packets on the list are temporally stored in Packet Buffer. If the Packet Buffer doesn't have enough space to store all captured packets, some packets will be lost according to the settings of Packet Buffer.
- Field Decode pane: Displays decoding information based on the protocols for packet transmission.
- Hex Decode pane: Displays the hexadecimal decoding information of a packet selected in the Packet List pane.

You can click  to show/hide the Packet List pane, click  to show/hide the Field Decode pane, and click  to show/hide the Hex Decode pane.

You can click  to switch the layout of the Packet view.

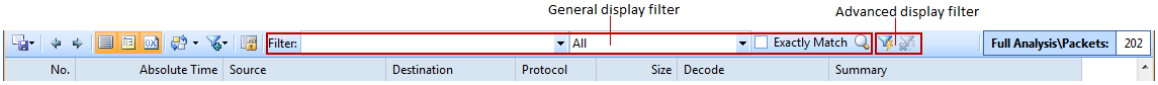
By right-clicking the column header of the Packet view, you can specify which columns to show in the list. Choose **Default** to show default columns and choose **More** to open **Display Column** dialog box to set which columns to show and to set the position, the alignment and the width of the column.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

To display-filter the Packet view with protocol field rule, see Advanced display filter for more information.

To know more information about decoding packets, see Decoding packets.

Advanced display filter

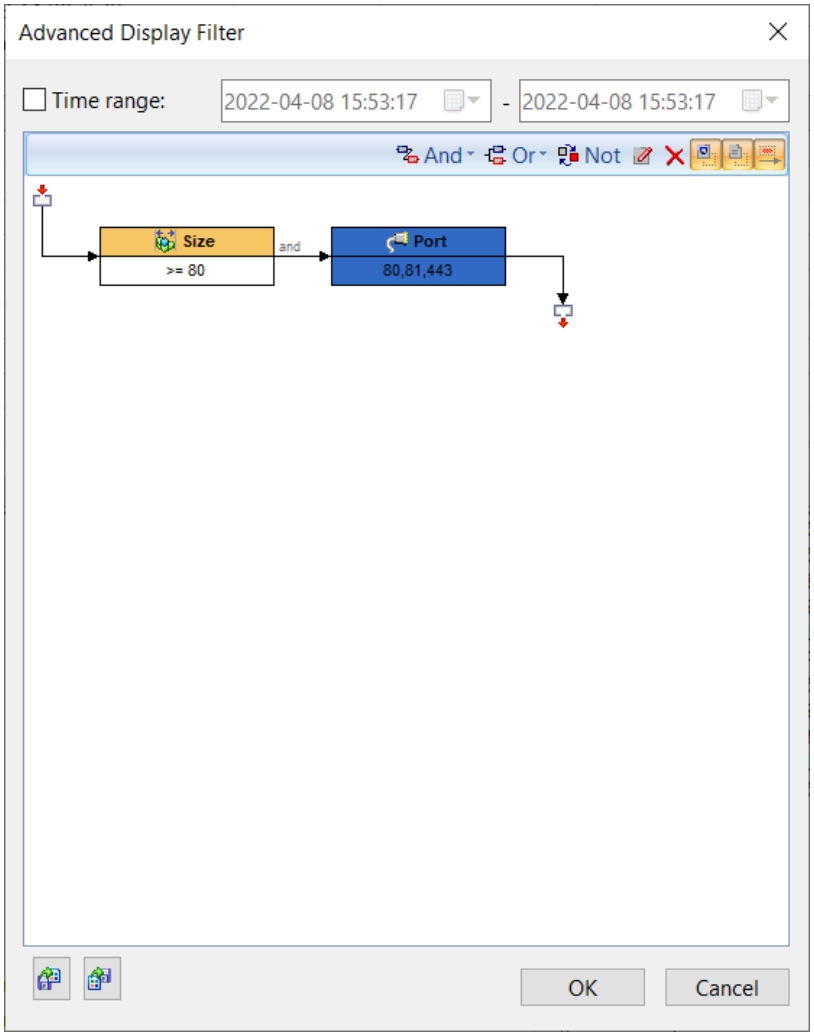
Capsa provides an advanced display filter to display-filter packets on the Packet view. The advanced display filter is just beside the general display filter on the toolbar of the Packet view.



The general display filter is for display-filtering the records according to the column fields on the view. It matches the display keyword with the records on the list. It is available on multiple views. For more information, please refer to Display Filter.

The advanced display filter is for display-filtering packets. It is only available for the Packet view. It matches the filter rule with packet content.

To apply an advanced display filter, click the Advanced Display Filter icon to open the Advanced Display Filter box:



Time range is for specifying which time duration of packets to match.

To add a rule, just click **Add** and then define a rule.

The rule section is just the same as that for advanced packet filter (see Creating Advanced Filter).

To disable advanced display filter, just click the disable button after the Advanced Display Filter icon.

Packet view columns

The following table lists and describes the columns of the **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 Port	The destination port number of the packet.
Decode	The decoding information of selected field on the Field Decode pane.
Summary	The summary information of the packet.
Process	The process of the packet.
Application	The application which sends or receives the packet.
Capture Filter	The name of the conversation filter enabled.
Payload	The payload length of the packet.

Decoding packets

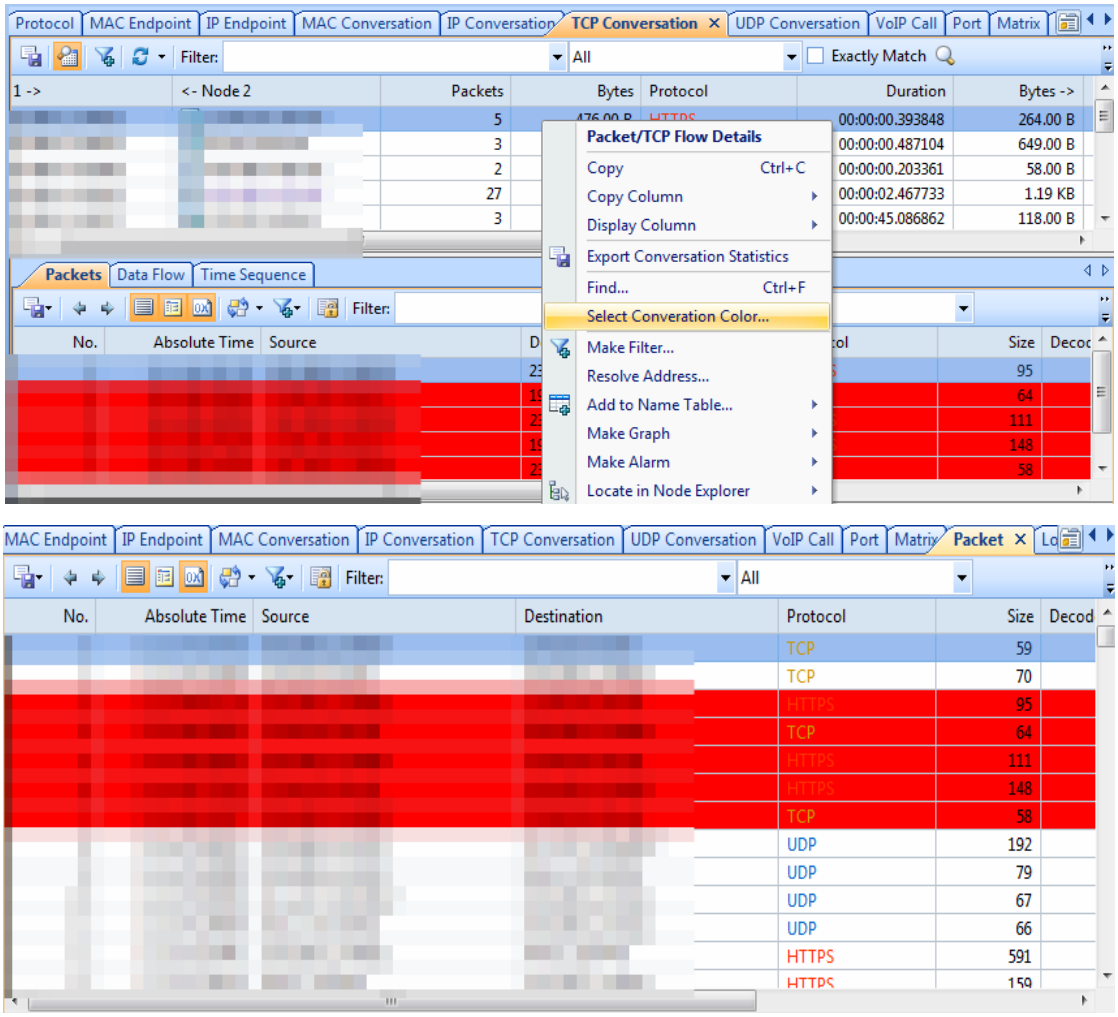
It is easy and useful to use the Packet view to view decoding information. Select a packet on the Packet List pane, the Field Decode pane will display the decoding information for the packet according to protocol layer.

When selecting a field in the Field Decode pane, the Hex Decode pane displays corresponding hexadecimal data for the selected field, and the column Summary on the Packet List pane displays the field decoding content for all packets on the Packet List pane. For example, if you select the SYN flag of TCP protocol for one packet, the column Summary lists the SYN flag for all packets on the Packet List pane:

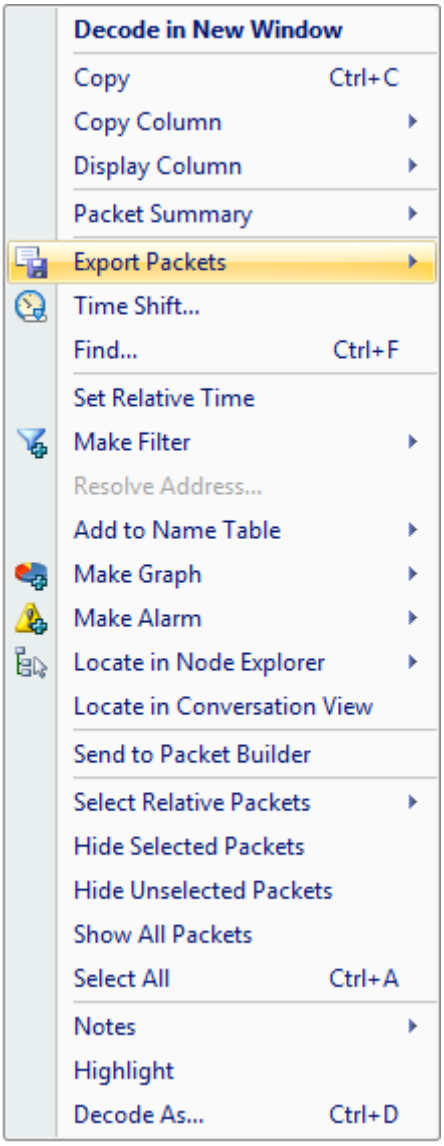
No.	Source	Destination	Size	Decode	Summary
18687	192.168.9.108:53499	192.168.0.206:445	66	.... ..1.	Seq=0990981149,Ack=0000000000,F=....S.,Len= 48,Win= 8192,Checksum Err...
18688	192.168.0.206:445	192.168.9.108:53499	66	.... ..1.	Seq=3580608107,Ack=0990981150,F=.A..S.,Len= 48,Win= 5840
18689	192.168.9.108:53499	192.168.0.206:445	58	.... ..0.	Seq=0990981150,Ack=3580608108,F=.A....,Len= 40,Win=64240,Checksum Er...
18690	192.168.9.108:53499	192.168.0.206:445	217	.... ..0.	C: Negotiate
18691	192.168.0.206:445	192.168.9.108:53499	64	.... ..0.	Seq=3580608108,Ack=0990981309,F=.A....,Len= 46,Win= 6432
18692	192.168.0.206:445	192.168.9.108:53499	189	.... ..0.	S: Negotiate Status = Success
18693	192.168.9.108:53499	192.168.0.206:445	200	.... ..0.	C: Session Setup And X
18694	192.168.0.206:445	192.168.9.108:53499	360	.... ..0.	S: Session Setup And X Status = Success
18695	192.168.9.108:53499	192.168.0.206:445	632	.... ..0.	C: Session Setup And X
18696	192.168.0.206:445	192.168.9.108:53499	164	.... ..0.	S: Session Setup And X Status = Success

```
Ack Number:                    0              [42/4]
TCP Offset:                    7              (28 Bytes)  [46/1]  0xF0
Flags:                         ..00 0010      [47/1]  0x3F
  Urgent pointer:              ..0. ....      [47/1]  0x20
  Acknowledgment number:       ...0 ....      [47/1]  0x10
  Push Function:               .... 0...      [47/1]  0x08
  Reset the connection:        .... .0..      [47/1]  0x04
  Synchronize sequence:        .... ..1.      [47/1]  0x02
  End of data:                 .... ...0      [47/1]  0x01
```

TCP Conversation view provides the feature of conversation coloring. Choose one TCP conversation, right-click it and choose "Select Conversation Color" in the pop-up menu, then the conversation has been set with background color. Related packets of this conversation have also been set with the same background color.



If you are interested in a packet, you can highlight it. To highlight a packet, just right-click a packet in the Packet List pane and then click **Highlight**.

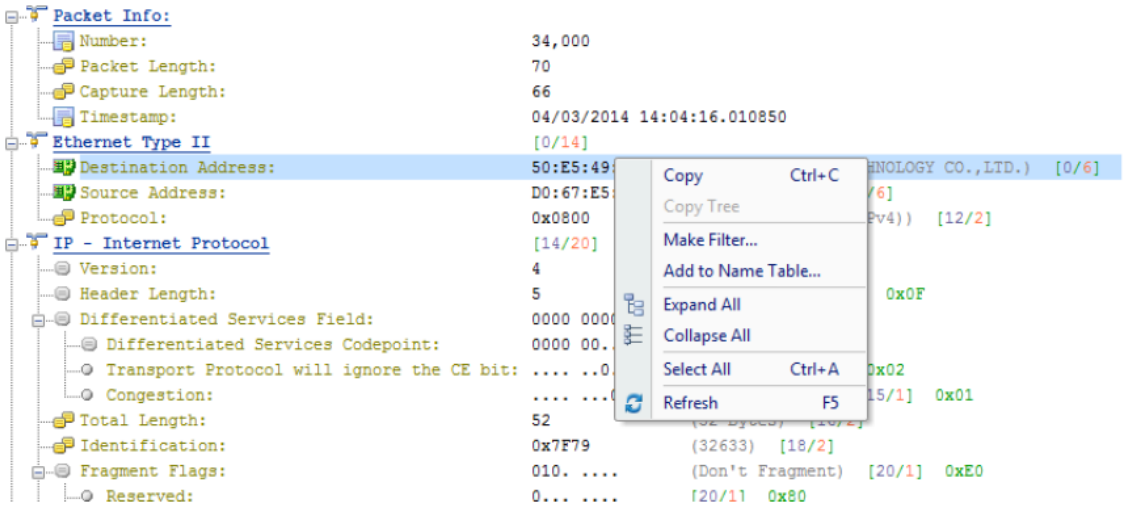


The following list describes all items on the pop-up menu:

- **Decode in New Window**: Opens a new window to show packet decoding information; alternatively, you can double-click the packet.
- **Copy**: 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.
    - **Auto**: 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 the 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**: Adds 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 Node 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.
- **Decode As**: Decodes the selected packet according to a certain protocol. After the configuration, all the packets that meet the condition will be decoded based on protocol.

When viewing the decoding information, you can click on the **-** minus or **+** plus signs in the margin to collapse or expand the hierarchy of any header section. You can also right-click decoding information to collapse or expand the decoding tree.



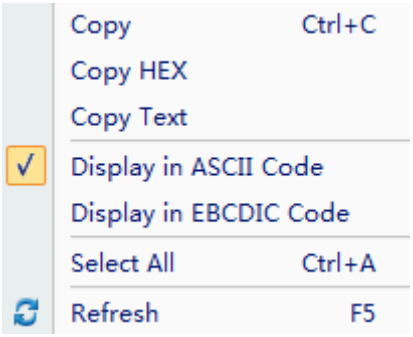
The following list describes all items on the pop-up menu:

- **Copy**: Copies the selection to the clipboard.
- **Copy Tree**: Copies the packet decoding 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**: Adds 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.

On the right part of the Hex Decode pane, you can display the data in ASCII code or EBCDIC code. Just right-click and choose the interested one.



The following list describes all items on the pop-up menu:

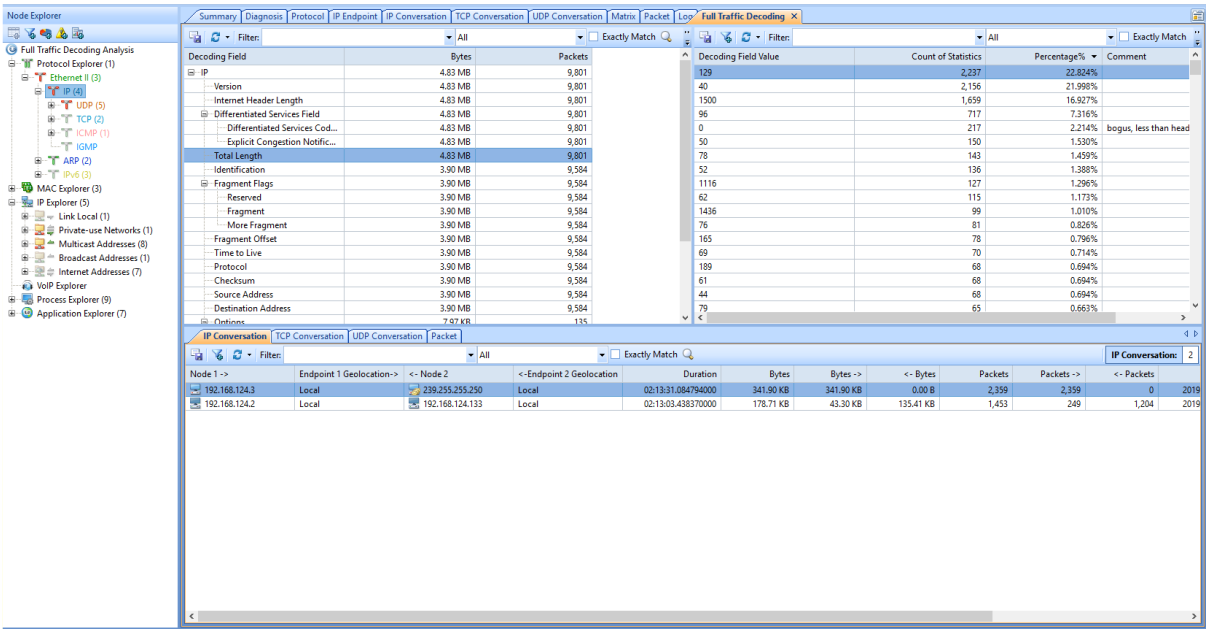
- **Copy**: Copies the data and puts it on the clipboard.
- **Copy HEX**: Copies the HEX digits and puts it on the clipboard.
- **Copy Text**: Copies selected text in ASCII/EBCDIC decoding area.
- **Display in ASCII Code**: Shows the decoded information as ASCII.
- **Display in EBCDIC Code**: Shows the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

Full Traffic Decoding

You not only can add names to Name Table, but also can use *Address Resolver* to auto-resolve The view of full traffic decoding uses the protocol as the statistical object to display all the decoding fields under a certain protocol, the field values corresponding to the fields, and the session statistics and packet statistics of the fields.

1. Full Traffic Decoding View

Choose a specific protocol in Node Explorer such as IP, TCP or UDP. The full traffic decoding view is shown below:



The full traffic decoding view details the statistics of the session and packet statistics corresponding to all the decoded fields and fields in the selected protocol.

Note The full traffic decoding view will only be displayed after the protocol is selected in the Protocol Browser in the Node Browser.

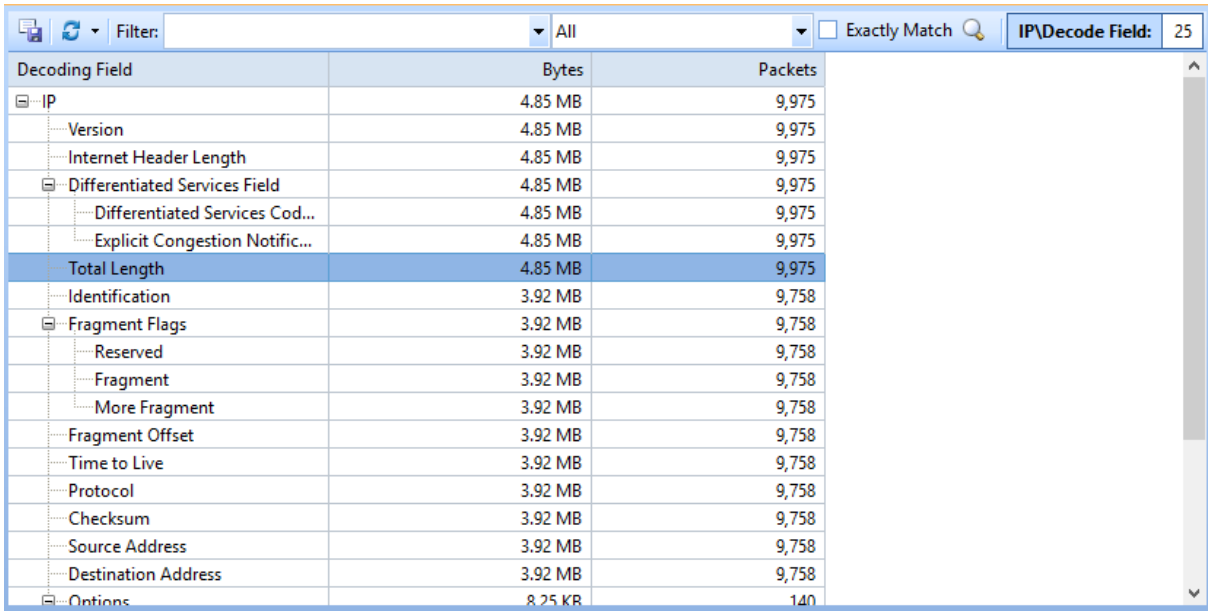
The toolbar of the full traffic decoding view is as follows:

The toolbar of the full flow decoding view from left to right functions as shown in the following table:

Function Name	Description
Export	Export all the data in the session list display area and save it to local disk in CSV format for viewing and saving as history record.
Flash	Set the view refresh interval.
Filter	Filter the condition input, you can enter any condition to quickly find the data.
All	Specific parameters can be specified in this drop-down menu to help you find data faster and improve search efficiency.
Exactly Match	A full-word match means that the search result will be displayed more accurately when it encounters a word that exactly matches the search criteria. The system does not enable full word matching by default.

2. Decoding Field Statistics

The decoding field statistics view is shown below:

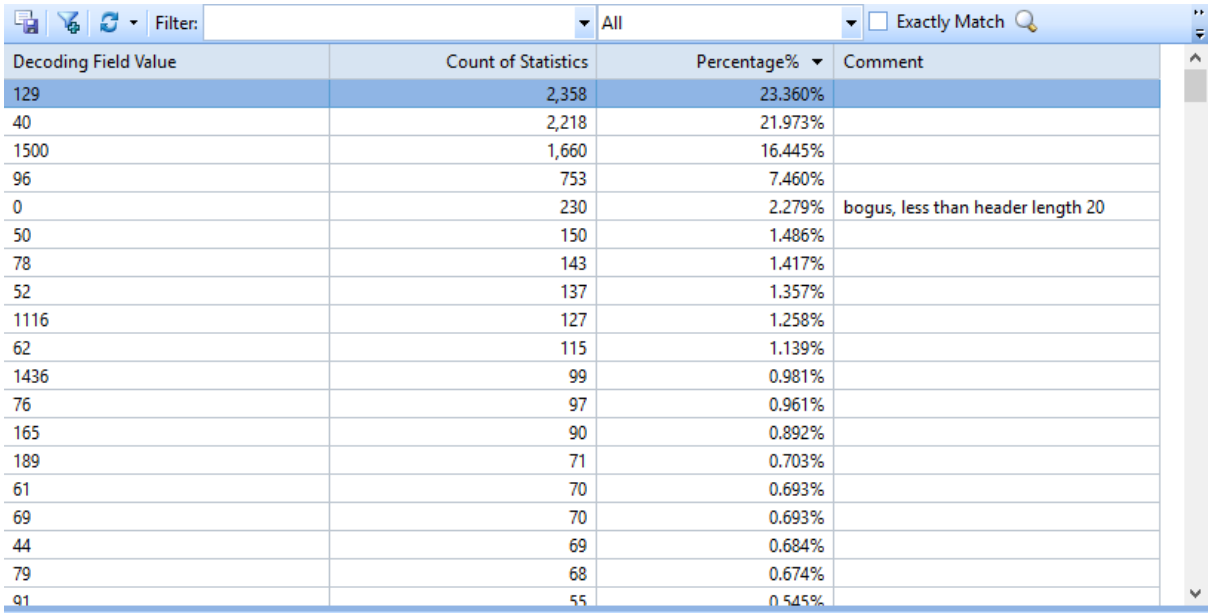


Decoding Field	Bytes	Packets
IP	4.85 MB	9,975
Version	4.85 MB	9,975
Internet Header Length	4.85 MB	9,975
Differentiated Services Field	4.85 MB	9,975
Differentiated Services Cod...	4.85 MB	9,975
Explicit Congestion Notific...	4.85 MB	9,975
Total Length	4.85 MB	9,975
Identification	3.92 MB	9,758
Fragment Flags	3.92 MB	9,758
Reserved	3.92 MB	9,758
Fragment	3.92 MB	9,758
More Fragment	3.92 MB	9,758
Fragment Offset	3.92 MB	9,758
Time to Live	3.92 MB	9,758
Protocol	3.92 MB	9,758
Checksum	3.92 MB	9,758
Source Address	3.92 MB	9,758
Destination Address	3.92 MB	9,758
Options	8.25 KB	140

The decoding field statistics view counts the number of bytes and the number of packets of all fields in the current protocol.

3. Field Value Statistics

The field value statistics view is shown below:

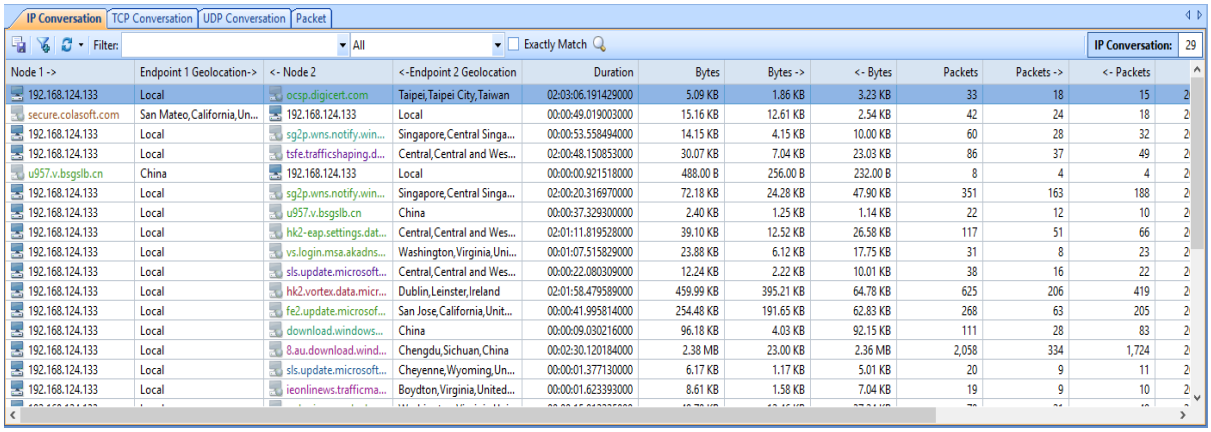

Filter: All Exactly Match

Decoding Field Value	Count of Statistics	Percentage%	Comment
129	2,358	23.360%	
40	2,218	21.973%	
1500	1,660	16.445%	
96	753	7.460%	
0	230	2.279%	bogus, less than header length 20
50	150	1.486%	
78	143	1.417%	
52	137	1.357%	
1116	127	1.258%	
62	115	1.139%	
1436	99	0.981%	
76	97	0.961%	
165	90	0.892%	
189	71	0.703%	
61	70	0.693%	
69	70	0.693%	
44	69	0.684%	
79	68	0.674%	
91	55	0.545%	

Field value statistics view details the value, number of times, percentage, and field description of the selected field.

4. Subview Display

The subview display area interface associated with the full traffic decoding view is shown below:


IP Conversation | TCP Conversation | UDP Conversation | Packet

Filter: All Exactly Match IP Conversation: 29

Node 1 ->	Endpoint 1 Geolocation->	<- Node 2	<-Endpoint 2 Geolocation	Duration	Bytes	Bytes ->	<- Bytes	Packets	Packets ->	<- Packets
192.168.124.133	Local	ocsp.digicert.com	Taipei, Taipei City, Taiwan	02:03:06.191429000	5.09 KB	1.86 KB	3.23 KB	33	18	15
secure.colasoft.com	San Mateo, California, Un...	192.168.124.133	Local	00:00:49.019003000	15.16 KB	12.61 KB	2.54 KB	42	24	18
192.168.124.133	Local	sg2p.wns.notify.win...	Singapore, Central Singa...	00:00:53.558494000	14.15 KB	4.15 KB	10.00 KB	60	28	32
192.168.124.133	Local	tsfe.trafficshaping.d...	Central, Central and Wes...	02:00:48.150853000	30.07 KB	7.04 KB	23.03 KB	86	37	49
u957.v.bsgslb.cn	China	192.168.124.133	Local	00:00:00.921518000	488.00 B	256.00 B	232.00 B	8	4	4
192.168.124.133	Local	sg2p.wns.notify.win...	Singapore, Central Singa...	02:00:20.316970000	72.18 KB	24.28 KB	47.90 KB	351	163	188
192.168.124.133	Local	u957.v.bsgslb.cn	China	00:00:37.329300000	2.40 KB	1.25 KB	1.14 KB	22	12	10
192.168.124.133	Local	hk2-eap.settings.dat...	Central, Central and Wes...	02:01:11.819528000	39.10 KB	12.52 KB	26.58 KB	117	51	66
192.168.124.133	Local	vs.login.msa.akadns...	Washington, Virginia, Uni...	00:01:07.515829000	23.88 KB	6.12 KB	17.75 KB	31	8	23
192.168.124.133	Local	sls.update.microsoft...	Central, Central and Wes...	00:00:22.080309000	12.24 KB	2.22 KB	10.01 KB	38	16	22
192.168.124.133	Local	hk2.vortex.data.micr...	Dublin, Leinster, Ireland	02:01:58.479589000	459.99 KB	395.21 KB	64.78 KB	625	206	419
192.168.124.133	Local	fe2.update.microsof...	San Jose, California, Unit...	00:00:41.995814000	254.48 KB	191.65 KB	62.83 KB	268	63	205
192.168.124.133	Local	download.windows...	China	00:00:09.030216000	96.18 KB	4.03 KB	92.15 KB	111	28	83
192.168.124.133	Local	8.au.download.wind...	Chengdu, Sichuan, China	00:02:30.120184000	2.38 MB	23.00 KB	2.36 MB	2,058	334	1,724
192.168.124.133	Local	sls.update.microsoft...	Cheyenne, Wyoming, Un...	00:00:01.377130000	6.17 KB	1.17 KB	5.01 KB	20	9	11
192.168.124.133	Local	ieonlinews.trafficma...	Boydton, Virginia, United...	00:00:01.623393000	8.61 KB	1.58 KB	7.04 KB	19	9	10

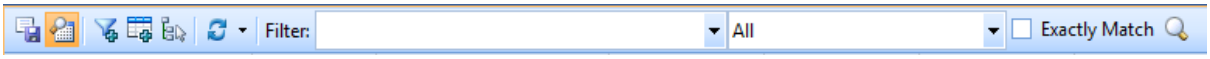
The subview display area counts sessions and packets containing the currently selected field.

Service Analysis

The service view counts and analyzes the communication status of each service according to various parameters such as IP address, port, geographic location, data packet, number of bytes, and load. You can learn the communication status of each service in detail.

1. Toolbar

The application view toolbar is shown below:

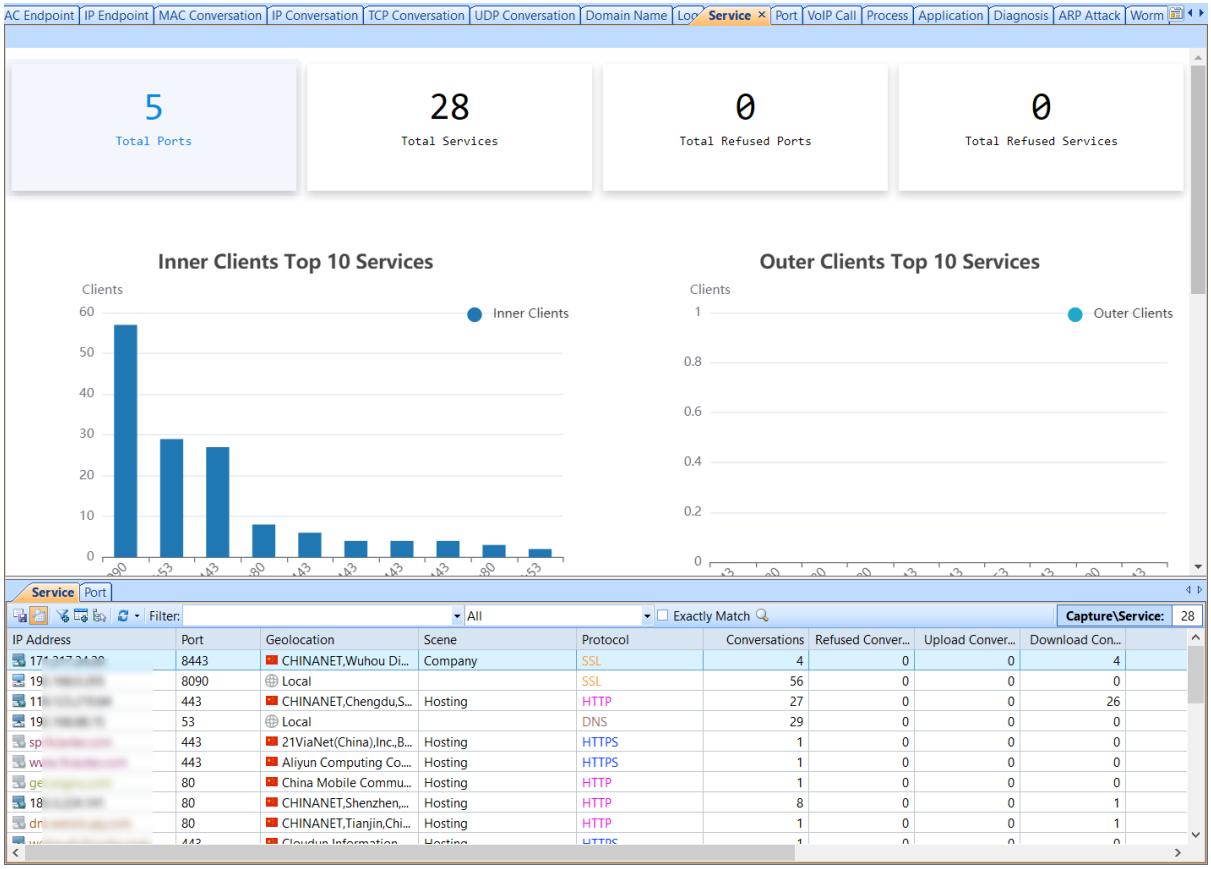


The toolbar's functions are shown from left to right in the following table:

Function Name	Description
Export	Export all the data in the session list display area and save it to local disk in CSV format for viewing and saving as history record.
Details	Hide or display application-related protocols, TCP, UDP windows.
Make Filter	Select a specific node to add it to the filter to generate a new filter.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.
Locate in Node Explorer	Select a specific node, click this button, directly locate the node in the node browser, and view other details of the node.
Flash	Set the view refresh interval.
Filter	Filter the condition input, you can enter any condition to quickly find the data.
All	Specific parameters can be specified in this drop-down menu to help you find data faster and improve search efficiency.
Exactly Match	A full-word match means that the search result will be displayed more accurately when it encounters a word that exactly matches the search criteria. The system does not enable full word matching by default.

2. Service statistics list

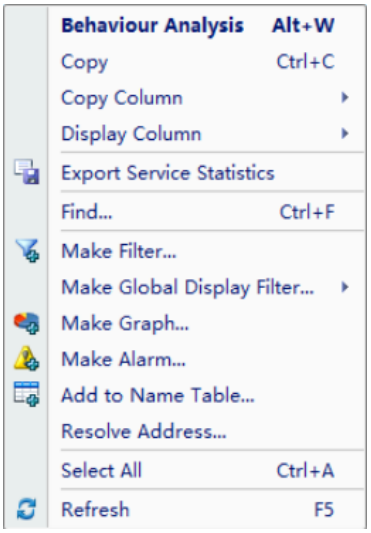
The service statistics list view is shown below:



The service view details the communication status of each service. In the sub-window of the view, the association displays the TCP and UDP session information included in the currently selected service.

Tips Select the field column and right-click or directly click on the custom column in the context menu. You can select more fields you want to view and select Reset to return to the default settings.

Service statistics support the right-click menu function, as shown below:



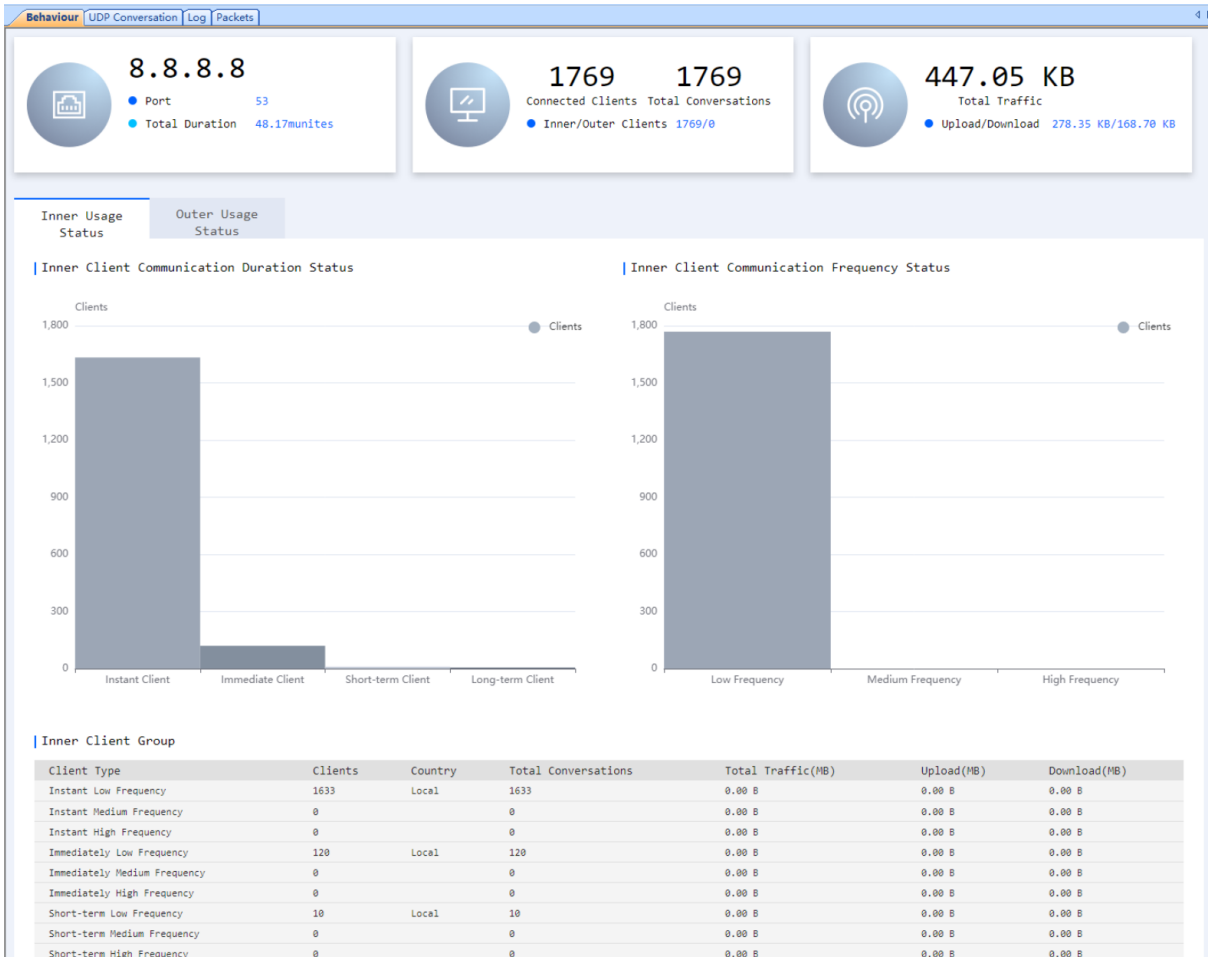
The specific functions are as follows:

Function Name	Description
Behavior Analysis	View Behavior, TCP conversation, UDP conversation, log and packets information in a new window.
Copy	Copy the information in a selected session list.
Copy column	Select to copy a field, such as Node1, Node2, Packet Number, etc.
Display column	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Export Service Statistics	Choose to increase the fields you want to view the relevant information of the node, such as the number of packets per second, the number of bytes per second, and so on.
Find	Enter to search the session you want. Support Fuzzy Search and Search Statistics.
Make filter	Select a specific node to add it to the filter to generate a new filter.
Make Graph	Select a specific node or segment to add it to the chart view and generate a new chart to help view the analysis.
Make Alarm	Select a specific node or network segment to add it to the Alerts view to generate new alerts to help you discover new issues in your network in a timely manner.
Add to Name Table	Select a specific node to add it to the name table, generate a new record in the name table and save it.
Resolve address	By proactively parsing the session you selected, you can get the IP address of the node to accurately determine which host on the network this IP node is.
Locate in Node Explorer	After clicking, the system automatically selects the current application in the application node browser.
Select All	Check all apps in the statistics list.

Reflash	Refresh the session statistics list.

3. Pop-up window display area

The pop-up window display area interface is shown below:



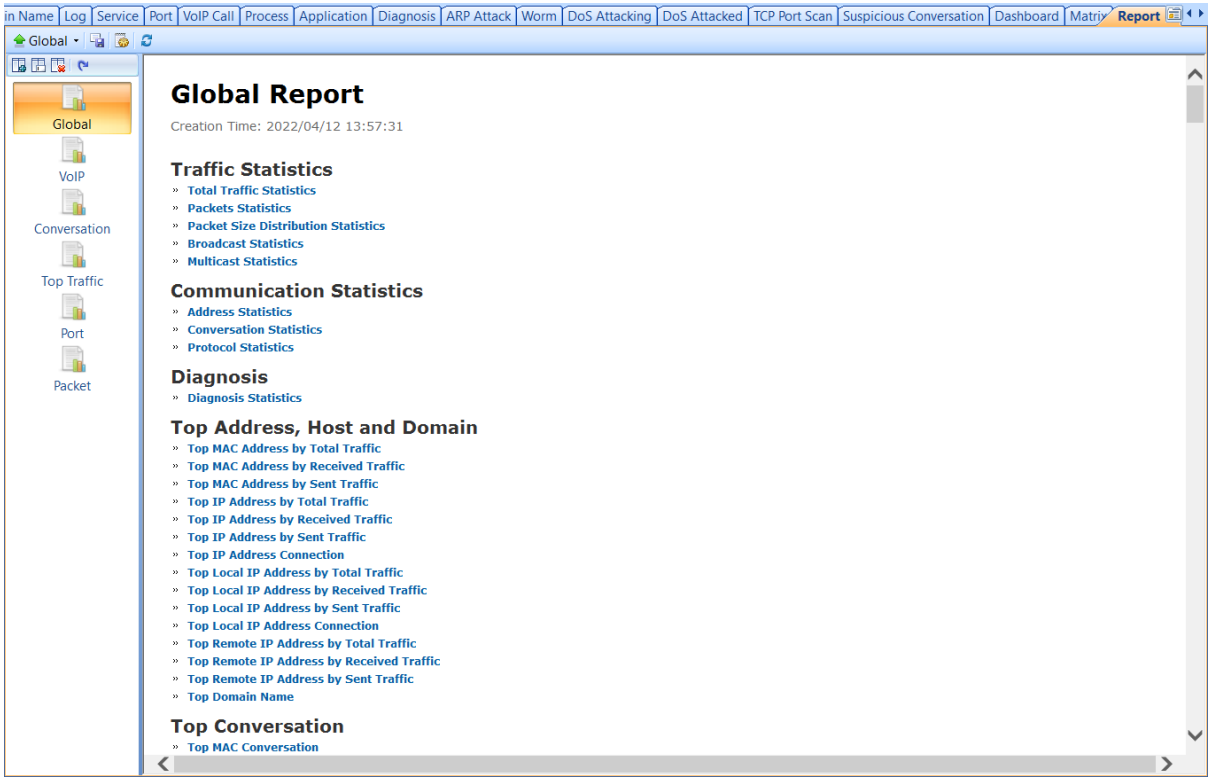
In the toolbar, click the "Behaviour Analysis" button to open the application-related subview, which details the Behaviour, TCP conversation, UDP conversation, log and packets information of the selected service.

Reports

The Report view

The Report view provides real-time traffic statistics of the whole network, including two parts: a left panel and a right panel. The left panel contains all reports and the right panel shows the report which is selected on the left panel.

By default, the left panel contains seven reports, as the figure below:



The Global Report contains all report items for an analysis project, and the VoIP Report records the statistics for VoIP analysis, and the like. You can click the report name to view the report.

Please note that the "Wireless" report is only available when you monitor a WiFi network, and the "VoIP" report is only available when the VoIP analysis module is enabled.

Besides the default reports, you can create new reports (see Creating report for details).

All reports consist of three sections: Report Header, Report Body, and Report Footer.

- Report Header section displays report name, report create time, company logo on the report, and company name.
- Report Body section 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, report viewers can have a clear understanding of the percentage comparison.

- Report Footer section displays the name of report creator.

By default, report create time, company logo, company name and report author are invisible. To show or to modify these settings, just click  (see Report Settings for details).

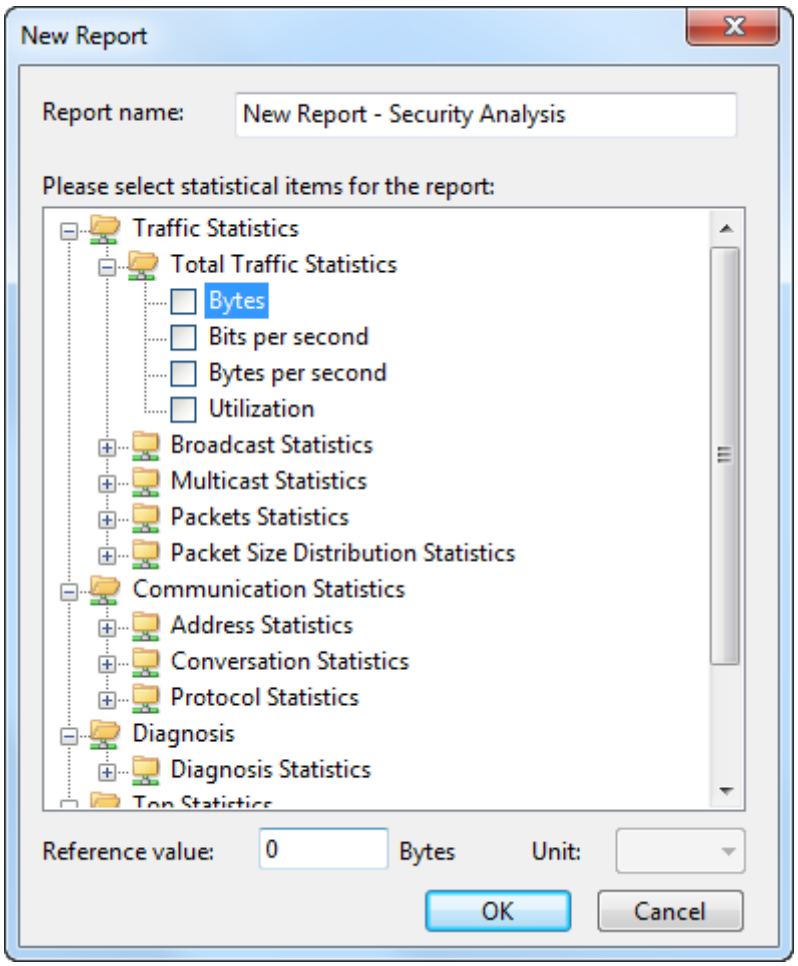
To save a report, just click  to save it. You can save a report .pdf or .html format.

Creating report

Capsa allows users to create reports according to need. The report can be defined based on the whole network or on a specified node.

To create a report for the whole network, follow the steps below:

1. On the Report view, click  to open 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 Settings for all report items).
4. Click **OK** to save the definitions.

To create a report based on a specified node, follow the steps below:

1. In **Node Explorer**, select a node that you want to make report about; click  on the toolbar to pop-up the **New Report** dialog box.
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.
4. Click **OK** to save the definitions.

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:

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: MAC 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 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 MAC Conversation, Top IP Conversation, Top TCP Conversation, Top UDP Conversation
- Top Application: Top Application Protocol

VoIP Statistics

- VoIP Diagnosis Statistics: SIP Client Authentication Error, RTP Packet Loss, RTP Packet Out of Sequence
- VoIP Call Status Statistics: Calls in Dialing, Calls in Talking, Closed Calls, Failed Calls, Total Calls
- VoIP MOS Distribution: Good, Fair, Bad, N/A

Top VoIP Statistics

Top Address and Host: Top IP by Call Frequency, Top IP by Call Duration, Top IP by Call Traffic

User Activity Logs

User activity logs record the network activities of a user. Capsa provides following log types:

- The Log view
- Global Log
- DNS Log
- Email Log
- FTP Log
- HTTP Log
- VoIP Call Log
- VoIP Signaling Log

Note What log types will display in an analysis project depends on the analysis modules selected.

The 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.

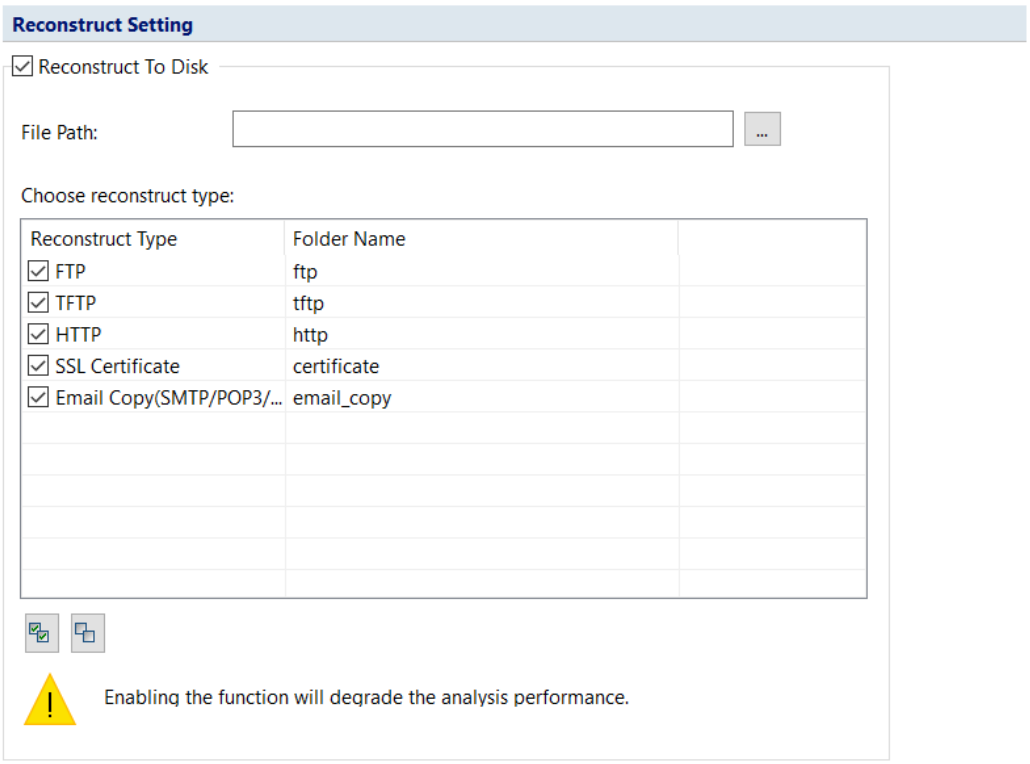
The Log view includes two parts: a left panel and a right panel. The left panel lists all the log types of current analysis settings and the right panel lists the logs of the corresponding log type which is selected on the left panel. Users can sort the logs according to the statistic parameters.

You can save the log list of current log type by clicking  on the toolbar. Furthermore, the logs can be automatically saved since the start of a capture. See Log Output for more information.

Note The logs will be displayed only when the log type is enabled. See Reconstruct Settings

Capsa is able to extract and fully reconstruct the files transmitted over FTP, TFTP, and HTTP, as well as SSL certificates.

To reconstruct files, enable the checkbox **Reconstruct To Disk** as the screenshot below, set the path to store the files to be reconstructed, and the reconstruct types.

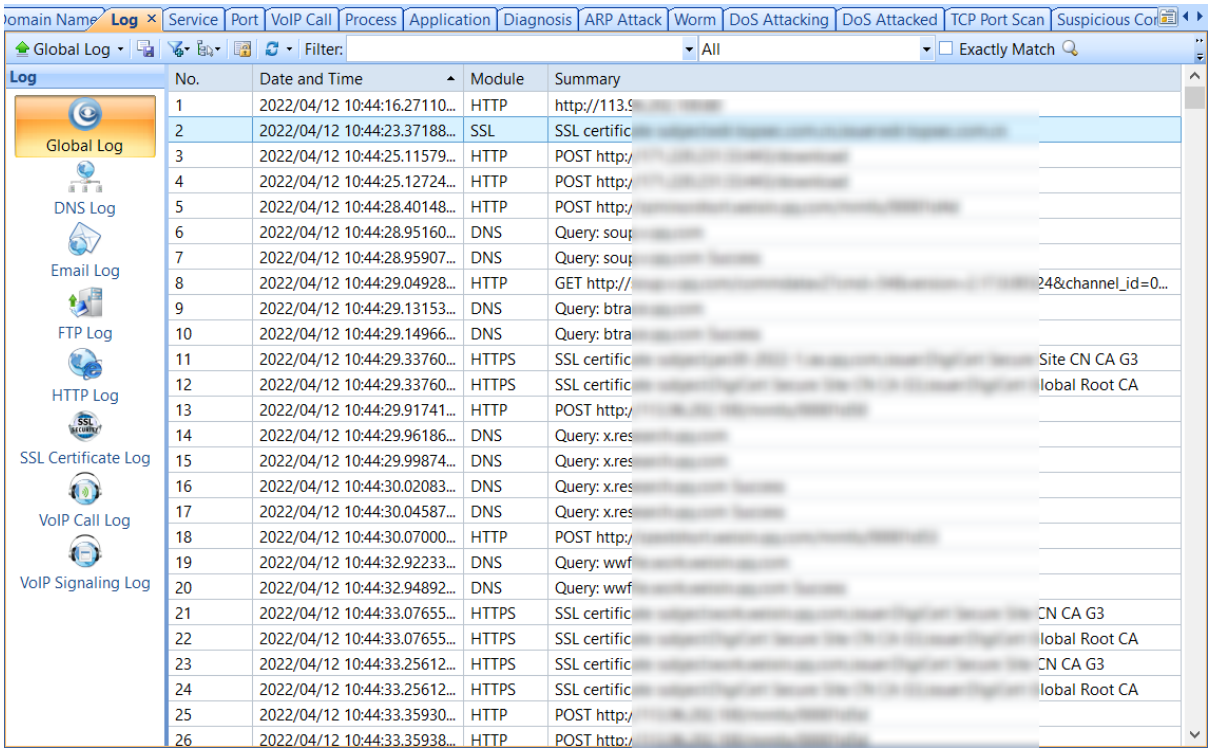


Note Enabling the reconstruction function will affect the system analysis performance a lot.

Log View for more information.

Global Log

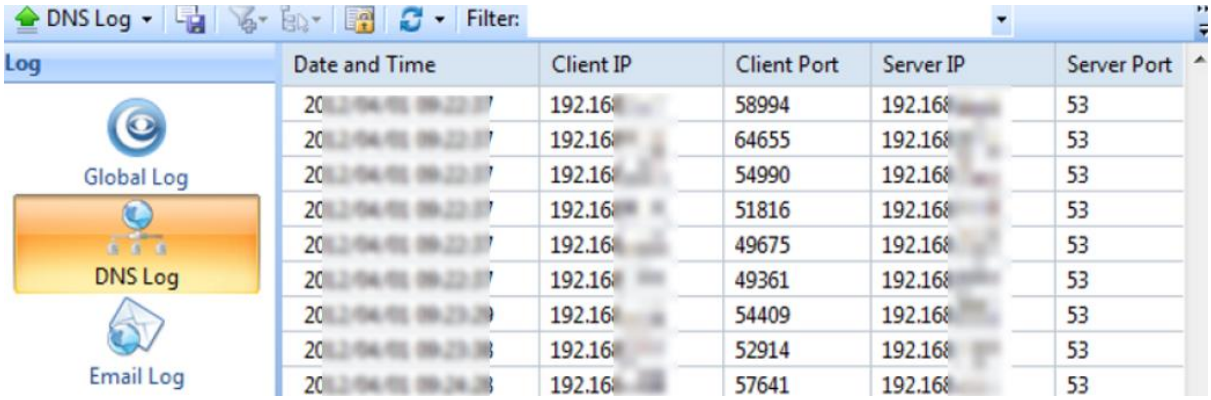
The **Global Log** collects the logs of other seven log types and displays the log information based on date and time. It appears as below.



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

DNS Log

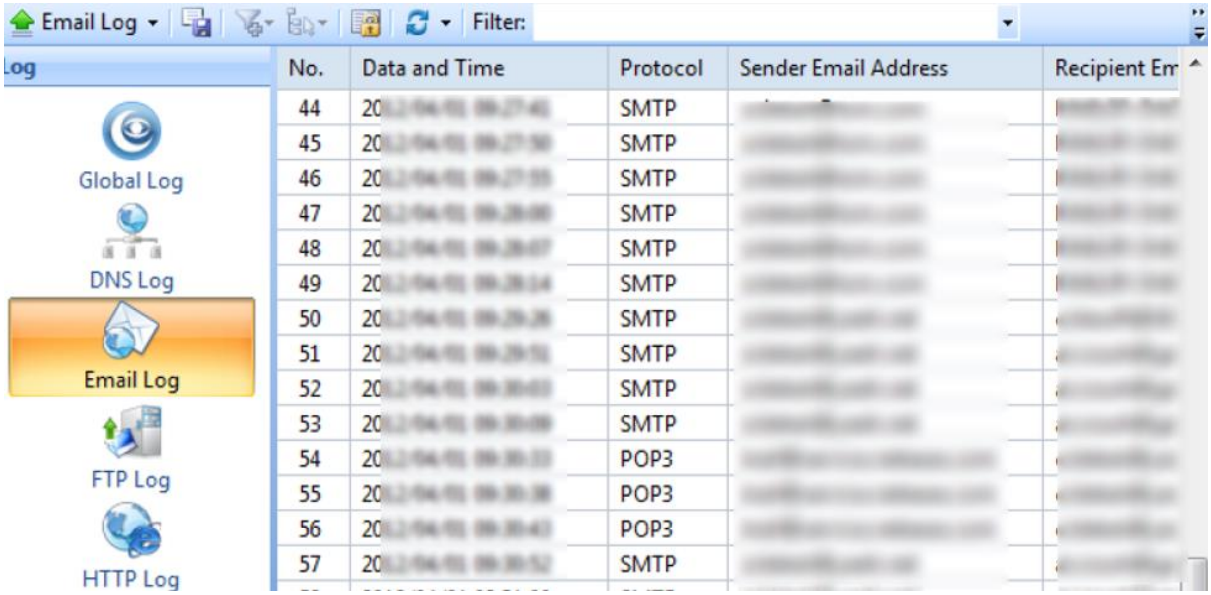
The **DNS Log** records DNS query application. It appears as below.



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

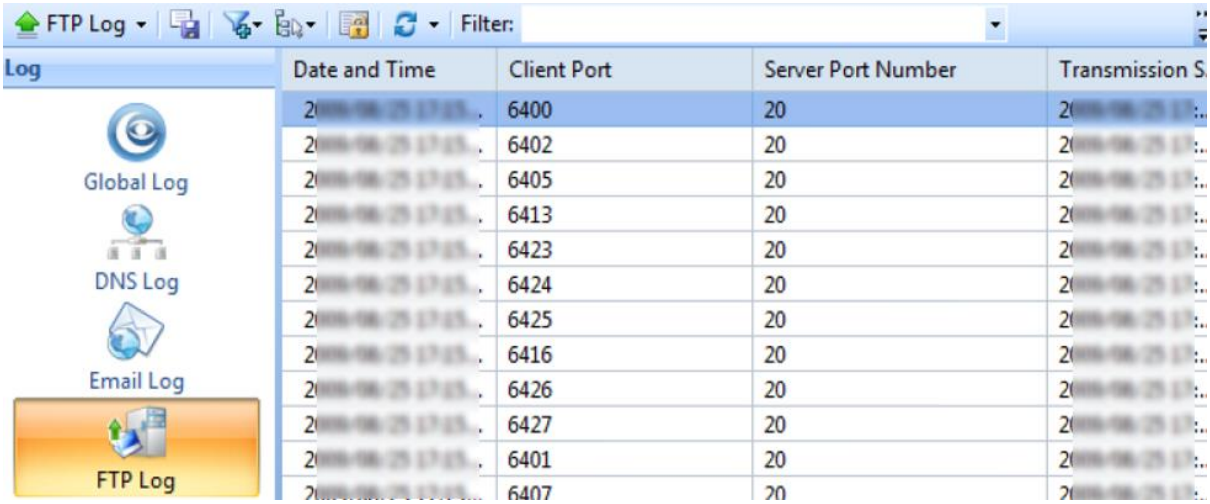
The **Email Log** records the information about the emails sent and received using SMTP and POP3 protocols. Double-click any item of the email log list, the email will be opened. It appears as below.



The Email Log includes columns **No.**, **Date and Time**, **Protocol**, **Client MAC**, **Client IP**, **Client Port**, Client Geolocation, **Server MAC**, **Server IP**, **Server Port**, Server Geolocation, **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

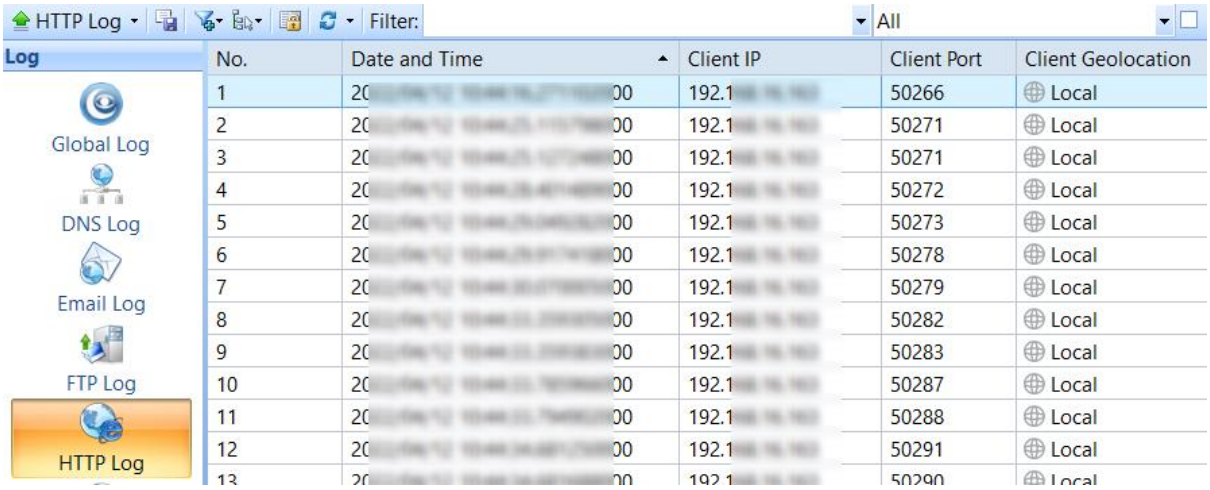
The **FTP Log** records the uploading and downloading from FTP server. It appears as below.



The **FTP Log** includes columns **No.**, **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, Client Geolocation, **Server IP**, **Server Port**, Server Geolocation, **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.

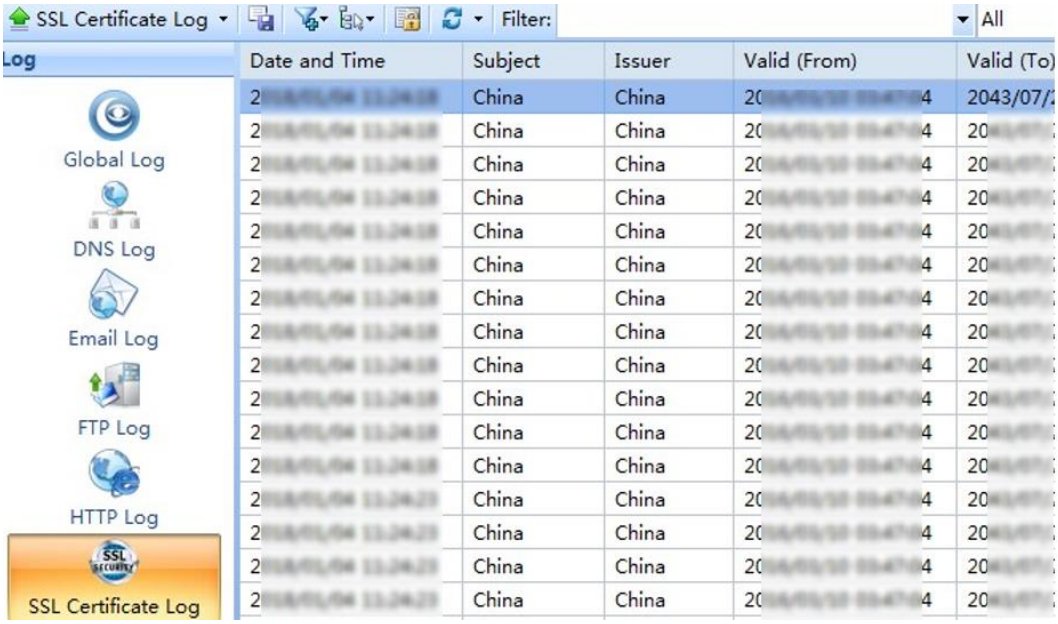


The **HTTP Log** includes columns **No.**, **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, Client Geolocation, **Server MAC**, **Server IP**, **Server Port** Server Geolocation**, Requested URL**, **Method**, **User Agent**, **Quote**, **Content Length**, **Content Type**, **Authentication**, **Client HTTP Version**, **Duration**,

Average Speed (Bps), X-Forwarded-For, **Status Code** and **Server Response**. To show a column, right-click the column header and select the column.

SSL Certificate Log

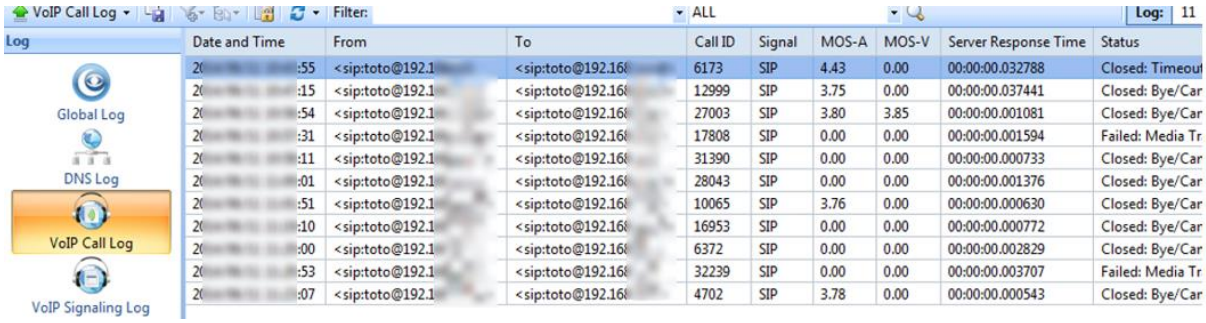
The **SSL Log** can detailedly count detailed log information that are extracted from SSL Certification. It appears as below.



The **SSL Log** includes columns **No.**, **Date and Time**, **Client MAC**, **Client IP**, **Client Port**, **Server MAC**, **Client Geolocation, Server IP, Server Port, Server Geolocation, Protocol, Certification Version, Subject, Issuer, Signature Algorithm, Valid(From), Valid(To) and Certificate File Path.** To show a column, right-click the column header and select the column.

VoIP Call Log

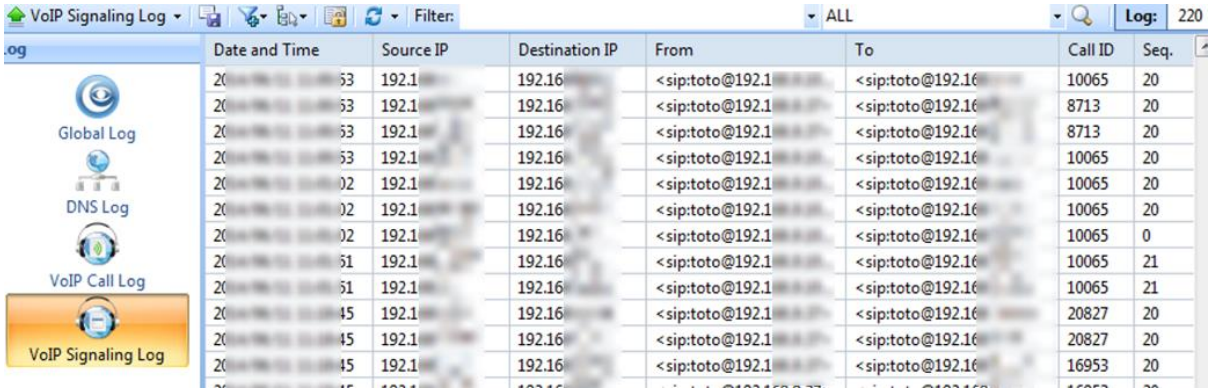
VoIP Call Log records VoIP calls. One VoIP call is recorded as one VoIP Call Log.



VoIP Signaling Log includes columns No.,**Date and Time**, **Caller**, **Callee**, **Call ID**, **Signal**, **MOS-A**, **MOS-V**, Talking Timeand **Status**. To show a column, right-click the column header and select the column.

VoIP Signaling Log

VoIP Signaling Log records the details of VoIP calls.



VoIP Signaling Log includes columns No., **Date and Time**, **Source IP**, **Destination IP, Source Geolocation, Destination Geolocation, Caller, Callee**, **Call ID**, **Summary**, Talking Time and **Status**. To show a column, right-click the column header and select the column.

Configurations in Capsa

About Global Configurations

Global Configurations mean the configurations for an analysis project. Global configurations include configurations as follows:

- Analysis Settings, including Basic Settings of the analysis settings, Node Group, Name Table, Alarm Settings, Analysis Object, Packets Buffer, Packet Filter, Log Output, Log display 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.

Before using Capsa to capture network traffic, you may do some configurations about the program, like configurations for system options and analysis 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 and the selection on analysis settings.
- The keys for APs.
- All settings for analysis settings.
- 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 and the selection on analysis settings will be memorized only when these selections are applied to an analysis project.

Configurations backup

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 **File** button, point **Configuration Backup** and select **Export** to export the global configurations as a local file.
- To import global configurations, click **File** button, point **Configuration Backup** and select **Import**.

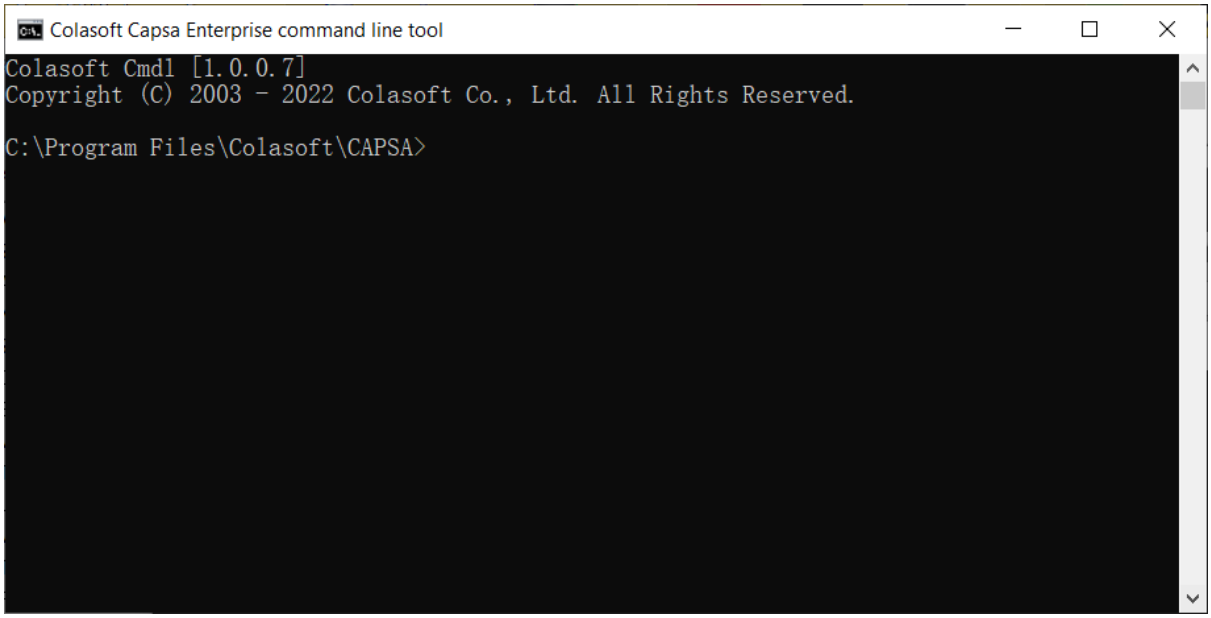
When a configuration backup file is imported, Capsa will automatically restart to make the configurations take effect.

Command Line Using

Capsa provides the command line mode. Users can do real-time analysis and replay packets to analyze the network through command lines.

Command Line Tool

Capsa provides command tool for analysis through command lines. Choose Start > All Programs > Colasoft Capsa > Colasoft Capsa command line tool to open the tool.



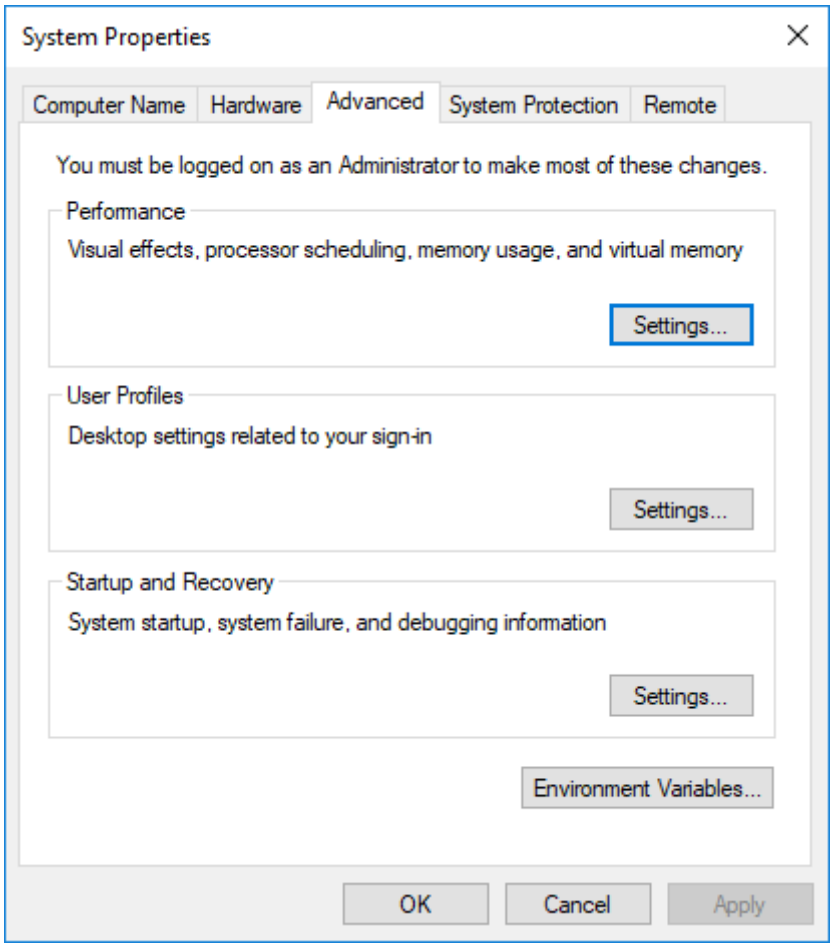
For using guide, please run cmdl --manual command to open the online help.

Command Line Introduction

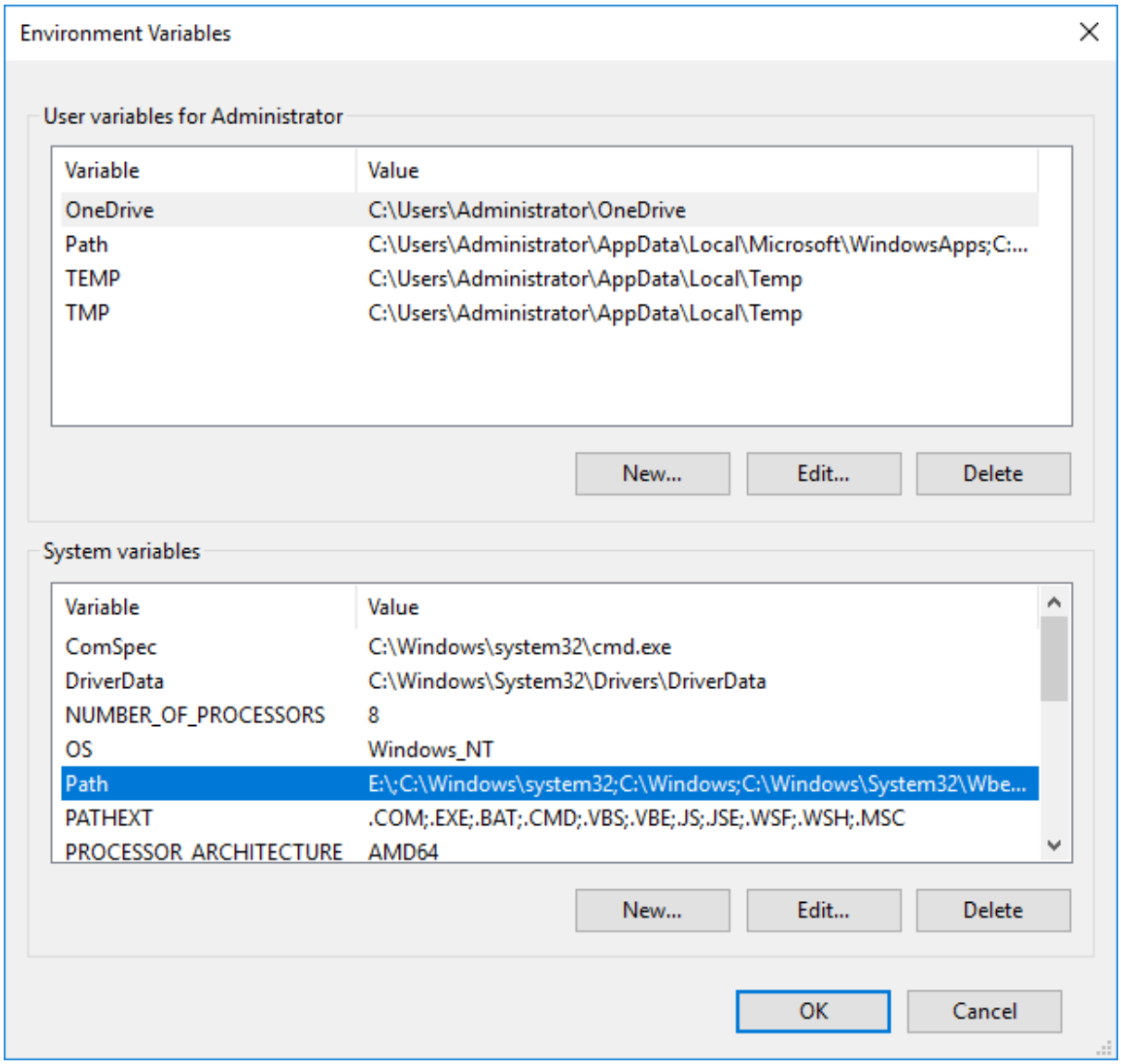
Environment Variables Setting

Before using command lines, users should finish environment variables setting, adding the path of the file named "cmdl.exe" to environment variables. The steps are shown below (Take Windows 10 flagship version for example):

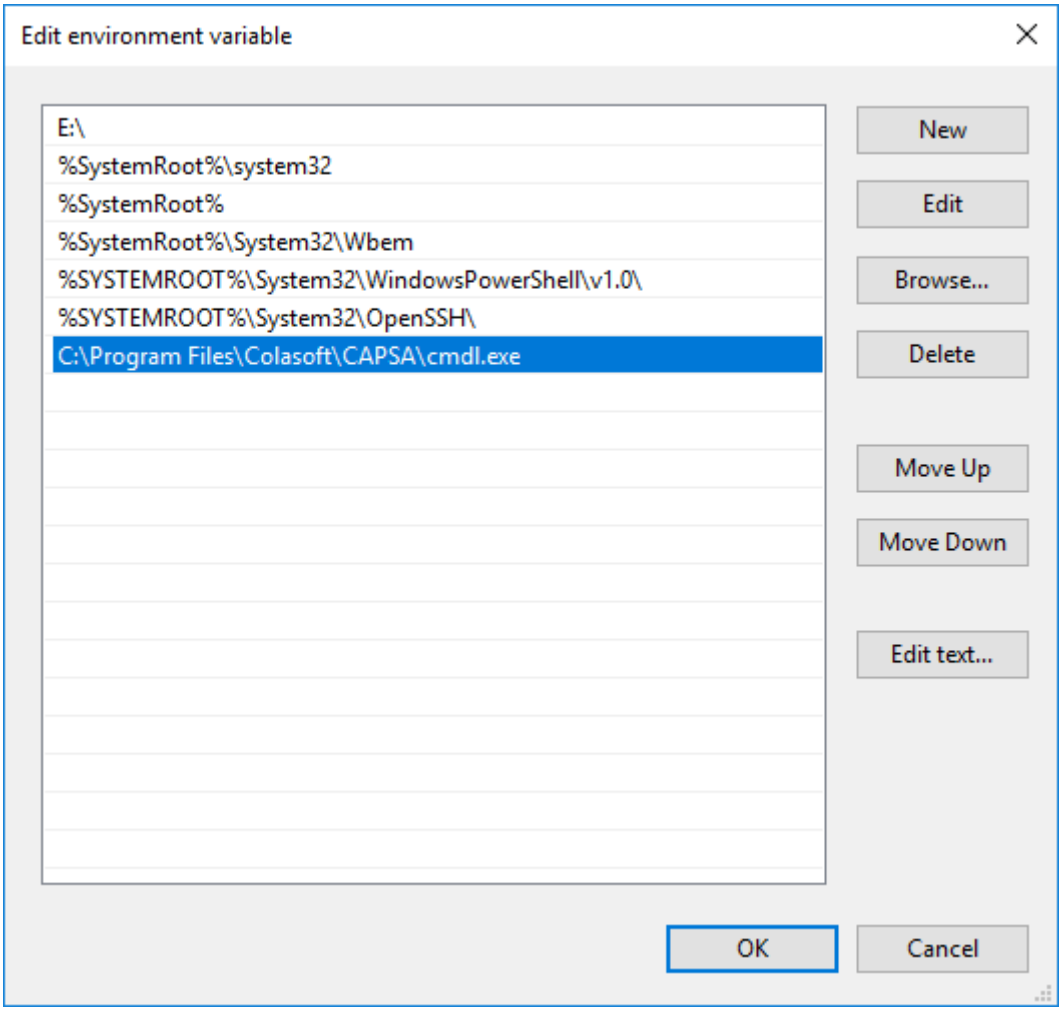
1. Right-click This PC on the desktop, choose Properties, then a dialog box pops up.
2. Choose Advanced system settings, the dialog box of System Properties pops up as shown below:



3. Click Environment Variables, a dialog box pops up as shown below:



4. Choose Path in System Variables, click Edit, the dialog of Edit System Variable pops up as shown below:

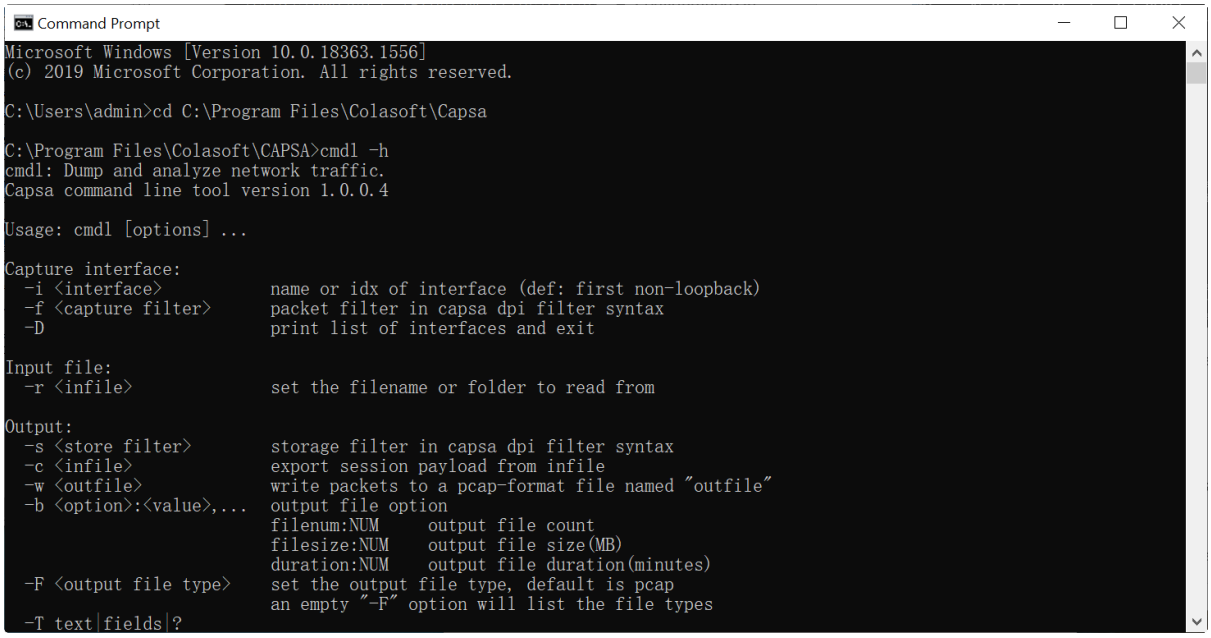


5. Add the path of the file named "cmdl.exe" to the input box of Variable value. Click OK, then environment variables setting is finished.
6. Click OK, then environment variables setting is finished.

Setting Verification

After finishing environment variables setting, users should verify whether it is successful. The steps are shown below.

1. Click Start, input "cmd" in the box of Search programs and files, click Enter, then the window of cmd pops up.
2. Input “cd path of the file named cmdl.exe”,eg, input “cd C:\Program Files\Colasoft\CAPSA\cmdl.exe”. Click Enter.
3. Input "cmdl -h", click Enter, if there is the content as below, it means the setting is successful:



4. If there isn't such content as above, please check whether environment variables setting is right.

Parameters Instruction

Instruction of parameters used in command lines:

Command	Description	Example
-?, -h	Show help information	cmdl -? cmdl -h
-v	Show version information	cmdl -v
-D	List name and numerical index of each network interface	cmdl -D
-i	-i <interface>: network interface name or index (default: first non-loopback interface) Set network interface name used for real-time packet capture. The network interface name can use the name listed by "cmdl -D" or the number index. Only single adapter is supported.	Capture packets from adapter ent0: cmdl -i eth0 cmdl -i 1
-f	-f <analyze filter>: packet analysis filter Set packet analysis filter.	Capture packets of specific host from adapter etho: cmdl -i eth0 -f "ip=192.168.1.1" Only capture packets whose protocol is tcp and destination port is 100:

	Only packets that meet the filter conditions will be used for decoding and analysis. Support Capsa dpi filter rules. If the filter string contains special symbols such as ||, && or spaces, it must be marked with double quotation marks "".	cmdl -f "protocol=tcp and dstport=100"
-r	-r <infile>: packet filename or path Set the file name and path of playback packets. Support setting multi - file, multi - directory, file directory mix.	cmdl -r test.pcap -r packet.pcap cmdl -r test.pcap -r D:/packet/
-s	-s <store filter>: packet storage filter Set the raw packet storage filter (can be used with -w parameter); Only the packets that meet the filtering conditions will be stored in the original packet file. Support Capsa dpi filter rules. If the filter string contains special symbols such as ||, && or spaces, it must be marked with double quotation marks "".	Stores packets with the specified protocol such as TCP, UDP, DNS, ICMP, HTTP, etc. : cmdl -i eth0 -s "protocol=tcp" -w proto.pcap
-c	-c <infile>: packet filename or path Export the load data of all TCP/UDP conversations in the specified packet file or directory to the -w specified path (can be used with -w parameter). Support setting multi - file, multi - directory, file directory mix.	cmdl -c vt.pcapng –w D:/output_folder/
-w	-w <outfile>: output file or path Set the output file of raw data or the output path of conversation data. By default, CMDL will output the decoding results to stdout. If you want to output the decoded results to a file, use the	Set the output file of raw data: cmdl -w output_packet.pcap Set the output file of decoding result: cmdl -T fields -e dstip –e dstport -E header=y > output_fields.txt

	redirect ">" instead of the -w parameter.	
-b	-b <option>:<value>,...: options: value,... Set the option to output packet files; Specifies options including: **filenum**: Number of files. If the number of files exceeds, the earliest generated files will be deleted, and all files will be retained by default. **filesize:** Size of files. Unit is MB. If it exceeds, a new file will be generated. Default is 1MB. **duration:** File duration. Unit is minute. If it exceeds, a new file will be generated. Default is 1minute. Command rule: A -b command supports setting multiple options, separated by commas ", ". When the same option is set multiple times, the latter option overrides the previous option. This command takes effect only if the -w command is set.	Capture the packets and generate the packets file, only the last 5 files are kept. Each file size is 5MB. The file name prefix is test, and the format is capsa5/ PKT: cmdl -w D:\output_folder\test.cscpkt –F capsa5/pkt –b filenum:5,filesize:5
-F	-F <output file type>: output raw file type Set the file format output of the -w option, the default is Libpcap-nanosecond/cap. Use -F to list all available formats.	cmdl -F capsa5/cscproj -w D:/output_folder/output_packet.cscproj
-T	-T text|fields: packet decoding information output format (default: text) Set the output format of packet decoding information, including: **fields**: the name of the field specified with -e, and the format is specified by the -E option.	cmdl -r packet.pcapng -T fields -e ip -E header=y cmdl -T text -r packet.pcapng cmdl -T text -r packet.pcapng >output_summary.txt

	text: Statistics information of each packet.	
-e	-e <field>: output field name If the -T fields option is specified, -e is used to specify the name of the output field. Support Capsa dip filter fields. Support for multiple -e settings for multiple output fields.	cmdl -T fields -e ip cmdl -T fields -e ip -e dstip
-E	-E <fieldsoption>=<value>: option=value If the -T fields option is specified, -E is used to set parameters of output formats, including: **bom=y|n:** Output utf-8 BOM **header=y|n:** Whether the first line prints the field name (similar to the header) **separator=/t|/s|<char>:** The field separator is tab, space or printable character. **quote=d|s|n:** Output values use double, single, or no quotes.	cmdl -T fields -e ip -E header=y
-l	-l <module>,...<option>=<value>: module, option = value,... Generate log file and its option settings. module: Specific module to generates logs, including: http_apache, http_extend, diagnosis, global, dns, email, ftp, ssl, voip_call, voip_event option: specific option, including: **path:** file path. **format=log|csv**: file format, log is txt format, csv is excel format. It's log by default. **filenum**: Number of files. If the number of files exceeds, the earliest generated files will be deleted, and all files will be retained by default.	Output the logs of all modules to D:\output_folder\, without dividing the log files: cmdl -l path=D:\output_folder\ Output the logs of global and dns module to D:\output_folder\, without dividing the log files: cmdl -l global,path=D:\output_folder\,dns Output logs of ssl, ftp, dns modules to D:\output_folder\, only the last 5 files will be kept, a single file lasts for 5 minutes, and the file format is text format (log): cmdl –l ssl,ftp,path=D:\output_folder\,dns,filenum=5,format=log,filesize=4,duration=5

	filesize: file size. Unit is MB. If it exceeds, a new file will be generated. Default is 1MB. **duration:** File duration. Unit is minute. If it exceeds, a new file will be generated. Default is 1minute. Command rule: The path in option must be set. Module and other options are optional. If module is not set, the logs of all modules will be output by default. If the module is set, only the log of the set module will be output. Support setting multiple modules and options at the same time, separated by commas ",". "=" means setting option, without "=" means setting module.	
-o	-o <protocol>,...path=<destdir>: protocol,... , export path Save the export object of the specified protocol to the specified directory. protocol: Specified protocols, including: all (cmdl supports all protocols of exported objects), ftp, http, ssl, tftp, email (smtp, pop3, imap4). Support to set multiple protocols at the same time, using commas ", "separated. Support not setting the protocol parameter, the default is all.	cmdl -o ftp,http,path=D:\output_folder\ cmdl -o all,path=D:\output_folder\ cmdl -o ftp,email,path=D:\output_folder\ cmdl -o path=D:\output_folder\
-eof	--eof <type>=<protocol:param1,...,protocol:paramn>: Type=Filter string Filter the exported object of the -o command.	Restore all files by default: cmdl -o ftp,http,path=D:\output_folder\ –-eof suffix Without setting the protocol, all the files with the suffix jpg will be restored:

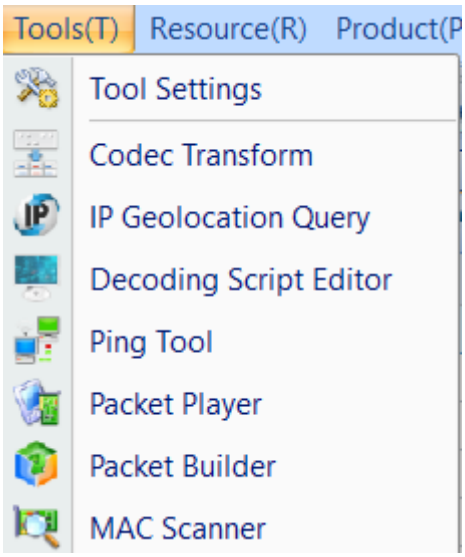
	type: specifies the type, including: suffix (file name). **Filter string rules:** An -eof command only supports a single type, setting multiple types can be achieved by setting multiple -eof commands. protocol: Specify the protocol, which is consistent with the protocol supported by the -o command. Protocol is optional (no colon ":" means no protocol is set, recognized as param). Directly write param to filter all protocols. param: the file suffix name, if the file suffix name is param, this file needs to be restored. Support to set multiple params at the same time, using comma ", "separated. If no protocol is set, no filtering will be performed and all files will be restored.	cmdl -o ftp,http,path=D:\output_folder\ –-eof suffix=jpg

Network Tools

For your convenience on network management, Capsa provides four network tools.

- Tool Settings
- Colasoft Base64 Codec
- Colasoft Ping Tool
- Colasoft MAC Scanner
- Colasoft Packet Player
- Colasoft Packet Builder

The tools are on the Tools tab:

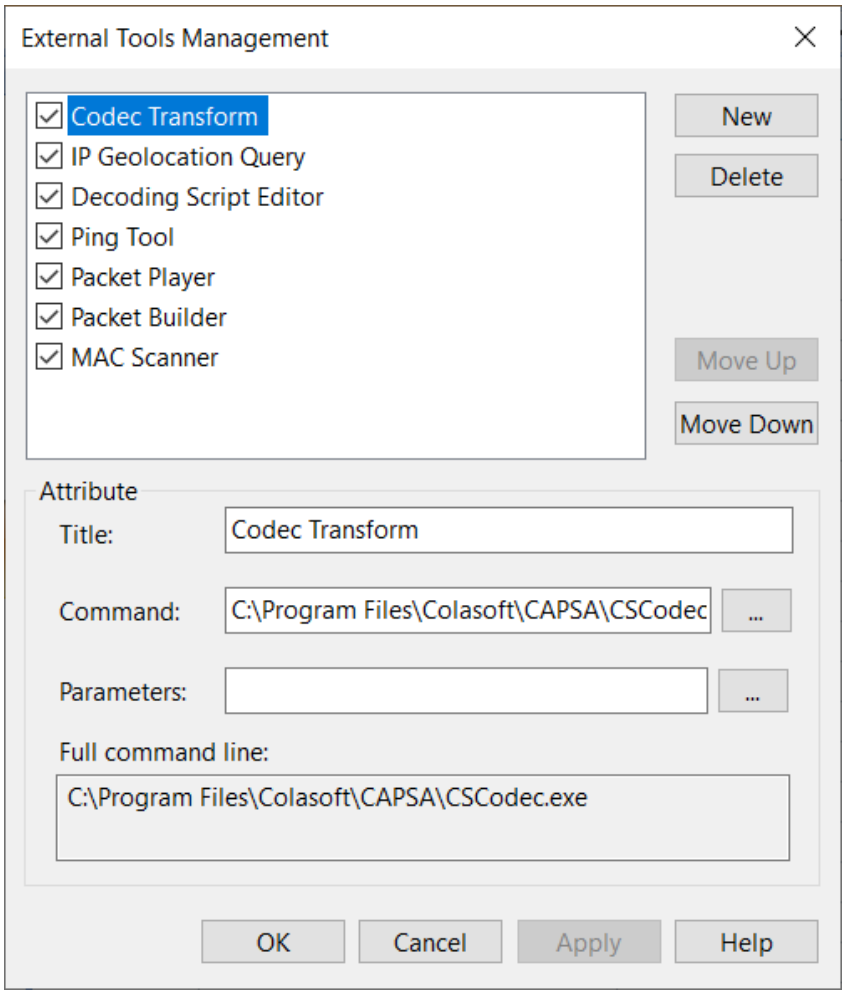


Tool Settings

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 the **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**.

Colasoft Codec Transform

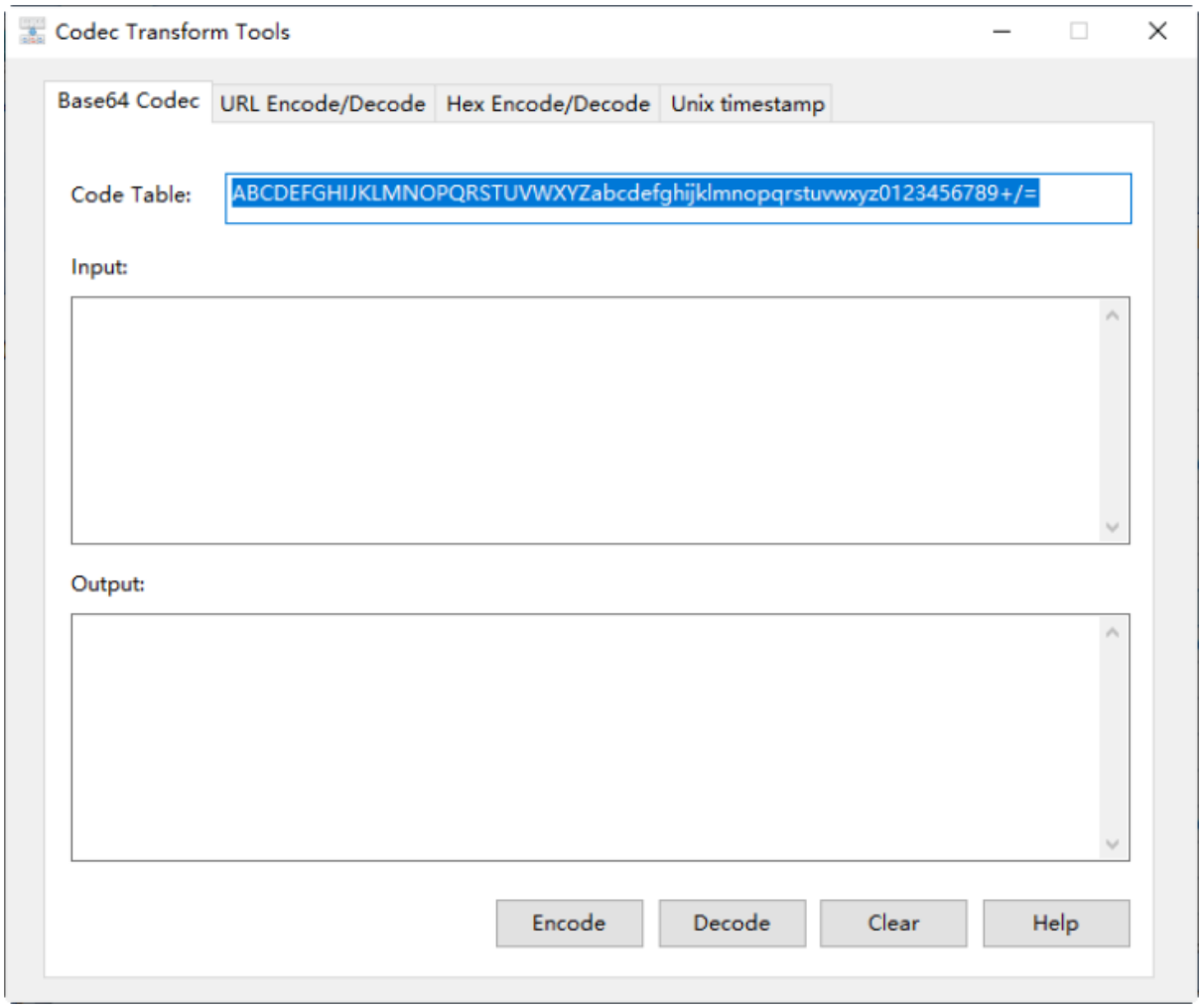
Colasoft Codec Transform is a tool for providing a variety of encoding/decoding features released by Colasoft Company.

Start

There are three ways to start Colasoft Codec Transform:

- **Start->Colasoft Capsa-> Colasoft Codec Transform;**
- Run Colasoft Capsa->Start analysis->Tools->Colasoft Codec Transform;
- **Start->Run->Input "cscodec" and press Enter.**

After starting Colasoft Codec Transform, the user interface shows as following screen shot.



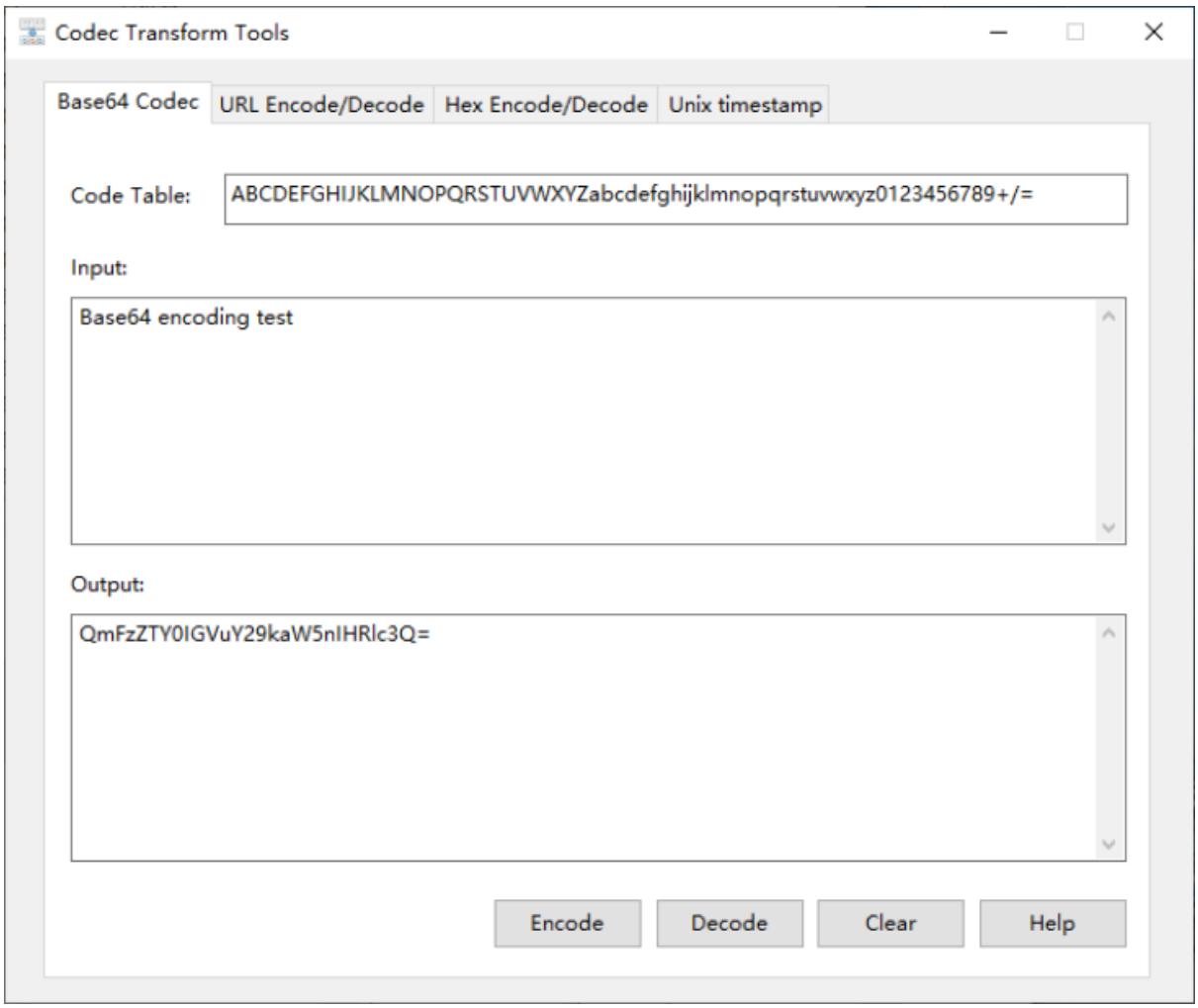
Colasoft Codec Transform includes Base 64 Codec, URL Encode/Decode, Hex Encode/Decode and Unix Timestamp four tabs.

Base 64 Codec

Base64 Encode

Please follow the steps below to encode a message:

1. Configure the code table. In most case, you could just use the default code table.
2. Put the message in the Input panel, click Encode button, and the system will display the result of encoding with Base64 method in the Output panel, as the screen shot shows below:

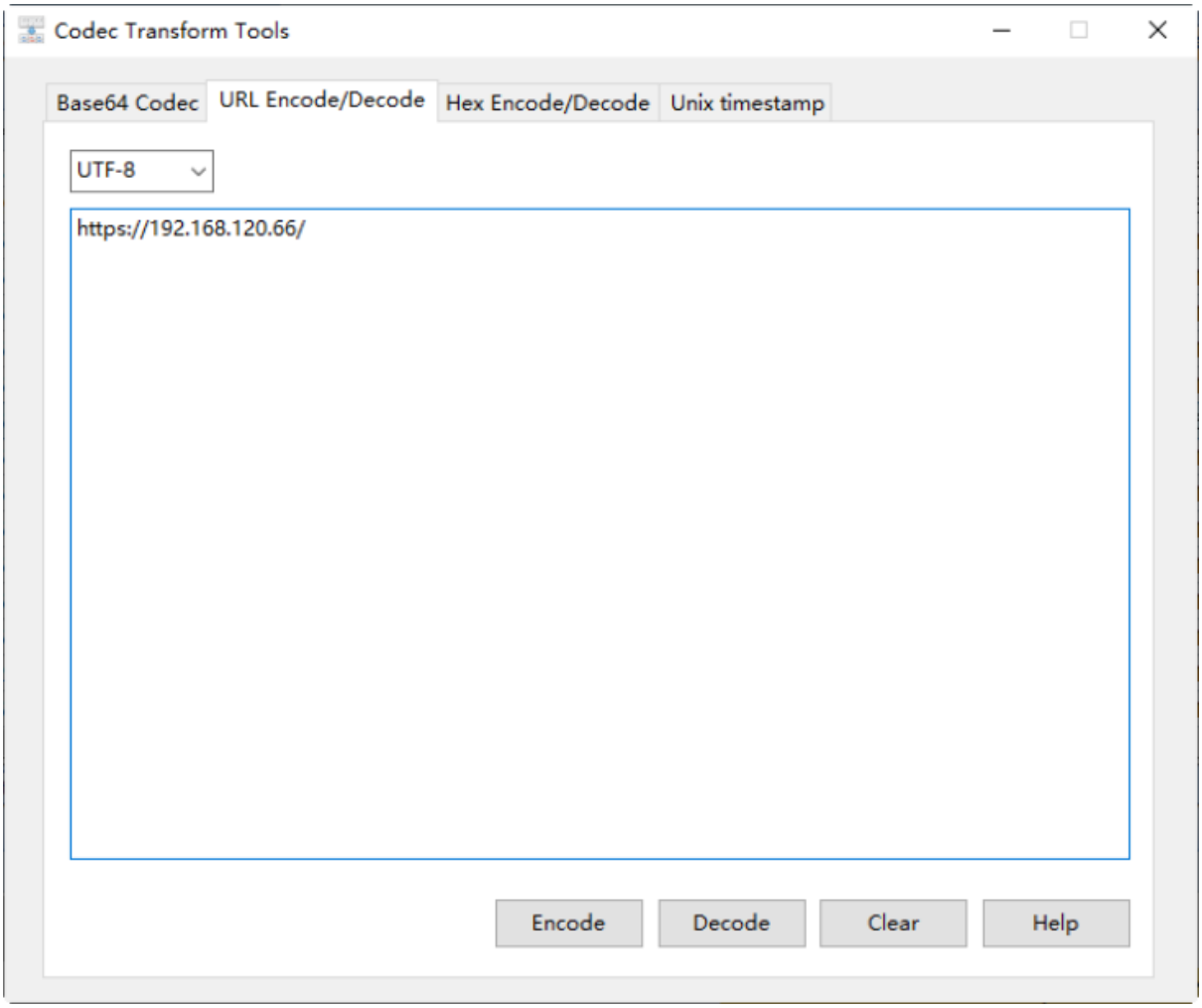


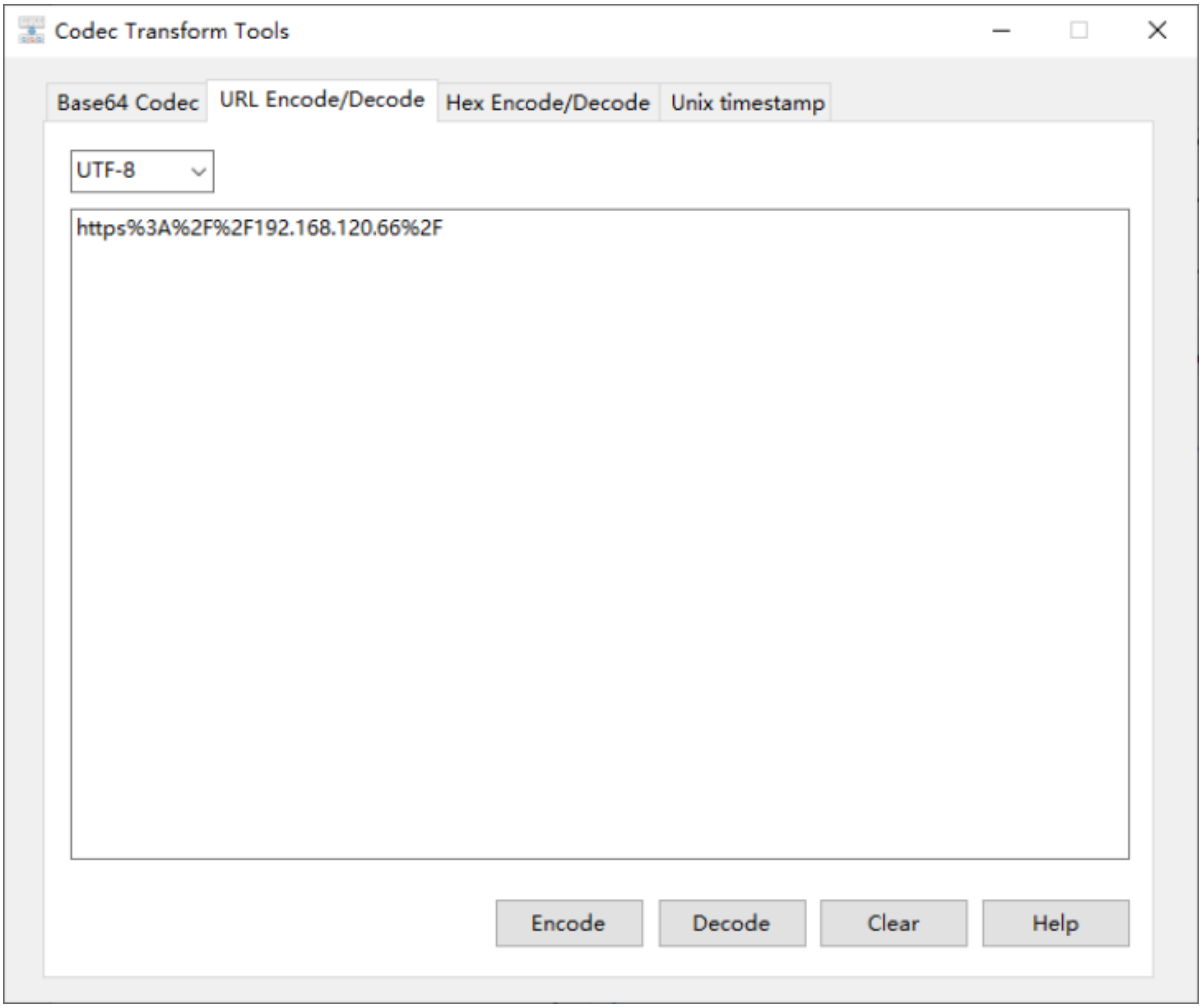
Base64 Decode

URL Encode

Please follow the steps below to decode a message:

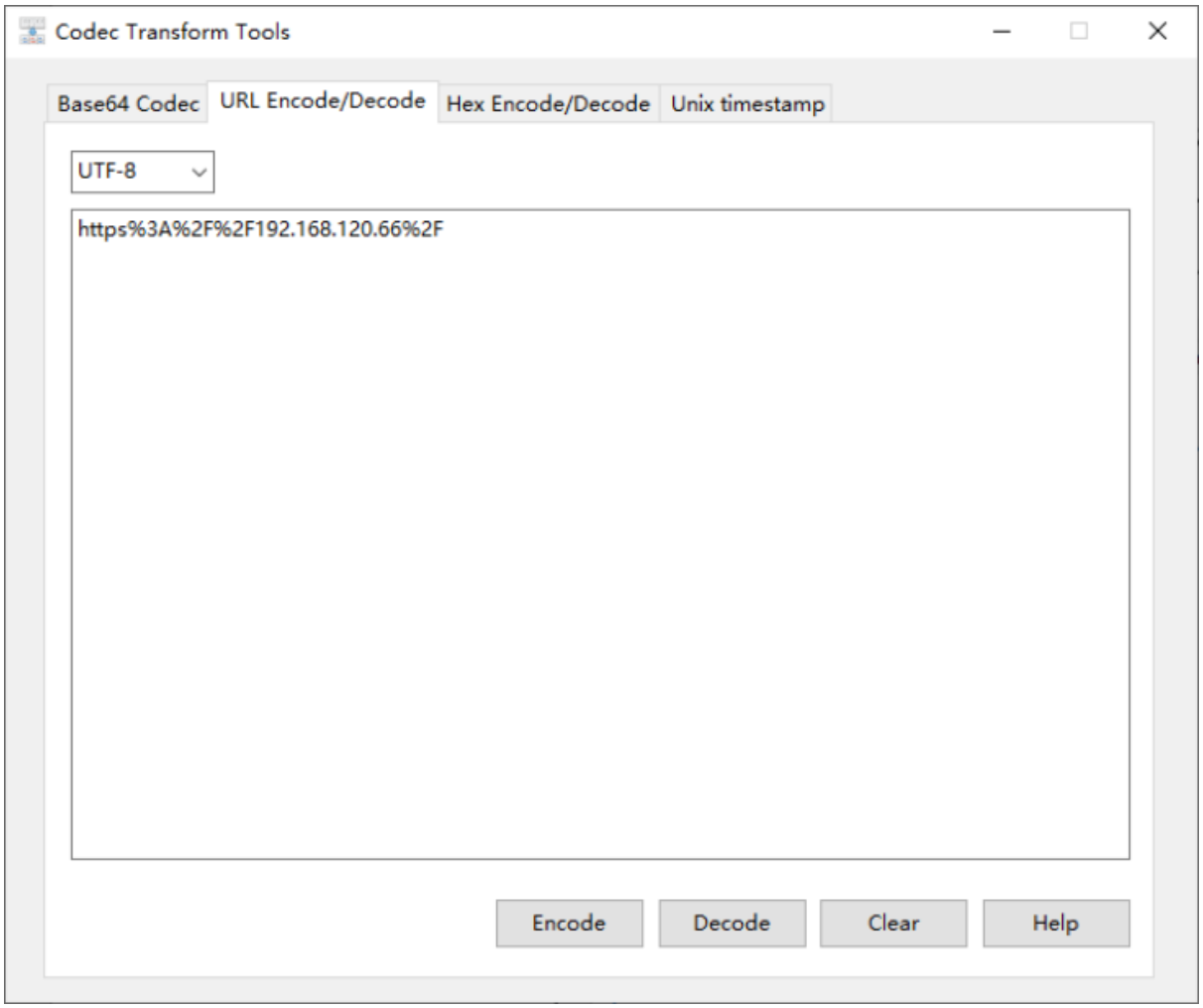
1. Select the encode/decode format. There are UTF-8 and GB2313 two formats.
2. Put the message in the Input panel, click Encode button, and the system will display the encoding result, as the screen shot shows below:

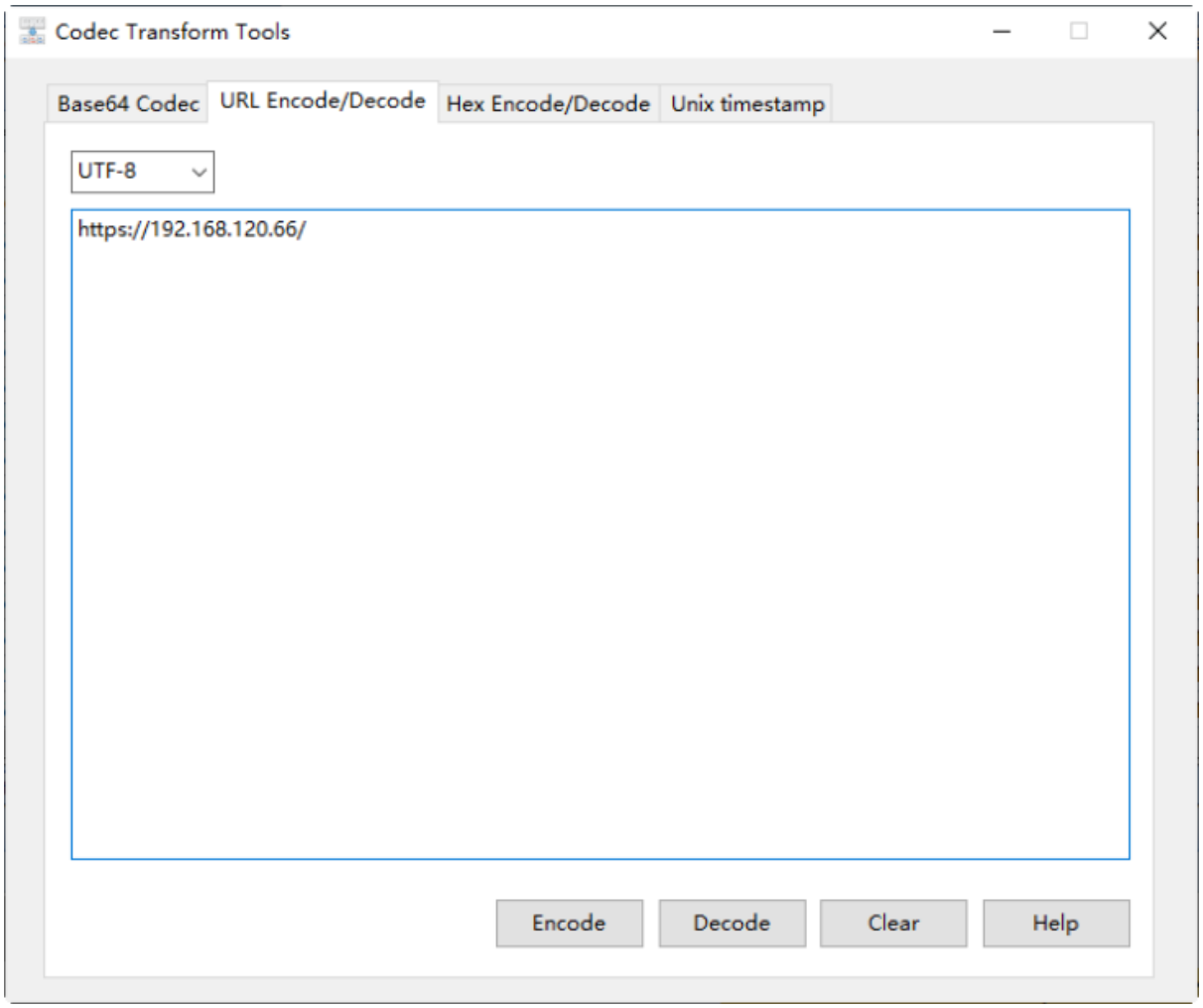




URL Decode

1. Select the encode/decode format. There are UTF-8 and GB2313 two formats.
2. Put the message in the Input panel, click Decode button, and the system will display the decoding result, as the screen shot shows below:

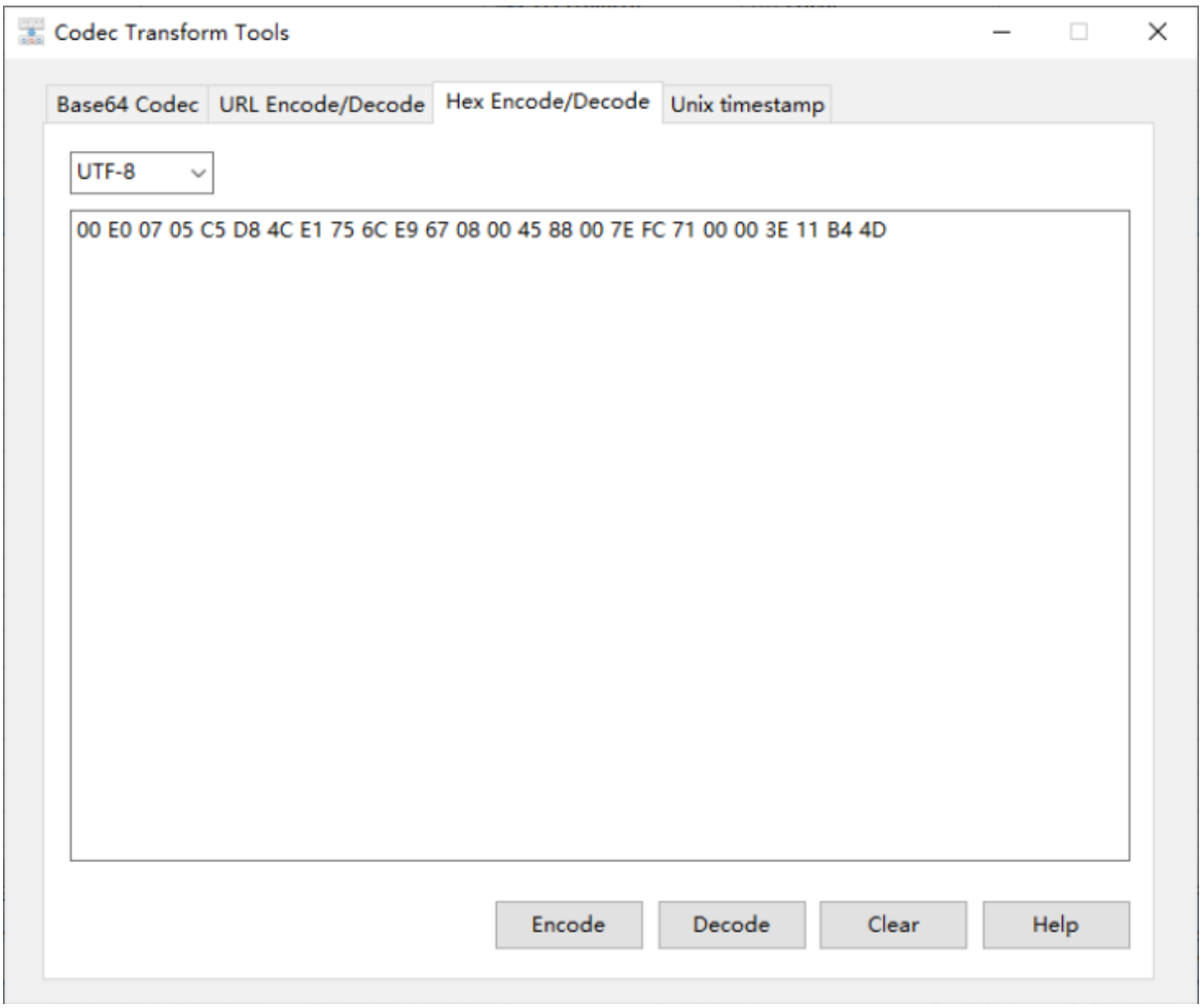


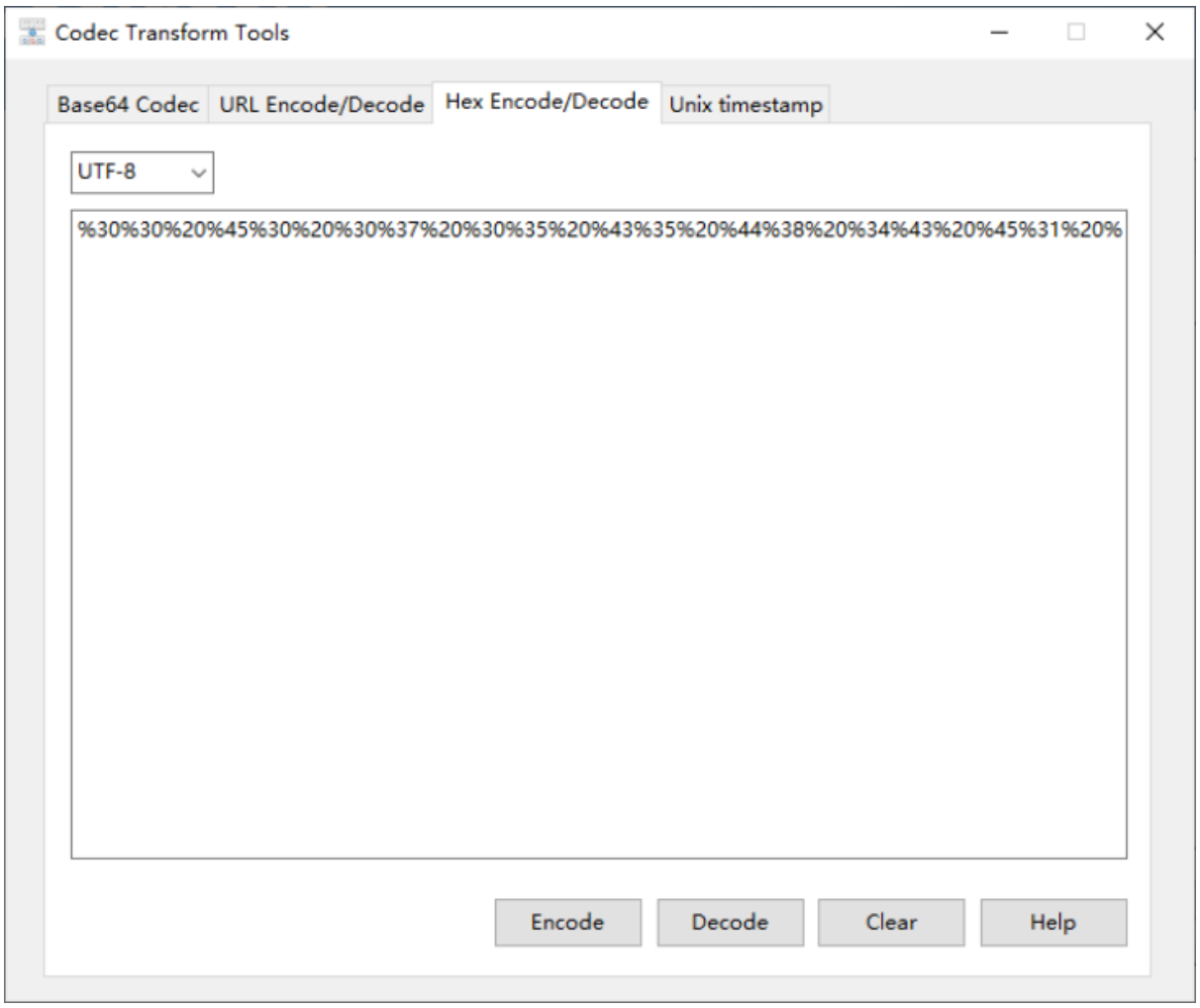


Hex Encode/Decode

Hex Encode

1. Select the encode/decode format. There are UTF-8 and GB2313 two formats.
2. Put the message in the Input panel, click Encode button, and the system will display the encoding result, as the screen shot shows below:

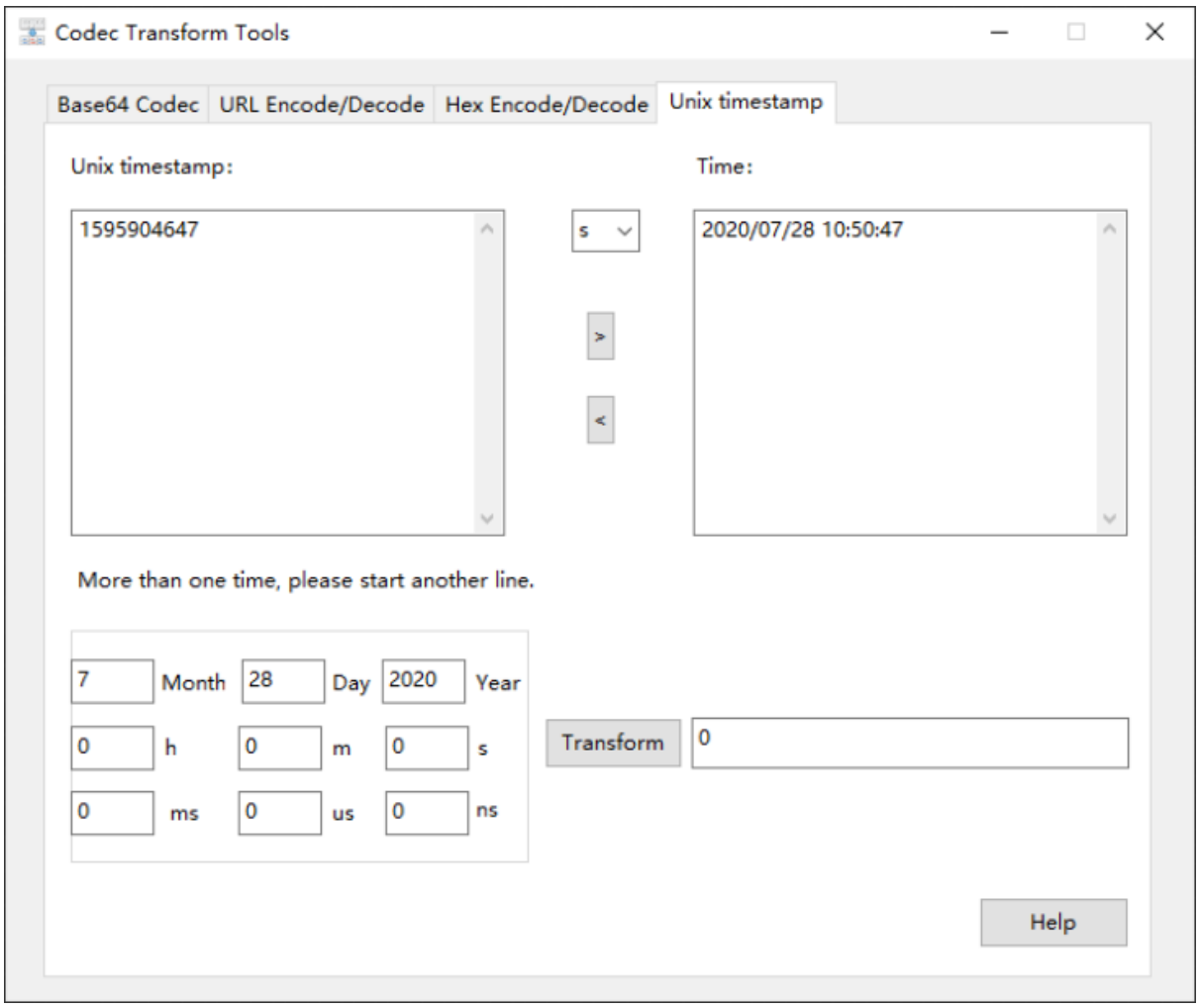




Unix Timestamp

Transform Timestamp to Data

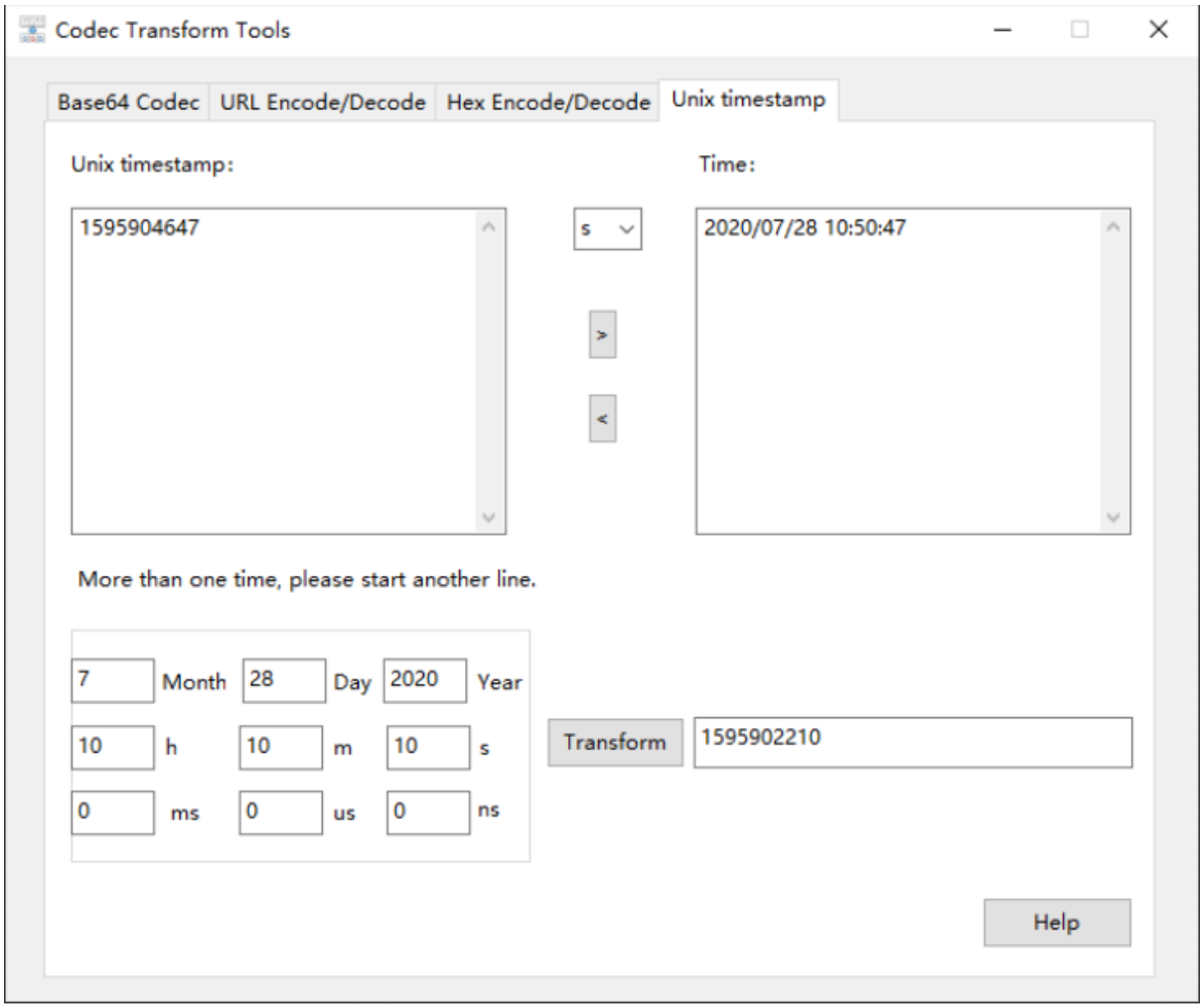
1. Select the unit of time. There are s, ms, us and ns four units.
2. Put the timestamp in the Input panel, click the button, and the system will display the transformation result, as the screen shot shows below:



Transform Date to Timestamp

There are two methods to transform date to timestamp. Besides the reverse method of transformation mentioned above, another method is as below:

Put the data in the Input panels, click the button, and the system will display the transformation result, as the screen shot shows below:



Colasoft Ping Tool

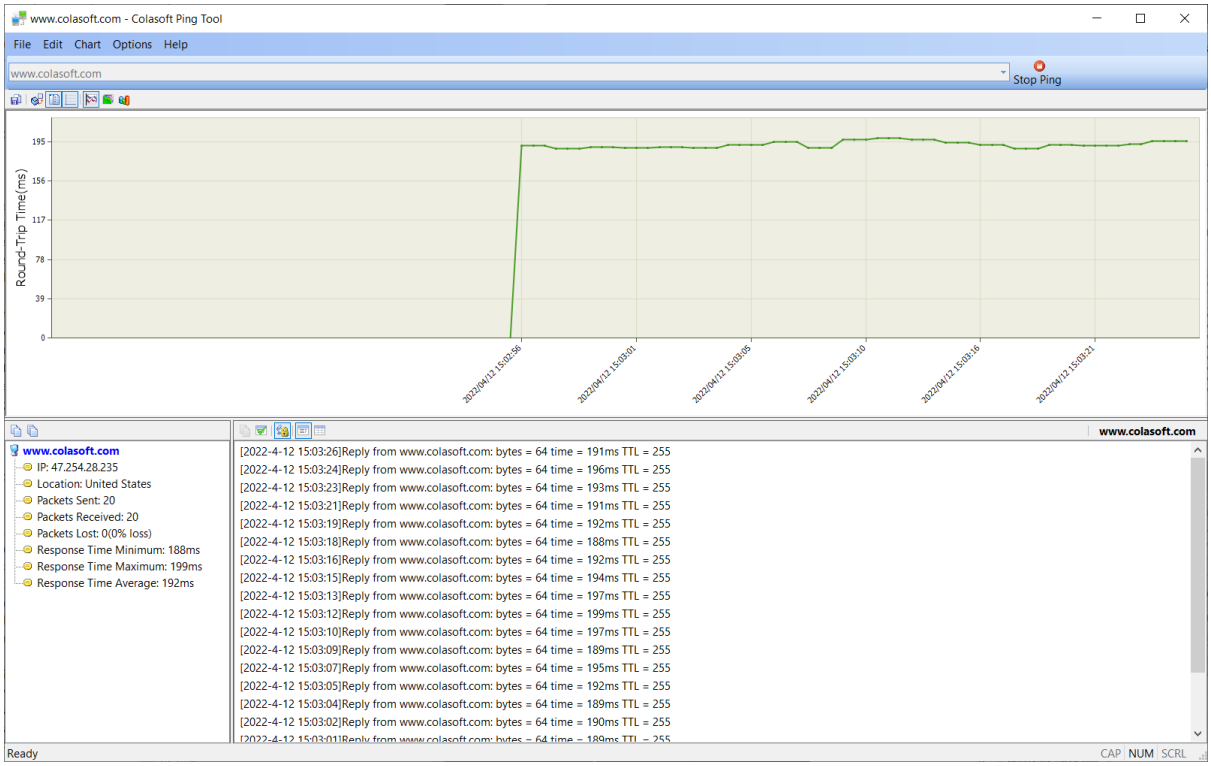
Colasoft Ping Tool is a powerful graphic ping tool, supports to ping multiple IP addresses at the same time, and compares response time in a graphic chart.

To start Colasoft Ping Tool, do one of the followings:

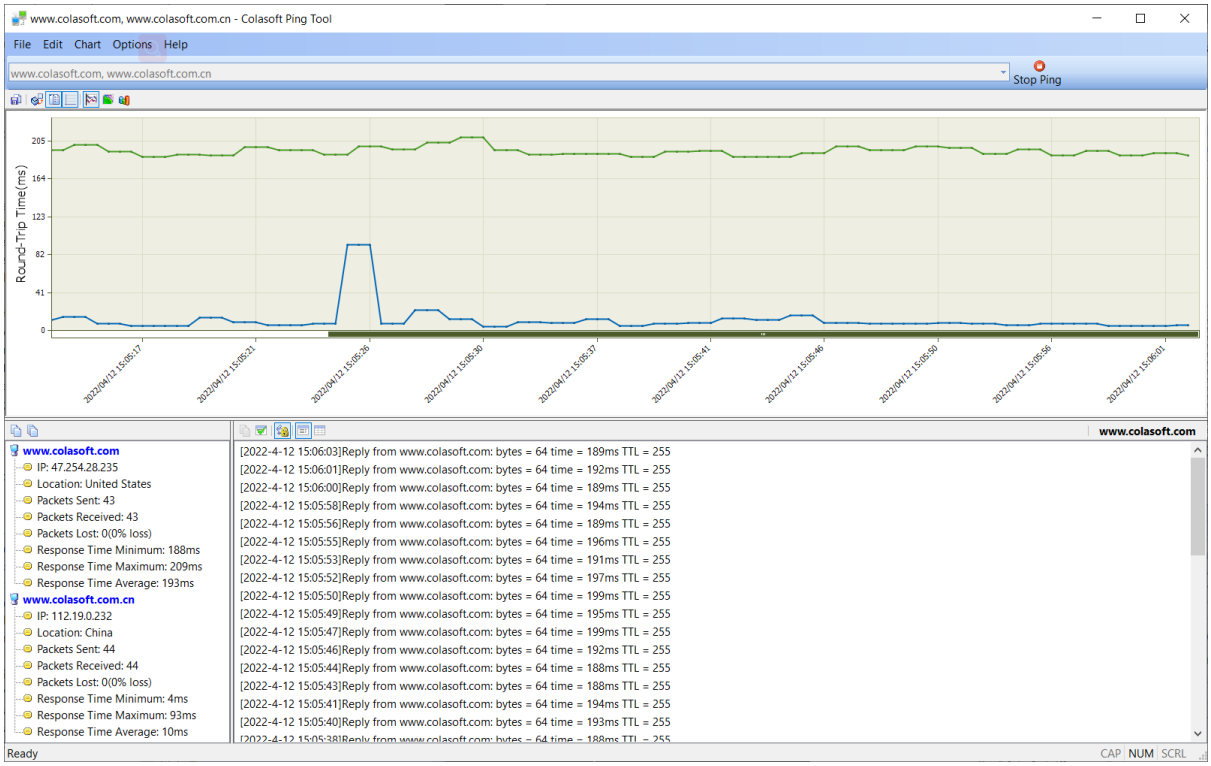
- Click **Ping** in the **Tools** tab of the ribbon.
- Choose **Start** > **All Programs** > **Colasoft Capsa** > **Ping Tool.**
- Choose **Start** > **Run**, enter "*cping*" and click **OK**.

Colasoft Capsa is very intelligent to let you ping either one single IP address (domain name) or multiple IP addresses (domain names). Enter IP addresses or domain names (multiple items are separated by comma), click **Start Ping** to start.

Ping a single domain name:



Ping multiple domain names:



By default, Colasoft Ping Tool will keep pinging the target hosts until you click **Stop Ping** to make it stop.

You can view historical charts and save the charts to a **.bmp* format file. With this tool, users can ping the IP addresses of captured packets in Colasoft Capsa conveniently, including resource IP, destination IP or both of them.

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

Colasoft MAC Scanner

Colasoft MAC Scanner is a tool used for scanning IP addresses and MAC addresses in a local network. It sends ARP queries to specified subnet, and listens to the ARP responses to get IP addresses and MAC addresses, with very fast scanning. You can also change the number of scanning thread to get better efficiency.

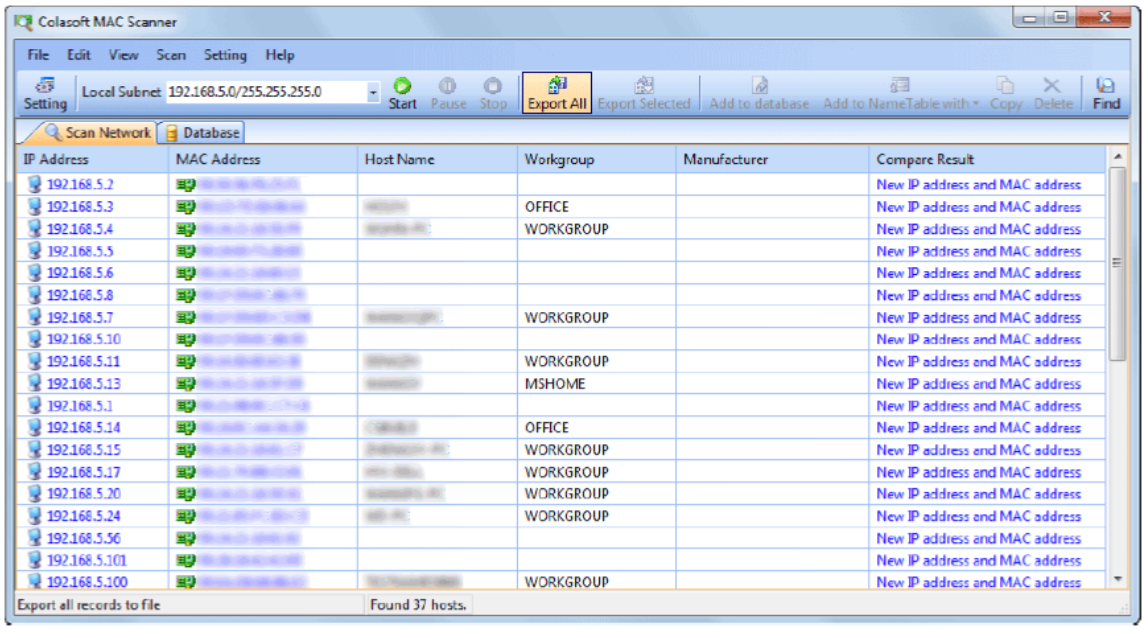
There are two useful new features added.

- **Database**: Lets you save your scan result here for later IP address and MAC address comparison.
- **Add to Name Table with**: Allows you add IP address, MAC address or both to **Name Table** directly.

To start Colasoft MAC Scanner, do one of the followings:

- Choose the **Tools** tab of the ribbon, click **MAC Scanner**.
- Choose **Start** > **All Programs** > **Colasoft Capsa** > **MAC Scanner**.
- Choose **Start** > **Run**, enter "*cmac*" and click **OK**.

The Colasoft MAC Scanner appears as below:



Colasoft MAC Scanner contains the following components:

Menu

Contains all items on the toolbar, the commands to control the window and **Help**.

Toolbar

Contains shortcuts of the most commonly used commands and allows you to customize.

Scan Network View

Scan Network View will display the scanned results, including IP address, MAC address, Host Name and Manufacture in the list. It will group all IP addresses according to MAC address if a MAC address configured multiple IP addresses. The scanned results can be exported as *.txt* file for future reference.

Database View

Database View saves your scan result to database, which is used by **Scan Network View** to inform you the discrepancies, if any, when you execute another scan later on.

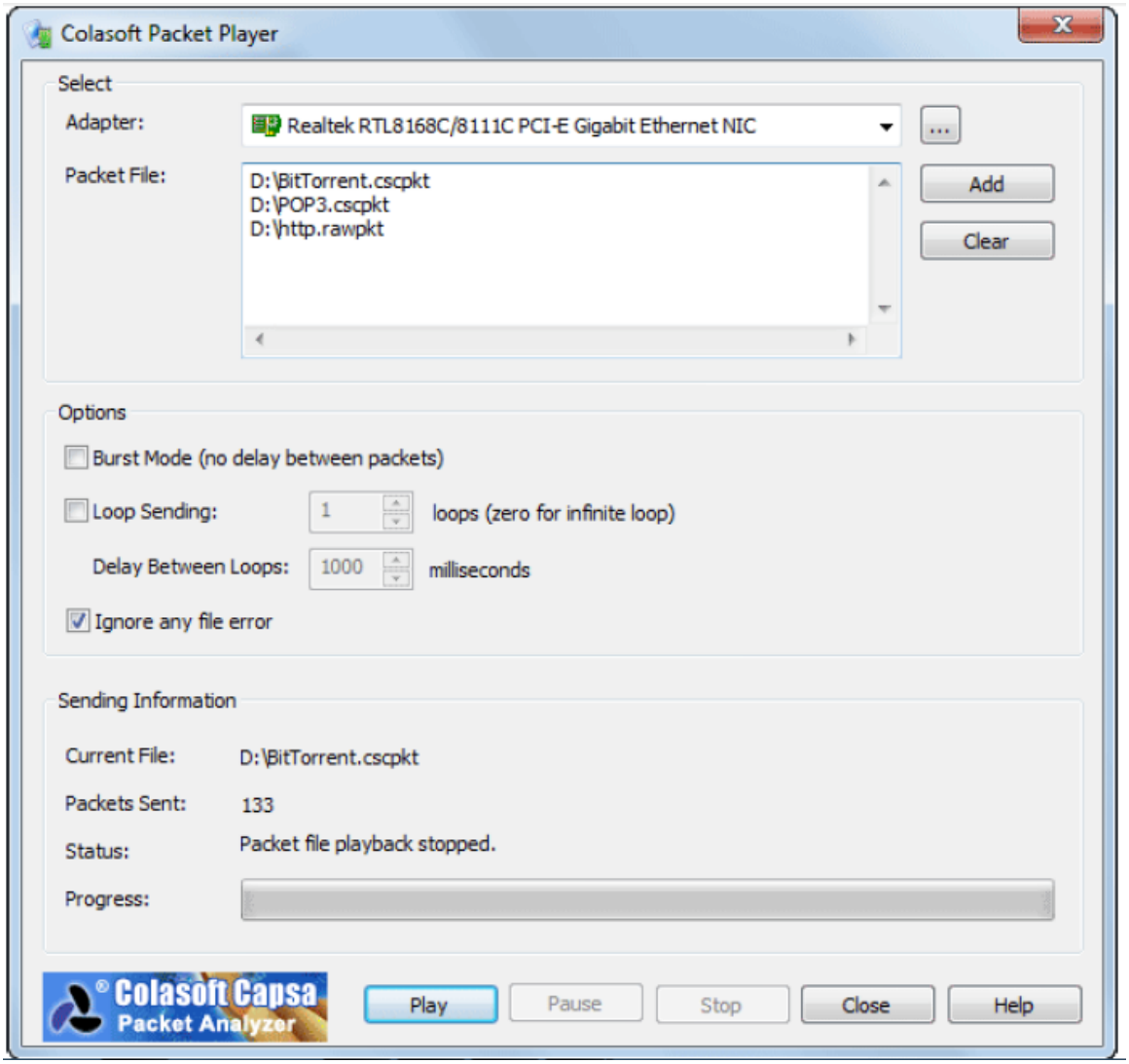
Colasoft Packet Player

Colasoft Packet Player is a replay tool which allows you to open captured packet files and playback to the network. Colasoft Packet Player supports many packet file formats created by many sniffer software products, such as Colasoft Capsa, Wireshark, Network General Sniffer and WildPackets EtherPeek/OmniPeek etc. It also can support burst mode and loop sending feature.

To start Colasoft Packet Player, do one of the followings:

- Click **Packet Player** in the **Tools** tab of the ribbon.
- Choose **Start** > **All Programs** > **Colasoft Capsa** > **Packet Player**.
- Choose **Start** > **Run**, enter "*pktplayer*" and click **OK**.

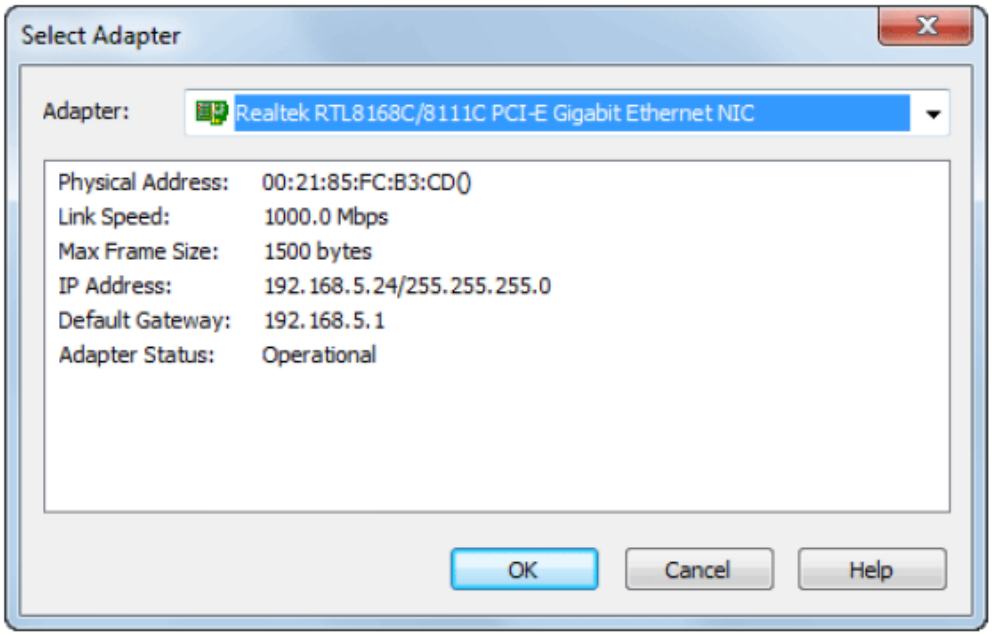
The Colasoft Packet Player appears as below:



You can find the following items in Colasoft Packet Player.

Adapter

You need to select one adapter for sending packets for no adapter selected by default. Click **Select** to open the **Select Adapter** dialog box, choose an adapter from the combo box. The window under the combo box will display the detailed information of the selected adapter.



Packet File

Defines the packet file you want to send. The file formats that Colasoft Packet Player support are listed below. You can add multiple files by clicking the **Add** button. Users also can replay a packet file have been sent out before from the combo box.

- Colasoft Capsa 5.0 Packet File (*.cscpkt)
- Colasoft Capsa 5.0 Raw Packet File (*.rawpkt)
- Colasoft Capsa 7.0 Packet File (*.cscpkt)
- Accellnt 5Views Packet File (*.5vw)
- EthePeek Packet File(V7) (*.pkt)
- EthePeek Packet File(V9) (*.pkt)
- HP Uinx Nettl Packet File (*.TRCO;TRC1)
- libpcap(tcpdump,Ethereal,etc.) (*.cap)
- Microsoft Network Mintor2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instuments Observer V9.0 (*.bfr)
- NetXRay2.0 and WINDWS Sniffer (*.cap)
- Sun_Snoop (*.snoop)
- Visual Network Traffic Capture (*.cap)

Advice You may use the **Clear** button to clear all the items in packet file list. To delete some items in the list, choose them and press **Delete** Key to delete them.

Bust Mode

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

Loop Sending

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

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

Ignore any file error

The Packet player will skip the file error in any packet file and keep playing.

Current File

Displays the path of the file.

Packets Sent

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

Status

Displays tips or the status of your actions.

Progress

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

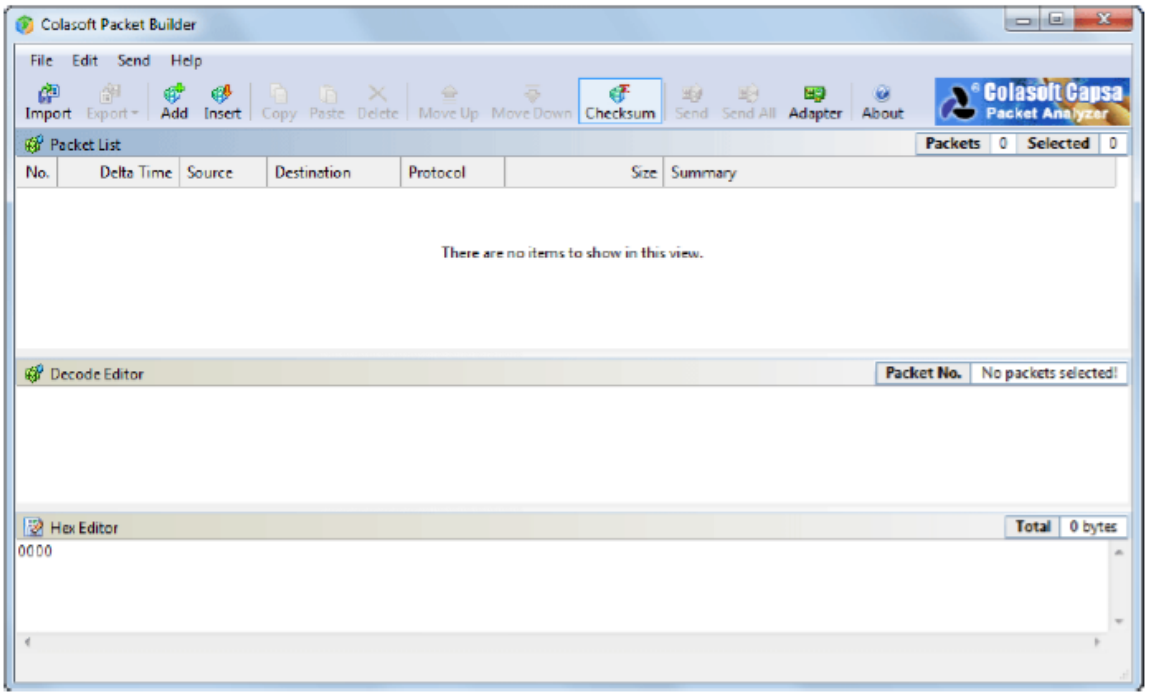
Colasoft Packet Builder

Colasoft Packet Builder is useful tool used for creating custom network packets, and you can use this tool to check your network protection against attacks and intruders. Colasoft Packet Builder provides you very powerful editing feature, besides common hex editing raw data, it featuring a Decoding Editor which allows you edit specific protocol field value much easier. In addition to building packets, Colasoft Packet Builder also supports saving packets to packet files and sending packets to network.

To start Colasoft Packet Builder, do one of the followings:

- Click **Packet Builder** in the **Tools** tab of the ribbon.
- Choose **Start** > **All Programs** > **Colasoft Capsa** > **Packet Builder**.
- Choose **Start** > **Run**, enter "*pktbuilder*" and click **OK**.

The Colasoft Packet Builder window appears as below:



Colasoft Packet Builder contains three panes in main view.

- Packet List
- Decode Editor
- Hex Editor

The last two panes collaborate with the Packet List pane. Once a packet selected, Decode Editor and Hex Editor decode the packet and you can just edit the packet in these two panes.

To customize the layout of the three panes, just drag their heads to move.

You can use Colasoft Packet Builder to:

Add or insert new packets

Simply you can add or insert packets from **Packet** tab of Colasoft Capsa or packet template (ARP, IP, TCP and UDP).

Edit packets

Just click the item or digit to edit packets in Decode Editor pane and Hex Editor pane.

Send packets

Click the Send or Send All button on toolbar to transmit the created packets to network.

Tips Save your packets to disk is also important. You can click Export to save selected packets or all packets to your machine. Now only **.cscpkt* format files is supported.

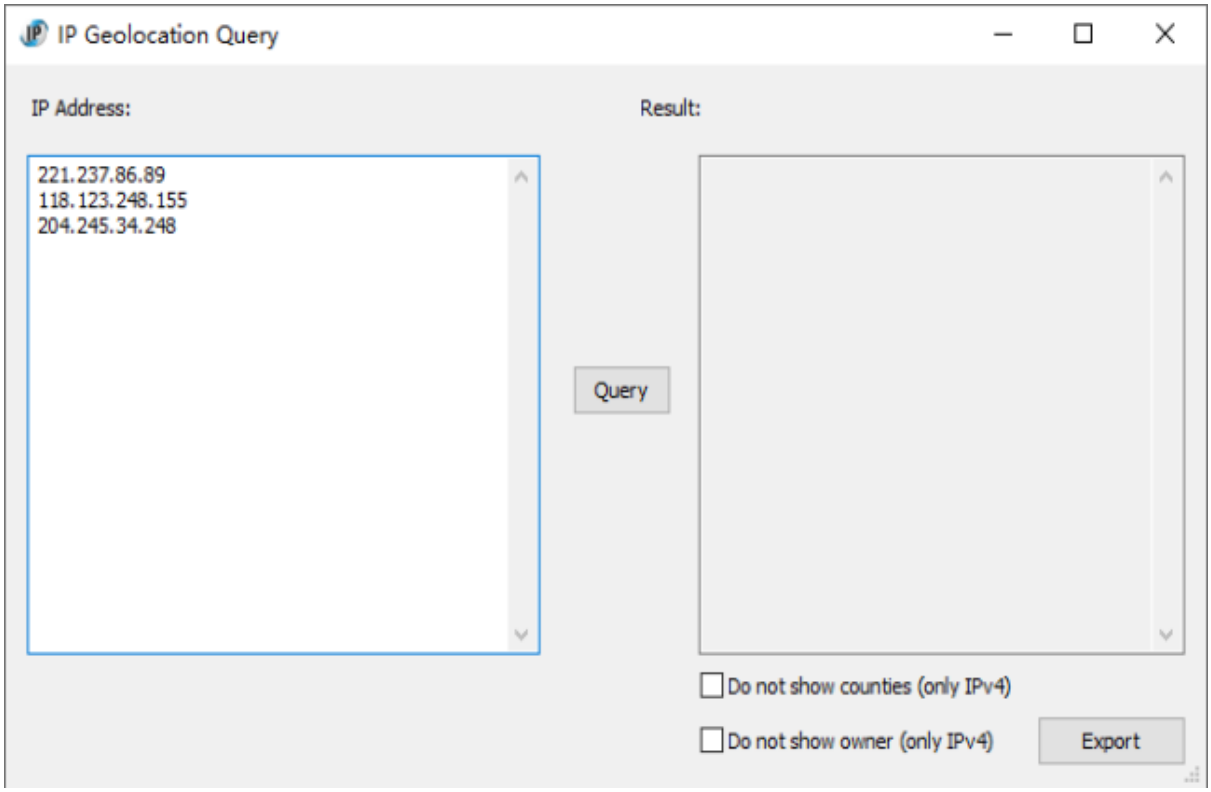
IP Geolocation Query

IP Geolocation Query is a geolocation query tool, can query the regions and countries to which the specific IP addresses belong. It supports to query multiple IP addresses at the same time.

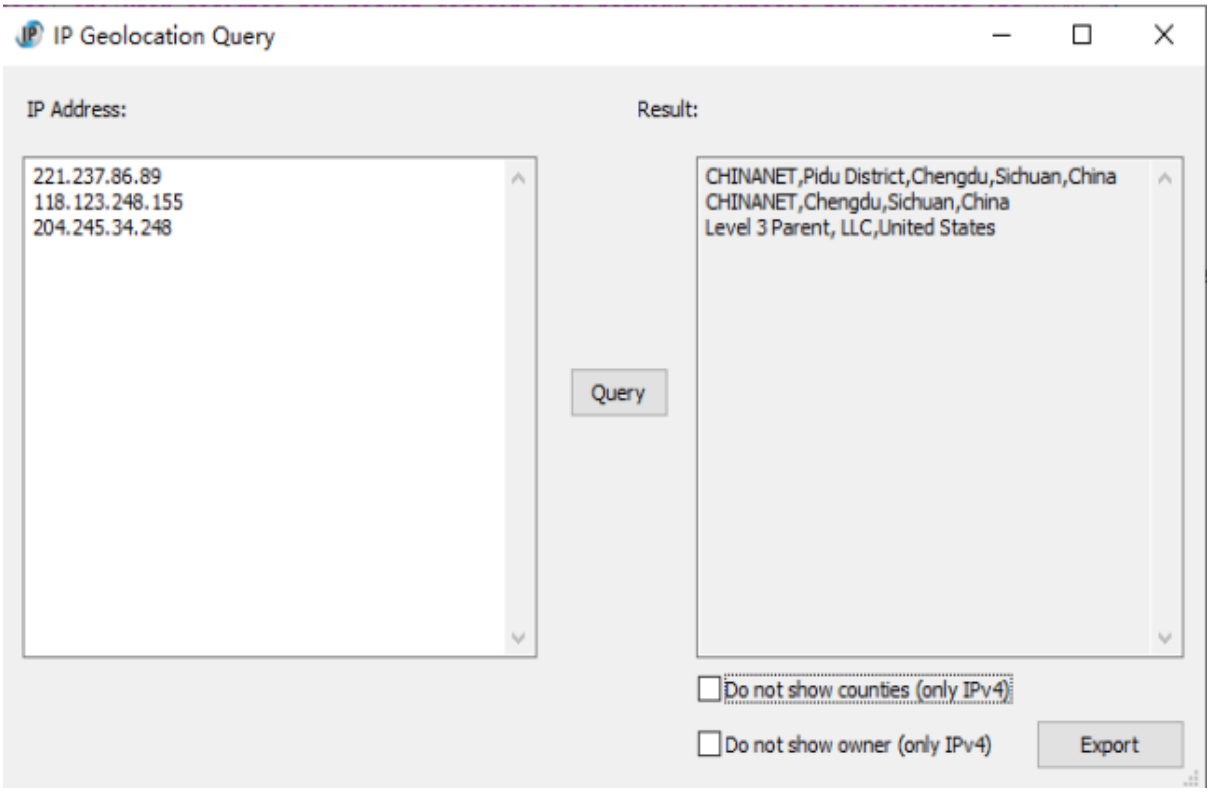
To start IP Geolocation Query, do one of the following:

- Click IP Geolocation Query in Tools tab of the Ribbon.
- Choose Start > All Programs > Colasoft Capsa > Network Toolset > IP Geolocation Query
- Choose Start > Run, enter "IpGeolocation" and click OK.

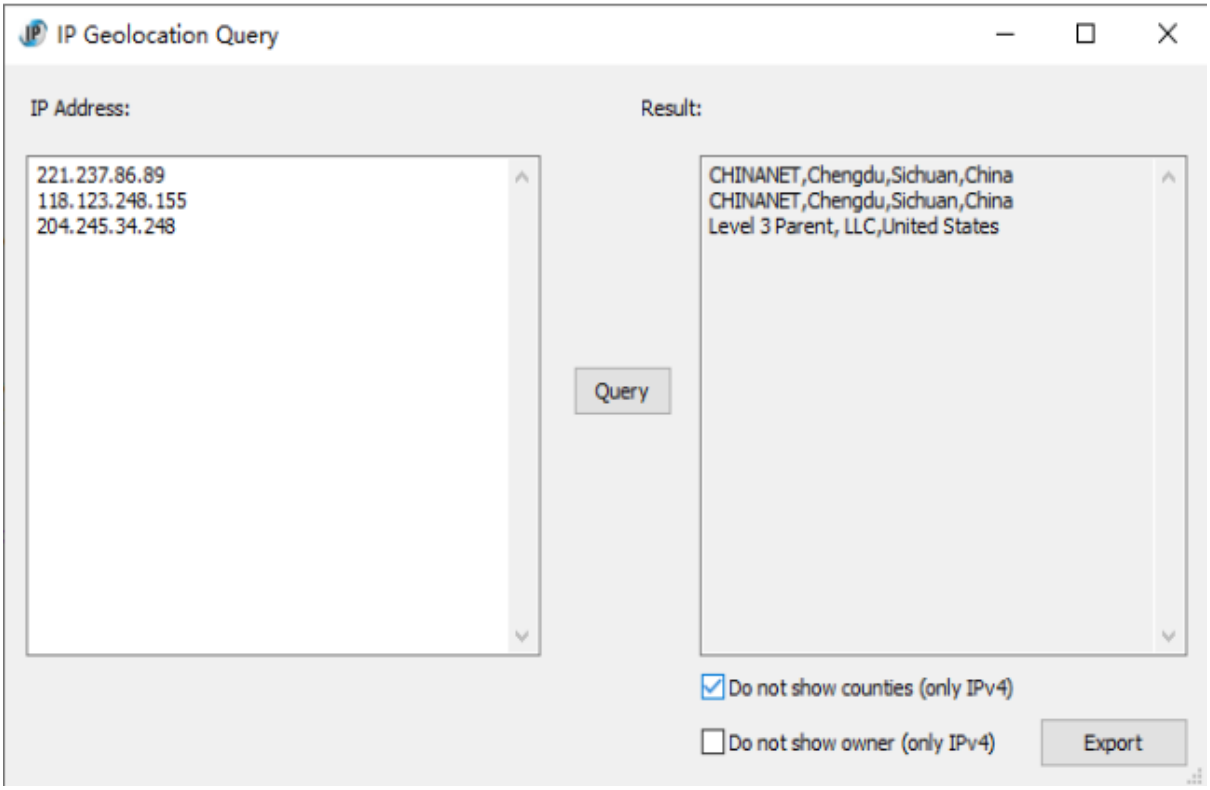
The **IP Geolocation Query** window appears as below:



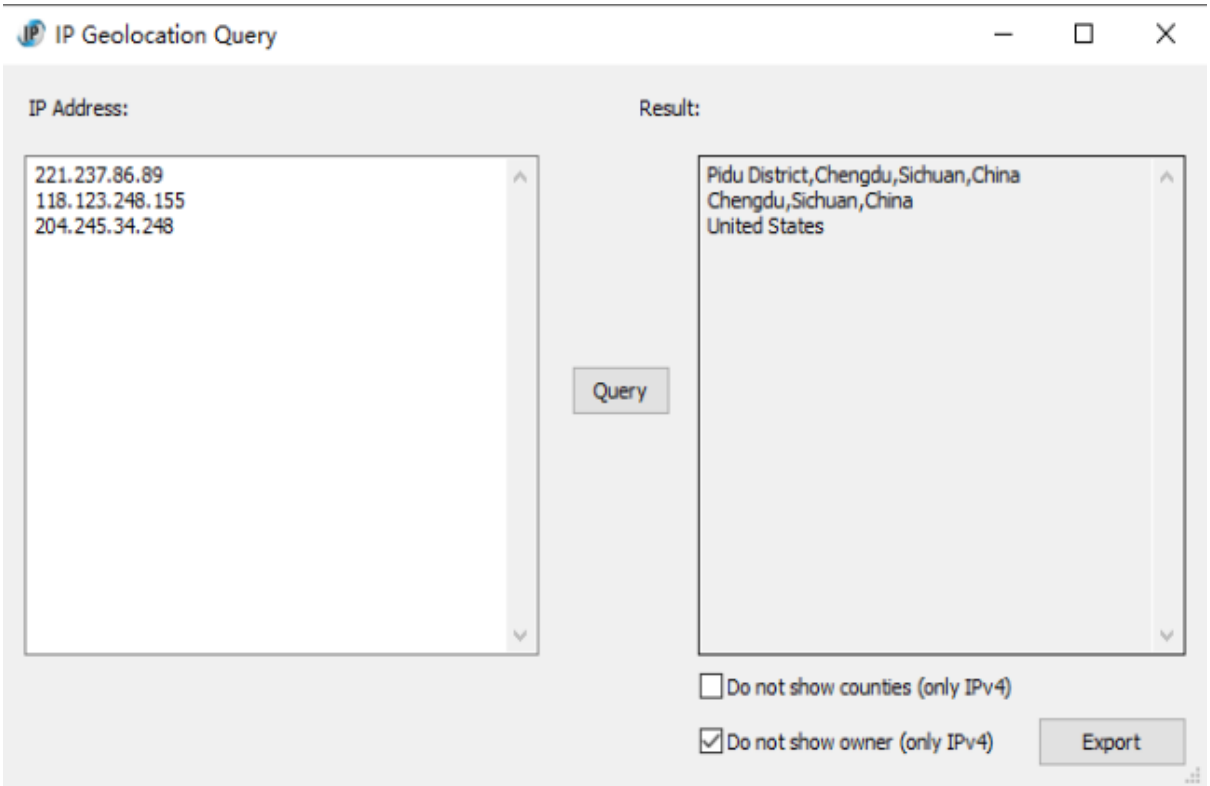
Enter IP addresses (multiple items are separated by Enter), click **Query** to query the geolocations, as the screenshot below:



Check **Do not show counties** to not display the location of the districts and counties of the address, as the screenshot below:

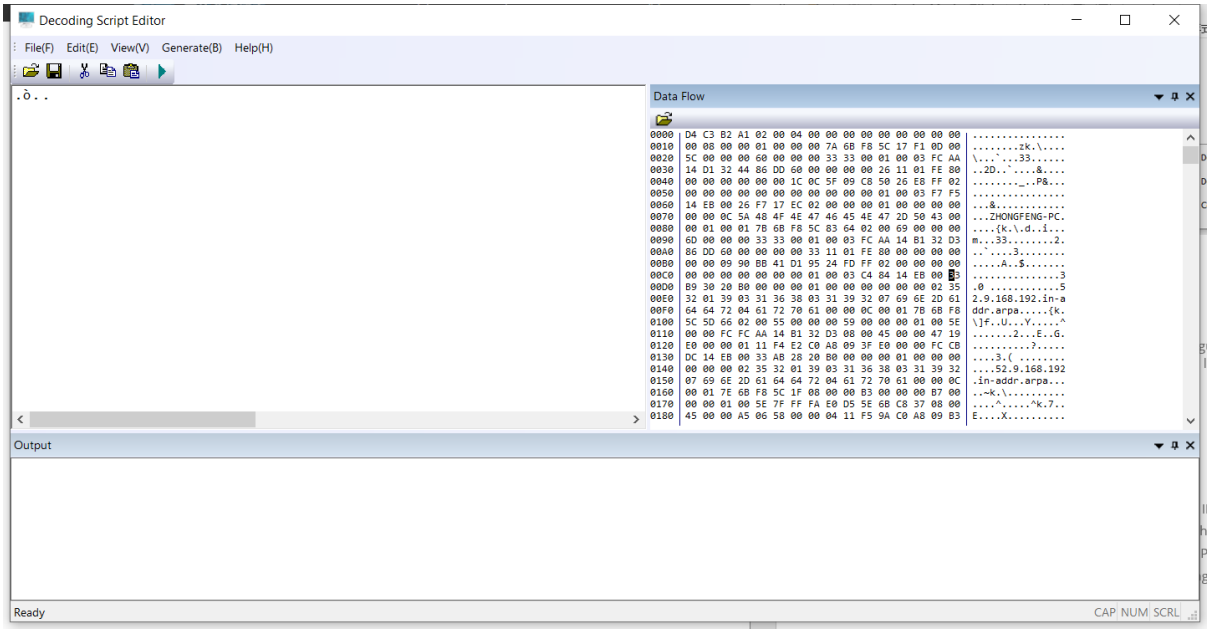


Check **Do not show owner** to not display the owner of the address, as the screenshot below:



Decoding Script Editor

(Fast Protocol Decode Language) FPDL is an interpretation language designed and used in the Colasoft fast protocol decoding engine FPDE, is an interpretation language specially designed for network protocol decoding.



Advantages of FPDL

Compared with general-purpose programming languages (such as C, C++, java, python), FPDL has the following advantages:

1) Designed for decoding, the syntax design is close to the decoding requirements, the number is small, the difficulty is low, and it is easy to learn;

2) The simple grammar is easy to use, and the extended grammar is gradually mastered, and the decoding script is produced quickly;

3) Decoding on demand, the granularity of the decoding field can be controlled at will;

4) The decoding script can be written and used immediately, and immediately verify whether the decoding result meets the requirements;

5) Compared with decoders implemented in C and C++, in most cases, the decoding performance of FPDL is higher and more stable.

Compared with other interpreted (scripting) languages or instruction sequences designed for decoding, FPDL has the following advantages:

1) Using a simpler syntax, supports decoding almost all network protocols;

2) The decoding performance is higher and more stable.

FPDL data types

PFDL supports two most basic data types: integer and string.

The integer bit width is automatically derived.

Appendices

FAQ

Q: What can I do with Capsa?

A: Capsa comprises many features.

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 M NIC, you can't see the traffic generated by 100 M 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 rules using **Simple Filter** 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 by using **Advanced Filter**.

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

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

Q: Does Capsa support analyzing VoIP traffic?

A: Yes, Capsa is capable of analyzing VoIP traffic, and the traffic of SIP and H.323 protocol can be analyzed.

Q: What can I do if Capsa crashes?

A: Please check if there is a crash report file under C:\Users\[username]\AppData\Roaming\Colasoft Capsa - Enterprise Edition\CrashReport. You should get it before re-opening Capsa after the crash happens, or the crash report file will disappear. If there is the crash report file, please send it to support team for further research.

Q: Why do I only capture traffic to and from my machine?

A: Generally, if your adapter supports promiscuous mode it can work well with Capsa. A possible reason is that you didn't connect your machine to the right network device, or misconfigured you switch to see all the traffic on your network.

Q: Can I monitor traffic of my remote business network?

A: In order to monitor the traffic for your remote business network, you should install Capsa on a workstation in your business network, and enable the Remote Desktop Access function of that workstation (Windows2000 Terminal Server, TeamViewer, Norton PcAnywhere, VNC Server, etc.), then you can access to Capsa via the local Remote Desktop client program.

We keep updating more FAQs on our official website. Please visit our website at www.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 has been fulfilled.
201	Created--The request has been fulfilled and resulted in the creation of a new resource.
202	Accepted--The request has been accepted for processing, but the processing has not been completed.
203	Non-Authoritative Information--The returned information is only partial.
204	No Content--The server has fulfilled the request, but there is no new information 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 server has fulfilled partial GET request for the resource.
300	Multiple Choices--The request resource has multiple possibilities, each with different locations.
301	Moved Permanently--The resource requested has a new location and the change is permanent.
302	Found--The resource requested has a different URI temporarily.
303	See Other--The response to the request is at a different URI and the resource should be accessed with 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--Not be used in the latest HTTP version.
307	Redirect Keep Verb--The redirected request keeps the same HTTP verb. HTTP/1.1 behavior.
400	Bad request--The request could not be fulfilled by the server because of invalid syntax.
401	Unauthorized--The client is not authorized to access resource or is refused to access resource even with authorization.
402	Payment required--This status code is reserved for future use.
403	Forbidden--The server understood the request, but refused to fulfill it.
404	Not found--The server didn't 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 failed to send a request in the time allowed by the server.
409	Conflict-- The request was unsuccessful due to a conflict with the status of the resource.
410	Gone-- The resource requested is no longer available at the server, and no forwarding address is available.
411	Length Required-- The server refused to 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 can process.
414	Request URI Too Long-- The server can not fulfill the request because the request URI is longer than the server can interpret.
415	Unsupported Media Type-- The server refused a request because the message body is in an inappropriate format.
416	Requested Range Not Satisfiable-- The server could not fulfill the client's request because the requested range is not satisfiable.
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 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 functionality 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 for the server being down or overloaded.
504	Gateway timeout-- The request was timed out waiting for a gateway.
505	HTTP Version Not Supported-- The server does not support or refuses to support the HTTP protocol version specified in the request header.