



Colasoft Capsa Getting Started

Colasoft Co., Ltd

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

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

www.colasoft.com

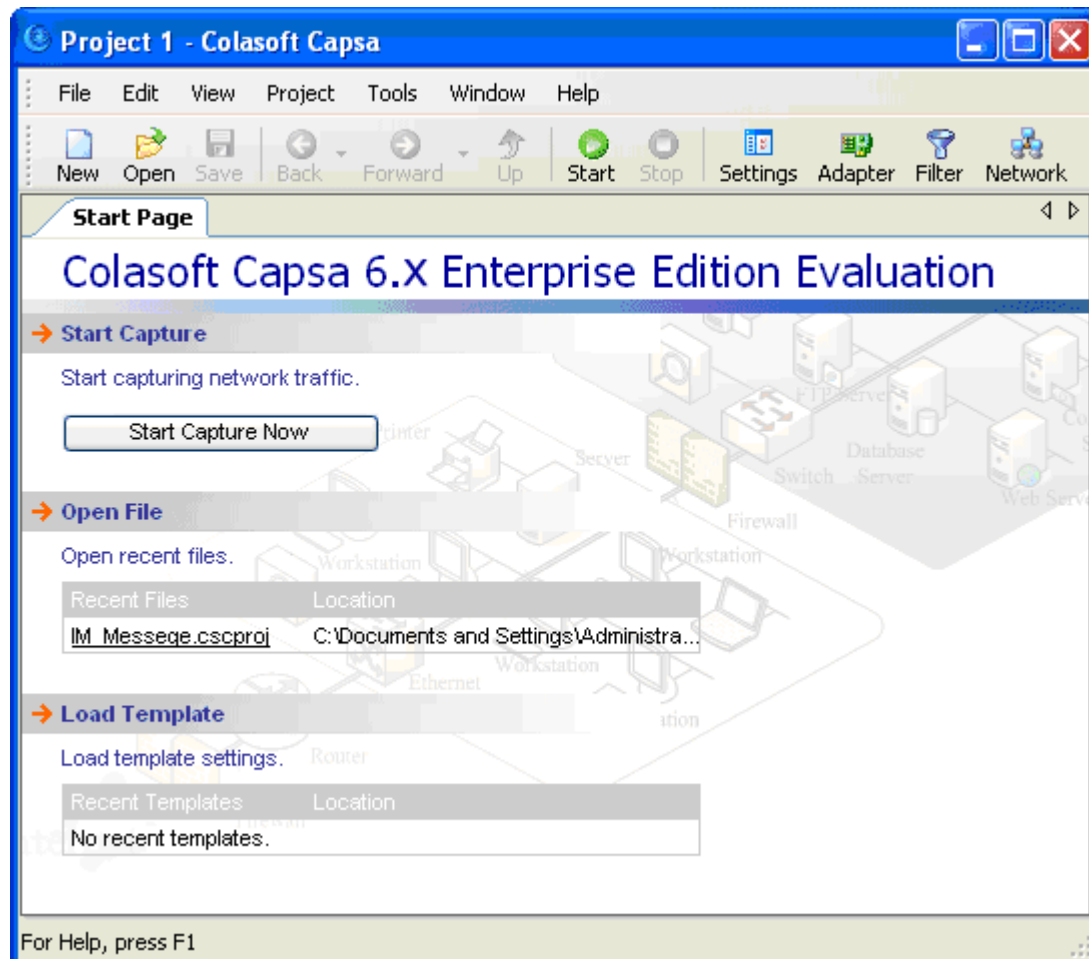
Content

Create a new project	2
Start Capture	2
Views Layout	5
Tool bar	6
Project Explorer	7
Project Status	8
Tab views	9
Summary view	9
Diagnoses view	10
Endpoints view	15
Protocols view	17
Conversations view	18
Matrix view	19
Packets view	20
Logs view	30
Graphs view	33
Reports view	36
Modify Project Settings	37
General	37
Adapter	39
Filter	40
Network	41
Log	42
DNS Log	42
Email Log	43
FTP Log	44
HTTP Log	45
Diagnoses	48
Data management	49
Saving	49
Saving a project	49
Saving project data	50
Saving as template	50
Importing & exporting packet file	50
Import a packet file	50
Export to a file	51
Printing	53

The following tutorial assumes that you have already installed Colasoft Capsa 6.7 Enterprise Edition on your machine.

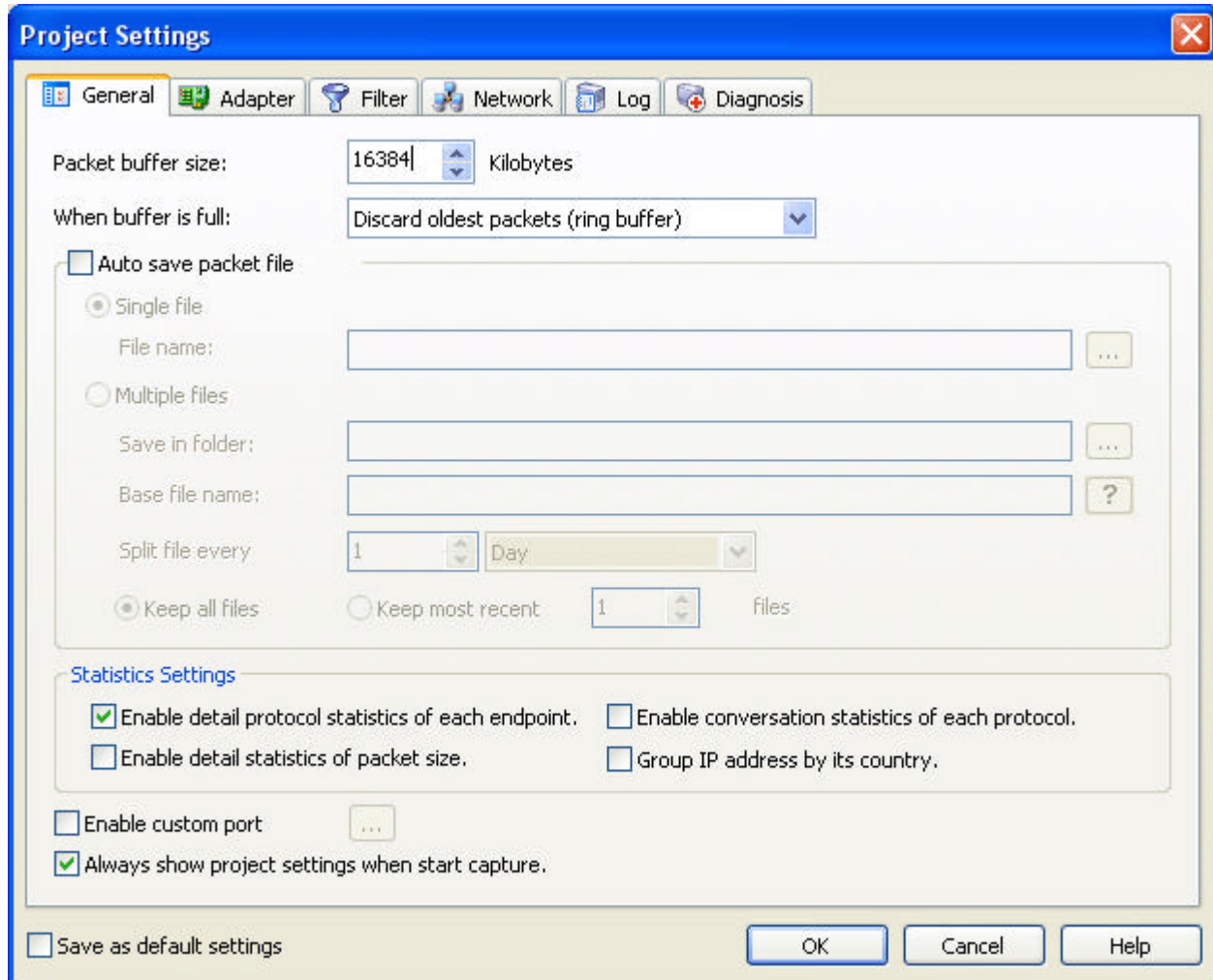
Create a new project

Run Colasoft Capsa. The **Start Page** is the first screen you will see.



Start Capture

To immediately start capturing packets, just click the **Start Capture Now** button, Colasoft Capsa will use the default project settings.

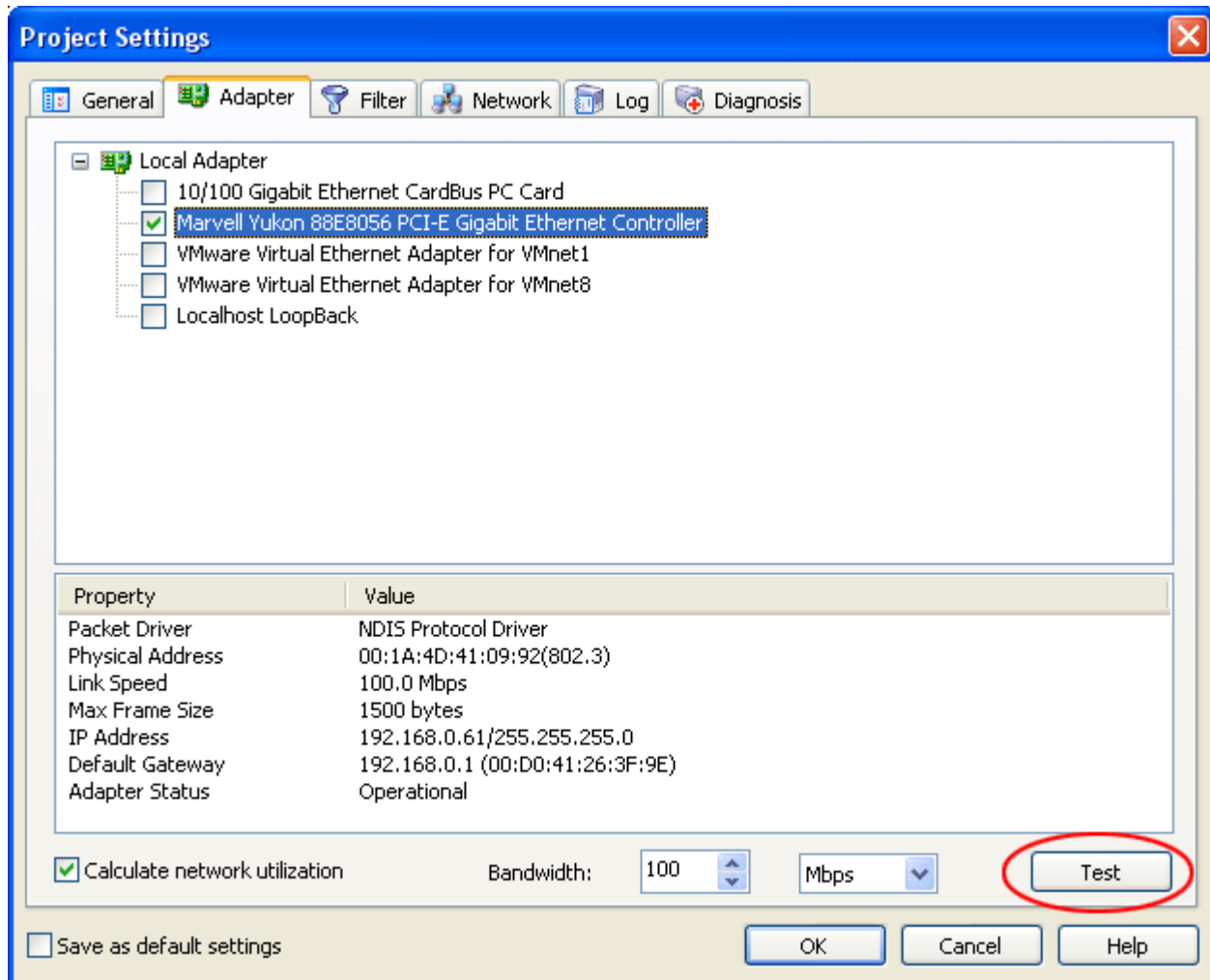


The **Project Settings** dialog box is shown with the **General** tab selected. It contains the following settings:

- Packet buffer size:** 16384 Kilobytes
- When buffer is full:** Discard oldest packets (ring buffer)
- Auto save packet file:** ☐ (disabled)
- Single file:** ☒
 - File name:** [empty text box]
- Multiple files:** ☐
 - Save in folder:** [empty text box]
 - Base file name:** [empty text box]
 - Split file every:** 1 Day
- Keep all files:** ☒ **Keep most recent:** ☐ 1 files
- Statistics Settings:**
 - ☒ Enable detail protocol statistics of each endpoint.
 - ☐ Enable conversation statistics of each protocol.
 - ☐ Enable detail statistics of packet size.
 - ☐ Group IP address by its country.
- Enable custom port:** ☐ [empty text box]
- ☒ Always show project settings when start capture.
- Save as default settings:** ☐

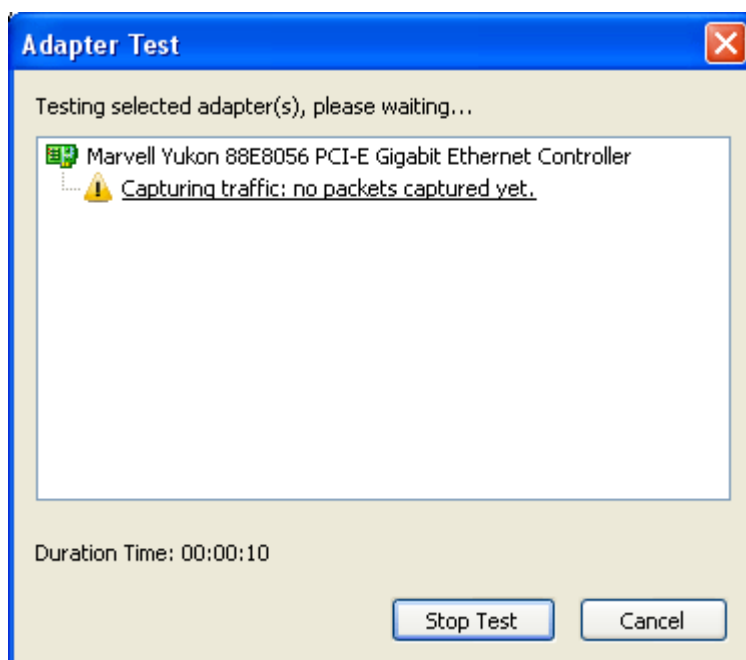
Buttons: OK, Cancel, Help

All available adapters are listed in this page, you may select two or more adapters from the list. The lower pane offers the property information of the highlighted adapter.

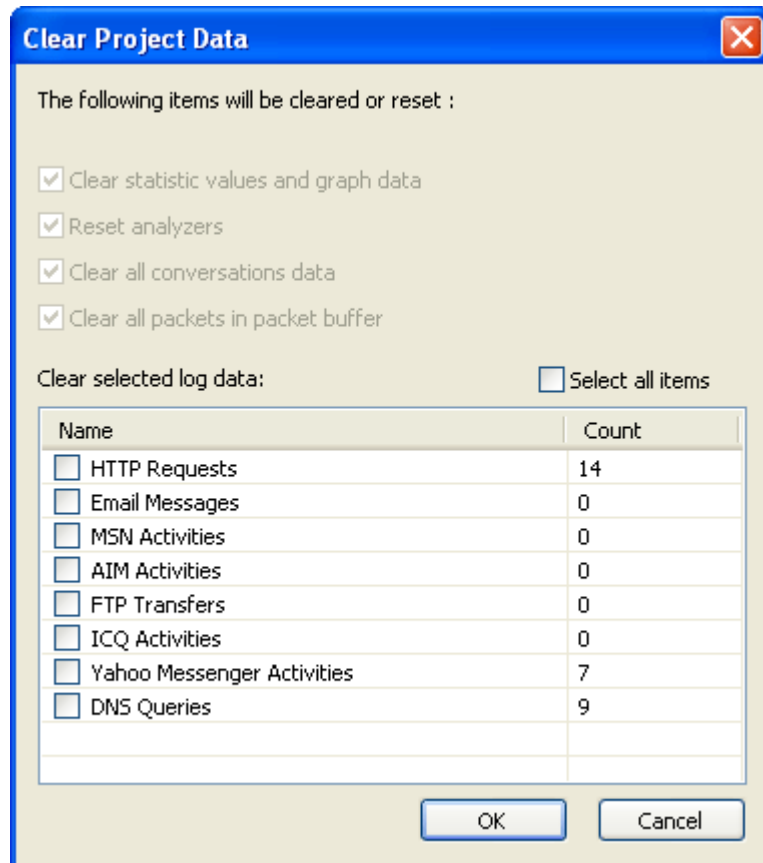


Test

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



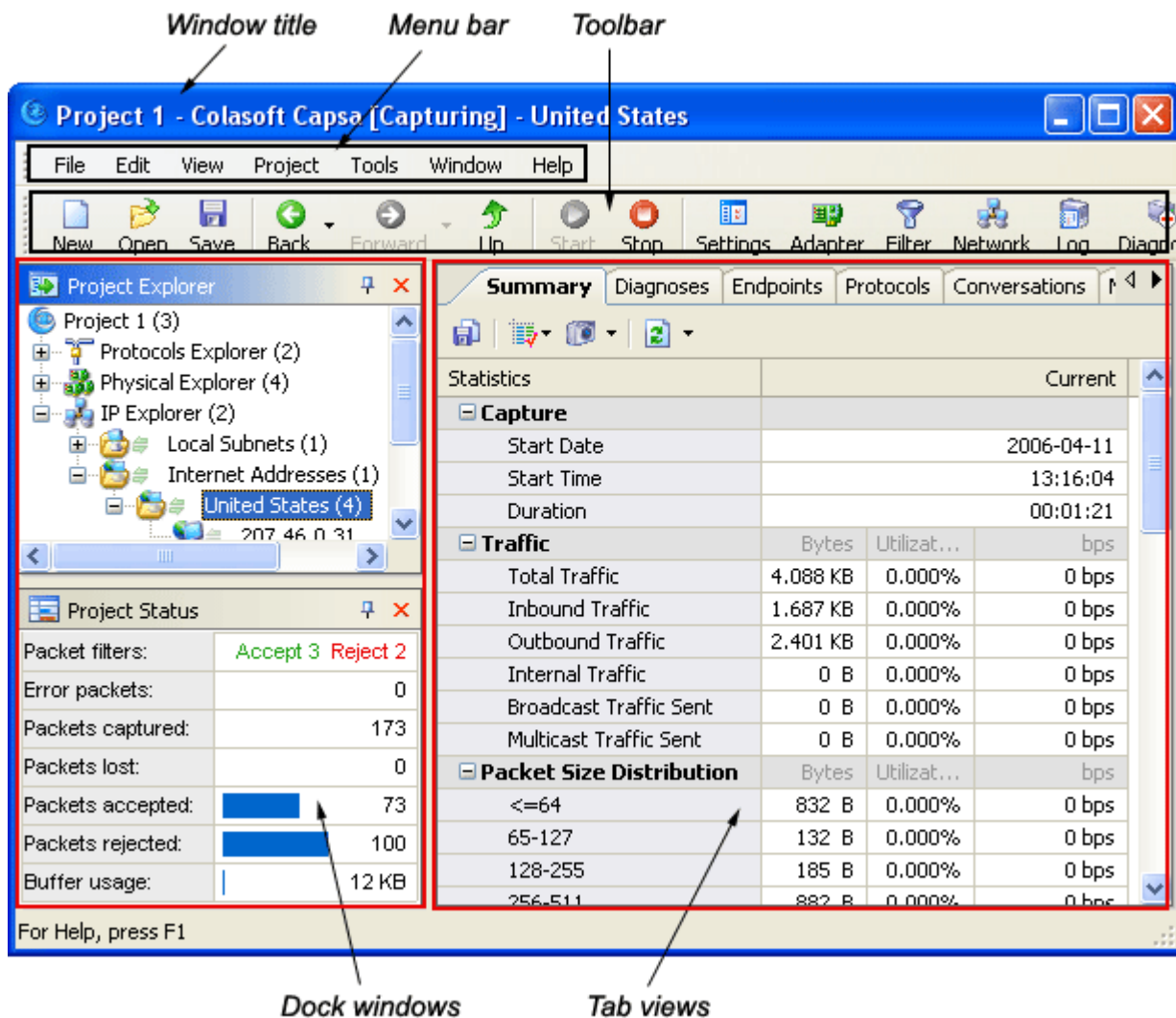
It is allowed to change adapter during the capture process, however, in order to keep the data displayed accurate and up to date, any change to adapter settings will clear or reset some project items, e.g. statistic values, graph data, analyzers, conversations and packet buffer. Log data are optionally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



Click the **OK** button to start capture.

Views Layout

This is the project window of Colasoft Capsa.



- **Window title** – shows the current project name.
- **Menu bar** – provides many useful commands of Colasoft Capsa.
- **Tool bar** – contains the buttons for the most commonly used menu commands, which can be added or remove.
- **Project Explorer** dock window – allows users to quickly switch among global statistics and the details of specific nodes
- **Project Status** dock window – presents the general information of the current project, some items can be displayed as either value (by default) or percentage.
- **Tab views** – Colasoft Capsa has nine tab views, each focusing on different network information. The table below offers the main usage of these views.

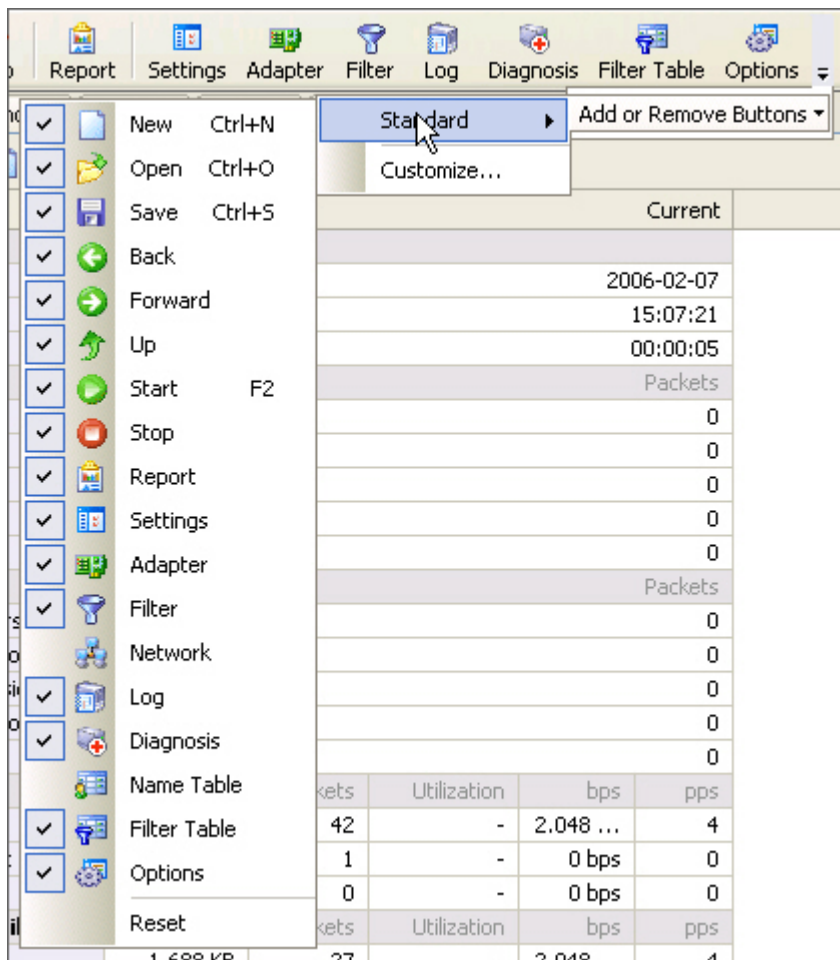
Tool bar

The toolbar provides the button navigation for frequently -used tasks in Colasoft Capsa.



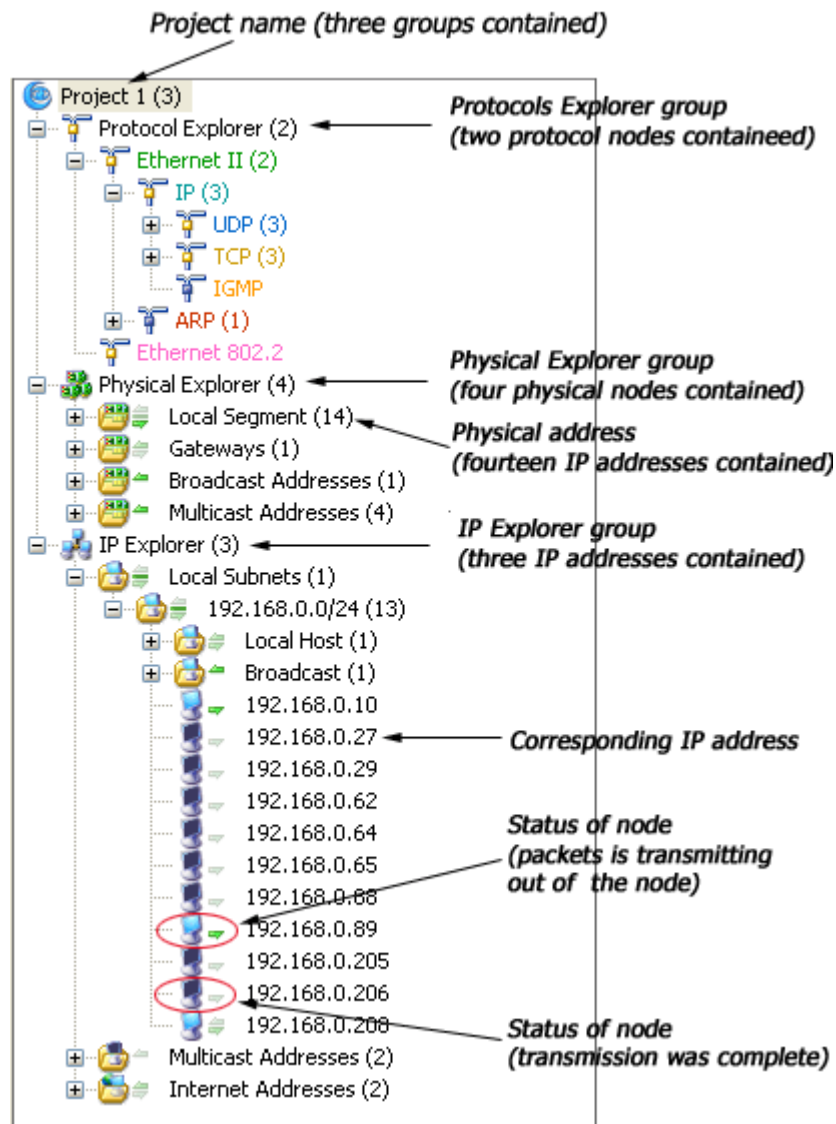
To add or remove buttons from the toolbar, click the **Toolbar Options** at the right of the toolbar, then move the

cursor over the **Add or Remove Buttons** and the **Standard** command, then check or uncheck the buttons you would not like to appear in the toolbar.



Project Explorer

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



Protocol Explorer - lists network endpoints by protocol.

Physical Explorer - lists network endpoints by physical address.

IP Explorer - lists network endpoints by IP address.

Project Status

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

The items **Packets lost**, **Packets accepted**, **Packets rejected** and **Buffer usage** can be displayed either as value (by default) or percentage, you can select from the context menu with a right click.

Tab views

Summary view

The Summary view provides the summary statistics of global network or specific network nodes.

Display Options

Save as Take snapshot Refresh

Summary Diagnosis Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports


Sub-column

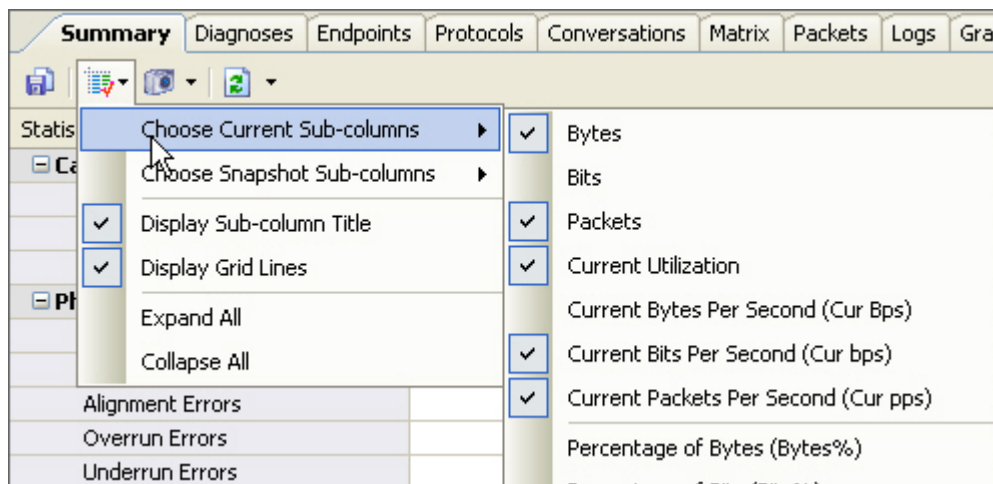
Statistics	Current				
[-] Capture					
Start Date	2007-08-16				
Start Time	16:17:57				
Duration	00:00:24				
[+] Physical Errors					
[+] 802.3 Errors					
[-] Traffic	Bytes	Packets	Utilization	bps	pps
Total Traffic	1.639 KB	22	0.003%	2.624 ...	4
Broadcast Traffic Sent	262 B	1	0.000%	0 bps	0
Multicast Traffic Sent	0 B	0	0.000%	0 bps	0
[-] Packet Size Distribution	Bytes	Packets	Utilization	bps	pps
<=64	1.188 KB	19	0.001%	1.024 ...	2
65-127	200 B	2	0.002%	1.600 ...	2
128-255	0 B	0	0.000%	0 bps	0
256-511	262 B	1	0.000%	0 bps	0
512-1023	0 B	0	0.000%	0 bps	0
1024-1517	0 B	0	0.000%	0 bps	0
>=1518	0 B	0	0.000%	0 bps	0
[+] TCP Packets					
[+] TCP Connections					
[+] DNS Analysis					
[+] SMTP Analysis					
[+] POP3 Analysis					
[+] FTP Analysis					
[+] HTTP Analysis					
[+] All Instant Messenger Activities					
[+] MSN Activities					
[+] AIM Activities					
[+] ICQ Activities					
[+] Yahoo Messenger Activities					

❖ Custom columns

By default, only some sub-columns are displayed. To view more statistic information in different

columns, right click in the display and put the mouse pointer on **Choose Current Sub-columns**

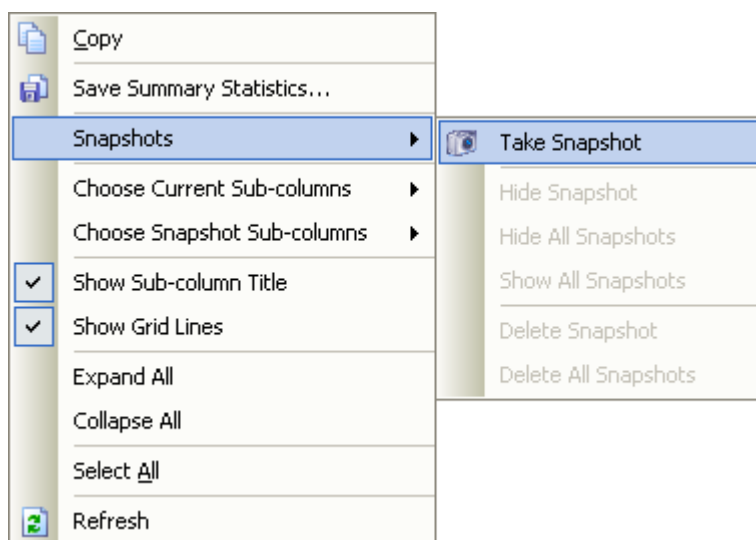
and then check columns from the context menu. Alternately, you can use the icon  to check more sub-columns.



❖ Snapshots

You can take snapshots for the summary statistics at any time, which will be very helpful if you want to compare your network state in the future.

Click the icon  or right click, select the **Take Snapshot** from the sub-context menu. Repeat the operations to take multiple snapshots.






Diagnoses view

The **Diagnoses** view presents the diagnosis events of global network or selected network node. You can find a diagnosis statistics according to network layers from the upper view, whereas the corresponding events are listed in the lower sub view, each event is assigned a severity level.








Save As Display options Refresh

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

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





Events




 0
  0
  0
  0
 All Diagnosis Events: 8,078

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

Show events of the selected item

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

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

❖ Event Properties

To get a detailed description and remedy suggestion, push the **References** tab in the lower sub view (if applicable).

Summary **Diagnoses** Endpoints Protocols Conversations

21.cscproj\Diagnoses

Name	Count
All Diagnosis Events	52
Application Layer	32
DNS Server Slow Response Time	1
HTTP Server Slow Response Time	31
Transport Layer	20
TCP Reset Connection	14
TCP Retransmissions	3
TCP Too Many Retransmissions	3

Events References

HTTP Server Slow Response Time

Description:
The average response time from the server is equal to or higher than the Slow Response Time threshold.

Possible causes and solutions:
The web server is overloaded.

You can also right click in the upper view and choose the **Properties** to view the references in a new window.

Summary **Diagnoses** Endpoints Protocols Conversations Mal

POP3 Server Returned Error

POP3 Server Slow Response Time

Transport Layer

TCP Repeated Connection

TCP Retransmissions

TCP Slow ACK

TCP Too Many Retransmissions

Network Layer

Events References

POP3 Server Returned Error

Description:

Copy Ctrl+C

Save Diagnosis Statistics...

Show Grid Lines

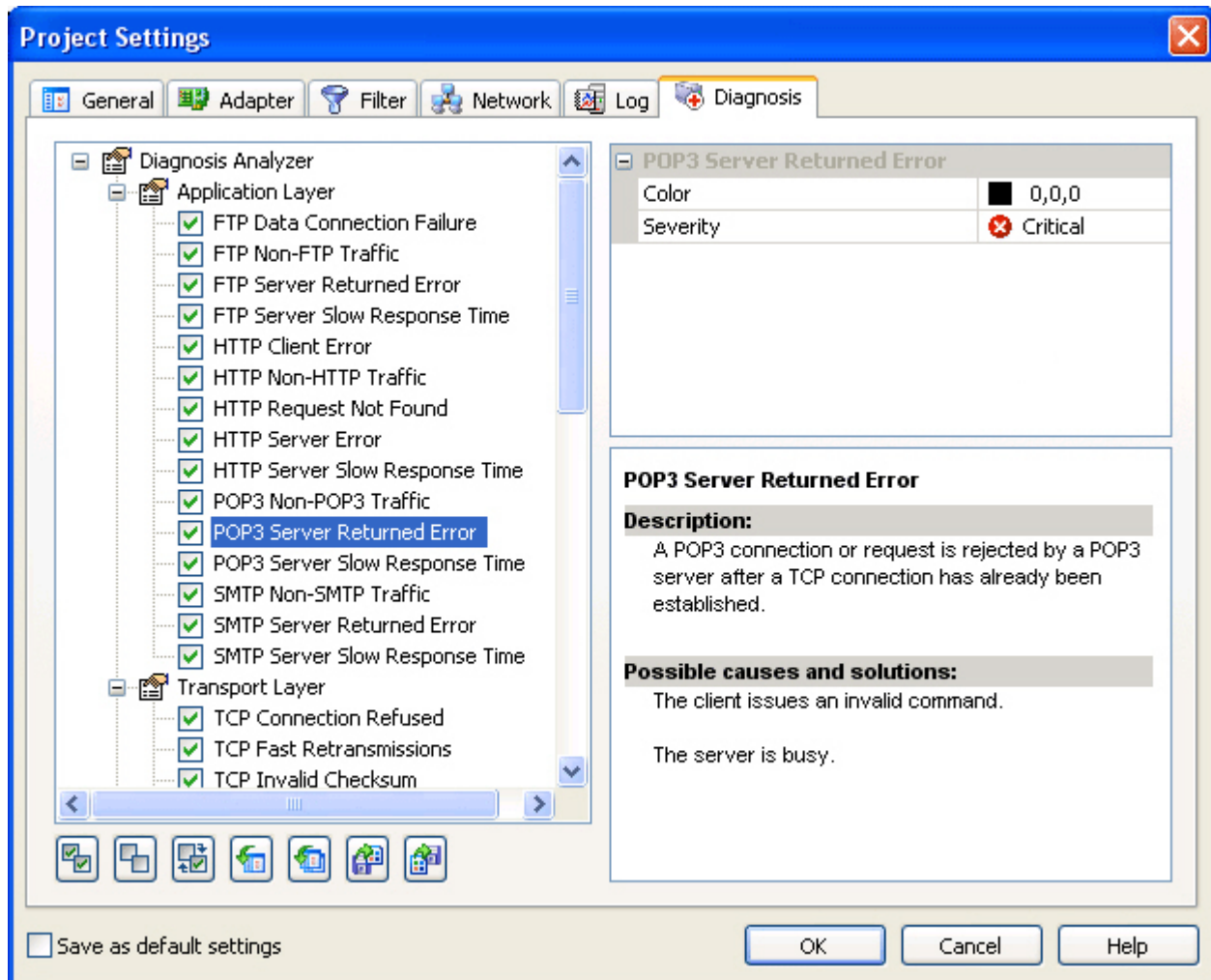
Expand All

Collapse All

Select All Ctrl+A

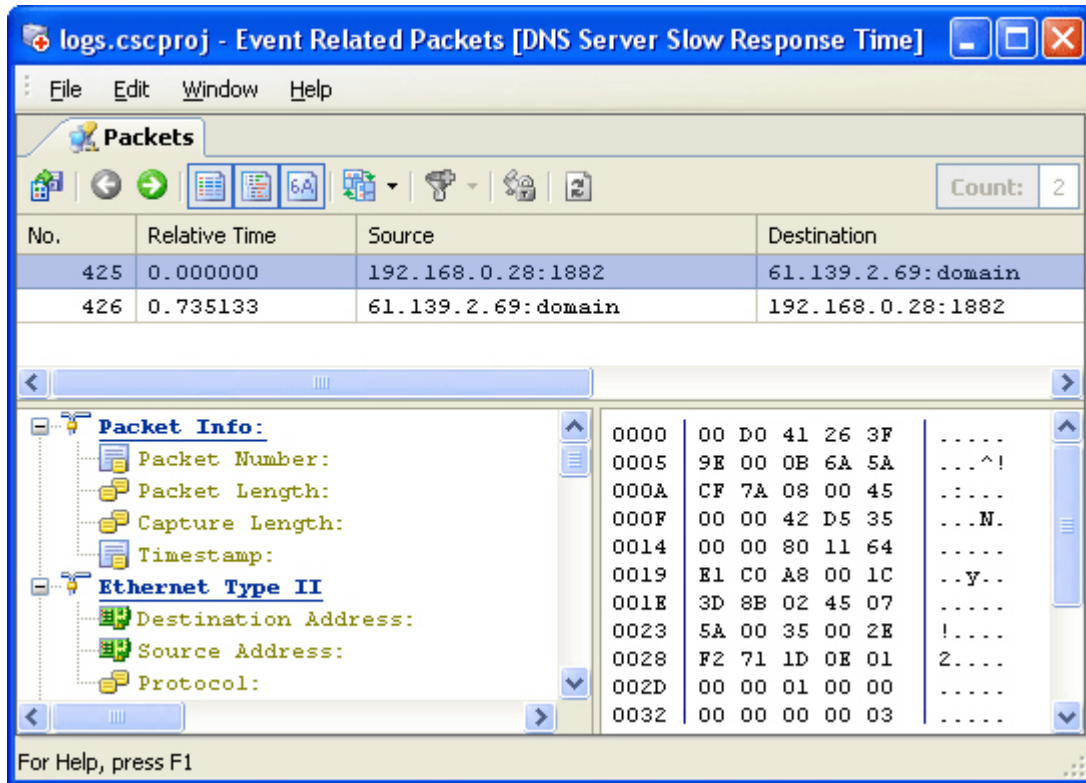
Refresh F5

Properties



❖ View relative packets of an event

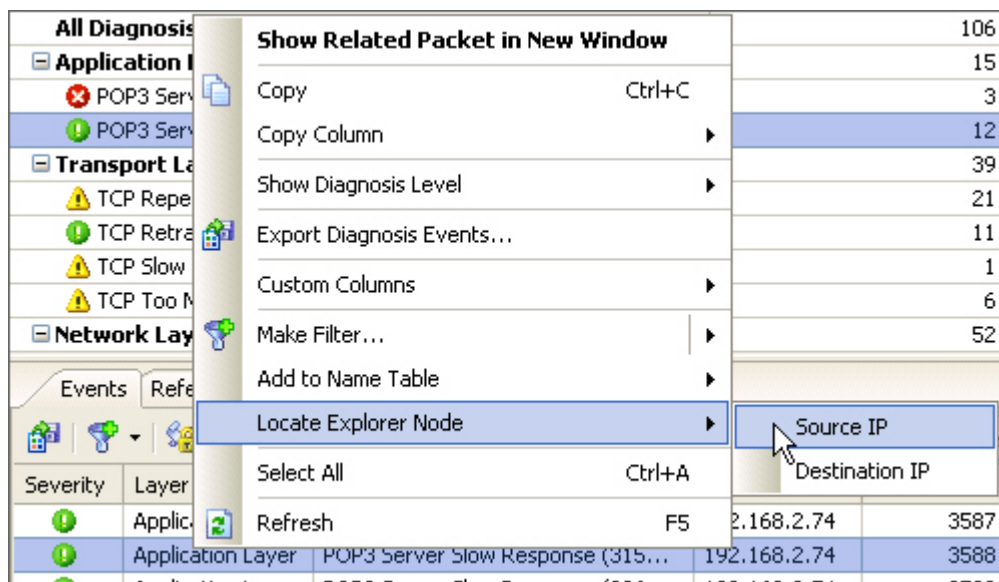
Double click an event in the **Events** sub view, Colasoft Capsa will open an **Event Relative Packets** window showing the related packet information to this event.



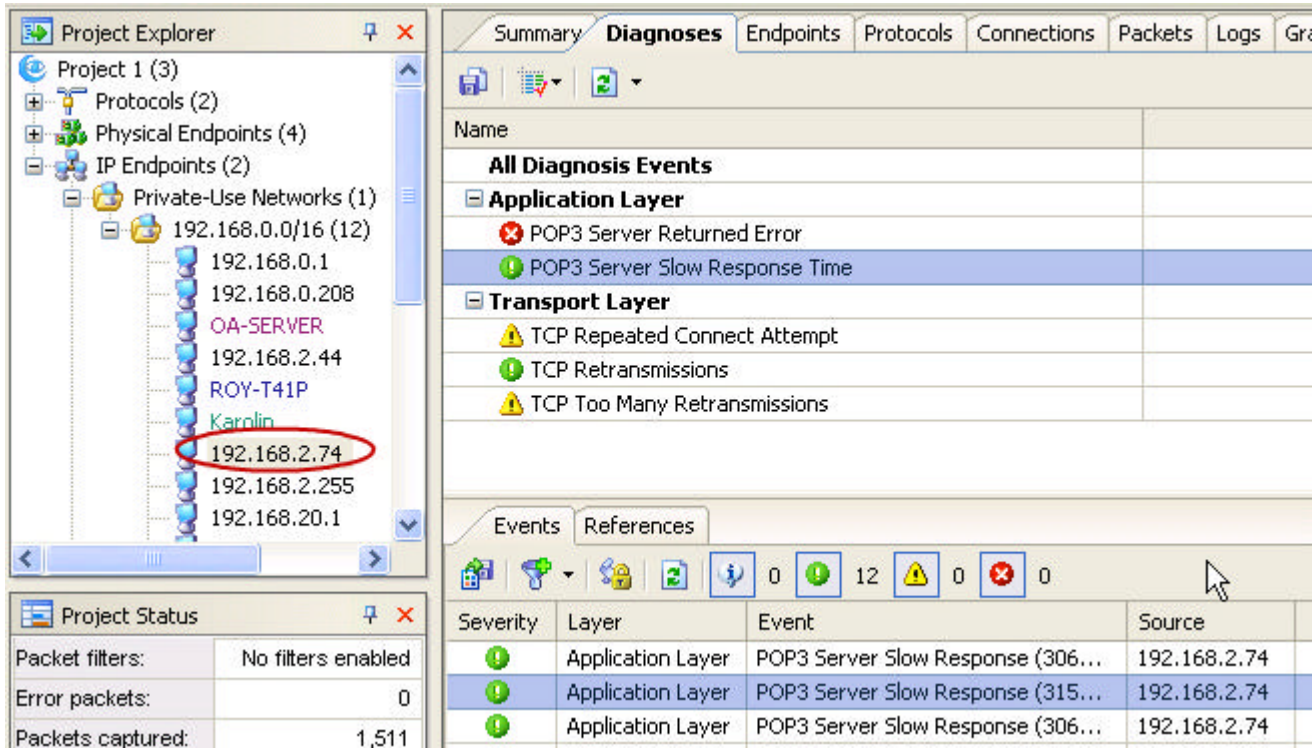
❖ Locate Explorer Node

You can locate the current node in the **Project Explorer**, and then switch to other views for more information on the node.

- Select an item and right click.
- Choose the **Locate Explorer Node** from the context menu and select the **Source IP/Destination IP**.



- The **Source IP** was highlighted in the **Project Explorer** window.



Project Explorer

- Project 1 (3)
 - Protocols (2)
 - Physical Endpoints (4)
 - IP Endpoints (2)
 - Private-Use Networks (1)
 - 192.168.0.0/16 (12)
 - 192.168.0.1
 - 192.168.0.208
 - OA-SERVER
 - 192.168.2.44
 - ROY-T41P
 - Karolin
 - 192.168.2.74**
 - 192.168.2.255
 - 192.168.20.1

Project Status

Packet filters:	No filters enabled
Error packets:	0
Packets captured:	1,511

Diagnoses

All Diagnosis Events

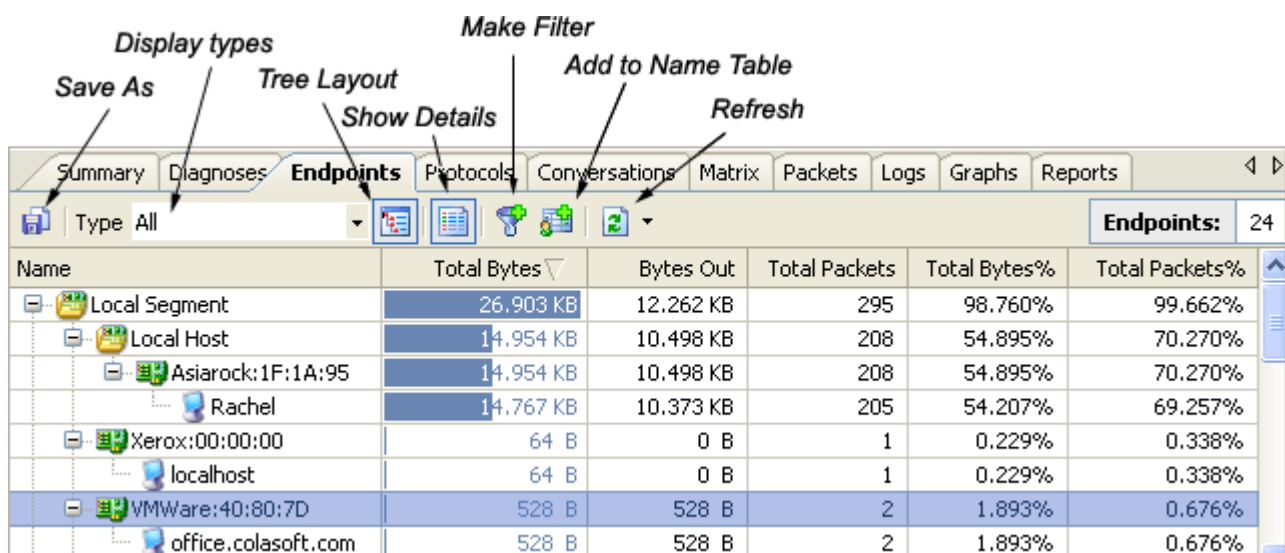
- Application Layer**
 - POP3 Server Returned Error
 - POP3 Server Slow Response Time
- Transport Layer**
 - TCP Repeated Connect Attempt
 - TCP Retransmissions
 - TCP Too Many Retransmissions

Events

Severity	Layer	Event	Source
!	Application Layer	POP3 Server Slow Response (306...	192.168.2.74
!	Application Layer	POP3 Server Slow Response (315...	192.168.2.74
!	Application Layer	POP3 Server Slow Response (306...	192.168.2.74

Endpoints view

The **Endpoints** view presents the detailed communications of each endpoint in network.



Endpoints

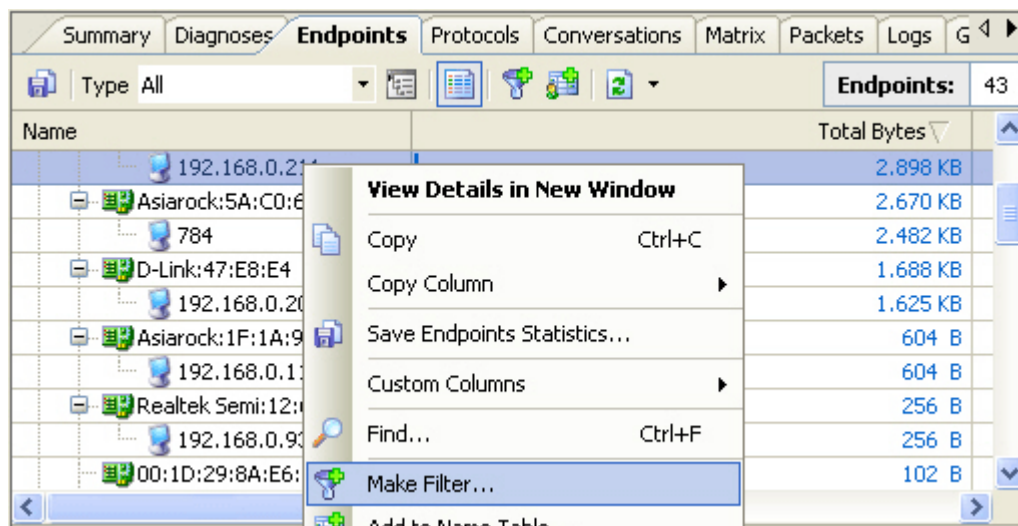
Endpoints: 24

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

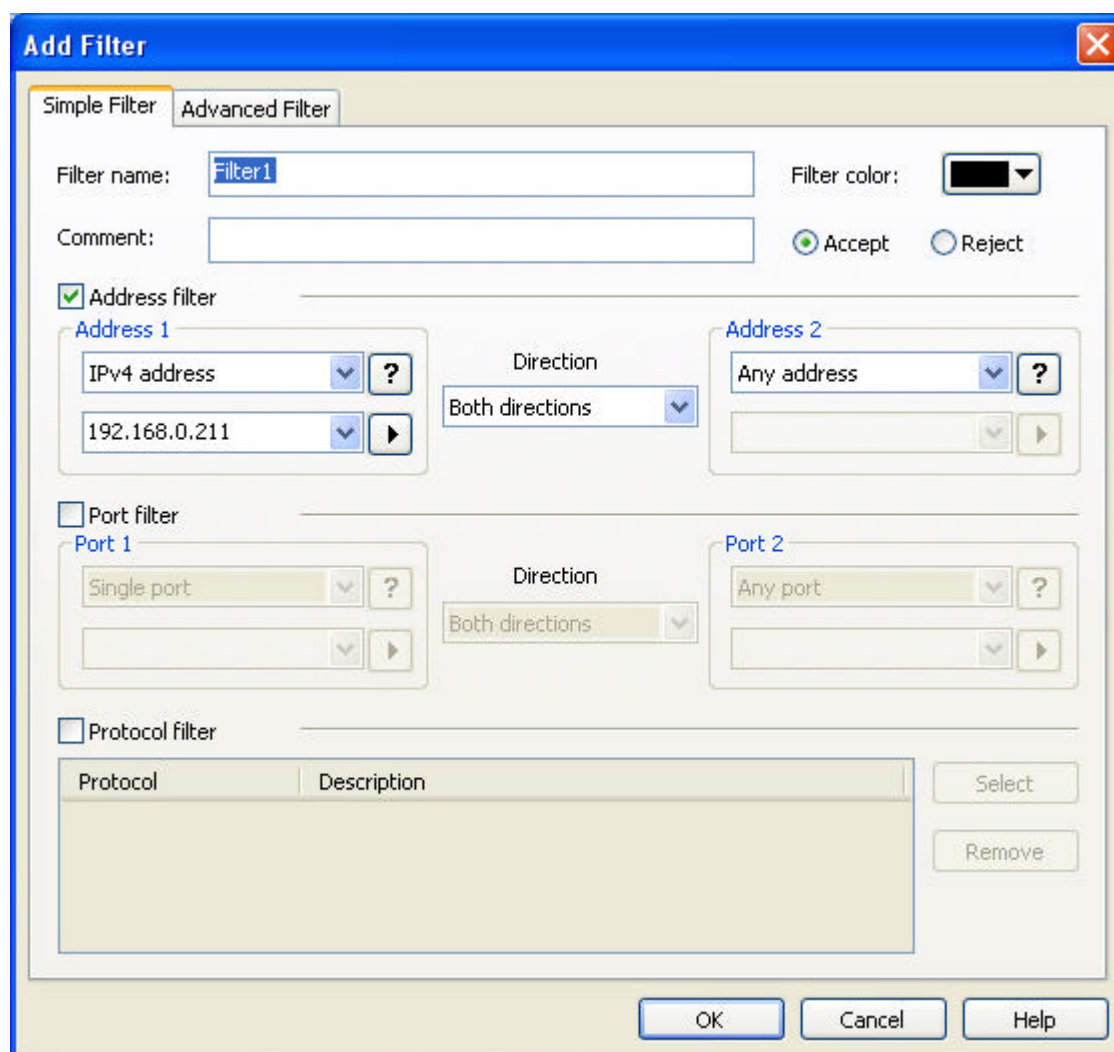
❖ Make a filter from captured packets

It is available to make filters directly from this view.

- Select an endpoint from the list.
- Right click and choose the **Make Filter...** command from the context menu.



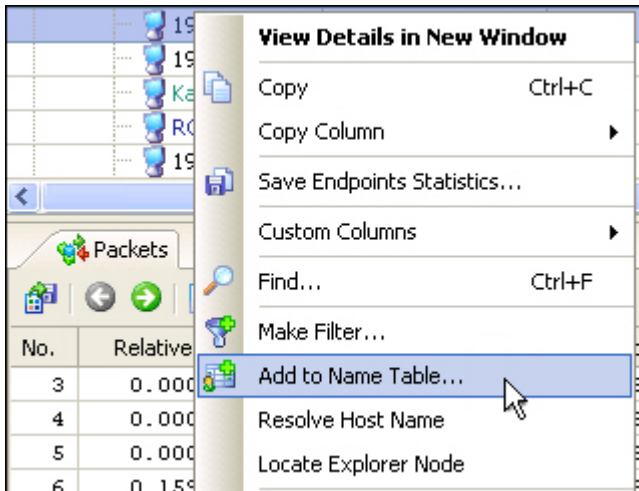
- You will see an **Add Filter** dialog the predefined parameters from the endpoint you selected. You can name it, give it a comment or modify its parameters.



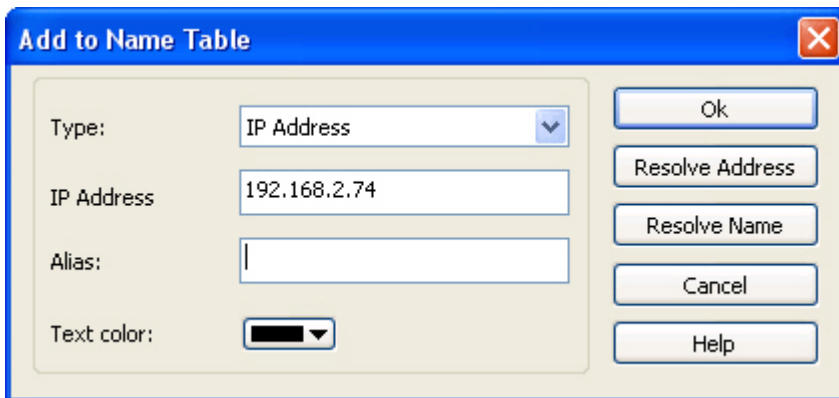
❖ Add Name Table

Use the **Name Table** to specify a new name for an endpoint and make it familiar to you.

- Select an endpoint, right click and choose the **Add to Name Table...** command.



Specify the type of the item, **IP Address**, **Physical Address** and **TCP-UDP Port**, the corresponding address or port number, alias and its color when showed in the **Name Table** and tab views.



Protocols view

The **Protocols** view displays the information of protocols used in network communications.

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

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

Display types *Make Filter* *Show Details* *Locate Explorer Node*

Save As Refresh

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

Type Hierarchical Protocols: 28

Name	Bytes	Packets	bps	Connections
Ethernet II	28.458 MB	56,815	1.217 Mbps	2,370
IP	28.451 MB	56,693	1.217 Mbps	2,370
UDP	25.384 MB	39,723	1.129 Mbps	0
Other	24.935 MB	35,430	1.118 Mbps	0
DNS	383.765 KB	3,877	9.224 Kbps	0
NetBIOS	31.406 KB	297	2.304 Kbps	0
Name Service	26.365 KB	275	2.304 Kbps	0
Datagram S...	5.041 KB	22	0 bps	0
RTCP	30.060 KB	87	0 bps	0
BOOTP	10.051 KB	30	0 bps	0
DHCP	10.051 KB	30	0 bps	0
HTTP Proxy	128 B	2	0 bps	0
TCP	3.067 MB	16,966	88.152 Kbps	2,370
HTTP	2.142 MB	5,636	39.576 Kbps	172
Other	322.208 KB	3,981	18.720 Kbps	673
CIFS	245.570 KB	3,256	15.312 Kbps	856
NetBIOS	159.510 KB	2,475	12.672 Kbps	635

You can sort the captured data by clicking on a column heading

Sort endpoints by Total Bytes

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

Type All

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

Conversations view

The **Conversations** view dynamically presents the real-time status of Physical, IP, TCP and UDP conversations between pairs of endpoints, the sub-views offer the related packets and

reconstructed stream the active conversation.

Conversations type Show Details Locate Explorer Node Refresh Conversations summary

Export Make Filter

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

Physical Conversations: 26

Conversation:

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

Packets

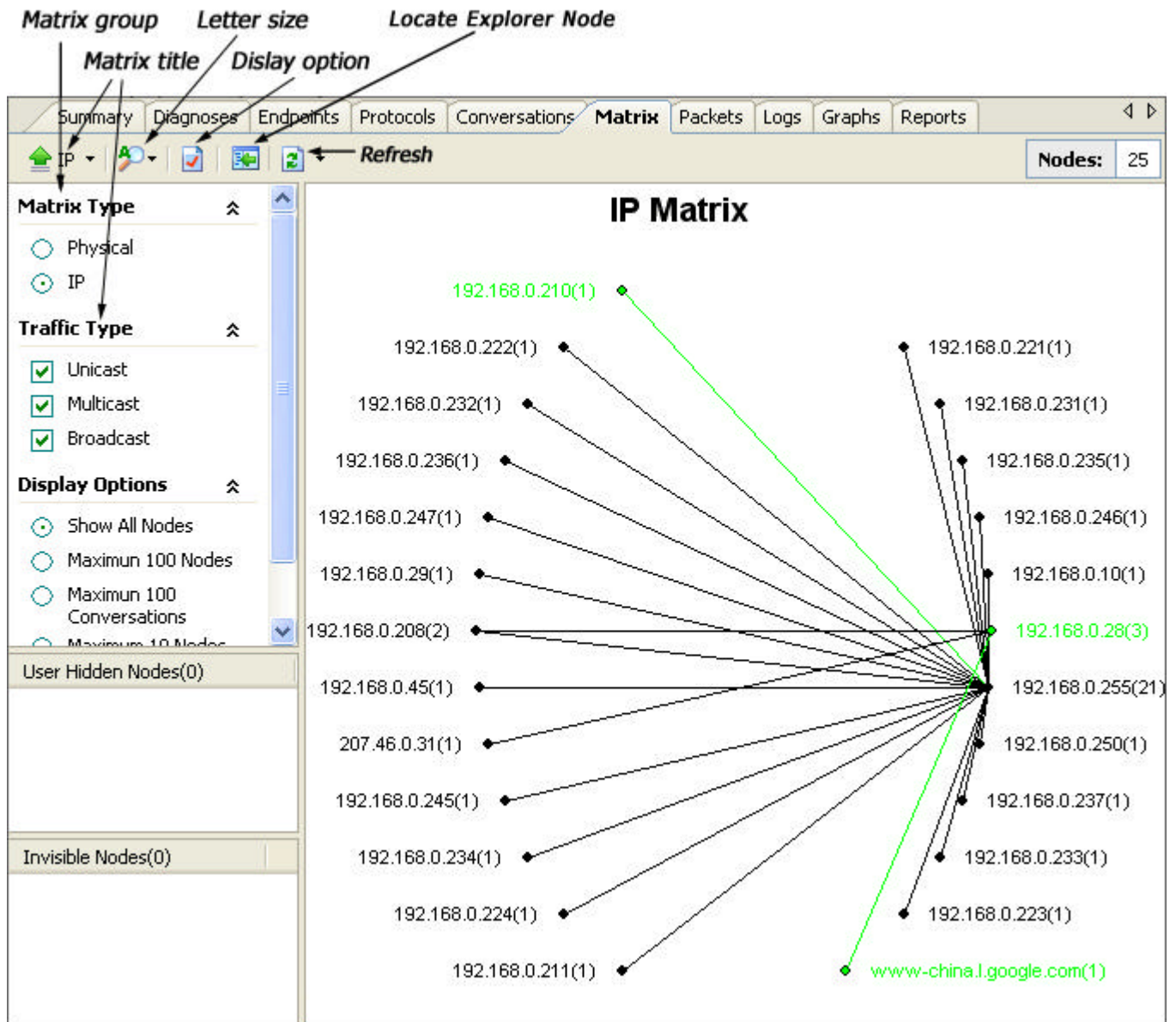
No.	Relative Time	Source	Destination	Size
12	0.000000	192.168.0.28:3325	209.237.237.101...	64
13	0.257804	192.168.0.28:2184	207.46.0.31:msnp	64
14	0.563397	207.46.0.31:msnp	192.168.0.28:2184	66
16	0.666863	192.168.0.28:2184	207.46.0.31:msnp	64

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

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

Matrix view

The **Matrix** view shows the network traffic statistics. The line weight indicate the volume of traffic between nodes arranged in an extensive ellipse indicate the traffic.



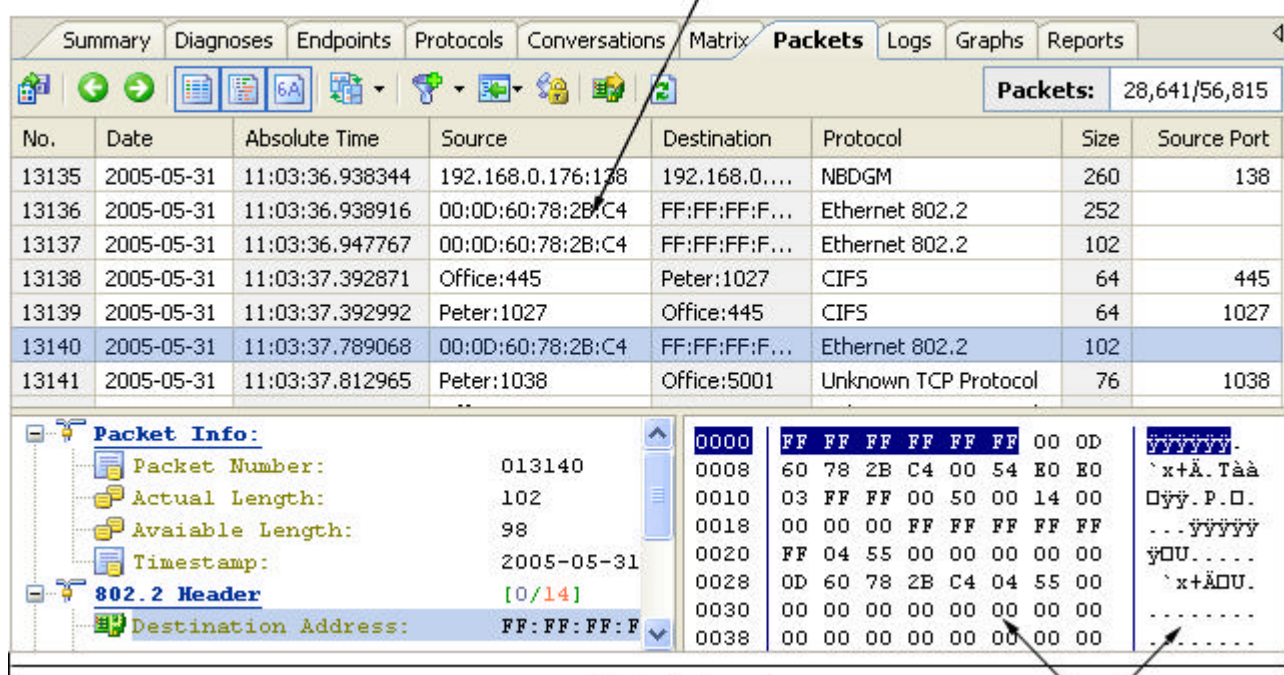
The **Matrix** view includes individual tools to customize the display types of network traffic. This lets you quickly create a picture of all the traffic or sending/receiving traffic.

The nodes around an elongated ellipse display the hosts in your network, the line weight present the volume of traffic between nodes. The green color reveals the traffic is transmitting current now and the black color displays the transmission is completed by default. When you drag nodes to a new position, the connecting lines rubber-band. Colasoft Capsa will popup a notice if the captured nodes exceed 1000.

Packets view

The **Packets** view presents a list of captured packets and the packet decode information in **Hex**, **ASCII** and **EBCDIC**.

Packet list



Packet list

No.	Date	Absolute Time	Source	Destination	Protocol	Size	Source Port
13135	2005-05-31	11:03:36.938344	192.168.0.176:138	192.168.0....	NBDGM	260	138
13136	2005-05-31	11:03:36.938916	00:0D:60:78:2B:C4	FF:FF:FF:F...	Ethernet 802.2	252	
13137	2005-05-31	11:03:36.947767	00:0D:60:78:2B:C4	FF:FF:FF:F...	Ethernet 802.2	102	
13138	2005-05-31	11:03:37.392871	Office:445	Peter:1027	CIFS	64	445
13139	2005-05-31	11:03:37.392992	Peter:1027	Office:445	CIFS	64	1027
13140	2005-05-31	11:03:37.789068	00:0D:60:78:2B:C4	FF:FF:FF:F...	Ethernet 802.2	102	
13141	2005-05-31	11:03:37.812965	Peter:1038	Office:5001	Unknown TCP Protocol	76	1038

Packet Info:

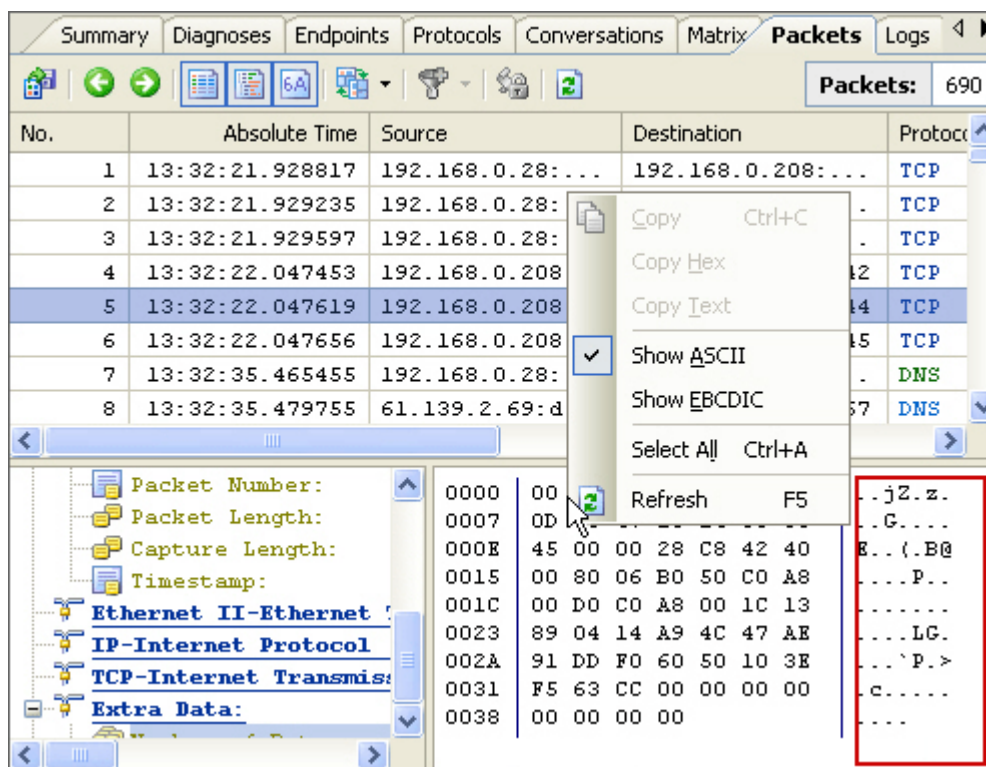
Packet Number: 013140
 Actual Length: 102
 Available Length: 98
 Timestamp: 2005-05-31
802.2 Header [0/14]
 Destination Address: FF:FF:FF:F

Packet decode

Hex/ASCII/EBCDIC view

❖ Packet decoding formats

- Right click and choose the **Show EBCDIC** command from the context menu.



Packet list

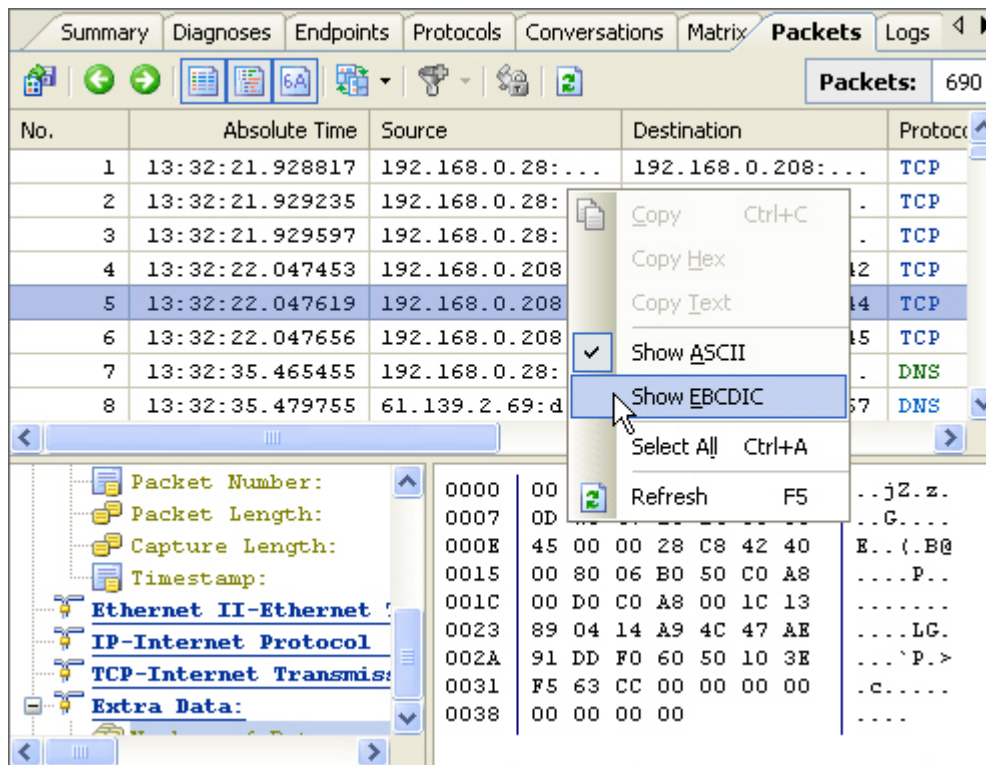
No.	Absolute Time	Source	Destination	Protocol
1	13:32:21.928817	192.168.0.28:...	192.168.0.208:...	TCP
2	13:32:21.929235	192.168.0.28:...	...	TCP
3	13:32:21.929597	192.168.0.28:...	...	TCP
4	13:32:22.047453	192.168.0.208	...	TCP
5	13:32:22.047619	192.168.0.208	...	TCP
6	13:32:22.047656	192.168.0.208	...	TCP
7	13:32:35.465455	192.168.0.28:...	...	DNS
8	13:32:35.479755	61.139.2.69:d	...	DNS

Packet Info:

Packet Number: 013140
 Packet Length: 102
 Capture Length: 98
 Timestamp: 2005-05-31
Ethernet II-Ethernet
IP-Internet Protocol
TCP-Internet Transmis
Extra Data:

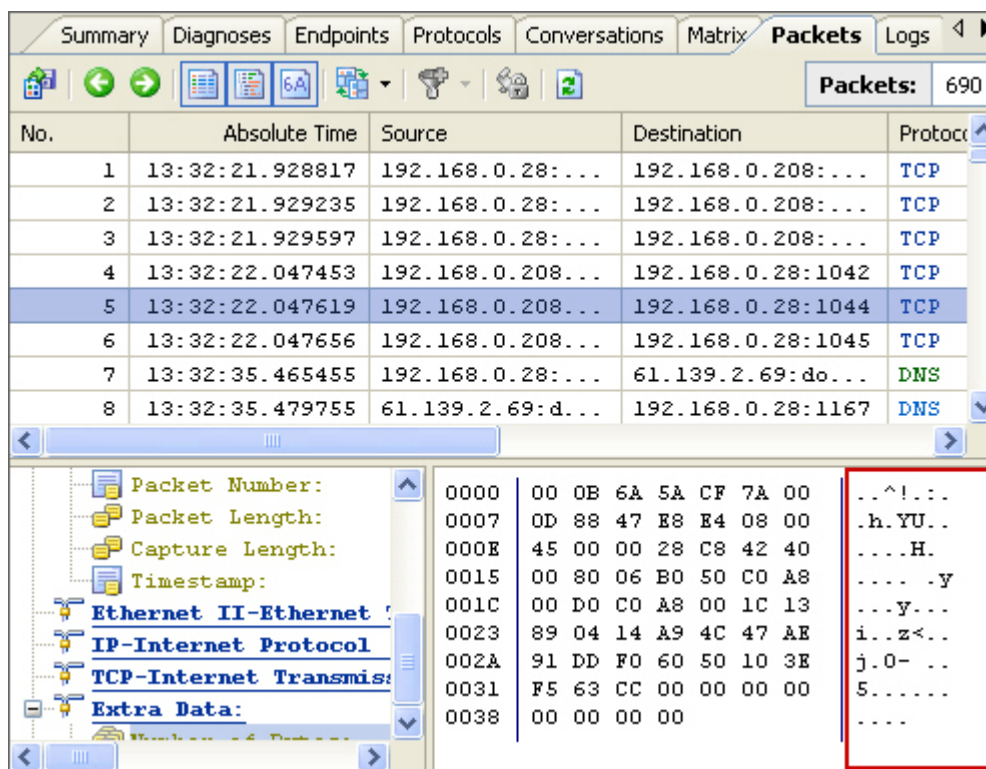
Packet decode

Hex/ASCII/EBCDIC view



The screenshot shows the 'Packets' tab in Colasoft Capsa. A packet list is displayed with columns: No., Absolute Time, Source, Destination, and Protocol. Packet 5 is selected. A right-click context menu is open over packet 5, showing options: Copy (Ctrl+C), Copy Hex, Copy Text, Show ASCII (checked), Show EBCDIC, Select All (Ctrl+A), and Refresh (F5). The packet details pane on the left shows the selected packet's structure: Ethernet II-Ethernet..., IP-Internet Protocol..., and TCP-Internet Transmis... The packet data pane on the right shows the raw data in hexadecimal and ASCII.

No.	Absolute Time	Source	Destination	Protocol
1	13:32:21.928817	192.168.0.28:...	192.168.0.208:...	TCP
2	13:32:21.929235	192.168.0.28:...	192.168.0.208:...	TCP
3	13:32:21.929597	192.168.0.28:...	192.168.0.208:...	TCP
4	13:32:22.047453	192.168.0.208	192.168.0.28:1042	TCP
5	13:32:22.047619	192.168.0.208	192.168.0.28:1044	TCP
6	13:32:22.047656	192.168.0.208	192.168.0.28:1045	TCP
7	13:32:35.465455	192.168.0.28:...	61.139.2.69:do...	DNS
8	13:32:35.479755	61.139.2.69:d...	192.168.0.28:1167	DNS



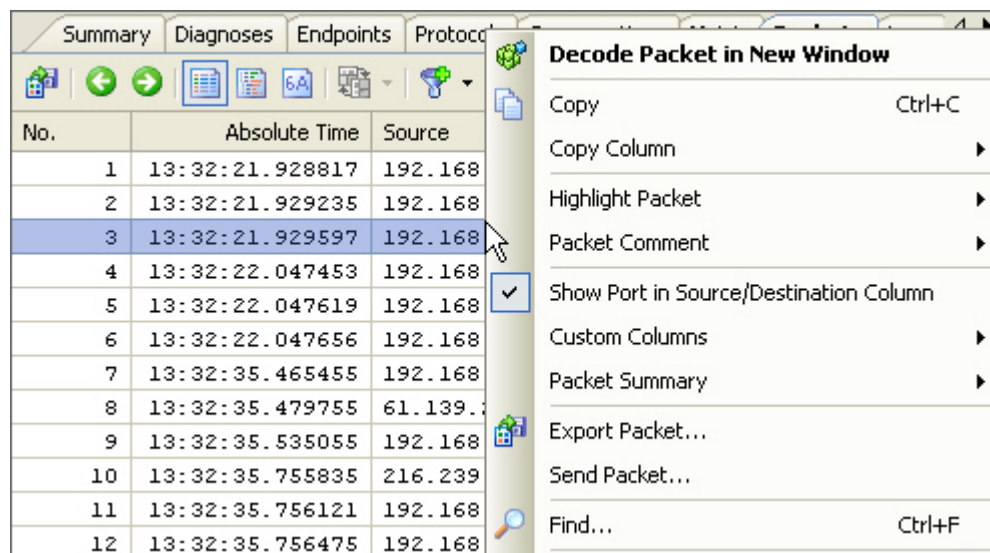
The screenshot shows the 'Packets' tab in Colasoft Capsa. A packet list is displayed with columns: No., Absolute Time, Source, Destination, and Protocol. Packet 5 is selected. The packet details pane on the left shows the selected packet's structure: Ethernet II-Ethernet..., IP-Internet Protocol..., and TCP-Internet Transmis... The packet data pane on the right shows the raw data in hexadecimal and ASCII. A red box highlights the ASCII data, which contains the text: ..^!... .h.YU... ..H... ..y... ..y... i..z<.. j.0- .. 5.....

No.	Absolute Time	Source	Destination	Protocol
1	13:32:21.928817	192.168.0.28:...	192.168.0.208:...	TCP
2	13:32:21.929235	192.168.0.28:...	192.168.0.208:...	TCP
3	13:32:21.929597	192.168.0.28:...	192.168.0.208:...	TCP
4	13:32:22.047453	192.168.0.208...	192.168.0.28:1042	TCP
5	13:32:22.047619	192.168.0.208...	192.168.0.28:1044	TCP
6	13:32:22.047656	192.168.0.208...	192.168.0.28:1045	TCP
7	13:32:35.465455	192.168.0.28:...	61.139.2.69:do...	DNS
8	13:32:35.479755	61.139.2.69:d...	192.168.0.28:1167	DNS

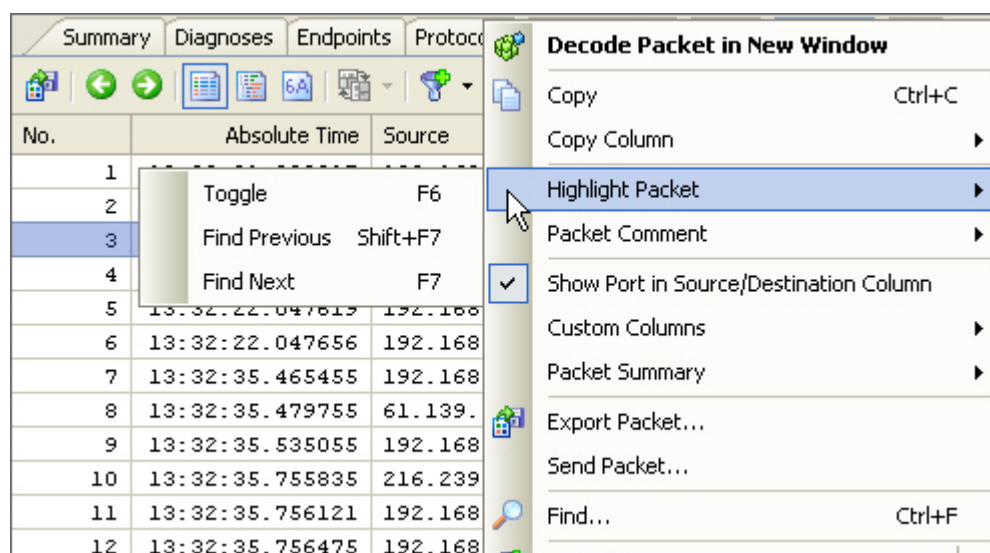
❖ Highlight packet

Highlight some suspect packets to make them easy to find.

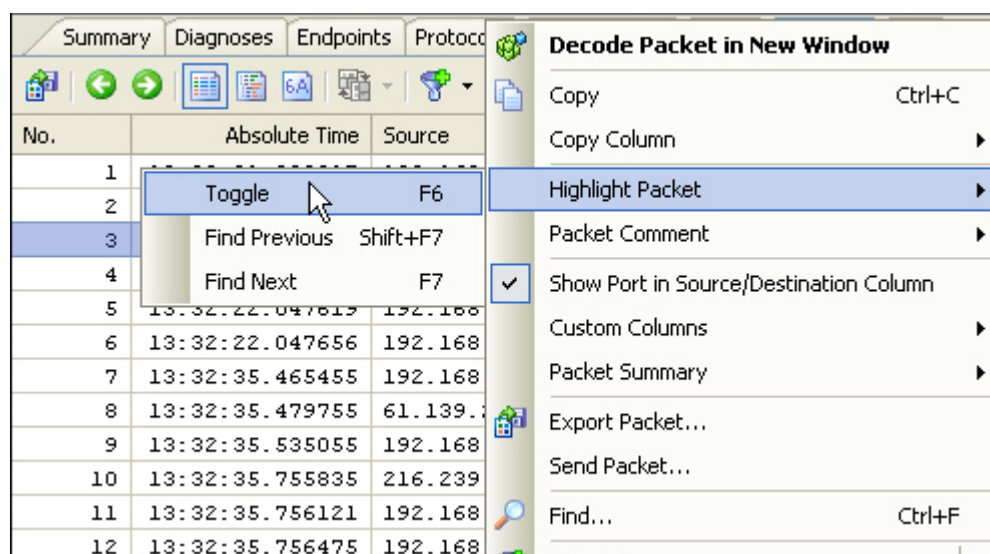
- Select a packet from the Packet list and right click.




- Choose the **Highlight Packet** command.



- Select **Toggle** command.



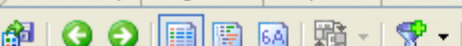
- The selected packet will be highlighted in the list.

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs				
 Packets: 690				
No.	Absolute Time	Source	Destination	Protocol
1	13:32:21.928817	192.168.0.28:...	192.168.0.208:...	TCP
2	13:32:21.929235	192.168.0.28:...	192.168.0.208:...	TCP
3	13:32:21.929597	192.168.0.28:...	192.168.0.208:...	TCP
4	13:32:22.047453	192.168.0.208:...	192.168.0.28:1042	TCP
5	13:32:22.047619	192.168.0.208:...	192.168.0.28:1044	TCP
6	13:32:22.047656	192.168.0.208:...	192.168.0.28:1045	TCP
7	13:32:35.465455	192.168.0.28:...	61.139.2.69:do...	DNS
8	13:32:35.479755	61.139.2.69:d...	192.168.0.28:1167	DNS
9	13:32:35.535055	192.168.0.28:...	216.239.63.104...	HTTP
10	13:32:35.755835	216.239.63.10...	192.168.0.28:2352	HTTP
11	13:32:35.756121	192.168.0.28:...	216.239.63.104...	HTTP
12	13:32:35.756475	192.168.0.28:...	216.239.63.104...	HTTP

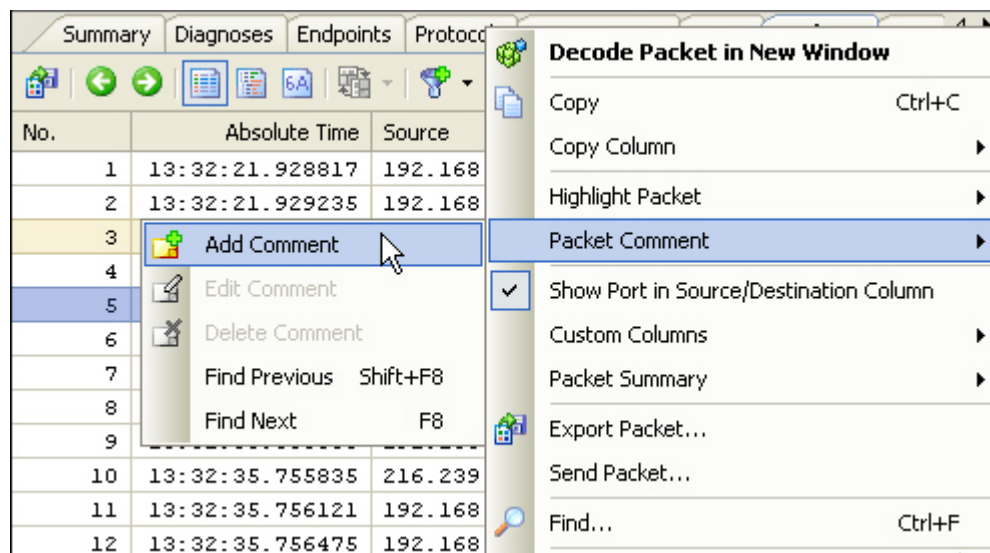
❖ Packet comment

Make a comment to the packet you are interested.

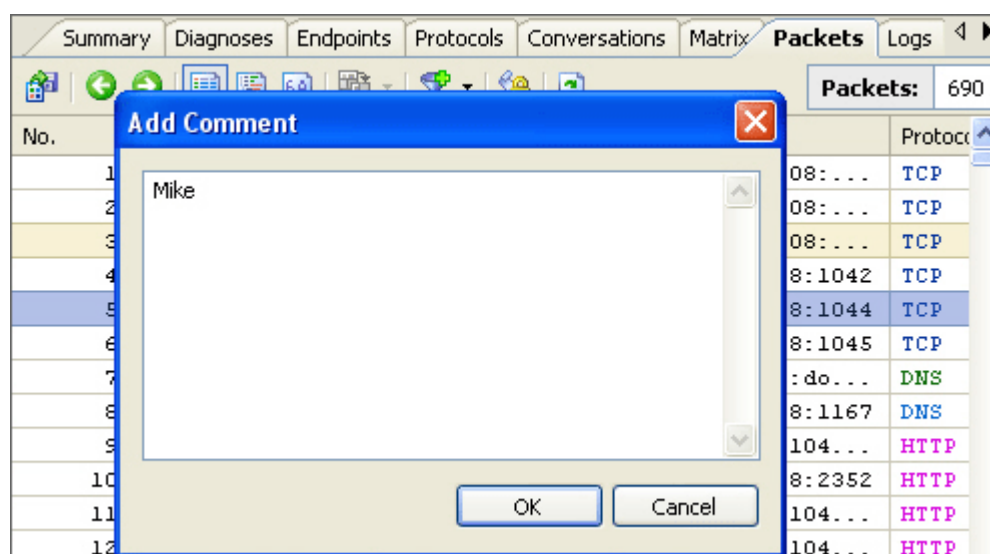
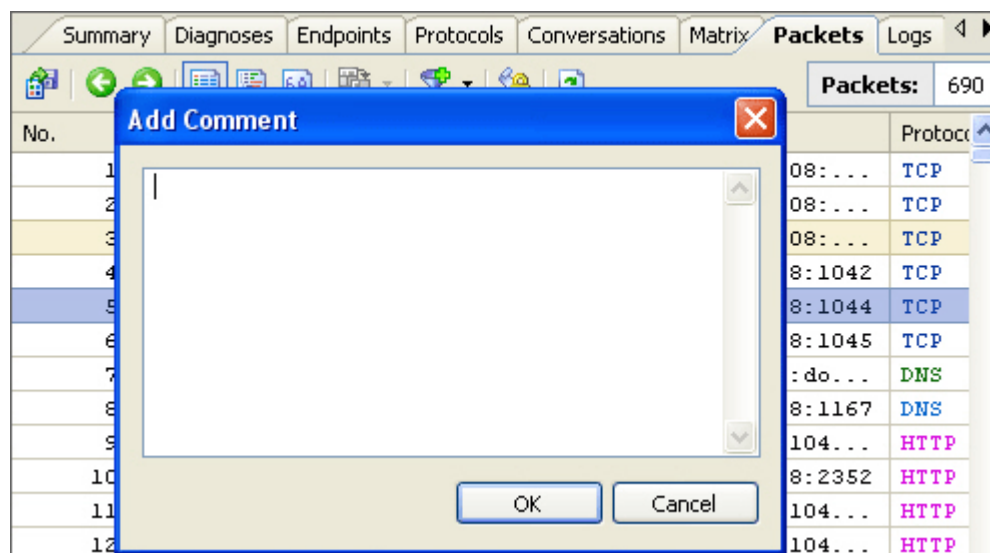
- Select an item and right click.

Summary Diagnoses Endpoints Protocols			
			
No.	Absolute Time	Source	
1	13:32:21.928817	192.168.	Decode Packet in New Window Copy Ctrl+C Copy Column ▶ Highlight Packet ▶ Packet Comment ▶ <input checked="" type="checkbox"/> Show Port in Source/Destination Column Custom Columns ▶ Packet Summary ▶ Export Packet... Send Packet... Find... Ctrl+F Make File...
2	13:32:21.929235	192.168.	
3	13:32:21.929597	192.168.	
4	13:32:22.047453	192.168.	
5	13:32:22.047619	192.168.	
6	13:32:22.047656	192.168.	
7	13:32:35.465455	192.168.	
8	13:32:35.479755	61.139.2	
9	13:32:35.535055	192.168.	
10	13:32:35.755835	216.239.	
11	13:32:35.756121	192.168.	
12	13:32:35.756475	192.168.	

- Choose the **Packet Comment** command in the context menu and select the **Add Comment** from the sub context menu.



- Enter comment in the **Add Comment** dialog.



- In the packet list view the packet you commented on was mark it with an icon.

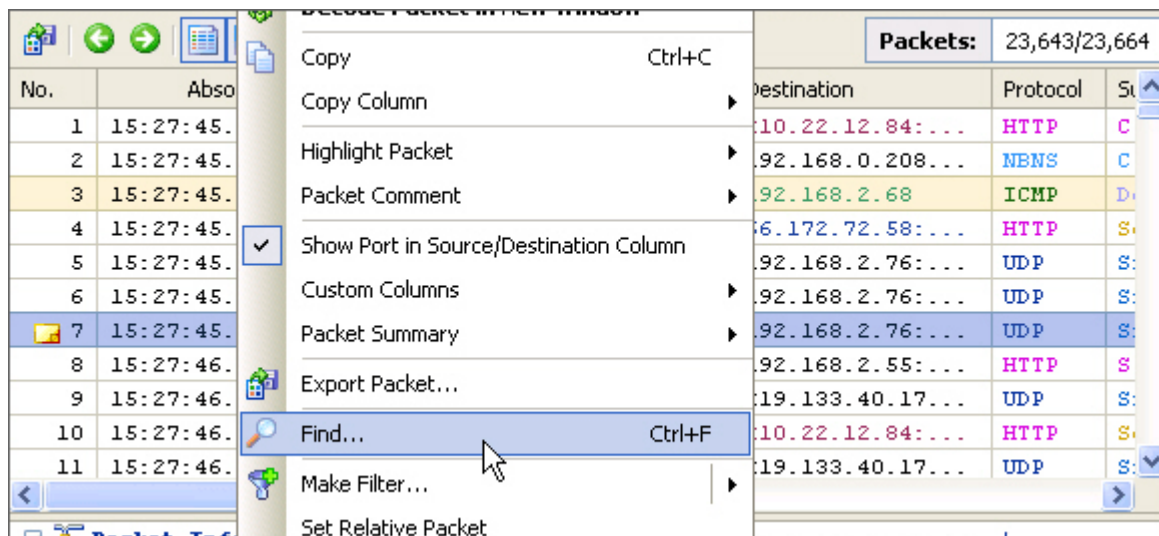
Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs				
Packets: 690				
No.	Absolute Time	Source	Destination	Protocol
1	13:32:21.928817	192.168.0.28:...	192.168.0.208:...	TCP
2	13:32:21.929235	192.168.0.28:...	192.168.0.208:...	TCP
3	13:32:21.929597	192.168.0.28:...	192.168.0.208:...	TCP
4	13:32:22.047453	192.168.0.208:...	192.168.0.28:1042	TCP
5	13:32:22.047619	192.168.0.208:...	192.168.0.28:1044	TCP
6	13:32:22.047656	192.168.0.208:...	192.168.0.28:1045	TCP
7	13:32:35.465455	192.168.0.28:...	61.139.2.69:do...	DNS
8	13:32:35.479755	61.139.2.69:d...	192.168.0.28:1167	DNS
9	13:32:35.535055	192.168.0.28:...	216.239.63.104:...	HTTP
10	13:32:35.755835	216.239.63.10:...	192.168.0.28:2352	HTTP
11	13:32:35.756121	192.168.0.28:...	216.239.63.104:...	HTTP
12	13:32:35.756475	192.168.0.28:...	216.239.63.104:...	HTTP

❖ Find

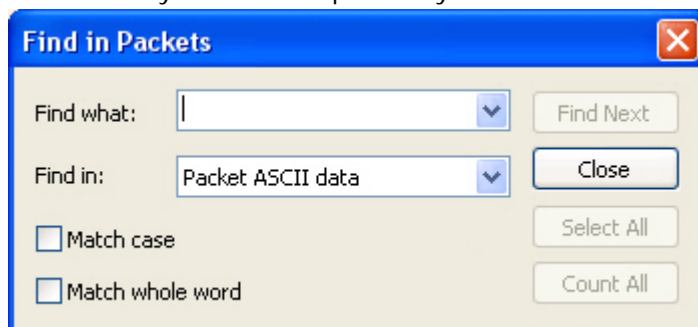
You can easily find a specific item in the **Project Explorer** dock window, **Endpoints** view, **Protocols** view, **Packets** view, **Connections** view and **Logs** view.

For example, find a packet in the **Packets** view.

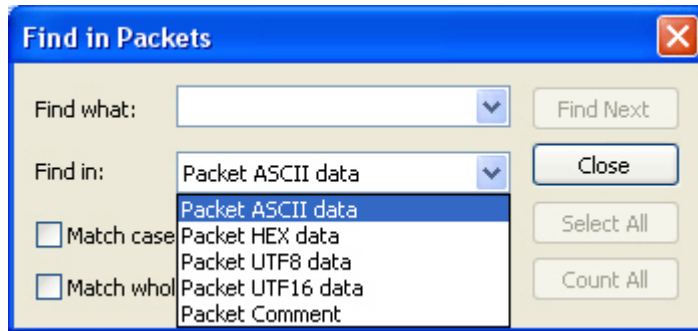
- Select an item, right click and choose **Find** command from the context menu.



- Enter key word of the packets you want to find out.



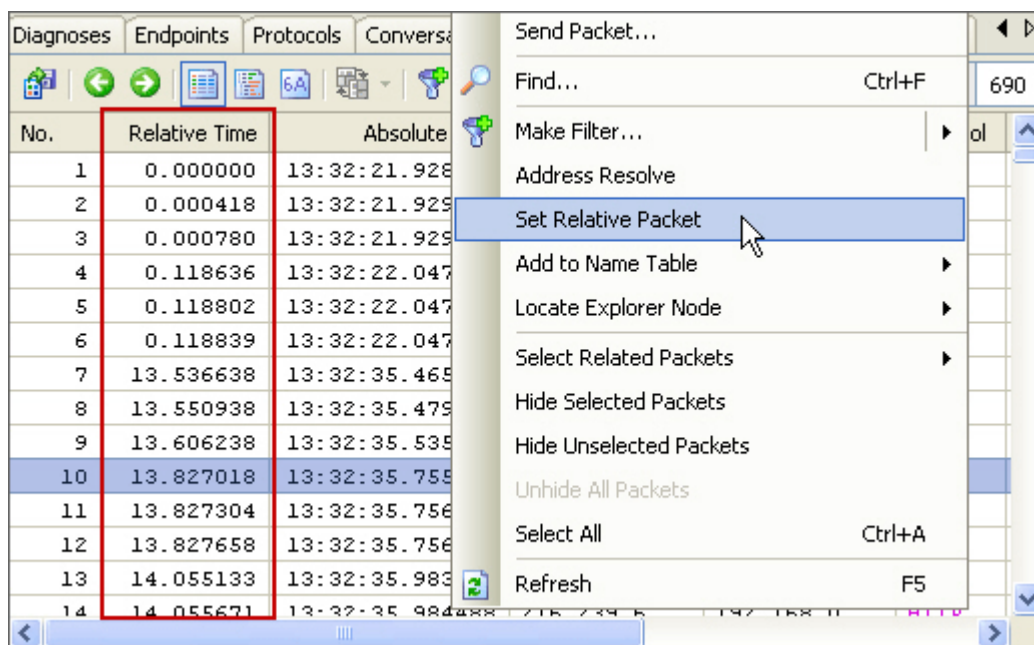
- Specify the scope you want to search in.



❖ Set relative packet

If you set a packet as the relative packet and show the **Relative Time** column, the column will display the time span of other packets from the relative packet.

The following figure is the relative time between every packet in the default order. Select the packet you want to set it as standard and right click. Choose the **Set Relative Packet** command from the context menu.

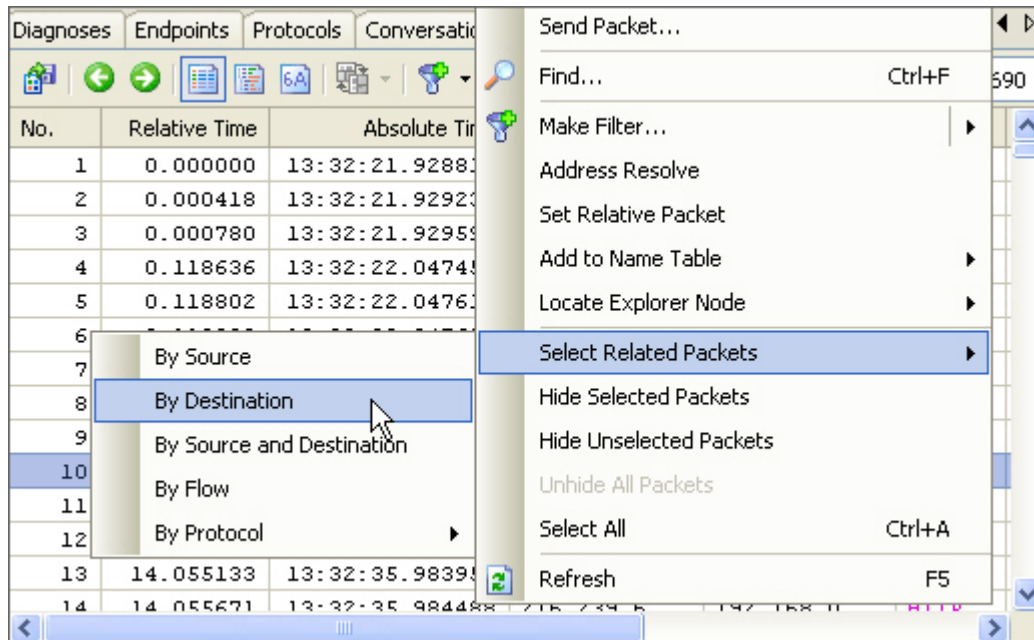


Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports					
					Packets: 690
No.	Relative Time	Absolute Time	Source	Destination	Protocol
1	-13.827018	13:32:21.928817	192.168.0...	192.168.0...	TCP
2	-13.826600	13:32:21.929235	192.168.0...	192.168.0...	TCP
3	-13.826238	13:32:21.929597	192.168.0...	192.168.0...	TCP
4	-13.708382	13:32:22.047453	192.168.0...	192.168.0...	TCP
5	-13.708216	13:32:22.047619	192.168.0...	192.168.0...	TCP
6	-13.708179	13:32:22.047656	192.168.0...	192.168.0...	TCP
7	-0.290380	13:32:35.465455	192.168.0...	61.139.2...	DNS
8	-0.276080	13:32:35.479755	61.139.2...	192.168.0...	DNS
9	-0.220780	13:32:35.535055	192.168.0...	216.239.6...	HTTP
10	0.000000	13:32:35.755835	216.239.6...	192.168.0...	HTTP
11	0.000286	13:32:35.756121	192.168.0...	216.239.6...	HTTP
12	0.000640	13:32:35.756475	192.168.0...	216.239.6...	HTTP
13	0.228115	13:32:35.983950	216.239.6...	192.168.0...	HTTP
14	0.228653	13:32:35.984488	216.239.6...	192.168.0...	HTTP


❖ Filter display packet

By selecting related packets, you can filter out unwanted packets simply and quickly

- Choose the packet you interested in and right click. Then click the **By Destination** listed in the **Selected Related Packets** command.



- The relative packets will be high lighted in the list.

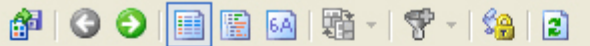
Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports					
					Packets: 690
No.	Relative Time	Absolute Time	Source	Destination	Protocol
1	0.000000	13:32:21.928817	192.168.0...	192.168.0...	TCP
2	0.000418	13:32:21.929235	192.168.0...	192.168.0...	TCP
3	0.000780	13:32:21.929597	192.168.0...	192.168.0...	TCP
4	0.118636	13:32:22.047453	192.168.0...	192.168.0...	TCP
5	0.118802	13:32:22.047619	192.168.0...	192.168.0...	TCP
6	0.118839	13:32:22.047656	192.168.0...	192.168.0...	TCP
7	13.536638	13:32:35.465455	192.168.0...	61.139.2...	DNS
8	13.550938	13:32:35.479755	61.139.2...	192.168.0...	DNS
9	13.606238	13:32:35.535055	192.168.0...	216.239.6...	HTTP
10	13.827018	13:32:35.755835	216.239.6...	192.168.0...	HTTP
11	13.827304	13:32:35.756121	192.168.0...	216.239.6...	HTTP
12	13.827658	13:32:35.756475	192.168.0...	216.239.6...	HTTP
13	14.055133	13:32:35.983950	216.239.6...	192.168.0...	HTTP
14	14.055671	13:32:35.984488	216.239.6...	192.168.0...	HTTP

- Right click and choose **Hide Unselected Packets** command.

No.	Relative Time	Absolute Time
1	0.000000	13:32:21.928817
2	0.000418	13:32:21.929235
3	0.000780	13:32:21.929597
4	0.118636	13:32:22.047453
5	0.118802	13:32:22.047619
6	0.118839	13:32:22.047656
7	13.536638	13:32:35.465455
8	13.550938	13:32:35.479755
9	13.606238	13:32:35.535055
10	13.827018	13:32:35.755835
11	13.827304	13:32:35.756121
12	13.827658	13:32:35.756475
13	14.055133	13:32:35.983950
14	14.055671	13:32:35.984488


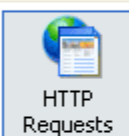



Send Packet...
 Find... Ctrl+F
 Make Filter...
 Address Resolve
 Set Relative Packet
 Add to Name Table
 Locate Explorer Node
 Select Related Packets
 Hide Selected Packets
Hide Unselected Packets
 Unhide All Packets
 Select All Ctrl+A
 Refresh F5

- Packets listed here are all related packet.

Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports					
					Packets: 690
No.	Relative Time	Absolute Time	Source	Destination	Protocol
4	0.000000	13:32:22.047453	192.168.0...	192.168.0...	TCP
5	0.000166	13:32:22.047619	192.168.0...	192.168.0...	TCP
6	0.000203	13:32:22.047656	192.168.0...	192.168.0...	TCP
8	13.432302	13:32:35.479755	61.139.2...	192.168.0...	DNS
10	13.708382	13:32:35.755835	216.239.6...	192.168.0...	HTTP
13	13.936497	13:32:35.983950	216.239.6...	192.168.0...	HTTP
14	13.937035	13:32:35.984488	216.239.6...	192.168.0...	HTTP
15	13.956738	13:32:36.004191	216.239.6...	192.168.0...	HTTP
17	13.976572	13:32:36.024025	61.139.2...	192.168.0...	DNS
19	14.090583	13:32:36.138036	64.233.18...	192.168.0...	HTTP
24	14.174682	13:32:36.222135	61.139.2...	192.168.0...	DNS
26	14.212673	13:32:36.260126	64.233.18...	192.168.0...	HTTP
27	14.213275	13:32:36.260728	64.233.18...	192.168.0...	HTTP
28	14.224616	13:32:36.272069	125.91.10...	192.168.0...	TCP

Logs view

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

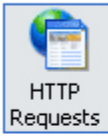



Summary Diagnoses Endpoints Protocols Conversations Matrix Logs Graphs Reports						
						Logs: 76
Log type	Time	Client	Requested URL	Met...	User Agent	Status...
Logs  HTTP Requests  Email Messages  FTP Transfers  DNS Analysis	13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://www.google.com/	GET	Mozilla/4.0 ...	200
	13:1...	192.168.0...	http://www.google.com/in...	GET	Mozilla/4.0 ...	304
	13:4...	192.168.0...	http://www.lycows.com/	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://toolbarqueries.qoo...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://data.alexa.com/dat...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://www.lycows.com/m...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200
	13:4...	192.168.0...	http://www.lycows.com/i...	GET	Mozilla/4.0 ...	200

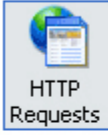


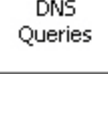
- **HTTP Requests** - presents the information of captured web accesses, you can open a listed URL with double clicks.

- **Email Messages** - shows the captured email messages transmitted in plain text, email list and related information.
- **FTP Transfers** - reveals the detailed records of FTP uploads and downloads.
- **DNS Analysis** - shows the details of DNS analysis results.
- **MSN Activity view** - offers the records of MSN activities.
- **AIM Activity view** - offers the records of AIM activities.
- **ICQ Activity view** - offers the records of ICQ activities.
- **Yahoo Messenger Activity view** - offers the records of Yahoo Messenger activities.

❖ Open URLs

You can open a URL with double clicks.

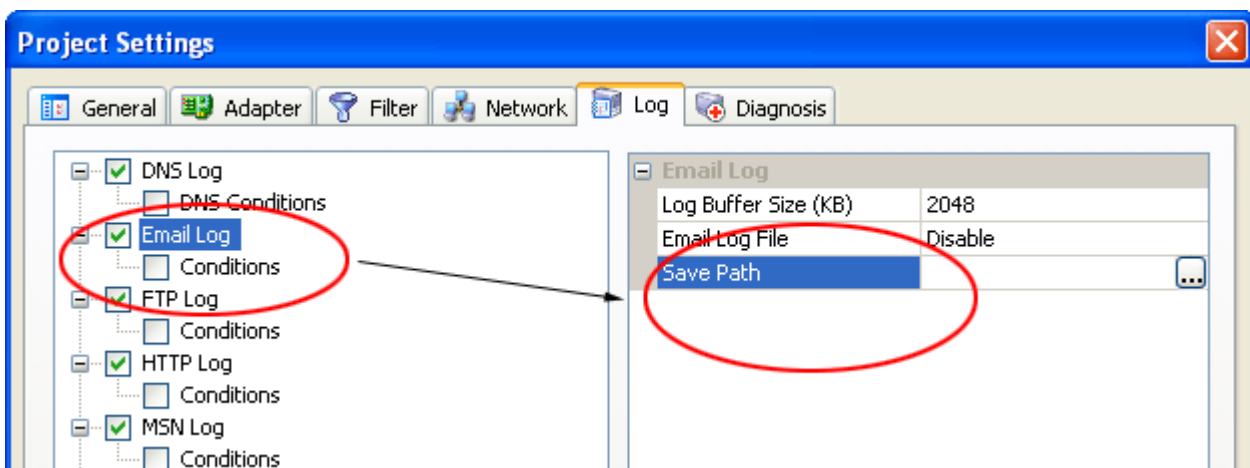
Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports						
HTTP Requests						Logs: 46
Logs	Time	Client	Requested URL	Method	Status ...	
 HTTP Requests  Email Messages  FTP Transfers  DNS Queries	17:15:48	192.168...	http://www.google.com/	GET	302	6
	17:15:48	192.168...	http://www.google.com/intl/zh-CN/	GET	200	6
	17:15:49	192.168...	http://data.alexa.com/data/mOse41ubZPQ...	GET	200	2
	17:16:02	192.168...	http://www.colasoft.com/	GET	200	6
	17:16:03	192.168...	http://www.colasoft.com/pub/js/cbe_core.js	GET	200	6
	17:16:03	192.168...	http://data.alexa.com/data/mOse41ubZPQ...	GET	200	2
	17:16:10	192.168...	http://www.colasoft.com/pub/js/cbe_event.js	GET	200	6
	17:16:11	192.168...	http://www.colasoft.com/pub/js/cbe_util.js	GET	200	6
	17:16:12	192.168...	http://www.colasoft.com/pub/js/cs_menu ...	GET	200	6
	17:16:13	192.168...	http://www.google-analytics.com/urchin.js	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/menu_on0...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/menu_off...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/pub/css/colasoftw...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/Chinese.gif	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/colasoft_l...	GET	200	6

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports						
HTTP Requests						Logs: 46
Logs	Time	Client	Requested URL	Method	Status ...	
 HTTP Requests  Email Messages  FTP Transfers  DNS Queries	17:15:48	192.168...	http://www.google.com/	GET	302	6
	17:15:48	192.168...	http://www.google.com/intl/zh-CN/	GET	200	6
	17:15:49	192.168...	http://data.alexa.com/data/mOse41ubZPQ...	GET	200	2
	17:16:02	192.168...	http://www.colasoft.com/	GET	200	6
	17:16:03	192.168...	http://www.colasoft.com/pub/js/cbe_core.js	GET	200	6
	17:16:03	192.168...	http://data.alexa.com/data/mOse41ubZPQ...	GET	200	2
	17:16:10	192.168...	http://www.colasoft.com/pub/js/cbe_event.js	GET	200	6
	17:16:11	192.168...	http://www.colasoft.com/pub/js/cbe_util.js	GET	200	6
	17:16:12	192.168...	http://www.colasoft.com/pub/js/cs_menu ...	GET	200	6
	17:16:13	192.168...	http://www.google-analytics.com/urchin.js	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/menu_on0...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/menu_off...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/pub/css/colasoftw...	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/Chinese.gif	GET	200	6
	17:16:13	192.168...	http://www.colasoft.com/images/colasoft_l...	GET	200	6












❖ Open Emails

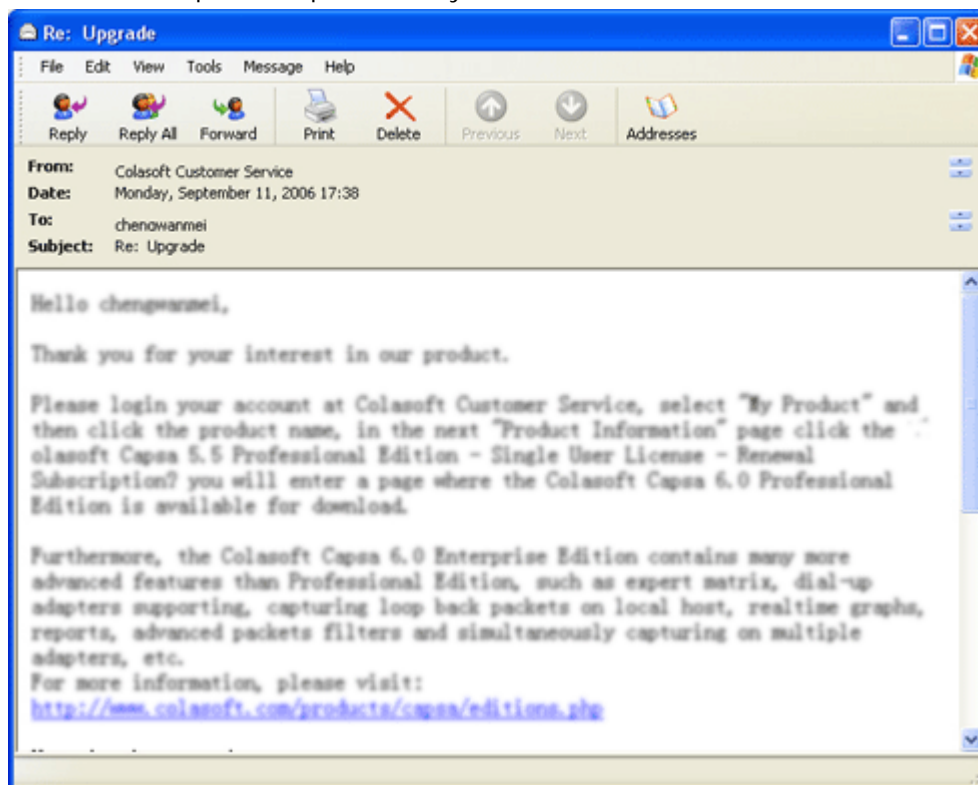
To view the reconstructed email contents, you must enable **Save Email Contents** in the Logs page of **Project Settings** dialog before capture emails.



- Select the email you interested in and double click.

Summary Diagnoses Endpoints Protocols Conversations Matrix Packets Logs Graphs Reports						
 Email Messages     <div>Logs: 22</div>						
Logs	Date	Time	Client	Server	Sender Name	
 HTTP Requests  Email Messages  FTP Transfers  DNS Queries	2006-09-11	17:22:38	192.168.0.28:2731	67.15.229.157:smtp	Colasoft Cust	
	2006-09-11	17:22:41	192.168.0.28:2733	67.15.229.157:pop3	Colasoft Cust	
	2006-09-11	17:22:42	192.168.0.28:2733	67.15.229.157:pop3	Colasoft Cust	
	2006-09-11	17:32:20	192.168.0.28:2750	220.181.12.16:smtp	Smith	
	2006-09-11	17:32:50	192.168.0.28:2752	220.181.12.16:smtp	Smith	
	2006-09-11	17:32:56	192.168.0.28:2754	220.181.12.101:pop3	Cathryn Anay.	
	2006-09-11	17:32:57	192.168.0.28:2754	220.181.12.101:pop3	Gregorio	
	2006-09-11	17:32:57	192.168.0.28:2754	220.181.12.101:pop3	Elmo Mcdaniel	
	2006-09-11	17:32:58	192.168.0.28:2754	220.181.12.101:pop3	Rod Lowery	
	2006-09-11	17:32:58	192.168.0.28:2754	220.181.12.101:pop3	Zelma Pelletier	
	2006-09-11	17:32:58	192.168.0.28:2754	220.181.12.101:pop3	Joyce Kerns	
	2006-09-11	17:32:59	192.168.0.28:2754	220.181.12.101:pop3	Jenna Key	
	2006-09-11	17:32:59	192.168.0.28:2754	220.181.12.101:pop3	clarence drozc	
	2006-09-11	17:35:36	192.168.0.28:2758	67.15.229.157:pop3	Smith	
	2006-09-11	17:38:57	192.168.0.28:2762	67.15.229.157:smtp	Colasoft Cust	

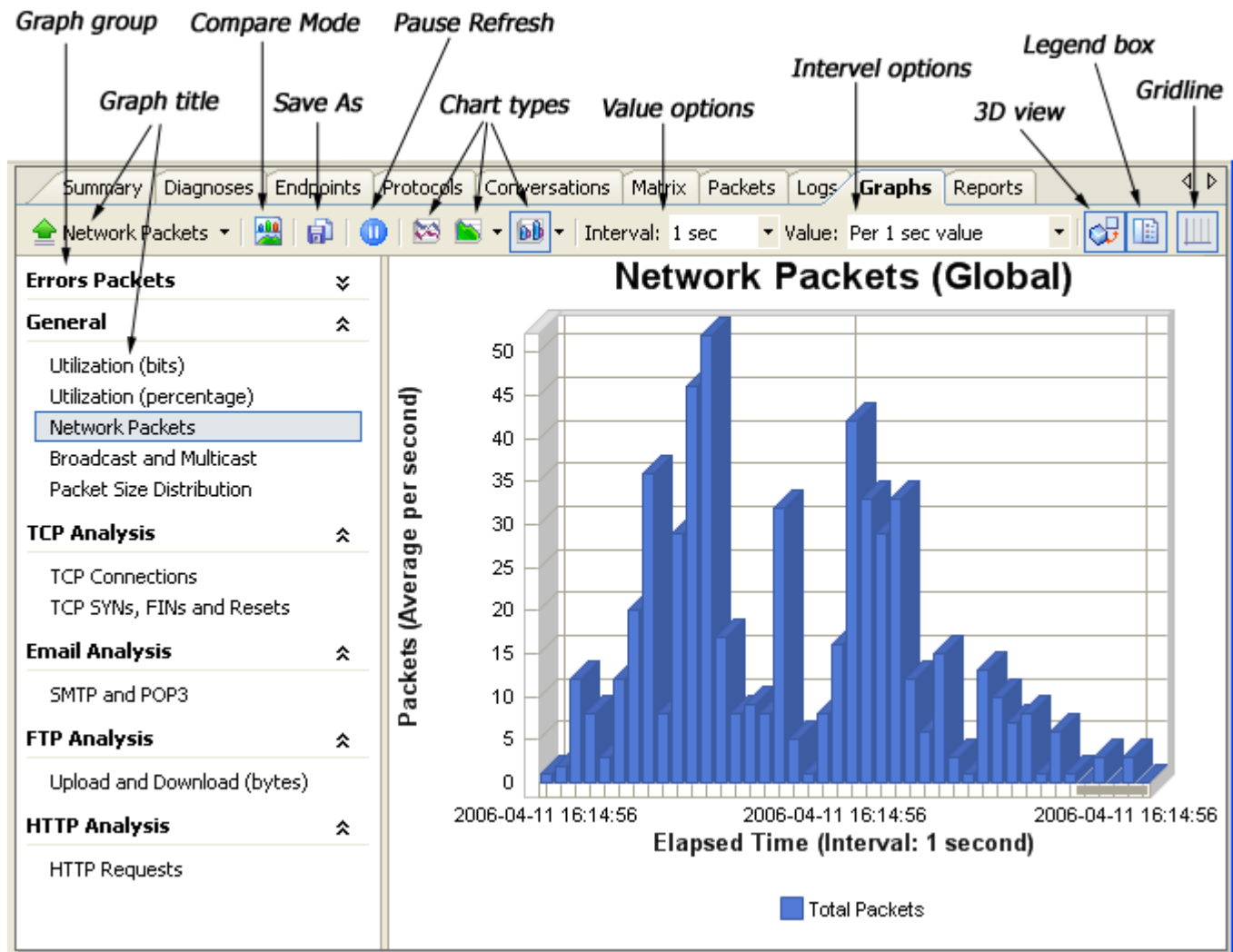
- Colasoft Capsa will open it with your email client software.



Graphs view

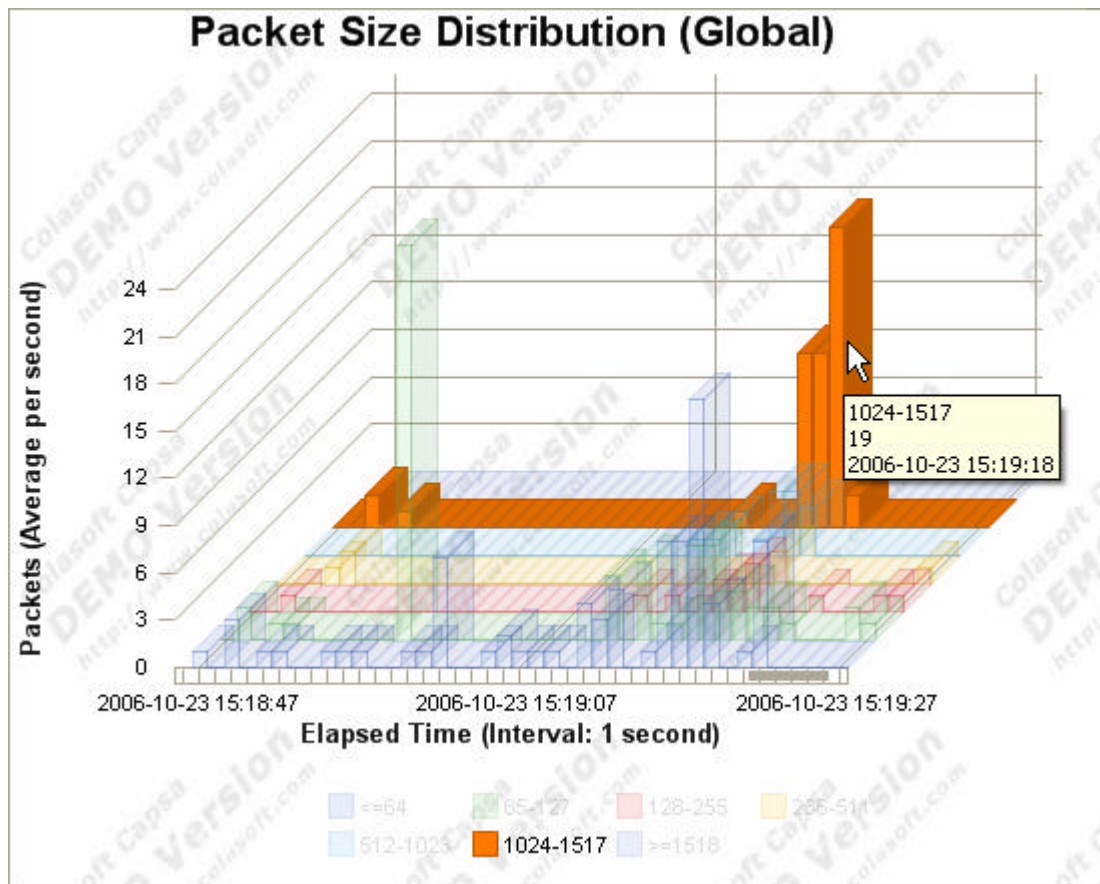
This view graphically presents the statistic data of the node you select from the **Project Explorer**

dock window. It contains a number of graph groups and multiple graph titles, including errors vs total packets, network utilization, packet size distribution, packet size details and many more.




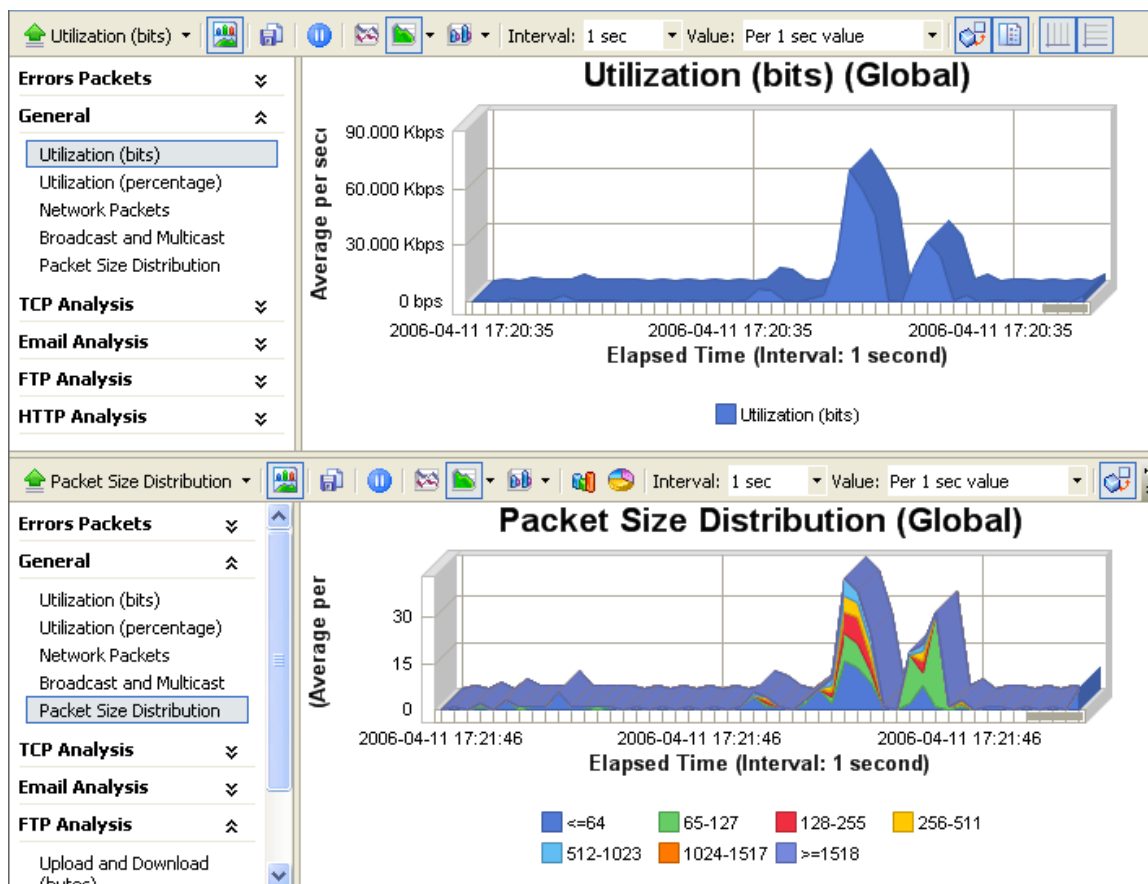
❖ Highlight an item

The highlight function in the **Graphs** view let you focus on any item displayed in graphs view. Colasoft Capsa will highlight the item and popup a description to indicate the statistic information you interested in when you push your mouse on it.



❖ Compare mode

The compare mode lets you compare two distinct graphs simultaneously in a single view. Click the icon  from the toolbar to split the display into two sections, each section has its own graph groups and display options.

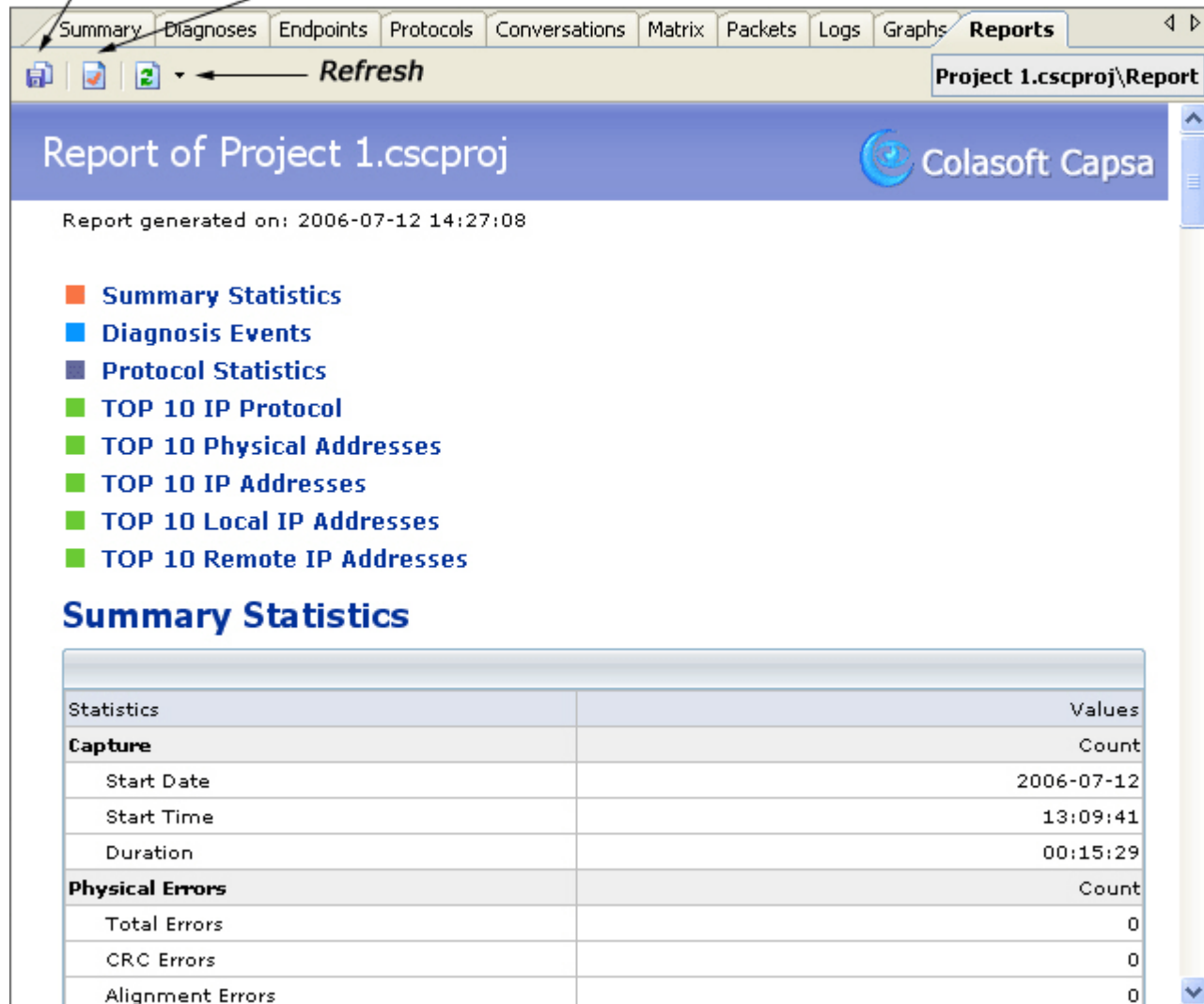


You can select a same graph title and different display value or interval value, or two graph titles with same display value and interval value.

Reports view

The reports view provides the real time reports of global network or a specific group.

Save As *Display Options*



Project 1.cscproj\Report

Report of Project 1.cscproj

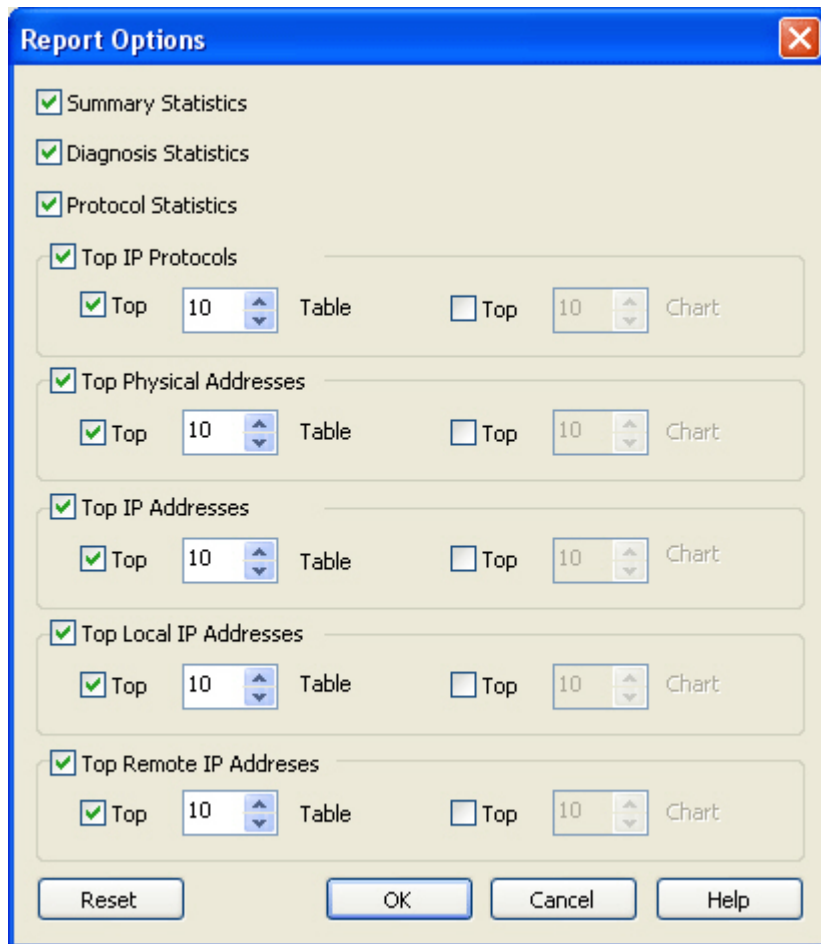
Report generated on: 2006-07-12 14:27:08

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


Summary Statistics

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

Click the  button to open the **Report Options** dialog and change the settings.

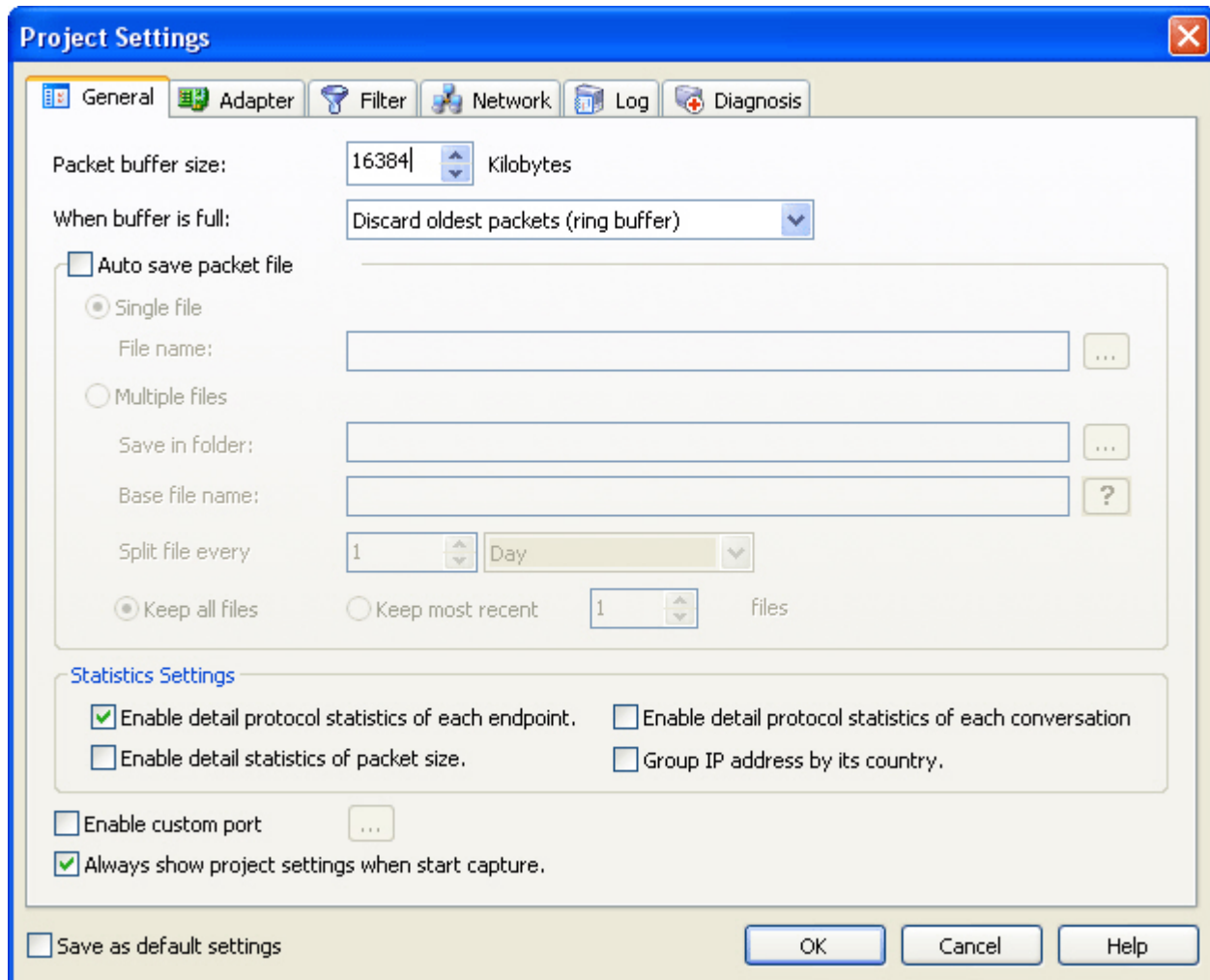


Modify Project Settings

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

General

This page provides some general project options.



- **Packet buffer size**

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

- **When buffer is full**

When the number of captured packets reaches the packet buffer size you have specified, Colasoft Capsa will do one of the following: **Discard oldest packets (ring buffer)**, **Discard new packets**, **Discard all old packets** and **Stop capture**.

- **Auto save packet file**

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

- **Statistics Settings**

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

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

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

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

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

Summary view.


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

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

- ◆ **Group IP address by its country**

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

- **Enable custom port**

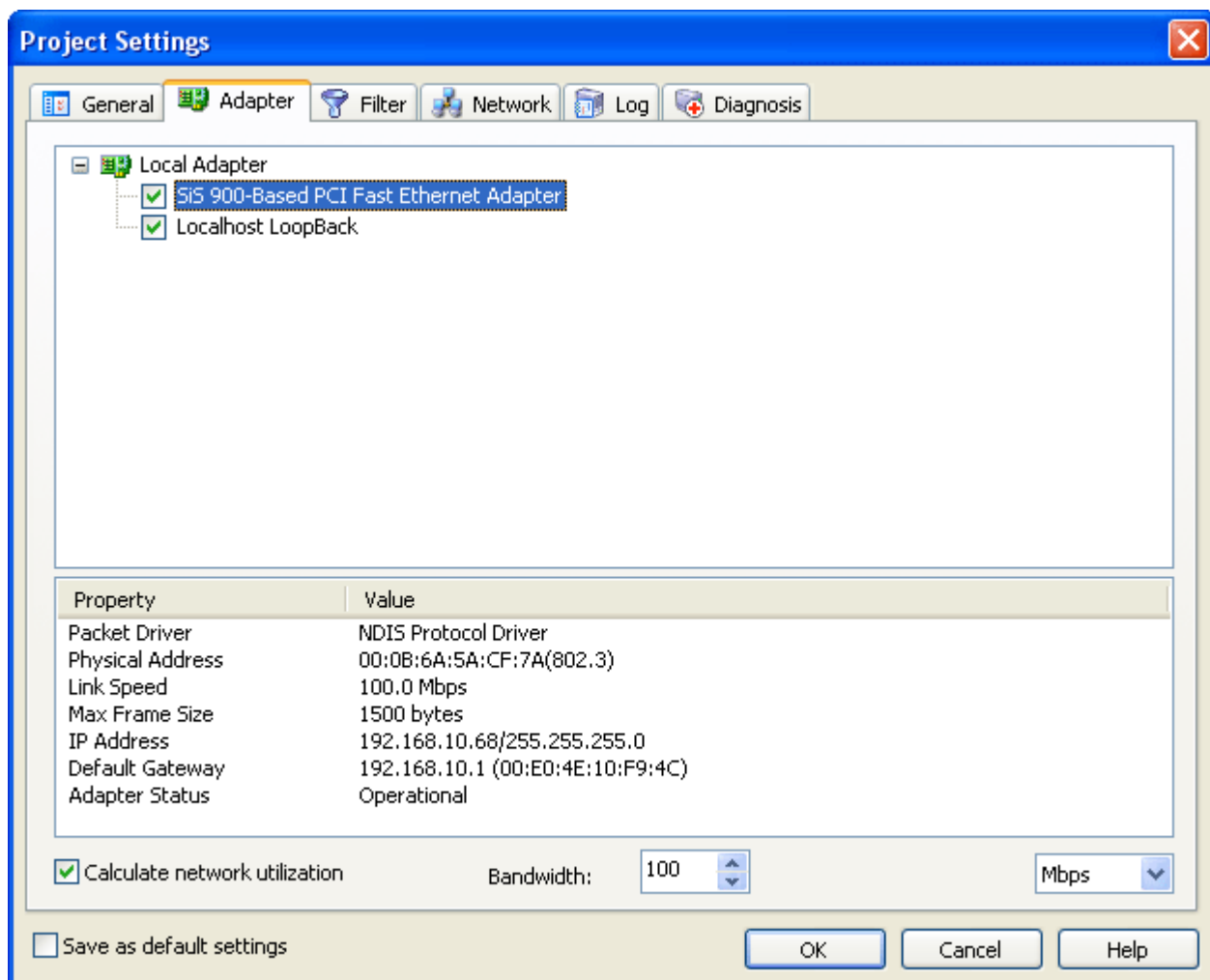
Check this option if you want Capsa to monitor non-standard ports, and then click the button  to add ports.

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

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

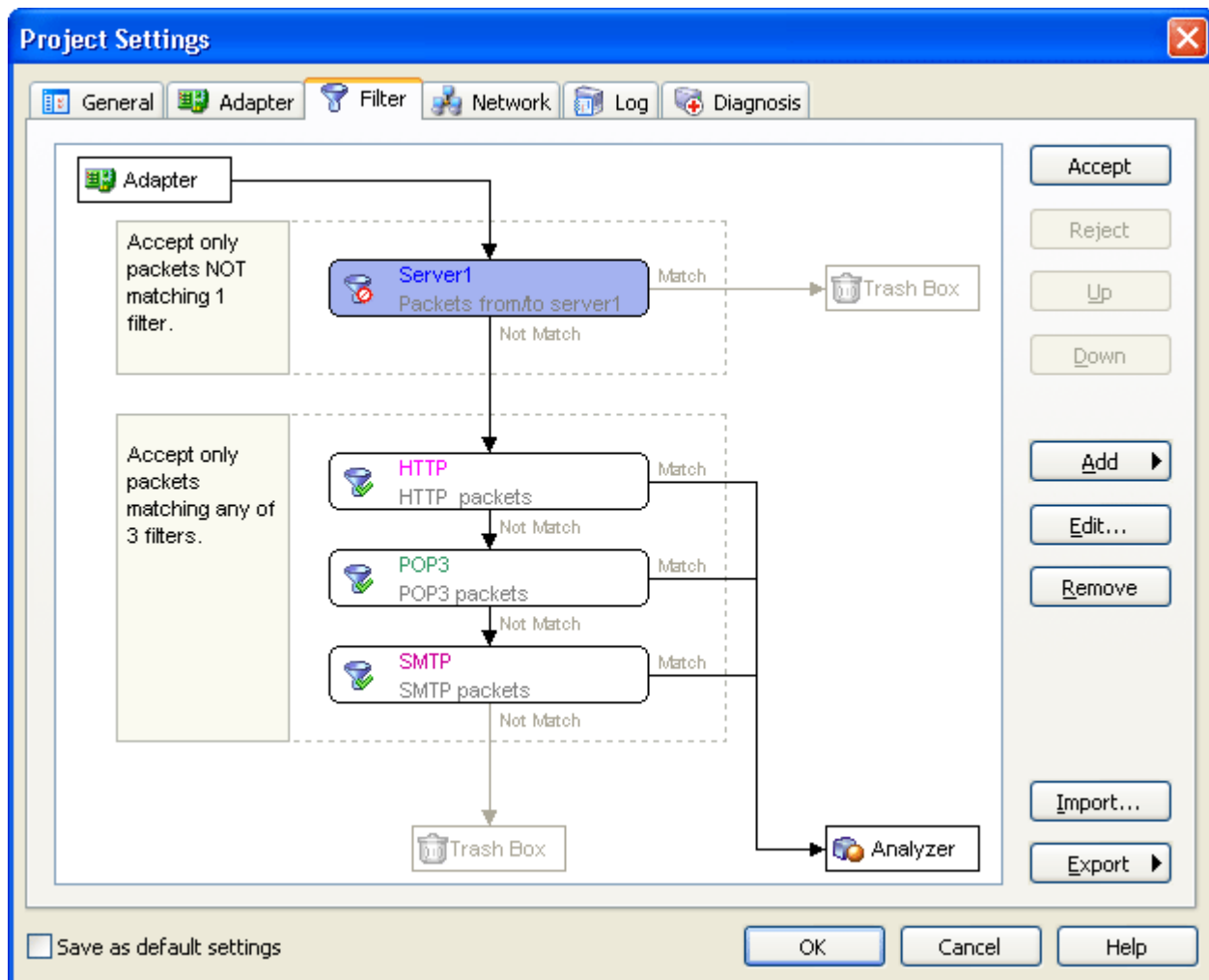
Adapter

Each time when you start a new capture, you are required to select the adapter. Available adapters are listed in the **Project Settings - Adapter** page, you can choose one or more adapters (only one adapter can be opened in the professional edition) for the current project.



Filter

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



- **Accept**

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

- **Reject**

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

- **Up**

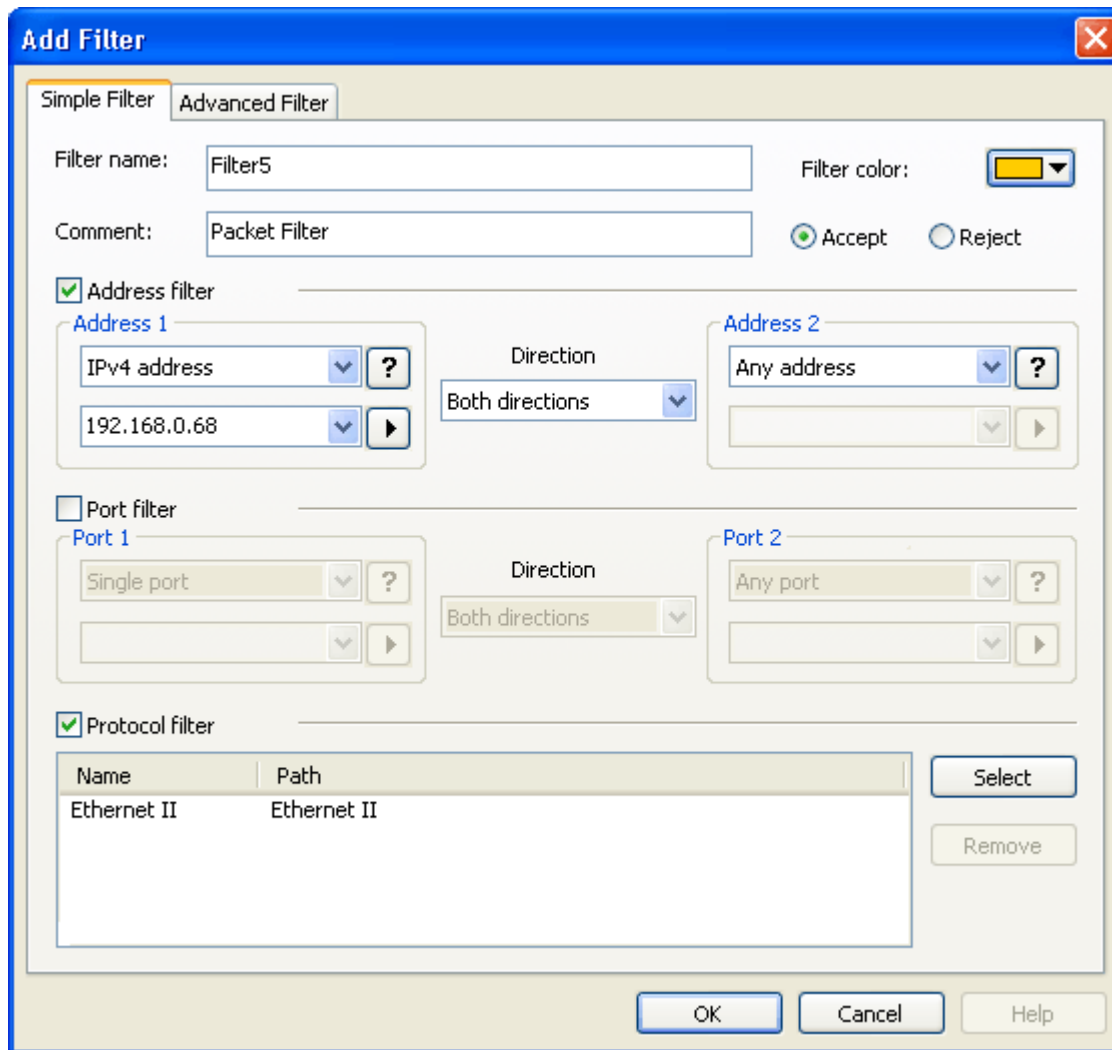
By clicking this button (if applicable), you can move up the current filter.

- **Down**

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

- **Add**

Click on this button and choose to create a new filter or add from the **Filter Table**.



The **Add Filter** dialog box has two tabs: **Simple Filter** and **Advanced Filter**. The **Advanced Filter** tab is active.

Filter name: Filter5
Filter color: [Yellow dropdown]
Comment: Packet Filter
☒ Accept ☐ Reject

☒ **Address filter**

Address 1
 IPv4 address [dropdown] [?] [?] [?]
 192.168.0.68 [dropdown] [?]
Direction: Both directions [dropdown]

Address 2
 Any address [dropdown] [?] [?] [?]
 [dropdown] [?]

☐ **Port filter**

Port 1
 Single port [dropdown] [?] [?] [?]
 [dropdown] [?]
Direction: Both directions [dropdown]

Port 2
 Any port [dropdown] [?] [?] [?]
 [dropdown] [?]

☒ **Protocol filter**

Name	Path
Ethernet II	Ethernet II

[Select] [Remove]

[OK] [Cancel] [Help]

- **Edit...**

To modify the current filter, click the **Edit...** button and open the **Modify Filter** dialog, note that the modifications made from this dialog is only project-related.

- **Remove**

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

- **Import...**

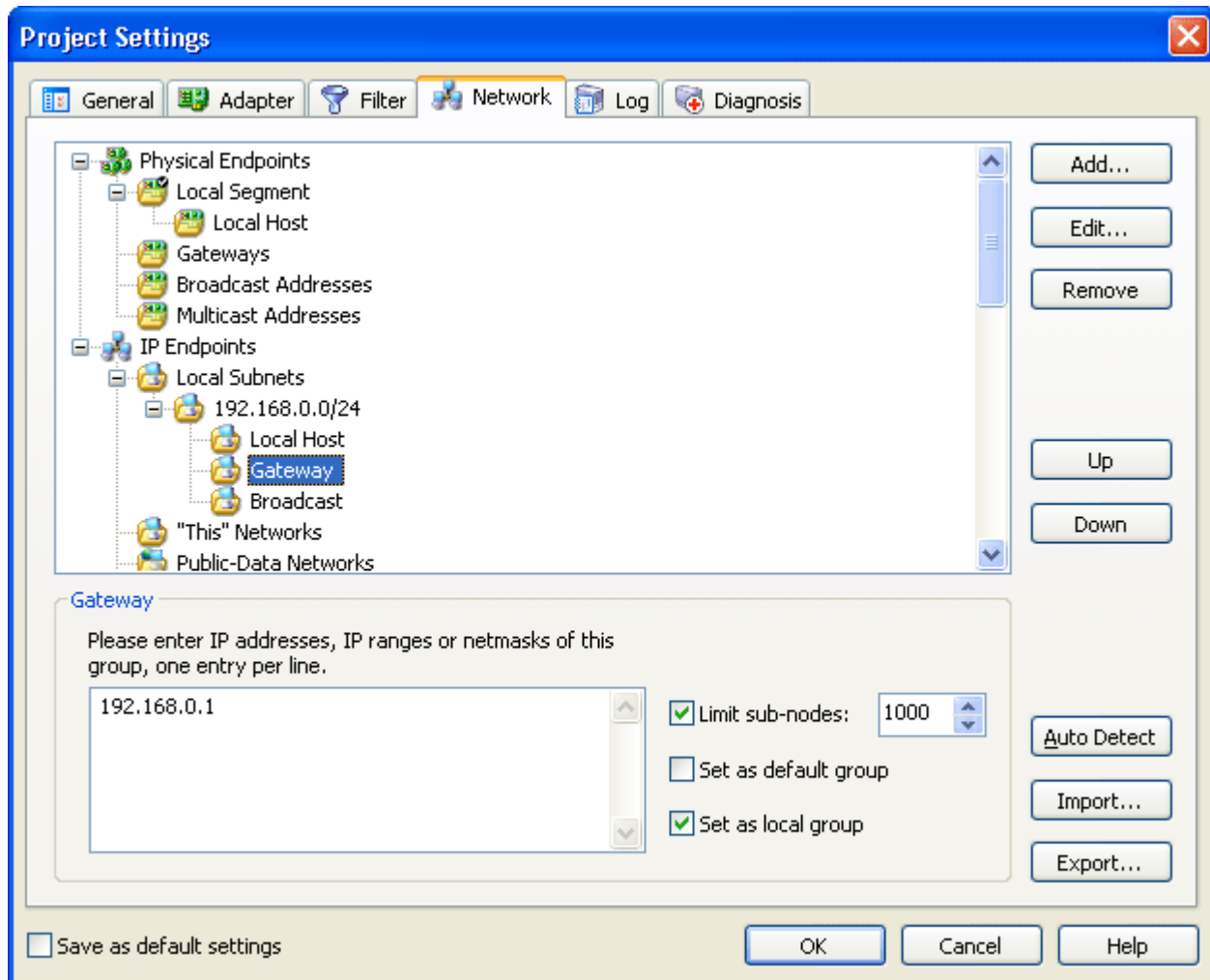
You can import filter from a saved filter file.

- **Export**

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


Network

In the **Network** page of **Project Settings**, you can customize one or more physical endpoints or IP endpoints, accordingly the network nodes in the **Project Explorer** will be reassigned or renamed.



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

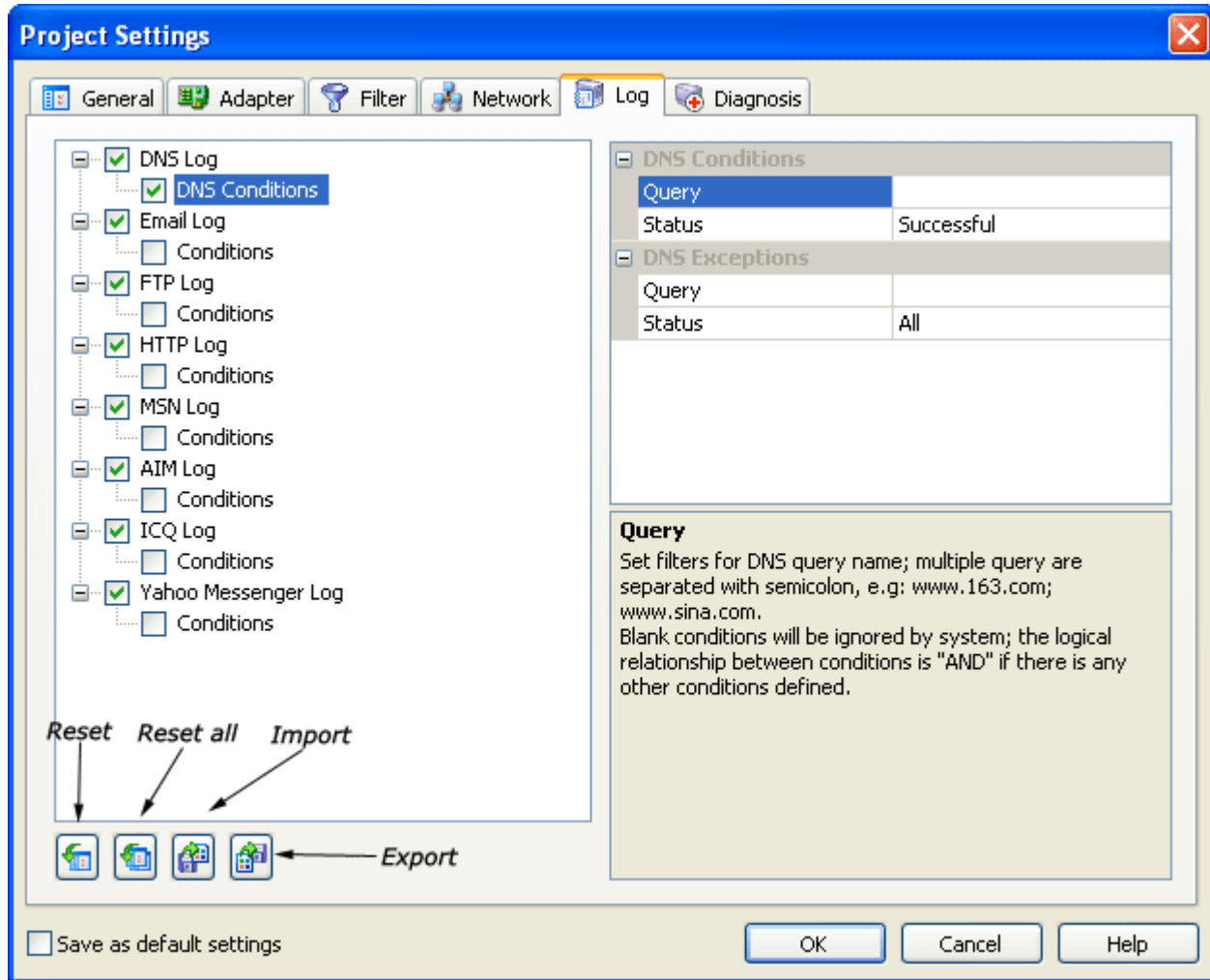
Log

In Colasoft Capsa, the analyzers are the basis of counters, logs and graphs, which provide additional highly focused analysis results for your network traffic. You can set conditions for these three kinds of log in the **Project Settings - Log** page by clicking the **Log** button  in the toolbar

DNS Log

In the setting page, you can define the DNS log's buffer size, select log file format, and set conditions for the display of DNS logs.

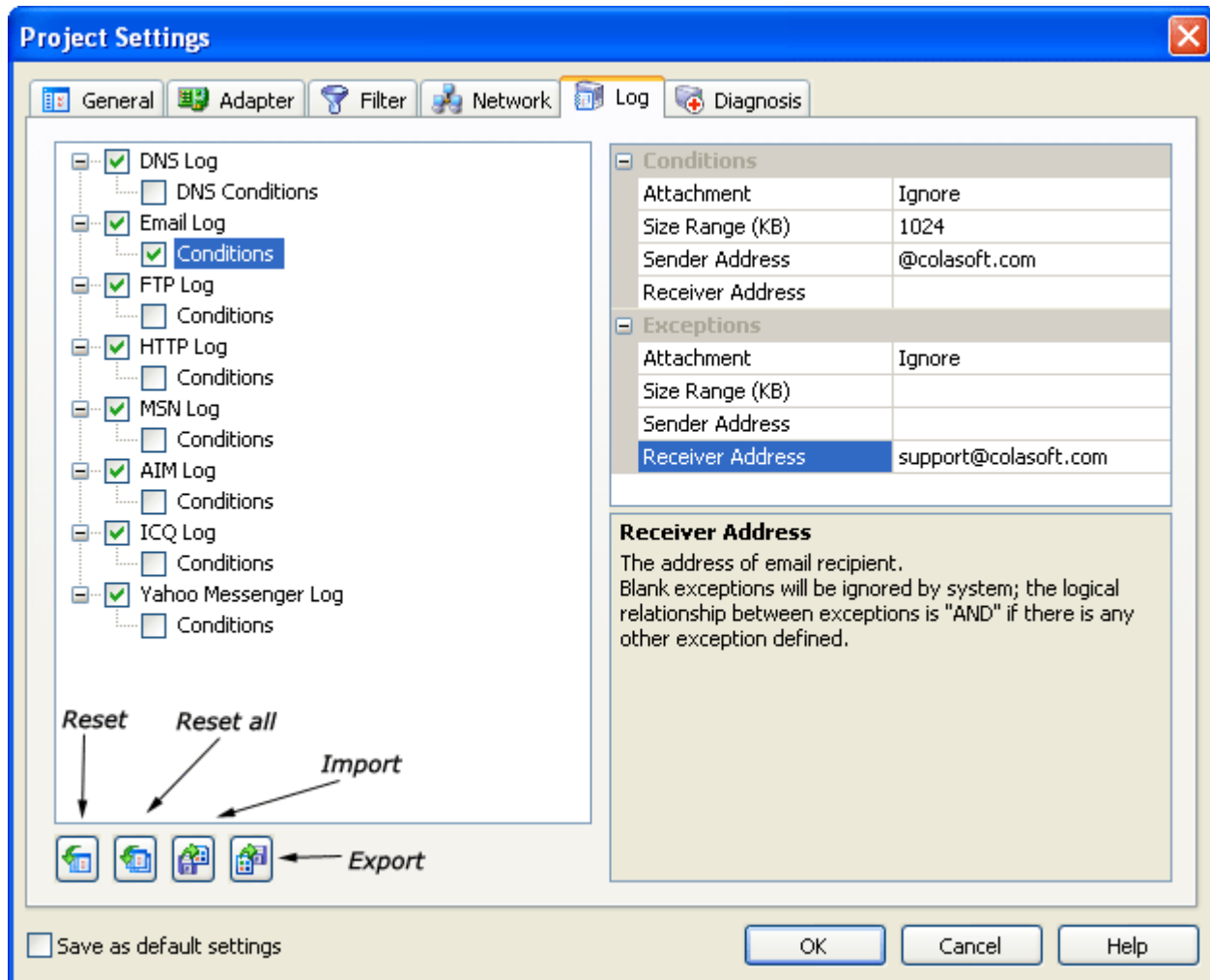
See the figures below as setting examples.



Email Log

In the setting page, you can define the email log's buffer size, select log file format, enable Colasoft Capsa to save email contents and set conditions for the display of email logs.

See the figures below as setting examples.

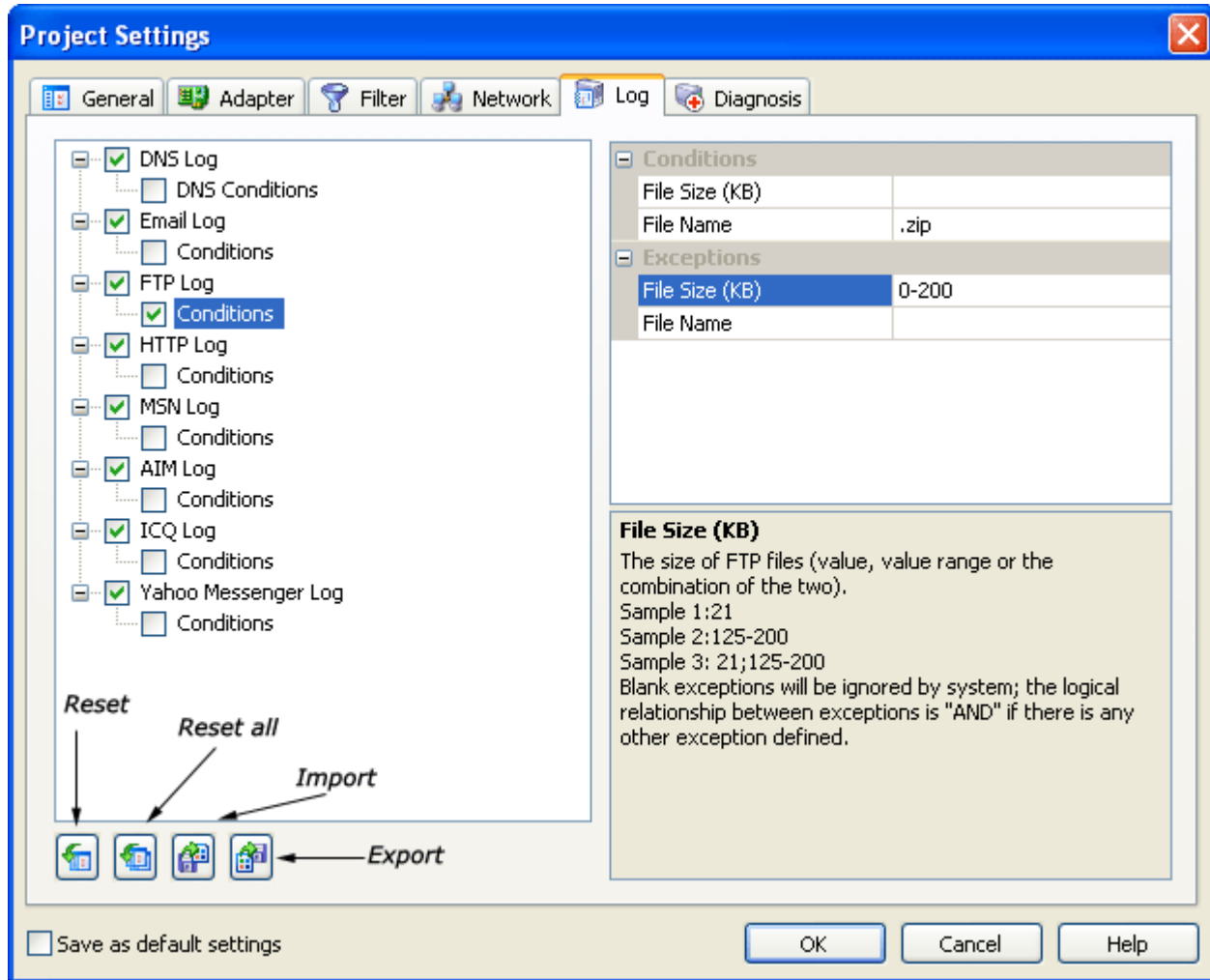


By default, the email log is enabled and the log buffer size is preset as 1024 KB. If you disable the email log, you can not see any email log information from the **Logs - Email Messages** view.

FTP Log

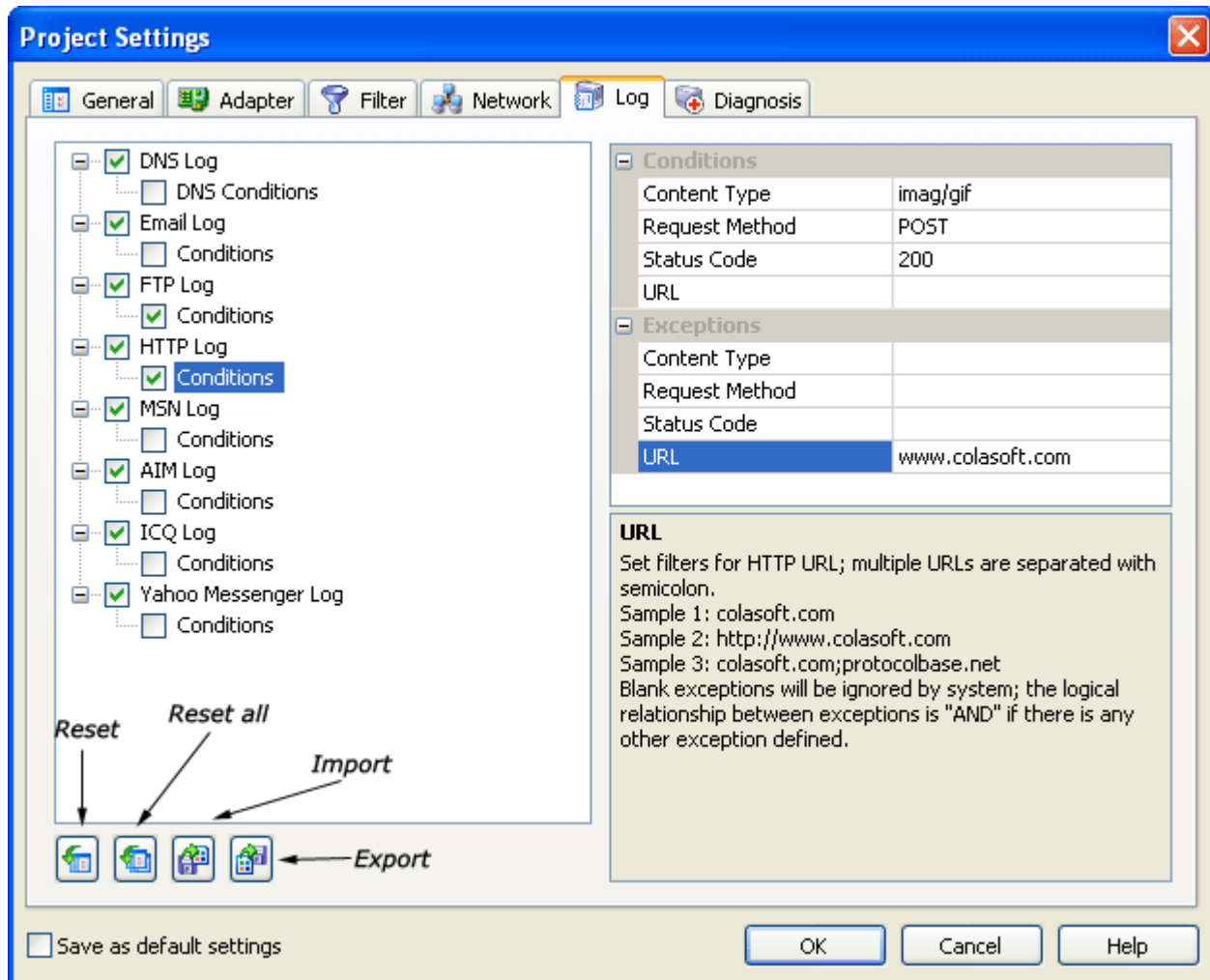
In the setting page, you can define the FTP log's buffer size, select log file format, and set conditions for the display of FTP logs.

See the figure below as setting examples.



HTTP Log

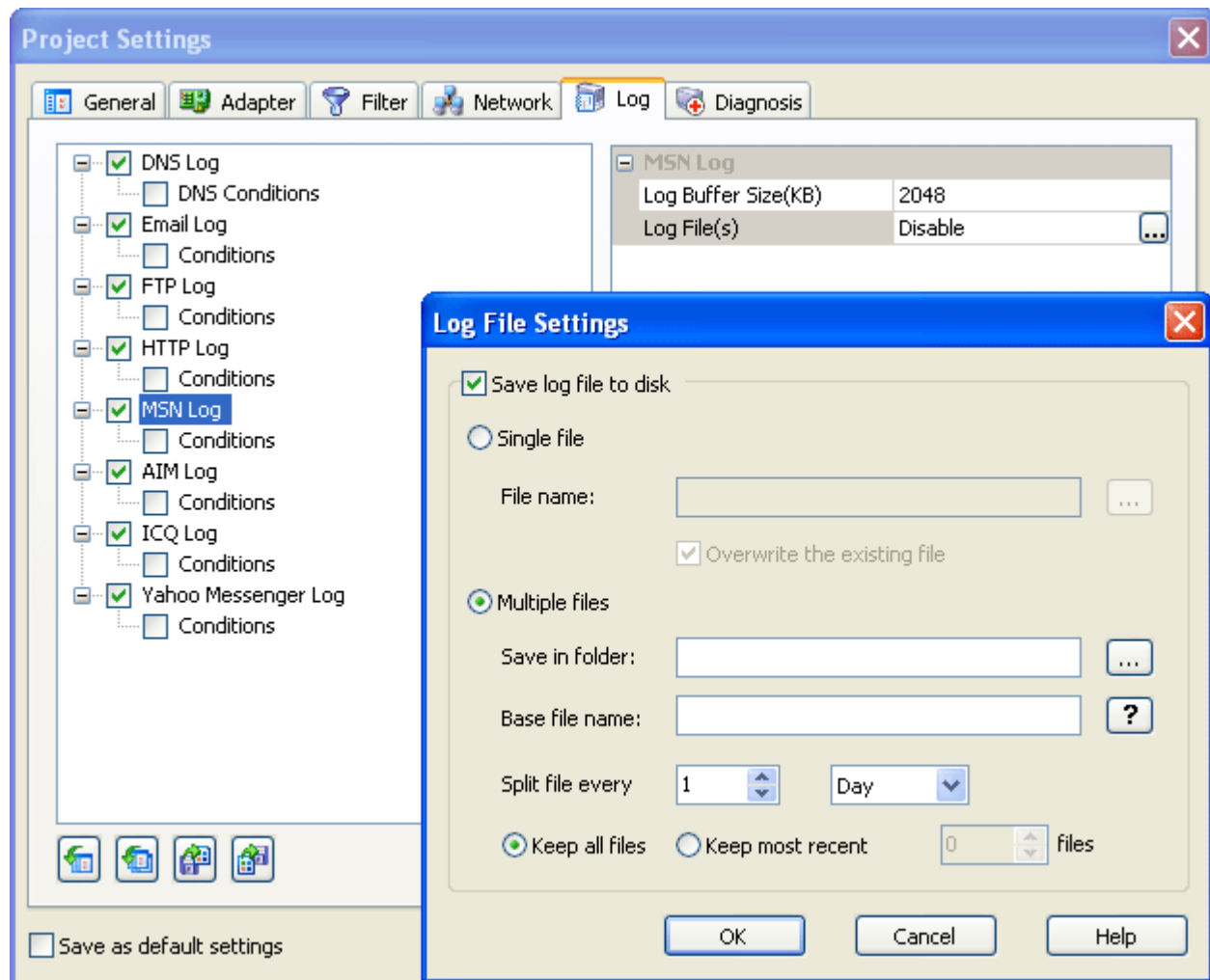
In the setting page, you can define the HTTP log's buffer size, select log file format, and set conditions for the display of HTTP logs. The settings or modifications made in this page will impact the results displayed in the **Logs - HTTP Transfers** view.



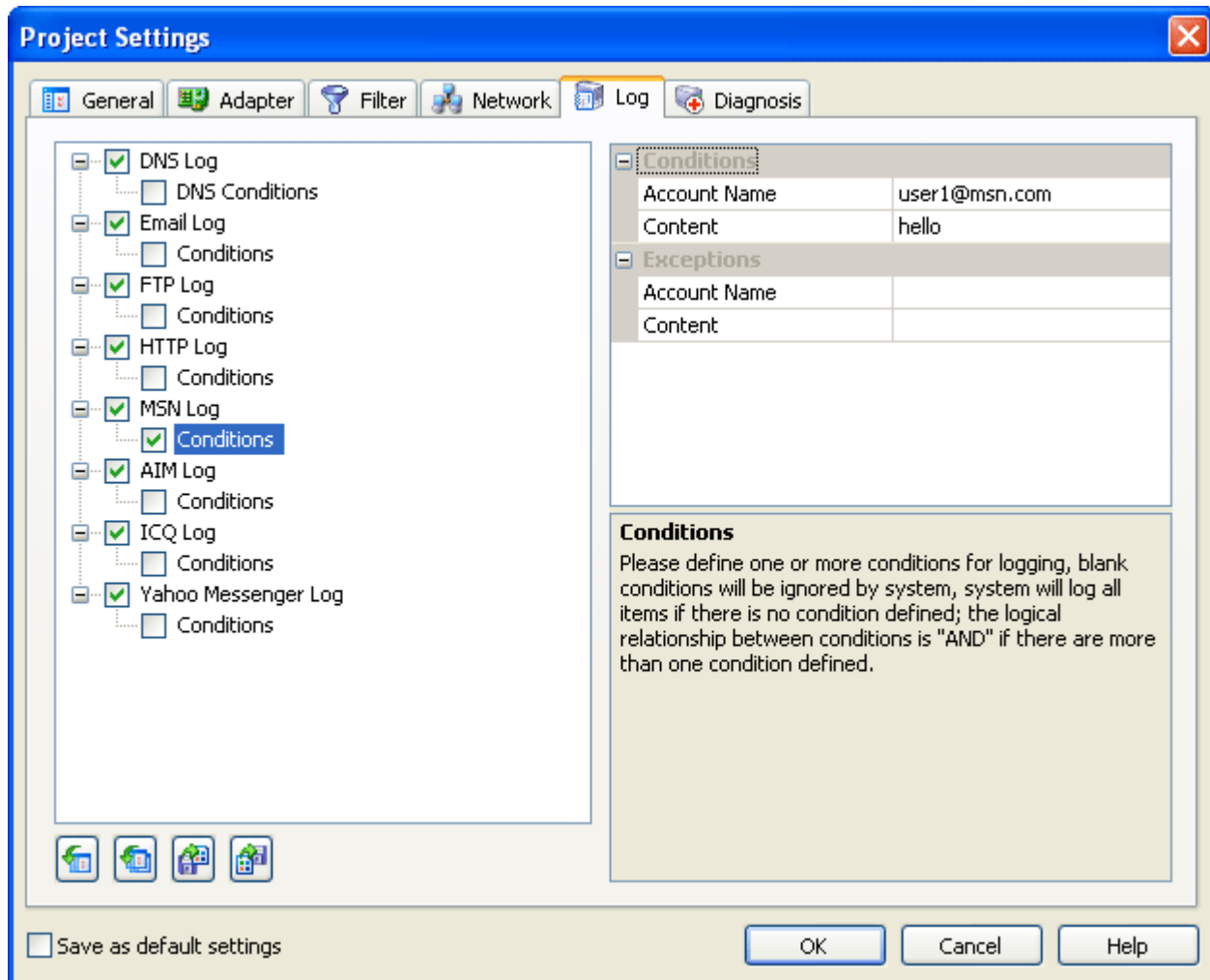
MSN Log, AIM Log, ICQ Log and Yahoo Messenger Log

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

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



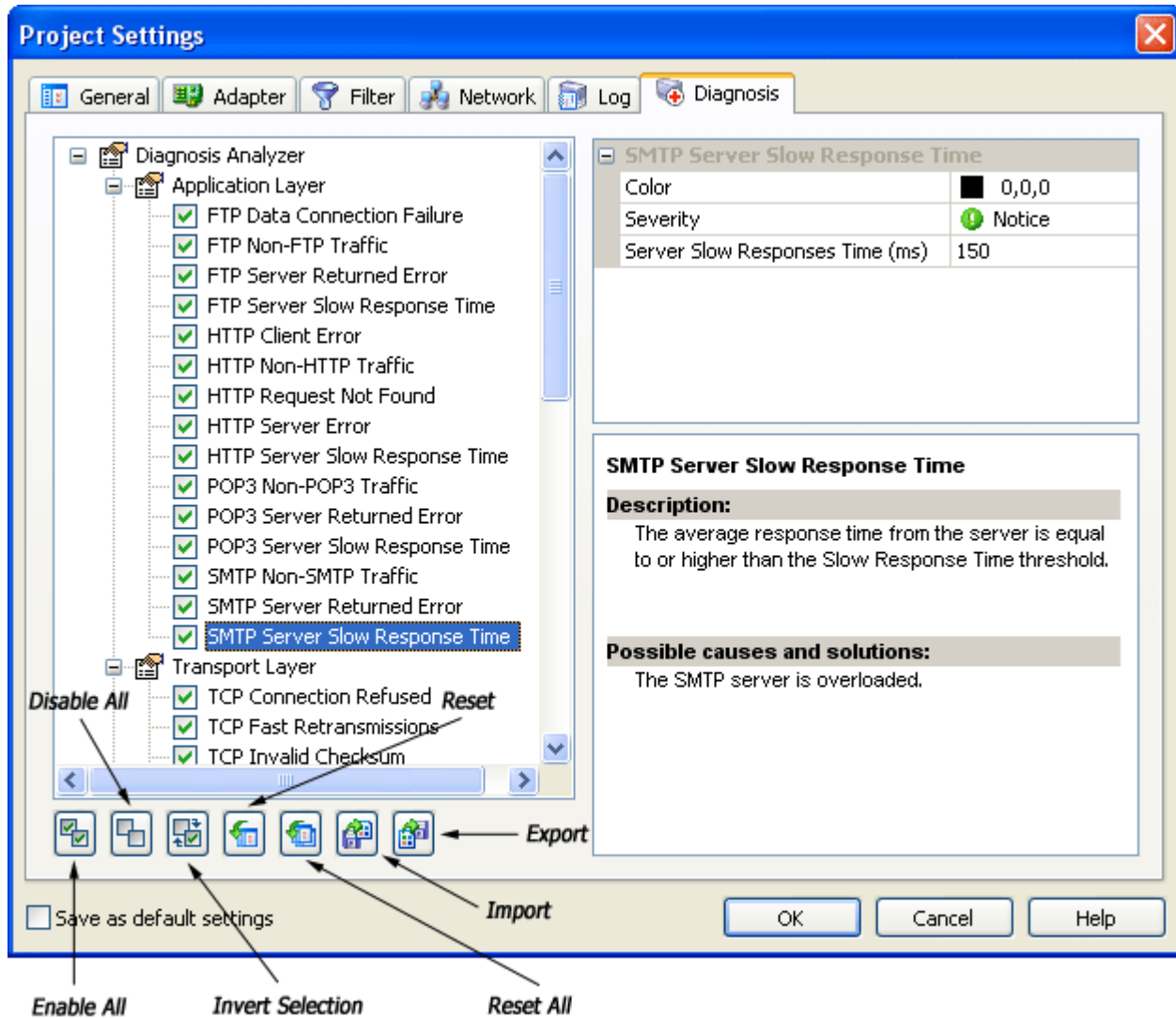
Conditions is a place where you can make settings for Account Name and Content. Blank conditions will be ignored by system; system will log all items if there is no condition defined.



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

Diagnoses

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




Data management

When your project buffer is full, Colasoft Capsa will discard some packets to keep the displayed packets up-to-date, use the assistant functions of Colasoft Capsa you can protect important packet information from being discarded.

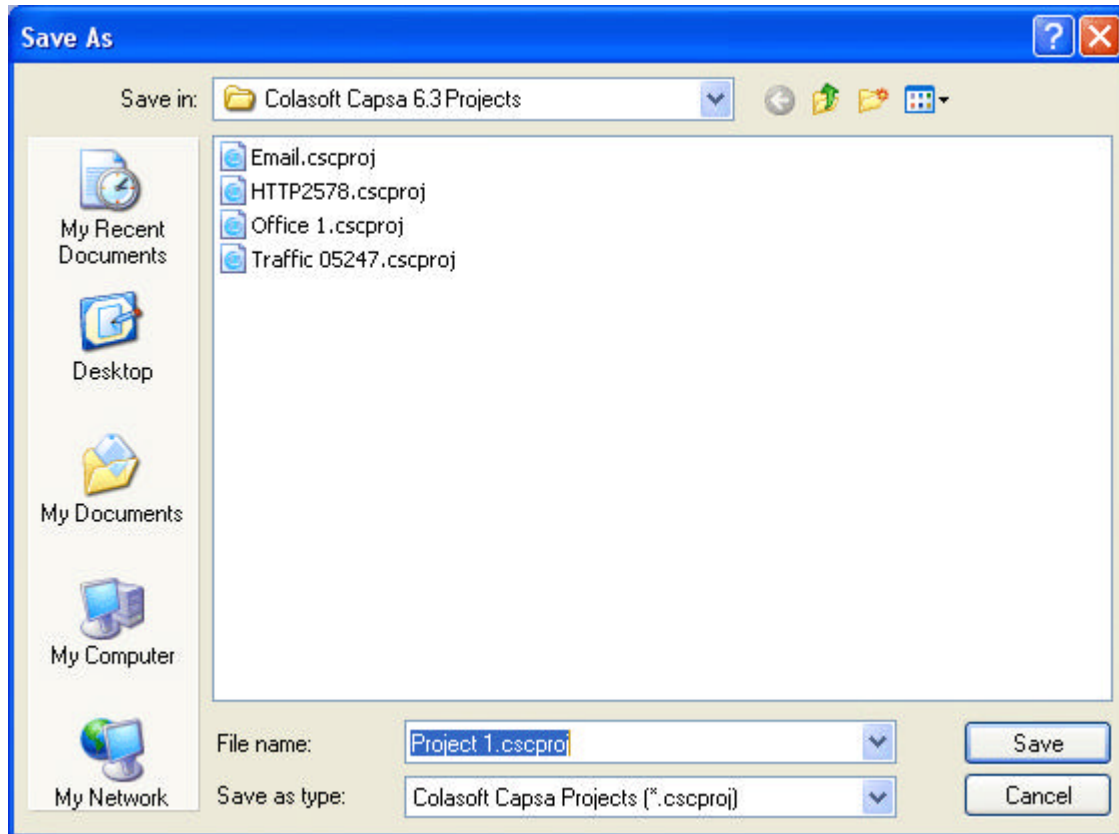
Saving

Saving a project


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

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

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



Saving project data

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

Saving as template

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

- **Save from the File menu**

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

- **Save from the Project Settings dialog**

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

Importing & exporting packet file

Import a packet file

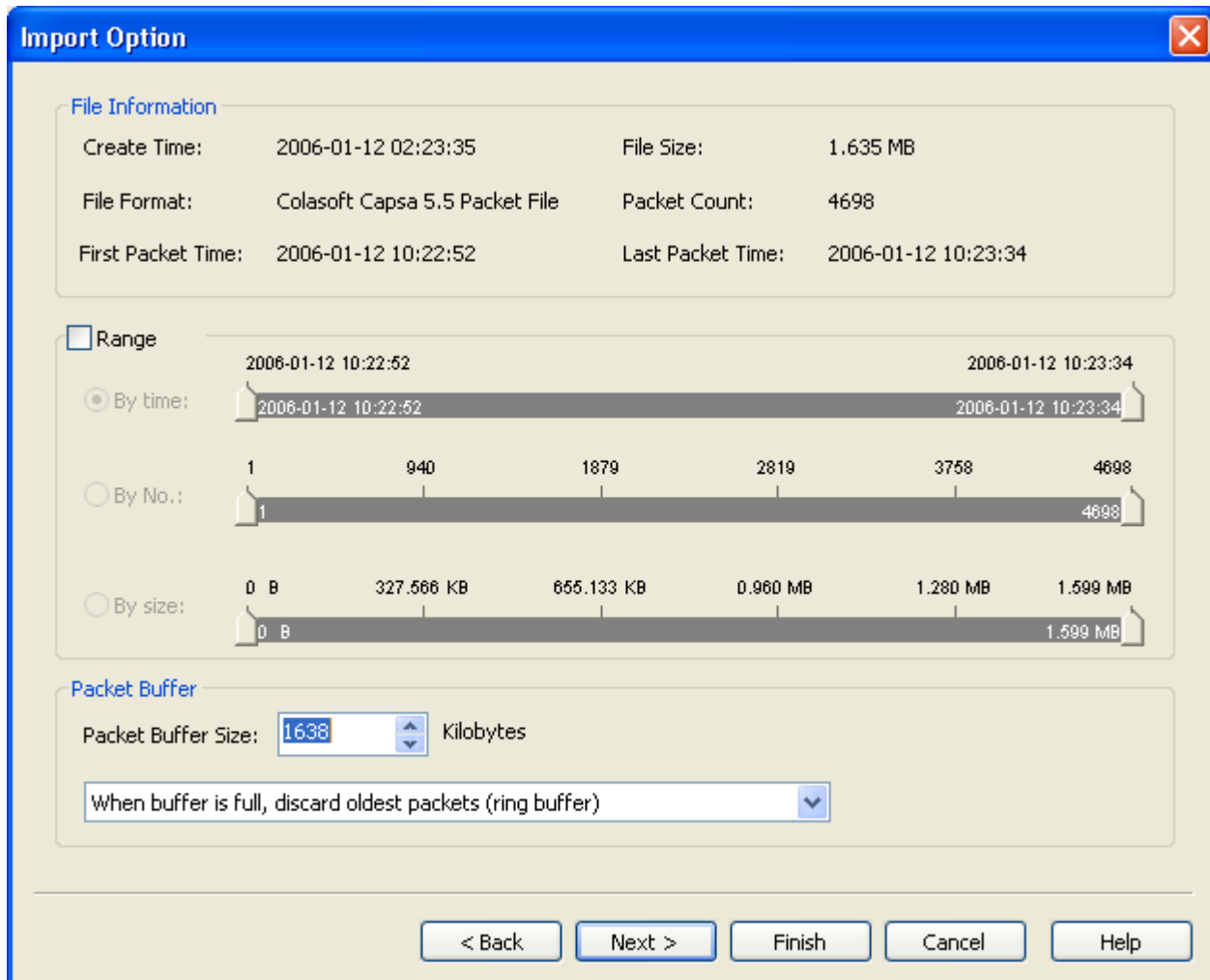
Colasoft Capsa supports the following packet file formats

- Colasoft Capsa native format (*.cscpkt)
- Colasoft Capsa previous format (*.cpf)
- Sniffer packet file format (*.cap)
- EtherPeek packet file format (*.pkt)
- TokenPeek packet file format (*.pkt)
- AiroPeek packet file format (*.pkt)
- Raw packet file format (*.rawpkt)
- Microsoft Network Monitor 2.x (*.cap)

- TCP DUMP File(*.dmp)

Import steps:

- Select **Import Packet File...** from the **File** menu.
- Specify the file name and file format.
- Customize the import options and project settings.
- The current project data will be cleared after you finish import.



Import Option

File Information

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

☐ **Range**

☒ **By time:**

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

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

☐ **By No.:**

1 940 1879 2819 3758 4698

1 4698

☐ **By size:**

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

0 B 1.599 MB

Packet Buffer

Packet Buffer Size: Kilobytes


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

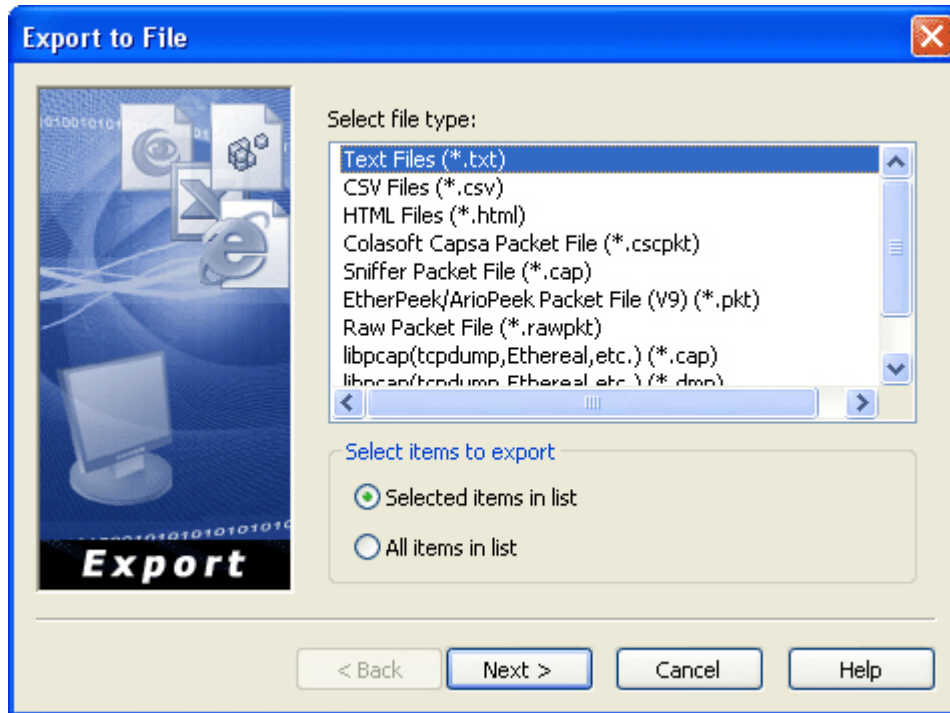
< Back Next > Finish Cancel Help

Export to a file

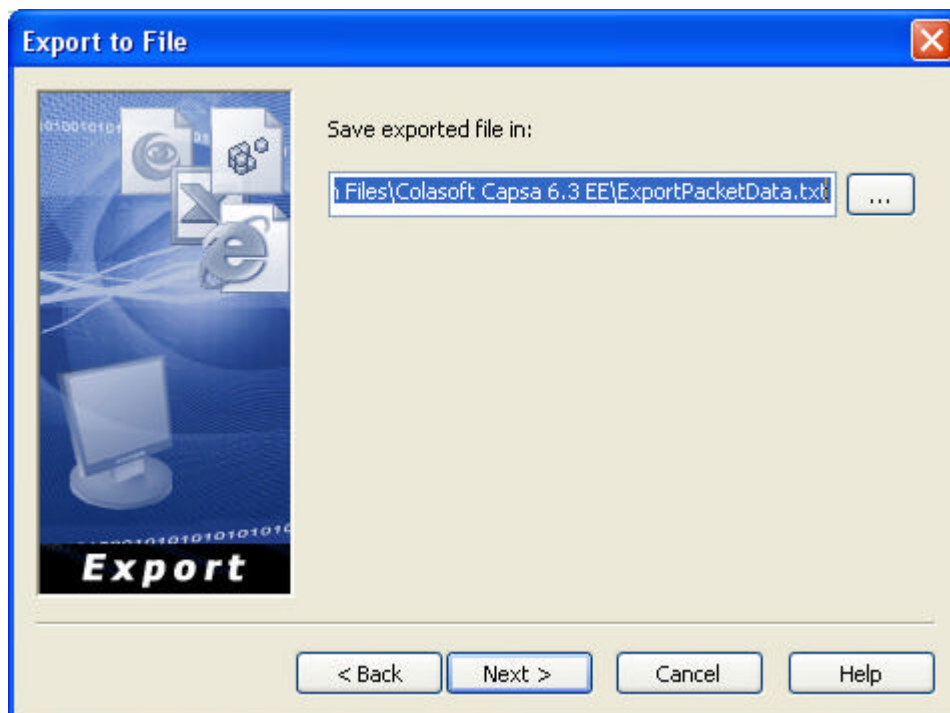
Captured packets and related information can be exported to a file in public formats such as Text and HTML. Packet list information can be exported from the **Packets** view, **Conversations** view and **Logs** view.

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

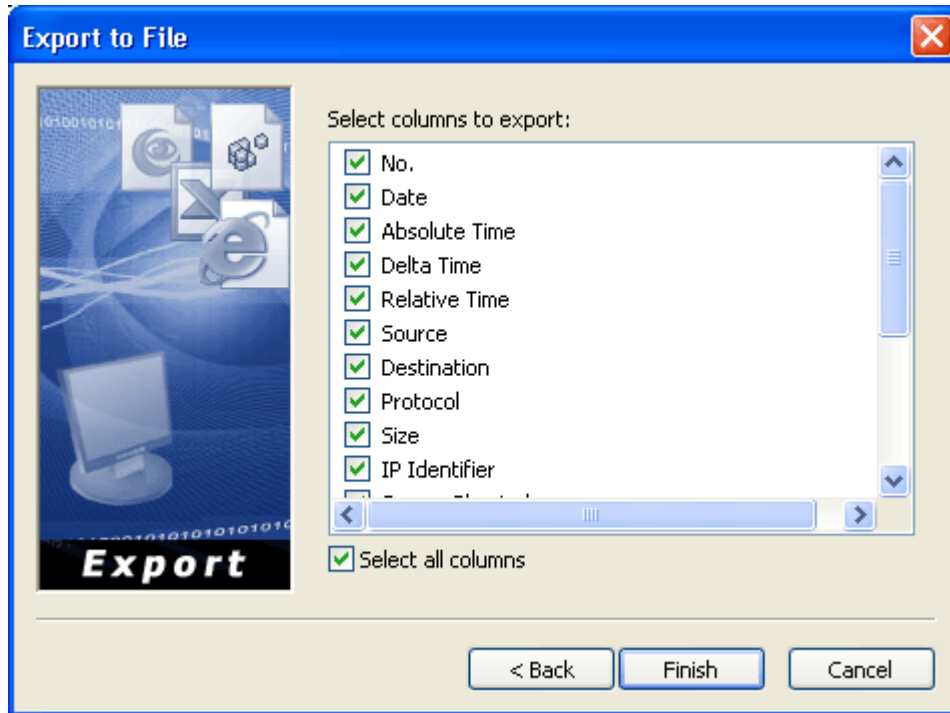
- Highlight the selected packets (use **Shift** or **Ctrl** key to select multiple items).
- Right click and select **Export Packet...**, or click the icon  from the toolbar.
- Specify the file type and items in the opened dialog.



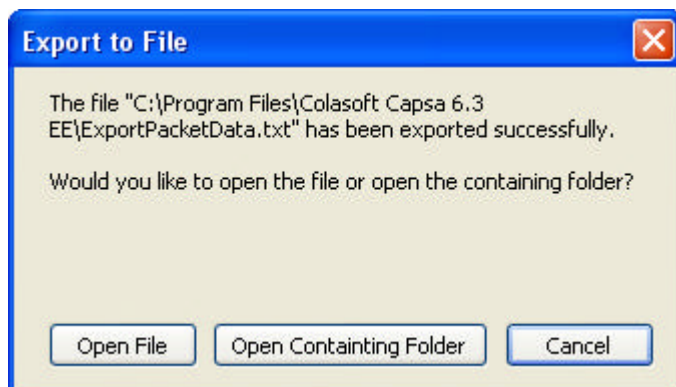
- Define the path to save the export file.




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



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



Printing

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