



Colasoft Capsa Whitepaper

This white paper is owned by Colasoft Co., Ltd. (Colasoft). No part of this white paper may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, for any purpose, without the express written permission of Colasoft.

© 2001-2008 Colasoft Co., Ltd. All rights reserved.

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

Index

Background	2
Overview	2
Design concepts and working principle	3
How to work	3
Data capture.....	3
Data analysis	4
Exporting data.....	5
Key features	5
Flexible Project Explorer	5
Reports.....	6
Matrix	6
Expert network diagnosis	6
Packet filters.....	6
Packet decoding.....	6
TCP stream reconstruction.....	7
Log analysis	7
Summary statistics.....	7
Statistic views	7
Operating multiple projects and multiple adapters	7
Technical Indicators	7
System Requirements.....	7
Supported Protocols.....	8
Decoding Protocols	9
Supported Networks	10
Capture Resources.....	11
Supported Packet File Formats.....	11
Log Analysis.....	11
TCP Stream Reconstruction Formats.....	11
Real-time decoding and analysis.....	11
Timestamp.....	12
Network Monitoring	12
Notes	12

Background

The rapid popularization and wide application of network, including various E-Commerce, E-Government, network office and other uses of modern information, offers opportunities of faster development to enterprises. However, while people are enjoying convenience and profits brought by network, they also have to be suffering its low efficiency, troubles and even breakdown, which may cause damages to enterprises/organizations' operation and result in incalculable loss.

As security management and performance maintenance is becoming more and more important, network engineers and administrators are facing the problems on how to improving network speed and efficiency. But on the other hand, due to network infrastructure being more complex and network technology developing amazingly quickly, it is more difficult than ever before to implement network maintenance and network arrangement. A good network tool, like Colasoft Capsa, can help administrators to be troubleshooting expert, find and solve network problems when problems are occurring.

Overview

With the abilities of data collecting, packet decoding and analysis, statistics, reports, logs and graphs, Colasoft Capsa makes your network transparent in the presence of you. It can help network administrators to fulfill safety management, network maintenance, network debugging, protocol analysis, performance optimization, replay network operation and so on. Network administrators can quickly locate network bottle-neck or attack with the real-time monitoring, packet decoding and data display, With Colasoft Capsa you can:

- Analyze non-normal traffic
- Analyze the mock IP and spoofed MAC address attack
- Analyze tiny fragment attack and buffer overflow attack
- Analyze DOS/DDOS/DRDOS attack
- Analyze TCP conversations in network
- Analyze whether emails transmission is normal in network
- Analyze whether FTP transfers is normal in network
- Identify the Broadcast/Multicast storm
- Identify the packets transmitted in network is correct or not
- Identify network troubleshoots
- Identify the access of My Network Place is correct or not
- Detect the circuit breakdown in network
- Detect worms attack in network
- Detect the PC infected virus
- Analyze and locate what result in network slow down
- Analyze and locate what cause network intermittence
- Analyze and locate why users can not access internet
- Detect the executions of scan and scan attacks
- Detect the password attacks
- Detect the web server attacks
- Detect the troubleshoots in the NIC, PC circuit and transmission rate of peer equipment
- Detect the operations of HTTP Proxy program, such as MSN

Design concepts and working principle

As a rule, all network interfaces of a same segment have the ability to visit all the data transmitted on physical medium and each network interface is supposed to have a hardware address which is different to other existing network interfaces' on network, and at the same time, every network should have at least a broadcast address. In common cases, a legal network interface should response to only these two kinds of frames:

- Target domain of frame has a hardware address matching to local network interface
- Target domain of frame has a broadcast address

In reality, all data are transmitted by the network interfaces in network, which has four kinds of work module:

- **Broadcast** - sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients (default).
- **Multicast** - multicasting refers to sending a message to a select group.
- **Directed** - receiving messages of itself in direct mode
- **Promiscuous** - promiscuous makes the interface receive all packets, regardless of whether they were destined for this host or not.

Although, in default, the NIC can only receive the messages sent to itself when work in broadcast mode, we can force a NIC into the promiscuous mode to receive all frames on the network devices in spite of its destination.

Colasoft Capsa is an application designed strictly complied with Ethernet work mode. We abstract every network frame as an object, e.g. **IP address**, **Physical address**, **Protocol** and **Packet**, which compose a **Project** in Colasoft Capsa. The objects changed continuously in a **Project** reveals the real time traffic in network.

Colasoft Capsa works as bypass based on the Ethernet sniffer technology. First, Colasoft Capsa makes the NIC

installed it can monitor all packets in the network by forcing the NIC into promiscuous mode. Colasoft Capsa analyzes monitored packets and displays the analysis results in its user interface then.

How to work

Data capture

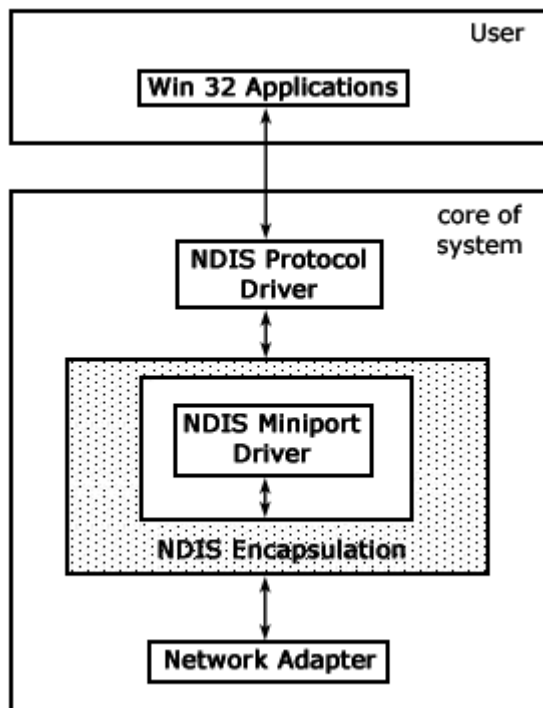
Before analyzes packets, Colasoft Capsa needs to collect the transmitted packets in network. Colasoft Capsa executes collecting packets on the data link layer to capture the packets of Ethernet lower layers.

There are four ways Colasoft Capsa to collect packets:

- Install Colasoft NDIS Protocol Driver on Windows collect the packets system transmitted from NIC.
- Install Colasoft NDIS intermediate Driver on Windows system collect the packets system transmitted from NIC.
- Installing Colasoft NDIS Protocol TDI Driver on Windows system to collect the loopback packets of local host.
- In default, Colasoft Capsa collects packets by installing Colasoft NDIS Protocol Driver and Colasoft TDI Driver.

Note: Users need to install the intermediate driver manually by doing as following: click the "Packet Capture Drivers..." command in the Tools menu, choose the "Colasoft NDIS intermediate Driver" from the combo box in the top of this page and then click the "Install" button.

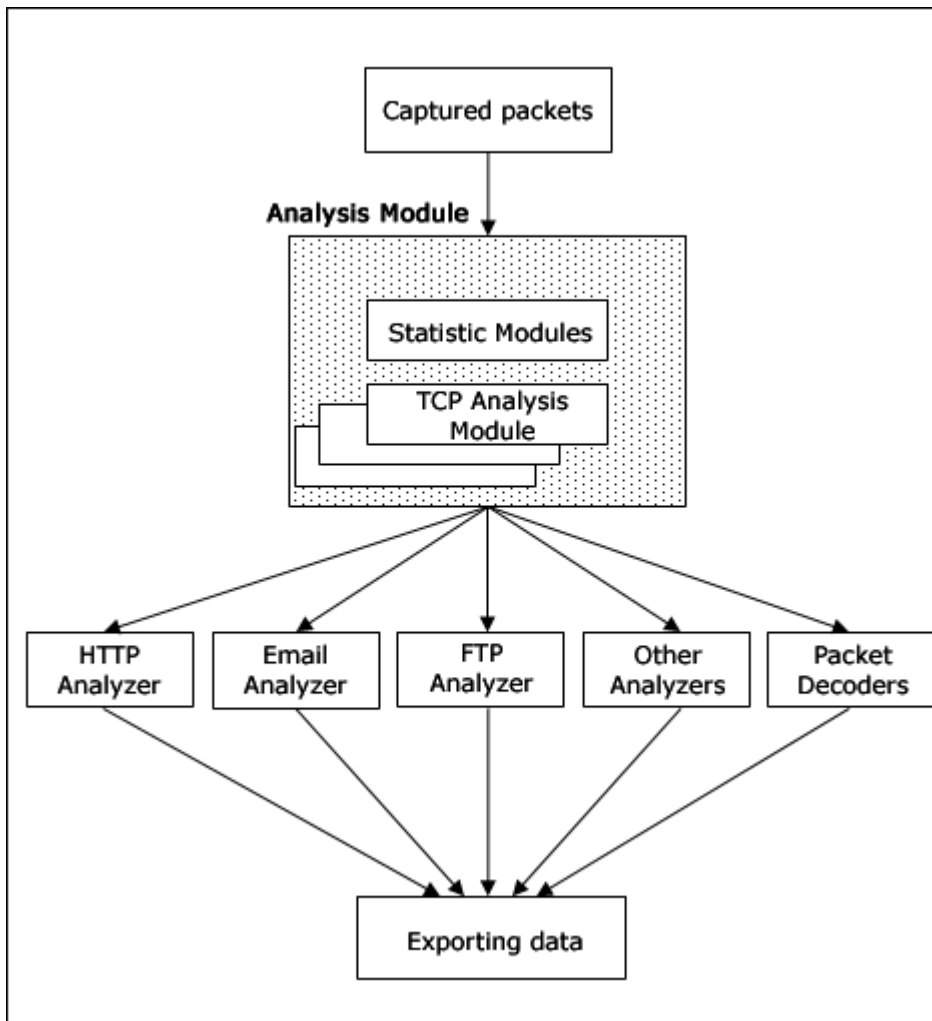
The collection efficiency is extraordinary important for collecting packets. To improve the collection efficiency, Colasoft Capsa filters the collected packets and discard those did not matching the filtering rules in its core of system to reduce the resource occupy during the process of packets transmitted from the core of system to user interface. In default, the packets collecting process of Colasoft Capsa is showed in the following figure.



(Figure1 - the data capturing process of Colasoft Capsa)

Data analysis

The core of system analyzes the packets match the filtering rules immediately after received them. The data analysis includes packets statistics, packets decoding, TCP reconstruction, protocol analysis and etc. The following figure is the data analysis process of Colasoft Capsa.



(Figure2 – the data analyzing process of Colasoft Capsa)

Exporting data

The detailed information of captured packets can be exported to a file in public formats such as Text and HTML after analyzed. The analysis results can be displayed in relative views, graphs, logs, and saved in project files and packet files.

Key features

Colasoft Capsa 6.x enhanced many powerful features, including some unique features different from other packet sniffer programs.

Flexible Project Explorer

The Project Explorer window, whose interface similar to the Windows Resource Manager's, is more convenient and functional. You can not only view the current status of each node but also quickly switch among global statistics and the details of specific network nodes. In this window, all network nodes are

classified into three kinds of group: Protocol Explorer, Physical Explorer and IP Explorer.

- Protocol Explorer - This group lists network endpoints by protocol.
- Physical Explorer - This group lists network endpoints by physical address.
- IP Explorer - This group lists network endpoints by IP address.

Reports

A report contains the statistic information of summary statistics, diagnosis events, protocol statistics, top 10 IP protocol and top 10 addresses, and all available graphs with the current settings. In addition, you can also save the reports as HTML format in a defined path.

Matrix

The Matrix view in Colasoft Capsa is a powerful tool for visualizing the analysis collected network traffic statistics in real time. The nodes were arranged in an elongated ellipse and line weight to indicate the volume of traffic between nodes. You can view matrix statistics not only for a global network, but also for specific network nodes.

Expert network diagnosis

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.

Packet filters

Colasoft Capsa provides two kinds of filters: **Simple Filter** and **Advanced Filter**. The simple filter allows you to customize some commonly used filters by address, port and/or protocol in a single filter. In addition to make simple filters by address, port and protocol, the advanced filters in Colasoft Capsa also allow you to create packet value filters, packet size filters and packet pattern filters based on the logical rules of And, Or and Not.

Packet decoding

Instantly decodes captured packets and displays detailed decode information in **Hex**, **ASCII** or **EBCDIC**. The packet information in the packet decode view, **Hex** and **ASCII/EBCDIC** view are consistent, when you select a section in one of these views, the corresponding portions will be highlighted in the other views.

TCP stream reconstruction

Initial information can be reversed from data fragments through restructuring packets. Analysts is able to see, from TCP stream in the Conversations view , the session and response between client and server, and the real data information received/sent by client or server, so that get hold of the actual operation of network.

Log analysis

Presents the records of network communications analyzed by advanced analyzers, including **Email messages** log, **FTP transfers** log, **HTTP requests** log and **DNS analysis** log. Display activities of four kinds of instant messengers: MSN, AIM, ICQ and Yahoo Messenger. Colasoft Capsa can generate single log file or split log files for the results analyzed by advanced analyzers.

Summary statistics

Provides general statistic information, including start date/time, general errors, 802.3 errors, traffic, packet size distribution, and many other statistics analyzed by multiple analyzers. 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.

Statistic views

The new statistic views comprise **Summary** view, **Endpoints** view and **Protocols** view. These views offer the statistics for network activities, allowing you to get an integrated impression of your network with a few glances. This feature is also very helpful when you need to compare graphs or view reports

Operating multiple projects and multiple adapters

Colasoft Capsa can operate multiple projects synchronous. If you have more than one adapter installed on the local machine, Colasoft Capsa can capture the traffic on all the adapters. You can create a project monitoring all adapters simultaneously, or just focusing on a specific adapter.

Technical Indicators

System Requirements

Minimum

- P3 500 CPU

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

Recommended

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

Notes

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

Supported Protocols

Application	BGP, BOOTP, CIFS, DHCP, DNS, Finger, FTP, FTP Control, FTP Data, Gopher, H.323, HTTP, HTTPS, IMAP, IMAP3, IMAPS, LDAP, LDAPS, Mobile IP, MSN, NFS, NNTP, NTP, POP2, POP3, POP3s, HTTP Proxy, RLOGIN, RTSP, SLP, SMB, SMTP, SNMP, Telnet, TFTP, QQ, BitTorrent, SNMP Trap, SSDP, ICP, COPS, RTP, RTP Audio, RTP Video, RTP Audio & Video, RTP Dynamic, COPS, Tunnel, Echo, CMIP-Agent, CMIP-Man, SFTP, RAP, RLP, Radius, Radius-acct, Radius-dynauth, eMule, PPlive, SShell, Kerberos, Citrix ICA, Time, Nameserver, Tacacs, Xns-time, JE, Discard, Sysstat, Qotd, MSP, Daytime, Msg-auth, Auditd, Ni-ftp, MPM, MPM-snd, Re-mail-ck, La-maint, XNS-ch, XNS-auth, XNS-mail, Tacacs-ds, Mit-mi-dev, CTF, NPP, DCP, Supdup, Swift-rvf, Tacnews, Mcidas, Pwdgen, Statsrv, Emfis-data, Emfis-cntl, HMP, PRM, RDP, IRTP, NETBLT, DCCP, IDPR, DDP, SDRP, IDRP, DSR, NARP, TLSP, PVP, SMP, PTP, CRTP, CRUDP, PIPE, FC, SPS, SNP, ISO-TP4, SKIP, CFTP, Login, Who, Yahoo Messenger, X-Window, UMA, ISO-TP0, ISO-IP, BFTP, SGMP-traps, NAMP, Send, R IS, MPP, CDC, Http-mgmt, PIP, Rtsp, Pdap, NSRMP, RSVP_tunnel, IBM-app, SNPP, RCP, NMSP, IDFP, SCC Security, Submission, SMIP, XDAS, RAMP, ACNET, Sflow, CRIP, TRIP, Mnet-discovery, Rwhois, Citrix ICA, Rexec, Biff, RTP with VLC
Presentation	AFP, Datagram Service, Name Service, NCP, NetBIOS
Session	RPC, SAP, Session Service

Transport	H.225, RTCP, SSH, TCP, UDP, NetBEUI
Network	CGMP, EIGRP, EGP, GRE, ICMP, IPv6, ICMPv6, IGMP, IGRP, IP, IP Fragment, IPX, OSPF, PIM, RSVP, VRRP, RIP, RIPv1, RIPv2, RIPv3, RIPv4, GDP, HSRP, RSVP, Cisco-fna, Cisco-tna, Cisco-sys, GGP, EIGRP Hello, EIGRP Query, EIGRP Reply, EIGRP Update, SGMP, Password-chg, CFS, SCCP
Data Link	ARP, RARP, Ethernet II, Ethernet 802.2, Ethernet 802.3, Ethernet SNAP, PPPoE, STP, VLAN 802.1Q, XNS, AARP, MPLS, Windows NLB
Others	Kerberos, GTP, L2TP, LPD, MGCP, MSRDP, MSSQL, PPTP, RSH, RTELNET, SCTP, SQL, SIP, WhoIs, WINS, AH, ESP, PUP, CDP

Decoding Protocols

- AH packet decoder
- ARP packet decoder
- BOOTP packet decoder
- COPS packet decoder
- CIFS packet decoder
- DHCP packet decoder
- DNS packet decoder
- EGP packet decoder
- ESP packet decoder
- Ethernet 802.2 frame decoder
- Ethernet 802.3 frame decoder
- Ethernet II frame decoder
- Ethernet SNAP frame decoder
- Finger packet decoder
- FTP Ctrl packet decoder
- FTP Data packet decoder
- Gopher packet decoder
- GRE packet decoder
- HSRP packet decoder
- HTTP packet decoder
- ICMP packet decoder
- ICMPv6 packet decoder
- ICP packet decoder
- IP packet decoder
- IPv6 packet decoder
- IPX packet decoder
- L2TP packet decoder
- LPD packet decoder
- MPLS packet decoder
- MSN packet decoder

- NetBIOS datagram service decoder
- NetBIOS name service decoder
- NetBIOS session service decoder
- NCP packet decoder
- OSPF decoder
- POP3 packet decoder
- PPP packet decoder
- PPP CHAP packet decoder
- PPP IPCP decoder
- PPP link control packet decoder
- PPP PAP decoder
- PPPoE discovery packet decoder
- PPPoE session packet decoder
- PPTP packet decoder
- QQ packet decoder
- RARP packet decoder
- RIPv1 decoder
- RIPv2 decoder
- RSVP packet decoder
- SAP packet decoder
- SCTP packet decoder
- SMB packet decoder
- SMTP packet decoder
- SPX packet decoder
- SSH packet decoder
- TCP packet decoder
- TELNET packet decoder
- TFTP decoder
- UDP packet decoder
- VLAN tag decoder
- VRRP packet decoder
- GGP packet decoder
- ISMP packet decoder
- IGRP packet decoder
- EIGRP packet decoder
- CDP packet decoder
- CGMP packet decoder

Supported Networks

Colasoft Capsa can monitor and analyze communications transmitted on Ethernet, Fast Ethernet or Gigabit Ethernet networks.

Capture Resources

- 100/1000 Mbps Ethernet adapters
- Loopback Interface (Windows 2000/XP)

Supported 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)

Log Analysis

- Email messages analysis
- FTP transfers analysis
- HTTP requests analysis
- DNS analysis
- MSN activities
- AIM activities
- ICQ activities
- Yahoo Messenger activities

TCP Stream Reconstruction Formats

- ASCII
- EBCDIC

Real-time decoding and analysis

Colasoft Capsa captures, decodes and analyzes network communication in real time.

Timestamp

Colasoft Capsa captures packets and decodes in microsecond and displayed in Hex, ASCII and EBCDIC.

Network Monitoring

Colasoft Capsa monitors network communication in real time.

Notes

As a network analysis program, Colasoft Capsa should be used by the users with basic knowledge on network technologies. It will more helpful in network management, network traffic analysis and network problems troubleshooting if users more skilled in network technologies.

The basic network technology for using a sniffer program including:

- The Ethernet work principle.
- The IP address, MAC address and often used protocols of TCP/IP suite.
- The work principle of some network devices, such as hub, switch and router.

Please visit <http://www.colasoft.com/capsa/> for more details.