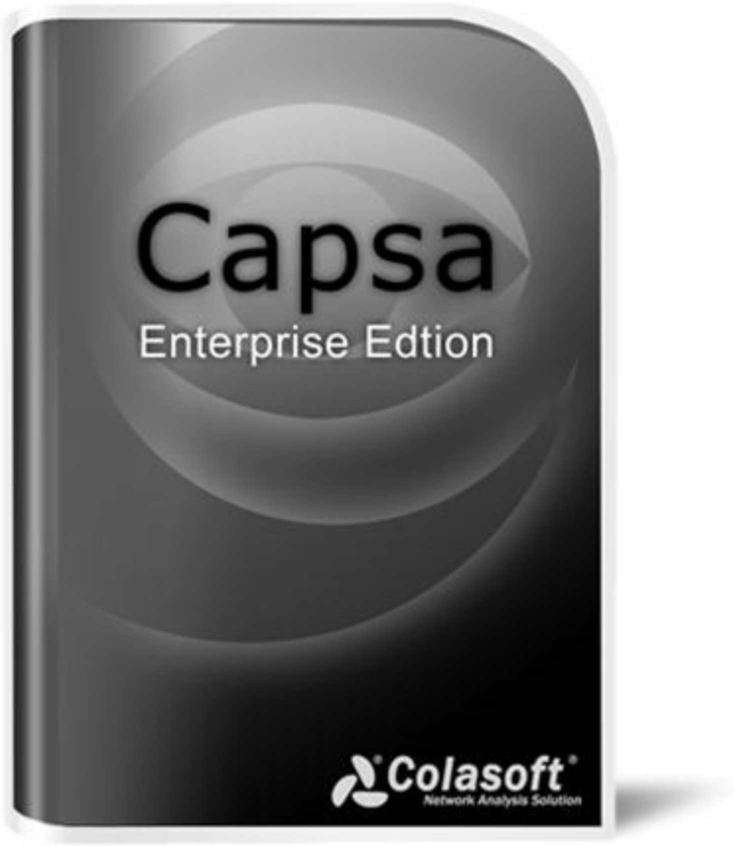
Colasoft
Maximize Network Value

Colasoft Capsa

Technical White Paper

Maximize Network Value



Content

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 suffer 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 are becoming more and more important, network engineers and administrators are facing the problem of how to improve network speed and efficiency. While on the other hand, due to network infrastructure being more complex and network technology developing amazingly fast, it is more difficult than ever before to implement network maintenance and network arrangement. A good network tool, like Colasoft Capsa, can help administrators find and solve network problem when it's occurred and become network experts.

Overview

With the abilities of data collecting, packet decoding and analysis as well as strong functions of 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 real-time monitoring, packet decoding and data display, With Colasoft Capsa you can:

- *Analyze abnormal 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*
- *Analyze and locate which computers are using BT downloading*
- *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*
- *Save all packets on the network to hard disk*

Concept and 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 is transmitted by the network interface 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, by 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. Colasoft Capsa makes the NIC work in promiscuous mode then analyzes captured packets and displays the analysis results in its user interface.

How to Work

Data capture

Before analyzing 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 three ways that Colasoft Capsa collects 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.
- Install Colasoft NDIS Protocol TDI Driver on Windows system to collect the loopback packets of local host.

By default, Colasoft Capsa collects packets by installing Colasoft NDIS Protocol Driver and Colasoft TDI Driver.

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 as the following figure.

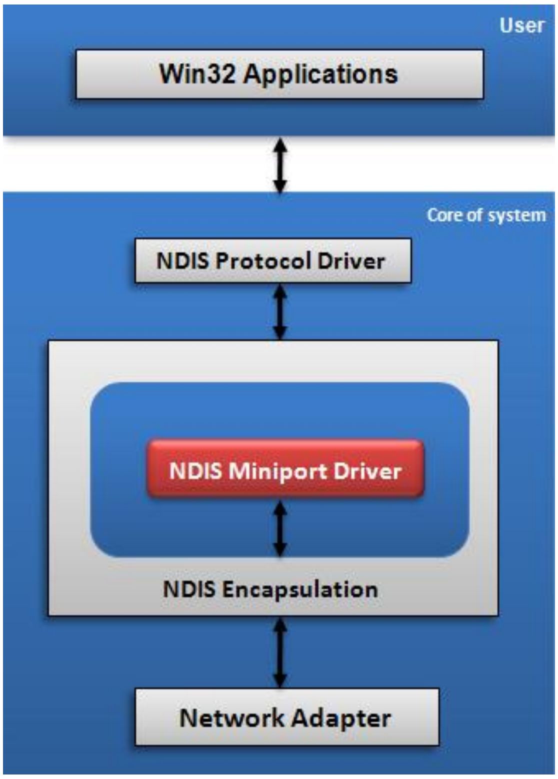


Figure1 - the data capturing process of Colasoft Capsa

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.

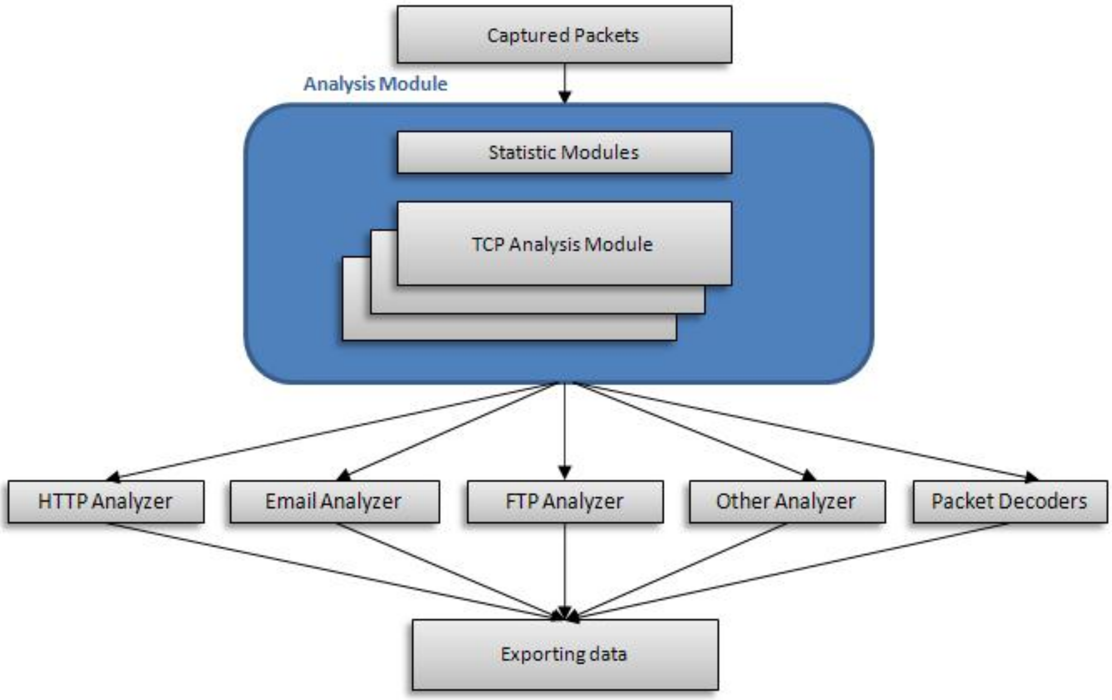


Figure2 – the data analyzing process of Colasoft Capsa

Exporting data

The captured packets will be stored in the dedicated buffer temporarily, and those packets can be exported to files in public formats. Packets in buffer can be automatically saved to disk in multiple files as well. The analysis results can be displayed in relative tabs, graphs, logs and reports. All statistics can be exported to hard disk.

Key Features

Colasoft Capsa 7.x enhanced many powerful features, including some unique features different from other packet sniffer programs.

Analysis Profile

Colasoft Capsa defines analysis profiles as containers of different analysis modules. This structure can make sure every analysis profile provides flexible, extensible and effective analysis performance. You can combine different analysis modules together to create your own analysis profile that focusing on certain applications.

Analysis Type	Analysis Profile	Description
Basic Analysis	Traffic Monitor	Provides analysis for large traffic network or traffic monitor (supports 1000M network adapters).
	Full Analysis	Provides in detailed analysis statistics of all traffics and applications.
Application Analysis	HTTP Analysis	Analyzes the HTTP traffic. Provides traffic statistics of clients and servers, performance diagnosis and logs of HTTP activities.
	Security Analysis	Analyzes the DoS (DDoS) attack, ARP attack, TCP – SYN attack, Worm activity and suspicious conversation in network.
	FTP Analysis	Analyzes the FTP traffic, Provides statistics on uploading, downloading, performance diagnosis and logs of FTP activities.
	Email Analysis	Analyzes the SMTP/POP3 traffics. Provides statistics on email communications, duplicating emails and logs of email activities.
	DNS Analysis	Analyzes the DNS traffic and provides statistics on DNS queries, performance diagnosis and logs of DNS activities.
Build-in Analysis	TCP Analysis	Analyzes the TCP traffics and provides data for upper application Analysis Profiles.

Network Profile

Colasoft Capsa can be installed on a laptop and move between different networks. Every network segment has its own network structure and property. Network Profile is used to save the general properties of different network segments, including: bandwidth, network structure, name table and alarms. When you need to analyze the same network segment again, you just load the network profile of that segment.

Protocol Customization

Colasoft Capsa recognizes more than 300 protocols and sub-protocols. You can easily create rules to recognize new protocols to your specific needs. You can specify protocols by Ethernet type, IP encapsulated protocol id, TCP port and UDP port.

Flexible Explorer window

The Explorer window, whose interface is similar to the Windows Resource Manager, 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 groups: 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.

Customizable Dashboard

The Dashboard provides a wide variety of graphical statistics and allows you to customize and create useful graphs and charts in different panels to get statistics on any MAC address, IP address and protocol, etc, or top ten statistics of certain statistics. These graphs and charts help you find out anomalies at a glance.

Real-time Alarm

In Colasoft Capsa, you can customize alarm triggers such as total traffic, protocol, conversations etc. You will be immediately notified via pop-ups with the critical parameters and related information to help you promptly deal with the anomaly. If you are not around, an alarm log will be made and critical information will be saved.

Reports

A report contains the statistic information of summary statistics, diagnosis events, protocol statistics, top 10's, and all available graphs with the current settings. In addition, you can customize the report template and save the reports as HTML or PDF format to disk.

Matrix

The Matrix view in Colasoft Capsa is a powerful tool for visualizing the analysis captured network traffic statistics in real time. The nodes are 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 pane, whereas the corresponding possible causes, remedy and relating addresses are provided to help you quick locate the host and solve the problem.

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 filers based on the logical rules of And, Or and Not. The new design lets you easily learn how the packet filter are combined and processed.

Packet decoding

Instantly decoding captured packets and displaying 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 revered from data fragments through restructuring packets. Analysis 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 as to 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, **DNS analysis** log and monitors **MSN** (aka **Microsoft Live Messenger**) and **Yahoo Messenger** messages. Colasoft Capsa can generate single log file or split log files for the results analyzed by advanced analyzers. Furthermore, Colasoft Capsa is able to not only log the email activities but also make a copy of each detected email message including its body and all the attachments.

Statistic views

The statistic views are redesigned, which reduce to total volume of statistic items and let you find more useful statistics with less clicks. 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.

Technical Indicators

System Requirements

Minimum

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

Recommended

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

Supported Operating Systems

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

Notes

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, QQ
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
Data Link	ARP, RARP, Ethernet II, Ethernet 802.2, Ethernet 802.3, Ethernet SNAP, PPPoE, STP, VLAN 802.1Q, XNS, AARP, MPLS
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

Supported Networks

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

Capture Resources

10/100/1000 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 queries analysis
MSN message analysis
Yahoo Messenger analysis

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 technology. It will be more helpful in network management, network traffic analysis and network problems troubleshooting if users are more skilled in network technology.

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.

www.colasoft.com
support@colasoft.com