Colasoft®
Maximize Network Value

Capsa

Real-time Portable Network Analyzer

Whitepaper

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

Contact Us

Sales

sales@colasoft.com

Technical Support

support@colasoft.com

Website

https://www.colasoft.com/

Contents

Introduction

This chapter describes the background, the system architectures, and the principle that how Capsa works.

Background

The rapid popularization and wide application of wired and wireless networks, 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. On the other hand, due to network infrastructure being more complex and network technology being developing amazingly fast, it is more difficult than ever before to implement network maintenance and network arrangement. Therefore, efficient network management solutions are very important for to administrators find and solve network problems.

Capsa, provided by Colasoft, is such a solution. It captures original packets in real-time, decodes, analyzes, and diagnoses captured packets, and then displays the results in straightaway views, visualized charts and structured reports, to thereby get the network administrators to know the network status comprehensively and quickly.

Working principle

In actual network communications, all data are sent and received by network adapters. By default, a network adapter only receives unicast packet traffic matching its MAC address and broadcast traffic on the network. If we put the network adapter in promiscuous mode, it will receive all traffic through it, regardless of the destinations.

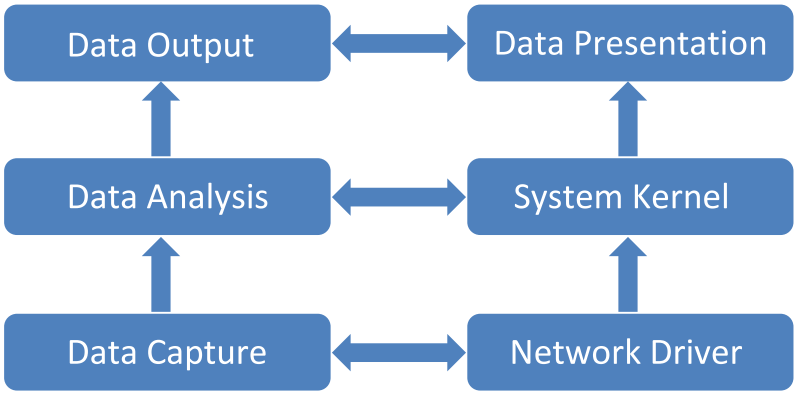
Colasoft Capsa utilizes such a mechanism to capture packets. It takes every network element, such as IP addresses, MAC addresses, protocols, packets, as a network object, and integrates them into a project. Therefore, every tiny change on the network will be monitored and analyzed to the project.

Based on Ethernet sniffer technology, Capsa captures traffic via bypass access. It first puts the network adapter of the computer on which Capsa is installed in promiscuous mode to capture all packets over the network, then delivers captured packets to analysis modules for analyzing, and at last displays the result on the screen and automatically diagnoses the problems.

System architecture

To analyze the traffic over the network, the traffic must first be captured. The network drivers at the bottom-level are the core module for detecting and capturing the data transmitted. And then all data are forwarded to high-level modules to be analyzed, summarized and outputted on screen. The architecture of Capsa is described as Figure 1.

Figure 1 Capsa Architecture



1. Network drivers are responsible for network traffic capture and ensure the data is accurate and complete.
2. All captured data is delivered to analysis modules for real-time diagnosis and analysis, such as diagnosis module, statistic modules and packet decoding module, and other analysis modules.
3. Finally, the analysis results are outputted to user interface and/or to hard disk.

Colasoft Packet Analysis Engine (CSPAE) II

The 2nd generation of Colasoft Packet Analysis Engine (CSPAE), powered by the innovative Colasoft dynamic object model (CSDOM), greatly improves analysis efficiency and performance under heavy traffic networks. The following new technologies are applied to Capsa.

- Multi-thread analysis
  - Upgrade single-thread analysis to multi-thread analysis technology, which take full advantage of the processing ability of multi-core CPU.
- Multiple Cycle Buffer (MCB)
  - Recycle multiple cache buffers
  - Parallelize data analysis and data accessing to avoid latency from analysis and data query
  - Decrease memory fragmentation
- Direct Memory Access (DMA)
  - Bypass kernel-level to transmit data directly to user-level
  - Speed up data transmission
- Protocol dynamic creation
  - Dynamically create protocol tree structure
  - Effectively identify protocol and sub-protocol types
  - Support custom protocol definition

Data capture

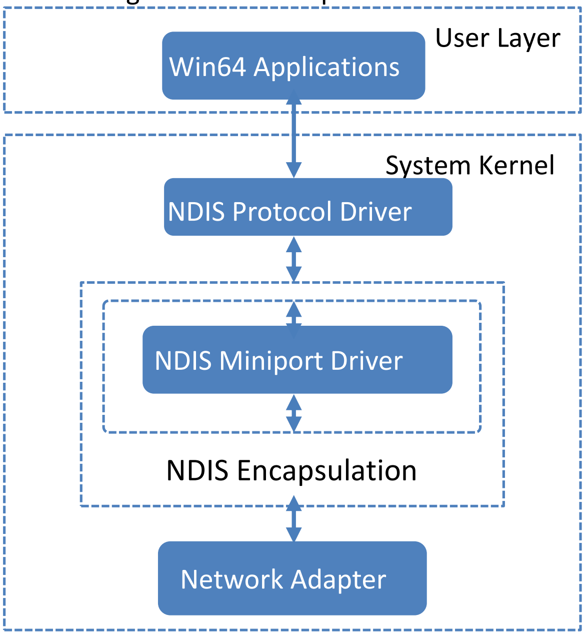
Capsa can capture packets by the following three methods:

1. With Colasoft NDIS Protocol Driver on Windows, capture packets by network adapters.
2. With Colasoft NDIS Intermediate Driver on Windows, capture packets by network adapters.

3. With Colasoft TDI Driver on Windows, capture local loop packets without network adapters.

By default, Capsa collects traffic via Colasoft NDIS Protocol Driver and Colasoft TDI Driver. The following figure outlines the data capture process for Capsa.

Figure 2 Traffic Capture Process

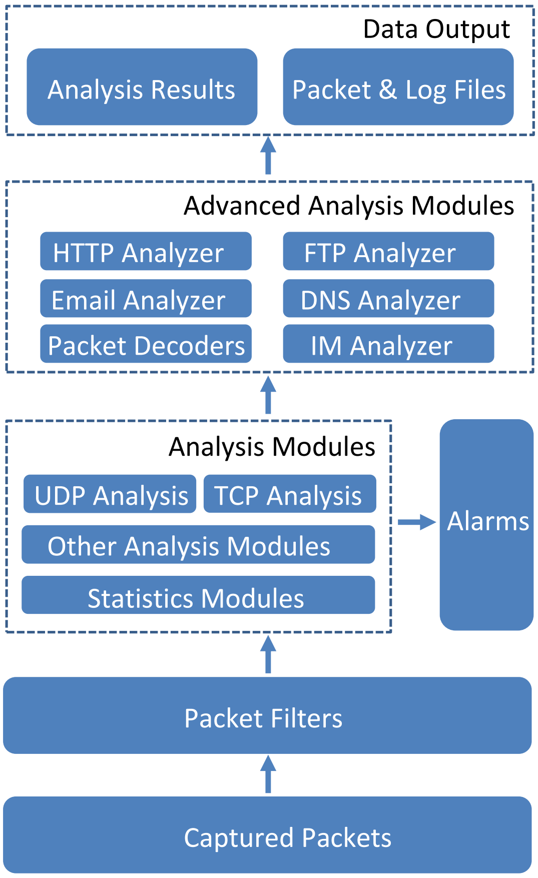


The efficiency of data capture at the bottom level is crucial to the following analysis missions. Thus, filters are implemented on this level to filter out the irrelevant packets so as to avoid the waste of the resource due to data transfer from driver level to application level.

Data analysis

When the driver gets a packet matching filtering conditions, it immediately delivers the packet to the system kernel for further analysis. The analysis includes statistics, in-depth packet inspection, packet decoding and protocol analysis. The following flowchart shows the packet analysis process of Capsa.

Figure 3 Packet Analysis Diagram



Data output and presentation

After packet analysis, all analysis results and statistics are presented in the form of charts, lists and reports on the screen. The analysis contents presented including packet decoding, nodes, protocols, IP flow, TCP flow, conversations and logs. In addition, these lists, reports and logs can be exported for further use according to the need.

Technical Characters

Capsa network analysis system provide multiple original functions, the most important of which will be introduced below.

A new analytics-guided experience

The start page guides users through network analysis tasks in a simple, intuitive view. Usually an analysis task is completed in the following 6 steps:

1. Select analysis mode
   - Provides two data acquisition and analysis modes, real-time analysis and playback analysis.
   - In the real-time analysis mode, you can choose to set the network adapter.
   - File and playback speed can be selected in playback analysis mode.
   - Both modes can additionally set packet capture filters.
2. Select network adapter

   Wired Network Adapter: Select the network adapter used to capture data. One or more network cards can be selected for data capture at the same time.

   Wireless Network Adapter: Only one network card can be selected for data capture. To capture wireless packets, select the wireless AP to be analyzed and enter the correct password. The system supports the analysis of multi-channel APs. When the selected AP is a multi-channel AP, you need to select an auxiliary network card for analysis.
3. Set Data Capture Filters

   Create new packet capture filters to quickly capture data sources.
4. Choose Analysis Settings

   According to the actual needs, the relevant analysis settings are selected in a targeted manner to achieve the best analysis application.
5. Start analysis

Real-time analysis and playback analysis

Capsa provides two kinds of analysis strategies: real-time and playback. Real-time analysis uses network adapter as data collection source, and provides intuitive display of adapter traffic status; playback back analysis uses packet storage file as analysis data source, and supports original-speed playback and Fast playback, convenient for users to perform retrospective analysis.

Useful Analysis Settings

Analysis settings are used to save configuration information for a specific analysis requirement, including parameter configuration of the analysis engine, loaded advanced analysis modules, and detailed parameter settings of each advanced analysis module.

Capsa builds several analysis settings for users to choose for typical analysis usage scenarios, and each analysis setting corresponds to a specific analysis requirement.

Flexible chart settings

Capsa provides a powerful chart customization function and provides users with a rich graphical real-time monitoring view of traffic. You can easily customize and add chart panels, and each chart panel can add various types of charts at will.

The system not only supports global chart settings, but also can create and add charts for specific network objects, and can create real-time chart monitoring, including detailed data information of TCP sessions, application traffic information, and alarm data information, so that users can the real-time running data of various network parameters can be seen more intuitively.

Custom protocol

Capsa has a powerful custom protocol function, users can customize the protocol according to the actual situation according to the following two types of fields.

- TCP
- UDP

Expert diagnosis

Expert diagnosis is one of the characteristic functions of Capsa. It can intelligently analyze the captured data, and automatically prompt the error information or fault information in the network. Users do not need to know the details of the data packets. content, you can troubleshoot network failures.

Diagnostic view has a new view layout, which not only provides detailed diagnostic events, diagnostic event logs associated with the host, but also displays detailed information and event reference information for each diagnostic event in detail. The current product supports four levels of fault diagnosis: application layer, transport layer, network layer and data link layer. At the same time, network errors and faults are divided into security levels, as shown in Table 1.

Table 1:Security level planning

Security Level	Describe
Information	Ordinary information notification is only used to record an event, and there is no network error.
Notice	Content that prompts network events or specific events and requires users to pay attention.
Warn	A warning prompt is given for errors or failures, and the user should deal with them in time.
Critical	This is a prompt for serious errors or serious faults, and users need to deal with them in time.

Traffic Analysis

Traffic analysis is one of the main functions of Capsa. Through this function, users can quickly find and locate the IP host point and physical host with the largest traffic volume. The system also supports clear statistics and ranking of endpoint traffic for each network protocol. For example, users can quickly find the top 5 IP hosts that use the HTTP protocol in the network.

The traffic analysis function of Capsa can analyze the specific traffic occupancy in the network, such as the host with the largest total traffic, the host with the largest sending traffic, the host with the largest receiving traffic, the host with the largest number of data packets sent and received, and the host with the largest number of data packets sent and received. Information such as the host with the most packets, the host with the most packets, the host with the most internal traffic, and the host with the most broadcast traffic. Through this information, we can determine whether there is a broadcast/multicast storm in the network, and help users troubleshoot network failures such as slow network speed, intermittent network, worm virus attacks, DOS attacks, and users unable to access the Internet.

Protocol analysis

The protocol analysis function of Capsa, according to the actual network protocol encapsulation sequence, is displayed to the user hierarchically, each protocol has its own color, in addition to the global protocol statistics, it can also provide protocol statistics under each network endpoint.

The protocol view can effectively display the protocols used for data communication in the network. The protocols are displayed in a tree-like hierarchy. For each protocol, the traffic occupied by it, the number of data packets using this protocol, and the traffic of this protocol are in total. The percentage of traffic and the percentage of total packets that use this protocol are counted. Through the statistics of the traffic occupied by each view and the percentage in the protocol view, the user can obtain the protocol that occupies the most traffic in the current network, that is, the service type that occupies the most traffic in the current network. Network failures such as intermittent network and users not being able to access the Internet.

Online real-time alerts

Capsa provides real-time global alerts to alert administrators of current events in a prominent manner. And display the number of currently triggered alarms in the lower right corner of the main view.

Provides user-defined alarm function. Users can create alerts for selected network objects from multiple views.

Each alert has the following properties:

- Alert object.
- Alert Type (Security, Performance, Failure), Severity (Information, Notification, Warning, Error).
- A rich source of alert statistics.
- Set alert entry conditions.
- Set the alarm cancellation conditions.

Key Features

Capsa provides many powerful features, including some unique features different from other network sniffer products.

Directive analysis guide

An easy-to-use Start Page is provided to guide users to start an analysis project. Usually an analysis project can be started within four simple steps:

1. Select an analysis mode: real-time monitor or replay captured packets.
2. Select the network adapters for capturing packets and then select a network profile, or select the packet files to be replayed.
3. Select an appropriate analysis profile.
4. Click to start an analysis project.

Analysis Settings

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

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

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

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

Name	Description	Modules Needed
Traffic Monitor	Provides traffic statistics and high efficient analysis of main objects, including MAC.	DNS
Security Analysis	Provides dedicated analysis of potential network security risk.	ARP, DNS, Email, FTP, HTTP, ICMP
HTTP Analysis	Analyzes Web applications (based on HTTP) and record clients' web activities and web communication logs.	DNS, HTTP
Email Analysis	Analyzes Email applications (based on POP3 and SMTP) and monitor Email content and attachments and log Email transactions.	DNS, Email
DNS Analysis	Analyzes DNS applications, diagnose DNS applications errors and record DNS application logs.	DNS.
FTP Analysis	Analyzes FTP applications (based on TCP port 21 and 20) and FTP transaction logs.	DNS, FTP

VoIP Analysis	Provides analysis and troubleshooting for VoIP calls.	ARP, DNS, ICMP, VoIP
Process Analysis	Provides network traffic analysis and statistics for all local processes.	ARP, NDS, Email, FTP, HTTP, ICMP

Node Explorer window

A Node Explorer window is provided to let users view the analysis and statistics of a specific node, a network segment or a protocol, conveniently. It is functionally a powerful filter and includes three types of node explorers: protocol node explorer for hierarchically displaying the protocols on the network, MAC explorer for users to view the communications between MAC addresses, and IP node explorer for providing analysis and statistics about IP nodes.

Powerful dashboard

Various charts and graphs can be defined to visualize the network traffic just by a few clicks, not only on the whole network but down to a specific node. In addition, top statistics can be displayed in charts to display the traffic of the network in real-time to get you know the network status directly and comprehensively.

Expert diagnosis

Capsa presents an expert system capable of performing fault and performance management through different levels. The export diagnosis module can identify and analyze more than 40 network problems automatically and advise solutions accordingly. Not only providing you with diagnosis results, Capsa tells you the suspect host addresses, possible causes and solutions for the problem. It is time saving and more effective for wireless network troubleshooting. Therefore, it helps network administrators with plans of corrective action.

Traffic analysis

With traffic analysis, the host with largest communication volume can be located easily and quickly. You can sort the nodes according to bytes, packets, bit rate, TCP conversation quantity, and many other parameters. Furthermore, the host with largest sending traffic, the host with largest receiving traffic, the host with largest broadcast volume, and the network segment with largest internal traffic can be located easily.

Protocol analysis

Capsa hierarchically presents the protocols according to actual encapsulation order of network protocols, with the traffic statistics of each protocol node, including the packets statistics, bytes statistics, bit rate, and traffic percentages. With protocol analysis, you can easily find the applications with largest traffic volume so as to assist you in troubleshooting the network.

Process analysis

Capsa provides a Process view, which provides traffic statistics for local processes, including total bytes, packets, Bps, bps, pps, path, etc. You can double-click a process to view all packets for that process. Also a Process Explorer is provided to group the processes, listing the process name and process ID in a tree-like structure. A Process column is provided for TCP Conversation view and UDP Conversation view to show the process name of that TCP/UDP conversation, which helps users troubleshoot quickly.

Application analysis

The application analysis is able to show all the traffic statistics for applications, including total bytes, packets, Bps, bps, pps, etc. Once an application is selected, the lower pane will show protocol and conversation information related to that application. Double-click an application, the Packet Decoding window will open to show packets related to that application.

Conversation analysis

Capsa provides four types of conversation analysis: MAC conversation which is conversation between MAC addresses, IP conversation, TCP conversation, and UDP conversation. Each type of conversation is provided with source address, destination address, packets as well as bytes for the conversation, start time as well as end time, and conversation duration.

TCP transaction analysis

Capsa presents a comprehensive high-level overview of health of applications on your network. From TCP transaction analysis, you can drill down to access more detailed information, including TCP server/client response time, delay, retransmissions, and further down to the server flow to observe the actual content of the flow. This unparalleled level of control and visibility speeds time to application problem resolution and minimize overall network downtime.

Detailed decoding

A decoding view is provided to display the detailed decoding information of all packets, including summary decoding, field decoding, hexadecimal decoding, ASCII and EBCDIC decoding. With the decoding information, you can know the original data transmitted over the network.

Flexible reports

A report contains the statistic information of summary statistics, diagnosis events, protocol statistics, and top 10’s traffic. In addition, you can make a report not only on the whole network but also on a specific node. Furthermore, you can customize the report template with the company name and private log picture, and save the reports as HTML or PDF format to disk.

Real-time alarms

Alarms can be defined to inform you network anomalies based on various traffic parameters, including the traffic, the packet size, the utilization, protocols, conversations, applications, expert diagnosis events, and many other parameters. In addition, the alarms can be defined both on the global network and on a specific node. When the alarms are triggered, a notification pops up and a sound generates to get you know the anomalies immediately. Besides, the triggered alarms can be notified with emails to get you know the details even if you are not around the computer.

Log analysis

Network communications analyzed by advanced analysis modules can be recorded and displayed in a form of logs, including HTTP request and reply logs, DNS query logs, email sending and receiving logs, FTP file transfer logs, SSL certification logs, VoIP calls logs and VoIP signaling calls logs. Furthermore, the Email logs can not only record the sending and receiving actions but save the copies of the email content, including its body and all the attachments. In addition, all the logs can be saved automatically, into one file or multiple files according to time length or the size.

Dedicated security analysis

Capsa provides an in-depth security analysis profile to detect security threats, including ARP attack, TCP port scan, worm activities, DoS attack, and suspicious conversations. Once those attacks are detected, the infected or attacked hosts will be listed, as well as the time when they are infected or attacked and the hosts who initiate the attack.

Complete 802.11 a/b/g/n support

Wireless networking is overwhelmingly compelling - it's cheap, easy, and portable. As an innovative and high quality network analysis solution for building the latest safe wireless network, Capsa is also designed to measure application performance, monitor network activities, troubleshoot network problems, and evaluate network security. Capsa for WiFi is launched with seamless Wi-Fi technology adoption for 802.11 a/b/g/n networks.

Efficient WEP/WPA/WPA2 decryption

Capsa for WiFi is able to not only capture wireless traffic, but also decode the encrypted wireless data. No matter which encryption type an AP uses, all WEP, WPA and even the hardest WPA2 wireless traffic can be decrypted with the pre-specified security key. Additionally you do not have to figure out the encryption type of an AP, Capsa for WiFi will identify and match the encryption type of keys automatically.

HTTPS decryption

Capsa enables users to decrypt the HTTPS message with the right configuration of key file. There are three common decryption method: RSA, PSK, and (P)MS log file. Capsa support all of these three methods. Users could choose either to edit the RSA key list, to use a PSK, import a (P)MS log file, or even use them all at the same time for the decryption.

Protocol customization

Capsa recognizes more than 1,700 protocols and sub-protocols. You can easily create signatures to recognize new protocols to your specific needs. You can customize protocols by Ethernet type, IP encapsulated protocol ID, TCP port and UDP port.

Application customization

Capsa has more than 1,800 system applications. Capsa also allows you to create signatures to identify new applications to your specific needs. You can customize applications by protocol, port, pattern, IP address, IP address pair, IP address + protocol, address + port, client + server, and address + port + pattern.

Automatic packet capture

A task scheduler is provided to automatically capture packets with pre-determined analysis settings. This function is designed for the mission to capture packets while the user is away from the network. For example, Capsa can be launched automatically to capture packets at midnight, and the packets can be analyzed later next morning. Capsa can also be scheduled to run capture periodically each day, or specified days of each week. For example, an auto-run packet capture task can be created if it's only needed to analyze network packets of each business day between 9:00 and 17:00 from Monday to Friday.

VoIP analysis support

Capsa provides a VoIP analysis module to real-time capture and analyze VoIP calls and graphically display VoIP analysis results. A VoIP view lists all VoIP calls as well as their related statistics and has a lower pane for analyzing voice and video control flows and media flows as well as their jitter, loss, MOS, etc., to visualize analysis data and assess voice and video quality. A VoIP Explorer groups private and public IP addresses for VoIP calls. A VoIP dashboard contains the VoIP analysis charts graphically. Furthermore, there are VoIP diagnosis events and VoIP logs.

Port number based statistics

A Port view is provided to present traffic statistics based on TCP/UDP port numbers. This feature is useful when you want to analyze a specific application. The port numbers are provided with above layer protocol, packets, bytes, average packet size, and common application. All TCP and/or UDP conversations are recorded for selected port number.

Deep packet inspection filter

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

Easy-to-use display filter

Besides the capture filter, Capsa provides display filters to display interested items. The simple display filter is based on the field columns on the statistical views. An advanced display filter is available for the Packet view to display-screen out uninterested packets based on the protocol fields of a packet. The advanced display filter can even display the packets of specified time range.

Technical Specifications

Supported network types

- Ethernet II， Ethernet 802.3， 802.1Q VLANs， 802.11 WLAN
- 10/100/1000 Mbps Base-T
- Layer 2 and layer 3 switching networks

Supported network adapters

- 10/100/1000 Mbps Ethernet adapters
- Supported wireless adapters including:
  - Atheros AR7015, AR6004, AR9380, AR9382, AR9390, AR9485, AR9462, AR958x
  - Intel 1000, 4965, 5100, 5150, 5300, 5350, 6200, 6250, 6300, 6350, AC 7260, 82579LM
  - Realtek RTL8188CU, RTL8192CU, RTL8187
  - Broadcom 4313GN 802.11 b/g/n
  - TP-Link TL-WDN3200 (5.1.7.5014), TL-822N v2
  - D-Link DWA-160 B2 (5.1.7.5014)

System requirements

Operating systems

- Windows Server 2012/2012 R2/2016/2019 (64-bit)
- Windows 7 SP1 (KB3033929) (64-bit)
- Windows 8.1 (64-bit)
- Windows 10 (64-bit)
- Windows 11 (64-bit)

Minimum

- CPU: Intel Core2 Duo 2.0Ghz
- RAM: 4 GB
- Internet Explorer 8.0
- 1GB free disk space

Recommended

- CPU: Intel Core2 Quad 3.2 GHz
- RAM: 8GB or more
- Internet Explorer 11.0 or higher
- 10GB additional space for packet files and logs

Supported packet file formats

Supported packet file formats to replay

- Colasoft Packet File (v6) (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt)
- Colasoft Raw Packet File (v2) (*.rawpkt)
- Accellent 5Views Packet File (*.5vw)
- EtherPeek Packet File (V9) (*.pkt)

- HP Unix Nettl Packet File (*.TRCO;TRC1)
- Libpcap (tcpdump,Ethereal,etc.) (*.cap)
- Microsoft Network Monitor2.x (*.cap)
- Novell LANalyer (*.tr1)
- NetXRay2.0,and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

Supported Diagnosis Events

Capsa supports application layer, transport layer, network layer and data link layer fault diagnosis, supporting 40 different types of events.

Application Layer		
Suspicious HTTP Conversation	HTTP Server Error	DNS Sever Slow Response
HTTP Sever Slow Response	HTTP Client Error	DNS Server Returned Error
HTTP Request Not Found	Non-exist DNS Host or Domain	SMTP Sever Slow Response
Suspicious SMTP Conversation	SMTP Server Returned Error	POP3 Sever Slow Response
Suspicious POP3 Conversation	POP3 Server Returned Error	FTP Sever Slow Response
Suspicious FTP Conversation	FTP Server Returned Error	
Transport Layer		
TCP Connection Refused	TCP Duplicate Connect Attempt	TCP Slow Response
TCP Retransmission	TCP Invalid Checksum	TCP SYN Storm
TCP Duplicated Acknowledgement	TCP Port Scan	TCP Header Offset Error
Network Layer		
IP Invalid Checksum	IP Too Low TTL	ICMP Source Quench
ICMP Destination Unreachable	ICMP Network Unreachable	ICMP Host Unreachable
ICMP Port Unreachable	ICMP Host Redirect	ICMP Network Redirect
IP Address Conflict		
Data Link Layer		
ARP Scan	ARP Request Storm	ARP Too Many Unrequested Replies
Invalid ARP Format	Physical Loop	

Supported protocols

Capsa supports identifying 1200+ protocols.

Decoded protocols

Capsa supports decoding 731 protocols.

Supported applications

Capsa supports identifying 3400+ applications.

Real-time capturing, decoding and analysis

Capsa can capture, decode and analyze packets in real time.

Technical Parameters

Support real-time traffic capturing for 1G network

By-pass deployment, without changing the original network topology and architecture

Support multi-NIC data aggregation analysis

Support import offline data

Support multi-NIC aggregation, which can aggregate, capture and analyze the traffic of multiple NICs

Support IPv4 and IPv6 packet analysis

Supports custom script filters to capture and display data

Support session filtering and packet filtering analysis, filtering conditions include IP address, port, protocol, packet size, packet value, country, protocol, etc.

Packet analysis accuracy reaches nanosecond-level

Support user-defined network protocol identification, including logical condition combination such as port and content characteristics

Support chunked encoding and reorganization and gzip compression and decoding

Support combined decoding and analysis of IP fragmented packets

Support packet construction and forwarding

Support expert diagnosis and automatic alarm

Support protocol decoding and exporting

Provide http analysis, mail analysis, DNS analysis, FTP analysis, VoIP analysis and other analysis views

Support file restoration, including HTTP, FTP, TFTP, email attachments (POP3, SMTP, IMAP4)

Support call Wireshark protocol library

Support custom protocol decoding and script language to decode unknown protocols

Support decoding field statistics

Support identify external network assets and statistics

Support SSL certificate restoration, and extract the original certificate information

Support record network protocol logs, provide extraction logs for HTTP access request, DNS resolution request and response, SMTP/POP3 sending and receiving, and SSL certificate information, and support automatic saving to log files

Support provide Matrix view for all nodes (MAC, IP)

Supports custom charts, which can display network traffic in real-time graphically

Support TCP/UDP conversation analysis, and provide time sequence analysis for TCP/UDP conversations, which can graphically display the data interactive transmission process in TCP/UDP conversations, and can graphically display the time interval in data transmission

Support statistically analyze the traffic of all ports, including port value, port type, protocol, number of bytes, number of packets, etc.

Supoort statistically analyze all network service (server address + port) traffic, including IP address, port value, GEO location, protocol, number of bytes sent (packets), number of bytes received (packets), etc.

Support packets to be saved on demand (specify the size of a single packet, specify file type, specify save method - single file, multiple files, only save packets without analysis, packet storage filter settings, etc.)

Support statistically analyze the process traffic, including process name, number of bytes, number of packets, packet send-to-receive ratio, bytes send-to-receive ratio, etc.