

Colasoft Capsa 7.x

Datasheet

Colasoft Capsa Enterprise enables you to:

Get information about complex, enterprise networks;

Provide 24/7 surveillance over your networks;

Enhance network security;

Gets real-time alarm of application violating your rules;

Discover performance bottlenecks, thus improve network performance;

Speed up your existing network problem detection and resolution process;

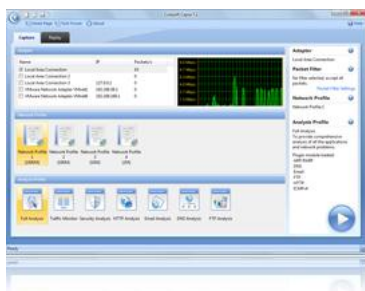
Increase ROI on existing networks;

Save time dealing with urgent network issues;

Reduce loss caused by network downtime and service degradation;

Reduce IT spending.

Capsa Overview

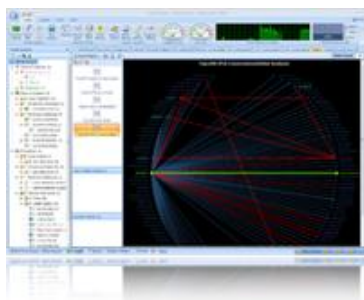


Trusted by both Fortune 500 as well as small and medium-sized companies as their management solution, Capsa Enterprise offers an easy, yet powerful way for network monitoring, analysis and troubleshooting. By providing vivid graphs, information-rich statistics and real time alerting via a well-designed GUI, Capsa Enterprise allows IT administrators to identify, diagnose, and solve network problems in real time, monitor user activities on their networks, and ensure their network's communication assets are safe.

With Capsa Enterprise, IT professionals are able to:

- Capture and save data transmitted over local networks and conduct both real-time and post-event analysis
- Identify and analyze more than 300 network protocols, as well as network applications based on the protocols
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data
- Get timely pop-up notification of network anomalies by real-time alarms
- Monitor internet, email, web browsing and file sharing, etc, helping keep employee productivity to a maximum
- Diagnose and repair network problems in seconds by detecting and locating suspicious hosts
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the entire network in an ellipse that shows the connections and traffic between each host

Step-by-step Analysis Experience



Even tracking with the line of clues, excluded lots of irrelevant elements, the information is still too huge that may submerge useful ones and make user feel lost. How to dwindle in information scope step by step, exclude unrelated information and keep useful ones and zoom out the key point, is now becoming the most significant task to make network analysis meaningful and solution oriented.

"Capsa Enterprise is an enormous, well-engineered, technical and highly professional product that provides almost everything you could want for network and protocol analysis and reporting at a reasonable price."
 -NetworkWorld.com

NETWORKWORLD

"Having the right tools on the network is critical to a network administrator's success. In this TechRepublic blog post, IT Jedi Rick Vanover takes a look at the Colasoft Capsa tool for network analytics."

 **TechRepublic**
 Real World. Real Time. Real IT.

"As computers become more ingrained in the daily operations of most companies, it seems that running into problems occurs more frequently and with greater consequences. When it comes to computer networks, the key issues are security, speed, and reliability. A newly improved network analyzer called Capsa 6.9 R2, developed by Colasoft Inc., can help companies monitor, detect, and troubleshoot network problems..."

 **PHYSORG.COM**
 SCIENCE : PHYSICS : TECH : NANO : NEWS

Network engineers can track upon the clue string and strip the onion skin step by step:

Choose analysis mode (capture real-time packets from adapters or replay packets from packet files) – choose network profile (properties of current network) – select analysis profile (focus on specific applications or traffic) – view statistics in main view (find anomalies) – locate node (filter out disrelated statistics)

Along with these steps, you are getting closer and closer to the target. This process blocks out all irrelevant information and help users quickly find what they really need, instead of floating aimless in countless statistic items and numbers.

Easy-to-navigate UI

Network Analysis is a topic about methodology which impresses people with a complex-tech-involved face at the first glance. And actually it is. But it can be easy and efficient for those who want it merely for problem solving rather than researches.



With the latest *Microsoft Office 2007* template and enhanced UE (user experience) design, users are able to navigate more friendly and get useful statistics with less mouse clicks and time.

Based on our understanding, network problem is not exactly a real problem in "network", which because "network" is not a physical existed object but a logical concept. While there are problems, and you drill down where it exactly is, in the final analysis, they always appear as individual fault on

devices (misconfiguration/device error) – which is the concept we called NODE based, or, maybe every device is working fine individually but they just don't cooperate, cannot work out together (deployment issue/design problem), they don't agree with each other – which is a PROTOCOL problem basically.

They are the fundamental idea of navigating users. We've integrated the idea and many powerful features in to the designation, and made Capsa to offer the spectrum unique component Explorer Bar which gives clues to connect large number of information, and avoid Information Silo.

In-depth Security Analysis

Security threats like virus, worm and all kinds of attack are always the biggest concern of network administrators. To the lowest level, these activities consume the bandwidth and affect the services and work on the network. But the hackers nowadays are more curious about the information and data stored on your mission-critical server and data storage center.



But no matter whether there is any malicious activities in the network, network administrators need a guard to prove it by evidences. With Capsa, there is no hidden for simple ARP attack, TCP port scanning and worm activities to serious DoS (DDoS) attack. Even it reports all the suspicious conversations to let network administrators not miss any trace.

"Chances are, if you're in charge of supporting a network of any size, you'll need to look at the actual packets that are passing back and forth across that network. Whether it's to see whether a specific machine is sending or receiving packets as it should, or you want to see the contents of the packets themselves, ..."

CrunchGear

"Wherever and whenever a networking issue arises I am always able to have my Colasoft Capsa on-hand to diagnose, and resolve, complex issues."



Powerful Dashboard



statistics on any MAC address, IP address and protocol, etc., or top ten statistics of certain objective. These graphs and charts help you find out anomalies at a glance without any viewing of statistic data.

Locate the right information is crucial to most Network analyze tool users with professional understanding of network knowledge, while translate the information into a more readable and understandable work may happens to be the narrower but more needed case when facing the non-technical users.

Graphs and charts are intuitive and helpful for users to learn whether the network is working normally. The Dashboard allows you to customize and create useful graphs and charts in different panels to get

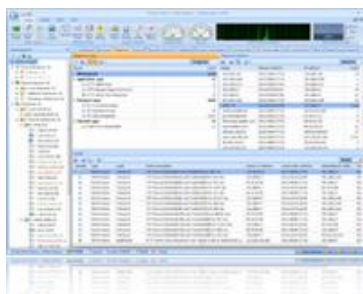
Timely Alarms



Alarms are a set of rules that monitor or do statistics on the communications of the network. Colasoft Capsa notifies you that a specific activity is violating the alarm rules by pop-up notifications to attract your attention timely. You can deal with the anomalies at the first place instead of noticing them until great damages. Alarm rules can be created from almost anywhere in the program by any MAC address, IP address and protocol etc. If you are not around, alarm actions are logged and saved to hard disk with groups of top 10 statistics for your later reference.

Expert Diagnosis

At the ancient network era when Ethernet arisen at the beginning, diagnosis can be easily handled because the data traffic is comparatively very small to the modem world one. Nowadays, network analysis could be really a harsh task upon with the bandwidth-demanded and traffic-increasing network. Manually compare data context and packet header to find the problem seems a mission impossible because the Intranet grow up rapidly that traffic data is innumerable as Gigabit is now generally desktop accessed.



In fact, most network issue goes with symptoms which are predictable. Capsa Enterprise has the module that compares, analyzes the symptoms automatically and summarizes them. This is much more than only an information collector but ulteriorly reorganizes and simply analyzes them. Not only providing you with diagnosis results, Colasoft Capsa tells you the suspect host addresses, possible causes and remedy of the problem. This is time saving and more effective for users to find symptoms and go deeper to the fundamental cause based on the diagnosis events.

Easy-to-set, Visualized Filters

Filter is an important way to exclude irrelevant packets.

Traditional Network Analyze tool gives only logical command expression or coding type filter. It could be flexible into byte accuracy but very annoying because of the extremely ignorable filter direction issue, and also because the complexity of expression grows higher rapidly upon with the flexibility.



Capsa Enterprise gives a visualized filter that users can view the status of filters applied to the project. It reduced the possibility of filter misconfiguration of misapplied direction. And the logic in a visualized way make sense more than only a command line over there.

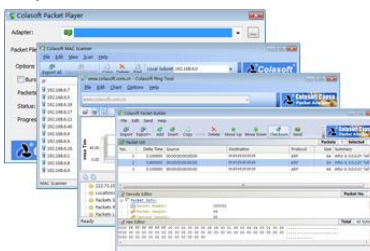
Useful and Valuable Built-in Tools

The built-in tools are simple but powerful. Similar to a scalpel, very sharp, but too sharp that could also be dangerous.

Some of them will allow user to manipulate the traffic as they like, and some will be able to do a total scan over the entire LAN or initiate a connectivity test to one or multiple specific Point throughout the network.

When using the built-in tools like packet builder, or packet player to manipulate the network traffic, a decent understanding of the current environment and professional knowledge of how TCP/IP over different media works is very important. So, it is ok to see the network by only scan or test, but don't try to manipulate the traffic unless you are an expert.

Featured Customers



About Colasoft:

Ever since 2001, Colasoft has been an innovative provider of all-in-one and easy-to-use software solutions for users to **monitor** network activities, **analyze** network performance, enhance network **security**, and **troubleshoot** network problems.

Currently, more than 5000 customers in over 80 countries trust the company's flagship product, Capsa Network Analyzer, as their network monitoring and troubleshooting solution. Featured customers include Alcatel, Airbus, Dell, Ericsson, IBM, Intel, and Pepsi. Our mission is to "**Maximize Network Value**" through providing affordable software that ensures customer's network is closely monitored and

in-time troubleshooted before any business loss is caused. Learn more about Colasoft and its solutions, please visit <http://www.colasoft.com/>.

