Colasoft Capsa [WORK]

Download File

How to Monitor and Troubleshoot Your Network with Colasoft Capsa

Colasoft Capsa is a powerful and easy-to-use network analyzer that allows you to monitor, analyze and troubleshoot your wired and wireless network in real time. Whether you are a network administrator, engineer, or enthusiast, Colasoft Capsa can help you protect and optimize your network performance. In this article, we will show you how to use Colasoft Capsa to perform some common network tasks, such as:

- Capturing and filtering network packets
- Identifying network problems and security threats
- Generating network reports and statistics
- Replaying network traffic for analysis

Let's get started!

Capturing and Filtering Network Packets

Colasoft Capsa can capture network packets from any network adapter on your computer, including Ethernet, Wi-Fi, Bluetooth, VPN, etc. You can also use a network tap device to capture packets from a specific segment of your network. To start a new capture session, click on the **New Project** button on the toolbar and select a capture profile. A capture profile defines the settings and parameters for the capture session, such as the capture mode, the adapter, the filter, the buffer size, etc. You can choose from several predefined profiles or create your own custom profile. Once you have selected a capture profile, click on the **Start** button to begin capturing packets. You can see the captured packets in the **Packets** tab at the bottom of the main window. You can also view various statistics and graphs of the network traffic in the **Dashboards**, **Summary**, **Matrix**, **Endpoints**, **Protocols**, **Conversations**, etc. tabs at the top of the main window. If you want to focus on a specific type of traffic or filter out unwanted packets, you can use the **Capture Filter** or the **Display Filter**. The Capture Filter allows you to specify which packets to capture based on their source or destination address, port, protocol, etc. The Display Filter allows you to specify which packets to display based on their content or attributes. You can use both filters together to narrow down your analysis scope.

Identifying Network Problems and Security Threats

Colasoft Capsa can help you identify and diagnose various network problems and security threats by providing comprehensive analysis and diagnosis features. For example, you can use the following features to troubleshoot your network:

- The **Diagnostics** tab shows you a list of potential network issues and their severity level, such as slow response time, packet loss, TCP retransmission, DNS failure, ARP attack, etc. You can click on each issue to see more details and possible solutions.
- The **Vulnerability** tab shows you a list of known vulnerabilities that may affect your network devices or applications, such as CVEs (Common Vulnerabilities and Exposures), CWEs (Common Weakness Enumeration), etc. You can click on each vulnerability to see more details and mitigation measures.
- The **Suspicious Hosts** tab shows you a list of hosts that may be involved in malicious activities or pose a risk to your network security, such as scanning ports, sending spam emails, downloading malware, etc. You can click on each host to see more details and actions.
- The **Suspicious Conversations** tab shows you a list of conversations that may be suspicious

or abnormal based on their traffic pattern or behavior, such as high bandwidth usage, long duration, large packet size, etc. You can click on each conversation to see more details and analysis.

- The **Email View**, **Messenger View**, **Browsing View**, etc. tabs show you the details of various network applications that may be used for communication or data transfer. You can see the sender, receiver, subject, content, attachment, URL, etc. of each email or message. You can also export or save the data for further

Colasoft Capsa

27f17ad7a0