

Capsa WiFi

White Paper

Contents

Contents.....	2
Background.....	3
How to Work.....	3
System Architecture.....	3
Data Capture	4
Data Analysis.....	5
Data Presentation & Output.....	6
Key Features.....	6
Complete 802.11 a/b/g/n Support.....	6
Compatible with Most Popular Wireless Adapters	7
Multi-AP Wireless Packet Capture.....	7
Efficient WEP/WPA/WPA2 Decryption	7
Logs for User Activities	7
Expert Diagnosis	7
Alarms: Alerts on Abnormal Traffic	7
Colasoft Packet Analysis Engine (CSPAE) II.....	8
Multi-Thread Analysis	8
Multiple Cycle Buffer (MCB)	8
Direct Memory Access (DMA)	8
Protocol Dynamic Creation	9
System Specifications	9
Comprehensive traffic statistics	9
Expert network problem diagnosis.....	10
Customizable protocol analysis	10
Conversation analysis.....	10
Security analysis.....	11
Performance evaluation.....	11
Product Specifications.....	12
Operating Systems	12
System Requirements	12

Minimum	12
Recommended.....	12
Supported Wireless Networks	12
Supported Wireless Adapters	12
Supported Encryption Types	12
TCP Reconstruction Formats	12
Supported Protocols	13
Supported Packet File Formats	13
Notes.....	13

Background

In networking field, the fast developing wireless network standard of 802.11x, with its advantages of mobility, simplicity and cost-effectiveness over traditional wired networks, is been implemented widely in E-Commerce, E-Government like businesses, campuses and governments etc. While the path of development of the wireless network is left behind and the management solutions for wired networks cannot be applied easily to wireless networks. Capsa WiFi is the powerful and easy-to-use wireless network analysis system, which provides complete wireless traffic capture, monitor and analysis solutions. Capsa WiFi can easily be used to capture and analyze 802.11 a/b/g/n wireless packets from AP(s), including data, control and management frames. Capsa WiFi inherits all the good natures of flexibility and usability from its predecessor Capsa to provide up-to-date wireless network data capture and analysis performance.

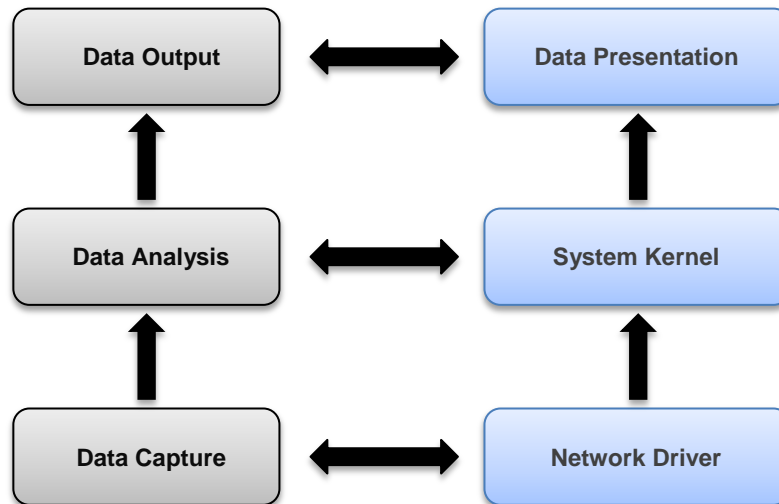
Capsa WiFi seamlessly integrates wireless analysis into the portable analysis platform of the wired analysis solution. Capsa WiFi is able to automatically scan and identify the APs around, and users can read the properties of the APs from the display, i.e. SSID, BSSID, protocol type, channel, encryption status and signal strength, which enable professionals to focus on to analyze and troubleshoot on specific wireless networks.

Capsa WiFi is the professional yet easy-to-use portable wireless network analysis product for wireless network administrators, security specialists and those who want to look into the wireless networking etc. This product, with its wireless driver developed on the latest Network Driver Interface Standard (NDIS) 6.0 framework, is compatible with Windows Vista and Windows 7 and support most popular wireless adapters in the market. While most of the wireless network analyzer of this kind is still running on previous generation of NDIS 5.0 which means that they only support some specific chosen network adapters.

How to Work

System Architecture

The same as analysis of wired networks that the wireless network analysis program has to start from capture of the wireless traffic. The wireless driver at the bottom-level is the core module that detects and captures the data transmitted on air. And then all data are forwarded to high-level modules to be analyzed, summarized and outputted on screen. The figure below presents the system architecture of the product.



(Figure 1 – System Architecture)

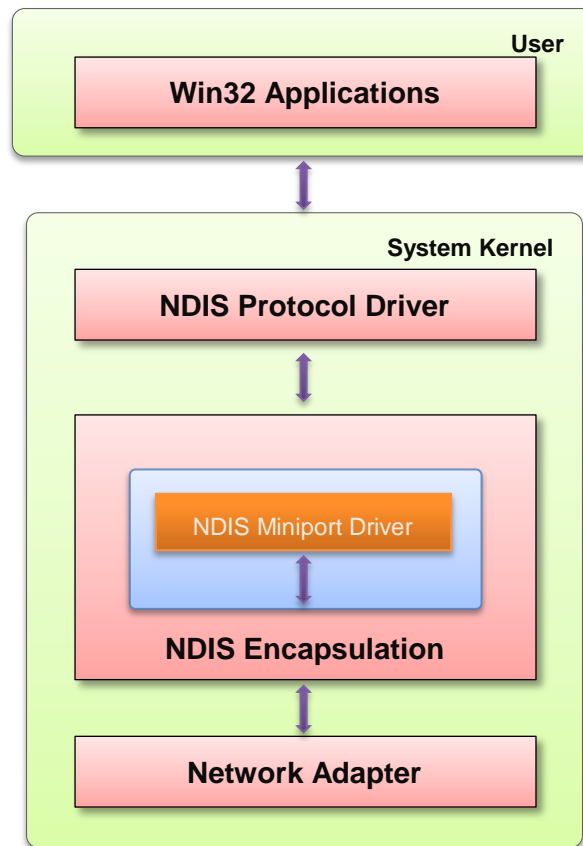
1. Network Driver is responsible for wireless network traffic capture and ensuring the data is accurate and complete.
2. All the captured data is delivered to the analysis modules for real time diagnosis and analysis, i.e. diagnosis module, statistic module and packet decoding module etc.
3. Finally the analysis results are outputted to user interface and/or to hard disk.

Data Capture

Before analyzing packets, Capsa WiFi needs to collect the transmitted packets in wireless networks. Capsa WiFi captures wireless traffic by any of the following two modes:

1. Install Colasoft NDIS Protocol Driver on Windows, and it collects data from the wireless adapter.
2. Install Colasoft NDIS Intermediate Driver on Windows, and it pulls data from the wireless adapter.

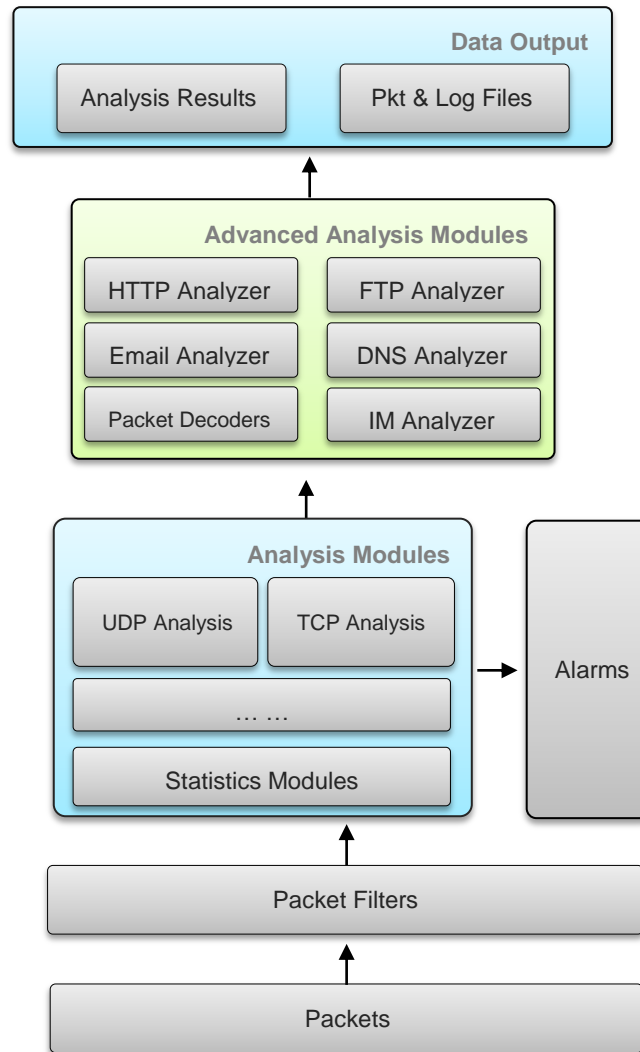
By default, Capsa WiFi collects traffic from Colasoft NDIS Protocol Driver. The efficiency of data capture at the ground level is crucial to the following analysis missions. Thus, filters are implemented on this level to get rid of the irrelevant packets in case the waste of the resource to transfer data from driver level to application level. The following figure outlines the data capture process of Capsa WiFi.



(Figure 2 - Data capturing process)

Data Analysis

When the driver gets a packet matching filtering conditions, it immediately passes the packet to the system kernel for further analysis. The analysis modules include statistics, in-depth packet inspection, packet decoding and protocol analysis etc. The flowchart below shows the packet analysis processes of Capsa WiFi.



(Figure 3– The data analyzing process)

Data Presentation & Output

After the processes of data analysis shown in figure above, all the analysis results, statistics are presented in forms of graphs, lists and reports on the screen. The analysis contents presented including packet decoding, nodes statistics, protocols, IP, TCP flow, conversations and logs.

Key Features

Colasoft Capsa WiFi enhanced many powerful features, including some unique features different from other wireless sniffer products.

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 WiFi helps to measure applications performance, monitor network activities, troubleshoot network problems, and evaluate network security. Capsa WiFi has been launched with seamless Wi-Fi technology adoption for 802.11 a/b/g/n networks.

Compatible with Most Popular Wireless Adapters

Conformance to the latest Network Driver Interface Specification (NDIS) 6.0 library, Capsa WiFi will run on almost all popular wireless adapters in the market, which means almost every wireless card working under Windows Vista and Windows 7 will work with Capsa WiFi. Most wireless solution providers in the market require a few dedicated wireless cards from certain producers. No need to waste your time and budget on additional wireless adapters with Capsa WiFi.

Multi-AP Wireless Packet Capture

All live access points around you can be scanned by Capsa WiFi. You are able to capture wireless traffic from a single AP, or from multiple APs (must be on the same channel). With the powerful 1000Mbps packet processing capability inherited from Capsa network analyzer, Capsa WiFi will not miss a single packet on-the-fly.

Efficient WEP/WPA/WPA2 Decryption

Capsa WiFi will be 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 WiFi will identify and match the encryption type of keys automatically.

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 gain access to 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.

Logs for User Activities

Log is one of the most useful features for Capsa, it is used to monitor and audit the user activities of DNS queries, SMTP and POP3 emails, FTP operations, MSN (Microsoft Live Messenger) and Yahoo Messenger. All activity logs can be saved to files automatically, and even the content of each email can be saved as well. It provides more detailed information and empowers administrators to track and audit common online activities of every user in their wireless networks.

Expert Diagnosis

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

Alarms: Alerts on Abnormal Traffic

In Capsa fault management system, an alarm will be triggered for an event. Whenever there is a service outage or network

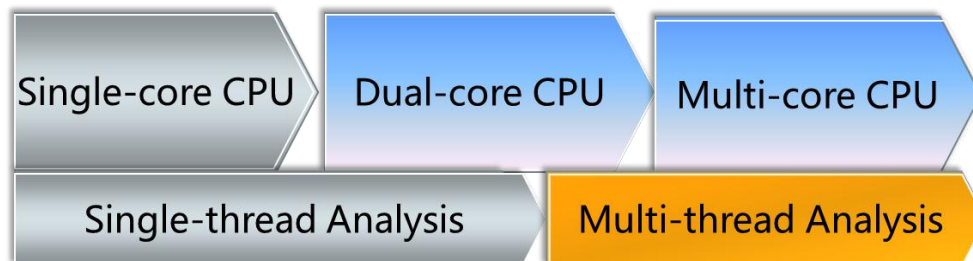
violation, Capsa WiFi notifies you by pop-up notifications to enable more efficient and reliable fault management. Capsa user can deal with the anomalies at the first place. Alarm rules are applied for each MAC address, IP address and protocol. Capsa users can check and track the alarm logs for reference.

Colasoft Packet Analysis Engine (CSPAEE) II

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

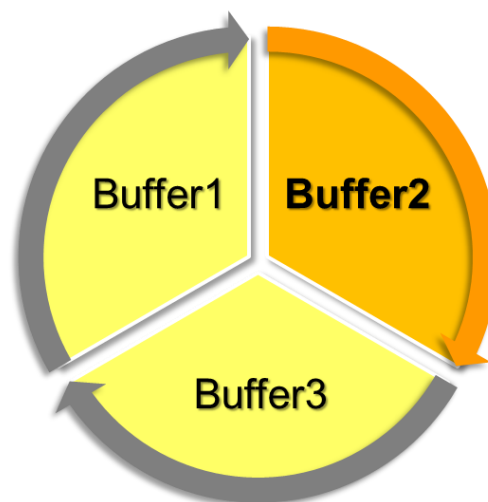
Multi-Thread Analysis

Upgrade single-thread analysis to multi-thread analysis technology, which take full advantage of the processing ability of multi-core CPU.



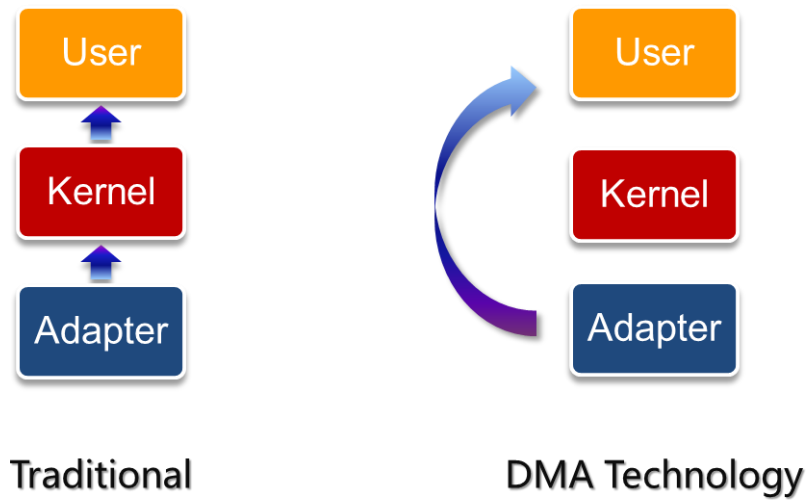
Multiple Cycle Buffer (MCB)

- Cycle use of multiple cache buffer
- Synchronous data analysis and data accessing, avoid latency between 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

- Dynamic create protocol tree structure
- Effective identify protocol and sub-protocol types
- Support user protocol definition that Capsa WiFi can recognize customized protocols

System Specifications

Comprehensive traffic statistics

- Total network traffic summary
- Total network traffic volume
- Broadcast traffic volume
- Multicast traffic volume
- Internal traffic volume
- Traffic volume of an IP address
- Traffic volume of a MAC address
- Traffic volume of a group
- Traffic volume of a VLAN
- Traffic volume of a service (protocol)
- Ingress (downlink) traffic volume
- Egress (uplink) traffic volume
- Ingress (downlink) packets volume
- Egress (uplink) packets volume
- Total packets count
- Physical layer conversation statistics
- IP layer conversation statistics
- TCP conversation statistics
- UDP conversation statistics
- Packets per second (pps) statistics

- Ingress traffic/egress traffic ratio (bit & bytes)
- Ingress traffic/egress traffic ratio (packets)
- IP country group
- Traffic, protocols and diagnosis alarms

Expert network problem diagnosis

- ARP scan
- ARP Man-in-the-middle attack
- ARP spoofing attack
- TCP port scan
- UDP port scan
- ICMP scan
- Data link layer diagnosis
- IP layer diagnosis
- Transport layer diagnosis
- Application layer diagnosis
- P2P file sharing
- IP address conflict
- Network loop
- Worm activity
- DNS service fault
- Email service fault (SMTP & POP3)
- HTTP service fault
- FTP file transfer fault
- Proxy service over port 80, 23 , 53, 110
- Abnormal traffic diagnosis
- Spam traffic diagnosis

Customizable protocol analysis

- Identify user-defined protocol
- Identify network service
- Analyze network service
- Analyze bandwidth consumption
- Summarize packets number
- Locate hosts running a specific service
- Decode protocol with HEX, ASCII and EBCDIC
- Identify abnormal protocol
- Identify packets with forged data
- Display protocol in OSI 7 layer structure

Conversation analysis

- Conversation between two MAC addresses

- Conversation between two IP addresses
- TCP conversation and transaction
- Reconstruct TCP traffic
- TCP packets sequence check
- UDP traffic
- BitTorrent traffic
- Network communication in matrix map
- TCP time sequence chart

Security analysis

- Fast spot network attacks
 - Fragment attack
 - TCP scan
 - UDP scan
 - ICMP scan
 - Email worm
 - DoS attack
 - MAC flooding attack
 - Suspicious conversation
 - Plain text transmission
 - Unauthorized access
 -
- Other abnormal network activities
- Potential network security threats
- Website security evaluation
- Email security evaluation
- DNS security evaluation
- FTP file transfer security evaluation
- Terminal security evaluation
- Network security baseline

Performance evaluation

- Evaluate the egress bandwidth demand
- Evaluate the egress bandwidth utilization
- Evaluate internal bandwidth use
- Evaluate packet size distribution
- Evaluate network upgrade performance
- Analyze TCP transaction performance
- Evaluate mission critical traffic and non-business traffic
- Evaluate network transmission performance
- Baseline network performance
- In-depth analysis of application performance

Product Specifications

Operating Systems

- Windows Vista and 64-bit Edition
- Windows 7 and 64-bit Edition

System Requirements

Minimum

- CPU: P4 2.8GHz
- RAM: 2GB
- 100 MB free disk space
- Internet Explorer 6.0

Recommended

- CPU: Intel Core Duo 2.4GHz
- RAM: 4GB or more
- 10 GB additional space for packet files and logs
- Internet Explorer 6.0 or higher

Supported Wireless Networks

Complete 802.11 a/b/g/n wireless networks transmitting on 2.4 GHz and 5 GHz bands.

Data Rates

- 802.11a: 6, 9, 12, 18, 24, 36, 48, 54, 72, 96, 108 Mbps
- 802.11b: 1, 2, 5.5, 11 Mbps
- 802.11g: 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 48, 54 Mbps

Supported Wireless Adapters

All integrated, USB, ExpressCard and PCI wireless adapters with Network Driver Interface Specification (NDIS) 6.0 driver library.

Supported Encryption Types

- WEP - 64, 128, 152 and 256-bit
- WPA
- WPA2

To decrypt packets, a predefined decryption key is required.

TCP Reconstruction Formats

- ASCII
- EBCDIC
- Unicode

Supported Protocols

IP, PPP, ARP, MPLS, RARP, VLAN, PPPoE, ARP, RARP, ICMP, TCP, BGP, Finger, FTP, HTTP, POP3, TELNET SMTP, UDP, TFTP, BOOTP, CIFS, DNS, SSH, DHCP, SMB, NetBIOS, NBDGM, NBNS, NBSSN, IPX, SPX, AH, ICQ, ESP, GRE, OSPF, IGMP, HSRP, RADIUS, RIP, NCP, SAP, LPD, COPS, L2TP, MSN, PPTP, SCTP, VRRP, Gopher, ICP, eMule, MSSQL, BitTorrent, Oracle

Capsa supports over 300 types of protocols and sub-protocols. For more information about the protocols, please visit:

<http://kb.colasoft.com/technical-problems-and-errors/97-supported-protocols>.

Supported Packet File Formats

- Colasoft Packet File (v6) (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt)
- Colasoft Packet File (v7) (*.cscpkt)
- Accellent 5Views Packet File (*.5vw)
- EtherPeek Packet File (V7) (*.pkt)
- EtherPeek Packet File (V9) (*.pkt)
- HP Unix Nettl Packet File (*.TRCO;TRC1)
- Libpcap (Wireshark, tcpdump, Ethereal, etc.) (*.cap)
- Microsoft Network Monitor 2.x (*.cap)
- Novell LANalyzer (*.tr1)
- Network Instruments Observer v9.0 (*.bfr)
- NetXRay 2.0, and Windows Sniffer (*.cap)
- Sun Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

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.

This white paper is owned by 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.

© 2001-2011 Colasoft. All rights reserved.

www.colasoft.com

support@colasoft.com