

IRIS[®] Network Traffic Analyzer

Visual Data Monitoring & Reassembly

Your company is dependent on its systems running smoothly and securely at all times. Unfortunately, the origins of most security or performance issues — whether due to malicious acts, user non-compliance or simple bandwidth misallocation — generally lie beneath the surface of your network.

Created by eEye[®] Digital Security, a leading developer of advanced network security products, Iris[®] is a highly sophisticated yet simple-to-operate network traffic analyzer. Iris allows you to easily examine the inner workings of your network, making the detective work of pinpointing a security breach or resolving a performance problem quick and effortless.

Quickly Decipher Raw Data

Rather than looking at raw data in packets and trying to understand what it represents, Iris takes network traffic and returns it to its original format with the simple click of a button. With Iris, you will be able to read the actual text of an email — as well as any attachments — exactly as it was sent. Iris will reconstruct the actual HTML pages that your users have visited and simulate cookies for entry into password-protected websites. Iris will even display instant messaging communications from both sides of the conversation.

Record & Playback Network Traffic

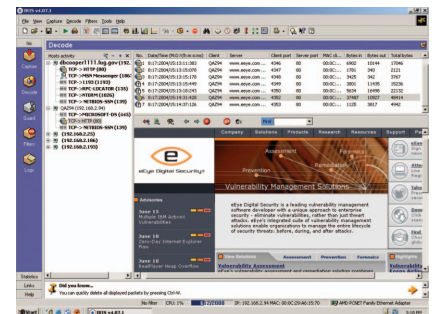
Iris functions similar to a VCR, recording communications data traveling across your network and playing it back at a later time or in real time. Iris allows you to take traffic captured in one area of your network and play it back in another to perform such tasks as stress-testing your network, verifying service levels, and monitoring applications in development. You can replay capture files created by another network traffic analyzer and perform data mining functions such as searching for keywords or reviewing traffic statistics for a complete analysis of the saved traffic.

Comprehensive Statistical Measurements

Iris provides a larger variety of statistical measurements than any other traffic analyzer available, providing information on protocol distribution, top hosts, packet-size distribution and bandwidth usage. By regularly analyzing how systems are being used, you can proactively identify and take steps to eliminate issues before they can result in major downtime for your users. You'll also be able to better maximize bandwidth across the network, reallocate resources and more effectively plan for future growth.

Fast Facts

- Runs on Windows 95/98/NT/2000/XP
- Provides instant network data capture and the ability to decode traffic in real time
- Records and replays traffic for a complete audit trail of suspicious network activity
- Helps identify performance problems before they result in network downtime
- Includes robust scheduling, alerting, and statistical reporting capabilities



eEye Digital Security[®]

IRIS[®] Network Traffic Analyzer

Additional Features and Benefits

- **Statistics and Reports**

Iris provides DNS names and comprehensive statistical measurements. The metrics can be viewed in an assortment of graphical formats (e.g. pie charts, bar graphs, etc.) and include:

 - *Protocol Distribution Stats*
Reports network usage based on MAC, IP and IPX layer protocols.
 - *Top Host Statistics*
Provides an analysis of the IP Layer traffic statistics collected for each host in real time and is ordered by the most "talkative" hosts.
 - *Size Distribution Statistics*
Displays the number of packets with sizes in six different ranges.
 - *Bandwidth Usage*
Charts the number of packets per second and bytes per second flowing across the network in real time.
 - *Traffic Reports*
Complete traffic data that can be viewed in a browser, saved, printed, or copied into another program.
- **Data Reconstruction**

Iris takes raw data in packets and turns it into complete HTTP, SMTP and POP3 sessions in their original format. The following are some of the protocols Iris reconstructs:

 - *Outgoing and incoming email messages*
The text of the message is readable as well as the subject and recipient. Iris will launch an email client to open the message, as well as any attachments, exactly as they were sent.
 - *Web browsing sessions*
Reconstruction of HTML pages in their original format.
 - *Instant messenger exchanges*
Iris will reconstruct all IM communications from both sides of the conversation.
 - *Non-encrypted web-based email*
 - *FTP transfers*
- **Network VCR**

Iris records communication data traveling across your network and plays it back either in real time or at a later time.
- **Packet Manipulation and Forging Capabilities**

Iris provides the ability to create custom packets to send across the network.
- **Extensive Filtering Options**

Iris allows you to capture specific data through packet filters based on hardware or protocol layers, keywords, MAC or IP addresses, source and destination port, custom data and packet size.
- **Post-Capture Data Analysis**

Iris' Data Miner can process any amount of data, from a single traffic file to large amounts of captured data, at one time. This feature is available for comprehensive analysis of saved traffic.
- **Protocol Decoding**

Iris organizes captured packets and categorizes them by protocol such as HTTP, PPOE, and SNMP, providing a list of all web-browsing sessions, all email grouped by incoming and outgoing, and more.
- **Powerful Sniffing and Spoofing Engine**

Iris can handle as much traffic as your network generates and still write logs and decode traffic in real time. The Iris engine can handle up to 9,000 packets per second.
- **Scheduling Function**

Iris is easily configured to automatically run and capture packets in specific time frames.
- **Alerting Capabilities**

Iris' Guard module monitors all connections to the local machine and can alert when a specific connection is detected.
- **Reconstruct TCP Sessions**

Iris support several Protocol Decoders through an open plug-in based architecture, including: ARP, CIFS, DNS, Ethernet II, 802.3, 802.2, ICMP, IP, TCP, UDP, Novell NetBIOS (IPX), SAP (IPX), RIPX (IPX), BCAST (IPX), NBDGM, NBNS, NBSS, NetBIOS, SMTP, AOL AIM, MSN Messenger, BOOTP/DHCP, RARP, POP3, SMTP, LCP (Link Control Protocol) (PPP), PAP (Password Authentication Protocol) (PPP), PPOE (PPP over Ethernet) (PPP), SMB, NNTP.

System Requirements

- Windows 95/98/Me/NT/2000/XP
- Internet Explorer 4.01 with comctl32.dll v5.0+ or Internet Explorer 5.0+
- Minimum System — Pentium 166, 32MB RAM, 1GB HDD
- Recommended System — Pentium 400, 128MB, 10 GB HDD



About eEye Digital Security

eEye Digital Security is a leading developer of network security products that deliver unsurpassed levels of vulnerability protection before, during and after malicious attacks. Driven by the world-renowned eEye Research Team, the company has won numerous awards and recognition in the field of network security, including the recent top 10 recognition in the Red Herring Top 100 Innovators awards for 2004. A global company with offices, partners and distribution channels around the world, eEye helps protect the digital assets of major corporations, educational institutions, and government entities in over 80 countries.

eEye Digital Security
www.eEye.com

U.S. Tel: 1.866.339.3732
N. America: 1.949.900.4100
Geneva: +41 22.718.7700
London: +44 (0) 208.956.2270

N. America: sales@eeye.com
International: sales.eu@eeye.com



eEye Digital Security[®]

VULNERABILITY IS OVER