



IRISTM Network Traffic Analyzer

Visual Data Monitoring & Reassembly

Your company depends on you to keep 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'll 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 key words 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
- Instant network data capture tool able to decode traffic in real-time
- Record and playback traffic for complete audit trail of suspicious network activity
- Identify performance problems before they result in network downtime
- Robust scheduling, alerting, and statistical reporting capabilities



eEye[®] Digital Security

IRIS™ Network Traffic Analyzer

Additional Features and Benefits

- **Statistics and Reports**

Provides DNS names and more statistical measurements than any other traffic analyzer. 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 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*
These are viewable in a browser window from which you can save the report, print, or copy into another program.
- **Data Reconstruction**

Takes raw data in packets and turns it into complete HTTP, SMTP and POP3 sessions in their original format. The following are viewable packets:

 - *Both outgoing and incoming email messages*
The actual 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 the actual html pages in their original format so the actual page the user visited is viewable.
 - *Instant messenger exchanges*
Iris will reconstruct all IM communications from both sides of the conversation.
 - *Non-encrypted web-based email*
 - *FTP transfers*
- **Network VCR**

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**

Able to create custom packets to send across the network.
- **Extensive Filtering Options**

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**

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

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

Can handle as much traffic as your network generates and still writes logs and decodes traffic in real time. Iris has a fast packet injector that handles up to 9,000 packets per second.
- **Scheduling Function**

Easily configured to automatically run and capture packets only in certain time frames. Can automatically capture data day or night during any number of time frames per week.
- **Alerting Capabilities**

The Guard module monitors all connections to your computer, and can alert when a specific connection is detected.
- **Reconstruct TCP Sessions**

Protocol Decoders through an open plug-in based architecture: 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), PPPoE (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 advanced network security products that deliver unsurpassed levels of protection against malicious attacks and undetected vulnerabilities. A global company with offices in the US and throughout Europe, eEye helps protect the digital assets of major corporations and government entities in over 40 countries.

eEye Digital Security
www.eEye.com

U.S. Tel: 1.866.339.3732
N. America: 1.949.349.9062
Geneva: +41 22.787.2282
London: +44 (0)20.7470.5630
Paris: +33 1.58.71.40.31



eEye® Digital Security

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

VULNERABILITY IS OVER