

Retrospective Network Analysis

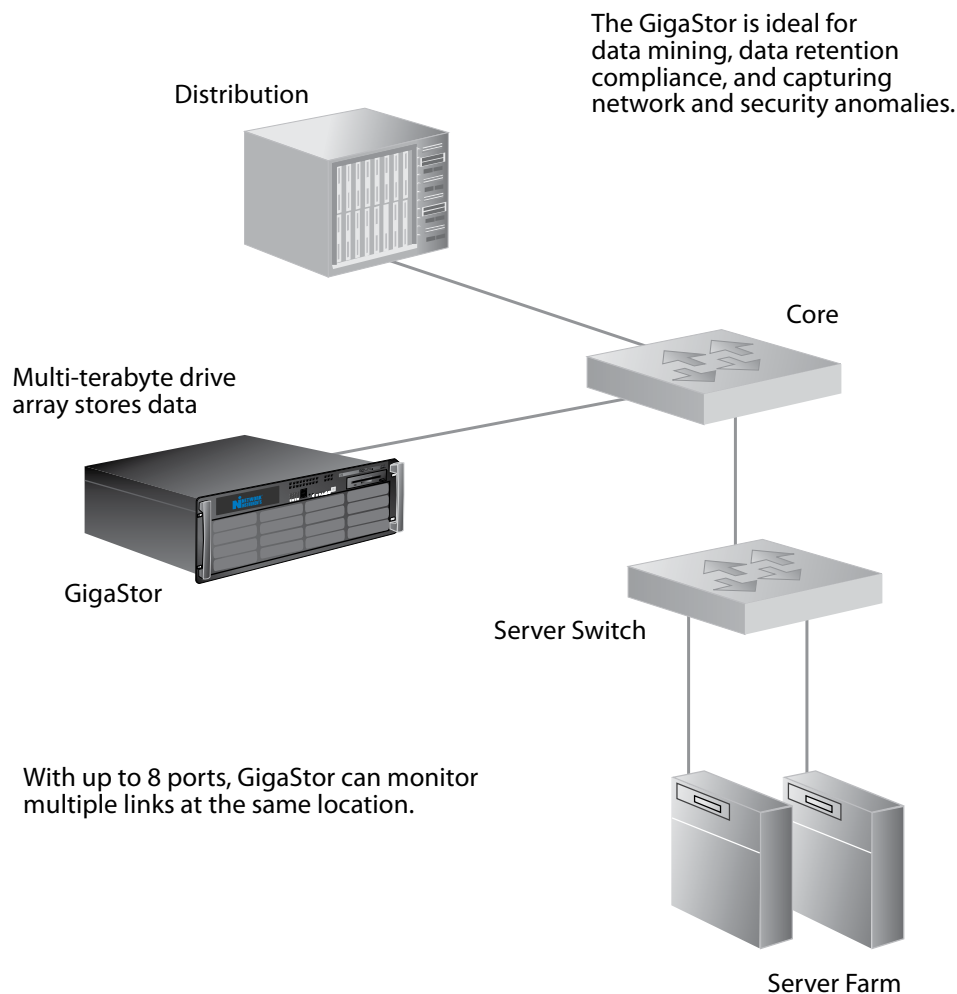
Stop waiting and start solving. Isolating and troubleshooting network, application, and security issues is simple when you can go back in time with GigaStor. GigaStor captures every transaction, every packet, every protocol, and it can store hours, days, weeks—even months of traffic. With this data and GigaStor's unique, time-based navigation, your network team has the benefit of 20/20 hindsight to tackle every network problem and anomaly. Now it is easy to “rewind” your network, determine the source of the problem, perform comprehensive analysis, and move on.

Turn Back Network Time

- Solve intermittent problems without having to recreate them
- Document compliance violations and provide evidence
- Isolate application issues by locating the problematic transaction
- Identify and view attacks and security anomalies in context of other network activities
- Answer VoIP call quality concerns by tracking over 70 VoIP metrics

High-Performing Appliances

- Capture 4, 8, or 12 terabytes of data or offload to a SAN
- Portable appliance for performing in-the-field forensics
- Monitor up to 8 ports for any combination of SPAN sessions, full-duplex links, and trunked links
- Benefit from long-term, real-time, and post-capture analysis
- Perform network and security forensics for deep-level packet investigations
- Supports gigabit, 10 GbE, WAN, LAN, Fibre Channel, and wireless links



Quickly identify and resolve any issue with GigaStor's massive data storage and comprehensive analysis.

Network Forensics

- Over 590 protocols decoded and 570 Experts to quickly isolate and identify network and application performance issues
- With Experts identify application problems, view application session flows graphically, reconstruct data packets, and isolate transaction delay
- For connection-oriented problems, right-click for further analysis

Security Forensics

- Identify attacks by comparing historical traffic against Snort rules
- Drill down to the packet level on any breach to determine the source and time of the incident
- Identify compromised machines and network infrastructure
- Validate and document compliance and security issues
- View security and access violations in the context of what else was happening on the network

Application Forensics

- Go back in time, track application communications, and pinpoint problems using Application Analysis
- Obtain statistics on errors, review application response times, and obtain in-depth application performance analysis
- In-depth analysis of SQL, Oracle, MS Networking (SMB), VoIP, DNS, FTP, HTTP, POP3, Telnet, SMTP, SNMP, MS Exchange, and Citrix

High Capacity Storage

- Capture and save up to 12 TB of network data. Hours, days, or weeks worth of data can be stored depending on utilization.
- Offload to a SAN for virtually unlimited storage potential

VoIP Performance Analysis

- Monitor H.323, SIP, MGCP, SCCP (Cisco "skinny"), Avaya CCMS, Nortel UNISim, and Mitel traffic
- Monitor calls with over 70 in-depth VoIP metrics
- Score call quality based on industry standards
- Acquire relevant actionable detail and diagnostics
- Save and play voice conversations or streaming video

Data Stream Reconstruction

- Rebuild communications from captured traffic
- Reconstruct web pages, e-mails, IM conversations, documents, and VoIP calls
- Document policy violations, investigate network problems, and identify unauthorized activities

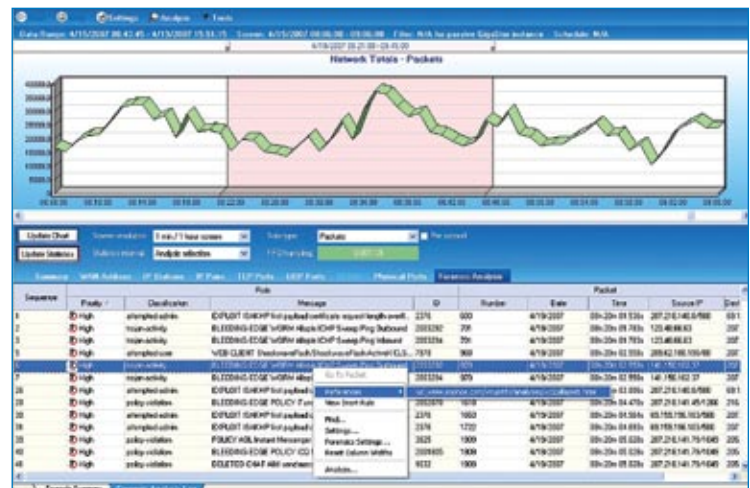
Deployment

The GigaStor is offered in rackmount and portable versions. The rackmount version easily integrates into your rack system with its standard 3U or 4U form factor. The appliance then reports back to any Observer® Expert or Observer Suite console on the network.

If mobility is a concern, Network Instruments offers GigaStor Portable, a luggable, all-in-one unit for performing in-the-field forensics. The portable unit includes 2 TB of total storage, Observer Suite, and GigaStor Probe software in a self-contained system for collecting, analyzing, and displaying all network data.



Use GigaStor to select a time period and quickly isolate and resolve network and application problems.



Security Forensics determines whether a security breach occurred by comparing historical traffic against a Snort-rules list of attacks and anomalies.

Comprehensive Analysis with Observer

- Nanosecond resolution for enterprise-level networks
- Graphical filter rule editor for easily creating complex filters
- Over 590 protocols and countless sub-protocols decoded
- Over 570 Expert events to speed troubleshooting
- Triggers and Alarms for immediate alerts on activities or errors
- NetFlow and sFlow® collection and reporting
- MPLS Expert analysis and reporting
- MultiHop analysis tracks conversations through up to 10 segments

GigaStor: Get proof. Take action. Move on.

By capturing and saving every packet traversing the network, GigaStor makes it easy to “rewind” your network, determine the source of the problem, perform comprehensive analysis, and move on. Use GigaStor to provide complete visibility into any network, application, or security problem. For example:

Network Troubleshooting

The help desk receives a notice of poor call quality sporadically impacting a specific user’s VoIP phone. All other phones are functioning properly, and aggregate statistics show that overall VoIP quality is high. A quick check of network statistics reveals that while some links have periodically experienced high usage, overall network usage appears to be normal.

Resolving network troubles with GigaStor is an easy three-step process:

1) Isolate the timeframe and user

Use GigaStor’s unique time-based navigation system to select a timeframe around the problem and the user reporting the problem.

2) Drill down on the call

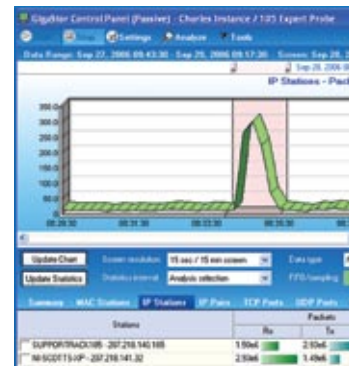
Select the specific time of interest around the user’s VoIP call attempt.

3) Let the Expert do the work

Use GigaStor’s comprehensive VoIP Expert with call detail records and aggregated VoIP health statistics to diagnose the issue. In this case the engineer determined based upon Expert analysis that the phone set was mistakenly configured to send packets with an incorrect TOS/Precedence Setting. When trying to converge over a router during peak usage, the lack of QoS resulted in contention, which caused poor call quality.

1

Isolate



2

Drill Down



3

Resolve

Compliance

GigaStor can provide network visibility and document any potential policy violation.

An employee was being reviewed for possible dismissal by human resources. Among the offenses, the employee was accused of browsing prohibited web sites. The network team was tasked with providing conclusive proof to HR of the infraction; providing only domain names and web addresses was not enough.

1) Isolate the timeframe

Rather than starting a packet capture and monitoring on-going activity, the administrator uses GigaStor to quickly isolate the employee’s most recent web activity. Using the GigaStor control panel, select the timeframe when the selected activity occurred.

2) Drill down on user data

Next, the engineer selects the specific user, whose traffic patterns are graphed to display periods of excessive activity from the system in question. The filtered data reveals all the web sites visited by the employee.

3) Get proof

By right-clicking on any Internet address, GigaStor can reconstruct the captured packets into the original web pages. The reconstructed web pages offer solid proof that the employee visited a prohibited site.

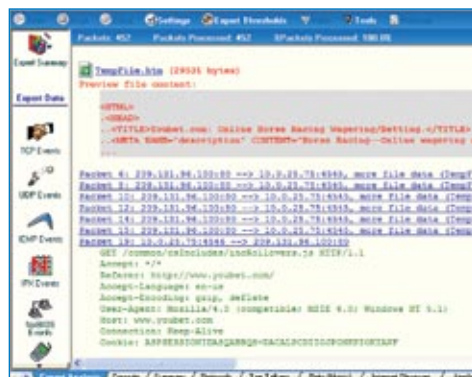
Isolate

1



Drill Down

2



3

Document



Gen2™ Technology

All Network Instruments full-duplex, gigabit, 10 GbE, and Fibre Channel GigaStor products include the Gen2 capture card designed by Network Instruments. The card takes advantage of 64-bit Observer to guarantee the fastest real-time processing and the largest capture buffers (124 GB) available. The Gen2 card delivers analysis port flexibility with the ability to monitor up to eight-gigabit ports (up to two ports per box for 10 GbE links) for any simultaneous combination of SPAN sessions, full-duplex connections, or trunked links. Gen2 also ensures accurate timestamping across multiple links by relying on one card (one clock) with nanosecond resolution to timestamp data across each link.



Gen2 Gigabit Capture Card

nTAPs Ensure Complete Captures

Using included nTAPs guarantees that all network traffic is visible to the GigaStor, including errors found in the physical layer. An nTAP™ passively transmits both the send and receive data streams simultaneously on separate dedicated channels, ensuring GigaStor records all data.

nTAP Advantages:

- Provides access to all network traffic including physical-layer errors
- Allows you to connect and disconnect the GigaStor from the network without breaking the full-duplex signal
- Supports redundant failover links on the network

Every GigaStor is equipped with multiple nTAPs (depending upon configuration). With an nTAP, you can see the whole picture, eliminate the risk of an attack (nTAPs do not have IP addresses), and never have to worry about interfering with network performance.

GigaStor Hardware Options



3U appliance captures up to 4TB of data



4U appliance captures directly to a SAN



4U appliance captures up to 8 TB or 12 TB of data



GigaStor Portable captures data in the field

GigaStor Rack Mount Specs

Platform 3U or 4U Rack Mount Probe

System Specs A complete appliance, running 64-bit Windows XP, high-performance RAID array, includes 10/100/1000 Ethernet management NIC, utilizes Gen2 capture card

GigaStor Portable Specs

Platform Luggable, all-in-one unit

System Specs Includes Observer Suite and GigaStor Probe Software. Capture card and memory buffer vary based upon configuration

About Network Instruments

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit www.networkinstruments.com.

Solution Bundles

Contact a Network Instruments representative or dealer to ask about product bundles that cover all of your network management needs.



Corporate Headquarters

Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801

www.networkinstruments.com

European Headquarters

Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881

www.networkinstruments.co.uk