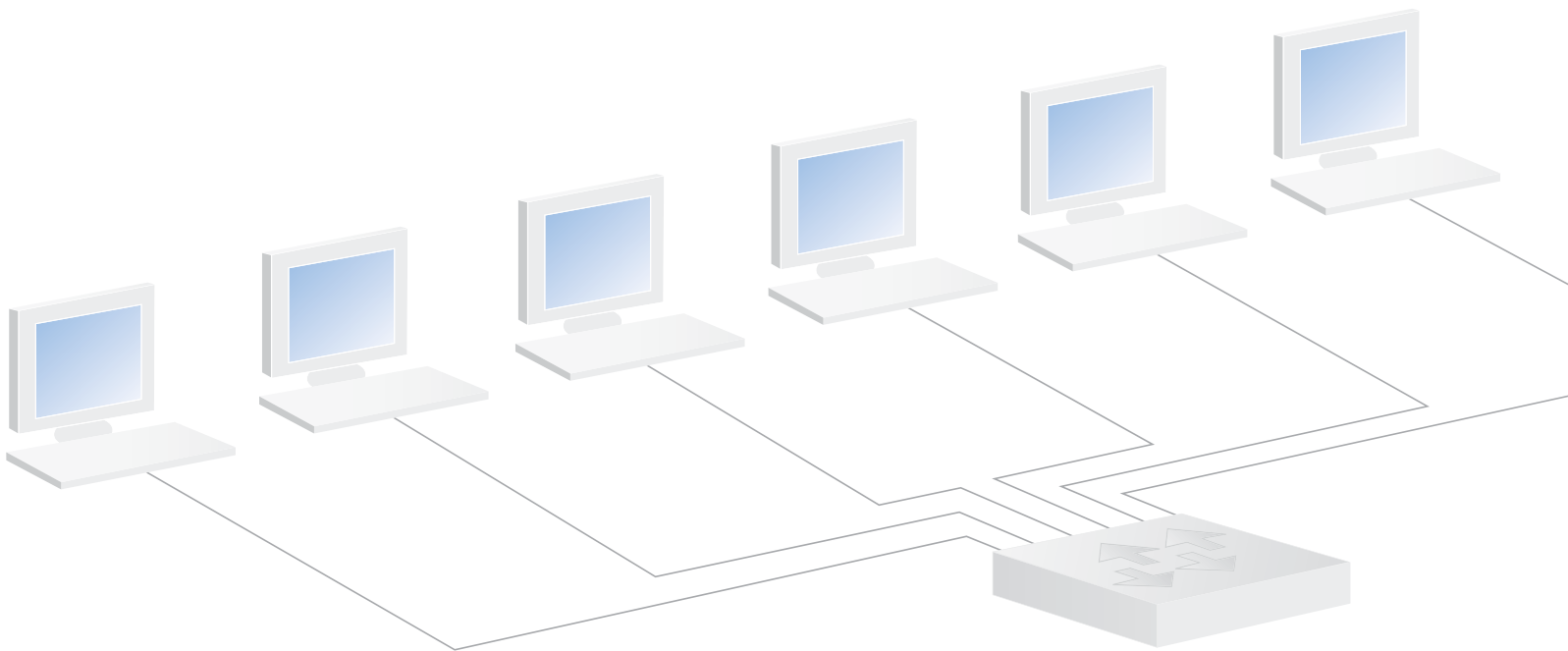


## Network Security Forensics

As security threats grow in complexity and organizations face stringent regulatory requirements to audit access to private data on the network, organizations require an increased level of network visibility and surveillance. Network security forensics, a new method of capturing and storing every packet traversing the network, has emerged to address this need.



## Summary

The world of network security has become an “arms race.” As organizations tighten their external defenses and install improved countermeasures, threats and attacks evolve to circumvent these security measures. Increasingly, this arms race is taking place in a regulated environment, where government rules such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and the EU Data Protection Directive require organizations to control access to private data and document security breaches.

The continual risk of circumvention and the need to have a record for investigation and compliance purposes is driving demand for a new type of network security monitoring solution known as network security forensics. A network security forensics appliance passively monitors the network, capturing and archiving every packet, transaction, and communication for later analysis. This is the best method for identifying and understanding what occurred during a specific event.

### This paper will:

- Identify the need for a network security camera to capture and archive all network transactions and activities
- Illustrate how network security forensic appliances provide new visibility and evidence for security and compliance investigations
- Highlight real-world examples from clients demonstrating the role network security forensics plays in identifying security and compliance violations
- Provide the key components to look for in any network security forensics solution

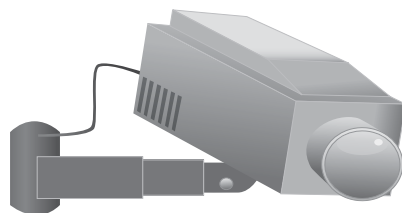


## The Need for Visibility

Network engineers face a variety of changing threats in ensuring their organization is secure. These threats range from hackers seeking to exploit unpatched systems to employees leveraging their “trusted” positions to steal company financial records. Although many organizations have taken significant measures to reduce their exposure to outside attacks, potential threats from trusted employees or contractors looking to exploit their knowledge of internal systems still remain. In addition, due to the evolving nature of security threats, existing security measures may be circumvented.

A need for greater network visibility resulted from these potential security breaches and new regulations that restrict access to customer information and corporate financials. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires that any organization that stores or processes Protected Health Information (PHI) must take steps to guard the data from unauthorized access. Organizations require a new level of network visibility, including data capture and analysis capabilities, to effectively ensure compliance and resolve security issues.

The need for surveillance and recording of business activities can be seen in environments outside networking. Although banks are secured with guards and alarms to prevent robbery, they rely on security cameras to record all activities should a break-in occur. The recording becomes an integral tool to complete the investigation, and to identify ways to prevent future incidents. In the network world, there is a need to capture and store every packet, transaction, and communication traversing the network for later investigation and future attack prevention.



### Where network security forensics is needed:

- Monitoring internal threats
- Documenting evidence for investigations
- Solving the “Whodunnit” mystery
- Regulatory audit compliance for HIPAA, SOX, GLB, and the EU Data Protection Directive
- Complying with corporate HR and acceptable-use policies

Network security forensic tools have emerged to address this need. The appliances are unique in their ability to capture and save terabytes of packet-level data to local disk or SAN. Administrators then select a specific time period of captured network activity, and the appliance sifts through the indexed traffic to identify any anomalous traffic or potential security breach. In analyzing and identifying security events such as an attack, these devices support intrusion detection rules such as Snort, or other signature-based rule systems. In addition to identifying security breaches, forensic tools should have the ability to reconstruct captured packet data into its original format, whether it be an e-mail, IM, web page, VoIP call, or other form of communication.



## Security Scenario

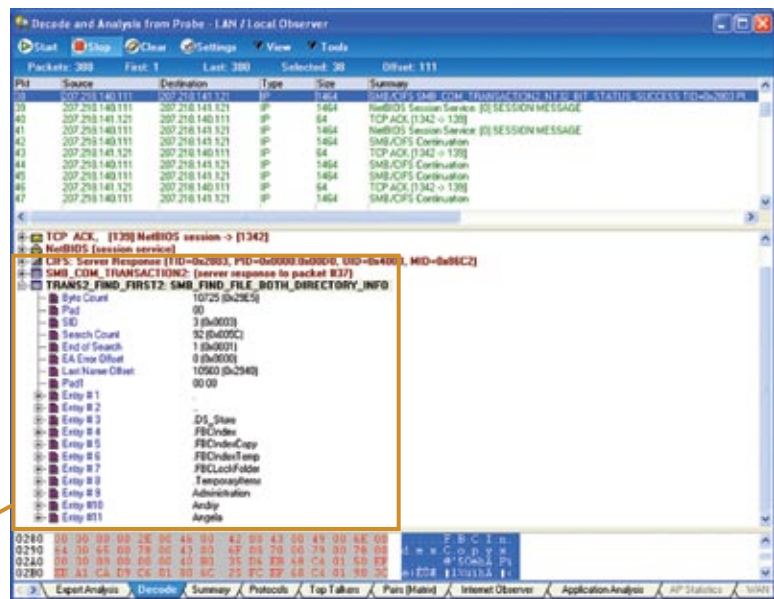
Over the weekend, seemingly random security anomalies began to appear in the organization's DMZ. The intrusion prevention system (IPS) was able to detect and successfully repel the attacks. During the same period, an intruder successfully compromised the default "Admin" account on the company's VPN concentrator without detection. Because the compromise was perpetrated via an encrypted SSL session, it was invisible to the IPS sensor.

After bypassing the perimeter firewall through a created VPN account, the intruder installed applications such as remote control utilities and keystroke loggers. Subsequent malicious activity was then perpetrated against key internal systems using these utilities. All packet-level data and network activities were recorded by the security forensics solution.

To identify the attacks, the network engineer first isolated the timeframe, beginning when the perimeter attacks began, and tracked internal activities over the weekend period. Using the latest intrusion signatures, the selected time frame was analyzed for evidence of exploits, covert communication channels, and unauthorized system access.

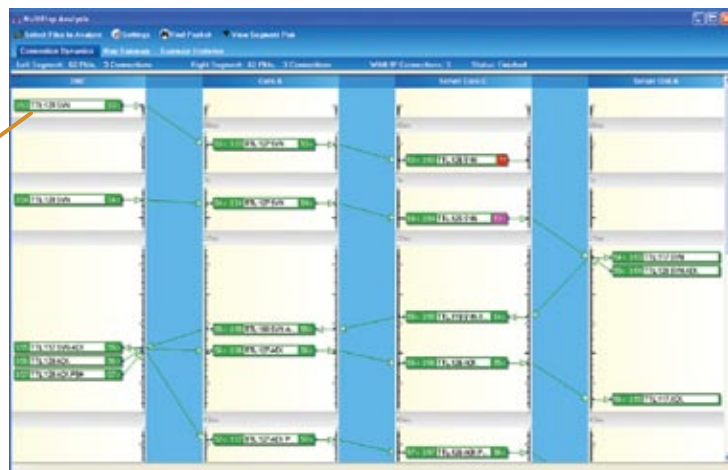
Once the exploit had been identified, the appliance drilled down into the individual frame to isolate any suspicious activities, such as data transfer under false pretenses. In this case, a brute-force password attack was used to access a critical file server.

Attack used to access Windows file system



In addition to documenting specific cases of data theft, the security forensic appliance also identified the intruder's path across the network, allowing the security staff to identify potentially compromised infrastructure.

Follow the hacker's route over the network.

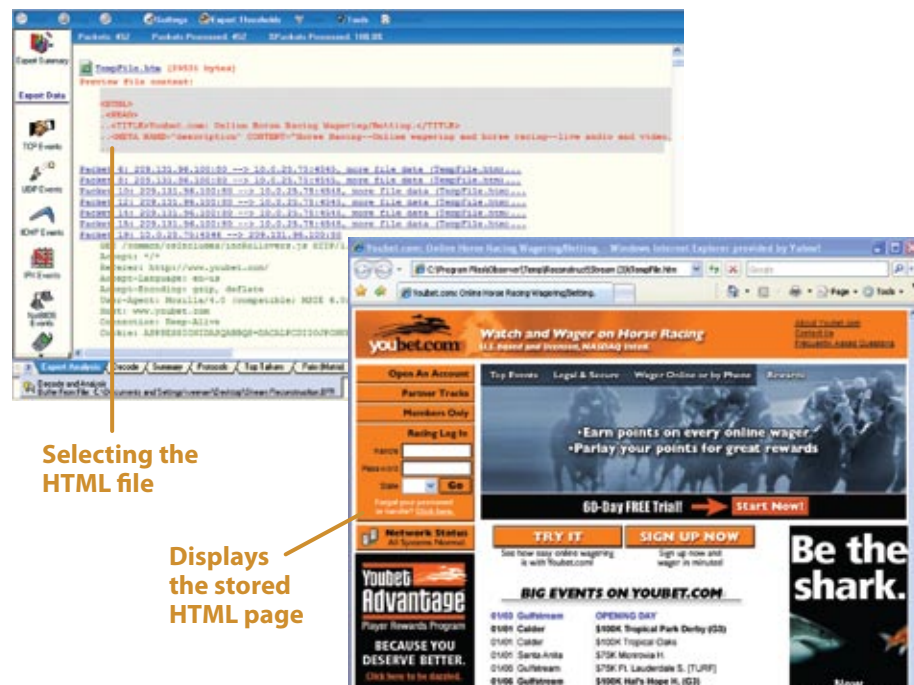


## Compliance Scenario

Security forensics can help document and ensure enforcement of internal HR policies as well as government regulations. At a large financial organization, an employee was being reviewed for possible termination by human resources. Among the offenses, the employee was accused of browsing prohibited web sites on company computers.

The network team was tasked with researching possible offences. In order to terminate the employee, HR needed conclusive proof of the infraction; providing only domain names and web addresses was not acceptable. The network team needed to document the incidents in a manner that would illustrate the activity the employee perpetrated and reduce the risk of a wrongful termination lawsuit.

In this scenario, the network team tracked the user's traffic patterns using the security forensics appliance, which allowed them to identify periods of high bandwidth utilization relative to other users in his department. In addition, attempted downloads of inappropriate content from web sites caught by the organization's web filter could be corroborated and documented. In this case all web sessions were captured and saved by the security forensics device. The specific HTML session was isolated and reconstructed to present the web site including images, exactly as it was when viewed by the user.



Once the employee was confronted by the evidence collected by the content filters and the security forensics appliance, he admitted to using company resources contrary to the company's acceptable use agreement. His employment was terminated with less risk of a legal challenge.

## Conclusion

New security tools will continue to emerge to combat constantly evolving security threats. To effectively address and prevent security breaches requires continuous monitoring and adjustment of infrastructure and policy. If a successful attack is perpetrated against an organization, the monitoring solution becomes even more critical to ensure the attack is accurately identified and appropriate steps are taken to prevent future attacks. Network security forensic devices are uniquely positioned to provide a full view of all activities before, during, and after the event. These tools also have the ability to isolate the breach, identify software, scripts and exploits used; and locate potentially compromised infrastructure.

The ability to capture all packet-level data is also critical to compliance enforcement and the documentation of potential violations. The ability to accurately diagnose the breach or policy violation through reports and reconstructing communications or web sessions provides evidence necessary for proving compliance.

## Security Forensics Checklist

The following is a checklist of key components that you should look for in a security forensics solution:

Network Security Forensics System Requirements	
Minimum storage capacity	4TB
Minimum capture-to-disk rate	250 MBps (2000Mbps)
Write-to-SAN capability	Yes
Data stream reconstruction	Reconstruct HTTP, IM, e-mail, VoIP, and documents
Security event and anomaly detection	Solution should support IDS rules, such as Snort rules
Ability to conduct time-based analysis	Administrator can select the time period for analysis
Handles multiple network topologies	Yes

### 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](http://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](http://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](http://www.networkinstruments.co.uk)