WildPackets®
Illuminate Your Network™

How Network Forensics Can Help Human Resource Compliance

By David Strom

May 2007

WHITE PAPER

Something wrong is happening on your network. Call it human nature or simply a few bad apples, but unless your organization is miraculously different from all others, someone is leaking information, someone else is dabbling in porn, and someone else is probably doing a handsome business on eBay—on one of your servers.

Your organization has policies about this—and your industry may have regulations that pertain, as well. You need to ensure these policies are complied with—or you need to collect evidence to take action when they're not.

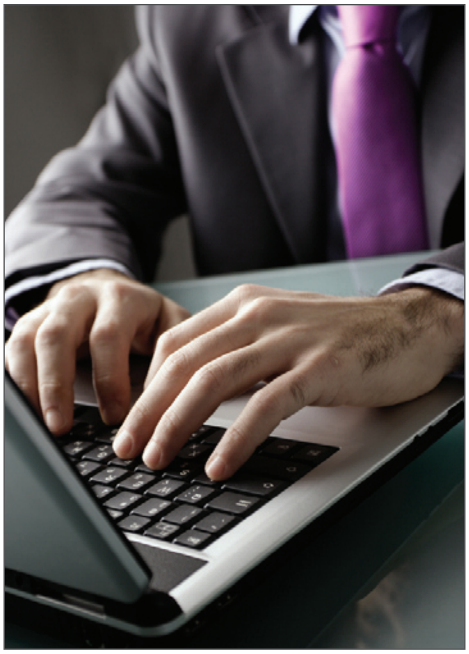
When you suspect something is wrong, do you have the means to conduct an investigation? How do you collect evidence—digital evidence—when there are so many channels of communication (email, Web mail, IM, etc.), and so many places to look on your network?

Time for network forensics.

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.wildpackets.com

Table of Contents

How Network Forensics Can Help Human Resource Compliance



Corporate officers are missing out on one of the most important means of protecting their business networks. It doesn't involve setting up a new firewall or other complex infrastructure, it doesn't cost much in terms of time or capital, and it can be easily administered by fairly low-level technical staff. It goes by the name of network forensics.

The term refers to **the capture and analysis of historical digital evidence that flows through your enterprise network**. The idea has been around for a while under different forms, yet the notion is simple: record every piece of network traffic to a single repository that can be examined after the fact. And by every piece, we mean just that: all emails, all database queries, all Web browsing. Whatever information is traversing your corporate network is recorded into one central place. Forrester Research calls this "digital forensics" and Network General uses the term "business forensics." But the idea is credited (according to searchnetworking.com) to security expert Marcus Ranum: "Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents."

Network forensics has been used in the past for a large class of troubleshooting issues and helps solve various network security problems. For example, forensics could provide information to fix badly behaving network elements: a failing router, a leaky firewall, an overwhelmed email server, an insecure database. It can also be used to fix poor network performance and troubleshoot connection issues, do attack analysis for security exploits, and also benchmark applications that ran across the network. These are still very valid reasons for using network forensics.

But today we need forensics for more business-critical issues that have nothing to do with connectivity, such as for problems that are related to particular criminal or unethical activities that can leave digital footprints. Things such as a rogue employee stealing corporate secrets, harassment scenarios and other inappropriate behavior, compliance lawsuits or the threat thereof, or employees running their own businesses using corporate assets. All of these are situations that can gain from the insights of network forensics.

It can happen to you!

Before you think your company is immune, think about some potential scenarios where you could be liable for legal action. Are you really sure none of these activities goes on inside your company? Are you willing to take the chance that you could be sued in the future over an incident, or that your corporate secrets will remain inside your company and not leak out? Let's look at a few situations:

- An engineer emails your latest product design and plans to his next employer,
- One employee is getting harassing emails from another, or carrying on a love affair with his or her supervisor,
- A marketing manager sends his entire contact database to his private Gmail account so he can use them to start up his own consulting business,
- Two employees are routinely surfing porn sites during their lunch hour, in full view of others in their department,

- A middle manager is running her eBay auction business, storing her digital inventory and accounts on a company-owned machine, and
- Several employees are using their PCs to run peer-file sharing sites, containing music and stolen software code.

"It is time to wake up and realize that there is a lot of stuff like this going on," says John Bennett, VP for Marketing at WildPackets. "Just because it isn't obvious doesn't mean that it isn't happening." These are very real scenarios, and the bigger your company is, the more likely that some of them – if not all – are going on in your buildings, over your networks, and exposing your company to legal and business risks today.

Part of the problem is that we now take our corporate networks for granted, because usually they work reasonably well and without a lot of issues. "We dramatically over engineer our networks, because it is cheaper to do so," says Joel Snyder, the managing partner of network consultancy Opus One. "But in the past we never really have known what is going on on our networks. We need tools that will provide information so we can build more secure and reliable networks."

But another part of the problem has nothing to do with technology, and all about the people that use it. A paper written for the US Department of Defense that studied network data exploits found some interesting conclusions about the types of dissatisfied people that were at the center of these exploits.

- Saboteurs had personal problems outside the workplace.
- Stressful events such as internal reorganizations increase the likelihood of malicious acts.
- Poor work ethics including performance or tardiness were often observed before and during sabotage.
- Insiders had a tendency to "set-things up" such as creating back door accounts.
- Organizations failed to detect or ignored policy rules such as forbidden downloads.
- A lack of access control for both physical locations and on-line computing resources.

"While personal problems can be tough to deal with, especially with touchy regulations like HIPAA, we can deploy tools to help us with technical matters," says Scott Haugdahl, the CTO of WildPackets.

That's the problem that network forensics can help solve. But the issue with forensics is all about timing: the digital evidence needs to be collected now, before any specific event actually happens. Just like laptop-theft prevention programs that are only useful once someone's laptop is stolen, network forensics relies on this massive data collection effort before a crime is committed or an employee is caught up in a sexual harassment lawsuit.

Sexual harassment and discrimination

Speaking of which, sexual harassment continues to be a major issue for corporations. In 2006, the U.S. Equal Employment Opportunity Commission received more than 12,000 filings of harassment, recovering nearly $50 million in damages. These days, harassment can occur in a variety of circumstances:

- The victim as well as the harasser may be of either sex, and could be of the same sex.
- The harasser can be the victim's supervisor, an agent of the employer, a supervisor in another area, a co-worker, or a non-employee.

- The victim does not have to be the person harassed but could be anyone affected by the offensive conduct.
- Harassment may occur without any economic injury to the victim.
- The harasser's conduct must be unwelcome.

The courts have broadly expanded the reach of the Civil Rights Act of the 1960s over the years. While outside the scope of this paper, there are numerous rulings by state and federal courts that have made it easier for victims to sue and recover damages from their employers. And the U.S. EEOC themselves have said, "Prevention is the best tool to eliminate sexual harassment in the workplace."

The same applies to discrimination cases, where the original civil rights legislation has been expanded over the years and now has fairly broad reach.

In 2006, the EEOC received more than 27,000 complaints and settled more than $60 million in claims. And this figure doesn't include additional punitive damages as a result of lawsuits. Clearly, this can be a significant exposure for many corporations.

Why forensics matters to HR managers

With all of the potential liabilities, Human Resource managers want to capture all kinds of forensic information that can help protect their companies. Part of the problem here is that because the enterprise digital network has become so pervasive, it is being used for the kinds of communications that are harder to track down. And as data leaks occur, you want to be proactive about monitoring your network to understand what kinds of information and how much has been lost.

"Corporations today need the right tools to be proactive in protecting their employees at work, and protecting themselves from litigation," says Mary Ann Miller, the Human Resources manager for the Iroquois Pipeline Operating Company. "With the proliferation of electronic communication in the forms of e-mail, bulletin boards, blogs and instant messaging, the venue of harassment and discrimination has somewhat shifted to a subtler, more evasive area that can be as difficult to track as it is damaging to the business."

Consider the situation where two employees are plotting to start their own company and taking some confidential information with them. In the past, they would use personal Web-based email accounts to avoid leaving any trace of their messages on the corporate email network. But with the right forensic tools in place, this Web-based traffic could be captured and examined to reveal the conversations and guilty parties.

Or how about another situation, whereby an employee brings his infected laptop onto a corporate network and inadvertently installs malicious software that can capture personal or confidential data and automatically send to a hacker off-site. This could happen even in the smallest companies with the best intentions and most trusted staff, and open up legal liability issues to the corporation who owns the compromised computing assets. Network forensics could indicate whose laptop was involved and what actually happened.

"Policies, procedures, training and communication are still the front line of defense against discrimination and harassment, but today's HR Leader must explore other avenues to assure their company is not being exposed to litigation in any media," says Miller. "We have our own home-grown system that captures emails and can be searched, but we built that because at the time we couldn't find anything on the market for this purpose."

The perfect storm for forensics

So why is now the time for using forensics? It lies at the perfect storm of a series of trends: First, **network capture technology has matured,** making applications-layer scanning easier to use and track. "In the past, you had to use lots of different tools to monitor or block individual applications," says Bennett. Now the tools have gotten better, and point solutions that monitor just Instant Messaging or email conversations aren't required.

Snyder talks about why forensics is so critical: "The network has become so critical to the enterprise that we can't continue to be sloppy in our engineering and throw more bandwidth at the problem. We want to know what happened, so tools that give us the ability to go back in time and find out what happened when some bad event occurred, are going to be required for enterprise networks."

"You need tools that can analyze application traffic," says Dennis Drogseth, an analyst with Enterprise Management Associates. "People don't want to have separate tools because it is costly and inefficient and creates separate frames of reference anyway. You want to invest in something that will scale as your organization and your needs grow, and where you can consolidate data for different sources in a consistent manner."

Second, **prices on storage continue to drop**, making universal collection reasonably cheap. "The tools are getting easier to mine this massive amount of data – a full 10 Gigabit network pipe can fill up a terabyte's worth of disk storage in less than six minutes. So that is a lot of traffic," said Haugdahl.

Third, the products are moving out of the realm of the network engineer and **usable by non-IT personnel**. "You want to be able to distill all this data down to something understandable, such as being able to summarize statistics and have better ways to detect anomalous activities," said Haugdahl. "You also want to be able to pick particular network IDs or IP addresses and focus on those particular packet flows."

Finally, **the number of data leaks and amount of private information being compromised is on the rise**, with each more spectacular experience getting lots of press play and generating bad publicity for the companies involved. "This data leakage is typically from the inside out. Most problems with credit card numbers have been insiders stealing information and taking it outside the company," says Bennett. "And there are plenty of regulations that control how private information needs to be protected by various state, US federal and other countries' laws." (See the sidebar on regulations summary on page 10 for just a few of the more relevant ones.)

Forrester Research sees that this combination of ingredients means that network forensics will become a key player in future investigations. They identify several futures for this marketplace[1]:

- Future laws and regulations will require certain organizations to have digital investigative capabilities. Senior management of companies that violate these laws and regulations will be held accountable.
- Demand for forensics products will accelerate. Tool providers will build more integrated, feature-rich and easy-to-use investigations solutions.
- The roles of the digital crime scene technician and digital evidence examiner will require significant dedication, training, and expertise.
- Consultancies and managed service providers will meet a big chunk of that demand. The digital investigations services will grow significantly during the next five years.

Three types of investigations

Given this potential landscape, what can companies do when they suspect a problem? There are three basic different forms of network forensic investigations:

- **Response to a specific network incident.** This could be anything from a breach on your network to finding out which laptop infected your network. It could also be theft of particular data from your company too, or situations where a batch of credit card numbers were inadvertently posted to the Internet. Indeed, during the same week we were writing this paper, tens of thousands of credit card numbers were leaked from a database server at the University of Missouri, exposing many people to identity theft issues and potential financial losses from misuse of these numbers. For these types of incidents, management generally won't invest in any network forensics solution until after the event happens.
- **Background for an internal corporate investigation.** Your human resources or legal department is conducting their own investigation of wrongdoing, inappropriate behavior, or violations of corporate policies. You want evidence that can show what someone has done over the corporate network, such as copies of their emails and Instant Message traffic and records of Web sites viewed by employees that contain offensive materials.
- **Support for a criminal investigation.** A crime was committed either on your company's property or by someone on your staff, and you want to get further information about what happened, and whether any corporate IT assets were used in the commission of the crimes.

For both internal and criminal types of incidents, management generally knows there is a problem and will work with their IT staff to capture the network data and solve the problem.

Each of these has different aims and methods, but all three share a need for a common collection of network traffic that is captured during the event that triggers the investigation. "For each of these scenarios, we want to be able to collect evidence and be able to prove or disprove malfeasance," says Bennett.

[1] *CSI:Cyberspace*, a January 2006 report by Michael Gavin, Forrester Research

Enter general-purpose forensic tools

In the past, many IT managers relied on special-purpose or applications-specific forensic tools. For example, there are several products that monitor and selectively block Instant Messenger conversations across an enterprise network. But what is clear from this paper is that these specialized tools are becoming outdated, as companies require more general-purpose tools that can reach across a broader spectrum of digital communications and cast a wider net for capturing digital evidence.

There are three basic elements of any general-purpose network forensics tool: capture, discovery, and analysis. Let's examine each one.

Data capture. This is the ability to store multiple gigabytes of data at high network throughput rates without dropping or missing any frames. You don't want your tool to bog down when lots of traffic is passing by, and you also want a device that can capture everything everywhere on the network, so that nothing gets past it. This includes both wired and wireless networks too.

Data discovery. Once the data is stored on disk, you want to be able to filter it or pare it down to particular items of interest, whether it be by IP address, user name, or type of application.

Data analysis. Finally, you want some built-in assistance to help examine the patterns and anomalies from the discovery process, to help you realize what actions were recorded in the captured packets.

As you go through each step in the process, you will need different skills to conduct your digital investigation, test various hypotheses, examine the evidence, and draw any conclusions. Keep in mind that a tool may be more useful or capable at only one of these steps, or for particular situations.

"When business managers -- including HR managers -- really take stock of all the things they need to know and all the types of problems they need to investigate, then it becomes clear that they need to be able to analyze what's happening on their network and collect the evidence they need for taking action. This is necessary regardless of which application (email, IM, or Web) is involved. Managers can recognize that network forensics is a new category of must-have technology. Having these tools available means being able to track something down and being sure that they can always absolutely find it," says Bennett.

Before you buy any tool, Haugdahl recommends asking these questions:

- What do you need to capture in your network, what is the nature of the traffic, and what are the capture bandwidth requirements?
- Is 100% capture to disk of massive amounts of data important to you? Or do you only need to be able to capture traffic involving certain IP addresses as part of an investigation?
- How long do you need to store the data you capture?
- How important are the distributed aspects and how efficient is the data conveyed to centralized consoles or distributed consoles shared by multiple investigators?
- Where should you do your analysis – on the machines that capture your traffic or offsite?

There are several general-purpose network forensic tools that are available as the table below indicates.

Company	Product	URL
WildPackets	OmniAnalysis Platform	wildpackets.com
Network Instruments	GigaStor	networkinstruments.com
Network General	Sniffer InfiniStream	networkgeneral.com
NetScout	NGenius Analytics	netscout.com

WildPackets OmniAnalysis Platform

Let's talk about what WildPackets is doing with its OmniAnalysis Platform product line.

First, it is a scalable, extensible, distributed platform for addressing network and application analysis needs across IT organizations. The platform comprises OmniPeek network analyzers, OmniEngine remote capture-and-analysis services, special-purpose products such as the OmniSpectrum RF analyzer for WLANs, and a growing family of software plug-ins that extend platform functionality.

In a typical network forensics configuration, network or data center engineers would use OmniPeek Enterprise network analyzers to start, stop, and analyze traffic captures on remote OmniEngines. Each OmniEngine can capture traffic from one or more network interfaces, including Ethernet, full-duplex Gigabit, 10 Gigabit, WAN, and 802.11. For network forensics, organizations typically deploy a WildPackets Omnipliance network recorder, a rack-mountable network appliance that includes a multi-terabyte disk farm and high-speed capture interfaces. OmniEngine software running on the Omnipliance captures and stores network traffic. Through the OmniPeek interface, engineers can run searches to mine the captured data for specific information, such as all the traffic from a certain IP address within a specific window of time.

The result is something that can meet a wide variety of forensics needs and be quickly deployed in many different situations. In fact, the OmniAnalysis Platform can address many types of forensics investigations:

- Compliance/HR Investigations, as described in this paper
- Security Attack Analysis, in order to enable security officers and IT staff to characterize and mitigate an attack that slipped past network defense
- Application Performance Benchmarking, in order to benchmark an application or pinpoint performance problems using the industry standard Apdex Application Satisfaction Index
- Transactional Analysis, providing the "ultimate audit trail" for business transactions, when server logs and other server-based evidence doesn't provide a thorough picture of a transaction
- Network troubleshooting, especially when the problem is an intermittent problem that occurs once or twice every few hours or days

"WildPackets has the most cost-effective, scalable analytics that is easier to deploy than its competitors and can be used by a variety of people within the enterprise for different roles," says Drogseth. "They are just easier to administer and to deploy, and have a wide breadth of analysis with a very light footprint. They have also adopted a very modular approach making them a great tool to get started in a mid-tier environment who doesn't have lots invested in other tools."

Privacy Regulations: A Summary

Today's corporate environment has to comply with a complex series of legal rulings and legislation. Here is just a sampler, by no means encyclopedic.

Sarbanes-Oxley (2002). This law requires accurate financial reporting and restricts access to this information to specific administrative individuals within a corporation. It also requires archives of communications regarding financial data between corporate officers and their accountants. To comply with Sarbanes-Oxley, an organization's email system must authenticate senders, encrypt confidential information, track and log message traffic, and support the indexing, archiving, and retention of messages.

California Security Breach Notification Act (2003). This requires any business, regardless of its location, to publicly disclose a security breach that could compromise the confidential information of any California resident.

Gramm-Leach-Bliley (1999). This law regulates the way that financial institutions manage the private information of individuals, and requires that this information is not carelessly divulged to the public.

Basel II (2008). This was developed by a group of European bankers and concerns the security of international banking transactions and email disclosures of confidential information.

NASD regulations. The National Association of Security Dealers have various regulations in place covering email communications between brokers and their clients, including how this information is stored and catalogued for later access.

HIPAA (1996). There are various regulations that effect patient privacy that is part of this legislation, including access to patient information and communications that include patient data between various parties.

Federal Information Security Act (2002). This requires all federal agencies and their partners to establish consistent, risk-based security processes. Agencies need to implement email security to protect their communications.

Canada's Personal Information Protection and Electronic Document Act (2000). This applies to all companies doing business in Canada and requires them to protect personal information using encryption.

Other International Data Protection Acts. Legislation passed by the European Union, Japan, the United Kingdom, and elsewhere call for companies to securely store personal data and provide access only to authorized users.

Civil Rights Act Title VII (1993). This original 1964 law has had its definitions broadened and as a result, victims of sexual harassment and discrimination can recover damages from their suits.

About the Author

David Strom is the former editor in chief of Tom's Hardware and Network Computing, the author of two computer books and thousands of magazine articles on Internet security, computer networking and other technical topics. He writes frequently for the New York Times, Computerworld, InformationWeek, eWeek, Information Security and other IT-related publications. He is a frequent speaker at many industry events, and writes blogs and records podcasts on numerous technical subjects. He lives in St. Louis, Mo., and can be reached at david@strom.com.