Network forensics isn’t just for troubleshooting or solving network security problems. With today’s increasingly interconnected, always online workforce, it’s often business-critical issues that have nothing to do with performance or cyber attacks, for example, violations of industry regulations or data breaches that drive the need for post-incident analysis. Whether accidental or malicious, the time to start capturing the digital evidence is before a specific event actually happens. Are you ready?
Network Forensics 101:
Finding the Needle in the Haystack

Introduction

Whether your organization is big or small, centralized or decentralized, you should have a network forensics solution up and running. If you already have a solution in place, you should be thinking about using it for business critical applications, such as regulatory/HR compliance, transactional analysis, etc., as well as for network troubleshooting. And the time to do it is now, before you need digital evidence for an investigation.

This white paper defines network forensics, dispels some common misperceptions, and describes what you could and should be using it for.

What is Network Forensics?

Network forensics is the capture, storage, and analysis of network events. You might also hear it referred to as packet mining, packet forensics, or digital forensics. Regardless of the name, the idea is the same: record every piece of network traffic – all emails, all database queries, all Web browsing, basically any information traversing your corporate network – to a single repository that can be examined after the fact.

Why do we Need Network Forensics?

Network forensics is commonly used for capturing an attack fingerprint and performing post-attack analysis for security exploits. This month’s denial-of-service (DDoS) attacks on Bitbucket.org – a Web-based code hosting service that relies on Amazon’s Elastic Compute Cloud (EC2)\(^1\) – and this summer’s DDoS attacks on Facebook and Twitter\(^2\) are recent headline examples.

With network forensics, you’re able to analyze historical network traffic in order to conduct investigations for security attacks. Using network forensics you can reconstruct the sequence of events that occur at the time of a breach and get the complete picture.

While security attacks get the most media attention, network forensics is more commonly used by IT for other problem incidents.

- Improving network performance
- Tuning intrusion detection solutions
- Identifying rogue device access to the net
- Stopping network hacks or viruses

If you limit yourself to using network forensics to answer infrastructure problems, you’re doing yourself and your company a disservice. Network forensics’ true value lays in its usefulness for business analysis.

Monitoring User Activity

Social networking sites like Facebook and Twitter have been shown to sap productivity in the workplace.\(^3\) As a result, many organizations have user policies that prohibit, or at least curtail such activities. Recently, the U.S. Marine Corp. banned marines from using Twitter for a year, as well as Facebook.\(^4\) Additionally, policies prohibiting non-work
related “bandwidth sucking” download activities (music, videos, games, etc) are common. Lastly, users may not be going through a proxy server, thereby opening up the network to various malware. Network forensics allows all these “rogue” activities to be monitored, revealing details as to who broke policy, what policy infraction was committed, and at what time it occurred.

Identifying the Source of Data Leaks

This fall, shortly after its latest Playstation hit the shelves – a release one reporter called “The Worst Kept Secret of the Internet” – Sony’s 2010 plans for its Playstation were revealed by Sega. How these leaks affect unit sales is anyone’s guess. According to a study conducted by the Ponemon Institute and sponsored by the PGP Corp, lost business accounted for nearly 70 percent of the cost of a data breach, averaging $4.6 million, and was mostly commonly caused by insider negligence.

As data leaks occur, you want to be proactive about monitoring your network to understand what information was released and/or how much has been lost. Using network forensics, you can track down the culprit and determine whether the leak was accidental or purposeful.

Business Transaction Analysis

For transactions that take place in clear text like SQL, HTTP request, FTP, or telnet, network forensics allows the network administrator to create the ultimate audit trail for business transactions. Not just server activity, but the business transactions enacted by clients and servers. Additionally, network forensics can serve to troubleshoot the transaction problems that server logs miss.

Pinpointing the Source of Intermittent Performance Issues

On a practical level, here’s where network forensics’ tools really come in handy – the capturing and handling intermittent network problems, especially those problems that occurred hours or days ago. Traditional “reactive” ad hoc troubleshooting can miss patterns that indicate network problems, so network forensics can be used to catch things that were originally missed.

What Purpose does Network Forensics Serve?

Network forensics allows you to find the details of network events after they happened. It essentially allows you to reconstruct the history of your entire network; think of it as “The Network Time Machine.”

The SANS Institute notes, “Network forensics can reveal who communicated with whom, when, how, and how often. It can uncover the low-level addresses of the systems communicating, which investigators can use to trace an action or conversation back to a physical device. The entire contents of e-mails, IM conversations, Web surfing activities and file transfers can be recovered and reconstructed to reveal the original transaction. More importantly, the protocol data that surrounded each conversation is often extremely valuable.”

By recording every single packet that is transmitted over your corporate networks, network forensics allows you to reconstruct any emails, instant messages, FTP traffic, or any other form of communication from the original
transmissions. It doesn’t get any more accurate than that. You’re able to use network forensics to analyze historical network traffic to conduct or assist in many types of investigations.

How does Network Forensics Work?

Types of Investigations

There are basically three types of investigations:

- Responding to a specific network incident
- Gathering background for an internal corporate investigation
- Supporting a criminal investigation

For both internal and criminal investigations, management generally knows there’s a problem and works proactively to capture the network data and solve the problem. When you’re responding to a network incident, you may not have network forensics tools at hand.

Each investigation has different aims and employs different methods. All three share the need for a common collection of network traffic that is captured during the event that triggers the investigation. For each situation, you need to be able to collect evidence and prove or disprove malfeasance.

Basic Elements of a Network Forensic Solution

To facilitate digital investigations, general purpose network forensics solutions have three capabilities: capturing (and recording) data, discovering data, and analyzing data.

- **Capturing (and Recording) Data:** This is the ability to capture and store multiple gigabytes of data at high network throughput (for example, 10 Gigabit) without dropping or missing any packets. Every network forensic solution has its limitations, including sustainable throughput, packets per second, data management, search functions, etc. These limitations can and should be determined through practical lab tests, and the results should be repeatable and documented. This includes both wired and wireless networks.

- **Discovering Data:** Once data are recorded on the storage media, the solution should provide a mechanism to filter particular items of interest, for example, by IP address, application, context, etc.

- **Analyzing Data:** Finally, you want some built-in assistance for examining the patterns and anomalies found during the discovery process to help you determine what actions were recorded in the captured packets.

When choosing a solution, you’ll want to consider that most investigations start with terabytes upon terabytes of data. With this much data, you’ll want to think about a solution that allows you to analyze data at the point of capture, thus eliminating the need for large data transfers that consume time and bandwidth. You’ll also want a simple and intuitive means to drill down into the relevant data, making easy work out of finding the needle in the multi-terabyte haystack.
The WildPackets Network Forensics Solution

The WildPackets OmniPeek Distributed Analysis Suite provides real-time visibility into every part of the network – simultaneously from a single interface – including Gigabit, 10GbE, Ethernet, 802.11a/b/g/n wireless, VoIP, and WAN links to remote offices. Using OmniPeek’s local capture capabilities, centralized console, distributed engines, and expert analysis, you can rapidly troubleshoot faults and fix problems and look for security exploits, restoring essential services and maximizing network uptime and user satisfaction. WatchPoint is a comprehensive reporting solution from WildPackets which allows you to receive NetFlow and sFlow statistics and correlate these with data from multiple WildPackets OmniEngines and Omnipliances.

In a classic configuration, you would use OmniPeek Enterprise network analyzers to start, stop, and analyze traffic captures on remote OmniEngine software probes. Each OmniEngine can capture traffic from one or more network interfaces, including Ethernet, full-duplex Gigabit, 10 Gigabit, WAN, and 802.11.

More typically for network forensics, you would deploy an 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, you 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.
With the WildPackets network forensic solution in place, various types of forensic investigations can be carried out:

- Regulatory compliance/HR investigations – to detect and analyze violations of HR policies or industry regulations and support compliance efforts for SOX, Gramm-Leach-Bliley, HIPPA, etc.
- Transactional analysis – to provide the “ultimate audit trail” for any transactions, where server logs and other server-based evidence doesn’t provide a thorough picture of a transaction
- Security attack analysis – to enable security officers and IT staff to characterize and mitigate an attack that slipped past network defense (e.g. zero day attack)
- Network troubleshooting – to handle any type of network problem, especially those that happen intermittently
- Network performance benchmarking – to provide detailed reporting on network performance, bottlenecks, activities, etc.

Conclusion

Network forensics can be a powerful tool to unlock mysteries found within your network – provided you’re capturing the digital evidence now, before any specific event actually happens. Make sure you have a network forensics tool best suited for your organization’s particular needs.

WildPackets helps you analyze data by capturing network traffic at key network points and minimizes traffic loads on the network that can be caused by polling devices. By storing data in a common, searchable format and by providing simple and complex filters for mining the data, the WildPackets Network Forensics solution allows you find the data you’re looking for quickly and easily.

To learn more about WildPackets solutions, please visit: http://www.wildpackets.com. Or contact WildPackets Sales: sales@wildpackets.com or (925) 937-3200.
Endnotes


