Network Forensics: How to Optimize Your Digital Investigation

WHITE PAPER

Every day your organization's network security comes under attack. To help mitigate these attacks, you're faced with monitoring security appliances, detecting intrusions, assessing compliance with policies, analyzing external threats, evaluating potential internal threats, and more. Yet network breaches still occur, and when they do you need a record of the breach so you can perform a forensic analysis on the attack and prevent future occurences. Network forensic solutions have four basic elements – data capture, data discovery, data analysis, and data record – to reduce your mean time to resolution when a problem is reported or detected. With throughput continuing to increase, you need to be able to sift through various data. This white paper covers three phases of a digital investigation so that you can get to the root cause quickly.

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

Network Forensics: How to Optimize Your Digital Investigation

Introduction

In the last twelve months, 90 percent of businesses fell victim to a cyber security breach at least once[1]. The typical cost? Cyber attacks cost businesses $682,000, including lost productivity, loss of data, lost revenue, loss of customer trust, regulatoriy fines, and theft of money or goods[2]. Unfortunately, attackers are moving from splash to stealth and you may not notice when an attack begins, causing you to miss critical data. Are you prepared? Can you afford not to be?

Network forensics has been used in the past for post-incident troubleshooting and fine-tuning network performance. For example, network forensics can provide information about why a network is performing badly, a failing router/firewall, etc. Nowadays it is commonly used for capturing the attack fingerprint and performing post-attack analysis for security exploits. According 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.”

To be able to respond and prevent future attacks, there are four basic elements to a classic network forensic solution. However, discovering you have a security threat is only a piece of a network forensics solution. You also need to be able to quickly sift through various data, using a variety of parameters such as source/destination IP address, source/destination port, time, date, protocol, string, and more, and perform analyses quickly. With historical data as well as real-time data in a common searchable format, you’ll be able to reduce the time to determine how an attack occurred.

Basic Elements in a Network Forensic Solution

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

- **Capturing and Recording Data:** This is the ability to capture and store multiple terabytes of data from high-throughput networks (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.
- **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.
- **Analzying 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.

Typical Situations

In real life, you will face two situations:

- First, you already have a case to work on. This could be a lead from your firewall or IPS log that requires you to access to the captured packets for further analysis.
- Second, you are trying to look for something abnormal or suspicious in all the traffic that you have recorded.

In the second case, you might want to leverage network forensics to quickly point you in the right direction. Several methods you might employ include:

- **Communication Matrix:** Provides a quick glance at all the communication in your networks. This could be the best tool for discovering DDoS attacks, worm attacks, or other abnormal activities.

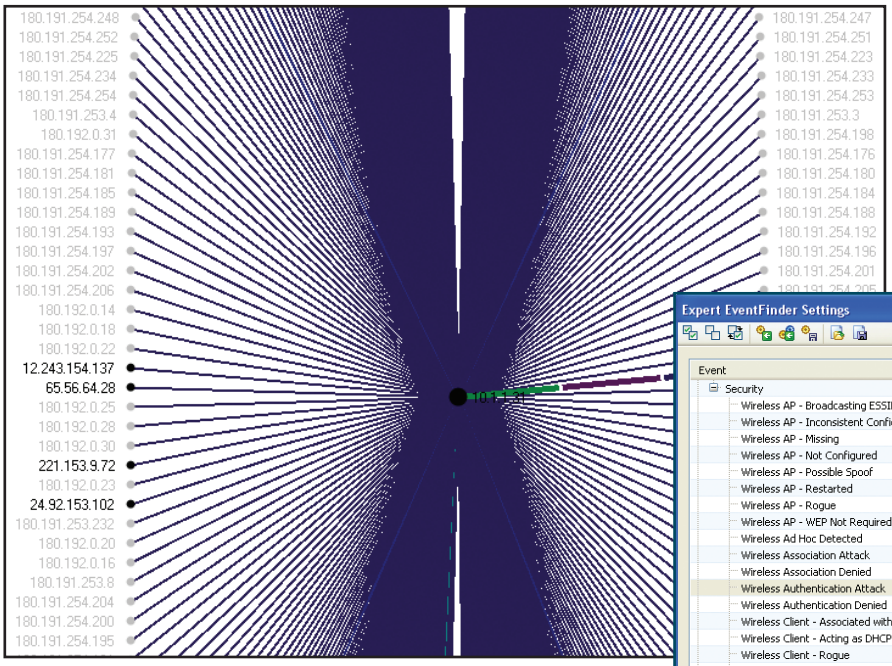


Figure 1: Communication matrix illustrating a worm attack

- **Top Stations and Protocols:** A list of top x stations gives a picture of whether your network is healthy. Usually, all the active servers appear at the top of the list. On the other hand, the top protocol list identifies the kind of activities occurring in your network.
- **Suspicious Events Discovery:** Expert modules, such as those embedded in the OmniPeek Distributed Analysis Suite, can detect potential attack activities or problems in any of the 7 OSI layers.

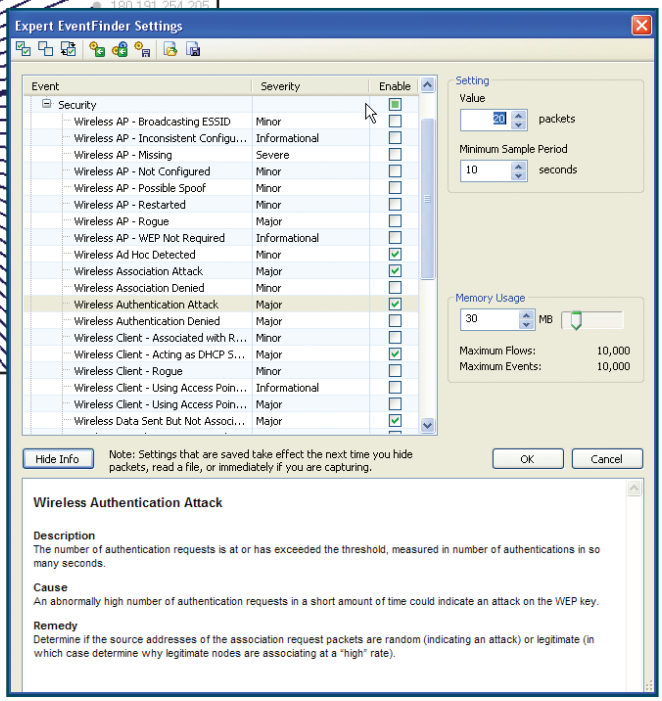


Figure 2: OmniPeek's Expert events and knowledgebase

Phases of Digital Investigation

As we have already discussed, data discovery and data analysis are two of the basic elements in a network forensics solution, and these are especially critical when you are dealing with huge amounts of captured network traffic. This section discusses some common steps in a digital investigation.

Data Discovery: Separate Network Data

Based upon suspicious activity, a network forensic analyst must be able to automatically extract or fetch network data using one or multiple parameters, such as source/destination IP address, source/destination port, time, date, protocol, string, and more.

With the comprehensive network forensics features in the OmniPeek Distributed Analysis Suite, each kind of expression (IP, MAC, Protocol, Port, Pattern, Value, Length, dedicated Analysis Module/Plug-in) can be searched individually or in combination with operators (and, or, not, Group) to extract the required data from gigabytes or even terabytes of captured traffic.

- **Apply Filters:** In situations with multiple data collection points (different segments or locations), the forensic analyst can apply a filter or filters to a specified data file set.
- **Isolate Data by Connection:** Additionally, the Expert modules in the OmniPeek network analyzer are able to assemble different sessions (connections) into flows and provide a quick method for you to isolate a specific connection for further investigation.

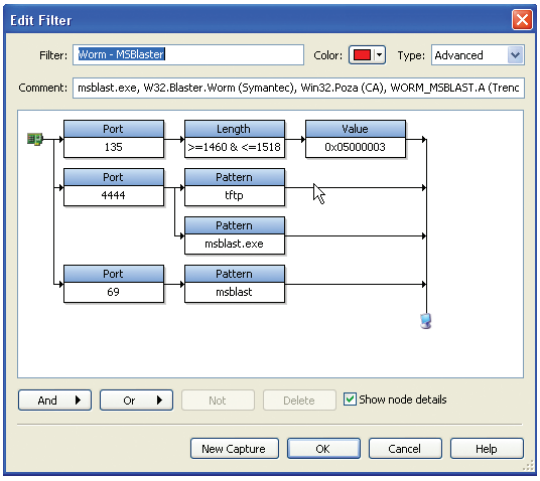


Figure 3: Filters like the MSBlaster worm filter can be used within forensics data searches

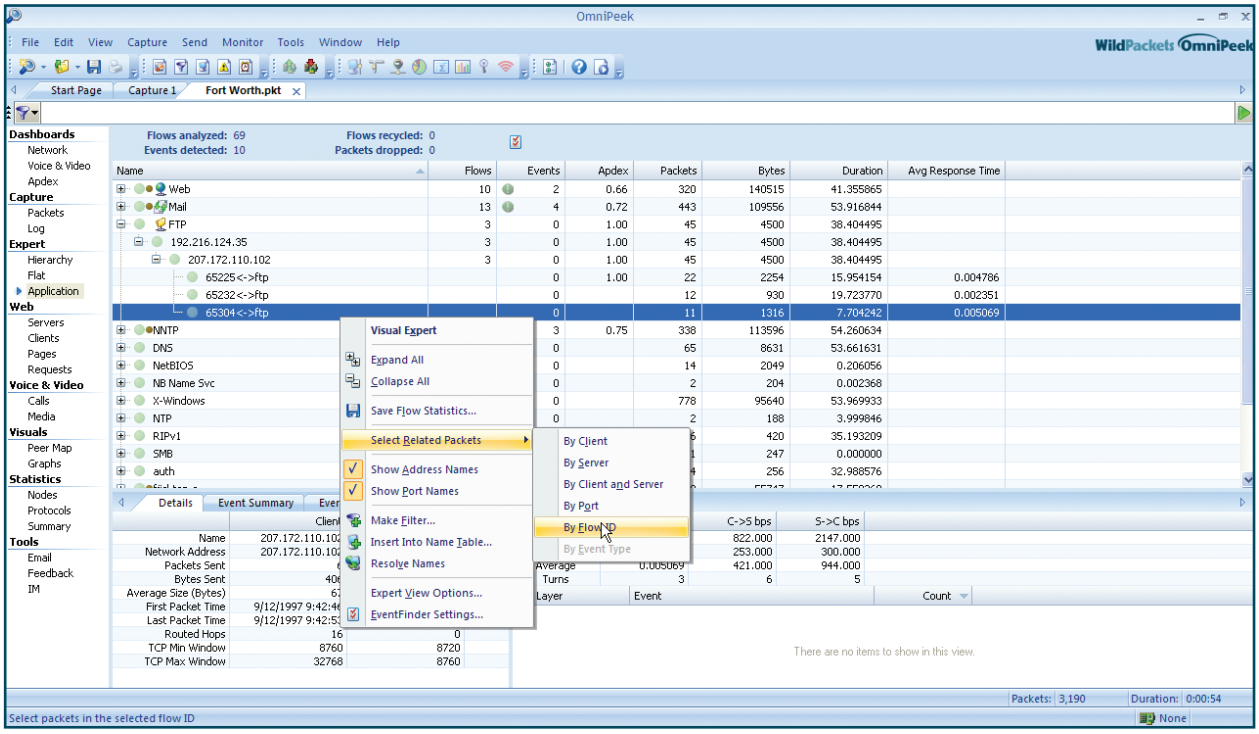
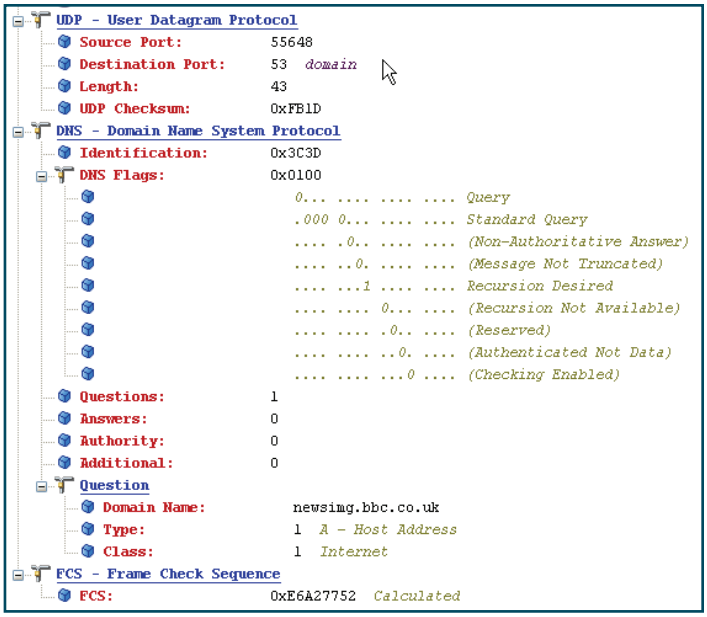


Figure 4: Isolating data by connection

Data Analysis: Perform Packet Drill-Down

Once you have acquired the suspicious data (packets) via the data discovery process, it's time for the data analysis process. During this process, these common steps will be performed.

- **Packet Decode:** Packet decode is one of the most detailed analyses that a forensic analyst will perform. By viewing the packet decode, you can investigate the bits, flags, and payload for each packet.
- **Packet Sequence Analysis:** Packet sequence analysis is commonly used for troubleshooting a connection performance problem (for example, RTP sequence analysis in VoIP). Packet sequence analysis is also one of the important steps in performing attack analysis, such as session hijacking. OmniPeek network analyzer provides various ways for you to analyze the packet sequence.



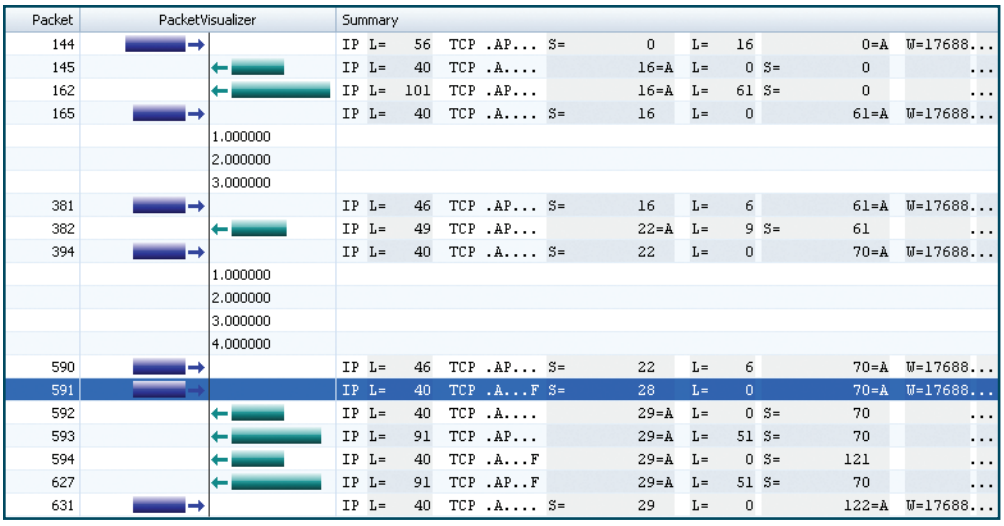


Figure 6: Packet Visualizer allows you to analyze the packet sequence

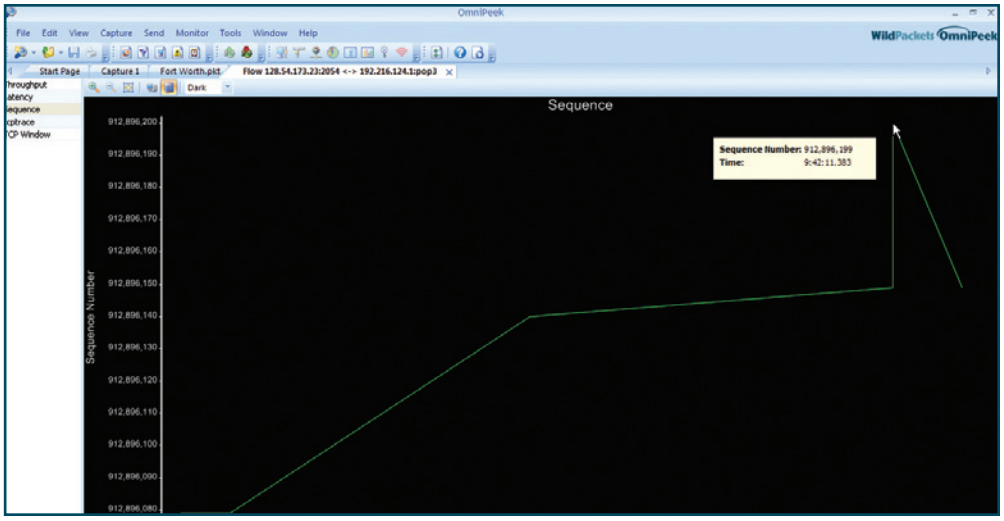


Figure 7: Sequence Number Analysis Graph

- **Multi-segment Analysis:** To analyze how the packets will behave after passing through one or multiple network device(s).

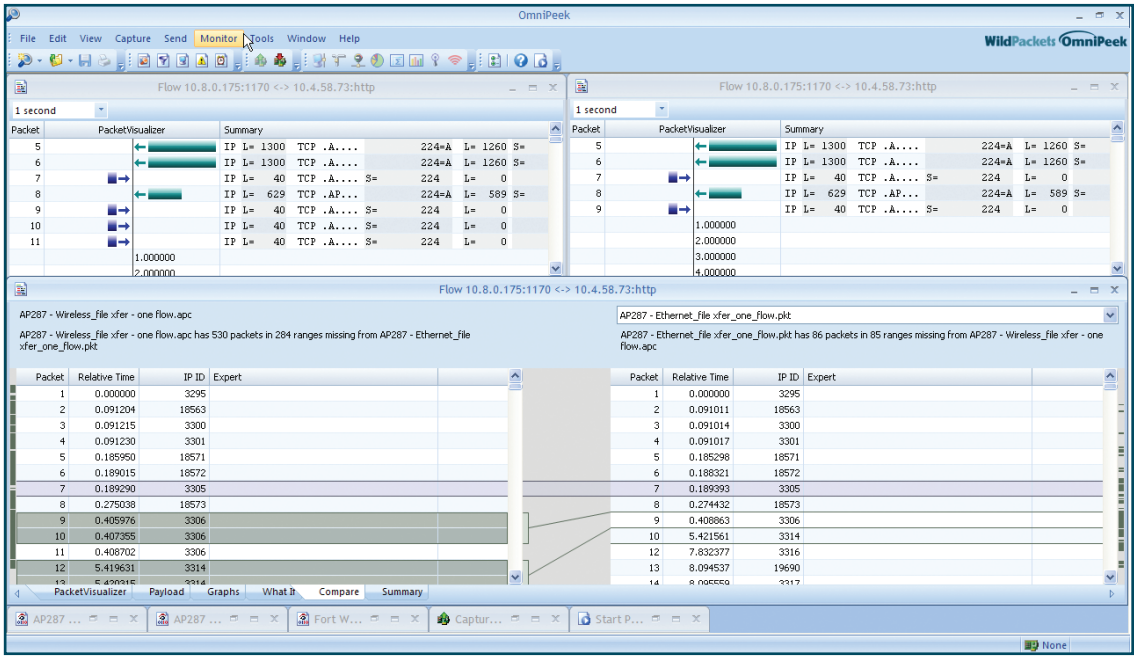


Figure 8: An example of multi-segment analysis

- **Extract Stream by IP/Protocol/Application:** The network forensics search can extract a stream easily in any form like IP pair, protocol, or application. This is critical when drill-down to a particular conversation is needed.

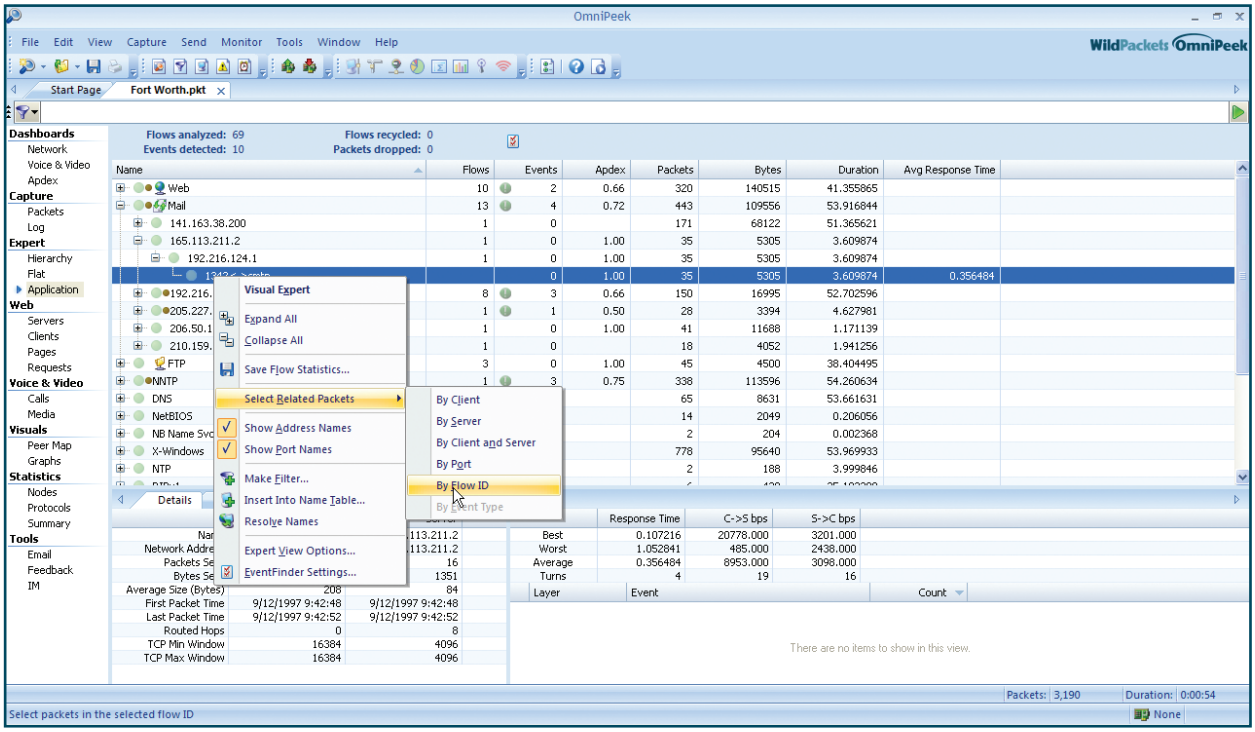


Figure 9: Quick extraction to a selected stream in OmniPeek

Data Analysis: Enumerate the Data

At times the network forensic analyst needs to extract and reconstruct the captured traffic into a readable format, for example, a work document, PDF file, email, web page, etc. A good network forensic solution provides the capability to reconstruct data and allows the analyst to develop his/her own modules for any proprietary (in-depth) analysis.

The OmniPeek network analyzer provides features to assemble any conversation and present its payload as a whole as depicted in Figure 10.

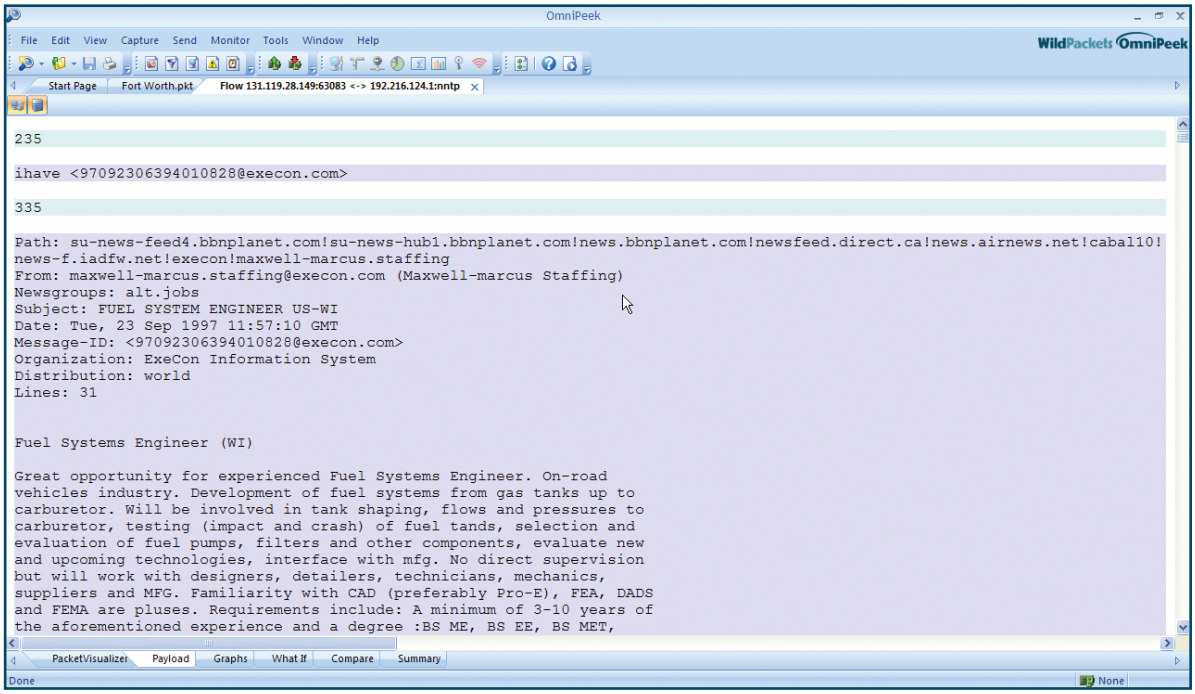


Figure 10: A NNTP conversation reconstruction in OmniPeek

When the payload contains a specific file format (e.g. JPEG, PDF, etc.), WildPackets provides an SDK to allow the analyst to develop their own analysis module or "plug-in" to reconstruct packets into the original form by using the published APIs.

Figure 11 shows captured email traffic that has been reconstructed and displayed in a simple email UI similar to Outlook. It illustrates a reconstructed email with its contents and attachment—the JPEG map is fully reconstructed as well.

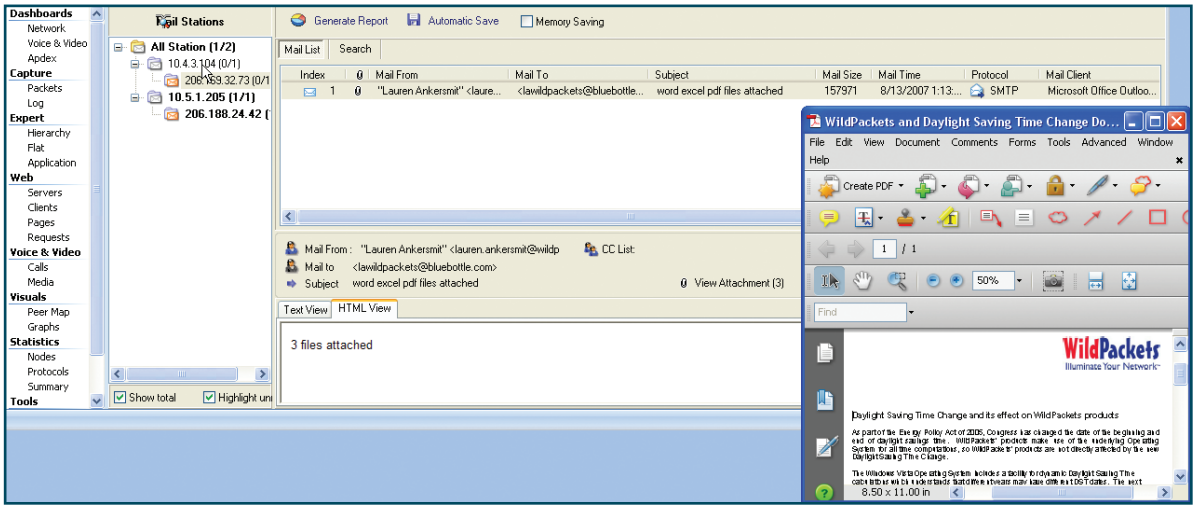


Figure 11: An example of forensic email reconstruction in OmniPeek using the Email Plug-in

WildPackets Network Forensics Solutions

Network forensics, or your 'network time machine,' helps you pinpoint the source of intermittent performance issues and conduct investigations to identify the source of data leaks, HR violations, or security breaches. Get ready now – before a specific event actually happens – so digital evidence is collected and ready to help you find that needle in the haystack.

With WildPackets Network Forensics solutions, data is always available for reconstruction and easy analysis of intermittent issues, cyber attacks, and network security or data breaches. All pertinent network traffic is collected in a single location, rather than scattered across the network. Data is captured in a common data format and does not need to be transferred or translated in any way for analysis.

Using our network forensics data mining tools, network engineers have the data they need to identify and fix problems users are complaining about that only occur intermittently, and security teams can reconstruct the sequence of events that occur at the time of a network breach or cyber attack and get the complete picture.

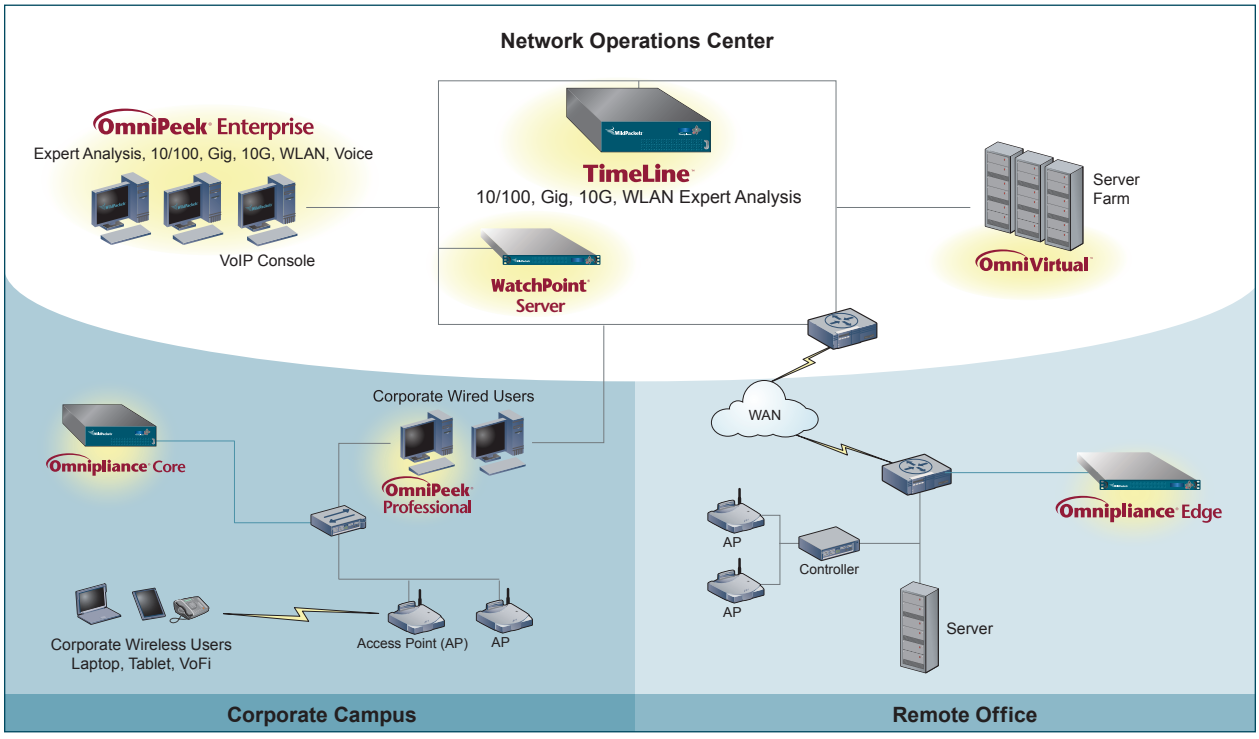


Figure 12: WildPackets Network Forensics Solutions

While other network forensics products force you to capture with one product, then transfer gigabytes or terabytes of data to another tool for analysis, WildPackets Network Forensics solutions enable you to analyze data at the point of capture, and eliminate the need for large data transfers that consume time and bandwidth. By utilizing Intelligent Data Transport™, WildPackets Network Forensics solutions minimize traffic loads on the network and let you find the data you're looking for, quickly and easily.

24x7 access to ALL network data and network forensics mining tools lets you:

- Ensure network and security data are captured 24x7 and not sacrificed when SPAN ports are needed for other applications
- Reduce Mean-Time-To-Resolution (MTTR) by eliminating the time consuming step of having to reproduce problems before they can be analyzed and responding to issues in real-time, often solving issues before mission critical applications are impacted
- Understand service-level compliance within your organization
- Comply with government regulations and Human Resources policies by auditing and tracking all network activity

If you're not already reaching for network forensics to address a pesky intermittent network issue, benchmark application performance for SLAs, or investigate a data breach, you should be. WildPackets Network Forensics solutions offer the following capabilities:

- **Comprehensive data collection:** Hours or even days of network traffic – anything that crosses the network, whether email, IM, VoIP, FTP, HTML, or some other application or protocol – collected by a single system and stored in a common, searchable format. Terabytes of data available through a single interface.
- **Flexible data collection:** Collect all data on a network segment for future inspection or focus on a specific user or server.
- **High-level analysis:** Eliminate the need for brute-force analysis across disparate data sources with access to WildPackets' award-winning Expert Analysis, graphical reports, and application performance scoring.

With WildPackets Network Forensics solutions in place, you can conduct various types of forensic investigations:

- **Network performance benchmarking** for detailed reporting on network performance, bottlenecks, activates, etc.
- **Network troubleshooting** for handling any type of network problem, especially those that happen intermittently.
- **Transactional analysis** for providing the "ultimate audit trail" for any transactions where server logs and other server-based evidence doesn't provide a thorough picture of a transaction. Remember, packets don't lie!
- **Security attack analysis** for enabling security officers and IT staff to characterize and mitigate an attack that slipped past network defense such as a zero day attack.

Learning More

- "Network Forensics 101: Finding the Needle in the Haystack" Think network forensics is just for security? This white paper defines network forensics, dispels some common misperceptions, and describes what you could and should be using it for.
- "Network Forensics: How to Optimize Your Digital Investigation" Time is of the essence when your

organization's network security comes under attack or you're investigating a business-critical issue such as a data breach or an industry regulation violation. This white paper shows how a network forensics solution with four basic elements – data capture, data discovery, data analysis, and data recording – reduces your mean time to resolution. Also covered are the three phases of digital investigation: separating network data, performing packet drill down, and enumerating the data.

- "Network Forensics in a 10G World" With highly utilized networks, capturing network traffic with individual SPAN ports and taps typically results in spotty overall visibility of your network. In today's 10 Gigabit (10G) world, you need a purpose built network forensics solution in place capturing ALL network data, 24x7, to ensure a stable and safe network. This white paper identifies the unique challenges of highly-utilized 10G networks, establishes guidelines for ongoing network data collection, and addresses the conflicting demands of traditional (TCP/IP) data analysis and VoIP analysis.

All of these white papers and more can be found at www.wildpackets.com under the Resources section.

About WildPackets, Inc.

WildPackets develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. WildPackets products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Motorola, Nationwide, and over 80 percent of the Fortune 1000. WildPackets is a Cisco Technical Development Partner (CTDP).

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

Conclusion

Network security is crucial in the digital age. Information leakage not only results in monetary losses but can be a serious threat to national security. Having the right network forensic solution in place can help to discover zero-day attacks, eliminate reoccurences in your network, and provide lawful interception capabilities when needed.

Endnotes

1. Ponemon Institute LLC. "Perceptions About Network Security: Survey of IT & IT security practitioners in the U.S." 6/2011. p.2. http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.

2. Higgins, Kelly Jackson. "Productivity, Data Losses Biggest Cost In Cyberattacks." *Security Dark Reading.* 11/03/2011. http://www.darkreading.com/security/perimeter-security/231902313/productivity-data-losses-biggest-cost-in-cyberattacks.html