# Network Forensics 101: Finding the Needle in the Haystack

WHITE PAPER

There's a paradox in enterprise networking today. Networks have become exponentially faster. They carry more traffic and more types of data than ever before. Yet as they get faster, they become more difficult to monitor and analyze. Details are lost, as IT organizations find themselves falling back on sampling and high-level metrics. But details can be critical when troubleshooting an outage, verifying business transactions, or stopping a security attack in a timely manner. No matter how fast the network is running, IT engineers still need to be able to find the needle in the haystack–the digital proof that solves a mission-critical problem. How can network forensics help?

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

# Network Forensics 101: Finding the Needle in the Haystack

## Network Analysis Today: Big Questions, Vague Answers

Organizations depend on their networks more than ever before, so monitoring and managing those networks is a mission-critical job for IT. But monitoring and managing networks has become increasingly difficult for several reasons.

- **Faster networks and greater data volumes**.
  Organizations are investing in faster networks. 1G networks, once considered "cutting edge, have become a "commodity" technology. Adoption of even faster networks, including 10G and 40G networks, grew 62% in 2012. 10G networks accounted for about 75% of investments in high-speed networks.[1] These high-speed networks are challenging IT departments to find network monitoring tools that can keep up with exponentially faster data rates. Unfortunately, the shortcomings of traditional monitoring tools to reliably capture and analyze high-speed traffic have become evident to IT departments. In a recent survey by TRAC Research, 59% of IT respondents expressed concern about their network monitoring tools dropping packets instead of reliably recording high-speed traffic for analysis. Similarly, 51% of respondents doubted the accuracy of the data being presented by their network monitoring tools.
- **Richer data**.
  VOIP has become the de facto standard for business telephony, and video over IP is a popular channel for business content. Organizations need tools for analyzing and optimizing these critical communications services regardless of whether they're running on traditional LANs or 40G networks. Network analysis tools that rely on sampling and high-level metrics often prove inadequate for resolving elusive performance problems for low-latency applications like VoIP.
- **Subtler and more malicious security threats**.
  A decade ago, the most common network security threats were deluges of spam and worms or other malware that might congest a network or interrupt operations. Today's security threats are more subtle, more sophisticated, and more pernicious. Instead of blatantly interrupting services or peddling foreign pharmaceuticals or counterfeit watches, today's security threats are more likely to slip unnoticed onto a network and prowl for data, such as product plans or customer records, which might be "exfiltrated" at a low-volume trickle to remote command-and-control centers, which might be located in a foreign country. No longer content with cybervandalism, today's attackers are after intellectual property, which can be sold on the black market, and confidential data that can be used for identity theft and financial fraud. Verizon's *2013 Data Breach Investigations Report* found that 75% of discovered data breaches were financially motivated. Equally concerning:  66% of breaches took months or longer to discover.[2] IT organizations seem to lack the tools necessary to adequately investigate and stop data breaches that threaten to cost organization's hard cash, competitive advantage, or both.

[1] http://www.infonetics.com/pr/2013/2H12-Networking-Ports-Market-Highlights.asp

[2] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

- **Sampled data and high-level statistics**.
  At the same time that network traffic is growing in volume and complexity, network analysis tools have been following a trend toward simplicity. Instead of analyzing all network traffic, many recent products settle for sampling traffic or reporting high-level flow statistics such as NetFlow and sFlow. Flow-based analysis systems certainly have their place in an IT organization's toolset. They provide an affordable solution for leveraging metrics automatically generated by network infrastructure such as routers and switches. Flow-base metrics do a serviceable job reporting network utilization and other aggregate measures of network activity. But when it comes to troubleshooting difficult problems or determining if message payloads contained the right data or malware, sampled or statistical data simply isn't sufficiently detailed and precise to enable IT engineers to efficiently the questions being investigated.

Together, these changes and challenges make it increasingly difficult for IT engineers to answer basic network performance and application delivery questions such as:

- What's causing the performance problems in our remote office in Chicago?
- Why are VoIP users complaining about choppy calls when the VoIP call manager software is reporting that everything is fine?
- How can I confirm that an ecommerce transaction was processed correctly now so that our call center can answer an angry customer wondering why the transaction was refused?
- How should I investigate an alert being raised by our Intrusion Detection System (IDS) about traffic on a network segment in Building 3?

To be able to answer these questions, IT engineers need access to network traffic, but that traffic is now flying by faster than ever before. Once it has passed through the network, it's no longer available for analysis–unless it has been recorded to disk. Network recording–or as it's more popularly known when combined with powerful data search and analysis tools, network forensics–would enable an IT organization to answer many of these questions.

When implemented correctly, network forensics enables IT engineers to find the proverbial needle in a haystack, whether they are searching for evidence of a security attack, the root cause of a network performance problem, or evidence that an employee has violated an HR policy.

There are many use cases in which IT organizations can apply network forensics to solve performance, security, and policy problems on today's high-speed networks.

# Introducing Network Forensics

## Network Forensics Defined

Network forensics is the capture, storage, and analysis of network events. It is sometimes also called packet mining, packet forensics, or digital forensics. Regardless of the name, the idea is the same: record every packet of network traffic (all emails, all database queries, all Web browsing–absolutely all traffic of all kinds traversing an organization's network) to a single searchable repository so the traffic can be examined in detail.

Collecting a complete record of network activity can be invaluable for addressing technical, operational, and organizational issues. As 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 emails, 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."[3]

## Use Cases for Network Forensics

Here are some of the more common uses of network forensics.

### Finding Proof of a Security Attack

In many IT organizations, network forensics is best known as a tool for investigating security issues such as data breaches. Often a security monitoring solution such as an Intrusion Detection System (IDS) will raise an alert about suspicious network activity without providing sufficient detail for IT engineers to confirm the presence of an attack. Examining a comprehensive record of network traffic from the time the alert was raised enables IT administrators to find proof of an attack, if there is one, and begin attack remediation.

Without an ongoing recording of network traffic, IT administrators can only wonder if a threatening activity occurred when an alert was raised.

### Troubleshooting Intermittent Performance Issues

Another use of network forensics is troubleshooting intermittent network problems. If the help desk is having difficulty replicating a user's problem, or if a problem occurs only in certain conditions or at certain times, IT engineers might want to record hours or days' worth of traffic and then hunt for the elusive behavior.

[3] SANS Institute. "Security 558: Network Forensics Course Description." http://www.sans.org/security-training/network-forensics-1227-mid..

### Monitoring User Activity for Compliance with IT and HR Policies

Because network forensics captures all network traffic, including email, email attachments, VoIP calls, videos, and other rich media communications, it can help IT administrators, legal departments, and HR departments confirm that a specific user is complying or not complying with specific policies about network usage, data privacy, and so on. Network forensics provides hard evidence of who transmitted what to whom.

### Identifying the Source of Data Leaks

A special case of IT and HR violations is data leaks. There are many ways that internal users can leak confidential information:  email, blog posts, social media updates and so on. Email gateways and Web gateways might catch some of these communications. Network forensics gives organizations a tool for catching leaks that might elude detection through traditional means.

### Monitoring Business Transactions

For transactions that take place in clear text like SQL, HTTP requests, FTP, or telnet, network forensics provides the ultimate audit trail for business transactions. Network forensics can serve to troubleshoot the transaction problems that server logs miss. Merchant services providers, for example, can use network forensics to resolve discrepancies between what's reported by a client and what's reported by a server. The recorded transmission is the ultimate authority for verifying that a transaction took place and certifying its contents.

### Troubleshooting VoIP and Video over IP

When IT engineers are asked to troubleshoot voice or video over IP traffic, network forensics provides an exemplary service:  it enables engineers to replay and analyze the calls and video transmissions themselves. Rather than extrapolating from metrics or log files, engineers can examine "live" call data and experience the source of end users' concerns.

## Requirements for a Network Forensics Solution

To facilitate digital investigations, network forensics solutions must provide three essential capabilities: capturing and 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 (including 10G and even 40G networks) 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 means of filtering particular items of interest, for example, by IP address, application, context, etc. IT engineers rely on discovery tools for sifting through terabytes of data to find specific network conversations or individual packets in a timely fashion.

- **Analyzing Data:** To further accelerate discovery and analysis, IT engineers benefit from a forensics solution's built-in assistance for examining the patterns and anomalies found during the discovery process. Automated analysis, including Expert analysis that explains the context of network events, helps IT engineers quickly identity anomalous or otherwise significant network events.

Beyond these three key capabilities, network forensics must be:

- **Precise**
  Network forensics solutions need to be able to capture high-speed traffic without dropping packets or reporting erroneous results. As the TRAC Research survey mentioned earlier showed, many organizations who have tried to analyze high-speed traffic are dismayed to find errors and omissions in their network forensics solutions.
- **Scalable**
  To support traffic capture on high-speed networks such as 10G and 40G networks, a network forensics solution should be able to capture, search, and analyze tens or even hundreds of terabytes in an affordable, manageable configuration.
- **Flexible**
  It's not unusual for IT organizations to need to capture traffic from network segments running at different speeds, such as a 1G segment and a 10G segment. A single network forensics appliance should be able to combine interfaces to heterogeneous networks, so that IT organizations do not have purchase a separate appliance for each network speed they want to monitor.
- **VoIP-smart**
  VoIP is the de facto standard for telephony in organizations of all sizes. Network forensics solutions should be able to reconstruct and replay VoIP calls and present Call Detail Records (CDR) for each call. Engineers should be able to examine and replay actual call data rather than relying on derived data such as logs from a third-party call manager.
- **Continuously Available**
  Network forensics solutions should be able to run continuously so that IT organizations don't find themselves in the position of wishing they had begun capturing traffic hours or days ago. While recording traffic continuously, they should also support real-time analysis, so that IT engineers can compare real-time network activity to past activity, and so that IT engineers do not have deploy, maintain, and train on two completely separate analysis tools:  one for forensic analysis and one for real-time analysis.

# WildPackets Network Forensics Solution

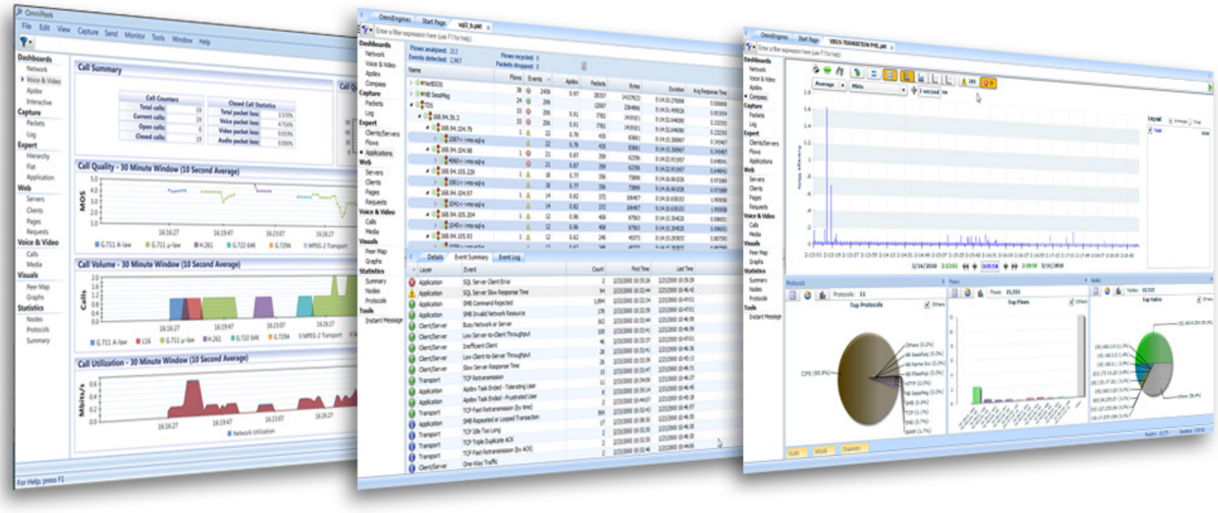
## Omnipliance Network Analysis and Recording Appliances

WildPackets' family of Omnipliances–powerful network analysis and recording appliances–gives IT organizations the network monitoring, recording, and troubleshooting solution they need for today's complex, high-speed networks.

Omnipliances provide 24/7 access to 1G, 10G, and 40G network traffic for detailed analysis, including forensic analysis of past events, Expert analysis for troubleshooting, voice and video over IP metrics, and critical network metrics like Top Talkers and Top Protocols.

Each Omnipliance features:

- Powerful network recording features for capturing terabytes of traffic with no packet loss.
- Award-winning OmniPeek Enterprise software for performing real-time analysis of live network traffic and forensic network analysis of recorded traffic.


Call Summary
Call Quality - 30 Minute Window (10 Second Average)
Call Volume - 30 Minute Window (10 Second Average)
Call Utilization - 30 Minute Window (10 Second Average)
Top Protocols
Top Flows

**The OmniPeek Enterprise network analyzer provides a rich tool set for analyzing and troubleshooting both real-time and recorded network traffic.**

Omnipliances meet the all the requirements for network forensics on complex, high-speed networks:

- **Loss-less capture and recording** of 1G, 10G, and 40G network traffic.
- **Powerful data discovery tools** that help IT engineers zero in on specific types and time spans of traffic.
- **Built-in analytics**, including Expert analysis, voice and video over IP metrics, and critical network metrics like Top Talkers and Top Protocols, all of which help reduce the Mean Time to Repair when troubleshooting network outages and performance issues.
- **Precision** in loss-less recording and accurate metrics, even for high-speed traffic.

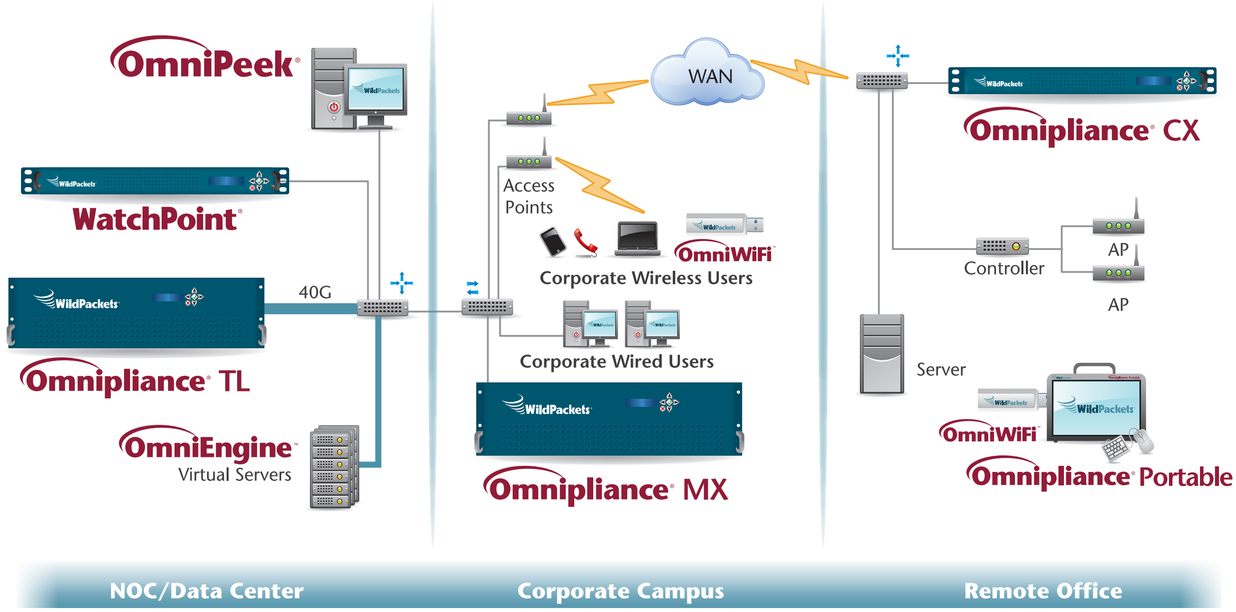
- **Scalability** that allows organizations to add and combine appliances to meet all their network forensic needs. A single Omnipliance TL with an OmniStorage disk array can capture up to 128 TB of network traffic.
- **Flexibility** that allows organizations to combine appliances and mix interface cards to create the most powerful and cost-effective configuration for monitoring their networks. Each Omnipliance can combine different speed interface cards.
- **Voice and video over IP analysis** that enables IT organizations to monitor and troubleshoot VoIP and video traffic. Omnipliance VoIP analysis includes complete signaling and media analyses as well as a Call Detail Record (CDR), providing full visibility into calls and video streams as well as comprehensive, real-time statistical and quality-of-service reports for baselining. IT engineers gain access to call data and can replay calls for troubleshooting. Call quality is assessed at both ends.
- **Continuously Availability** of analysis through 24/7 network recording. Each Omnipliance supports a Forensics Capture, which is optimized for post-capture forensic analysis, and a Monitoring Capture, which is optimized to produce more detailed expert and statistical data in real time.

## Omnipliance Configurations

Omnipliances are available in the following configurations:

- **Omnipliance TL**
  An ideal solution for monitoring busy high-speed networks, the Omnipliance TL provides real-time recording, monitoring and forensic analysis for up to 64 TB of recorded traffic. Optional OmniStorage disk arrays allow the internal storage of the Omnipliance TL to be doubled, increasing the capacity of a single Omnipliance TL to 128 TB.
- **Omnipliance MX**
  A powerful, affordable network appliance for capturing and analyzing traffic from more demanding 1G and 10G networks, including datacenters, network backbones, and WAN links.
- **Omnipliance CX**
  WildPackets’ most affordable network traffic recorder, is an ideal solution for monitoring less demanding 1G and 10G networks like those found in small- medium-sized businesses (SMBs), and remote locations such as branch offices.
- **Omnipliance Portable**
  Omnipliance Portable is a rugged, portable appliance capable of recording and analyzing up to 6 TB of network traffic from 1G and 10G networks. Traffic captured with Omnipliance Portable can be analyzed with OmniPeek Enterprise or OmniPeek Connect.

The diagram below shows how Omnipliances can be deployed on an enterprise network. Individual Omnipliances continuously collect and analysis network traffic from network segments throughout the organization. The optional WatchPoint server provides high-level reporting and trend analysis for all network segments under management.



**Omnipliances monitoring a distributed enterprise network.**

## Conclusion

Networks are continuing to increase in speed and complexity. Security attacks are likely to continue evolving in complexity and stealth. User expectations for network performance will continue rising and increasingly involve a variety of rich media formats and mobile devices. Network complexity is here to stay. Business operations will remain network-centric. To ensure that networks are performing optimally and securely, IT organizations must have continuous access to in-depth analysis of network traffic--and network forensics provides that critical access.

WildPackets helps IT organizations analyze data by capturing network traffic at key network points while minimizing 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, WildPackets Omnipliances enable IT organizations to continuously monitor, optimize, and secure networks of all speeds.

## 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 at sales@wildpackets.com or (925) 937-3200.