Miercom

Lab Testing Summary Report

October 2010

Report 101026

Product Category:

Network Recorder

Vendor Tested:

WildPackets

Products Tested:

TimeLine Network Recorder

Miercom Performance Verified™

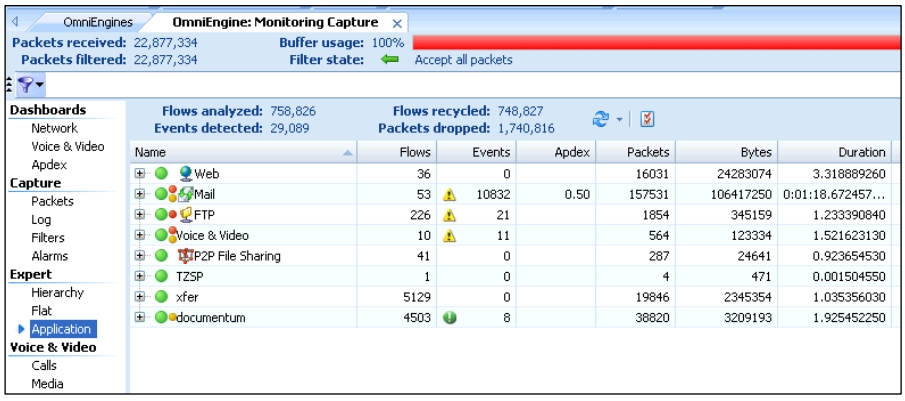
Key findings and conclusions:

- **WildPackets TimeLine network recorder simultaneously captures and analyzes network traffic to disk at a sustained rate of 11.2 Gbps with zero packet loss**
- **Displays crucial network statistics in an intuitive visual format with no negative impact on capture-to-disk rate**
- **Historical data retrieval efficiency is maximized**
- **Network recorder analyzes multiple types of traffic, protocols and packet sizes traversing the enterprise network**
- **When compared to similar products, TimeLine Network Recorder is one of the fastest, continuous network capture and analysis solutions in its class**

WildPackets TimeLine network recorder featuring the OmniPeek network analyzer software was evaluated by Miercom for the functionality and performance of its forensic capture and real-time monitoring capabilities. We examined the network information provided by the timeline graph, real-time monitoring performance and tested the forensic search capabilities of the appliance using the included forensic search templates.

The OmniPeek network analyzer software is designed to work with the TimeLine Network Recorder as a console to analyze network forensics consisting of all frame size distribution with speeds of up to 11.2 Gbps. See *Figure 2 on page 2*. Network forensics were analyzed by capturing traffic to disk or by monitoring the traffic in real time. The TimeLine 10G Bundle allows high data rate captures in enterprise networks. The TimeLine network recorder features up to 32TB of hard drive storage for data capture. WildPackets TimeLine captures traffic to disk for later review of the recorded data for further forensic analysis. The real-time

Figure 1: WildPackets Timeline Network Recorder Application Tab Analysis



Source: Miercom, October 2010

Screen shot section of the application tab displaying the different types of application protocols flowing through the network, as seen by the network recorder.

monitoring feature allows the analysis of high traffic rates in detail as it is happening without losing any performance.

Capture to Disk

The capture to disk feature records network traffic directly to TimeLine. As the forensic capture is recording data from the network, the Forensics tab displays the amount of data being captured. This tab displays traffic in various formats as it is being captured. The display can be switched between Mbits/s, unicast/multicast/broadcast, packet sizes, VLAN/MPLS, Mbits/s and Packets/s and then broken out by protocols, depending on what needs to be examined. All data is represented on the timeline graph in charts.

Forensics Analysis

The Forensic Search option has a few preset templates based on common traffic types that can be used for focusing on analyzing data as it passes through a network. The Overview template searches the data captured and displays the network overview, captured packets, statistics of nodes, protocols and a summary. TimeLine also allows the creation of a custom template for the type of data being analyzed. A forensic search can be initiated either during the processing of data capture or at the end of the capture.

Forensic search is initiated by choosing a time-range on the timeline graph by selecting two points. The two selected points each represent a date and time for the TimeLine network recorder to perform its forensic analysis. Before starting the forensic search, the date and time can be further edited to meet a specific time period. Other options such as filters, analysis and output can be configured for more granular results. See *Figure 3 on page 3.*

The TimeLine network recorder can analyze an enterprise network consisting of many types of traffic, protocols and packet sizes. Complex networks need the capabilities of network forensics to ensure that they are running at top performance without network issues.

Real-time Monitoring

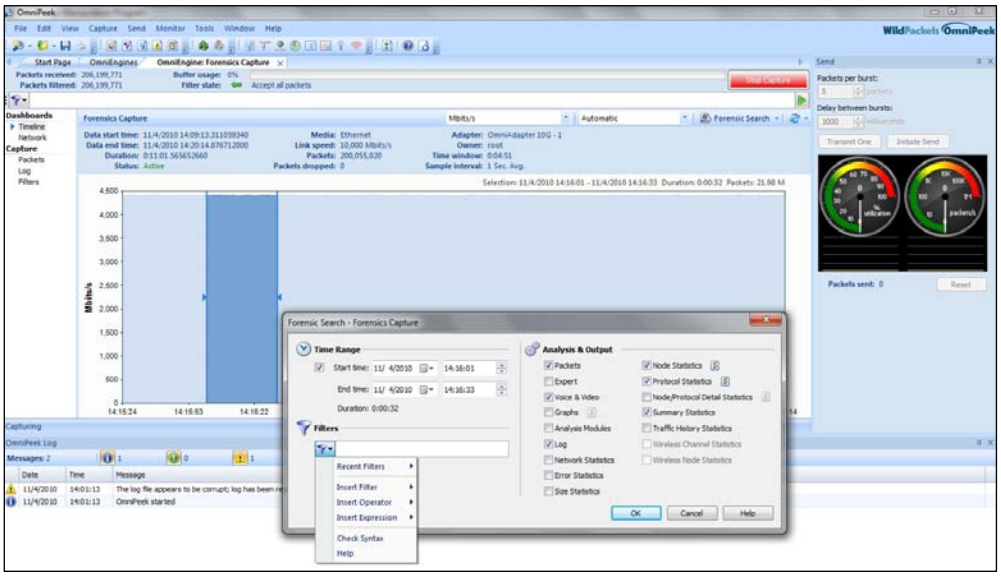
The WildPackets TimeLine network recorder is capable of displaying network traffic in real-time as data is being passed through the network without being captured directly to disk. In our testing, we simulated voice traffic passing through the TimeLine network recorder. TimeLine was able to

Figure 2: WildPackets TimeLine Network Analyzer Forensics Tab View Mbits/Second Display

Source: Miercom, October 2010

Screen shot of the Forensics tab on the TimeLine Network Analyzer showing 11.2 Gbps sustained capture-to-disk rate while displaying key network statistics with zero packet loss.

Figure 3: WildPackets TimeLine Network Recorder Timeline Chart
Time range selected for forensic search

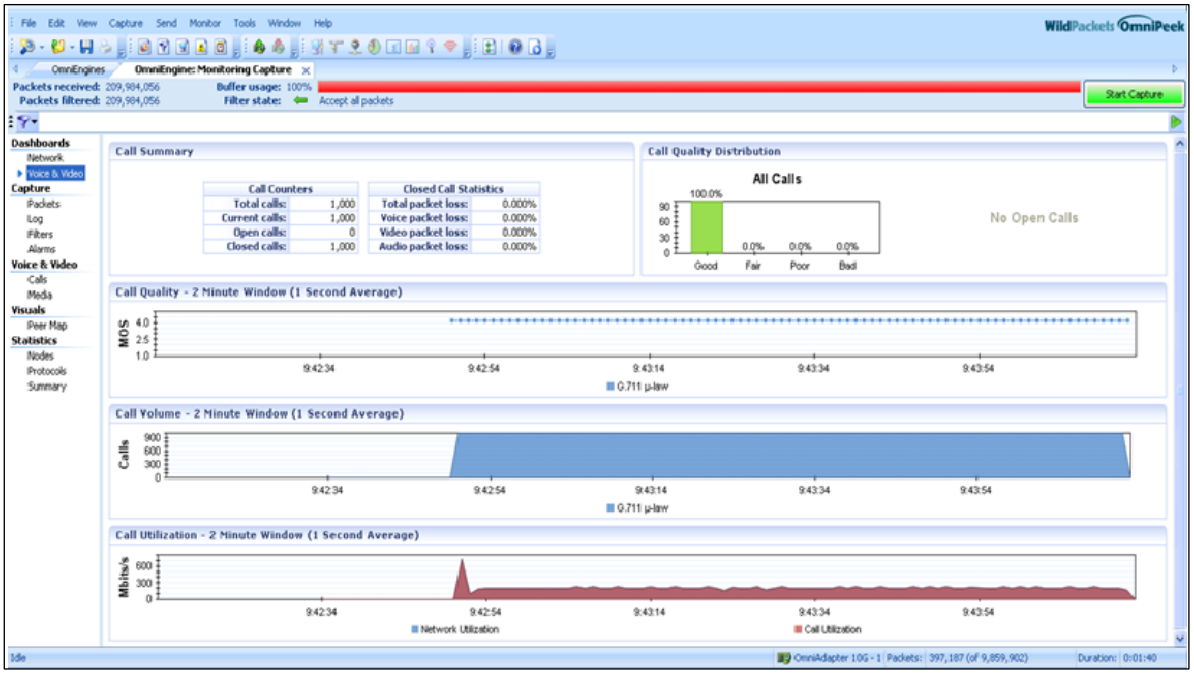


Source: Miercom, October 2010

The selected time range on the Forensic Search dialog box is shown with the different options to choose in creating a forensic search.

give in-depth information about the calls being generated. Call quality, call quality distribution, call volume, and call utilization are included in the default view of the Voice and Video dashboard in the Monitoring Capture window. See *Figure 4 on page 3.* We were impressed by the amount of information that is available when the TimeLine network recorder is running in real-time monitoring mode. The TimeLine network recorder was able to analyze 1,000 concurrent simulated voice calls and

Figure 4: OmniEngine Monitoring Capture
Voice and Video Dashboard in the Monitoring Capture Window

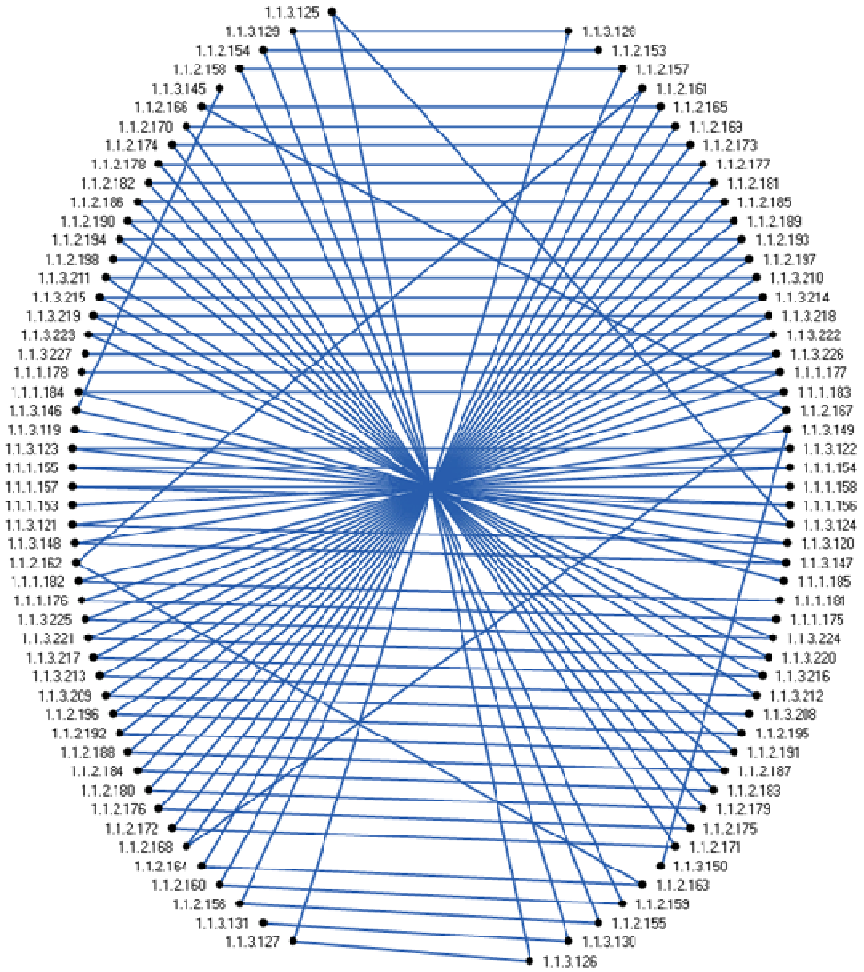


Source: Miercom, October 2010

The Voice and Video dashboard displays call information that was seen on the network.

Peer map diagram of a healthy network that consists of simultaneous voice calls in real-time monitoring mode.

Figure 5: Peer Map
Simultaneous Voice Calls in Real-time Monitoring Mode



Source: Miercom, October 2010

display information about the calls without compromising the performance of the appliance.

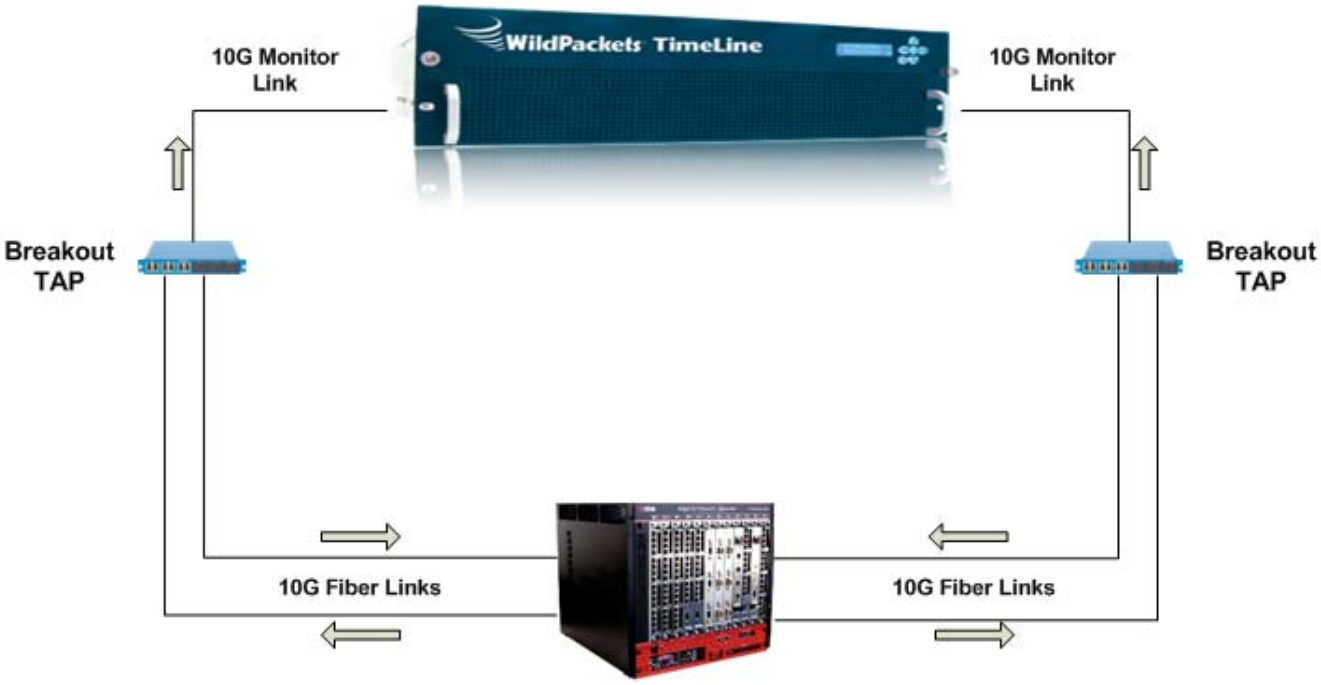
The Peer Map option shows how end-to-end devices are communicating through connecting IP addresses. The Peer Map can be a useful tool for troubleshooting network problems, such as traffic overloads or faults. For example, if there is a slowdown in the network or in the number of calls being dropped, the Peer Map can display the communication addresses to examine the problem. See *Figure 5.*

Bottom Line

The WildPackets TimeLine network recorder was capable of continually capturing and analyzing network forensics in a high data rate network.

Testing showed that forensic analysis provided much insight into the current, moment-to-moment status of an enterprise network. Overall, the TimeLine network recorder proved to be an easy to use, professional network forensics analyzer.

Test Bed Diagram



How We Did It

The WildPackets TimeLine network recorder was tested for functionality of its forensic capture to disk and real-time monitoring features. We validated the capabilities of capturing traffic at 10Gb/s rates and performing network forensics in real-time. The timeline graph, forensic search templates and filtering features were also reviewed to ensure accurate functionality of the product.

The Ixia XM12 chassis was used to generate an Emix and simulated voice calls. Emix traffic consisted of HTTP, POP3, FTP, SMTP and p2p file sharing. Voice calls were generated using the G.711audio codec, each call containing a unique SSRC with all calls totaling 1,000. All traffic contained various protocols, packet sizes and nodes at high data rates and was passed through the TimeLine network recorder using two Network Critical 10G Fiber Optic Breakout TAPs (http://www.networkcritical.com/).

Miercom recognizes Ixia (www.ixia.com) as an industry leader in the testing of networking equipment. Generated traffic was sent from the Ixia XM12 which passed through the breakout TAPs and forwarded to the TimeLine network recorder through the TAPs monitor ports. All traffic that the Ixia chassis sends is mirrored out of the monitor port and is either captured or monitored by the TimeLine for forensic analysis.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for details on the configurations applied to the Switch Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

Miercom Performance Verified

Based on our hands-on testing and review, the WildPackets TimeLine network recorder is awarded Performance Verified for being one of the fastest, continuous network capture and analysis products of its class.

TimeLine Network Recorder simultaneously captures and monitors enterprise network traffic at an impressive sustained rate of 11.2 Gbps with no packet loss.

Highlights of the TimeLine network recorder are the high capture to disk speed for traffic recording, real-time visual forensics displays and device communication using peer mapping. This recorder shows superior design and performance for use in network forensic analysis.

WildPackets TimeLine Network Recorder

WildPackets Inc.
1340 Treat Boulevard
Suite 500
Walnut Creek, CA
1-800-466-2447
www.wildpackets.com

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report. Consult with professional services such as Miercom Consulting for specific customer needs analysis.