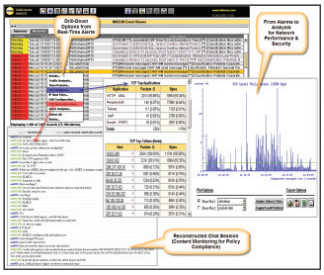
We examine tools that do much of what traditional forensics tools do, alongside solutions that analyze traffic over the network as well, says Peter Stephenson.

There are two classes of tools that seem to be lumped into the network forensics category. The first category is tools that do much of what traditional computer forensics tools do – only they do it over a network. The second category is tools that analyze traffic over the network. We saw both.

The tools that analyze computers over the network usually are able to look at some things that typical computer forensics tools cannot see. It also is easy to watch file openings and closings. These additional abilities provide the analyst with more forensic data, while allowing a traditional view of the device's media.

The network forensic tools that watch the traffic on the network are of more than one type as well. Some of these tools are designed specifically for forensic analysis of network activity. Some – most, in fact – are intended to do double duty as log aggregators/analysts and forensic analysis tools.

NetDetector



Vendor	NIKSUN
Price	starts at $10,000
Contact	www.niksun.com

The NIKSUN NetDetector goes way beyond simple network-based forensics. This appliance features not only the ability to do forensics and incident analysis, but it also has an onboard intrusion detection system and can do complete network security surveillance. Beyond analysis deep within the packet, this product can also reconstruct applications, such as web browsers and even chat and web-based email.

SC MAGAZINE BEST BUY

We found this product quite easy to use. The setup takes just a few minutes and most of it is unpacking the appliance. Initial configuration can be done by either connecting a monitor and keyboard directly to the appliance or through a HyperTerminal connection. After entering a few commands to set time and date, we were taken through a brief setup wizard to set IP addresses and IP settings, such as DNS and gateway. Once that was completed, we just plugged it into our network tap and accessed the web GUI. The Java-based web GUI is easy and intuitive to navigate and we were looking at data in no time.

This product is a solid performer. It sits off of a hub, the span port of a switch or a network tap so it sees all network traffic and is able to record anything that goes in or out of the enterprise. When doing analysis, we found drilling down into the many graphs to be an easy task, and finding the exact data was quick and efficient.

This product comes with two main guides. Both guides include many screen shots and diagrams.

Customers get one year of support included with the purchase of the NIKSUN appliance. Support offered includes phone and email support, as well as access to a support portal via the web. This portal includes access to the latest technical advisories, FAQs, worm/virus notes, learning tools and product documentation.

At a price starting at $10,000, this product is an excellent value for the money. The combination of analysis capability and application reconstruction, along with simple intuitiveness, makes the NIKSUN NetDetector a solid asset to almost any organization.

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Easy to use with deep drill down and application reconstruction ability.
Weaknesses None that we found.
Verdict A solid product that not only provides good log analysis, it has the forensics chops to get the investigative job done. Our Best Buy.

A solid product that not only provides good log analysis, it has the forensics chops to get the investigative job done. Our Best Buy.

Peter Stephenson

NIKSUN®

NIKSUN, Inc.
1100 Cornwall Road
Monmouth Junction, New Jersey 08852
Toll-Free: (888) 504-3336
Tel: (732) 821-5000 • Fax: (732) 821-6000
Email: info@niksun.com