

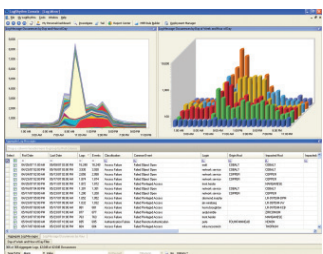
We examine tools that do much of what traditional forensics tools do, alongside solutions that analyze traffic over the network as well, says Peter Stephenson.

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.

## LogRhythm v4.0



**Vendor** LogRhythm  
**Price** \$20,000  
**Contact** [www.logrhythm.com](http://www.logrhythm.com)

This is a serious log analysis tool. It covers all the bases that you need to cover for network forensics. The appliance contains all of the features you would expect in a SIM [security information management], plus the ones you need for managing log evidence. Its log management program allows long-term archiving of log contents. In a forensic environment, you would save the raw logs in a chain of custody and perform all analysis on LogRhythm's archived data, never taking the chance of corrupting actual evidence.

The LogRhythm appliance is easy to setup and deploy. Since it is watching the network all the time in its role as a log correlator and analyzer, it will have everything you need to perform network forensics. It has the ability to take data from most types of logs found on a network. Additionally, its universal database log adapter allows it to gather logs from most types of database systems. This is a major forensic benefit.

If we were to pick a single feature that characterizes high performance for the forensic capabilities of this product it would be the Log Miner. This function provides multiple, innovative ways to view log data from multiple sources. The displays tell a story quickly, leading to drill-downs that access exactly what you are looking for.

LogRhythm provides good documentation to meet the needs of both administrators and end-users. The documentation is well laid out and easy to follow with good examples and script code.

Users have the the option of web, email, and phone support. Also, LogRhythm offers a support portal

that includes specific resources to assist customers in troubleshooting problems. To round out the help list, other available services offered by the company are deployment and implementation planning, custom configuration, training and managed services.

Starting at \$20,000, this is a very good value, even if all you want it for is forensics. If you plan to implement the LogRhythm appliance as a full featured SIM, it is an even better deal.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>Strengths</b> One of the best network log analysis tools we've seen	
<b>Weaknesses</b> None that we found.	
<b>Verdict</b> Top-end network analysis tool. This one gave our Best Buy a strong run for its money, but still we rate it Recommended.	



One of the best network log analysis tools we've seen

Peter Stephenson

3195 Sterling Circle, Boulder, CO 80301  
 Phone: 303-413-8745 • Fax: 303-413-8791 • [www.logrhythm.com](http://www.logrhythm.com)