

Valuable data resides in a number of locations throughout the digital continuum, but an interdisciplinary approach is required to find and interpret it, says **Keith Gilbert**.

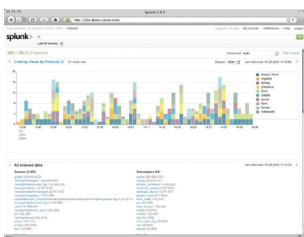
One are the days in which conducting a forensic analysis meant pulling the plug and imaging the hard drive. We now know that valuable investigative data resides in a large variety of locations throughout the digital continuum. A successful investigation may rely on the ability to find

and interpret a variety of data from these multiple locations.

As a result, the number of tools being designed and marketed with forensic capabilities is growing. The traditional media analysis tools definitely still have a firm place in the investigative process, but they now often include the ability to

carry out all the traditional tasks over the network. Adding to those traditional tasks, some of these tools also include the ability to complete a live analysis of a target system over the network as well. Once you've moved past the more traditional products, they become more specialized, and in some cases, less obvious.

## Splunk



**Vendor** Splunk

**Price** enterprise license starting at \$7,500

**Contact** [www.splunk.com](http://www.splunk.com)

Where a normal search engine would let you search the web, Splunk is advertised as a software solution that indexes and searches all info in your data center environment, giving easier access to logging utilities for incident response and network forensics.

Installation is simple, asking only whether or not to log data from the current machine. Splunk supports many different log types and logging utilities from which it can monitor, analyze and correlate data. The entire interface is intuitive and easy to navigate. It takes little time to understand and use basic features. The management system in Splunk is hassle-free – from adding data inputs to adding users.

Users can be restricted to specific data sets and to displaying correlations of the sets. Splunk has features to graph and chart, making the data easier to grasp, as well as to explain to others. The product also has a “Live Tail” feature, letting you view, in near real-time, all incoming logs. In our test bed, Splunk performed very well, with searches taking seconds. It uses AJAX to display results.

Splunk has basic, free support, as well as paid options. At no cost, there are support forums, email and online ticket-based systems and IRC support channels. When purchasing enterprise support, at 20 percent the list price, users receive phone support and guaranteed response times.

There are several different options for documentation. It's all easy to understand. There are also FAQs and cheat-sheets to help along the beginning administrator or user.

Depending on the level of support necessary and the amount of logging required, the enterprise licensing may be worth it – the free Splunk Basic can handle up to 500mb of data, but if more is needed the enterprise edition is a must-have, starting at \$7,500.

Splunk is an excellent and efficient product for aggregating the logs in your entire IT infrastructure, whether for security, network, event or general log management. However, it must be used with other forensic tools since it is not really a forensic tool in its own right.

Splunk just announced its Enterprise Security Suite (ESS), which includes some basic forensic searches and alerts. In July 2009, Splunk ESS 2.0 will include a more robust set of searches, alerts and correlations for forensic uses.

### SC MAGAZINE RATING

Ease of use	★★★★★
Features	★★★☆☆
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

### OVERALL RATING ★★★★★

**Strengths** Intuitive interface, expansive documentation.

**Weaknesses** No functions specifically for forensic analysis and management of logs.

**Verdict** Powerful yet simple log aggregation technology. Definitely worth a look.



Intuitive interface, expansive documentation.

Keith Gilbert



#### Splunk Inc.

250 Brannan Street, San Francisco, CA 94107  
 phone: +1 415.848.8400 • fax: +1 415-568-4259  
 +1 866.GET.SPLUNK (1 866.438.7758)  
 info@splunk.com • www.splunk.com