

Corporate needs driven by regulatory necessity and incident management are beginning to call the shots in the forensic arena, reports **Peter Stephenson**.

This month we looked at a wide variety of digital forensic tools. This category has been growing rapidly, diversifying and maturing in the past two years. However, there are some interesting aspects to those growth phenomena. First, we are beginning to see real inno-

vation in tool sets, but virtually none of it is in traditional computer forensics tools. In that class, we saw, essentially, nothing new since we reviewed them last year.

In many respects, the computer forensics product leaders are indistinguishable from each other. Advances that have come at all

have been in areas that are intended to keep pace with emerging forensic requirements, such as the increasing number of media types that need to be analyzed.

This year our observation is that there really is very little difference among the leaders beyond a feature here or there.

Device Seizure v. 1.1



Vendor Paraben
Price \$895, plus support
Contact www.paraben.com

This is what Paraben is noted for. Device seizure is a neat little product that lets you seize and perform forensic analysis on cell phones, PDAs and other mobile devices. The single CD has everything you need, and it even comes with PDA and cellular device seizure procedures.

Set-up is about as simple as one could want. Put the CD in the computer you are going to use as your analysis computer, tell it to install, and stand back while the program does all the work. Once the installation is complete, you have a clean, easy to manage user interface that looks a lot like the typical forensic tool interface. Experienced

forensic analysts will feel at home in the desktop's familiar surroundings.

One excellent feature of Device Seizure is its embedded case management software. This allows the creation of detailed reports that can be provided with evidence, or used as stand-alone forensic reports. The product really is a collection of dedicated modules that install under a common user interface. The modules are very well integrated, but should it become necessary, it is easy to add new modules as they become available.

In addition to handling most of today's popular cell phones, this nifty tool handles PDAs that use a variety of operating systems, including Palm, BlackBerry, Windows CE and Symbian, among others. Searching the device is a snap and full GSM SIM card information can be acquired. The tool reads email and can read the Windows CE registry. Virtually every function needed to perform a forensic analysis on a cell phone or PDA is here. Images are encrypted and hashed, of course, and the tool

can be used to analyze PDA files, such as backups stored on a PC.

There is no manual with Device Seizure, but there is a help file. However, the product is intuitive and using it effectively is almost a no-brainer for digital forensic analysts with experience. Support is available 24/7, although we cannot imagine needing much. The price is right as well. At \$895, we think it is a very good value and a must-have that won't break the bank for any lab that needs to process cell phones and PDAs.

SC MAGAZINE RATING	
Documentation	★★★★☆
Ease of use	★★★★★
Features	★★★★★
Performance	★★★★★
Support	★★★★☆
Value for money	★★★★★
OVERALL RATING	★★★★★
Strengths Simple to use; good reporting; lots of features.	
Weaknesses We'd like a little more documentation.	
Verdict If you are processing mobile devices, you need this tool.	



Simple to use;
good reporting;
lots of features.

Peter Stephenson



Paraben Corporation
 PO Box 970483
 Orem UT 84097-0483
www.paraben.com