



the DIGITAL INVESTIGATOR

JULY/AUGUST 2010



Partners in Crime (Fighting)

Paraben offers comprehensive digital forensic solutions designed to help investigators keep pace with the latest technologies.

Computer forensics examiners face a constant struggle to keep up with the ever-changing array of hardware and software encountered in the field. Often they must retreat to their labs to test the behavior of new technologies. Networking and sharing knowledge with other specialists also helps them keep pace with technological development. Even then, investigators need a strong vendor partner to provide new investigative tools.

Paraben Corp. has played a key role in the advancement of computer forensics since 2002, when it released the first commercial tool for forensic examination of PDAs. Paraben remains committed to developing useful and innovative solutions to the problems faced by investigators and law enforcement.

“Paraben was founded in 1999 as a shareware company that developed games, flow charts and other helpful

Continued on page 2

Partners in Crime (Fighting)

tools for the consumer market,” said Paraben CEO Amber Schroader. “When I came on board full time in 2001 we changed direction and began developing digital forensic tools. Our first tool, PDA Seizure, was the first of its kind in the industry to process PDA devices as digital evidence. Since that time we have added many digital forensic tools for cell phones, hard drives, networks and now the end-user market.”

Paraben recently released Device Seizure version 4.0, a giant leap forward in the processing of digital evidence from handheld devices. Device Seizure 4.0 supports new models, bringing the total number of supported devices to well over 2,500. Device Seizure 4.0 also includes improved reporting and display of GPS-related data in Google Earth, additional import and export options and new functionality for parsing data from iPhones.

“Most commercial cell phone forensic software only gets logical data files. However, deleted data and user data such as text messages and images can often be found in a physical data dump of a phone,” said Schroader. “If a tool doesn’t have advanced analysis features, it’s probably not getting enough data to analyze. Device Seizure was designed from the ground up as a forensic-grade tool that has been upheld in countless court cases.”

Staying a Step Ahead

Paraben’s products also deliver unmatched performance. P2 Commander features a database-driven, multithreaded architecture for processing digital evidence from hard drives and other media. Version 1.6 improves upon the innovative P2 Commander platform by simplifying the process while adding 64-bit support of Windows 7 and Windows Vista, a new Offline Store (OST) processing engine for e-mail analysis, and many other features. Image Analyzer allows investigators to quickly scan multimedia and graphics files in forensic images to find pornography and other illicit content based on a multiter statistical engine.

Paraben has brought that capability to the end-user with Porn Detection Stick, a thumb drive device that scans all the images on a computer — including deleted images and Internet cache files — and creates a report of suspected pornographic content. It also can be used to securely delete objectionable images. No software is installed on the target machine so there’s no evidence of the search.

Porn Detection Stick is ideal for parents and school and church administrators seeking to eradicate the porn that can easily contaminate a computer, even if no one is actively seeking it out. Probation officers and others in law enforcement can use this tool to quickly determine if pornographic images are present on a computer without training and without involving forensic examiners. Employers can use the Porn

Detection Stick to find pornographic content that can expose the company to legal risks.

Paraben’s latest focus has been in enterprise forensics. P2 Enterprise takes a unique, proactive approach to forensics by monitoring the enterprise and learning user behavior. Any violation of preset rules or deviations from normal behavior sparks an automatic forensic response. P2 Enterprise Shuttle is a live forensic solution for examiners responsible for incident response.

“All of Paraben’s products are developed within the paradigm of the ‘360 degrees of digital forensics.’ Paraben strives to innovate in each facet of digital evidence, from seizure and acquisition throughout the lifecycle of the investigation and examination process,” said Schroader.

Digital Forensics Mastermind

Schroader has been involved in the field of computer forensics for two decades, gaining extensive experience working with federal, state and local agencies, corporations and private parties. She has developed and taught numerous courses for the computer forensic arena, specializing in wireless forensics and mobile technologies, and has been a contributor to several books in the field.

For Paraben, she is the driving force behind many innovative technologies designed to help investigators with the extraction of digital evidence from hard drives, e-mail and mobile devices. With an aggressive development schedule, she continues to bring new and exciting technology to the computer forensic community worldwide and is dedicated to supporting the investigator through new technologies and training services.

“Paraben has always pushed for innovative approaches to the problems that face the digital forensic investigator and is known for value, integrity and quality when it comes to our tools,” Schroader said. “We continue by giving back to the industry through Paraben’s Forensic Innovation Conference, which is held annually in Park City, Utah, in November.”

Paraben’s Forensic Innovation Conference (PFIC) is affordable and offers a comprehensive agenda in digital forensics, e-discovery and security. For 2010, PFIC has brought together new lab tracks that will provide a hands-on lab experience for computer forensic examiners at all levels. A new vendor showcase room will feature live product demonstrations.

With new technologies constantly being produced, computer forensic examiners cannot be experts in all areas, and may frequently be expected to analyze something they have never encountered before. Paraben is the investigator’s partner in crime fighting, constantly developing tools to analyze new technologies and facilitate the examination of all types of digital evidence.

Blended Cyber Attacks on the Rise

Sophisticated multi-stage (“blended”) attacks combining messaging and Web elements are allowing cybercriminals to improve the effectiveness of their attacks, according to Web security firm Commtouch. The firm’s Threats Trend Report for Q2 2010 finds that fraudsters, malware distributors and spammers used messaging and search results tied to trusted brands such as Apple and Google, holidays such as Mother’s Day, or current events such as World Cup soccer to lure victims to sites hosting spam advertising, malware or phishing.

“Cybercriminals have been forced to change their techniques to evade improved detection technology,” said Asaf Greiner, Commtouch vice president, products. “Complex multi-stage attacks with improved social engineering are proving to be the preferred technique.”

During Q2, Gmail and Yahoo kept the top spots as far as spoofed domains for e-mail distribution, but they have been joined in the top six by Twitter. The Twitter domain was faked in a widespread mailing designed to lure users to a “password reset” Web page that contained malware.

Fighting Retail Crime

The world’s largest online marketplace is partnering with the world’s largest retail trade association to tackle organized retail crime. This unique partnership between eBay and the National Retail Federation will tie in support from the Federal Bureau of Investigation, retailer participation and new technology to identify and attack organized retail crime — specifically crimes in which goods are stolen from brick-and-mortar stores and then sold online.

Organized retail crime has long been an issue plaguing both retailers and secondary marketplaces. In an NRF survey conducted in 2009, 92 percent of retailers said they were victimized by organized retail crime in the previous year, and nearly three-fourths (73 percent) also reported the level of organized retail crime activity had increased.

“Through this partnership, NRF and eBay are putting criminals on notice that they will no longer be able to steal from retailers and abuse the online marketplace for profit,” said eBay spokesman Paul Jones.

The Digital Investigator

Copyright © 2010 CMS Special Interest Publications.
All rights reserved.

Editorial Correspondence:

4941 S. 78th E. Ave., Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address:

Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

The Digital Investigator is published by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.



GET A CLUE

With issues regarding electronic discovery becoming a central aspect of civil and domestic litigation, legal and paralegal professionals increasingly require the ability to identify, collect, preserve and examine data found on computer hard drives and digital storage media.

Ispirian’s digital forensic investigators can help.

Our focus on the digital forensics discipline gives us the training, litigation support experience, report-writing skills and professional involvement necessary to support the e-discovery process and deliver quality, defensible results.

Ispirian’s comprehensive case management solution streamlines communication and provides attorneys and support staff with real-time updates as your cases progress. Using a secure Internet portal, Ispirian investigators and their clients can exchange information, update schedules and view key evidence with 24-hour access to budgets, documents, photos and reports.



Ispirian is a member of the High Technology Crime Investigation Association (HTCIA).

When it comes to making sense of digital evidence, it makes sense to call Ispirian Computer Forensics: (800) 301-4294.



Ispirian Incorporated
Chesterfield, MO 63017
Ph: 636.898.1093
Fax: 636.594.2000

Ispirian Computer Forensics is a licensed Missouri professional investigative agency (MO PI Agency License #2010008265) specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA. Copyright 2010, All Rights Reserved.



Discovering *E*-discovery

E-discovery doesn't always involve litigation. Organizations are using e-discovery processes to aid internal investigations and reduce risk.

E-discovery conventionally refers to the identification, preservation, collection, preparation, review and production of electronically stored information (ESI) in legal and regulatory proceedings. Nearly 90 percent of attorneys expect law firms to engage in e-discovery processes more frequently, according to a recent study by IT industry trade association CompTIA. That fact is hardly surprising since more and more cases involve ESI.

However, many organizations are planning to increase their use of electronic discovery in ways one might not expect. A growing number of firms routinely engage in data collection and informal investigations related to personnel matters, violations of company policies and security breaches. Although these practices do not involve the legal

system, they may nevertheless fall under the umbrella of e-discovery.

In fact, 53 percent of the more than 650 IT professionals surveyed by CompTIA expect the use of e-discovery within their organizations to increase over the next few years. Situations that most often trigger the use of e-discovery include the investigation of an employee suspected of violating company rules (cited by 66 percent of survey respondents), a security breach stemming from an outside threat (cited by 62 percent), a pending lawsuit (cited by 60 percent), an intentional internal security breach (cited by 53 percent), and an unintentional internal security breach (cited by 44 percent).

Reducing Risk

These survey results point to the broader context in which organizations

are looking to utilize e-discovery processes to manage both business and IT risks. According to Tom Eid, research vice president at Gartner, e-discovery helps link business performance with governance, risk and regulatory compliance through data accessibility and transparency. The use of real-time, continuous monitoring and controls for transactions, segregation of duties, application configuration and master data mitigates IT risk, while fraud detection and improved user- and application-level security reduce exposure to legal and regulatory risks.

“Increasingly, more organizations are being confronted with litigation regarding bribery and corruption, foreign corrupt practices, securities and financial fraud, government contracting abuses, and healthcare fraud,” said Eid. “Such unplanned events underscore the need for a more effective enterprise information strategy and information governance policies.”

Fifty percent of organizations surveyed by CompTIA say they have already developed an e-discovery strategy, either partial or comprehensive.

Another 26 percent indicate that their organization has no official e-discovery strategy but has engaged in e-discovery processes informally. Among organizations that have yet to develop an e-discovery strategy, cost and expertise are cited as the primary reasons.

“Many organizations lack expertise in this emerging area,” said Tim Herbert, vice president, research, CompTIA. “That’s significant because the increasingly connected and digital world in which companies operate means the number of situations calling for e-discovery will only grow.”

See You in Court

Of course, litigation is also on the rise, according to the Sixth Annual Litigation Trends Survey released by international law firm Fulbright & Jaworski. Corporate counsel anticipate a big year of litigation, with 42 percent of U.S. respondents anticipating an increase in legal disputes. Sixteen percent of respondents also expect regulatory investigations and whistleblower allegations to increase in 2010.

E-discovery accounts for 30 percent to 50 percent of litigation costs, and 16 percent of those surveyed are planning to spend more on e-discovery this year. However, in-house counsel are also looking at ways to reduce those costs. About a quarter of all companies are using law firms that specialize in e-discovery services. Nearly half of all survey respondents are keeping at least some e-discovery activities in-house, while 22 percent of U.S. companies are outsourcing their main e-discovery functions. Stricter document retention policies, such as systematic destruction, also help keep e-discovery costs down.

Until recently, the market for e-discovery products and services has focused on the U.S., which accounted for approximately 90 percent of revenue in 2008, according to Gartner. Going forward, however, market growth is also expected in common-law jurisdictions, such as Australia, Canada, South Africa and the U.K., as new civil litigation regulations are passed regard-

ing privacy and disclosure. In addition, many organizations based in the U.S. have subsidiaries in countries around the world that will provide further pockets of regional growth. Gartner forecasts worldwide e-discovery software revenue to surpass \$1.2 billion in 2010, a 23 percent increase from 2009.

“The December 2006 amendments to the Federal Rules of Civil Procedures

in the U.S. regarding the discovery of electronically stored information and passing of subsequent similar statutes in other countries has really spurred market interest in e-discovery,” said Eid. “This is prompting many companies to rethink their overall information management strategies, from the policy level to the implementation level.”

Legal, Regulatory Requirements Drive IT Purchasing Decisions

A recent survey of legal, compliance and IT professionals indicates that litigation hold and automated document retention functionality are key drivers in information management purchasing decisions. The survey was conducted at LegalTech New York 2010 by Kroll Ontrack, a provider of information management, data recovery and legal technologies.

The ability to retain documents for business continuity or legal purposes was ranked as the most important factor when utilizing technology to manage electronically stored information (ESI). Survey respondents also consider early case analytics (which allows organizations to identify, classify and sort relevant ESI prior to e-discovery), automated document destruction and storage optimization to be important factors when utilizing technology to manage data for business continuity or legal purposes.

“In addition to managing the growing volumes of electronic data, corporations must cost-effectively and defensibly respond to investigations and requests for production of electronic data,” said George May, vice president of product strategy, Kroll Ontrack. “Organizations must implement defensible retention policies and adequate technology to respond effectively to investigations, litigation and regulatory matters. To stay on top of these demands, implementing an archiving system with robust legal hold capabilities and automating an organization’s document retention and disposal process is more important than ever.”

More than 60 percent of respondents believe their organizations manage corporate data well in preparation for, or response to, legal and regulatory requirements. However, 63 percent claim that inadequate technology and resources are the biggest barriers to effectively managing ESI to meet evolving business needs. One-third of respondents confirm that they either do not have or do not know if they have the appropriate technology tools or an archiving platform to manage the storage and destruction of ESI.

“The most defensible litigation holds center around effective document retention policies and seamless execution. But all too often organizations rely solely on technology without considering the other part of the equation: people and process,” said Jason Straight, vice president of legal technologies business development and consulting services, Kroll Ontrack. “A combination of a sound document retention program, the right tools and a team approach ensures organizations are prepared for the inevitable and can perform a credible, repeatable and defensible ESI request response process.”

Taking Chances

Studies indicate even savvy computer users take unnecessary risks online.

While most computer users consider online privacy to be of extreme importance, many do little or nothing to protect themselves, according to a recent study from the Ponemon Institute.

Meanwhile, another recent study shows some of the most tech-savvy cities in America also rank among the riskiest for cybercrime.

The Ponemon study reveals that Americans are particularly lax when it comes to the amount and type of personal information they share on social media sites. Although more than 80 percent of respondents expressed concern about their security while using social media, more than half of these same individuals admitted they do not take any steps to actively protect themselves.

Remarkably, 90 percent of respondents were under the impression that using social media sites posed no risk, and 60 percent weren't even sure if the social media provider was able to protect their identity. Approximately 40 percent admitted sharing their physical home address through social media applications.

"The study results are extremely telling, especially about measures that users take, or fail to take, in order to protect their identity while using social networks," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute.

Techs and the City

Online risk is particularly high in some cities regarded as hotspots of technology innovation and knowledge, according to a separate study from Symantec's Norton product group. Seattle, Boston and Washington D.C. ranked as the riskiest cities in America for cybercrime, with San Francisco; Raleigh, N.C.; Atlanta; Minneapolis; Denver, Austin, Texas; and Portland, Ore., rounding out the top 10.

Symantec, which partnered with Sperling's BestPlaces to come up with rankings for the nation's 50 largest metro areas, said the survey demonstrates that even skilled and experienced Internet users are at risk when it comes to cybercrime and online insecurity. Norton Internet safety advocate Marian Merritt noted that cybercrime is generally on the rise everywhere, affecting one in five online shoppers and costing Americans \$560 million in 2009 due to online fraud.

"With more people than ever relying on the Internet to stay in touch, shop and pay their bills, feeling confident and secure in our information-driven world is vital," Merritt said.

"This study highlights the cities most at risk of cybercrime and reminds individuals, families and businesses across the country of the hazards they face each time they go online."

The rankings relied on data from Symantec's Security Response team for factors such as the number of malicious attacks, infected machines and spam-generating zom-



bie computers per capita. Sperling's contributed data on the prevalence of computer ownership, Internet use and potentially risky online activities, including online banking and online shopping.

The Wi-Fi Factor

The report noted a clear correlation between the number of public Wi-Fi hotspots and the incidence of cybercrime. San Francisco tops the list for riskiest online behavior and highest number of Wi-Fi hotspots per capita. Atlanta residents experience the most cyber attacks and potential infections. Minneapolis and Portland are near the top for risky online behavior, while Denver and Austin score high across the board.

At the other end of the spectrum, Detroit residents were less likely to participate in risky online behavior compared to other cities in the study, and it also ranked low in cybercrime, access to the Internet, expenditures on computer equipment, and wireless Internet access.

"Despite people's familiarity with technology and the Internet, this study shows that everyone is exposed to a certain level of risk when they are online," said Bert Sperling, founder and researcher of Sperling's Best Places. "No matter where you live — be it Seattle or Detroit — it's important to be vigilant in everyday online behavior in order to protect yourself against cybercrime of all types."

ProtectMyID.com, which sponsored the Ponemon Institute study, offers these suggestions to help users guard their personal information and reduce their exposure to cybercrime:

- **Log off when you leave.** Always log off or enable a secure screen saver when away from the computer or it is not in use. More than 80 percent of respondents leave their computers unsecured.

- **Install and update antivirus software.** Keep antivirus software up-to-date in order to maximize protection against keystroke loggers and other malware commonly used for identity theft. Nearly 70 percent of respondents stated that they do not use any form of antivirus protection on their computer.

- **Make sure your wireless network connection is secure.** If you are operating on a wireless network, always make sure that the network is secure to avoid exposing your personal information while it is in transmission. Approximately 75 percent of individuals said they use an unsecured network.

- **Review and customize security settings.** Research the default account settings when visiting social media sites and make sure to customize personal privacy settings in order to only share information with people you choose.

- **Pick a password that can't be cracked.** Do not choose a password that incorporates common information, such as a pet's name or your hometown. Approximately 40 percent of those surveyed said they use a password known to individuals other than themselves.



Files lost?

E-mails missing?

System hacked?

WE'RE ON THE CASE!

It is estimated that 90 percent of the world's information is now created and stored in electronic format. Normal data collection and preservation techniques aren't always sufficient when something goes wrong.

Ispirian Incorporated's computer forensic experts have the tools, training and expertise to get to the bottom of any digital mysteries, whether they involve possible computer crimes, regulatory compliance or simply tracking down lost data.

Ispirian understands how data is stored, where to look for digital evidence and how to recover that evidence from various types of file systems while ensuring that it is not altered in any way. This allows us to identify, locate, extract and preserve data from computer systems and media for specific purposes, such as to provide evidence of a cyber crime or to confirm a violation of corporate policies.



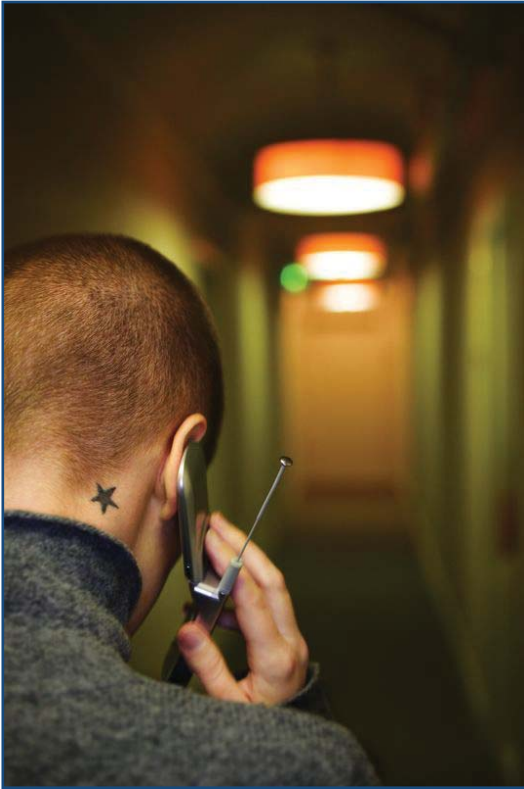
Ispirian is a member of the High Technology Crime Investigation Association (HTCIA).



Ispirian Incorporated
Chesterfield, MO 63017
Ph: 636.898.1093
Fax: 636.594.2000

Ispirian Computer Forensics is a licensed Missouri professional investigative agency (MO PI Agency License #2010008265) specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA. Copyright 2010, All Rights Reserved.

Is it just a phone call, or is it the scene of a crime?



Millions of people today rely on mobile gadgets for personal and professional communications. Unfortunately, these devices are also frequently used in dishonest or criminal acts. Paraben's Device Seizure is a powerful tool for searching these devices for evidence of illicit activity.

Unlike other forensic tools that are simply modified data management software, Device Seizure has its roots in digital forensics with features such as full physical data acquisition, deleted data recovery, advanced analysis, evidence protection and comprehensive reporting. It supports thousands of cell phone models, as well as a wide range of PDA operating systems and Garmin GPS devices.

From software to hardware, Paraben covers the complete range of needs of any investigator — whether at the forensic or detective level. The data is within, and we have what the tools to extract, maintain and validate handheld evidence.

