

# the DIGITAL INVESTIGATOR

MARCH/APRIL 2010

## Licensed to Investigate?

Computer forensic examiners in Missouri must now obtain a Private Investigator license.

*“Badges? We don’t need no stinking badges!”*

— *Blazing Saddles*

**N**o, you don’t need a badge to be a computer forensic examiner. But you do need a Private Investigator license in the State of Missouri.

A growing number of states are requiring that anyone who performs computer forensic work be a licensed private detective. Missouri’s statewide private investigator licensing rules went into effect August 28, 2008, and the Missouri Board of Private Investigator Examiners (BPIE) has interpreted the

new rules to apply to computer forensic examiners.

According to Section 324.1100 of the Missouri Statutes, a private investigator is anyone who receives a fee for “any investigation for the purpose of obtaining information pertaining to:

(a) Crimes or wrongs done or threatened against the United States or any state or territory of the United States;

(b) The identity, habits, conduct, business, occupation, honesty, integrity, credibility, knowledge, trustworthiness, efficiency, loyalty, activity, movement, whereabouts, affiliations, associations, transactions, acts, reputation, or character of any person;

(c) The location, disposition, or recovery of lost or stolen property;

(d) Securing evidence to be used before any court, board, officer, or investigating committee;

(e) Sale of personal identification information to the public; or

(f) The cause of responsibility for libel, losses, accident, or damage or



Continued on page 2

# Licensed to Investigate?

injury to persons or property or protection of life or property.”

“A computer forensic investigation will routinely incorporate several of those activities,” said Tom Smith, a forensic scientist with Ispirian Computer Forensics and a member of the American College of Forensic Examiners Institute (ACFEI). “Organizations call on computer forensic scientists to investigate the activities of employees, contractors, and other individuals, and obtain evidence to be used in court. Clearly, except for a limited number of exemptions under the statute, anyone engaging in this line of work must have a PI license.”

## Detective Work

However, many firms that provide these services employ examiners who are not properly licensed. Some computer forensics examiners may be unaware of the law. Even those who are aware of it may not have the background necessary to meet the application requirements.

“The BPIE requires that every PI license applicant pass a written examination on investigator rules and regulations. It’s not the sort of thing a computer technician would know without a background in the field,” said Smith. “In addition, a licensee must complete 16 hours of continuing education biennially. An individual not licensed as a private investigator but hired as an employee of a private investigator agency must complete eight hours of continuing education biennially. The continuing education must be relevant to the PI business and approved by the Board.”

There is an ongoing debate as to whether the PI licensing requirement is needed to protect those who hire computer forensic examiners. The American Bar Association argues that the PI license qualifications have nothing to do with the individual’s expertise in computer forensics, and has asked states not to institute the requirement.

“Opponents to the new rule say that computer experts with many years of experience may not qualify for a PI license, whereas anyone who obtains a PI license can hang out their shingle as a computer forensic examiner, even if they have little or no technical expertise. However, many of us in the computer forensics field have long been frus-

trated by the lack of standards. Just because you’re a ‘techie’ doesn’t mean that you know how to conduct an investigation and collect evidence. At Ispirian, we have both sets of skills and I believe that sets us apart,” said Smith.

## Abide by the Law

The penalties for violating Missouri’s new PI rules are stiff. A first violation is a Class A misdemeanor, punishable by up to a year in prison and a fine of up to a \$1,000. A second or subsequent violation is a Class D felony, punishable by up to four years in prison and a fine of up to a \$5,000 or twice the amount of the offender’s gain from the crime, not to exceed \$20,000.

Those who hire unlicensed computer forensic examiners may also be penalized. For example, lawyers and their clients could face costly and damaging court sanctions. In any event, the efforts of an unlicensed examiner are of little value if the evidence collected cannot be used in court.

“It is a significant risk to your case to hire an examiner who isn’t properly licensed,” Smith said. “It is therefore important to ensure that the examiners who are working for you are not only qualified technology experts, but also hold a valid Missouri PI license or are employed by a properly licensed PI agency.”

Missouri has joined the growing number of states that require computer forensics examiners to be licensed private detectives. Examiners don’t need to carry a badge, but they do have to have the proper credentials to conduct an investigation and gather evidence.

**“Just because you’re a ‘techie’ doesn’t mean that you know how to conduct an investigation and collect evidence. At Ispirian, we have both sets of skills.”**

## 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.

## Botnet Targets Corporate Networks

**A** dangerous new botnet has infected the computers of more than 2,500 corporations around the world, according to NetWitness, a network security firm. The infestation, dubbed the “Kneber botnet” after the username linking the infected systems worldwide, uses a well-known Trojan Horse previously identified as ZeuS to gather login credentials from infected computers.

The company said it first discovered the botnet in January during a routine deployment of the advanced monitoring solutions. Deeper investigation revealed an extensive compromise of commercial and government systems that included 68,000 corporate login credentials, access to e-mail systems, online banking sites, Facebook, Yahoo, Hotmail and other social networking credentials, 2,000 SSL certificate files, and dossier-level data sets on individuals including complete dumps of entire identities from victim machines.

“Conventional malware protection and signature-based intrusion detection systems are by definition inadequate for addressing Kneber or most other advanced threats,” said Amit Yoran, CEO of NetWitness and former director of the National Cyber Security Division. “Organizations that focus on compliance as the objective of their information security programs and have not kept pace with the rapid advances of the threat environment will not see this Trojan until the damage already has occurred. Systems compromised by this botnet provide the attackers not only user credentials and confidential information, but remote access inside the compromised networks.”

## Security Spending Increase Expected

**A**pproximately 40 percent of businesses will significantly increase their spending on new IT security technologies in 2010, according to Forrester Research. The firm expects 42 percent of enterprises to increase IT security spending on new technologies by 5 percent or more this year, and 37 percent of small to mid-sized businesses (SMBs) to do the same.

While data security is perennially the largest budget item for IT organizations, the greatest spending increases are in the area of network security, where 40 percent of enterprises and 36 percent of SMBs expect to spend more in 2010.

Of utmost concern to IT security professionals surveyed is the consumerization of IT — the proliferation of consumer devices in the workplace. Nearly half of all enterprises (46 percent) noted their concerns about smartphones, while 38 percent of enterprises were concerned about Web 2.0 technologies. More than 80 percent of businesses — large and small — identified managing vulnerabilities and complex threats as a high priority in the coming year.



## 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.

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



*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

Copyright © 2009, Ispirian Incorporated, USA. All rights reserved.  
Ispirian Computer Forensics is a Missouri private investigative agency specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA.

# Effective E-mail Management

*An e-mail retention policy and archival solution helps protect against legal, regulatory and business risks.*

If your organization were the target of litigation or a regulatory investigation, you'd likely be required to produce financials, customer records, contracts and related documentation, right?

Not so fast.

All of those e-mails zipping through your messaging system would also be subject to scrutiny. That's right: you would be forced to sift through all of the forwarded jokes, gossip, lunch invitations and other purely social messages to find those relating to the legal or regulatory issue in question. Worse yet, this process could yield messages that might prove damaging to your organization.

A comprehensive e-mail retention policy coupled with an effective e-mail archival solution can help mitigate these risks. By establishing best practices and implementing the right technology tools, organizations can ensure the successful management of e-mail business records, reduce e-discovery costs, improve productivity and enhance security.

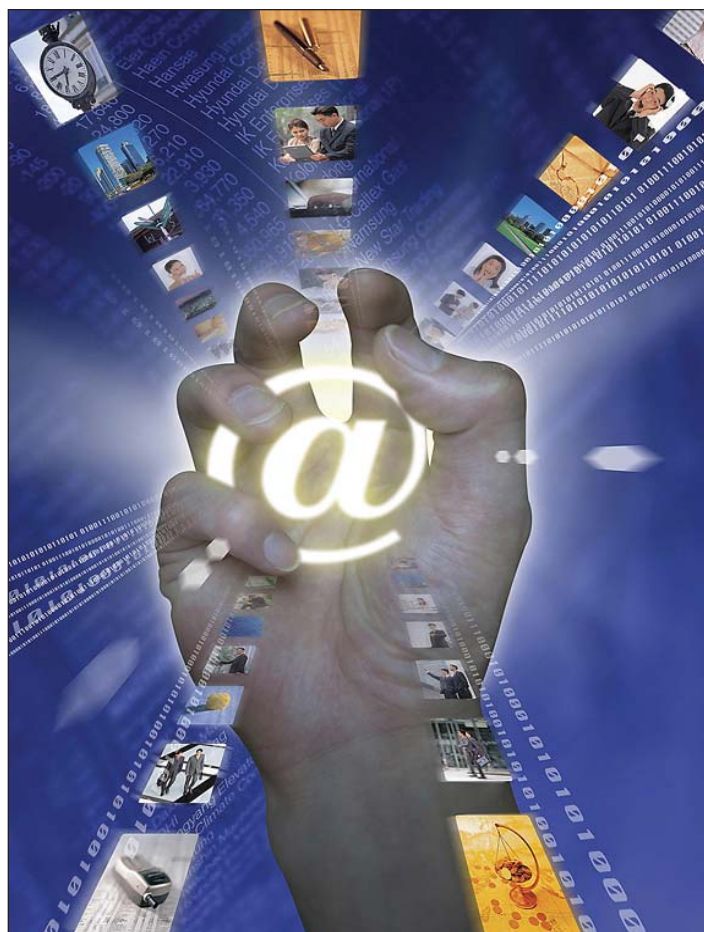
Unfortunately, too few organizations have such policies and procedures in place, waiting instead for an e-discovery or regulatory request before even thinking about e-mail retention and archival. This reactionary approach can prove very costly.

## What Is a 'Business Record?'

A recent study conducted by the Association of Record Managers and Administrators (ARMA) International reveals that a large majority of records management professionals feel unprepared when it comes to e-mail management (72 percent) and e-discovery (68 percent). The study also found that 62 percent of respondents lack an e-mail archiving system.

It's important to remember, however, that implementation of an e-mail archival solution is the final hurdle. An effective e-mail management strategy begins with the development of an e-mail retention policy. Given that only 34 percent of organizations have a formal e-mail retention policy in place, according to the ePolicy Institute, additional education is clearly needed.

The first step is to define, from a legal and regulatory perspective, what constitutes an electronic business record. This clearly written definition helps the organization distinguish messages involving business-related activities and transactions from insignificant and purely personal e-mails.



Once this definition is in place, the organization should make sure that every employee knows what kinds of messages must be retained, and understands his or her role in the organization's overall e-mail retention strategy. Because e-mail is generated throughout the organization, e-mail retention practices cannot focus on the IT department. All employees must take part in the archival of business-related e-mails and the purging of extraneous messages.

## Processes, Training and Automation

Next, organizations should establish the policies and procedures necessary to ensure compliance with legal and regulatory e-mail retention rules. The e-mail retention policy should also address business requirements and risks, and be updated regularly as laws change and new technologies are adopted. In addition to establishing e-mail retention processes, organizations should define electronic business record lifecycles and delete messages as they become outdated.

Employees throughout the organization should receive training on how to comply with the formal e-mail retention policy. This training should stress that policy compliance is

mandatory. Enforcement through disciplinary action and technology tools not only helps ensure effective e-mail management but illustrates to courts and regulators that the organization is serious about its e-mail retention obligations. Demonstrated consistency increases the odds of a favorable ruling should the organization become embroiled in an e-discovery dispute.

E-mail archival solutions play two key roles. First, these technology tools reduce e-discovery costs and help ensure policy compliance by automating e-mail archival processes. E-mail business records are preserved in a way that enables structured searches for rapid compliance with e-discovery and regulatory requests as well as day-to-day business operations.

Second, e-mail archival tools help ensure that e-mail business records meet evidentiary requirements. Because e-mail must be authentic, trustworthy and tamperproof to be considered legally valid, e-mail archival solutions should encrypt messages and protect against the deletion or alteration of archived e-mail.

## Business Benefits

E-discovery is typically touted as the primary reason for establishing an e-mail retention policy and archival solution. Without effective e-mail management, organizations face incredibly expensive and time-consuming e-discovery challenges as well as the potential for costly court sanctions if they fail to meet e-discovery deadlines.

Regulatory requirements also compel organizations to get a handle on e-mail. Sarbanes-Oxley, HIPAA and the Gramm-Leach-Bliley Act all require the preservation, protection and control of business records, with the potential for huge fines and civil and criminal liability for non-compliance. Other government and industry regulations may also come into play.

However, effective e-mail management can provide organizations with a number of key benefits. E-mail is not always a “smoking gun” — in fact, e-mail can often be used to protect the organization from legal liability. The ability to produce the right e-mail records at the right time helps win lawsuits, and may even compel an opponent to settle out of court. E-mail business records also help document transactions and personnel matters and aid in decision-making.

Given today’s litigious environment and increased regulatory scrutiny, organizations face significant e-mail-related risks. Organizations of all sizes need an e-mail retention policy and automated e-mail archival solution to help speed the retrieval of e-mail records related to a legal claim. Effective e-mail management also helps ensure compliance with government and industry regulations and facilitates day-to-day business activities. E-mail is not a simple communication tool but rather a key component of any organization’s business records.



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



# Fake Tech? Arrrrrr!

*Pirated software and hardware costs billions and puts users at risk.*

**C**lassic movie pirates typically were adventurous, clever and courageous fellows with a certain moral ambiguity but a strong sense of honor that would always shine through by the third reel. Today's technology pirates share few of the characteristics of the Hollywood swash-bucklers, apart from a taste for ill-gotten treasure.

Software and hardware piracy costs manufacturers billions of dollars a year in lost sales, to say nothing of the additional costs to consumers in the form of viruses, worms and spyware or defective drives, processors and batteries that wreck their systems. The Business Software Alliance (BSA) estimates software piracy costs at more than \$50 billion annually, while the Alliance for Gray Market and Counterfeit Abatement (AGMA) has pegged knockoff hardware costs at more than \$100 billion a year.

Many counterfeiters operate overseas, and Daniel Baldwin, U.S. Customs and Border Protection (CBP) assistant commissioner for international trade, recently stressed the importance of international partnership in reducing the

growing threat from counterfeit and pirated high-tech products.

"The United States still sees intellectual property as a major priority. And we recognize that this global challenge cannot be solved without global cooperation and collaboration," Baldwin said during a speech at the 2009 International Law Enforcement IP Crime Conference in Dublin. "The problem is huge, but there are lots of things we can accomplish together."

## **Beyond Borders**

Baldwin cited two recent examples of how international cooperation interrupted the counterfeit supply chain. In Operation Cisco Raider, the CBP collaborated with the Royal Canadian Mounted Police and other U.S. government agencies in more than 400 seizures of counterfeit Cisco network hardware and labels with an estimated retail value of more than \$76 million. This joint effort effectively dismantled the North American supply chains for these counterfeit products from China. In Operation Infrastructure, the CBP

worked closely with the European Union to seize 360,000 semiconductors and network hardware components bearing 40 different trademarks during a three-week period.

Baldwin further noted that in fiscal year 2008, the Department of Homeland Security made a record 14,992 intellectual property seizures with a domestic value of more than \$272 million. This was a 10 percent increase in seizures and a 38 percent increase in value over fiscal year 2007.

“We recognize the huge value of our collaboration with the Canadians and the EU on these operations, and we are committed to expanding this type of cooperation,” said Baldwin. “The lessons of these successes were very clear. As we move forward, we can help each other recognize and share information on global risks.”

## The P2P Connection

Software piracy has become a trickier issue due to the relative ease with which transactions can be made online. Individuals are turning to peer-to-peer (P2P) networks and auction sites in staggering numbers to acquire or transfer illegal software, according to the 2009 Internet Piracy Report from the BSA.

BSA uses special technology to monitor P2P networks and auction sites, issuing “takedown requests” when it finds suspicious software being offered. In the first half of 2009, BSA stepped up its efforts in this area and issued almost 2.4 million takedown notices related to P2P and BitTorrent file sharing, an increase of more than 200 percent over the same period in 2008. During the same time frame, BSA used its in-house Internet “crawler” to request the removal of almost 103,000 torrent files from nine of the largest BitTorrent hosting sites worldwide. These torrent files were being used by nearly 2.9 million individuals to download software with a retail value of more than \$974 million.

“Peer-to-Peer networks are ideal for distribution of a wide variety of materials that can be legally shared with large groups and are a tool used by more businesses to enhance productivity. Unfortunately, P2P technology is also a favorite channel for software pirates who see it as the perfect channel through which to distribute illegal and potentially dangerous software,” said Jenny Blank, Senior Director of Legal Affairs for the

BSA. “One of the great disappointments of this technology, for all of its benefits, is that it is now too often seen as the domain only for pirates and malcontents who place no value on the work of software developers and designers.”

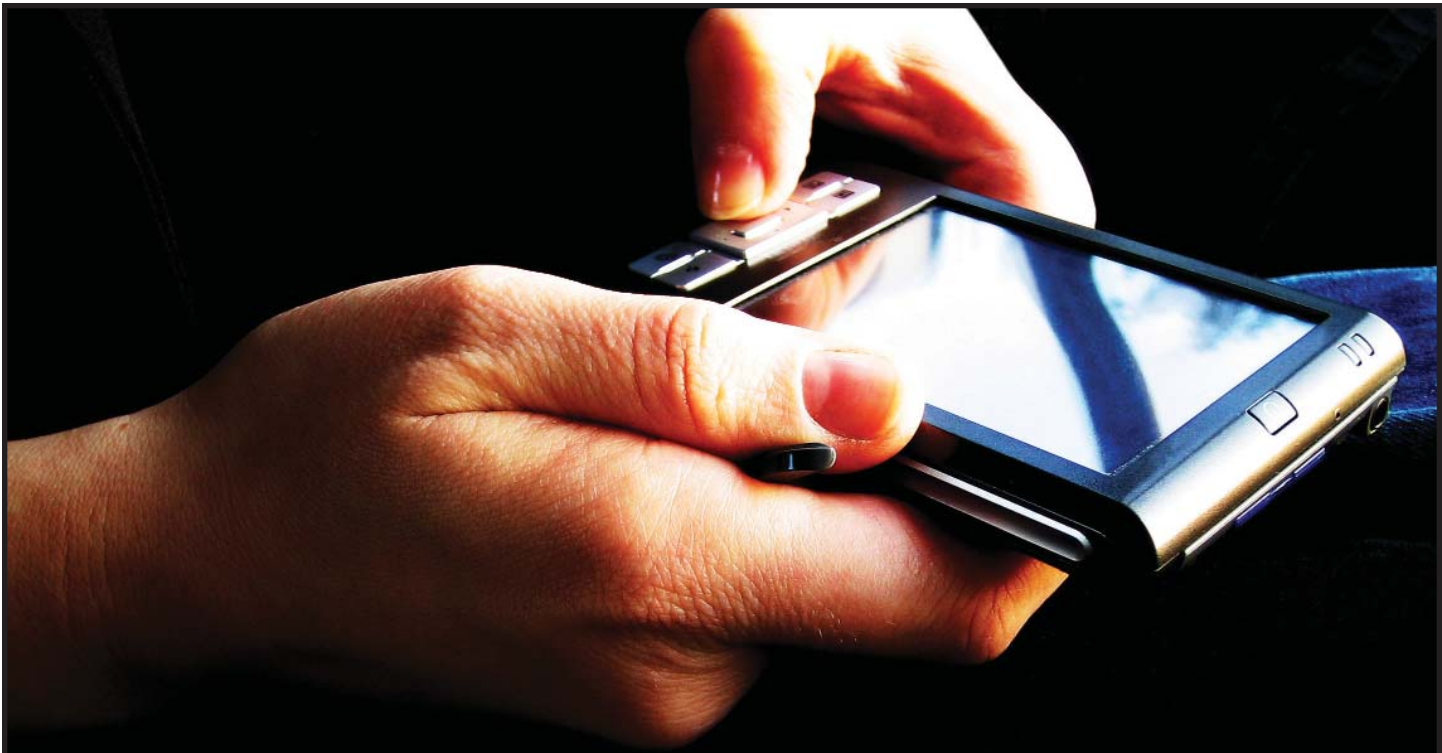
## No Bargain

Beyond the direct economic impact of technology piracy, the BSA report also draws correlations between Internet piracy and the spread of malware. To bypass installation and licensing protections in today’s software, counterfeiters must physically alter the software’s code. Essential elements of the program are often deleted, while unnecessary extras can be inserted. Deleted code will cause the software to behave erratically — displaying error messages or failing to work with other software and devices — and the extra code inserted by counterfeiters may include malware or spyware that can be used to infect a PC with viruses, change settings or even track how someone uses the computer, such as tracking Web sites visited or keystrokes entered. This malicious software can be used to steal personal information such as usernames, passwords and credit card numbers.

“Software piracy is a threat on multiple fronts,” Blank said. “Pirated software can be a breeding ground for malware and can also open users up to crimes such as identity theft. Those who decide to acquire illegal software harm the economy and companies of all sizes. Moreover, those who engage in piracy open themselves up to civil and criminal prosecution.”

While technology piracy has an obvious detrimental impact on manufacturers, end-users run a high degree of risk as well. Beyond malware and viruses, fake software and hardware can lead to computers that freeze, crash or won’t start — while also potentially corrupting critical data. Of course, since the product is counterfeit, there is no hope for tech support, updates or upgrades. All in all, it’s enough to shiver anyone’s timbers.

**“P2P technology is also a favorite channel for software pirates who see it as the perfect channel through which to distribute illegal and potentially dangerous software.”**



## Funny, it doesn't look like a smoking gun.

Cell phones, GPSs, PDAs and other handheld devices have become practically indispensable as business and personal productivity tools these days. In many cases, they can also be repositories of a variety of dirty little secrets in the form of data, text messages and photographs. As such, they have become increasingly important in a broad range of criminal and civil investigations.

Handheld devices are really tiny computers with their own operating systems, file systems, file formats and methods of communication.

Performing a forensic examination on one of these devices takes special software and special knowledge of the way they work, as well as where possible evidence could be stored.

Ispirian Incorporated's computer forensic experts have the specialized tools, training and expertise to properly identify, collect and protect evidentiary data from handheld devices. Call us today to learn more.



*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