



DIGITAL INFORMATION GATHERING & INVESTIGATIVE TECHNOLOGIES, INC.



# fingerprints



Volume II, Issue V

Newsletter Date June 2009

## CONSULTING SERVICES:

- Computer Forensics and Data Recovery
- Corporate Computer Investigations
- Litigation Support Services
- Network Security Advisory services
- General Computer Consulting services

## INSIDE THIS ISSUE:

Proactive Forensics	1
Employee Profile	1
HR Program	2
Who We Are	3
Qualified, Expeirienced	3
Case Study	4

## Proactive Forensics: Shifting the Reactive Paradigm *by Brad Bartram*

When a person hears the phrase “Computer Forensics” more often than not their mind wanders to an episode of CSI or NCIS or another piece of modern entertainment. A professional who has retained the services of a forensics expert might be drawn to their prior experience, which usually surrounds the retrieval of bits and fragments of data from someone’s computer. What both of these perspectives have in common is that they are post-mortem, which is to say they are reactive measures taken to accomplish a defined purpose. Entertainment uses

computer forensics to lift that one piece of critical evidence in order to advance the plot. The legal profession uses computer forensics to build their case.

Computer forensics certainly has its place in the above examples, but forensics can also be used proactively as well. Take, for example, an auditor. This could be a financial auditor or it could be an internal security audit. For purposes of this example, company XYZ retains the services of an outside firm to perform an audit of internal controls that have been placed in operation and testing of operating effectiveness. To-

*continued on page 3*

## Bradley J. Bartram-Senior Forensic Consultant

Bradley J. Bartram has been an information technology professional for over 10 years with a primary focus towards system design, data analysis, and computer and data security. Bradley is currently a Certified Forensic Computer Examiner (CFCE) and Certified Electronic Evidence Collection Specialist (CEECS) through the International Association of Computer Investigative Specialists.

Bradley began his career in the mid-1990s as a technical project manager dealing with satellite communications and the emerging field of satellite internet. His responsibilities included managing large commercial installations on a nationwide scale and reporting to senior executives for many fortune 500 companies as well as managing internal technology resources. Parts of this effort laid the groundwork for a best-of-breed workflow management system that directly allowed the company to secure \$22 million in venture funding.

In 2002, Bradley took a position with a small software consulting company to primarily manage and organize internal network operations as well as be a key asset in ex-



*continued on page 2*



Let DIGITS be your  
digital detective

**“Computer  
Forensics plays  
an important  
role in just  
about every  
forensic  
accounting  
engagement.”**



Information on digital  
media can be difficult  
to find and extract

## Importance of Third Party Forensic imaging and analysis:

The founders and specialists at DIGITS examine the data as digital detectives rather than just IT experts. We are independent, objective, un-biased and conduct our review of the digital facts without prejudice while ensuring that the evidence meets admissibility standards in all courts of law. We maintain proper chain of custody of the evidence and follow strict law enforcement evidence handling procedures. While your IT staff is extremely qualified in managing digital information, special care must be taken to ensure that the files and data is not modified, altered or contaminated during the process of extraction and analysis. A significant number of cases have been settled unfavorably due to good intended IT staff extracting important data and inadvertently modifying important files and metadata that resulted in sanctions under the new Federal Rules of Civil Procedure. Even if your in-house personnel had the necessary tools and training, they (i) will be viewed as lacking independence, (ii) will not have the legal-related experience, and (iii) may not be qualified to serve as an expert in computer forensic investigations in court.

## Bartram *continued from Page 1*

panding their network and security consulting business. During his tenure, Bradley was in charge of development of “next generation” workflow management software and with designing and implementing a scheduling and routing application to manage service industry resources. The resulting software has since been used by some of the largest names in retail and construction industries. From the data and experience collected, Bradley wrote a technical article for the Linux Journal entitled, “Stress Testing an Apache Application Server in a Real World Environment”, which led to an offer by Apress publishing company to act as technical reviewer and contributing author of the 2004 authoritative reference, Pro Apache, 3<sup>rd</sup> Edition.

In 2005, Bradley took time off to complete a degree in Economic Crime Investigation from Hilbert College where he focused on Computer Security. Bradley also worked extensively on a data analysis project as part of the Buffalo Anti-Flipping Task Force where millions of records of public real estate transaction data were analyzed to identify possible leading indicators of fraud. This work assisted in a successful prosecution by the New York

State Office of the Attorney General and also led to presentations and later consultation with the New York State Banking Department about ways fight the problems identified. In 2007, Bradley graduated Summa Cum Laude with a B.S. from Hilbert and as a winner of the Hilbert College award for academic excellence.

After graduation, Bradley took a position with a New York State law enforcement agency, where his first task was to design and implement a system to collect and hold investigative data relating to one of the largest undercover internet investigations taken to date. His efforts on the case helped lead to several industry-changing agreements and being recognized as one of the winners of the High Technology Crime Investigator’s Association 2008 Case of the Year Award. Bradley was also a fully certified Forensic Examiner where he worked on some of the largest cases undertaken by the agency.

Bradley is currently an Adjunct Professor at Hilbert College teaching Computer Forensics and Internet Investigations. He is a current member in good standing of the HTCIA and IACIS.

## Proactive Forensics *continued from page 1*

---

day, most of those controls exist and are based on computers. The audit would normally consist of standard procedures like reviewing documentation in the form of logs, notes, and reports as well as configuration settings for affected systems. Depending on the depth of the audit engagement, interviews with staff would be conducted. All of this is fine and accepted practices, but does it really provide a complete picture? Enter computer forensics.

In today's world, business operates almost exclusively in binary. It is estimated that nearly 80% of all business records produced are never printed. The Computer Security Institute annual Survey estimates that the most expensive computer security incidents were those involving financial fraud with an average reported cost of close to \$500,000. Employees typically have one or more desktop computers connected to various corporate resources. They have laptop computers, smart phones as well as a multitude of computer storage ranging from USB flash drives to external hard drives and even online storage. We also have online access to an array of com-

puter services and resources ranging from email to online collaborative documents to social networking. All of this presents a challenge to a traditional audit because given the sheer numbers of ways for data to be received or transmitted, just finding the right questions to ask can be daunting. Luckily, the computers and devices are adept at keeping track of all of this information, and computer forensics brings that information back into the audit process.

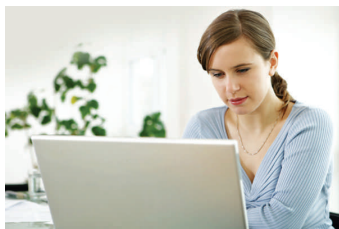
Back to our original example, the audit firm finds that one document in particular is important and needs to be tracked. The XYZ company has it on a protected storage area of the network and five employees have access. An interview with each staff member appears legitimate and it appears the document has been under strict control. But is that the end of the story? That document could have left the company in ways undetectable to normal IT systems. It may have been copied to an external storage device or even mailed using an online service. Forensically, evidence of the document's movement could

be obtained by looking at deleted files or the system registry or even through a careful analysis of the user's internet history. All of this could be done during the audit and possibly prevent this from happening during discovery.

Unfortunately, for a professional that has used a computer forensic professional in the past, the connotation is that computer forensics is expensive and prohibitive except in the direst of circumstances. How could the cost be justified for something as mundane as an audit? The answer is that computer forensics is time consuming and therefore expensive when not approached correctly, but it can be very reasonable when approached as a tool to polish existing audit work. In our scenario, computer forensics would be brought in towards the end of the engagement once the critical pieces of data were identified. The process was employed to identify and report occurrences of a violation of various rules by a small set of employees / documents or both. An exam that would be narrow enough to minimize cost while providing a tangible benefit to the client and provide an unparalleled depth to the firm's audit report.

### **Qualified, Experienced, Tested**

DIGITS team of computer forensics, digital evidence, and information security experts is unparalleled in the industry. The co-founders hold Top Secret Security Clearances with the U.S. Government. Drawing from an array of backgrounds in law enforcement, Academia and the private sector, DIGITS professionals hold certifications from the leading computer forensic associations and software providers. DIGITS experts have provided services and instruction to corporations, federal, state and local law enforcement and governmental agencies around the world, including high level and top secret intelligence and investigative agencies. The DIGITS founders, Michael G. McCartney and James L. Domres, have successfully investigated some of the largest and most complex computer crime cases in the country and are recognized by their peers as leaders in the computer forensic and computer investigative fields. DIGITS professionals are battle-tested, with extensive trial experience, testifying and qualifying as experts in all levels of the justice system.



**DIGITS team of computer forensics, digital evidence, and information security experts is unparalleled in the industry. We can help you meet the IT requirements and components of your SAS70 audit reports .**

## Case Study:

### Forensic Email and Deleted File Analysis – Sexual Harassment

#### The Facts:

ABC Company hired Jane to work in a unit of the company supervised by Jack. After six months, Jane began missing work and eventually ABC Company terminated her employment. Two days later, Jane's attorney sent the Company a letter alleging sexual harassment by Jack. During an internal investigation conducted by the company, it was learned that Jack had a history of sexually inappropriate conduct with the female employees in his unit. Fortunately, the company hired an outside independent computer company which forensically escrowed a copy of Jane's computer upon her termination. A forensic image of Jack's computer was also escrowed and examined as part of the sexual harassment investigation in preparation for litigation.

#### Forensic Findings:

The forensic examination of Jack's computer revealed several deleted performance evaluations during Jane's probation period. The deleted reports indicated that she was a mediocre employee at best. However, the actual performance evaluations located on the computer and ultimately submitted by Jack showed Jane as a stellar employee with the highest ratings available. Jack also had several emails indicating a mutual sexual relationship between Jack and Jane. The forensic examination of Jane's computer showed an even more telling picture. Located within several forensically recovered

deleted-deleted emails on Jane's computer, were very sexually charged and proactive advances towards Jack. The emails revealed that Jane sought out the relationship and was an eager participant in the conduct. There was also evidence in the deleted emails that Jane had promised sexual favors in exchange for positive performance reviews during her probation period.

#### Risk Factors:

The Company was facing a significant sexual harassment claim by a female employee against a supervisor that, through investigation, was determined to have had "some" prior sexual harassment issues that the company should have been aware of. These factors taken alone would have probably resulted in a very unfavorable settlement or verdict.

#### Bottom Line:

The Company was able to present the computer forensic information to the opposing counsel prior to the filing of a formal action and as a result, stopped the action dead in its tracks. Had the company NOT had the forethought to forensically escrow, preserve and analyze the employee computers, they most certainly would have had to rely on standard IT data and investigative information and would have probably settled the action for a substantial amount of money. The Forensic Image and Analysis of the suspect employee computers literally saved the company hundreds of thousands of dollars.

DIGITS  
P.O. BOX 66  
EAST AMHERST, NY 14051

