

technical[®]

Supporting Enterprise Networks and Operating Environments

SUPPORT



The Globalization of the IT Industry

Looking Back and Looking Forward

The IBM REXX/370 Compiler

Page 21

Some Steak Tips for Beefing Up Your Security

Page 23

Recursive SQL

Parsing, Syntax Checking and Interpretation

Conduct a Compelling Business Impact Analysis

JCL Simplified

Infosec Institute's Computer Forensic Examiner Certification

Moving Toward SOX Compliance

APRIL 2006

VOLUME 14, NUMBER 4

NASPA HEADQUARTERS
7044 S. 13TH STREET
OAK CREEK, WI 53154

CHANGE SERVICE REQUESTED

PRRST STD.
U.S. POSTAGE
PAID
PERMIT #1
RANDOM LAKE, WI

FEATURE

**10 The Globalization of the IT Industry—
Looking Back and Looking Forward***By Bill Elder*

ARTICLES

16 Recursive SQL—Part Two*By Rob Mala***21 The IBM REXX/370 Compiler—Part One***By Dave Salt***23 Some Steak Tips for Beefing Up Your Security***By Elizabeth M. Ferrarini***26 Parsing, Syntax Checking and
Interpretation—Part One***By Richard Tsujimoto***30 Conduct a Compelling Business Impact
Analysis***By Leo A. Wrobel***35 Infosec Institute's Computer Forensic
Examiner Certification***By Keith Zielinski***37 Moving Toward SOX Compliance—Part Two***By Dinesh Dattani***NaSPA MISSION STATEMENT:**

The mission of NaSPA, Inc., a not-for-profit organization, shall be to serve as the means to enhance the status and promote the advancement of all network and systems professionals; nurture member's technical and managerial knowledge and skills; improve member's professional careers through the sharing and dispersing of technical information; promote the profession as a whole; further the understanding of the profession and foster understanding and respect for individuals within it; develop and improve educational standards; and assist in the continuing development of ethical standards for practitioners in the industry.

NaSPA serves Information Systems technical professionals working with z/OS, OS/390, MVS, VM, VSE, Windows Operating Systems, UNIX, NetWare and Linux.

The information and articles in this magazine have not been subjected to any formal testing by NaSPA, Inc. or Technical Enterprises, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry and/or changes or enhancements to components, either hardware or software.

The opinions expressed by the authors who contribute to *NaSPA Technical Support* are their own and do not necessarily reflect the official policy of NaSPA, Inc. Articles may be submitted by members of NaSPA, Inc. The articles should be within the scope of host-based, distributed platforms, network communications and data base, and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories and articles become the property of NaSPA, Inc. and may be distributed to, and used by, all of its members.

NaSPA, Inc. is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate computing professionals are welcome to join NaSPA, Inc.

For information on joining NaSPA and for membership rates, see www.NaSPA.com.

NaSPA Technical Support (ISSN 1079-3135) (IPM Agreement Number 0806773) is published monthly by Technical Enterprises Inc., 7044 S. 13th Street, Oak Creek, WI 53154-1429.

POSTMASTER: Send address changes to *NaSPA Technical Support*, 7044 S. 13th Street, Oak Creek, WI 53154-1429.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

COLUMNS

39 MVS Tools & Tricks

Internationalization

*By Sam Golob and Courtney Taylor***41 Shareware Spotlight**

Let's Get Small

*By Jim Justen***43 Working Smarter**

JCL Simplified

*By Jim Moore***45 Career Corner**

Make Sure that Your Resume Gets You in the Door and Keeps You in the Door

By Kathy Bornheimer

DEPARTMENTS

6 President's Letter**7 NaSPA News****7 NaSPA Education Foundation Sponsors****8 The Education Corner****46 NaSPA Services Directory**

Infosec Institute's Computer Forensic Examiner Certification

By Keith Zielinski

OVERVIEW

Not many things today are as important on a global scale as the war on terror is. In an effort to battle this menace to the peace of the world, computers have been put into the forefront of the battle as one of the tools used to combat this threat. Computers are being used by both sides. For example, Ayman al-Zawahiri, the advisor and doctor to Usama Bin Laden, kept a computer in his office building in Afghanistan. In a lucky event for a journalist named Alan Cullison and ultimately the coalition forces, Cullison was able to acquire al-Zawahiri's computer after Kabul fell to the American-led Coalition in late 2001. Unbelievably, that computer had almost a thousand documents, from as far back as 1997. Many of the documents were locked with passwords or encrypted. Though most of them were written in Arabic, some were in French, Farsi, English, or Malay. They involved detailed plans and administrative details for the Al-Qaeda terrorist organization. The journalist sent the computer to a computer forensics examiner. Like in a real life CSI episode, that examiner was able to pull information from the hard drive, including budgets, recruits training manuals, and scouting reports for international attacks. Other documents were also uncovered that showed in detail things such as personnel matters of al-Zawahiri and debates about the merits of suicide operations. As if that wasn't enough, video files, photographs, scanned documents, and web pages that were part of the group's alarmingly sophisticated efforts to establish a global Internet-based publicity and recruitment effort were also retrieved from the computer and used against the group for military and justice cases.

Even without the war on terror, computer crime is not going away and is only getting more and more pervasive. From terrorism and organized crime, to the hacking and cracking of high school kids, the challenges are rising to counter the new threats. For those threats, computer forensics specialists are needed by today's companies and governments to determine the root cause of a hacker attack, collect evidence legally admissible in court, and protect corporate or individuals assets and reputation. It is a highly sought after field and training opportunities abound for those with the interest. If you are one of those with such an interest in the field, the best way to become a forensics expert is to attend a training session with a computer forensics training expert. That, of course, takes time for the training and the money involved in course fees.

Many managers responsible for authorizing training classes can be asking themselves, "We have talented IT people, why should we spend the money on certification on something they already have the skills for?" It really isn't a matter of how smart the staff is, but really more of a matter of ignorance and/or legality. A former drill instructor of mine told me the difference between ignorance and stupidity. He said that stupidity means

you can never learn something remotely complex even if you wanted to; ignorance on the other hand, is being in a position of not knowing something that you can learn, given the time. Granted, there were a lot fewer words used by my former drill instructor and a lot more swearing that is surely not appropriate for this article, but I think you get the point without the colorful commentary. Being ignorant is simply a matter of not knowing what you don't know. Muddling through learning how to find what you are looking for probably depends on what you think you are looking for. If you are looking for information in a non-binding format and you don't positively need to know for certain that you have expunged all of the relevant information from the computer device as possible, then certification training may not be right for you. On the other hand, the legal issues implied in making sure you are grabbing the data from the computer in a fashion that is admissible in a court of law are pretty vast. Expecting someone to pick up those skills is asking a lot for even the most brilliant of IT gurus, though I am sure it has been done.

Another damaging fact to consider with having an untrained person rifling through that computer is the potential for allegations of impropriety and fabricating evidence if the proper standards, techniques, and documentation is not enforced. The following is from www.expertpages.com which defines the legal requirement of what it takes to be an expert witness in court: "Rule 26, Federal Rules of Civil Procedure, requires an expert witness to provide a written report which includes all opinions, the basis for the opinions and the information that was considered in coming to the opinions. The report must include exhibits, such as photographs or diagrams that will be used. Along with the basic qualifications of the witness, education, training and experience, a listing of all publications authored by the witness for the preceding ten years must be provided." Certification clearly would be a method for proving the capabilities of the examiner.

Incorrect methods of examination also have the distinct possibility of damaging evidence. For example, if an ignorant person would access a Word document by opening it in Word first to examine the contents, the date that the file was last accessed would not show that date instead of the original date. The forensic methods and processes deployed by an Infosec Institute certified examiner are designed to safeguard every bit of every byte of data available to be used as evidence.

What differentiates Infosec Institute from the competition? InfoSec Institute was one of the first private companies to offer Computer Forensics training, and has trained over 5,000 computer forensics examiners. Students train in a state of the art computer forensics lab where they have the opportunity to work through 43 different hands-on exercises. The exercises range from recovering data deleted by a criminal, to processing evidence in a legally sound manner, and even performing an exhaustive examination of digital devices including cell phones, PDAs,

and iPods. InfoSec Institute is unique in the industry for offering Live Cases every evening for the duration of the training session, where students get to practice forensics skills on real Department of Justice cases. Expert instructors are on hand with dozens of years of law enforcement and computer forensics experience to guide students past the most common pitfalls in gathering and processing evidence. Following is a quote from a past student, "The computer forensics training at InfoSec Institute is top notch, this is the best IT course I have attended in over 15 years of professional experience. Your program is invaluable to our organization and will help us detect the origins of computer crime and general IT abuse. The instructor is extraordinary and has real-world experience has helped us differentiate the different tools with their benefits. He has provided very valuable knowledge and I would recommend anyone interested to attend this course."

Nagaraj Kedda
JP Morgan Chase/BankOne
FVP INFORMATION SECURITY

GETTING CERTIFIED

Like in life, you should have something that proved you were there. Certification is one way of proving that you have what it takes to do the job of a computer forensic examiner and that you took the training that got you there. It also is the standard that many employers use to see how you rate against your peers. A 5 day training course is offered by InfoSec Institute in various locations and follows the following schedule:

Day 1:

- ▼ Introduction to the theory of computer forensics.
- ▼ The legal, privacy, and ethical considerations to make during a real world case.
- ▼ Foundation of computer forensics and file recovery on Windows operating systems.

Day 2:

- ▼ File recovery and the disk imaging process.
- ▼ Creating a forensics boot disk with forensics utilities.
- ▼ Recovery of various Windows file metadata.
- ▼ Recovery of internet usage data.

Day 3:

- ▼ Court of law findings presentation process.
- ▼ Process to make exact copies of media.

Day 4:

- ▼ Learn techniques to deal with situations where people have hidden files.
- ▼ Forensics for mobile digital devices. i.e. Cell phone, PDA, and Digital Camera.

Day 5:

- ▼ Linux Operating system
- ▼ Online examination (Described below as the CHFI)

Required Prerequisites:

- ▼ Firm understanding of the Windows Operating System.
- ▼ Attendees can be anyone involved in the security of information assets: information security officers and managers, network administrators, Windows administrators.
- ▼ Desire for computer forensics training.

You can register for InfoSec Institute certification exams at <http://www.2test.com>.

FINAL THOUGHTS

The bottom line on computer examiner certification is there are a lot of choices that need to be considered when exploring the exploding computer forensic examiner certification world. Certifications are offered in a University setting with years of training and others are done with much shorter boot camp like training sessions. With the market as varied as it is today, it would seem that choosing which one is right for you is a matter of preference and current abilities. The question is still out on who should and who should not get certified but at the very least, certification will at least ensure that individuals have the concepts of what can/should be done within their organization.

ADDITIONAL RESOURCES

Certification Providers Website
InfoSec Institute - <http://www.InfoSecInstitute.com>

InfoSec's Custom Computer Forensics Enterprise Suite includes every program covered in the course for at home study. Computer Forensics Enterprise Suite is available for individual purchase without the course for \$1,499.

Books

- ▼ The Shellcoder's Handbook: Discovering and Exploiting Security Holes - \$50
 - ▲ ISBN: 0764544683
- ▼ Intrusion Detection with Snort - \$45
 - ▲ ISBN: 157870281X
- ▼ Snort for Dummies - \$19.79
 - ▲ ISBN: 0764568353
- ▼ Snort Cookbook - \$26.37
 - ▲ ISBN: 0596007914

NaSPA member Keith Zielinski is a senior Programmer/Analyst at a Fortune 100 retailer. He has 13 years of IT experience including Network Administration and ERP Implementations.