Challenges in Forensic Computing

The ever-changing nature of technology contributes to the problems encountered by experts when collecting and preparing digital evidence for courtroom presentation.

In recent years, forensic computing has evolved beyond that of an ad hoc pseudoscience to a recognized discipline with certified practitioners and guidelines pertaining to the conduct of their activities. With the ubiquity of computer-based devices in everyday use, forensic techniques are increasingly being applied to a broad range of digital media and equipment, thus posing many challenges for experts as well as for those who make use of their skills.

According to Computer Forensics World (www.computerforensicsworld.com), the field primarily involves the "use of analytical and investigative techniques to identify, collect, examine, and preserve evidence/information which is magnetically stored or encoded." Forensic investigations may also address the analysis and reporting of digital evidence after an incident has occurred, with the goal of preparing "legally acceptable" materials for courtroom purposes (see www.aic.gov.au). Matters may involve computer security breaches, computers used in committing illegal deeds, criminal activity that had a computer as its target, or computer-based devices that inadvertently collected information pertinent to a crime or dispute (see www.forensics.nl).

Forensic computing experts can be deployed in a broad range of criminal, municipal, and civil arenas. I have worked on a variety of cases in this capacity, including:

- Investigation of a law firm's accounting information by a state Office of Attorney Ethics to determine whether escrowed funds had been misused;
- Reconstruction of thousands of deleted text and image files in a murder case, in order to gather information about the activities of the victim and various suspects;

PAUL WILEY

- Examination of source code used in the construction of an MPEG decoder chip set, to see if patents had been violated;
- Evaluation of the contents of a database to determine the cost of its production, as mitigating evidence in a large financial disagreement between business partners;
- Consideration of possible foul play by a former company employee, in the damage of computer records;
- Mathematical analysis of photographs to see if they had been digitally altered; and
- Preparation of explanations for an abnormally high missed vote rate exhibited by certain self-auditing electronic election equipment.

Many forensic matters (including some of those mentioned here) do not go to trial, especially in the business arena where a convincing set of data often suffices to induce an out-of-court settlement, or where investigative techniques are applied on a "need-to-know" basis, such as to determine whether internal or external corporate espionage or malicious activity has occurred. Experts may assist in preparing legal briefs, they can be requested to provide sworn testimony and opinions in city, state, and federal hearings conducted by legislative bodies and their commissions or task forces, and they frequently work hand-in-hand with computer security teams to assist in the development of procedural, policy, and control techniques to help prevent (or assist in mitigating) losses. Investigations can be performed in a few hours or days on simple matters, or can persist over the course of years for complex cases. Although some experts are engaged for the full range of investigative and testimonial tasks, those who are valued for their highly persuasive verbal skills, and who can react well to on-the-spot challenges, may only review and present (or rebut) evidence prepared by other forensic computing specialists.

Unless appointed by the court to provide a neutral interpretation of findings from all sides of a dispute, forensic experts tend (unofficially, of course) to be looked upon or identify themselves as either "black hats" (typically those working for defense teams) or "white hats" (those allied with plaintiff or prosecution teams). Law enforcement officers are usually branded as being "white hats" since their experts are often used as witnesses by the district attorneys in criminal cases. But, in practice, since digital media evidence is typically impounded in the custody of state and local police, or similar federal agencies, such officers must necessarily also cooperate with the defense team in allowing their experts to access the data for discovery and case-preparation purposes.

Given the adversarial nature of this process, and since the caveat of "possession being nine-tenths of the law" applies to the ease with which computer-based data can be (often undetectably and/or non-recoverably) modified during its collection, impounding, and analysis, certain new "rules of evidence" have evolved from the more general (non-computer) codes of practice. These rules address the chain of custody that must be authenticated when digital evidence is introduced. An example of such procedures concerns the use of materials that have been duplicated. In general, according to the U.S. House Advisory Committee on Rules, with regard to its Rule 1003 (Admissibility of Duplicates) in the Federal Rules of Evidence, "a counterpart serves equally as well as the original, if the counterpart is the product of a method which insures accuracy and genuineness." It should be noted that although these Rules of Evidence (see www.law.cornell.edu/rules/fre/overview.html) are required only for Federal court proceedings, many state codes are modeled after them, and thus are fairly consistent. Determination of violation of these rules may be the focus of efforts by defense experts in order to dismiss or raise suspicion about the authenticity or accuracy of the digital materials.

Because of the particular care that must be taken with digital media, forensic investigation efforts can involve many (or all) of the following steps (see www.itsecurity.com):

- Securing materials via appropriate chain of custody;

- Making full (or mirror) copies of digital information from impounded sources;
- Following procedures to prevent alteration of data and files;
- Using software and hardware tools to ensure that the original media is not damaged or compromised in any way, and that the copies do not contain extraneous material (such as residual data that may be introduced through prior uses of the medium now holding the mirror copy);
- Maintaining any data that resides in "free space," including restoration of deleted information on the original devices, using the mirror copies;
- Keeping a complete and comprehensive audit trail of steps performed in the preceding processes; and
- Ensuring that client-attorney privileges and other privacy issues related to the digital evidence are not breached by the experts who have examined the data.

Certain digital information, beyond the contents of the data itself, may be pertinent to case development. This information can include file time and date stamps, folder structure hierarchies, and message transmission tags. Real-time data collection efforts may need to address surveillance legalities and privileges, and avoid inadvertent damage claims (such as may occur when a server is made inaccessible for a period of time). Things to be wary of include alterations to the digital media that could occur when the electronic device is turned on or off, and inadvertent activation of Trojan horse or time-bomb malware that was left behind to corrupt data and confound forensic efforts. One caveat is that "you should only find what is actually there," but ensuring this is so, may involve the development and implementation of collection, blocking, prevention, and tracking techniques. This is where evidence collection kits, containing software and hardware tools, can be usefully applied.

The forensic examiner's bag of tricks generally includes operating system utilities (for backups, disk manipulation, string searches, and so forth), data recovery software (to thwart file deletion attempts), file viewers and Hex editors (to perform Win/Mac data conversions and reveal information contents and patterns), and commercial firewalls (for network sniffing and port scanning during investigations). There are also packages that provide turnkey assistance for forensic examinations, complete with case management tracking for procedures, reports, and billing. Experts may build their own scripts and tools in order to provide specialized investigations, or to gain an edge over firms providing similar services.

Some useful lists of forensic products are maintained by Danny Mares and Company at www.dmares.com/maresware/linksto_forensic_tools.htm, by the

Organization	Certificate	Web site	Estimated Cost
International Society of Forensic Computer Examiners	CCE	www.certified-computer-examiner.com	$395
CyberSecurity Institute	CSFA	certifications.cybersecurityinstitute.biz/testCSFA.htm	$400
International Association of Computer Investigative Specialists	CFCE	www.cops.org/html/training.htm	$675
University of Georgia	CFE	www.gactr.uga.edu/is/cf/	$1,995
InfoSec Institute	CISSP	www.infosecinstitute.com/courses/cissp_bootcamp_training.html	$2,300
SANS	GCFA	www.sans.org	$2,965
Guidance Software	EnCE	www.guidancesoftware.com	$3,500
InfoSec Academy	CHFI	www.infosecacademy.com/us/forensics.asp	$3,995

*Not intended as a comprehensive list nor an endorsement.

Forensic computing examiner certifications.

Continual changes in digital technology pose far more complex challenges than those involving other "traditional" forensic disciplines.

Computer Crime Research Center at www.crime-research.org/library/resource.htm, and by the University of Western Sidney's School of Computing and Information Technology at www.cit.uws.edu.au/compsci/computerforensics/Software/. Although a considerable amount of this software is freely downloadable (and yes, used by hackers as well as trackers), generally you get what you pay for—namely, some of these free offerings can be a bit of a kludge. Some of the most user-friendly commercial products are sold only to law-enforcement agencies or are priced prohibitively for defense teams, so justice may not necessarily be even-handedly served with regard to examination capabilities.

If access to digital evidence is not forthcoming from an impounding agency, court orders may be necessary to obtain the data as well as use of the extraction tools, in order to determine whether protocols had been appropriately applied. Conversely, a prosecution or defense team may wish to suppress evidence from discovery, if they believe it could be damaging to the case. Here is where the time-consuming aspects of the forensic examination may come into play. Typically it is not possible to perform a comprehensive decomposition and logging of all materials (such as the contents of every sector of a terabyte hard drive, or thousands of hours of digital video from a surveillance camera), so a "scratch-and-sniff" approach might be used to yield promising information. Even though cost-effective, tactical decisions to proceed with only a partial investigation may be regretted in hindsight if a post-mortem comprehensive analysis shows that an alternative outcome might have prevailed.

In response to the need to analyze, preserve, protect, and defend forensic evidence, an initiative was begun in 1999 (prior to the homeland security era), in San Diego, CA, to construct and staff Regional Computer Forensic Laboratories (RCFLs). This was done through the Federal Bureau of Investigation in cooperation with local and state law enforcement [1]. By year's end, 13 of these RCFLs will be available for use by more than 1,000 agencies, spanning 15 states (see www.rcfl.gov). I had the opportunity to tour the RCFL in Hamilton Township, NJ that is a part of the newly constructed Forensic Science Technology Center administered by the FBI, the NJ Office of the Attorney General, the NJ Division of Criminal Justice, and the NJ State Police. In addition to the RCFL, the $2.2 million, 200,000-square-foot facility houses laboratories for ballistics, DNA, drug analysis and toxicology, crime scene investigation, and forensic anthropology and photography. The RCFL section contains bulletproof windows and walls, examination bays, a classroom, and a state-of-the-art digital evidence room (the modern-day equivalent of a Faraday cage) to shield impounded materials that could be sensitive to radio-frequency signals (such as cellular telephones, PDAs, and wireless-equipped computers).

The New Jersey RCFL (www.njrcfl.org) provides free digital forensic training services for law enforcement investigators and analysts, who can also receive FBI digital forensic examiner certification through participation in a 12–18 month sequence that includes coursework facilitated by the lab, and on-the-job training. Even though the unit's 21 examiners successfully handled hundreds of cases in the lab's first year of operation, they still must balance and leverage constraints of time, budget, and capacity. Toward this end, they prioritize requests into five levels: 1) immediate threats to property or peo-

ple; 2) similar but potential threats; 3) general criminal investigations, such as fraud and child endangerment/pornography; 4) administrative inquiries; and 5) digital forensic research and development.

NJRCFL's laboratory director, FBI Supervisory Special Agent Larry Depew, noted that continual changes in digital technology pose far more complex challenges than those involving other "traditional" forensic disciplines, since some of the latter are, relatively speaking, performed on a "fixed box" of information. He believes the value of the computer forensic laboratory is seen not only in its investigative and archival functions, but also includes its continual improvements in process methodology. Depew views this with respect to the importance of determining "not only what I know, but what I know that isn't so." Security expert Rebecca Bace [3] also identifies this as a key challenge in forensic computing—the application of inductive reasoning on the data to determine "what is or was" as well as deductive thinking in order to intuit "what is not or was not." What adds to the complexity, she says, is that "often there is little symmetry between the inductive and deductive aspects of a particular case."

Another problem encountered by forensic examiners (especially those unaided by RCFL facilities) is that they must seek out and provide for their own training on an ongoing basis. This is a confusing matter, as it has only been since 2003 that forensic computing has been recognized as a laboratory discipline. The NJRCFL, for example, is applying for accreditation by the Board of the American Society of Crime Laboratory Directors (ASCLD; www.ascld.org). Although ASCLD approval in the category of Digital and Multimedia Evidence is available for labs meeting its standards for any or all of four subdisciplines (computer forensics, forensic audio, video analysis, and image analysis), it does not presently certify the examiners who work in these labs. Many examiner certifications are new and their relative merits may be dubious, especially as compared to the broader knowledge, flexibility, and skills of well-trained and experienced computer scientists, engineers, or IT professionals. The CompuForensics Web site (www.compuforensics.com/training-faq.htm) even mentions that the field "is as yet not regulated by any credible centralized certification authority." Some of these credentials (see examples in the table here) could be obtained via short courses taken by a computer-savvy high school graduate, although an FBI or police background check may also be required.

While a few community colleges and universities have begun to feature forensic computing specializations, there is not yet any consensus on curriculum requirements, although as the field evolves there will likely be further course offerings and some standardization. Trends seem to suggest these topics are primarily hosted by IT departments, whose graduates would typically deal with front-line defense and incident response against activities that potentially require forensic investigation [2].

Most certainly, forensic computing is an exciting profession that can be both elating and frustrating for its practitioners. Even if it were somehow possible to eradicate nefarious intent, equipment failures will continue to provide a market for investigative and reconstructive services as with any engineering endeavor (like the Space Shuttle and the power grid). The continuing maturity of this field will invariably bring some stabilization in best practices, training, certification, and toolsets, but new challenges will always emerge because of the dynamic nature of the technology at its root. C

References

1. Garrison, D. Regional computer forensic laboratories. *Evidence Technology Magazine 1*, 4 (Nov./Dec. 2003); www.evidencemagazine.com/issues/novDec03/RCFL.htm.
2. Kruse, W. and Heiser, J. *Computer Forensics—Incident Response Essentials*. Addison-Wesley, 2002.
3. Smith, F. and Bace, R. *A Guide to Forensic Testimony*. Addison-Wesley, 2003.

Rebecca Mercuri (mercuri@acm.org) recently completed a fellowship with the Radcliffe Institute for Advanced Study at Harvard University, and has resumed her expert witness and forensic computing work at Notable Software, Inc.