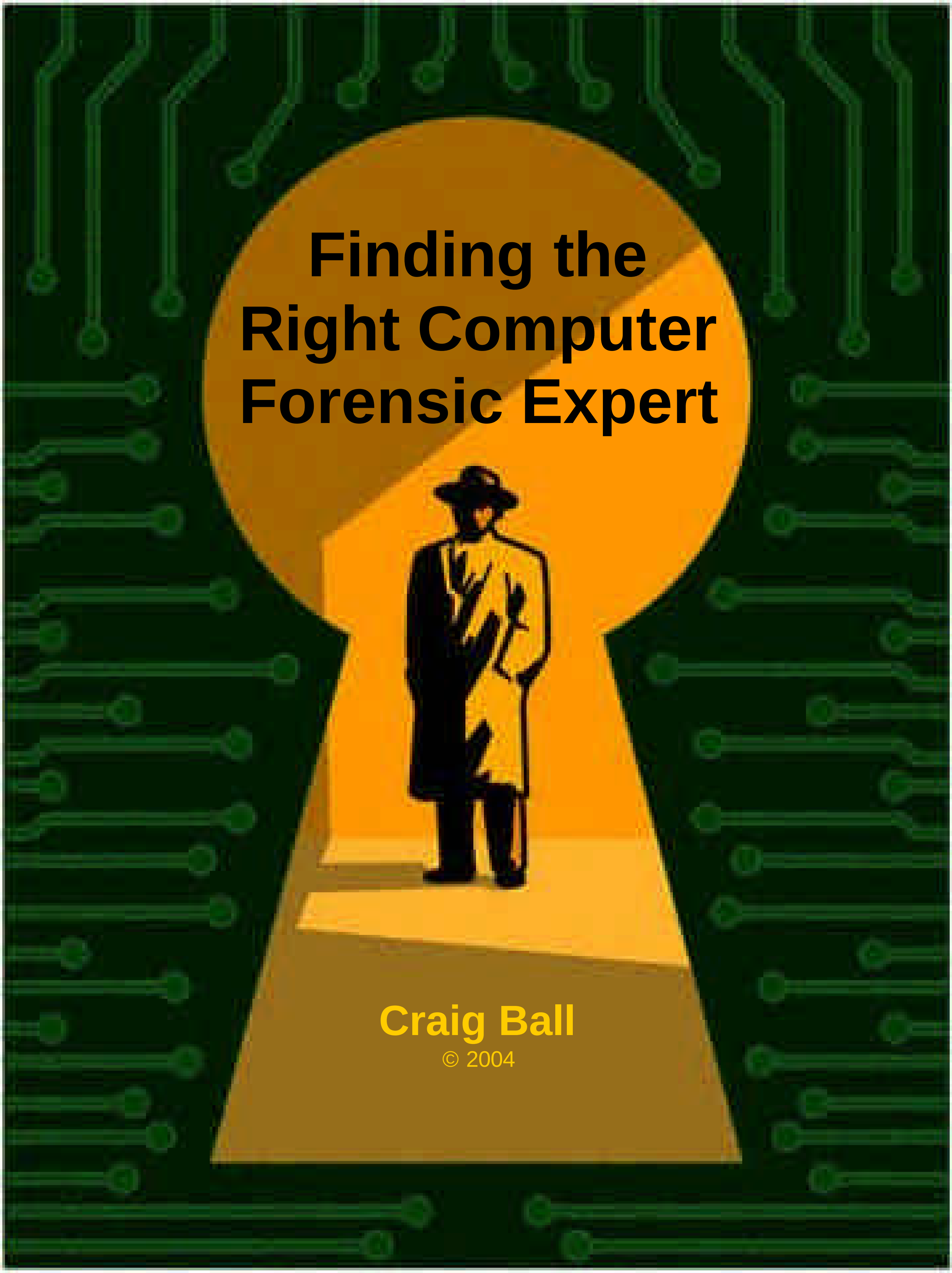

Finding the Right Computer Forensic Expert

Craig Ball

Finding the Right Computer Forensic Expert
Craig Ball

Is deleted-but-not-gone electronic evidence a "bet the case" concern? Ask convicted financier Frank Quattrone, domestic maven Martha Stewart or accused murderer Scott Peterson. Ask anyone at accounting giant Arthur Andersen. Wait, can't do that. Arthur Andersen is *gone,* hoisted on a petard of e-mail and shredded work papers.

Far more information is retained by a computer than most people realize. You could say that a personal computer operating system never intentionally erases anything, even when a user deletes a file. Instead, PCs just hide a deleted file's contents from view, like crumbs swept under a rug. Computer forensics (CF) is the identification, preservation, extraction, interpretation and presentation of computer-related evidence. It's reconstructing the cookie from the crumbs. But unless specialized tools and techniques are used to preserve, examine and extract data, and proper interpretive skills are brought to bear, evidence will be lost, overlooked or misinterpreted.

Everyone uses computers. If you're a prosecutor, litigator or in-house counsel, a computer forensics expert is in your future. You *must* know how to choose a CF pro for your side or test the opposition's choice.

Computer forensic examiners aren't licensed. No standardized exam establishes their competency. Anyone who knows a bit from a byte can put "computer forensic examiner" on their business card. Nevertheless, a cadre of formidably skilled and principled computer forensics examiners remains the core of the profession. The challenge is to tell one from the other and to help the judge and jury see the difference, too.

Finding a CF Expert

The best ways to find a good CF expert are the same used to find experts in any technical discipline: ask other lawyers and judges who to use and avoid, and delve into the professional literature to spot scholarship and leadership. If you practice in a small community and can't secure local recommendations, contact one of the professional associations for CF examiners (the High Technology Crime Investigation Association at www.HTCIA.org is the largest) and get the names of nearby members. Internet searches for experts may turn up worthwhile leads, but don't judge qualifications by where the expert appears in a search engine. It's just too easy to buy or engineer favorable placement. Instead, use the 'net to troll for publications and for networking. The non-commercial Electronic Evidence Information Center (www.e-evidence.info) is a superb starting point for a wealth of information on leading computer forensics practitioners.

Many experienced CF examiners come from law enforcement and the military. Look for, e.g., former DOD, IRS, FBI and Secret Service credentials. Sadly, child pornography represents the bulk of CF work by many ex-law enforcement investigators, so ask about broader experience with other computer crimes. Extensive experience on the civil side is a plus.

Plenty of computer savvy folks lacking forensic training or experience offer their services as experts. But, just as few doctors are qualified as coroners, few systems administrator have any forensic qualification. A background in law, law enforcement or investigation is important, whereas programming experience has little bearing on computer forensic ability. Be certain to obtain the witness' C.V. and check it for accuracy. Look for membership in professional CF associations, formal training and certification. Has the expert published articles on computer forensics or regularly participated in online CF forums? Read these contributions to gauge knowledge, commitment to the profession and communication skill, then weigh the following when evaluating qualifications:

Is the examiner certified?

An increasing number of organizations offer certification in computer forensics. Some indicate real expertise and others mean little. In evaluating certification, find out exactly what the expert had to do to be certified. Was written testing required? Was there a practical component? What about peer review and a minimum experience threshold? Who taught and certified the expert? Do any applicants fail to obtain the certification? Was expertise certified in a discipline or in the use of a particular tool or software package?

How much time devoted to computer forensics?

Question the focus of a CF expert wearing many hats for hire as, e.g., PC repair specialist, network installer, programmer or private investigator. A large firm's far-ranging claims of expertise may be justified, but for the solo or small shop expert, "dabbling" in computer forensics is not an option.

How experienced as a witness?

If the expert you're evaluating held up in past courthouse challenges, chances are she will again. Look for experience in the type of case you're handling. A veteran of porno prosecutions may not be well-suited to a case of sexual discrimination or IP infringement. You can't be an effective CF examiner if you don't understand what the case is about, so be certain your choice knows the ins-and-outs of civil litigation. Talented CF experts convey hyper technical concepts without lapsing into jargon or acronyms and possess easy facility with simple analogies.

How much classroom training?

Ideally, a CF expert has been formally trained and can demonstrate dozens or hundreds of hours of CF classroom work. Note, however, that some of the best qualified experts in computer forensics have little or no formal training in the discipline. They're largely self-taught and have been at it since the dawn of MS-DOS. These veterans, too, should be able to demonstrate time in the classroom…as the instructor.

What will it cost?

Good computer forensics is expensive. Even a basic computer forensic examination costs several thousand dollars or more. A complex exam can run to six figures. One veteran examiner analogizes that a top-notch cardiac surgeon can teach anyone to perform a routine heart bypass in an afternoon—it's just plumbing—but the necessary expertise and attendant high cost spring from the decades it took to learn what to do *when things go wrong.*

A CF expert should clearly communicate hourly rates and anticipated expenses, but there are typically too many variables to quote a bottom line cost. If you can supply reliable information about the systems, electronic media and issues, experience may permit the expert to project a range of expected cost. Recognize that competent examiners routinely decline requests for a "two-hour quick peek." No one wants to be taken to task in court for missing something because they didn't have time to do the job correctly.

What do other clients think?

Before you commit to spend thousands, ask for references and spend a few minutes calling attorneys who've worked with the expert. Some client identities might be withheld as confidential, and those supplied probably won't be the disgruntled folks, but you're sure to glean *something* useful respecting billing practices, reporting skill, discretion, preparation or professionalism. If nothing else, an expert unable to identify satisfied clients might not be the one for you.

Beware of the Tool Tyke

Poorly-trained experts rely on software tools without understanding how they work. They're Tool Tykes. Of course, all of us trust technologies we don't fully understand, but an expert should be able to explain *how* a tool performs its magic, not offer it up as a black box oracle. Tool Tykes dodge attacks on their lack of fundamental skills by responding, "The tool is not on trial," or citing how frequently the testimony of *other* witnesses using the same tool has been accepted as evidence in other courts. The use of proven tools and software is essential, but even a rock-solid tool in unskilled hands is unreliable. Forensic software suites are principally designed to automate repetitive tasks that would otherwise be performed manually. Your expert should understand those underlying operations, not just know the keystroke required to initiate them.

Building your E.Q.

Working with your expert will be easier if you learn all you can about computer forensics. My article, "*Computer Forensics for Lawyers Who Can't Set the Clock on their VCR,*" at www.craigball.com/cf.pdf is a good start. For approaches to managing the other side's CF expert, look at "*Cross-Examination of the Computer Forensics Expert*" at www.craigball.com/expertcross.pdf.

Craig Ball, a trial lawyer and certified computer forensics examiner. He can be contacted as craig@ball.net or via www.cybersleuthing.com.