Digital Investigation (2004) 1, 7–15

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

Current issues confronting well-established computer-assisted child exploitation and computer crime task forces

Monique Mattei Ferraro[1], Andrew Russell[2]

Received 9 January 2004

Introduction

Over the past five years, a large number of agencies have developed specialized units to deal with high technology crimes and Internet crimes against children. The United States currently funds approximately 45 Internet Crimes Against Children Task Forces.[3] This article talks about some of the issues confronting established Internet crimes against children and high technology crime units and examines approaches to their resolution. First, the tension between forensics and investigations is discussed. With the first computer forensic laboratory being accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB), pressure to split the functions is increasing attention to unit functions (Casey, 2004; Ferraro and Casey, 2004a). Next, the article addresses the continued confusion over obtaining information from Internet service providers.[4] The third issue discussed is the burgeoning problem of storing and returning evidence years after its seizure. In some cases the courts order return of evidence containing contraband, and often impose arduous duties on the unit personnel that are more akin to what a computer technician at a private shop would perform under contract than what law enforcement personnel should do to accommodate the owner of evidence to facilitate its return (Ferraro and Casey, 2004a).

The tension between forensic science and investigations

Issue 1: expert examination versus investigative review

Established computer crime units are beginning to feel pressure to become accredited. Accreditation schemes for laboratories parallel those used for hospitals, universities and police departments. There are general directives that apply to the entire laboratory and there are particular standards that apply to specific disciplines such as serology and document examination. Some of the standards are mandatory and some are elective. In order to maintain accreditation, labs must conform to a percentage of the essential standards and a certain level of important standards.

An emerging issue is the potential difficulty that some units that house both forensic examination and investigations have with accreditation standards. Generally, lab accreditation schemes require

E-mail address: mfer.ccu@snet.net (M.M. Ferraro).

[1] M.S., Northeastern University, J.D., University of Connecticut School of Law, Certified Information Systems Security Professional.

[2] J.D., Western New England School of Law.

[3] United States Department of Justice Office of Juvenile Justice and Delinquency Prevention. There are hopes that an additional four task forces will be added in the near future.

[4] Ferraro and Casey, Ferraro, Monique, "An Argument for Uniform State Long-Arm and Full Faith and Credit Provisions Regarding Compulsory Process for Information Held by Communication Service Providers" (tentative title) as yet unpublished, available from the author (2004).

1742-2876/$ - see front matter
doi:10.1016/j.diin.2004.01.004

a system of technical and administrative review of examination reports. Examiners must follow established procedures and document their findings. The lab must conduct proficiency testing of examiners. Testing can be internal as well as external and use blind and/or open samples with results that are unknown to the examiner but known to the test administrator. Additionally, examiners must pass competency examinations in each area in which they will perform examinations. With regard to computer forensic examiners, it means that they must be competent in each software and hardware tool they use. Finally, examiners must possess certain minimum academic credentials and training. The standards applicable to computer laboratory personnel require that examiners have at least a Bachelor's Degree with science courses (Ferraro and Casey, 2004b).

Established computer crime units and Internet crimes against children task forces have not received accreditation requirements enthusiastically. For many who work in this area, the requirement of a bachelor's degree could force them out of working in the computer crime field. Other objections go to the basics. First, many investigators believe that examining a computer system for evidence is not a matter for a "forensic scientist," but within the realm of an "investigative review of the evidence." It may seem like a minor distinction to some, but the entire future of this emerging field hinges on which direction the law enforcement community takes.

One does not have to be clairvoyant to predict that computers will be ubiquitous in nearly every sort of crime soon enough. If we set the standard such that we expect a forensic scientist to conduct an examination in every computer related crime, the demand for computer forensic scientists will be enormous. Every law enforcement agency will either have a laboratory of its own or rely upon a computer forensics laboratory to process its evidence. Unless the world is preparing to meet the demand for forensic science services that outstrip the meager resources we now have, some alternative will be necessary.

Full-blown forensic examinations are usually unnecessary. This is particularly so when the suspected criminal activity involves only a small portion of the storage media. For example, in child pornography possession, an examination looking for questionable images should be sufficient to obtain the necessary evidence to support a criminal investigation and possible prosecution. The lengthy process involved in a forensic examination, which requires duplicating all seized media, outlining the system setup and reviewing all of the files is more than what is necessary to prove that there were images of child pornography held in storage (see Casey, 2004 for details on the examination process).

Another example would be of a "traveler" who engages in online chat with the intended victim. When he travels to the prearranged spot, police arrest him. Some agencies conduct full forensic examinations of the suspect's hard drive, the victim's computer and execute search warrants for Internet service provider records as well. This practice expends resources on a misdemeanor or low-level felony that are typically used in a homicide investigation. Rather than expend the resources on the multiple forensic examinations, a printout of the chat logs together with the testimony of the investigating officer to authenticate it may be sufficient to prove that the communication took place. Of course, the scope of the forensic examination is an issue ultimately determined by the prosecutor (hopefully she will take into consideration the sound advice of forensic examiners and investigators).[5]

It is easier to train existing personnel than to recruit candidates who already possess the sought after skills. For that reason, law enforcement agencies have mostly opted for training existing personnel to perform computer forensic examinations. While this approach has been expedient, there are problems with it. One problem is that police officers have a relatively high turn over rate. Sworn officers often have to work only 20 years before they are eligible to retire, as opposed to civilian employees who usually need to work 30 or more years before they may retire. Civilians also are less likely to rotate out of the examination position because they make a commitment to being a forensic examiner rather than a police officer. In order to advance in rank, police officers usually cannot stay in one unit or division for long, due to a limited career ladder.

Another problem with training police officers to do forensic examinations of computer systems is that they may not possess the education and training necessary to qualify them as expert witnesses. The lack of formal university education is not a problem unless the examiners work in a laboratory seeking accreditation or the defense makes it a problem, but it is a factor. If the defense expects the computer forensic examiner to qualify

[5] For guidance in this area, see *United States vs. Tank*, 200 F.3d 627 (2000) and Cobb, J. Allen 39 Brandeis L.J. 785, 'ARTICLE: Evidentiary Issues Concerning Online "Sting" Operations: A Hypothetical Based Analysis Regarding Authentication, Identification, and Admissibility of Online Conversations—A Novel Test for the Application of Old Rules to New Crimes' (Summer 2001).