INTRODUCTION

In the years since the first edition of this book, there has been an explosion of interest in digital evidence. This growth has sparked heated debates about tools, terminology, definitions, standards, ethics, and many other fundamental aspects of this developing field. It should come as no surprise that this book reflects my positions in these debates. Most notably, this text reflects my firm belief that this field must become more scientific in its approach. The primary aim of this work is to help the reader tackle the challenging process of seeking scientific truth through objective and thorough analysis of digital evidence. A desired outcome of this work is to encourage the reader to advance this field as a forensic science discipline.

AREAS OF SPECIALIZATION

Currently, there is little clarity in this field regarding areas of specialization and who should receive what training. For instance, there is no clear distinction between digital crime scene technicians (a.k.a. first responders) and digital evidence examiners, despite the fact that data recovery requires more knowledge than basic evidence documentation, collection, and preservation. The investigative process detailed in Chapter 4 suggests three distinct groups with different levels of knowledge and training.

- *Digital Crime Scene Technicians*: Individuals responsible for gathering data at a crime scene should have basic training in evidence handling and documentation as well as in basic crime reconstruction to help them locate all available sources of evidence on a network.
- *Digital Evidence Examiners*: Individuals responsible for processing particular kinds of digital evidence require specialized training and certification in their area.
- *Digital Investigators*: Individuals responsible for the overall investigation should receive a general training but do not need very specialized training or certification. Investigators are also responsible for reconstructing the actions relating to a crime using information from first responders and forensic examiners to create a more complete picture for investigators and attorneys.

For the purposes of this text, the more general term "digital investigator" is used to refer to individuals who play a key role in digital investigations, including computer security professionals, attorneys, law enforcement officers and forensic examiners.

Training and certification programs in this field should take into account these different areas of expertise.

RELIABILITY OF DIGITAL EVIDENCE

Digital investigators do not currently have a systematic method for stating the certainty they are placing in the digital evidence they are using to reach their conclusions. This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of digital investigators' conclusions. The Certainty Scale presented in Chapter 7 provides a consistent method of referring to the relative certainty of different types of digital evidence. The immediate aim of the Certainty Scale is to improve our ability to assess the reliability of digital evidence.

Ultimately, it is hoped that this Certainty Scale will point to areas that require additional attention in digital evidence research. Debate over C-values in specific cases may reveal that certain types of evidence are less reliable than was initially assumed. For some types of digital evidence, it may be possible to identify the main sources of error or uncertainty and develop analysis techniques for evaluating or reducing these influences. For other types of digital evidence, it may be possible to identify all potential sources of error or uncertainty and develop a more formal model for calculating the level of certainty for this type of evidence.

THE NEED FOR STANDARDIZATION

> Digital evidence is just another form of "latent" evidence that must be handed with scientific principles and legal boundaries. There is an investigative component for electronic crimes and a laboratory component for the digital evidence associated with those crimes. (Carrie Whitcomb, 2001, "*A Forensic Science Perspective on Digital Evidence Training, Education, and Certification*," National Center of Forensic Science)

In 1994, the O.J. Simpson trial exposed many of the weaknesses of criminal investigation and forensic science. The investigation was hampered from the start with incomplete evidence collection, documentation and preservation at the crime scenes. Arguably, as a result of these initial errors, experienced forensic scientists were confused by and incorrectly interpreted important exhibits, introducing sufficient doubt for the jurors. The controversy surrounding this case made it clear that investigators and forensic scientists were not as reliable as was previously believed, undermining not just their credibility but also that of their profession. This crisis motivated many crime laboratories and investigative agencies to revise their procedures, improve training, and make other changes to avoid similar problems in the future. More recently flaws have been found in the fingerprint and DNA analysis performed by some crime laboratories, calling many convictions into questions and creating doubts about the analytical techniques themselves.

A similar crisis is looming in the area of digital evidence. The lack of generally required standards of practice and training allows weaknesses to

persist, resulting in incomplete evidence collection, documentation and preservation as well as errors in analysis and interpretation of digital evidence. Innocent individuals may be in jail as a result of improper digital evidence handling and interpretation allowing the guilty to remain free. Failures to collect digital evidence have undermined investigations, preventing the apprehension or prosecution of offenders and wasting valuable resources on cases abandoned due to faulty evidence. If this situation is not corrected, the field will not develop to its full potential, justice will not be served, and we risk a crisis that could discredit the field. The only reason we have not already encountered such as crisis is that our mistakes have been masked by obscurity. As more cases become reliant on digital evidence and more attention is focused on it, we must take steps to establish standards of practice and compel practitioners to conform to them.

There have been several noteworthy developments toward standardization in this field. The International Organization of Computer Evidence (www.ioce.org) was established in the mid-1990s "to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state." In 1998, the Scientific Working Group on Digital Evidence (www.swgde.org) was established to "promulgate accepted forensic guidelines and definitions for the handling of digital evidence." In 2001, the first Digital Forensics Research Work Shop (www.dfrws.org) was held, bringing together knowledgeable individuals from academia, military and the private sector to discuss the main challenges and research needs in the field. This workshop also gave new life to an idea proposed several years earlier – a peer-reviewed journal – leading to the creation of the *International Journal of Digital Evidence* (www.ijde.org). In 2003, the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) updated its accreditation manual to include standards and criteria for digital evidence examiners in US crime laboratories. In 2004 the UK Forensic Science Service plans to develop a registry of qualified experts, and several European organizations, including the European Network of Forensic Science Institutes (ENFSI) will publish examination and report writing guidelines for digital investigators. Also, Elsevier will begin publishing Digital Investigation: The International Journal of Digital Forensics and Incident Response (http://www.compseconline.com/digitalinvestigation/).

Historically, Forensic Science disciplines have used certification to oversee standards of practice and training. Certification provides a standard that individuals need to reach to qualify in a profession and provides an incentive to reach a certain level of knowledge. Without certification, the target and rewards of extra effort are unclear. This is not to say that everyone who handles digital evidence requires the same level of skill or training. A strong certification program needs to have tiered levels of certification facilitating

progression upwards, setting basic requirements for crime scene technicians, and setting higher standards for specialists in a laboratory and for investigators who are responsible for analyzing evidence.

Although there are a growing number of certification programs for digital investigators, many are only available to law enforcement personnel and none are internationally accepted. In 2004, representatives from around the world convened to discuss the feasibility of an internationally accepted certification for digital investigators. The outcome is not decided and there are obstacles to such a certification. Some feel that proposed training requirements are too high while others fear that certification will enable anyone to enter the field and obtain specialized knowledge, even individuals who work for the defense on criminal cases. There is also the fear that setting standards and placing additional requirements on practitioners will make it more difficult to get digital evidence admitted in court.

Paradoxically, some of those concerned that training requirements will exclude them also want to exclude individuals who perform criminal defense work. In addition to being unethical, any attempt to withhold knowledge from criminal defense attorneys and experts stifles improvement and progress in the field by allowing misunderstandings and poor practices to persist. If we cannot work together despite our differences to improve the field, the only winners will be the criminals and the losers will be the innocents. The aim of everyone in this field should be to ensure the best reasonable standards and quality. In the long run, digital evidence processed properly by certified professionals is less likely to be impeached or cause an injustice.

The investigation into the Starnet Internet gambling company provides a good example of the successes of proper training and preparation. The August 1999 raid of Starnet's offices in Vancouver, BC, was the culmination of more then a year's worth of investigative effort and preparation by the Royal Canadian Mounted Police. Over 100 personnel from all over Canada were brought together to search and seize Starnet's systems. Search teams were trained to implement standard operating procedures to ensure consistency and were given sufficient equipment to store the large amounts of data that were anticipated. As a result of this planning, Starnet's office building and the network it contained were secured in a few minutes. Although it took several days, digital evidence from more than 80 computers was preserved. In 2001, Starnet pled guilty to violating Section 202 (1) b of the Canadian criminal code by having a machine in Canada for gambling or betting.

Although professionalization may not be desirable for some, it is necessary for all. Without generally accepted standards, there is no basis to judge work. Without certification, there is no basis upon which to assess qualifications. Our community has a duty to agree upon standards of practice and training, and to require practitioners to meet these standards through certification.

> This duty exists because in the forensic disciplines our opinions and interpretations are allowed to impact whether people are deprived of their liberties, and potentially whether they live or die. (Turvey, B., 2000, "*The Professionalization of Criminal Profiling" in Criminal Profiling*, Academic Press)

ROADMAP TO THE BOOK

This book draws from four fields: Law, Computer Science, Forensic Science, and Behavioral Evidence Analysis. The Law provides the framework within which all of the concepts of this book fit. Computer Science provides the technical details that are necessary to understand specific aspects of digital evidence. Forensic Science provides a general approach to analyzing any form of digital evidence. Behavioral Evidence Analysis provides a systematized method of synthesizing the specific technical knowledge and general scientific methods to gain a better understanding of criminal behavior and motivation.

This book is divided into five parts, beginning with a presentation of relevant legal issues and investigative methods in Part 1 (Chapters 1–7). Chapter 1 provides an overview. Chapter 2 (History and Terminology) provides relevant background, history, and terminology. Chapter 3 (Technology and Law) discusses legal issues that arise in computer related investigations, comparing US and European law. Chapter 4 (Investigative Process) discusses a systematic approach to investigating a crime based on the scientific method, providing a context for the remainder of this book. Chapter 5 (Investigative Reconstruction) describes how to use digital evidence to reconstruct events and learn more about the victim and the offender in a crime. Chapter 6 (Technology, MO, and Motive) is a discussion of the relationship between technology and the people who use it to commit crime. Understanding criminal motivation and behavior is key to assessing risks (will criminal activity escalate?), developing and interviewing suspects (who to look for and what to say to them), and focusing investigations (where to look and what to look for). Chapter 7 (Digital Evidence in Court) provides an overview of issues that arise in court relating to digital evidence.

Part 2 of this book (Chapters 8–13) begins by introducing basic Forensic Science concepts in the context of a single computer. Learning how to deal with individual computers is crucial because even when networks are involved, it is usually necessary to collect digital evidence stored on computers. Case examples and guidelines are provided to help apply the knowledge in this text to investigations. The remainder of Part 2 deals with specific kinds of computers and ends with a discussion of overcoming password protection and encryption on these systems.

Part 3 (Chapters 14–18) covers computer networks, focusing specifically on the Internet. A bottom-up approach is used to describe computer networks,

starting with the raw data transmitted on networks and progressively building up to the types of data that can be found on networked systems and the Internet. The "top" of a computer network is comprised of the software that people use, like e-mail and the Web. This upper region hides the underlying complexity of computer networks and it is, therefore, necessary to examine and understand the underlying complexity of computer networks to appreciate fully the information found at the top of the network. Understanding the "bottom" of networks – the physical media (e.g. copper and fiber optic cables) that carry data between computers is also necessary to collect and analyze raw network traffic.

Part 4 of this book (Chapters 19–22) focuses on specific types of investigations starting with Computer Intrusions in Chapter 19. Tools and techniques specific to this type of investigation are presented and detailed case examples are used to demonstrate key points. Chapter 20 covers investigations of Cyberstalking. Chapter 21 details Sexual Predators on the Internet and Chapter 22 discusses computers as alibi.

Part 5 is a short segment that provides guidelines for handling and processing digital evidence. This text does not cover forensic image, video and audio analysis. For information about image/video/audio enhancement and other aspects of this kind of analysis, see Electronic Evidence by Gruber (Gruber 1995).

The Forensic Science concepts described early on in relation to a single computer are carried through to each layer of the Internet. Seeing concepts from Forensic Science applied in a variety of contexts will help the reader generalize the systematic approach to processing and analyzing digital evidence. Once generalized, this systematic approach can be applied to situations not specifically discussed in this text. In place of the CD-ROM in the first edition of this book, an interactive Web site (www.disclosedigital.com) provides practical exercises based on actual cases to demonstrate key aspects of investigating computer related crimes and to help the reader apply the concepts in this book to his/her own investigations. This Web site epitomizes a general educational model that others can replicate or borrow from to create inexpensive, educational resources to assist investigators.

DISCLAIMER

Tools are mentioned in this book to illustrate concepts and techniques, not to indicate that a particular tool is best suited to a particular purpose. Digital investigators must take responsibility to select and evaluate their tools.

Any legal issues covered in this text are provided to improve understanding only, and are not intended as legal advice. Competent legal advice should be sought to address the specifics of a case and to ensure that nuances of the law are considered.