An Historical Perspective of Digital Evidence: A Forensic Scientist's View

Carrie Morgan Whitcomb, Director, National Center for Forensic Science

Author's Comments

During my tenure as director of the Postal Inspection Headquarters Laboratory (1988-1992), a Postal Inspector submitted a computer to examine for the presence of specific evidence he had enumerated in the letter of request. The evidence technician logged in the computer, assigned it a case number, and brought the request to me, inquiring "What should we do with this?" That was the beginning of an odyssey that I still pursue.

The Inspection Service Laboratory had a Questioned Document Section. Since a computer seemed to be an obvious evolution of paper documents, I called the manager of that section, Drew Somerford, and asked him to take the case. He was reluctant to sign for the evidence. Even though there might have been "documents" on the hard drive, it was outside his expertise. How do you secure and preserve the evidence? How do you collect it without changing it? What are the accepted practices related to computer evidence that would stand the scrutiny of court? What are the examination protocols? It was technology that we did not know how to handle in the crime laboratory.

We submitted the computer evidence to the Federal Bureau of Investigation (FBI). The FBI Laboratory had a unit for computer evidence, and they worked the case. The Postal Inspection Service had a team of inspectors who were trained to work computer crime cases, but the laboratory was not equipped to assist them in processing evidence at that time.

Background

> Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer evidence. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART). Although CART is unique in the FBI, its functions and general organization are duplicated in many other law enforcement agencies in the United States and other countries (Noblett, Pollitt, & Presley, 2000).
>
> An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. These resources were often scattered throughout the agency. Today, there appears to be a trend toward moving these examinations to a laboratory environment. In 1995, a survey conducted by the U.S. Secret Service indicated that 48 percent of the agencies had computer forensic laboratories and that 68 percent of the computer evidence seized was forwarded to the

experts in those laboratories. As encouraging as these statistics are for a controlled programmatic response to computer forensic needs, the same survey reported that 70 percent of these same law enforcement agencies were doing the work without a written procedures manual (Noblett, et al., 2000).

From Computer Forensics to the more inclusive "Digital Evidence"

In 1990, the Postal Inspection Service Laboratory moved to a new facility at Dulles, Virginia, and by 1996-97, had established a Computer Forensic Unit. The Inspection Service had worked closely with the FBI for several years in the development of computer forensic capabilities. About the same time, audio and video enhancement was moving from analog to digital format. Should the same guiding principles be applied to all forms of digital evidence regardless of the output? Would an inclusive "Digital Evidence Unit" be more appropriate than a "Computer Forensic Unit"?

The federal crime laboratory directors in the Washington, DC, area met twice a year to discuss issues of mutual interest. They were instrumental in forming what is now known as the Scientific Working Group Digital Evidence (SWGDE). The concept of finding "latent evidence on a computer" was known as computer forensics at that time. The concept of digital evidence, which included digital audio and digital video evidence was brought before the federal laboratory directors on March 2, 1998, at a meeting hosted by the U. S. Postal Inspection Service, Forensic and Technical Services Division, Dulles, Virginia. This first discussion concentrated primarily on digital photography. The discussion about digital evidence, including digital computer evidence, digital audio and video evidence, needed technical people to lead the discussion. A second meeting was held on May 12, 1998, and the directors brought their technical experts to the meeting to further discuss the technical merits of digital evidence. Dr. Don Kerr, then Assistant Director, FBI Laboratory, invited Mark Pollitt, Unit Chief of the FBI's Computer Analysis and Response Team, to speak to the directors about the concept of digital evidence. Scott Charney, head of the Department of Justice, Computer Crimes and Intellectual Property Section (CCIPS), was invited to discuss legal aspects of computer evidence and to talk about search warrant requirements for seizing digital evidence. The outcome of the May meeting was the formation of another Technical Working Group to address the forensic issues related to digital evidence.

There are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. As early as 1991, a group of six international law enforcement agencies met with several U. S. federal law enforcement agencies in Charleston, South Carolina, to discuss computer forensic science and the need for standardized approach to examinations. In 1993, the FBI hosted an International Law Enforcement Conference on Computer Evidence that was attended by 70 representatives of various U.S. federal, state and local law enforcement agencies. All agreed that standards for computer forensic science were lacking and needed. This conference again convened in Baltimore, Maryland, in 1995, Australia in 1996 and the Netherlands in 1997, and ultimately resulted in the formation of the International Organization on Computer Evidence (IOCE). In addition, a Scientific Working Group on Digital

> Evidence (SWGDE) was formed to address these same issues among federal law enforcement agencies (Noblett, et al., 2000).

On June 17,1998, the Technical Working Group Digital Evidence (TWGDE) held their first meeting. Mark Pollitt, Special Agent, FBI, was elected Chair and Carrie Morgan Whitcomb, Manager, Forensic Services, U. S. Postal Inspection Service was elected Co-Chair. Federal forensic laboratories that were represented included the Bureau of Alcohol, Tobacco and Firearms (ATF), U. S. Customs, the Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA), U. S. Secret Service (USSS), and the U. S. Postal Inspection Service. TWGDE met monthly to prepare organizational procedures and develop relevant documents. Mark Pollitt gave many international presentations to groups such as the International Organization on Computer Evidence (IOCE) and INTERPOL concerning the work of TWGDE.

From Technical Working Groups (TWGs) to Scientific Working Groups (SWGs)

In forensic science, groups of experts in a particular forensic discipline have evolved into bodies that develop standards, best practices, and protocols. They began as Technical Working Groups (TWGs) in the early1990s. In 1999, the name was changed to Scientific Working Groups (SWGs) in an attempt to distinguish the FBI supported long term working groups from National Institute of Justice (NIJ) TWGs that were of short duration and usually had a single deliverable, such as a guidebook on a specific topic. SWGs are ongoing groups that meet at least once per year, comprised of no more than 50 federal, state and local members. The members may be either sworn (law enforcement) or non-sworn.

The first SWG was organized to deal with the issues related to new forensic technology, DNA. It was called the Scientific Working Group for DNA Analysis Methods (SWGDAM).

> Since the early 1990s, the FBI Laboratory has led the way in sponsoring Scientific Working Groups (SWG) to improve discipline practices and build consensus with our federal, state, and local forensic community partners. In early 1998, the FBI Laboratory performed a strategic review of all SWGs" (Adams & Lothridge, 2000).

The result was the development of a framework for operational bylaws for the SWGs.

> The establishment, constitution, and goals of a Scientific Working Group (SWG) are a matter of the needs of the particular scientific discipline and professional expertise. Bylaws are required to effectively implement and execute the deliberations of SWGs, and it is important that each SWG develop written bylaws for operation. Although not every SWG can or should be covered by preset standardized rules, certain standards of performance that are common to all SWGs are necessary" (Adams and Lothridge, 2000).

Processes have been developed by SWGs to gain input from non-members on proposed guidelines and procedures before finalizing such documents. In February 1999, TWGDE was changed to SWGDE. The Scientific Working Group Image Technology (SWG-IT) is closely associated with SWGDE and was originally part of SWGDE. For example, the taking of digital pictures of evidence at a crime scene is digital imagery. When the digital picture itself is the evidence (as in the case of child pornography), it would be digital evidence and part of SWGDE. As SWGIT develops enhancement protocols, there is much commonality between the two SWGs. "The mission of the Scientific Working Group on Imaging Technology (SWGIT) is to facilitate the integration of imaging technologies and systems in the criminal justice system by providing definitions and recommendations for the capture, storage, processing, analysis, transmission and output of images" (SWGIT, 1999).

Defining Digital Evidence

"Digital Evidence is any information of probative value that is either stored or transmitted in a binary form," (SWGDE, July 1998). Later "binary " was changed to "digital". Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. The discussion following the formulation of this definition suggested that it was important to put a date on definitions. In the future, time stamps might also be needed to keep up with the changing technologies.

At the August 1998 meeting, SWGDE began to draft definitions. These definitions, as well as standards, were presented at the International Hi-Tech Crime and Forensics Conference held in London in October 1999 (SWGDE/IOCE, 2000).

Draft SWGDE Definitions, Standards and Principles

> *Acquisition of Digital Evidence*: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collection of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.
>
> *Data Objects*: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.
>
> *Digital Evidence*: Information of probative value stored or transmitted in digital form.
>
> *Physical Items*: Items on which data objects or information may be stored and/or through which data objects are transferred.

Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.

Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Standards

Principle 1

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

Standards and Criteria 1.1

All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

Discussion. The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an agency's management authority.

Standards and Criteria 1.2

Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

Discussion. Rapid technological changes are the hallmark of digital evidence, with the types, formats, and methods for seizing and examining digital evidence changing quickly. In order to ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

Standards and Criteria 1.3

Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

Discussion. Because a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to remain flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

Standards and Criteria 1.4

The agency must maintain written copies of appropriate technical procedures.

Discussion. Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

Standards and Criteria 1.5

The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.

Discussion. Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem. Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

Standards and Criteria 1.6

All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

Discussion. In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person could evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.
The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation must be maintained for all digital evidence.

Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Standards and Criteria 1.7

Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

Discussion. As outlined in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes (SWGDE/IOCE, 2000, pp. 3-7).

Accreditation of Digital Evidence by ASCLD/LAB

While SWGDE was working on best practices, it was determined that we must also have a deliberate plan for gaining acceptance by the forensic science community. We were on the "frontier" of a new forensic science. Others have blazed the trail and all we need to do is follow it. DNA created the SWG process. The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) has an accreditation process that spells out criteria that must be met by specific disciplines in forensic laboratory operations. SWGDE voted to follow the format of the ASCLD/LAB Accreditation Manual for writing their standards. The major categories are: Principle, Standards and Criteria, Discussion. The manual addresses Laboratory Management and Operation, Personnel Qualifications, and Physical Plant.

Membership in The American Academy of Forensic Sciences (AAFS) for Digital Evidence Examiners

The AAFS is the most prestigious national organization for forensic scientists. Thus far, digital evidence papers have been presented in various sections. If the digital evidence community is to consider forming their own section, there must be a minimum of fifty academy members that petition the board to form such a section. As the Executive Secretary of SWGDE, I gave a presentation to the AAFS Board of Directors at the 2002 meeting concerning the activities of SWGDE and the status of forensic digital evidence. AAFS suggested that all potential members in the digital evidence discipline, who wanted to take part in a digital evidence program, could join the General Section of the Academy. From there, a separate section might be formed.

Chaos and Certification of Digital Evidence Examiners

I believe that the ultimate organization of this diverse community lies with professional certification, covering all aspects of digital evidence. The issues of good science and lawful

procedures span the collection of digital evidence at the crime scene, the forensic examinations in laboratories, and the analysis of data by law enforcement. There must be consistent principles that apply to all areas of digital evidence for justice to be served. By the very nature of digital evidence, professional certification is also an international issue. Until we have a universal measure of individual competency and expertise, it will be difficult to move forward in an organized and effective manner. Technology will push the standards and protocols, which in turn will push training and education, which will feed into certification processes. The legal system will be the end user and will dictate process and procedures. The community must be organized with processes that will meet these many challenges.

The issue is how to successfully bring the multitude of experts along an organized and effective path to address the many issues related to digital evidence with rapidly changing technology. We must create a structure in which the response to change can produce a technically competent workforce of massive proportions. Is an international certification body operated by a consortium of national and international organizations the answer? The National Center for Forensic Science will facilitate a discussion on international professional certification issues utilizing representatives from a broad spectrum of existing organizations and groups to participate.

If chaos precedes a higher level of organization, then we may be ready for professional certification.

References

Adams, D. E., & Lothridge, K. L. (2000). Scientific Working Groups [on-line]. Forensic Science Communications, 2(3). Available: http://www.fbi.gov/hq/lab/fsc/ backissu.htm.

Noblett, M.G. (1995). Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. Proceedings of the 11th INTERPOL Forensic Science Symposium, Lyon, France. Boulder, CO: The Forensic Sciences Foundation Press.

Noblett, M.G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence [on-line]. Forensic Science Communications, 2(4). Available: http://www.fbi.gov.hq/lab/fsc/backissu/oct2000/computer.htm.

Scientific Working Group on Digital Evidence and International Organization on Digital Evidence. (2000). Digital Evidence: Standards and Principles [on-line]. Forensic Science Communications, 2(2). Available: http://www.fbi.gov/hq/lab/fsc/ backissu/april2000/swgde.htm

Scientific Working Group on Imaging Technologies. (1999). Definitions and Guidelines for the Use of Imaging Technologies in the Criminal Justice System [on-line]. Forensic Science Communications, 1(3). Available: http://www.fbi.gov/hq/lab/fsc/ backissu/oct1999/swigit2.htm.

About the Author

Carrie Morgan Whitcomb (whitcomb@mail.ucf.edu) is the Director of the National Center for Forensic Science (NCFS), a program of the National Institute of Justice (NIJ) hosted by the University of Central Florida (UCF) in Orlando, Florida. The NCFS provides research, education, training, tools and technologies to serve the current and future needs of the forensic science, investigative, and criminal justice communities.

Ms. Whitcomb serves on many committees working on definitions, best practices, and standards in the digital evidence field including: Co-Chair of Scientific Working Group for Digital Evidence (SWGDE), and Chair of the Industry and Academia Portfolio of the National Cybercrime Training Partnership (NCTP).

She earned a Masters of Science in Forensic Science, 1976 from George Washington University in Washington, DC and a Bachelors of Science in Zoology and a minor in Chemistry from the University of Kentucky in 1967.