THE VERY BRIEF HISTORY OF DIGITAL EVIDENCE STANDARDS

Mark M. Pollitt
Regional Computer Forensic Laboratory Program, Federal Bureau of Investigation
Washington, DC

Abstract: This paper will trace the development of forensic standards from the early efforts of law enforcement officers to its current state. The author will describe the role that national and regional groups have had upon the evolution of forensic practice. A number of current standards will be described as well as some developing ones.

Key words: Evidence, forensics, standards, laboratories

1. INTRODUCTION

Digital computers have been in use since the Second World War. For a majority of their existence, they have been large, cumbersome and controlled by government or industry. Their major impact was on the ability of industry and government to process business data. There were some prescient thinkers, like Donn Parker [1], who recognized that computers could be criminally victimized by people controlling other computers.

But that has all changed in the last twenty years! By July of this year (2002), over one billion computers had been sold. That number is predicted to double by 2008 [2]. The impact of computers and then the Internet has been felt in every country in the world. While some in law enforcement recognized the potential for computers to become a significant source of probative evidence, the mainstream forensic science community has only recently been engaged in the forensic process involved in developing procedures for this new, digital form of latent evidence.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35693-8_16
M. Gertz (ed.), *Integrity and Internal Control in Information Systems V*

2. A VERY ABRIDGED HISTORY OF COMPUTER FORENSICS

No one has recorded the very first forensic examination of digital information. It may well have been in the 1960's. Many of the people that are currently practicing the forensic examination of digital evidence would date the beginning of computer forensics to the late 1980's. It was then that investigators came across computers and media in the possession of "average" criminals. Since there was no formal mechanism to examine these items, any computer-literate policeman/investigator/public servant would do. It was truly a matter of "necessity being the mother of invention". After a while formal training began to be offered by organizations such as the Federal Law Enforcement Training Center [3] and the International Association of Computer Investigative Specialists [4]. These digital pioneers recognized that if done improperly, evidence could be altered, damaged or destroyed. So, they tried to be careful. Often they succeeded. Occasionally they failed. Eventually, preservation of the original evidence became a driving force in examinations of digital evidence, second only to getting the information.

These early pioneers reached out to each other and this was, in effect, the only support network available. The agencies, the prosecutors and the courts provided little encouragement or support. Often, examiners had to operate using personally owned equipment and software and on their own time. By the late 1990's most agencies had grudgingly acknowledged the need for "somebody" to do this work.

What evolved was a patchwork quilt of models and skills. Many agencies, even to date, do not have any digital evidence recovery program. Some utilize part-time personnel from a variety of organizations within law enforcement. Many agencies utilize sworn officers assigned to fraud, computer crime or high technology crime units to perform both investigative and forensic duties. Other agencies separate the forensic process and have digital evidence laboratories, sometimes within traditional crime laboratories.

Since the mid-1990's, a number of commercial ventures have entered the digital forensics business. Some grew out of data recovery businesses. Others took on contract computer forensic work for private companies, government agencies or both.

Whatever the future of digital forensics, it is certain to be both rapidly changing and growing in depth, as there will be and more sources of digital "trails" every year.

3. THE DEVELOPMENT OF STANDARDS

Digital evidence grew to prominence right behind DNA as a forensic discipline. The application of judicial tests for the admissibility of both scientific evidence and forensic examiners had recently been tested in the DNA field. The FBI Laboratory believed that DNA might be a model for developing the nascent discipline. DNA had gone through a series of meetings and symposia where the leading figures in biology and genetics were gathered to discuss, publish, and critique the use of DNA as a forensic tool. What issued was a consensus concerning the reliability of the technique and the best practices to utilize in conducting examinations. Perhaps, a gathering of the leading practitioners in digital evidence would be a good start.

In June of 1993, the FBI Laboratory gathered over 35 practitioners, from agencies representing twenty-six countries at Quantico, Virginia. During the course of this meeting, it was clear that the digital evidence community was receptive, but not ready to adopt standards. But the meeting served as the first formal bridge between the small groups of practitioners around the globe. An important insight was the recognition that even though most of these practitioners developed their skills in isolation, most had ultimately adopted very similar approaches, tools and techniques. There seemed to be a surprising level of common ground. The other product of this meeting was a consensus request to hold additional meetings of this sort. It was believed that an organization could be formed that would ultimately be in a position to develop standards once the community was ready.

4. FORMATION OF IOCE

It would be two years before this group could reassemble. They did so in Baltimore, Maryland. While many of the same people were in attendance, they and their agencies had matured in the interim. There was clear consensus that there was a need for a formal international organization which would provide a venue in which to exchange lessons learned and see the state of the art in other parts of the world. There was tacit recognition that standards would someday play a role, but that the community was still not ready. In fact, the Bylaws established for this new organization used terms like "recommendations". But the International Organization on Computer Evidence [5] (IOCE) was formed, and its first Chairman was Detective Sgt. David Thompson from the Victoria (Australia) Police. As such, it was his duty to host the next conference.

In February, 1996, the second meeting of the IOCE was held in Melbourne, Australia. There were a number of presentations made concerning computer forensic practices and techniques. While no substantial work was completed concerning the development of standards, the meeting's venue attracted many of the senior management of the practitioners who formed IOCE. As a result, management support was obtained for these practitioners continued participation in the organization.

5. THE HAGUE, 1997

The next meeting of IOCE was held in The Hague, Netherlands. Since the IOCE's start, computer forensics had achieved a modest level of recognition. Some agencies had developed units, laboratories and digital evidence programs. Others were seeking to do the same. At this meeting, the membership reached the conclusion that it was time to start on the idea of digital evidence standards. In addition to electing a new leadership team, the members called for IOCE Executive Board to find a way to move the development of computer forensic standards forward.

Within a month, the leaders of the G8 met in Washington, DC. The product of this meeting was a Statement of Principles and an Action Plan [6]. The eighth principle was as follows:

"Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed."

And the Action plan called for:

"Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions"

Immediately following this meeting, Scott Charney, who was the Chief of the U. S. Department of Justice's Computer Crime Section and the Chair of the G8 High Tech Crime Sub-Group, asked IOCE if they would be willing to undertake this challenge. After an Executive Board meeting, IOCE agreed.

IOCE's challenge was how to accomplish this task, given that IOCE meetings were held, at best, annually. By this point in history, there were

emerging several national and regional computer forensic groups that were dabbling in the development of standards. In the United Kingdom the Association of Chief Police Officers (ACPO) was in the process of developing a Good Practice Guide for computer based evidence [7]. The European Network of Forensic Science Institutes [8] (ENSFI) was forming a high tech working group. And in the United States, the Federal Laboratory Directors established a technical working group for digital evidence. The IOCE Executive Board decided that one way that might speed up the process would be to have the national/regional groups' work on the problem and bring proposals to the annual IOCE meetings for review and approval.

6. THE DEVELOPMENT OF SWGDE

In early 1997, the sixteen Directors of the Federal Forensic Laboratories in the United States chartered a Scientific Working Group on Digital Evidence[1] (SWGDE). This group was composed of representatives of the Federal Forensic Laboratories as well as representatives of several agencies that performed digital forensics outside the traditional forensic laboratory. Soon representatives from state and local agencies were invited to participate. The first order of business was to develop a document that included some definitions in digital evidence as well as a best practices document. The product that was produced was written in the American Society of Crime Laboratory Directors [9] (ASCLD) format, as that was the body that would likely accredit digital evidence laboratories in the United States. This document was presented to the IOCE meeting in London in 1999.

This document has been edited several times. At the time of this writing (October, 2002), the ASCLD Laboratory Accreditation Board (ASCLD-LAB) is voting on defining digital evidence as an accredited forensic discipline and adopting the SWGDE document [10] into the ASCLD-LAB Manual.

7. THE BEGINNING OF SYNTHESIS

In late 1999, the IOCE met in conjunction with the International High Tech Crime and Forensics Conference held in London, England. Delegates

[1] It was originally called the Technical Working Group on Digital Evidence. It changed title, along with all of the other working groups in 1998.

met to try and synthesize some common principles from the ACPO Good Practice Guide and the SWGDE proposed guidelines. What emerged was a set of IOCE Principles and Definitions. The Principles were consistent with both the ACPO and SWGDE documents. The definitions were lifted directly from the SWGDE document. This document was then forwarded to the G8 High Tech Crime Sub-Group for consideration as the foundation document for the G8 Action Item Eight.

It would take all of the year 2000 and part of 2001 for G8 to fine tune the IOCE document and adopt the G8 Principles. The difference in these documents is minimal and they are entirely consistent [11]. Meanwhile, during the 2000 IOCE meeting held in Paris, a more granular approach to good practice was explored. Working groups produced first drafts of good practice guides for various forms of digital evidence [12].

8. THE RISE OF ISO 17025?

During ASCLD's 2001 meeting, a proposal was put forward that ASCLD-LAB should adopt the ISO 17025 format and schema for forensic laboratory accreditation. While this proposal failed by a very narrow margin, it heralded a new phase of international cooperation on standards.

Europe has led the world in the adoption of ISO standards. So, it was not surprising that the ENSFI Forensic Information Technology Working Group developed a best practice document based on ISO 17025. At the IOCE meeting held in June of 2002 in Orlando, Florida, this document became the basis for further development by the assembled delegates [13].

9. THE FUTURE

In the span of less than a decade, digital evidence standards have come a long way. But, because digital evidence is likely to become the dominant form of evidence in the twenty-first century, it will become even more crucial. Trying to develop practical standards in a dynamic environment of new technology will be a continuing challenge. But the men and women who have freely given their energy and intellectual capital to the effort over the last ten years have left a solid foundation for those that follow.

REFERENCES

[1] Donn B. Parker: Crime by Computer. Charles Scribner's Sons. New York. 1976

[2] http://www3.cosmiverse.com/news/tech/tech07020201.html

[3] http://www.fletc.gov/

[4] http://www.cops.org/

[5] http://www.ioce.org/

[6] http://birmingham.g8summit.gov.uk/prebham/washington.1297.shtml

[7] http://www.ja.net/conferences/security/january01/N.Jones.pdf

[8] http://www.enfsi.org/

[9] http://www.ascld.org/

[10] http://www.swgde.org/swgde2002reportsProducts.shtml

[11] http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html

[12] http://www.ioce.org/2000/2000_cp.html

[13] http://www.ioce.org/2002/Guidelines