A History of Digital Forensics

Mark Pollitt

Chapter 1

A HISTORY OF DIGITAL FORENSICS

Mark Pollitt

Abstract The field of digital forensics is relatively new. While its history may be chronologically short, it is complex. This paper outlines the early history of digital forensics from the perspective of an early participant. The history is divided into four epochs: pre-history, infancy, childhood and adolescence. Each of these epochs is examined from the perspective of the people involved, the criminal targets, the forensic tools utilized, the organizational structures that supported digital forensic practitioners and how the community formed. This history is, by necessity, incomplete and biased. There is a need for rigorous historical research in this area before all traces of the past are forgotten or obliterated.

Keywords: Digital forensics, history

1. Introduction

One of the important rules in public speaking is to never begin with an apology. I have often broken this rule when delivering speeches and will do so again in this paper. My audience for this paper will be – for the most part – scientists, who expect well-documented foundations, reliable data and rigorous logic. Hence, my apology: there is little, if any, of these things in this paper.

It would be tempting to frame this exploration as historical research. And while I have done some research, which is duly referenced, this is fundamentally a personal history, which I have lived since the early 1980s. I am biased and less than fully informed; I have an unreliable memory and selective recall. Those of us who worked in this field from the beginning gave little thought to documenting a history. We were just trying to do our jobs.

So why should anyone read this paper? There are several reasons. For those who currently work in digital forensics and the students who are just entering the field, it is important to understand how we got here. During my tenure as a criminal investigator, one of my wisest informants insisted on teaching me the history of Baltimore, its ways and its people. He said, very correctly, that if I did not understand how people got where they did, I would not understand what they were doing now, what they might do in the future and why.

To those of us who have an interest in history, especially related to cyber crime and digital forensics, this paper is merely a starting point with many gaps that have to be filled. In some small measure, I hope this paper will serve as motivation to correct and expand the history as well as begin a dialog about the field, its past and its future. We must not delay – digital forensics is almost three decades old and many of the original players are moving on.

2. Epochs and Lenses

Even the simplest history has to have at least three phases: before, during and after. It may be called something more prosaic, but there is an inherent need for logical structure, even in something as illogical as history. For this story, I have chosen to use the notion of "epochs." It is, of course, entirely arbitrary on my part but it has both factual and logical bases. The epochs are: pre-history, infancy, childhood and adolescence.

Like traditional history, it is useful to explore a time period using a particular perspective. These are often called "lenses," as a metaphorical attempt to focus both the writer and the reader on specific elements of the historical data. In reviewing the history of digital forensics, I realized that there were some critical elements that combined to create the discipline. In my view these are: people, targets, tools, organizations and the community as a whole. I make no assertions that they constitute the totality of the history, but they are key vectors that help capture the essential elements of the history.

Modern electronic computers evolved during the second half of the 1900s. The History of Computing Project defines 1947 as the beginning of the Industrial Era of Computing [18] and we are still in the midst of this era. So much has happened in computing since 1947 that it is helpful to break it down into manageable chunks. In particular, digital forensics – or forensic computing as some like to call it – has a shorter history. As a result, I choose to make some further arbitrary divisions based on events that were significant to the digital forensic community.

3. Pre-History

The first epoch, which I label as pre-history, covers the period prior to 1985. It is not surprising that this is the least documented epoch because much of what happened was not focused on digital forensics. In fact, the term simply did not exist. From the 1960s until the early 1980s, computers were primarily an industrial appliance, owned and operated by corporations, universities, research centers and government agencies. They required a large physical infrastructure, including massive amounts of power and air conditioning, and highly skilled, dedicated staff. Their function was largely data processing. It is in this role that computers first became of interest to the information security, legal and law enforcement communities.

Donn Parker's 1976 book, *Crime by Computer*, is perhaps the first description of the use of digital information to investigate and prosecute crimes committed with the assistance of a computer. System administrators were, for the most part, responsible for the security of their own systems, most of which were not significantly networked to the outside world. System audits were designed to ensure the efficiency and accuracy of data processing, which was very expensive at the time. In effect, these audits constituted the first systematic approach to computer security. A byproduct of these efforts was that information collected during audits could be used to investigate wrongdoing [12]. This was not totally lost on the law enforcement community.

Organizations such as the Department of Defense, Internal Revenue Service (IRS) and Federal Bureau of Investigation (FBI) created *ad hoc* groups of volunteer law enforcement agents, who were provided with rudimentary mainframe and mini-computer training. These computer-trained investigators would assist other case investigators in obtaining information (primarily) from mainframe computers – stored data and access logs. Usually, the computer-trained investigators would work in cooperation with systems administrators.

Cliff Stoll's 1990 book, *The Cuckoo's Egg* [16], captures the practice and the ethos of early digital forensics. It also highlights the reluctance of government agencies to engage in this new area. It was difficult for traditional managers and investigators to grasp the potential of computers to be both tools and victims of crime. Stoll, then a Unix systems administrator, was attempting to reconcile two system accounting programs that were reporting a small difference in usage. After much investigation, he realized that hackers were accessing a large number of computers, including some sensitive systems. Using system administration tools and considerable experimentation, he developed, on his own initiative, a method for recording the hackers' malicious activities in real time.

Ad hoc and individual are the defining characteristics of the first epoch. There were virtually no dedicated organizations, procedures, training or tools specifically designed for digital forensics. Operating system tools and utilities were utilized along with traditional scientific and investigative problem-solving approaches.

4. Infancy (1985-1995)

The advent of the IBM PC in the early 1980s resulted in an explosion of computer hobbyists. The PCs, while powerful, had relatively few applications and were not, despite the advertising copy, user-friendly. Many of these hobbyists had previously worked with Commodore 64s, Radio Shack TRS-80s and Ataris. These early computers enabled hobbyists to write program code and access the internals of the operating systems and hardware. These skills were channeled to the new IBM PCs and PC-compatible computers.

Among the hobbyists were law enforcement personnel from a wide variety of organizations. Some of the key individuals were Mike Anderson, Danny Mares and Andy Fried from the IRS; Ron Peters and Jack Lewis from the U.S. Secret Service; Jim Christy and Karen Matthews from the Department of Defense; Tom Seipert, Roland Lascola and Sandy Mapstone from local U.S. law enforcement agencies; and the Canadians, Gord Hama and Steve Choy. Many of them became charter members of the first organization (to my knowledge) dedicated to digital forensics – the International Association of Computer Investigative Specialists (IACIS).

There were many other individuals as well. What they all shared was an understanding that computers would play a critical role in criminal investigations and, specifically, that computers are important sources of evidence. All these individuals believed this to the extent that they spent much of their own time and money to learn about new computing technologies. Their agencies were not supportive of their efforts, but we owe these individuals a debt of gratitude for the personal and financial investments that they made. Without their inspired and timely efforts, much of what we do today in the discipline of digital forensics would not be possible.

The early efforts were by no means limited to North America. Law enforcement officials in Europe, Asia and Oceania were struggling with the same problems and making the same personal commitment to prepare themselves and their organizations for the future that they knew was coming. In 1993, the FBI hosted the First International Conference on Computer Evidence at the FBI Academy in Quantico, Virginia, which was attended by representatives from 26 countries. At this conference, it was agreed that the community needed to band together at the agency level to coordinate efforts, share experience and provide assistance to each other. In 1995, the second conference was held in Baltimore and the International Organization on Computer Evidence (IOCE) was founded [21].

The cases investigated by these pioneers were very basic by today's standards. Much of the focus was on recovering data from standalone computers. Data recovery was a major issue because storage was costly and users routinely deleted data and re-formatted media. The Internet was not yet popular, but criminals were using dial-up access to compromise computers.

The use of inexpensive computers to hack the telephone system was a new dimension of fraud. Telephone service was billed by distance and use. Criminals and adolescents found that by hacking telephone networks they could obtain "free" telephone service as well as previously unavailable levels of anonymity [6].

The subjects of computer crime investigations were generally traditional criminals who used computers to support their activities or young people who used their technical skills to illegally obtain computer access and software. While IBM PCs and PC-compatible computers running DOS and early Windows variants were the most commonly encountered devices, early Apple products as well as Commodore and Atari computers were often encountered.

The tools used by the pioneering investigators included home-grown, command line tools and commercial products adapted to forensic use. Andy Fried's IRS Utilities, Steve Mare's Maresware, Steve Choy's IACIS Utilities and Gord Hama's RCMP Utilities were all command line tools that were distributed within the law enforcement community. Each of these tools tended to solve a specific digital forensic problem, such as imaging or identifying deleted files. Some of the later variants, like Hama's REDX, allowed for multiple operations and rudimentary piping. Norton Utilities and PC Tools, both commercial products designed for data recovery and file management, proved to be very powerful tools for digital forensics and virtually all the forensic training during the epoch utilized one or both of these tools. Another noteworthy product of this period was SafeBack, which was created by Chuck Guzis in 1991 to acquire forensic images of evidence. SafeBack may well have been the first commercial digital forensic product.

During this epoch, digital forensic practitioners conducted their examinations wherever they could find space. Often it was at their desks, in their basements at home or in unused storage space. The notion of a purpose-built laboratory was years away. Even large law enforcement agencies had hardly any funds for equipment – examiners had to use surplus equipment or the very equipment that they seized.

At the time, digital forensics was an arcane area that operated in direct conflict with the geographically- and statutorily-bound practice of criminal investigations. Criminals operated across city, state and national boundaries in almost real time, but investigators had no choice but to communicate and work directly with their peers, wherever they were located.

Digital forensic practice also operated in direct conflict with the traditional, laboratory-based practice of forensic science. However, some agencies did see the need for digital forensic capability. The IRS created the Seized Computer Evidence Recovery Specialist (SCERS) Program, the U.S. Secret Service its Electronic Crimes Special Agent Program (ECSAP), the FBI its Computer Analysis Response Team (CART), and the U.S. Air Force Office of Special Investigations its Computer Crime Investigator (CCI) Program and what eventually became the Defense Computer Forensic Laboratory (DCFL). Each agency adopted a different model of selection, training and operations based on its structure and culture. But these agencies were the exception; the majority of digital forensic investigations were performed by individual officers with minimal training, often using personal equipment, and without any supervision or formal quality control.

But the digital forensic community was growing. In addition to IACIS, many grassroots efforts were underway to pool knowledge, resources and talent. In the Midwestern United States, the Forensic Association of Computer Technologists (FACT) created training opportunities and a network of geographically-dispersed practitioners. In the Baltimore area, forensic practitioners from the FBI, U.S. Secret Service, Maryland State Police and Baltimore County Police started an *ad hoc* organization called "Geeks with Guns." In the United Kingdom, practitioners from many law enforcement agencies formed the Forensic Computing Group (FCG) under the auspices of the Association of Chief Police Officers (ACPO). It was during this epoch that the High Tech Crime Investigation Association was formed.

Forensic training was developed and offered by these organizations as well as by some of the larger law enforcement agencies. The demand for quality, affordable training far exceeded the availability, a situation that continued to plague the field of digital forensics for many years (some would argue that it continues to this day). During this period, the academic community was almost totally disinterested in the field, with two notable exceptions: Gene Spafford, from Purdue University and Dorothy Denning, then at Georgetown University. These two professors encouraged many law enforcement agents and students to venture into this important new field.

5. Childhood (1995-2005)

The next decade proved to be one of tremendous growth in size and maturity. This growth had numerous drivers, but there were three that had the most significance.

The first driver was the explosion of technology that occurred during the epoch. Computers became ubiquitous, cell phones became essential and the Internet became the world's central nervous system. At the beginning of the epoch, most voice calls were via landline, most computer network connections were via dial-up and most people had not heard of the Internet. By the end of the epoch, almost everyone had an email address, a cell phone, relied on the Internet, and most homes and businesses had networks. Computer technology was embedded in virtually every element of daily life and that included criminal activities.

The second driver was the explosion of child pornography cases. This can be traced back to the George Stanley Burdynski, Jr. case in 1993. The investigation revealed that computers were used to traffic in illegal images of minors and led to the establishment of an online undercover operation called Innocent Images in 1995. Ten years later, there was a separate child pornography task force in half of all FBI offices; many other law enforcement agencies also operated their own task forces. This "new" violation resulted in the seizure of ever-increasing volumes of digital evidence and was a major driver in the growth of digital forensics [4, 17].

The highly anticipated Y2K problem proved to be a non event from a computer perspective, but the events of September 11, 2001 rocked the digital forensic world, just as it did the world at large. While computers played little direct role in the hijackings, investigators would find bits and pieces of evidence on computers around the world. The terrorists were using computers in the same ubiquitous ways as everyone else. This was further reinforced on the battlefields of Iraq and Afghanistan. The intelligence community, law enforcement and the military realized that the lack of digital forensic capabilities was a blind spot that needed immediate attention. The amount of time, money, people and resources devoted to digital forensics increased to massive levels.

At the beginning of this epoch, digital forensic practitioners were typically self-declared professionals or "resident experts," a term used to describe individuals who were seemingly effective computer users. With increasing volume, technical sophistication and legal scrutiny, it became increasingly important to carefully select and train digital forensic practitioners. The field itself began to become even more specialized. Digital audio, video and embedded devices such as cell phones required specific knowledge and training, separate from traditional storage media and network-focused forensics. Even these two fields were beginning to diverge at some levels, as the study of network intrusions became ever more complex. The discipline of digital forensics began to be driven by government agencies and professional organizations rather than by individuals.

The formalization of digital forensics made great strides during this epoch. The IOCE, G-8 High Tech Crime Subcommittee and Scientific Working Group on Digital Evidence (SWGDE) all published digital forensic principles between 1999 and 2000 [3, 7, 10, 15]. Going beyond mere principles, the American Society of Crime Laboratory Directors – Laboratory Accreditation Board (ASCLD-LAB), in cooperation with the SWGDE, recognized digital evidence as a laboratory discipline. In 2004, the FBI's North Texas Regional Computer Forensic Laboratory became the first ASCLD-LAB accredited digital forensic laboratory [1, 11].

Meanwhile, forensic tools underwent a metamorphosis. The home-grown, command line tools of the earlier epoch became complex, graphical user interface suites. The first of the new tools was Expert Witness, a product designed by Andy Rosen for Macintosh forensics that evolved into EnCase. EnCase, along with Forensic ToolKit (FTK), became commercial successes and are now standard forensic tools.

Several U.S. Government agencies also took on the task of developing tools. The FBI's Automated Case Examination System (ACES) and IRS's iLook tool had some success. However, the ability of commercial entities to evolve their products in step with advancing technology doomed the agency-developed tools to obsolescence. Meanwhile, the open source community stepped up, developing Linux tools such as Helix, Sleuth Kit and Autopsy Browser.

The digital forensic community likewise underwent a maturation process. Forensic services were being provided by a wide variety of entities, organized in a wide array of structures. Traditional forensic laboratories began offering digital examinations. The Department of Defense created its central Defense Computer Forensic Laboratory (DCFL) to service the law enforcement, intelligence and operational needs of the U.S. military [19]. The FBI started building a constellation of joint (federal, state and local law enforcement) laboratories dedicated to digital forensics – the Regional Computer Forensic Laboratories (RCFLs) [13]. Each laboratory would provide service to a geographic area and operate according to ASCLD-LAB standards. The U.S. Secret Service established a network of Electronic Crimes Task Forces, modeled on the highly-effective New York entity [20]. These task forces would provide investigative and forensic services within their area of operations. Many law enforcement agencies also developed dedicated units to handle digital forensic investigations.

6. Adolescence (2005-2010)

Since 2005, digital forensics has grown in depth and breadth. It has far more practitioners, performing many more examinations of a wider variety, involving ever larger amounts of evidence. In 2006, the United States Courts adopted new Rules for Civil Procedure that defined digital information as a new form of evidence and implemented a mandatory system, called electronic discovery or "eDiscovery," for dealing with digital evidence [5]. The workload in traditional law enforcement mushroomed. In Congressional testimony, the FBI announced that its Computer Analysis and Response Team (CART) examined more than 2.5 petabytes of evidence in 2007 alone [9].

Information security professionals now recognize digital forensics as a core skill area. While their objectives and needs often differ from those of law enforcement, the concepts and tools are often identical.

The digital evidence practitioners of today are far more likely to have had academic preparation in addition to formal training. They are likely to hold an array of certifications. Digital forensics is now considered "career enhancing," a far cry from just a few years ago.

Academic programs continue to spring up across the globe. While research funding for digital forensics lags other more traditional disciplines such as information security, colleges and universities have recognized the popularity and marketability of digital forensic education. Recently, the Forensic Education Program Accreditation Commission (FEPAC) took the first steps toward accrediting U.S. academic programs in digital forensics. The American Society of Testing Materials (ASTM) Technical Committee E-30 formulated a draft standard for digital forensic education and training programs [2].

Another measure of the academic health of a field is the number and quality of conferences. The Digital Forensic Research Workshop (DFRWS) is in its tenth year. The International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics is in its seventh year and the International Conference on Systematic Approaches to Digital Forensic Engineering just celebrated its fifth anniversary.

The materials that are being examined have also matured. Virtually every device that uses electricity now has some form of digital storage. Wired or wireless networks connect many of the devices that we use in our daily lives. This, in turn, has driven the development of many network- and web-based services, including cloud computing. Some of these services, such as Facebook and Twitter, are changing the way in which people interact. This change is starting to drive how digital evidence is collected. Email has already become a major source of probative information and a forensic and information management challenge [8].

During this epoch, forensic suites, most notably EnCase and FTK, have moved into the network/enterprise environment. They are being deployed in a prospective fashion in enterprises for corporate security and electronic discovery purposes. These same tools are being adapted to work in the emerging forensic environment of virtualized laboratories (using products such as VMWare) and storage area networks (SANs). Meanwhile, high-speed networks are being utilized to support the online review of evidence by investigators and prosecutors. The market for electronic discovery is booming, with vendors developing proprietary tools to automate the extraction and review of digital information.

This is an interesting time for the digital forensic community as a whole. The law enforcement, military and intelligence communities have designed organizational structures and processes to support their mission view. While there are some in these communities that are considering the impact of future technologies, there is far less emphasis on how targets will utilize these technologies and how customers will utilize the forensic products. Defining the forensic products of the future is another challenge. A strong tactical approach exists, but a long-term strategic plan is missing.

7. The Future

Predicting the future is a fool's game. Knowing that I will be wrong about many of my predictions, I will play the fool.

Digital forensics is a complex and evolving field. The practitioners of the future will be even better educated and trained; they will be team players trained to perform specific aspects of the forensic process. Forensics will no longer be a linear process focused on recovering data, but an evidence-based knowledge management process that will be integrated into investigations, intelligence analysis, information security and electronic discovery. There will be career digital forensic educators and researchers in addition to practitioners and managers. I fear that this new generation will be unaware of the early history and pioneering spirit that propelled the early years.

Our adversaries will be better organized, funded and educated. Criminals have recognized the value of distributed and collective efforts. Their payoffs will be significantly larger as the value of access and information grows along with society's dependence on the information infrastructure. Everyone (and their information) everywhere will be at risk at all times. Safety and security will be constantly threatened.

To counter these threats, digital forensic tools will have to improve. To overcome the sheer volume, the tools will have to be automated. In addition to performing data recovery, the tools will need to have built-in analytical capabilities, enabling important items to be identified without having to view every item. The tools will have to be semiotic, understanding human language and communications, and able to interpret content and context.

The organizations that employ digital forensic practitioners and those who rely on them will have to evolve as well. They will need to be accredited, with strong quality management and individual certifications. Much will ride on their reported results. Society needs assurance that the information collected and the conclusions reached are reliable. Organizations will have to cooperate and support the interoperability of people, tools and processes. Given the global scope of the problem, international legal standards will have to evolve.

8. Conclusions

In less than thirty years, digital forensics has blossomed from the germ of an idea, nurtured by brave pioneers, developed and expanded by professionals, to its current state. Many individuals have contributed their efforts, knowledge and enthusiasm to give the discipline a solid foundation for the future.

I apologize to the many worthy people who I have failed to mention in this narrative out of ignorance or forgetfulness. I earnestly hope that others will correct my errors, fill in the gaps and extend this work. Recording a complete history of digital forensics will benefit those who come after us. In the immortal words of George Santayana, "Those who cannot remember the past are condemned to repeat it" [14].

References

[1] American Society of Crime Laboratory Directors – Laboratory Accreditation Board, Garner, North Carolina (ascld-lab.org).

[2] ASTM International, ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics, West Conshohocken, Pennsylvania (www.astm.org/Standards/E2678.htm), 2009.

[3] R. Downing, G-8 initiatives in high tech crime, presented at the *Asia-Pacific Conference on Cybercrime and Information Security*, 2002.

[4] Federal Bureau of Investigation, Innocent Images National Initiative, Washington, DC (www.fbi.gov/innocent.htm).

[5] Federal Judicial Center, Materials on Electronic Discovery: Civil Litigation, Federal Judicial Center Foundation, Washington, DC (www.fjc.gov/public/home.nsf/pages/196).

[6] K. Hafner and J. Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Touchstone, New York, 1991.

[7] International Organization on Computer Evidence, G8 Proposed Principles for the Procedures Relating to Digital Evidence, Ottawa, Canada (ioce.org/core.php?ID=5), 2000.

[8] E. Iwata, Enron case could be the largest corporate investigation, *USA Today*, February 18, 2002.

[9] M. Mason, Congressional Testimony, Statement before the House Judiciary Committee, Federal Bureau of Investigation, Washington, DC (www.fbi.gov/congress/congress07/mason101707.htm), 2007.

[10] M. Noblett, Report of the Federal Bureau of Investigation on the development of forensic tools and examinations for data recovery from computer evidence, presented at the *Eleventh INTERPOL Forensic Science Symposium*, 1995.

[11] North Texas Regional Computer Forensics Laboratory, Dallas, Texas (www.ntrcfl.org/index.cfm).

[12] D. Parker, *Crime by Computer*, Scribner's, New York, 1976.

[13] RCFL National Program Office, Regional Computer Forensics Laboratory, Quantico, Virginia (rcfl.gov).

[14] G. Santayana, *Reason in Common Sense*, *Life of Reason, Volume 1*, Scribner's, New York, 1905.

[15] Scientific Working Group on Digital Evidence, Digital evidence: Standards and principles, *Forensic Science Communications*, vol. 2(2), 2000.

[16] C. Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, New York, 1990.

[17] The Charley Project, George Stanley Burdynski Jr., (www.charley project.org/cases/b/burdynski_george.html).

[18] The History of Computing Project, Timeline: Chronology of the history of computing, The History of Computing Foundation, Maurik, The Netherlands (www.thocp.net/timeline/timeline.htm), 2010.

[19] U.S. General Accounting Office, Crime Technology: Department of Defense Assistance to State and Local Law Enforcement Agencies, Letter Report GAO/GGD-00-14, Washington, DC (fas.org/irp/gao /ggd-00-014.htm), 1999.

[20] U.S. Secret Service, Electronic Crimes Task Forces and Working Groups, Washington, DC (www.secretservice.gov/ectf.shtml).

[21] C. Whitcomb, A historical perspective of digital evidence, *International Journal of Digital Evidence*, vol. 1(1), 2002.