# 1

# A Definition of Computer Forensics



## INTRODUCTION

In this chapter, I introduce the science of computer forensics—both what it is and what it is not. Although the term is heard these days with increasing frequency, the discipline itself has existed for only a short time. Only within the past 20 years has the admission of digital evidence gained consistent recognition in our court systems. In fact, some courts systems around the world may not admit certain types of digital evidence. As you might imagine, given the relative youth of this area of study, some mistakes were made early on. It is to be hoped that those mistakes have been long since corrected, and, while completely smooth sailing is doubtful, at least calmer seas are on the horizon. As we begin this journey, it is only fitting to lay some groundwork. This groundwork, in the form of history, will help provide a clearer picture of the role that computer forensics plays in our legal system. It begins with a discussion of forensics itself.

## FORENSIC SCIENCE

The term "forensics" is often misunderstood and is frequently misused. Whether in popular television or the news media, the term is often thrown around without regard to what it actually means. From the Latin *forensis*, the term means "belonging to, used in or suitable to courts of judicature or to public discussion and debate."[1] Forensics exists independently of any particular field of study.

For example, forensic entomology, while grouped with other forensic fields, is really nothing more than the scientific study of insects, with the added qualifier that it is done with a goal of introduction into court. In fact, Gil Grissom of television's *CSI* is probably America's most famous forensic entomologist, albeit a fictional one, and has single-handedly made bug lovers sexy.

In reality, although there are a small group of fields in which forensic analysis is common, practically any field of study is amenable to such work. For example, most people have heard of forensic psychologists, who offer evidence in court regarding mental states and conditions; few people know that there are forensic engineers, who offer scientific evidence within their subspecialty. For example, a forensic electrical engineer might offer testimony regarding the cause of a fire related to faulty wiring. Fewer people still have heard of the field of forensic linguistics. Since linguistics is the study of language, a forensic linguist might be used to analyze the language used in a suicide note, compared to miscellaneous writings of the deceased prior to death, to try to determine if the note was in fact written by the deceased.

Therefore, by extension of this logic, computer forensics is the scientific study of computers in a manner consistent with the principles of the rules of evidence and court rules of procedure. This is exactly what the field of computer forensics is. It is also important to understand what it is not.

Even among those knowledgeable in the field, some confusion exists over what particular areas of computer science should actually be included under the umbrella of computer forensics. In order to better illustrate what is, and what is not, traditionally considered computer forensics, a brief history of the evolution of computer science into the study of computer forensics is helpful.

## HISTORY OF COMPUTER FORENSICS

The most influential aspects of computer history are the history of the machines themselves. The evolution of the computer from a mysterious black

box of interest only to academics and technical types, to a ubiquitous fixture in nearly every home, is a unique and interesting story.

Once of the biggest changes to occur is the sheer size of the computer. In the early 1950's the first computers were housed in buildings dedicated solely to their operation. These behemoths, less sophisticated than today's three-dollar calculator, were unbelievably costly and amazingly temperamental. Designed and built using conventional vacuum tubes, many of the circuits were large enough for computer scientists to actually walk among the components removing debris and small bugs that were causing malfunctions—hence the term "bug," which in computer lingo signifies an operating glitch. Their size and cost made the first computers little more than curiosities for the average American. In fact, until 1981, when IBM released its first personal computer (PC), personal home computers were a rarity.[2]

Or perhaps the mystique that shrouds the computer is the result of the fact that computers speak their own language. Originally computers were nonprogrammable in the sense we think of today. Eventually, as they evolved, the ability to change their configuration emerged, and while difficult under the best conditions, changes could be made to their functionality. As the power of the computational ability of computers expanded during the late 1940s and 1950s, interacting with the computers became a greater focus.

In 1954 John Backus, an employee of IBM, developed the first high-level programming language.[3] This language, FORTRAN, short for formula translation, was subsequently released commercially, and thus began the computer revolution. Prior to FORTRAN and other high-level languages that would follow, such as COBOL and C++, the only way to communicate with the computer was through machine language: a series of 0s and 1s. Machine language eventually led to a second layer of language known as assembly language, which turned the 0s and 1s of machine code into human words, such as PUSH, POP, and MOVE.

From this highly complicated language system emerged FORTRAN and COBOL and later C+. These high-level languages, while much simpler than machine language, were still well beyond the capabilities and comprehension of the average citizen, which contributed to the mystique of computers. Unlike the telephone, which was an unprecedented phenomenal scientific advancement in its own right, you needed to know an entirely new language to communicate with computers.

Whatever the reason, whether cost or communication barriers, computers remained an academic and military phenomenon for much of their early lives. However, as computers began to take a foothold, a cottage industry of home

computer kits emerged. These kits, ranging in cost from $1,500 to $4000, were targeted to computer and electronics hobbyists who wanted to own their own computer—some assembly required.[4]

Historically, many of the advances in the home computer, later rebranded the personal computer thanks to IBM's marketing of the IBM-PC, occurred in a hobbyist, garage-tinkering way. Industry leaders such as Bill Gates, Steve Jobs, and Steve Wozniak began their careers by building home-brewed versions of commercial products. Were it not for the innovations of these early pioneers, the PC would not have evolved in the fashion it had.[5] This characteristic is much more than an interesting footnote to history. On the contrary, I believe it is the single most important factor influencing the nature of computer forensics.

The modality through which early home computers evolved promoted an environment of innovation and tinkering, the heart and soul of which is exploration and adaptation. I liken the environment of the 1970s and early 1980s, during which some of the greatest advancements in home computers were made, to a young child disassembling a parent's transistor radio to figure out how it works. This spirit of exploration, while at the heart of most all innovations and inventions, would have been no different from the exploration of our ancestors such as Guglielmo Marconi and Enrico Fermi, but for the influence of one phenomenon: the Internet.

There is some disagreement over the actual origin of the Internet. Some claim that it was built in cooperation with the Department of Defense as a vast nationwide "communications bomb shelter." Others argue that it was more about linking research institutions together than providing for the common defense.[6] Regardless of which side you believe, the Internet was in fact originally a small network of computers known as the ARPANET. The ARPANET originally consisted of four computers located at research facilities at the University of California at Los Angeles, Stanford, the University of California at Santa Barbara, and the University of Utah. From those humble beginnings there arose the phenomenon we know today.[7]

Much like the PC, the environment in which the ARPANET began to grow greatly influenced its development. From its early days, the Internet began to evolve as a space for the exchange of information—a common, if you will, where both ideas and academic materials could flow freely. This flow of information was in fact so freely flowing that as the network began to grow, so did military concerns for security. After more and more nonmilitary institutions began joining the network, the Department of Defense decided to abandon it in favor of its own network. In 1983 MILnet was formed using the same basic backbone of the original system.[8]

It was from this original academic mind-set that the Internet as we know it emerged. Understanding the academic background of the Internet is important because of the type of community that it promoted among its users. This community was formed in the spirit of cooperation and free sharing of information. Academic pursuit thrives on knowledge and information and the free flow of ideas and unfettered access. In the early days, the concept of ownership and regulation of this "cyber" space were the last things on the minds of the newly emerging netizens. In this almost "Wild West frontier" environment, the rules, such as they were, were loose, highly fluid, and designed as honor codes more than traditional rules. Information and free access were king and queen, and citizens of this new domain were short on regulation and long on enthusiasm.[9]

This attitude coupled with the developments in the PC world created the beginnings of our computer forensic industry. Computer icons like Bill Gates, Steve Jobs, and Steven Wozniak built their fortunes on more than merely the spirit of competition. They built them on innovation born of the spirit of exploration and tinkering and a how-can-I-make-it-better attitude. The Internet in its early days of nonregulation was an environment tailor made for this entrepreneurial spirit. Additionally, the average computer user during the early days of the Internet was more like Bill Gates than today's black-box user.

Computers were more a phenomenon of the hobbyist and electronics buff than a fixture in every home. As a result, these users shared much more closely the personality traits of the early adopters like Gates, Wozniak, and Jobs. All these traits—openness, innovation, and exploration—combined to create a free-wheeling world in which the only rules were that there were really no rules.

## WORLD WIDE WEB

For some readers not old enough to remember, there was a day in which the Internet was not the World Wide Web. Although those two terms are often used interchangeably, they are in fact two different concepts. The Internet, as I explained, is the network infrastructure upon which the communications between linked nodes traverse. The World Wide Web is the linked set of the pages that make up each site on the Internet. In a way very similar to the impact that the graphical user interface (GUI) had on the PC, the development of hypertext markup language (HTML) revolutionized the Internet.

Prior to HTML, the Internet was in use by scientists, academic types, and serious hobbyists with a strong technical grounding. However, the rest of us

were still living in the real world, not the cyberworld. The reason for this is again language.

Prior to the adoption of HTML, Internet communication was done through typed commands and very technical instructions. The most prevalent language at that time was a form of the high-level programming language known as UNIX. While a very powerful language, and the origin of many subsequent languages, such as C and C++, UNIX requires memorization of often confusing keywords that must be typed, precisely, on a blank screen. One misspelled word and the command is rejected. This was no different from the state of personal computers under the Disk Operating System (DOS) and Control/Program Monitor (CP/M) operating systems. The GUI changed this.

The GUI, first introduced in the Lisa computer introduced by Apple, made the functionality of the computer independent from the user's knowledge of computer commands.[10] Point and click, drag and drop, and iconic selection were born and in turn gave birth to the World Wide Web revolution. The GUI made the average user, without the slightest knowledge of computer language, a computer genius.

HTML became the GUI of the Internet. By presenting users with pictures, buttons, and tabs from which to choose, programmers removed the requirement of well-developed computer knowledge. Computer access for the masses was born. However, just because the revolution was in progress does not mean that UNIX and the way of the computer guru had disappeared. It was in this environment, on the cusp of the Internet revolution, that I first had a chance to encounter the computer counterculture.

## HACKER COMMUNITY

My first encounter with hacking can be instructive in that it illustrates how computer forensics has evolved from intrusion detection and why the two are entirely different areas with entirely different goals.

In the "old days," circa 1990, while working as a criminal investigator, I was introduced to two young boys roughly 15 years old. They were not yet old enough to drive but were quite computer literate. A road patrol officer dropped them at my desk explaining they had been caught prowling around the bushes in a middle-class neighborhood. In their backpacks officers found a stack of computer paper (the old perforated continuous-form kind), a spiral notebook, a flashlight, and an orange lineman's handset (the sort of handheld telephone receiver with alligator clip connectors that telephone repairmen use to test lines). Unsure of what crime they might be committing, but sure they were up to no good nonetheless, they brought them to me. Not because I

was the high-tech detective, but because I happened to have the misfortune of being the first in the office.

After an unproductive series of grunts and smirks and a final "I've got nothing to say," they were both released to their parents with juvenile referrals for loitering and prowling. Their backpack remained behind.

An inventory of its contents would send me into a new world, one in which I would spend a large portion of the rest of my career. The purpose of the flashlight was clear; the purpose of the rest of the contents, not so much.

The computer printout could just as easily have been in a foreign language, and the lineman's handset, while I was familiar with what it does, did not immediately reveal what the boys were up to. What did was the notebook. Within its pages were a list of phone numbers with distant area codes and exotic names. Research revealed that these names and phone numbers were for computer bulletin board systems (BBSs). These bulletin boards were the forerunner to today's Internet, and were private sites to which callers could connect through dial-up modems.

Before the days of the Internet and World Wide Web, the only way to connect from site to site was through a direct-dialed connection. While fairly simple in theory, in practice this became a very time-consuming—and expensive—undertaking. At that time, cell phones were a speck on the horizon, and the days of unlimited calling were unheard of. In order to connect to a BBS in a distant area code, the caller would incur long-distance charges. Add to that the technology bottleneck of a modem operating at 28.8 Kbps (kilobits per second; compared to the average speed of 6 to 8 Mbps [megabits per second] for today's Digital Subscriber Lines (DSL) and cable modems, and phone bills in the range of thousands of dollars were common.

What possible reason would someone risk an exorbitantly high phone bill in order to connect to a distant computer? Besides child pornography (which was as popular then as it is today), computer hacking. The two boys in my office were computer hackers who, armed with a list of hacker Web sites, were downloading small program excerpts known as exploits that would help them break into computers. In addition to exploits, the BBSs provided tutorials, computer manuals on most large mainframe computer systems, and an assortment of tools to equip the well-armed hacker.

For me, this was an eye-opening experience. It began me on my journey, a journey in which I would learn about a community that operated by a different set of rules, a set of rules that set the stage for all that would follow in the computer forensic world.

At that time, computer hackers subscribed to a code known as the "Hacker Manifesto," a pithy rebellious explanation or, more accurately, a

rationalization for what they do. This page-long diatribe allegedly written in 1986 by a hacker named "The Mentor" blames a society of adults for the angst of the teen and uses this as justification for their knowledge-seeking behavior. The credo was written shortly after his arrest in 1986 and first appeared the hacker underground newspaper *Phrack.* The final few paragraphs of this credo are particularly appropriate:

> *This is our world now . . . the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore . . . and you call us criminals. We seek after knowledge . . . and you call us criminals. We exist without skin color, without nationality, without religious bias . . . and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.*
>
> *Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.*
>
> *I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all . . . after all, we're all alike.*[11]

The Mentor, who was later identified as Loyd Blankenship, was a member of an underground hacking group known as the Legion of Doom, believed by some to be the largest and best-organized of the hacker groups in the 1980s. Their attitude is typical of the attitude of the hacker community during that time.[12]

I use the term "community" purposely, since during that time the way of thinking was very much a community of us versus them: hacker versus nonhacker. The manifesto's stated goal of knowledge seeking and exploration probably hit its most fevered pitch during the Great Hacker War. While the title seems melodramatic, the competition that raged between the Legion of Doom and its rival faction, Masters of Deception, during a brief period during the early 1990s was driven by the goal of gaining entry to computers for the sake of prestige within the community.

Knowledge seeking, as you may recall, fits in well with the personality of the computer entrepreneur and the Internet founders. My introduction to this mind-set in the "Hacker Manifesto" ultimately led me to seek information from the mainstream computer community.

At that time, PCs were not yet household items. Although most major universities offered courses in computer science, computers were still something of an oddity in the home. Mainframe computers, however, were well established, so I turned to a number of local computer professionals. With their guidance, I learned my second essential lesson: Computer professionals

were more concerned with protection than prosecution. At first, this distinction may sound negligible, but in the context of the evolution of computer evidence, it proves to be a key element.

The prevailing mind-set was to identify the vulnerability, patch the hole, and kick intruders off the system. For most if not all system administrators (to the extent that that position even existed back then), this approach was necessitated for two reasons.

First, when dealing with a large company, the admission that a hacker compromised the system would be extremely damaging to the public image. We see this even today. By admitting that a system has been hacked, the business admits that it has failed to protect customer assets. In many cases, the loss of revenue due to the admission is far greater than the cost of simply plugging the hole and moving on.

Second, many viewed the intrusion as an inconvenience, not a crime. It is helpful to keep in mind that many of the information technology (IT) professionals in system administrator positions share a common bond with the hacker community: shared inquisitiveness. As a result, many system administrators saw intrusions, especially where nothing was stolen or damaged, as more prank than grounds for prosecution.

In this atmosphere, there was very little room for concern over things like the admissibility of evidence and chain of custody. Administrators were both ignorant of and complacent about the rules of evidence and the need to secure a conviction. As I mentioned, their concern was a secure system. To the extent that administrators began asking for police assistance, most of the time it was done after the fact, and after, as we discuss in later chapters, valuable evidentiary data had been destroyed.

In this atmosphere, by the time police were called, the law enforcement response suffered from an overwhelming lack of knowledge, which manifested itself on several levels. First, during this era, most police agencies, even large ones, had no one trained to recognize or investigate computer crimes. It was not until computer crime began gaining more media attention that police departments began identifying and training investigators in the unique demands of computer investigations. Even today, a number of small and medium-size agencies do not maintain a full-time high-tech crime unit, and a handful still fail to routinely train officers in digital evidence recovery. These agencies ignore the fact that recovering digital evidence differs in some substantial ways from recovering nondigital evidence.

At another level, the public response was lacking. By this I mean that the system itself—our criminal justice system—was ill-prepared to handle and prosecute these types of offenders. For example, during the early years of

the rise in computer-based crime, laws for dealing with the unique elements comprising a computer crime were often ineffective. As a result, prosecutions were often impossible because, by law, the suspect's conduct was not "illegal." Fortunately, since that time, all states have addressed this issue, and fairly uniform laws are in place nationwide and federally to deal effectively with all types of computer crimes.

Finally, since computer evidence recovery was in its infancy, there were no established and documented procedures in place. Although the general rules of evidence offered guidance, a lack of knowledge about the nature of digital evidence made the application of the rules very difficult. In short, we were learning as we went, and in doing so, the only model we had for use was the model of the computer professional: a nonlegal model. Adding to this lack of knowledge was the fact that those from whom we could seek legal guidance were equally clueless regarding the true nature of digital evidence. These factors made early evidence collection methods highly suspect by today's standards.

Fortunately, as we have moved forward, our knowledge of digital evidence and of the role the computer professional plays in its recovery has improved vastly. It is the role that the computer professional plays that brings me to my conclusion that intrusion detection, while perhaps a subfield of computer forensics, is essentially not a forensic field.

Experts in the area of intrusion detection can, and often should, think like computer forensic technicians; however, many of the things that intrusion detection requires are not necessarily compatible with the best practices of forensic recovery. For example, tracking down and kicking out an intruder to a system will, by its very nature, require the alteration of digital evidence. The alteration of digital evidence is something that forensic technicians must protect against in order to establish reliability of the evidence. Therefore, the actions of a system administrator who identifies an intruder and subsequently deletes the Trojan horse or exploit that was planted to gain superuser access will compromise future ability to prosecute the intruder. Likewise, in some cases collecting the evidence necessary to prosecute the intruder may reduce the system administrator's ability to protect the system, at least in the short term. In the end, both approaches require a compromise. Succeeding with both roles simultaneously is not impossible; it does require, however, that both jobs recognize the limitations and demands of the other.

## CONCLUSION

As you can see, my earlier statement that intrusion detection and computer forensics have different goals is correct. Because I see the role of the intrusion

detection profession as different from the role of the computer forensic professional, I would categorize them separately, and do not consider intrusion detection under the broad umbrella of computer forensics. Ultimately it will be up to you to decide, and if you are an IT professional or direct an IT staff, on occasion you may be faced with the dilemma of having to choose between those two goals. As we move into the next chapter, bear in mind the brief history that we have covered here. While far from comprehensive, it should help you to understand better the direction we may be headed.

In the next chapter, we begin our discussion of exactly what computer forensics entails and get to know the components and processes of a computer system. As always, remember that this is not a how-to manual or a reference source on collecting digital evidence but an introduction to the field of computer forensics and its limitations.

## NOTES

1. *Webster's New Universal Unabridged Dictionary,* 2nd ed. (New York: Barnes & Noble Books, 2003).
2. See generally Paul E. Cerruzzi, *The History of Modern Computing,* 2nd ed. (Cambridge, MA: MIT Press, 2003).
3. IBM Archives, "John Backus," www-03.ibm.com/ibm/history/exhibits/builders/builders_backus.html.
4. See generally Christos J. P. Moschovitis, Hilary Poole, Tami Schuyler, and Theresa M. Senft, *History of the Internet: A Chronology, 1843 to Present* (Santa Barbara, CA: ABC-CLIO, 1999). See also Mary Bellis, "The First Hobby and Home Computers: Scelbi, Mark-8, Altair, IBM 5100," Inventors of the Modern Computer, http://inventors.about.com/library/weekly/aa120198.htm
5. Ibid.
6. Moschovitis et al., *History of the Internet,* pp. 52–55; See also Bellis, "ARPANET—The First Internet," Inventors of the Modern Computer, http://inventors.about.com/ library/ weekly/aa091598.htm.
7. Moschovitis et al., *History of the Internet.*
8. Ibid.
9. See generally Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
10. Mary Bellis, "The History of the Graphical User Interface," Inventors of the Modern Computer, http://inventors. about.com/library/weekly/aa043099.htm.
11. The Mentor, "The Conscience of a Hacker," *Phrack, Inc.* 1, no. 7 (1986); available at: http://www.phrack.org/phrack/7/P07–03.

**12.** Bernadette H. Schell and John L. Dodge, *The Hacking of America* (Westport, CT: Quorum Books, 2002), p. 123. See also *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/w/index.php?title=Loyd_Blankenship&oldid=76258023.

## SUGGESTED READING

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. New York: Penguin Books, 1994.

Slatalla, Michelle. *The Masters of Deception: The Gang that Ruled Cyberspace*. London: Harper-Perennial, 1996.