CHAPTER 1
Introduction

Information in This Chapter:

- What Is Forensic Science?
- What Is Digital Forensics?
- Uses of Digital Forensics
- Role of the Forensic Examiner in the Judicial System

"Each betrayal begins with trust."

—"Farmhouse" by the band Phish

INTRODUCTION

Your computer will betray you. This is a lesson that many CEO's, criminals, politicians, and ordinary citizens have learned the hard way. You are leaving a trail, albeit a digital one; it's a trail nonetheless. Like a coating of fresh snow, these 1s and 0s capture our "footprints" as we go about our daily life.

Cell phone records, ATM transactions, web searches, e-mails, and text messages are a few of the footprints we leave. As a society, our heavy use of technology means that we are literally drowning in electronically stored information. And the tide keeps rolling in. Don't believe me? Check out these numbers from the research company IDC:

- The digital universe (all the digital information in the world) will reach 1.2 million petabytes in 2010. That's up by 62% from 2009.

If you can't get your head around a petabyte, maybe this will help:

> "One petabyte is equal to: 20 million, four-drawer filing cabinets filled with text or 13.3 years of HD-TV video."
>
> **(Mozy, 2009)**

The impact of our growing digital dependence is being felt in many domains, not the least of which is the legal system. Everyday, digital evidence is finding

The Basics of Digital Forensics. DOI: 10.1016/B978-1-59749-661-2.00001-2

its way into the world's courts. This is definitely not your father's litigation. Gone are the days when records were strictly paper. This new form of evidence presents some very significant challenges to our legal system. Digital evidence is considerably different from paper documents and can't be handled in the same way. Change, therefore, is inevitable. But the legal system doesn't turn on a dime. In fact, it's about as nimble as the Titanic. It's struggling now to catch-up with the blinding speed of technology.

Criminal, civil, and administrative proceedings often focus on digital evidence, which is foreign to many of the key players, including attorneys and judges. We all know folks who don't check their own e-mail or even know how to surf the Internet. Some lawyers, judges, businesspeople, and cops fit squarely into that category as well. Unfortunately for those people, this blissful ignorance is no longer an option.

Where law-abiding society goes, the bad guys will be very close behind (if not slightly ahead). They have joined us on our laptops, cell phones, iPads, and the Internet. Criminals will always follow the money and leverage any tools, including technology, that can aid in the commission of their crimes.

Although forensic science has been around for years, digital forensics is still in its infancy. It's still finding its place among the other more established forensic disciplines, such as DNA and toxicology. As a discipline, it is where DNA was many years ago. Standards and best practices are still being developed.

Digital forensics can't be done without getting under the hood and getting your hands dirty, so to speak. It all starts with the 1's and 0's. This binary language underpins not only the function of the computer but how it stores data as well. We need to understand how these 1's and 0's are converted into the text, images, and videos we routinely consume and produce on our computers.

WHAT IS FORENSIC SCIENCE?

Let's start by examining what it's not. It certainly isn't Humvees, sunglasses, and expensive suits. It isn't done without lots of paperwork, and it's never wrapped up in sixty minutes (with or without commercials). Now that we know what it isn't, let's examine what it is. Simply put, **forensics** is the application of science to solve a legal problem. In forensics, the law and science are forever integrated. Neither can be applied without paying homage to the other. The best scientific evidence in the world is worthless if it's inadmissible in a court of law.

WHAT IS DIGITAL FORENSICS?

There are many ways to define digital forensics. In *Forensic Magazine*, Ken Zatyko defined digital forensics this way:

> "The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper

> search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation."
>
> **(Zatyko, 2007)**

Digital forensics encompasses much more than just laptop and desktop computers. Mobile devices, networks, and "cloud" systems are very much within the scope of the discipline. It also includes the analysis of images, videos, and audio (in both analog and digital format). The focus of this kind of analysis is generally authenticity, comparison, and enhancement.

USES OF DIGITAL FORENSICS

Digital forensics can be used in a variety of settings, including criminal investigations, civil litigation, intelligence, and administrative matters.

Criminal Investigations

When you mention digital forensics in the context of a criminal investigation, people tend to think first in terms of child pornography and identity theft. Although those investigations certainly focus on digital evidence, they are by no means the only two. In today's digital world, electronic evidence can be found in almost any criminal investigation conducted. Homicide, sexual assault, robbery, and burglary are just a few of the many examples of "analog" crimes that can leave digital evidence.

One of the major struggles in law enforcement is to change the paradigm of the police and get them to think of and seek out digital evidence. Everyday digital devices such as cell phones and gaming consoles can hold a treasure trove of evidence. Unfortunately, none of that evidence will ever see a courtroom if it's not first recognized and collected. As time moves on and our law enforcement agencies are replenished with "younger blood," this will become less and less of a problem.

BIND. TORTURE. KILL.

The case of Dennis Rader, better known as the BTK killer, is a great example of the critical role digital forensics can play in a criminal investigation. This case had national attention and, thanks to digital forensics, was solved thirty years later. To all that knew him before his arrest, Dennis Rader was a family man, church member, and dedicated public servant. What they didn't know was that he was also an accomplished serial killer. Dennis Rader, known as Bind, Torture, Kill (BTK), murdered ten people in Kansas from 1974 to 1991. Rader managed to avoid capture for over thirty years until technology betrayed him.

After years of silence, Rader sent a letter to the Wichita *Eagle* newspaper declaring that he was responsible for the 1986 killing of a young mother. The letter was received by the *Eagle* on March 19, 2004. After conferring with the FBI's Behavioral Analysis Unit, the police decided to attempt to communicate with BTK through the media.

In January 2005, Rader left a note for police, hidden in a cereal box, in the back of a pickup truck belonging to a Home Depot employee. In the note, he said:

> "Can I communicate with Floppy and not be traced to a computer. Be honest. Under Miscellaneous Section, 494, (Rex, it will be OK), run it for a few days in case I'm out of town-etc. I will try a floppy for a test run some time in the near future-February or March."

The police did the only thing they could. They lied. As directed, they responded (via an ad in the *Eagle*) on January 28. The ad read "Rex, it will be ok, Contact me PO Box 1st four ref.numbers at 67202."

On February 16, a manila envelope arrived at KSAS, the Fox affiliate in Wichita. Inside was a purple floppy disc from BTK. The disc contained a file named "Test A.rtf." (The .rtf extension stands for "Rich Text File"). A forensic exam of the file struck gold. The file's metadata (the data about the data) gave investigators the leads they had been waiting over thirty years for. Aside from the "Date Created" (Thursday, February 10, 2005 6:05:34 PM) and the "Date Modified" (Monday, February 14, 2005 2:47:44 PM) were the "Title" (Christ Lutheran Church) and "Last Saved By:" (Dennis).

Armed with this information, investigators quickly logged on to the Christ Lutheran Church web site. There they found that Dennis Rader was the president of the church's Congregation Council. The noose was tightening, but it wasn't tight enough. Investigators turned to DNA to make the case airtight. Detectives went on to obtain a DNA sample from Rader's daughter and compared it to DNA from BTK. The results proved that BTK was her father. On February 25, three days after the DNA sample arrived at the lab, Rader was arrested, sealing the fate of BTK. He is currently serving ten consecutive life sentences (Witchita *Eagle*).

Civil Litigation

The use of digital forensics in civil cases is big business. In 2011, the estimated total worth of the electronic discovery market is somewhere north of $780 million (Global EDD Group). As part of a process known as **Electronic Discovery (eDiscovery),** digital forensics has become a major component of much high dollar litigation. eDiscovery "refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case" (TechTarget, 2005).

In a civil case, both parties are generally entitled to examine the evidence that will be used against them prior to trial. This legal process is known as "discovery." Previously, discovery was largely a paper-based exercise, with each party exchanging reports, letters, and memos; however, the introduction of digital forensics and eDiscovery has greatly changed this practice.

The proliferation of the computer has rendered that practice nearly extinct. Today, parties no longer talk about filing cabinets, ledgers, and memos; they talk about hard drives, spreadsheets, and file types. Some paper-based materials may

come into play, but it's more the exception than the rule. Seeing the evidentiary landscape rapidly changing, the courts have begun to modify the rules of evidence. The rules of evidence, be they state or federal rules, govern how digital evidence can be admitted during civil litigation. The Federal Rules of Civil Procedure were changed in December 2006 to specifically address how electronically stored information is to be handled in these cases.

Digital evidence can quickly become the focal point of a case, no matter what kind of legal proceeding it's used in. The legal system and all its players are struggling to deal with this new reality.

Intelligence

Terrorists and foreign governments, the purview of our intelligence agencies, have also joined the digital age. Terrorists have been using information technology to communicate, recruit, and plan attacks. In Iraq and Afghanistan, our armed forces are exploiting intelligence collected from digital devices brought straight from the battlefield. This process is known as **DOMEX (Document and Media Exploitation)**. DOMEX is paying large dividends, providing actionable intelligence to support the soldiers on the ground (U.S. Army).

MOUSSAOUI

It's well documented that the 9-11 hijackers sought out and received flight training in order to facilitate the deadliest terrorist attack ever on U.S. soil. Digital forensics played a role in the investigation of this aspect of the attack.

On August 16, 2001, Zacarias Moussaoui was arrested by INS agents in Eagan, Minnesota, for overstaying his visa. Agents also seized a laptop and floppy disk. After obtaining a search warrant, the FBI searched these two items on September 11, 2001. During the analysis, they found evidence of a Hotmail account (pilotz123@hotmail.com) used by Moussaoui. He used this account to send e-mail to the flight school as well as other aviation organizations.

For those not familiar with Hotmail accounts, it's a free e-mail service offered by Microsoft, similar to Gmail and Yahoo!. They're quite easy to get and only require basic subscriber information. This information is essentially meaningless, because none of the information is verified. During the exam of Moussaoui's e-mail, agents were also able to analyze the Internet protocol connection logs. One of the IP addresses identified was assigned to "PC11" in a computer lab at the University of Oklahoma.

The investigation further showed that Moussaoui and the rest of the nineteen hijackers made extensive use of computers at a variety of Kinko's store locations in other cities. Agents arrived at the Kinko's in Eagan hoping to uncover evidence. They were disappointed to learn that this specific Kinko's makes a practice of erasing the drives on their rental computers every day. Now forty-four days after Moussaoui's visit, the agents felt the odds of recovering any evidence would be somewhere between slim and none. They didn't bother examining the Kinko's computer. The Eagan store isn't alone. Other locations make a routine practice

of erasing or reimaging the rental computers as well. This is done periodically, some as soon as twenty-four hours, others as long as thirty days. The drives are erased to improve the performance and reliability of the computers as well as to protect the privacy of its customers (Lawler, 2002).

Administrative Matters

Digital evidence can also be valuable for incidents other than litigation and matters of national security. Violations of policy and procedure often involve some type of electronically stored information, for example, an employee operating a personal side business, using company computers while on company time. That may not constitute a violation of the law, but it may warrant an investigation by the company.

THE SECURITIES AND EXCHANGE COMMISSION (SEC)

In 2008, while the economy was in the beginning of its historic downward spiral, the Securities and Exchange Commission (SEC) should have been policing Wall Street. Instead, many of them were spending hours of their days watching pornography. Computer forensics played heavily in this administrative investigation.

In August 2007, the SEC's Office of the Inspector General (OIG) officially opened an investigation into the potential misuse of governmental computers. The OIG was alerted to a potential problem after firewall logs identified several users that had received access denials for Internet pornography. The SEC firewall was configured to block and log this kind of traffic. The logs showed that this employee attempted to visit sites such as www.thefetishvault.com, www.bondagetemple.com, www.rape-cartoons.com, and www.pornobaron.com.

On September 5, 2007, the OIG notified the Regional Director that one of his employees was the focus of an investigation regarding the misuse of their government computer. On September 19 this same employee reported that her laptop hard drive suddenly crashed. She was issued a replacement drive and went back to work. A forensic analysis of her hard drive found 592 pornographic images (in her temporary Internet files) along with evidence that she had attempted to bypass the SEC's Internet filters.

The scope of this investigation eventually expanded considerably, identifying several more employees or contractors that were viewing pornography on their governmental computers while at work.

After further investigation, the OIG found that:

- A Regional Staff Accountant received over sixteen thousand access denials for pornographic web sites in a single month.
- A Senior Counsel for the Division of Enforcement accessed pornography from his SEC laptop computer on multiple occasions. His hard drive contained 775 pornographic images.
- A Senior Attorney at Headquarters downloaded so much pornography that he literally ran out of disk space.

The report went on to list the policies that prohibited these behaviors. It says in part:

> "SECR 24-4.3 TK IIIC, provides that '[m]isuse or inappropriate personal use of government office equipment includes the creation, download, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited etc' id at 3. The cover memorandum to SEC employees accompanying SECR 24-4.3 states that employees are prohibited from "accessing materials related to illegal or prohibited activities, including sexually explicit materials."

In the end, as this was not considered to be a crime, the entire matter was referred to the SEC administration for disposition (U.S. Securities and Exchange Commission).

LOCARD'S EXCHANGE PRINCIPLE

Locard's exchange principle says that in the physical world, when perpetrators enter or leave a crime scene, they will leave something behind and take something with them. Examples include DNA, latent prints, hair, and fibers (Saferstein, 2006).

The same holds true in digital forensics. Registry keys and log files can serve as the digital equivalent to hair and fiber (Carvey, 2005). Like DNA, our ability to detect and analyze these artifacts relies heavily on the technology available at the time. Look at the numerous cold cases that are being solved as a result of the significant advances in DNA science. Viewing a device or incident through the "lens" of Locard's principle can be very helpful in locating and interpreting not only physical but digital evidence as well.

SCIENTIFIC METHOD

As an emerging discipline in forensic science, digital forensics is undergoing some expected growing pains. As of today, digital forensics lacks the vast foundation and long-term track record set by forensic DNA. DNA is now considered by many to be the "gold standard" of the forensic sciences. Digital forensics simply lacks the years of development, testing, refining, and legal challenges DNA has undergone since its inception.

Plotting the course forward are several organizations that are looked on to establish the protocols, standards, and procedures that will push digital forensics ahead. The following sections provide more information on these important organizations.

ORGANIZATIONS OF NOTE

There are several organizations that make significant contributions to the discipline of digital forensics year in and year out. These organizations not only set standards and establish best practices, they provide leadership as well. Examiners

should be familiar with these entities, the roles they play, and the contributions they make. As professionals, it's our responsibility to participate in one or more of these organizations.

Scientific Working Group on Digital Evidence

http://www.swgde.org/

Standards and techniques are an essential part of valid and accurate forensic science. They are its foundation, its core. Along with other federal agencies, the FBI has supported the formation and efforts of a wide range of Scientific Working Groups (SWGs) and Technical Working Groups (TWGs) (Federal Bureau of Investigation). These collaborative groups draw their members from "forensic, industrial, commercial, academic and in some cases international communities" (Federal Bureau of Investigation). Some examples include the Scientific Working Group for DNA Analysis Methods (SWGDAM) and the Scientific Working Group for Firearms and Toolmarks (SWGGUN). Digital evidence has now joined the party with the formation of SWGDE.

Formed in 1998, the **Scientific Working Group on Digital Evidence (SWGDE)** is made up of "federal government agency, state or local law enforcement agency involved in the digital and multi-media forensic profession" (Scientific Working Group on Digital Evidence).

The mission of SWGDE is as follows: "Brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as ensuring quality and consistency within the forensic community" (Scientific Working Group on Digital Evidence).

American Academy of Forensic Sciences

http://www.aafs.org/

The **American Academy of Forensic Sciences (AAFS)** is considered the premier forensic organization in the world. Members of the Academy work for the National Institute of Standards and Technology (NIST) and National Academy of Sciences (NAS). The directors of most federal crime labs are members of AAFS. Members of AAFS are also active in the various Scientific Working Groups including SWGDE. The Academy plays a critical role in developing consensus standards of practice for the forensic community.

The Forensic Science Education Programs Accreditation Commission (FEPAC) was a creation of AAFS to ensure quality forensic science education and background for future forensic scientists.

The AAFS has approximately six thousand members and is divided into "eleven sections spanning the forensic enterprise." The Academy comprises "physicians, attorneys, dentists, toxicologists, physical anthropologists, document examiners, psychiatrists, physicists, engineers, criminalists, educators, digital evidence experts, and others" (American Academy of Forensic Sciences).

The Digital & Multimedia Sciences section represents digital forensics. As of November 3, 2010, the Digital Evidence section had 103 members. Despite the name, the reach of the AAFS is truly global, representing over sixty countries around the world (American Academy of Forensic Sciences).

American Society of Crime Laboratory Directors/Laboratory Accreditation Board

http://www.ascld-lab.org/index.htm

ASCLD/LAB (pronounced as-clad lab). The ASCLD is to forensic laboratories what Underwriters Labs is to household products. ASCLD/LAB is the "oldest and most well known crime/forensic laboratory accrediting body in the world." ASCLD/LAB accredited labs are the "gold standard" in the world of forensics. A lab becomes accredited only after successfully meeting all of the standards and requirements set forth in the ASCLD/LAB accreditation manual. These requirements and standards cover every aspect of a lab's operation and must be strictly followed. Adherence to these standards must be thoroughly and completely documented (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

National Institute of Standards and Technology (NIST)

http://www.nist.gov/itl/ssd/computerforensics.cfm

National Institute of Standards and Technology **(NIST)** was founded in 1901 and is a part of the U.S. Department of Commerce. It was the first federal physical science research laboratory. Some of NIST's areas of focus include bioscience and health, chemistry, physics, math, quality, and information technology (National Institute of Standards and Technology).

NIST is heavily involved in digital forensics. Some of the programs and projects include:

- National Initiative Cyber Security Education (NICE)—A national cyber-security education program teaching sound cyber practices that will improve the country's security.
- National Software References Library—A collection of known software file signatures that can be used by examiners to quickly exclude files that have no investigative value. This would include things like operating system files. This can really reduce the time spent on an examination.
- Computer Forensic Tool Testing—Intended to develop testing methodologies and standards for forensic hardware and software.

(National Institute of Standards and Technology)

American Society for Testing and Materials (ASTM)

http://www.astm.org/Standards/E2763.htm

Another major player in the development of standards is **ASTM**. ASTM is a global organization that has developed approximately twelve thousand standards that

are used to "improve product quality, enhance safety, facilitate market access and trade, and build consumer confidence." ASTM, founded in 1898, comprises about 30,000 members broken into 141 committees. The Forensics Sciences committee, known as E30, is further divided into several subcommittees. The Digital and Multimedia Evidence subcommittee is known as E30.12 (ASTM).

ROLE OF THE FORENSIC EXAMINER IN THE JUDICIAL SYSTEM

The digital forensics practitioner most often plays the role of an expert witness. What makes them different than nonexpert witnesses? Other witnesses can only testify to what they did or saw. They are generally limited to those areas and not permitted to render an opinion. Experts, by contrast, can and often do give their opinion. What makes someone an "expert?" In the legal sense, it's someone who can assist the judge or jury to understand and interpret evidence they may be unfamiliar with. To be considered an expert in a court of law, one doesn't have to possess an advanced academic degree. An expert simply must know more about a particular subject than the average lay person. Under the legal definition, a doctor, scientist, baker, or garbage collector could be qualified as an expert witness in a court of law. Individuals are qualified as experts by the court based on their training, experience, education, and so on (Saferstein, 2011).

What separates a qualified expert from a truly effective one? It is their ability to communicate with the judge and jury. They must be effective teachers. The vast majority of society lacks technical understanding to fully grasp this kind of testimony without at least some explanation. Digital forensic examiners must carry out their duties without bias. Lastly, a digital forensics examiner must go where the evidence takes them without any preconceived notions.

The CSI Effect

It seems that everyone either does or has watched one or more versions of the popular TV series *CSI*. These shows and others like it tend to convince jurors that some form of forensic science can solve any case. In other words, they now *expect* it. These unreasonable expectations can lead to incorrect verdicts. The jury could acquit a guilty defendant simply because no scientific evidence was presented, the presumption being that if the defendant was guilty, there would be some kind of scientific evidence to prove it (Saferstein, 2011).

SUMMARY

In this chapter we looked at what forensic science, particularly digital forensics, is and is not. Forensic sciences aren't the fast-paced crime-solving dramas that we watch on television, but a scientific method of collection, investigation and analysis used to solve some kind of legal problem. Digital forensics isn't limited to computers. It encompasses any kind of electronic device that can

store data. These devices include cell phones, tablets, and GPS units just to name a few.

Digital forensics is applicable well beyond criminal investigations. It's used routinely in civil litigation, national and military intelligence matters as well as the private sector.

There are multiple organizations that help establish the standards and best practices used in digital forensics. These organizations include the American Academy of Forensic Sciences, the Scientific Working Group on Digital Evidence, and ASTM.

As a practitioner, communication skills are extremely important. You will spend a significant amount of time explaining your findings to police officers, attorneys, and clients. Most important, you must be able to explain these things to judges and juries. All of these stakeholders must be able to understand your methods and findings. Like all scientific evidence, digital evidence can be quite confusing and overwhelming. With this kind of testimony, it's very easy to lose people. Losing a judge or jury in a trial can have disastrous consequences such as having your findings ignored or misunderstood.

References

American Academy of Forensic Sciences. (n.d.). *About AAFS*. Retrieved February 4, 2011, from: http://www.aafs.org/about-aafs

ASTM. (n.d.). *ABOUT: ASTM*. Retrieved February 23, 2011, from: http://www.astm.org/ABOUT/aboutASTM.html

ASTM. (n.d.). *E30*. Retrieved February 23, 2011, from: http://www.astm.org/COMMIT/SUBCOMMIT/E30.htm

ASTM. (n.d.). *Overview: ABOUT: ASTM*. Retrieved February 23, 2011, from: http://www.astm.org/ABOUT/overview.html

Carvey, H. (2005, January 27). *Locard's Exchange Principle in the Digital World: Windows Incident Response*. Retrieved February 23, 2011, from: http://windowsir.blogspot.com/2005/01/locards-exchange-principle-in-digital.html

Federal Bureau of Investigation. (n.d.). *Scientific Working Groups: Federal Bureau of Investigation*. Retrieved February 19, 2011, from: http://www.fbi.gov/about-us/lab/swgs

Lawler, B. A. (2002, September 4). *Government's Response to Court's Order on Computer and Email Evidence*. Retrieved September 13, 2011, from FindLaw.com: news.findlaw.com/hdocs/docs/moussaoui/usmouss90402grsp.pdf

McKendrick, J. (2010, May 12). *Size of the Data Universe: 1.2 Zettabytes and Growing Fast: ZDNet*. Retrieved February 23, 2011, from: http://www.zdnet.com/blog/service-oriented/size-of-the-data-universe-12-zettabytes-and-growing-fast/4750

Regional Computer Forensics Laboratory. (n.d.). *RCFL: Regional Computer Forensics Laboratory*. Retrieved February 4, 2011, from: http://www.rcfl.gov/

Saferstein, R. (2006). *Criminalistics: An Introduction to Forensic Science* (College Edition). Upper Saddle River, New Jersey: Prentice Hall.

Scientific Working Group on Digital Evidence. (n.d.). *Scientific Working Group on Digital Evidence—About Us*. Retrieved February 4, 2011, from: http://www.swgde.org

Stuart, J., Nordby, J. J., & Bell, S. (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques*. February 20, 2009 (3rd ed.). Boca Raton, FL: CRC Press.

U.S. Army. (n.d.). *Document and Media Exploitation (DOMEX): 2010 Army Posture Statement*. Retrieved February 23, 2011, from: https://secureweb2.hqda.pentagon.mil/vdas_armyposturestatement/2010/information_papers/Document_and_Media_Exploitation_%28DOMEX%29.asp

U.S. Department of Justice. (2009). *RCFL Annual Report for Fiscal Year 2009*. Washington, DC: U.S. Department of Justice.

Zatyko, K. (n.d.). *Commentary: Defining Digital Forensics*. Retrieved February 19, 2011, from: http://www.forensicmag.com/node/128