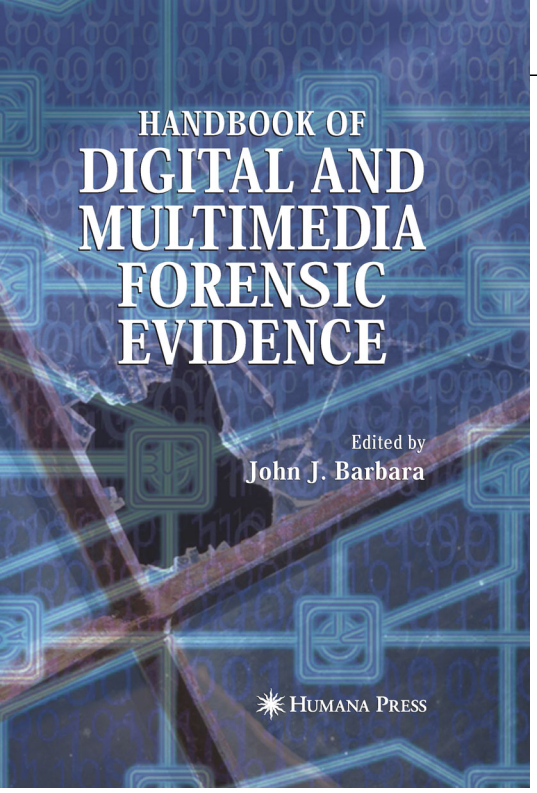
HANDBOOK OF
DIGITAL AND
MULTIMEDIA
FORENSIC
EVIDENCE
Edited by
John J. Barbara
HUMANA PRESS

Handbook of Digital and Multimedia Forensic Evidence

Handbook of Digital and Multimedia Forensic Evidence

Edited by

John J. Barbara

Humana Press Totowa, New Jersey

999 Riverview Drive, Suite 208
Totowa, New Jersey 07512

www.humanapress.com

This publication is printed on acid-free paper. ♾
ANSI Z39.48-1984 (American Standards Institute)

Permanence of Paper for Printed Library Materials

Cover design by Karen Schulz
Production Editor: Michele Seugling

For additional copies, pricing for bulk purchases, and/or information about other Humana titles, contact Humana at the above address or at any of the following numbers: Tel.: 973-256-1699; Fax: 973-256-8341; E-mail: orders@humanapr.com; or visit our Website: www.humanapress.com

Printed in the United States of America. 10 9 8 7 6 5 4 3 2 1

e-ISBN 978-1-60327-124-0

Library of Congress Control Number: 2007931072.

About the Editor

Mr. Barbara has worked in forensic crime laboratories for over 30 years and currently supervises the Digital Evidence Section (Computer Forensics) in a state crime laboratory in the United States. Mr. Barbara became an American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) Legacy Inspector in 1993 and an ASCLD/LAB ISO 17025 certified Technical Assessor in 2004. He has participated in over 25 laboratory inspections for ASCLD/LAB, serving as an Inspector, Site Leader, Team Captain, and Technical Assessor. He has inspected the disciplines of Controlled Substances, Toxicology, Firearms and Toolmarks, Trace Evidence, Questioned Documents, and Digital & Multimedia Evidence (Computer Forensics, Forensic Audio, Image Analysis, and Video Analysis). On three occasions, he has assisted ASCLD/LAB with the training of their Digital & Multimedia Evidence Inspectors and was appointed by the ASCLD/LAB Board as Chairperson of its Digital & Multimedia Evidence Proficiency Review Committee. He is a member of the Editorial Advisory Board of *Forensic Magazine* and author of a regular column in *Forensic Magazine* titled "The Digital Insider." He has presented numerous information programs and workshops and has authored many articles pertaining to Digital & Multimedia Evidence Accreditation.

To Ralph M. "Bud" Keaton for your years of dedicated, uncompromising efforts to improve the quality of forensic laboratory services provided to the criminal justice system. You were there at the "dawn" of forensic laboratory accreditation, long before many of us even understood what accreditation meant. Over the years, you have been, and continue to be, a constant force promoting the necessity for forensic laboratories to become accredited. You have ensured that the accreditation process is impartial, objective, and conducted under the highest standards of ethical practice. Under your guidance, the Digital & Multimedia Evidence discipline was added to the ASCLD/LAB accreditation programs. Forensic laboratories that achieve ASCLD/LAB Legacy or ASCLD/LAB-International accreditation in this discipline (and any of the others that are offered) can be considered as having attained accreditation from the premier forensic laboratory accreditation program in the world today. Job well done "Bud!"

Preface

In April 2005, I received a telephone call from Humana Press Senior Editor, Harvey Kane, inquiring whether there might be a need for a book to be published concerning the different aspects of computer forensics. During a subsequent meeting to discuss the current state of available texts covering this topic, I noted to Mr. Kane that there were several excellent computer forensics books already published and readily available. Mr. Kane then inquired as to what were some of the commonalities and differences between those books. My response was that they all discussed computer forensics analysis in detail. (Indeed, the purpose of one in particular was to guide the individual to becoming a skilled computer forensics examiner.) Furthermore, I indicated that some of the books included topics such as different operating systems as well as chapters on evidence collection and processing. Still others dealt specifically with incident response. Mr. Kane then asked me two questions: "If a person wanted to pursue a career in computer forensics, is there any one book currently available that provides an overview?" and if not, "If you were to write a book on computer forensics, what topics would you include in the book?" The meeting ended with Mr. Kane asking me to draft a scope document concerning a possible book on computer forensics.

Shortly thereafter, I attended a local Infragard meeting. The speaker's topic for the meeting was incident response and the role that computer forensics can play in identifying the evidence of a Denial of Service (DoS) attack. After the presentation, a number of those present asked the speaker such questions as: "What training is necessary to become an examiner in this field?" "How and where can you obtain such training?" "Where can you get the software to investigate this type of crime?" "Does an information technology (IT) person have to be certified?" "How do I go about obtaining certification?" "What certifications are available?" "What are the legal issues involved in searching and seizing digital data?" "What education is necessary to be hired in the IT field?" "What happens if you have to testify in court?"

Over the past several years, I have been asked many of those same questions by high school and college students and other individuals interested in entering the computer forensics field. One question in particular stands out: "How and where does a person look to obtain the necessary information if he or she is thinking of a career in this field?" All of these questions exemplify how difficult it is at times to obtain necessary information to make career choices.

As I began to develop an outline and scope document, I reflected back upon the field as a whole, trying to determine how we got to where we are now. In doing so,

I began to identify some issues that should potentially be addressed. All of us are aware that digital and multimedia data is found everywhere in our society. From the shoplifter who is captured on video tape to the victim of identity theft, digital and multimedia data is somehow involved in the analysis of the evidence. Over the past 10 years or so, considerable emphasis has been placed on the need to find, capture, store, examine, and preserve digital and multimedia data for investigative purposes. There are many practitioners who, on a daily basis, perform complex analyses to gather necessary information for subsequent courtroom litigation. The educational skills of these practitioners range from the self-taught to those with doctoral degrees in applicable fields of analysis. However, multifaceted analyses can at times become overwhelming, particularly regarding differentiation of the techniques involved. For instance, consider the following real-case scenario:

> Several digital cameras at a convenience store allegedly capture an armed robbery of the store by several suspects. A hard drive from the video surveillance system is submitted to a computer forensics examiner for analysis. The hard drive contains 24 hours of multiplexed video. The investigator believes that somewhere on the hard drive is the video of the armed robbery. Along with the hard drive, the investigator submits a compact disk (CD) containing digital images of several potential suspects. The examiner is requested to analyze the hard drive, find the video of the armed robbery, capture and enhance the video images of the robbery suspects, and compare those images to the ones provided on the CD. Furthermore, the examiner is also requested to decipher, if possible, what the suspects said during the armed robbery.

This scenario raises all sorts of questions: "What type of analysis will the examiner be performing?" "Do we know for sure if the examiner will be performing computer analysis, video analysis, audio analysis, imaging analysis, or all four?" "Does the examiner have sufficient training?" "What is the experience level of the examiner?" "Where did the examiner obtain the necessary tools?" "Have they been validated and/or verified?" "What type of standards and controls will be used during the analysis?" The scenario depicts the need for conformity or uniformity in defining, handling, and examining digital and multimedia evidence. Evidentiary items may include both analog and digital media and/or the information contained therein. For practicality purposes, digital and multimedia analysis can be grouped under one discipline, the Digital & Multimedia Evidence discipline. This discipline can be further broken down into at least four subdisciplines: Forensic Audio Analysis, Computer Forensics, Image Analysis, and Video Analysis.

Many national and international organizations, such as the Scientific Working Group on Digital Evidence (SWGDE), the International High Technology Crime Investigation Association (HTCIA), the Digital Forensic Research Workshop (DFRWS), the Institute of Computer Forensic Professionals (ICFP), and the International Organization on Computer Evidence (IOCE) exist to provide guidance and leadership to the practitioners of the discipline. Furthermore, journals such as the *International Journal of Digital Evidence*, the *International Journal of Digital Forensics & Incident Response*, and others provide a forum for the dissemination of technical information. Other print media, such as *Forensic Magazine*, contain articles that discuss relevant topics. Organizations such as the International Association of Computer Investigative Specialists (IACIS) offer certifications to examiners to help ensure reliable analytical results. Even with this wealth of available resources, there continues to be one constant need in this

emerging field that is not likely to change: an overview of the major elements of the discipline itself. Until now, there has been no one general source or reference that ties together such diverse topics as:

- The foundation of the discipline, analog and digital data
- How the Internet and Internet-related crime has affected our society
- The applicable laws on search and seizure
- What educational skills and training are needed to become an examiner
- Certification and accreditation
- Information security in the private and governmental sector
- How to investigate cybercrime
- How to collect evidence at a typical crime scene
- The types of digital and multimedia analysis performed
- Preparation for courtroom testimony.

This book, *Handbook of Digital and Multimedia Forensic Evidence*, was put together with the intent to be that reference. It can serve as a foundation and guide for (a) students considering a career in this field, (b) the law enforcement investigator assigned to work cybercrimes, (c) establishing training programs for forensic examiners, (d) the IT professional, (e) the veteran forensic examiner, and (f) the prosecutor faced with litigating cybercrime cases brought before a trier of fact. Because there is not any one person who is totally knowledgeable in all of these topics, a distinguished group of authors was selected to write individual chapters to address his or her specific areas of expertise. After reading this book and knowing that technology, techniques, and analyses change literally week to week, the reader will not become an "expert" in this field but rather will come away with a greater understanding of this multifaceted discipline.

John J. Barbara

Contents

Contributors

Rebecca Gurley Bace
Infidel, Inc.
Scotts Valley, California

Philip Craiger
National Center for Forensic Science
Department of Engineering Technology
University of Central Florida
Orlando, Florida

Philippe Dubord
Tampa, Florida

Erin E. Kenneally
University of California San Diego
San Diego Supercomputer Center
La Jolla, California

Larry R. Leibrock
Office of Deputy Secretary of Defense
Joint Improvised Explosive
Device Defeat Organization
Austin, Texas

Mark M. Pollitt
Digital Evidence Professional Services, Inc.
Ellicott City, Maryland

Donald Justin Price
Former Computer Forensic Examiner
for the Florida Department of Law Enforcement
Boyertown, Pennsylvania

Fred Chris Smith
Santa Fe, New Mexico

1

Chapter 1

The Analog and Digital World

Donald Justin Price

Summary

Digital devices shape every aspect of our lives—from online banking to ordering milk when your refrigerator detects you are low. These advances in technologies have been used to advance and improve our daily lives and, truly, the way in which we live. Unfortunately, these advances also have a dark side. Electronic devices are the new weapons of choice used by today's criminals. These activities range from sophisticated network intrusion to money laundering to exploiting children. Criminals attempt to hide behind digital zeros and ones in an effort to protect their identities while exploiting the identities of others. It is the responsibility of law enforcement and corporate America to understand digital devices and how to uncover a criminal's true identity through specialized training, sophisticated software, and a little bit of luck.

This chapter will introduce you to the world of digital information. It will briefly describe the basic fundamentals of digital and analog devices. It is not the intent of this chapter to cover every aspect of digital devices but rather to present a solid foundation of understanding for further detailed study of the subject matter. Let us start from the beginning; understanding the impact of mathematics.

Key Words: Bitmap, Bits, Bytes, MD-5, Partition, Sectors.

1. The Binary World

Digital information is represented by two states; "0" or "1." This representation of two states is referred to as *binary*. Let us take a quick look at how binary digits are computed and how they are used to represent human-recognizable characters, numbers, and symbols. Each binary digit, "0" or "1," is called a *bit*. A bit is the smallest unit processed by digital devices. In order to represent more than two possibilities, digital information is combined into 8 bits, termed a *byte*. Each of the 8 bits has a specific

From: *Handbook of Digital and Multimedia Forensic Evidence*
Edited by: J. J. Barbara © Humana Press Inc., Totowa, NJ

Bit Position:	8^{th}	7^{th}	6^{th}	5^{th}	4^{th}	3^{rd}	2^{nd}	1^{st}
Value:	128	64	32	16	8	4	2	1

Fig. 1. Value placement within a byte.

value associated with its position. The value assigned to each bit increases from right to left, by a multiple of two (Fig. 1).

There are a total of 2^8, or 256, possible combinations within a byte. The American Standard Code for Information Interchange (ASCII) is a coding-based system that is used to represent characters, numbers, and various symbols. Each ACSII value has an assigned byte combination, totaling 256 possible characters, numbers, and symbols. When referencing an ASCII conversion chart, it is helpful to convert the binary digits into a decimal (base 10) or hexadecimal (base 16) value. How is this conversion accomplished?

Presume that we want to convert the following byte, "01010110," into a decimal value. Each bit has a specific value associated with its position. As you move from right to left, the bit's value becomes more significant. If the binary value is a "1," then the value assigned to that placeholder is added. If the binary value is a "0," then nothing is added. Now that we have all of the values assigned to each bit, all we have to do is add them together and get a decimal value of 86 (Fig. 2). Referencing an ACSII conversion chart, we note that the decimal value of 86 represents the capital letter "V."

Now let us look at converting the same byte into a hexadecimal value. When converting binary to hexadecimal, you first have to break the byte into two 4-bit segments. This 4-bit segment is called a *nibble*. Each bit within the nibble has a specific assigned value, just like the decimal conversion. Combining the values of each nibble yields the hexadecimal conversion (Fig. 3). Referencing an ASCII table, the hexadecimal value of 56 represents the capital letter "V," just as we expected from the previous example. In a hexadecimal system (base 16), the possible values are from 0 to 9 and A through F, "A" being equal to 10, "B" being equal to 11, and continuing until "F" equals 16. So why do we use hexadecimal to represent digital information? We do so simply because it takes less space to represent a single character, number, or symbol. Each hexadecimal value represents four binary values.

Byte:	0	1	0	1	0	1	1	0
Bit Value:	128	64	32	16	8	4	2	1
Conversion:	0	64	0	16	0	4	2	0
Decimal Value (86):		+64		+16		+4	+2	

Fig. 2. Converting a byte to a decimal value.

Byte:	0	1	0	1	0	1	1	0
Bit Value:	8	4	2	1	8	4	2	1
Conversion:	0	4	0	1	0	4	2	0
		+4		+1		+4	+2	
Hexadecimal Value:			5				6	

Fig. 3. Converting a byte to a hexadecimal value.

2. Digital Recording

Now that we have a very general understanding of the binary world, let us explore how this information is stored on magnetic devices, such as hard drives, floppy diskettes, tapes, and so forth. Magnetic storage is based on the physics of magnetism. The magnetic storage device determines the magnetic property of each particle on a medium. The particle is either positively or negatively charged. As defined above, this is a true binary system. For example, a hard drive consists of platters, actuator arms, and read/write heads. The platters are normally made of aluminum or glass, which cannot flex. These platters contain a magnetic coating, which is used for data storage. Three popular types of magnetic coatings are oxide media, thin-film media, and antiferromagnetically coupled (AFC) media *(1)*. As the read/write head(s) of the hard drive move over each magnetic particle, the polarization of the particle will generate a pulse. Based on the particle's magnetic orientation between the read/write head, the particle will generate a positive or negative pulse. This is a very simple and basic description of how magnetic particles are converted into binary "0" and "1."

Binary information is stored on magnetic devices in areas called *sectors*. A sector is the smallest physical unit that can be used to store digital information. Each sector contains 512 bytes of storage space. The physical size of a sector is slightly larger, however; addressing information and error checking consumes a portion of the storage space. Sectors are organized in centric circles called *tracks*. The density of the media determines how many sectors per track the media contains. For example, a floppy diskette may have between 8 and 36 sectors per track; a higher density hard drive may have 900 or more sectors per track *(2)*. There are two recording processes possible when the sectors and tracks are created during the formatting process. These recording types are referred to as *standard* and *zone* recording. The standard recording process creates the same number of sectors per track across the entire magnetic device. This creates a major loss of data storage and an overall decrease in efficiency. In other words, you would have the same number of sectors per track on the innermost circles as you would on the outermost circles. This inefficiency led to the development of zone recording. When zone recording is used, there is an increased number of sectors per track within each track as you move out from the center of the medium.

Each storage unit on a magnetic device must have an address so that the hard drive knows where to find the data being requested. As magnetic devices have become more advanced and larger capacities are demanded, the number of addressable sectors

has clearly approached its limit. Each storage unit is identified by using a set number of bits. The number of bits used in the address scheme is determined by how the medium is formatted. The formatting process prepares the medium for data storage and is accomplished within three steps: low-level format, partitioning, and high-level format. The low-level formatting process physically creates the tracks and divides them into sectors. Each sector is given its location address, and the data area is filled with test values *(3)*. The partitioning phase creates partitions on the medium. This allows multiple filing systems and/or operating systems to coexist. The last and final stage is the high-level format, which creates the infrastructure needed to properly manage the files that will be stored on the drive. This entire process is analogous to a new housing development. Several acres of land are parceled, streets are created, and appropriately sized lots for new homes are established. If needed, several subdivisions are created, one being for upscale homes, one for townhomes, one for single-family dwellings, and so forth. Finally, the homes are constructed in order to manage all of the families that live within the same community. Let us look at an example of how the formatting process affects data storage. A FAT16 formatted system uses a 16-bit value to address each storage unit. Therefore, there are a total of 65,536 addressable storage units. This limitation dictates that the largest maximum volume size cannot exceed 2 gigabytes. On the other hand, a FAT32 formatted system uses 32 bits for addressing storage units. Therefore, a total maximum volume size of 4 terabytes is theoretically possible *(4)*. A cluster, or allocation unit, is a group of one or more sectors on a disk. This represents the smallest logical unit in which data can be stored. Figure 4 illustrates an example of standard recording. In this formatting scheme, each cluster is made up of four sectors. Therefore, the smallest allocation unit assigned to any file is 2048 bytes.

In the binary world, all types of files are stored magnetically in this fashion: programming codes, Microsoft Word documents, sound files, and video files.. It is the function of the operating system and program(s) to interrupt the ones and zeros as they are being generated by the read/write heads of the hard disk. Let us look at an example of a bitmap graphics file. In a bitmap graphics file, each byte represents specific intensities of the three primary colors, red, green, and blue (RGB). Therefore,

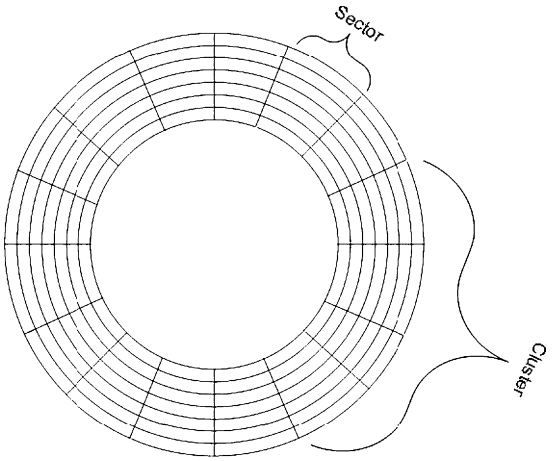

Fig. 4. Example of a cluster.

each RGB value contains 3 bytes, each byte representing an intensity of color *(5)*. Previously discussed was the concept of a byte; it consists of 8 bits. Each of the bits has a predetermined value associated with its location. The bit farthest to the left is called the *most significant bit*, because it has a value of 128. In contrast, the bit farthest to the right is the *least significant bit*, because its predetermined value is 1.

When a bitmap image is called by a program, the program will interpret each byte being generated by the hard drive's read/write heads. The programming code will know to read each byte and display the appropriate intensity of RGB and therefore produce an image that represents the collection of millions of these bytes. Figure 5 shows examples of the binary representation of three different common colors.

The technology of *steganography* takes advantage of this fact when concealing files within files. If a bitmap graphics file is used to conceal another file, the steganography program will replace the least significant bit within each byte. The file size of the original bitmap does not change, and the degradation of the image is undetectable by the human eye.

Another area within magnetic recording deals with random versus linear recording. Hard drives, floppy diskettes, and zip diskettes benefit from random recording. This gives the read/write heads of the device control of where to store the data. The system tries to be as efficient as possible and tends to store files in the closest available spaces to the read/write heads. The other option is to store the files sequentially, assuming the space is available. This type of operation is known as random recording, being able to "jump" around the disk to store digital information. A magnetic tape is a good example of a device that uses linear recording. This process has a greater "overhead" when trying to read and write digital information. If the user requests data that is stored at the end of the tape, the device must forward the tape to the proper location, wasting valuable time.

Optical media differ from magnetic media in that optical media use the principles of light to read and write data as opposed to magnetism. Examples of common optical media would be compact disks (CDs) and digital versatile disks (DVDs). The type of polymer being used will dictate if a disk is writable and/or rewritable. When the recording phase of optical media is initiated, a laser light is used to scribe pits into the polymer material. As the laser light transverses the disk, the reflection of the laser light is calculated and converted into electrical pulses, which are interpreted as binary zeros and ones (Fig. 6). Just like in magnetic devices, density plays a critical role in determining how much data can be stored on any given disk. A DVD has a much higher density than a CD; therefore, it can store almost seven times the amount of data.

Binary Code:	**RGB Value:**	**Displayed Color:**
000000000000000000000000	0,0,0	Black
000000001111111100000000	0,255,0	Green
100000001000000010000000	128,128,128	Gray

Fig. 5. Examples of three common colors and their respective binary representation.

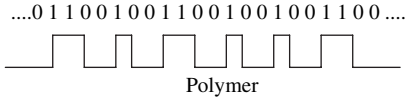

Fig. 6. Profile view of the "lands" and "pits" as observed on optical media.

3. Analog Recording

Analog information is continuous; the transmitted signal is analogous to the original signal *(6)*. A sound wave is an example of an analog system. The intensity of the sound is directly proportional to the sound wave. Converting or recording analog information to its digital counterpart is called *digitizing*. In the conversion process, the analog sound waves are broken up into many pieces and converted into numbers and stored digitally (Fig. 7). The quality of the conversion process is directly affected by the rate of sampling. Naturally, a higher sampling frequency will generate a higher quality digital audio conversion. Each specific number generated from the recording phase is proportional to the voltage level during playback. Just like the RGB values of graphics files, the *bit value* plays an important role in audio files.

4. Image Analysis

Digital photography has been well accepted and embraced. The advances of digital cameras and their corresponding technology has become so mainstream that professional-grade cameras are within the price range of average consumers. With the proliferation of digital cameras in society, criminals have taken advantage of this technology. This has forced law enforcement to develop and refine techniques of image analysis. There is a definite need for comparing, enlarging, repairing, enhancing, and analyzing graphics files. With the advances of modern technology, we are able to accomplish each of these tasks with great precision and accuracy. Gone are the days of using magnifying glasses and destructive chemicals and processes to analyze

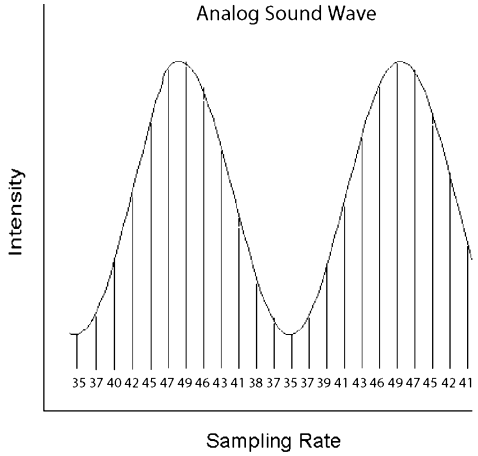

Fig. 7. Digitizing an audio sample.

```
000a0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20 
000b0 20 20 20 20 20 20 20 20-20 20 20 20 20 00 53 4f              ·SO
000c0 4e 59 00 4d 56 43 2d 43-44 33 35 30 00 48 00 00 NY·MVC-CD350·H··
000d0 00 01 00 00 00 48 00 00-00 01 00 00 00 41 43 44 ·····H·······ACD
000e0 20 53 79 73 74 65 6d 73-20 44 69 67 69 74 61 6c  Systems Digital
000f0 20 49 6d 61 67 69 6e 67-00 32 30 30 34 3a 30 38  Imaging·2004:08
00100 3a 32 38 20 31 37 3a 35-33 3a 30 36 00 1c 00 9a :28 17:53:06····
00110 82 05 00 01 00 00 00 57-02 00 00 9d 82 05 00 01 ·······W········
00120 00 00 00 5f 02 00 00 22-88 03 00 01 00 00 00 02 ···_···"········
00130 00 00 00 27 88 03 00 01-00 00 00 a0 00 00 00 00 ···'·····••••••••
00140 90 07 00 04 00 00 00 30-32 32 30 03 90 02 00 14 ·······0220·····
```

Fig. 8. Example of image header information.

images. Through research and software and technical developments, we are able to analyze these images and uncover their hidden past or true identity. A simple example of image analysis would be to determine the manufacturer and model number of a digital camera that captured a questioned photograph. Using a hex editor program, the image file's hexadecimal values can be examined. The beginning part of a file is called the *header information*. Various types of information can be contained within this area. Information such as file type (i.e., Microsoft Word document, JPEG, BMP, etc.), digital camera information, or program information could be extracted from the header information. Figure 8 shows an example of the header information within a digital photograph taken with a Sony Mavica CD-350 digital camera.

Of course, this is an extremely simple example of image analysis. More complex issues involved with image analysis include, among others, image enhancement, image authentication, comparison, and stereography detection. Major strides have been made to perfect this critical need within digital evidence. Sophisticated tools are capable of bit manipulation within the binary data in order to interpolate and enhance resolution of imagery.

Mathematical algorithms can be used to authenticate or compare images. MD-5 (Message Digest) is a standard algorithm used in digital evidence and could be used for comparing digital images. The MD-5 algorithm is a polynomial in which binary information is introduced that in turn generates a unique alphanumeric sequence. This MD-5 value can be accepted as a digital fingerprint of the data that was processed. The odds of any two files generating the same MD-5 hash value are roughly 1 in 3.4×10^{38}. Therefore, if two digital photographs need to be authenticated as being exact duplicates of each other, the file's binary information could be inserted into the MD-5 hash algorithm. If the alphanumeric values match, then you have reasonable certainty that the two digital photographs are identical. Keep in mind that this procedure could be used for any file type, not just digital photographs.

5. Effects of Digital Information in Society

As mentioned in the beginning of this chapter, digital information shapes every aspect of our lives. It seems we have become more reliant on digital information than on crude oil. National defense, utility infrastructure, business, and entertainment rely on digital information. In fact, most of these would not exist in their current forms without

it. So what does this mean for you and me? As we become more dependent on digital information, it becomes even more important for us to understand the technology and defend it against individuals who choose to exploit and misuse the technology. Computers, smart phones, PDAs, and such are becoming smaller and more advanced yet, at the same time, increasing their capacity to store information. The discipline of digital evidence must constantly adapt and change with technological developments in order to be an effective front against digital crime. Digital technology is changing in four main areas: physical size, storage capacity, processing power, and data security. Let us take a look at each area and how it affects law enforcement and society.

5.1. Physical Size

From the Motorola razors to ultrathin laptops to the iPod nano, digital information can be stored anywhere. Individuals can be carrying gigabytes of digital information in their pockets, around their necks, or even in their watches. This should cause great concern for law enforcement and society itself. Criminals are now able to store their incriminating evidence on these (and other) small devices. Officers need to be properly trained to recognize that virtually any digital device can be/is capable of storing digital evidence. To avoid being arrested and prosecuted for a crime, one of a criminal's best defenses is the concealment of evidence. If the incriminating digital evidence is never found, charges could not be filed. One simple example of this could be an individual suspected of Internet fraud. The user's Internet activity would be crucial to their prosecution. If the suspect was using a U3 enabled thumb drive, all of the user's Internet activity would reside in the thumb drive, not on the computer itself. If the seizing agent never noticed the thumb drive, critical evidence could be lost forever. Training and experience is a critical piece to the puzzle. Any sworn law enforcement officer who executes search warrants should have a basic understanding of this technology and be able to recognize such critical pieces of evidence. As technology advances, digital storage devices will take on an array of shapes and sizes. Ink pens are no longer just ink pens and watches are no longer just watches. They should be thought of and treated as potential pieces of evidence.

5.2. Storage Capacity

The technology used to store digital information is also constantly changing. The industry demands not only smaller devices as mentioned above but also large storage capacities. Consumers want to be able to store entire music collections and family video footage without a concern for free space. With the advent and proliferation of digital cameras and digital video cameras, having a storage capacity of 500 gigabytes to 1000 gigabytes is not uncommon for the consumer. As technology of perpendicular recording becomes more prevalent, storage capacities are going to be increasing exponentially. This will place a certain burden on law enforcement. Digital evidence examiners will be required to make well-informed decisions when determining what information to capture, how to capture the information, and ultimately how to process the enormous amount of data. The art and science of digital forensics relies on the ability of the examiner to find the "needle in the haystack." However, as the needle gets smaller in size, the haystack is getting bigger.

5.3. Processing Power

Processing power is the only area that benefits the criminal as well as law enforcement. Being able to process more data per second will not only lower the total processing time but also will allow the examiner to find the data more efficiently. However, this becomes less effective as storage capacity continues to expand. In an ideal world, a computer's processing power would be directly proportional to its storage capacity. As we all know, our world is far from perfect.

5.4. Data Security

Password protection and encryption are examples of data security. Society must be mindful of personal information being stored on digital devices. Any digital information that could be exploited must be protected. Password protection and encryption only allow authorized users to access the protected information. Cryptography is the process of concealing the contents of a file from all except for authorized users. As cryptographers create more secure algorithms used in data encryption, others will be testing their vulnerabilities and exploiting any weakness. Encryption schemes and strong passwords are very effective ways of ensuring data security. This fact alone should impose great concern to law enforcement when processing digital evidence. It requires examiners to think "outside-the-box" when dealing with cases known to involve encryption. Basic encryption schemes need to be understood by examiners. This understanding will allow them to make sound decisions when seizing digital evidence. During the execution of a search warrant, just walking into a residence or business and "pulling-the-plug" on a computer is no longer a viable option. Seizing agents must be more mindful of encryption programs and must understand how to best deal with the technology in an already highly stressful situation. If left unchecked, valuable data could be lost forever. Remember, the main purpose of encryption is to conceal or secure data from unauthorized access. If the suspect is using encryption, you can bet that the critical data is secured. However, as encryption schemes become more secure, so does the technology used to circumvent the process. Code-breaking software is an indispensable tool to digital evidence examiners. A weak password or pass phrase coupled with the strongest encryption scheme is meaningless. "The chain is only as strong as its weakest link" is an effective principle to apply when using passwords. Code-breaking tools use this fact to exploit the entire process in order to recover the password and, ultimately, to read the decrypted file.

Encryption is a two-edged sword. Cryptographers are constantly striving to develop the world's perfect encryption algorithm. If such an algorithm exists or is even possible, the direct effect on our society could be detrimental. A "would-be" terrorist could use this "perfect" encryption algorithm to conceal their radical views and plans to commit terrorist acts against any person or country. For this reason, the computer industry, law enforcement, and intelligence agencies should strive to work together in an effort to improve software products and digital devices without tying the hands of law enforcement.

6. Conclusion

Law enforcement and society will always play a cat and mouse game when it comes to developing technology. As new digital devices are invented, their inherent weaknesses are determined and exploited. As a result, the developers start the building process all over again, which ultimately leads to a better and stronger product.

References

[1]Mueller, S. (2002). *Upgrading and Repairing PCs*, 14th ed. Indianapolis: Que, p. 610.
[2]Ibid., p. 601.
[3]Ibid., pp. 604–608.
[4]Ibid., p. 607.
[5]Lewis, J., and Loftus W. (2005). *JAVA Software Solutions*, 4th ed.. New York: Pearson Education, Inc., p. 95.
[6]Newton, H. (2003). *Newton's Telecom Dictionary*, 19th ed. San Francisco: CMP Books, p. 61.

2

Chapter 2

Training and Education in Digital Evidence

Philip Craiger

Summary

Digital forensics is a relatively new science that is becoming increasingly important as tech-savvy criminals use computers and networks in their illegal activities. Demonstrated competency in digital forensics requires a varied knowledge and skill set that includes an in-depth understanding of computer hardware and software, computer networks, forensic science, applicable local, state, and national laws, as well as the ability to communicate in both verbal and written forms. The purpose of this chapter is to provide the reader with an overview of education and training in digital forensics. Issues specifically addressed include differences between education and training; the "core competencies" of the digital forensics examiner; guidelines on the knowledge and skills students should expect to learn in a college/university educational program; a description of various types of training programs; as well as pointers to Web resources for current information on available educational and training programs.

Key Words: Core competencies, Digital forensics, Examination plan, Hashing, IACIS, NW3C, Operating systems, SWGDE, TWGED.

1. INTRODUCTION

Law enforcement and business and industry increasingly encounter crimes that involve *digital evidence*. In 2000, the Scientific Working Group on Digital Evidence (SWGDE) defined digital evidence as "…any information of probative value that is stored or transmitted in a binary form" *(1)*. The new science of *digital forensics* is the application of science and technology to the identification, recovery, transportation, and storage of digital evidence. Digital forensics is a relatively new forensic science compared

From: *Handbook of Digital and Multimedia Forensic Evidence*
Edited by: J. J. Barbara © Humana Press Inc., Totowa, NJ

with biological (e.g., DNA) and physical-based (e.g., Gun Shut Residue (GSR), explosions, fingerprints, tool marks) forensics. Due to the ubiquity of digital media and its use in criminal activities, law enforcement, business, and industry, the forensic science community has become increasingly aware of the importance of digital forensics and the fact that it must be addressed as a profession and a science given its importance in many court cases. Accordingly, it is crucial that those involved in the recovery, examination, and preservation of digital evidence have the requisite training and education to deal effectively with the growing amount of evidence they will encounter.

The reader is presented with two caveats concerning this chapter. First, technology changes quickly—technologies become obsolete, and new technologies are created on an almost daily basis. These changes have a significant effect upon the practice of digital forensics, making it a "moving" target that requires practitioners to update their knowledge and skills to remain current of these changes. The second caveat concerns existing educational and training programs. Discussions of specific educational and training programs in this chapter are intentionally limited as they change on a regular basis. Discussions of specific vendor-supplied training and university programs would make this chapter essentially obsolete or incomplete by the time of publication. Consequently, in this chapter the focus is upon the fundamentals of digital forensics (i.e., principles, procedures, knowledge, and skills that are likely to be important for the foreseeable future). The reader can then use this information to compare and contrast university educational programs and training programs to determine the extent to which these programs meet these criteria. Discussed are a limited number of training programs that have been in existence for some time and most likely should continue to be in existence for years to come. Included at the end of this chapter are links to Web-based resources that are updated on a regular basis and that the readers can use to identify programs of interest.

2. Training Versus Education

People often confuse the terms *training* and *education*. Although definitions of the two often appear to be similar (compare Merriam-Webster's online dictionary for the definitions of *educate* and *train*), for the purposes of this chapter they are treated as generally distinct concepts that are not interchangeable but rather complementary. The primary distinction for this chapter is that (good) educational programs, offered at colleges and universities, provide knowledge and skills as a means of *developing a student's general problem-solving skills*. Thus, educational programs focus on instilling *fundamental knowledge and skills* revolving around a particular subject. There are also distinctions between undergraduate and graduate university programs. Students in an undergraduate program are exposed to a breadth of topics and experiences, whereas graduate programs (master's and doctoral programs) are more focused in scope and require a greater level of mastery of subject matter. Graduate programs usually involve a research component where the student must demonstrate their mastery of a subject or a particular problem through the creation of new knowledge about a subject.

Students in computer-related university degree programs may use software tools to demonstrate their understanding of the subject matter; however, students are expected to be able to demonstrate this understanding using other tools that were not discussed during the course and to apply the knowledge and skills required to problems that the

student might not have encountered during the course. Because of the diversity and depth of technology-related problems, students often participate in internships, during or after their degree, to expand their knowledge and skill sets.

Training programs, in contrast, are typically focused on procedural knowledge (i.e., how to complete a task in step-by-step fashion). Whereas educational programs are broader in focus, a typical training program focuses on a targeted set of knowledge and skills and is usually of short duration (a few days to a few weeks). Technology-related training programs also tend to have a heavy hands-on component, where students work directly with software tools to develop a level of competency with the tools.

3. The Digital Forensics Examiner

There are a number of positions (jobs) in which someone with a background (experience and/or education) in digital forensics may be competent to serve. The most common position that is relevant for this chapter is the position of a *digital forensics examiner*. FBI Special Agent Mark Pollitt (retired), former director of the FBI's Computer Analysis Response Team and manager of the FBI's Regional Computer Forensics Labs, defined a digital forensic examiner as

> …[someone who] forensically acquires, preserves, examines and presents information stored or transmitted in binary form which may be probative in a legal context. They may (or may not) conduct investigative analysis *(2)*.

Although the actual title of *digital forensics examiner* is more likely to be found in law enforcement, parties in industry perform these same tasks under varying names, as well as consultants who freelance on case-by-base basis.

The job of digital forensics examiners requires a varied knowledge and skill set. A competent examiner must be able to exhibit a technical understanding of various types of computer hardware, computer networks, operating systems, file systems, and various types of application software; an understanding of local, state, and federal laws that may come into play during the computer-related crime investigation; the ability to write a detailed report of the procedures used and the findings of the examination in both a technical and nontechnical manner; and finally to be able to accurately testify to the findings in a court of law to a jury of laypersons. Very few existing college/university programs (as of mid-2007) offer a comprehensive package of courses that encompasses this varied knowledge and skill set.

As mentioned previously, at the end of this chapter there are Web references where the reader may find specific information about educational programs that offer a degree or courses in digital forensics. Rather than including a list of educational programs in this chapter, which would become out-of-date within a short period of time, the knowledge, skills, and abilities (KSAs) that an examiner must exhibit in order to be assessed as competent or proficient are presented for review. It is suggested that readers interested in participating in an educational degree program use this list as a guideline for comparison with educational offerings to determine the appropriateness of the degree or courses to fit the need of the individual.