As each academic year ends in May, many students look forward to a summer break from school, but the work of the editors at the Stevenson University Forensics Journal is just beginning. For those readers wondering how our selection and editing process works, what follows is a glimpse into the creation and design of the Stevenson University Forensics Journal which is published by the School of Graduate and Professional Studies (GPS).

In the three GPS master’s degree programs in Cyber Forensics, Forensic Science, and Forensic Studies, writing well is emphasized, underscoring the importance that professionals in forensically related fields must be able to communicate clearly in written form. Although the majority of the articles come from students in the Forensic Studies program, in many years we are fortunate to have contributions from Forensic Science and Cyber Forensics students as well. This year, we have a piece from a Forensic Science student titled, "Correlation Between Occupational Stress, Burnout, and Job Satisfaction in Forensic Scientists."

The entire submission, editing and revision process runs on a rolling basis throughout the calendar year. During any course, when a student submits written work that is particularly well done, the Professor will encourage the student author to submit the piece to the Forensic Journal for publication consideration. Should the student wish to pursue publication, a strict set of submission requirements must be followed. The requirements ensure that all work is presented in the same format and requires as little editing as possible. For example, all papers must be written and properly cited in MLA format, have required margins and font and must be free of errors in structure, syntax and grammar. For some authors, this means reviewing and revising multiple times prior to submission. When the student author has finalized the piece, it is reviewed by the Editorial Board.

Once submitted, articles are sent to the Editorial Board for consideration. The Editorial Board selects those articles for publication that are timely, interesting to a wide variety of readers and well written. Each accepted article is reviewed by an editor for grammar, syntax, citation accuracy and formatting. The goal is to keep the substance of the piece intact, while ensuring accuracy and editing to improve the overall "readability" of a piece. Any recommended changes are provided to a second editor, who reviews and either accepts or rejects those changes. After final decisions regarding the edits have been made, the articles and all citations are reviewed again by an editor as well as the author prior to publication.

Although the process continues throughout the year, the Journal editors are busiest in the late winter and early spring. Publication typically occurs in April and final revisions, cover design and layout occur between January and March. Each year there are a few articles that do not make the final publication deadline and these articles are held until the following publication year.

I hope readers enjoy this issue of the Stevenson University Forensics Journal with a new appreciation for the effort that each author and editor puts into every article.

Carolyn Hess Johnson, Esquire
Editor and Publisher
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>PAGE</th>
<th>TITLE</th>
<th>AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>CAROLYN JOHNSON</td>
</tr>
<tr>
<td>4</td>
<td>ANTI-FORENSICS</td>
<td>ADELINE HEUCHAN</td>
</tr>
<tr>
<td>14</td>
<td>AUTHENTICATING ART</td>
<td>ALISIA ALEXANDER</td>
</tr>
<tr>
<td>22</td>
<td>FORENSIC ACCOUNTING: THE TERRORISM EXPLOSION</td>
<td>AMBER SEIBEL</td>
</tr>
<tr>
<td>30</td>
<td>MOBILE FORENSICS: CURRENT ISSUES WITH THIRD-PARTY APPLICATIONS ON MOBILE DEVICES AND MOBILE DEVICE ENCRYPTION</td>
<td>BRANDON LEE</td>
</tr>
<tr>
<td>39</td>
<td>THE ADDICTION FACTOR IN WHITE COLLAR CRIME: NEW PERSPECTIVES ON PREVENTION AND PUNISHMENT</td>
<td>C. MORGAN LITTLE</td>
</tr>
<tr>
<td>47</td>
<td>CORRELATION BETWEEN OCCUPATIONAL STRESS, BURNOUT, AND JOB SATISFACTION IN FORENSIC SCIENTISTS</td>
<td>ELIZABETH ELLIOTT</td>
</tr>
<tr>
<td>58</td>
<td>THE VALUE AND POTENTIAL OF FORENSIC MODELS</td>
<td>JACQUELYN A. D. JONES</td>
</tr>
<tr>
<td>66</td>
<td>NON-FINANCIAL MEASURES: A VIABLE AND EFFECTIVE WAY OF DETECTING FRAUD IN ACCOUNTING RECORDS</td>
<td>KEVIN MCKELVE</td>
</tr>
<tr>
<td>74</td>
<td>DIGITAL ROADS LESS TRAVELED IN CRIMINAL INVESTIGATIONS: NEW SOURCES OF DIGITAL EVIDENCE</td>
<td>MORGAN RONE</td>
</tr>
<tr>
<td>83</td>
<td>WALTER PAVLO RESEARCH PAPER</td>
<td>SHAUN MADARY</td>
</tr>
<tr>
<td>86</td>
<td>DISASTER RESPONSE</td>
<td>JOYCE WILLIAMS, DNP, FAAN</td>
</tr>
</tbody>
</table>
Anti-Forensics
Adeline Heuchan

INTRODUCTION

In 1984, government organizations, such as the FBI, DOD, IRS, and various other law enforcement agencies, started to develop programs with the intent to examine evidence of criminal activity on any computer system. At first, law enforcement officials from various government and law enforcement agencies volunteered their time to learn and execute these investigations. The goal was to find evidence or stored information on mainframe computers to assist case investigators. In the late 1980s, after the introduction of the IBM PC, there was a boom of computer hobbyists. The personnel of various law enforcement agencies also became avid computer hobbyists; many of these professionals later became instrumental in the creation of multiple forensic organizations, including the International Association of Computer Investigative Specialists (IACIS). The FBI hosted the first International Conference on Computer Evidence in 1993 at the FBI Academy in Quantico Virginia (Chow 5-9).

Over the next decade, computer forensics would expand with the ever more increasing, intricate, and mobile technology. The introduction of cell phones and the Internet to households opened doors for criminal activities to expand. With this expansion have come newer methods of hiding and even attempting to remove incriminating data within digital media. There are many tools and techniques that can be used by criminals to try to hide, alter, or even remove incriminating data on their systems; and in some cases, the tools and techniques truly do their job, making it extremely difficult for a digital forensic examiner to identify or find the evidence. These tools and techniques fall under a specific branch of forensics called anti-forensics. Anti-forensics is used by civilians to thoroughly remove unwanted data from a system and make room for other files and information, but it can also be used by criminals to prevent investigators from finding incriminating evidence. This paper focuses on the use of standard computer systems as digital media and the different ways that criminals can attempt to circumvent forensic examination of this digital media using anti-forensics.

DIGITAL FORENSICS AND ANTI FORENSICS

To understand anti-forensics, the topic of digital forensics itself must be explained. In a journal article written by Ryan Harris in 2006, forensics was defined as “the application of science to those criminal and civil laws which are enforced by police in a criminal justice system” (Harris). Merriam-Webster’s Dictionary also defines forensic as “the application of scientific knowledge to legal problems; especially: scientific analysis of physical evidence (as from a crime scene)” (Forensic). These two definitions support the statement that forensics is the application of the scientific method to evidence used in criminal and civil court. The National Institute of Standards and Technology (NIST), an organization that creates worldwide standards for information technology, stated in their Special Publication 800-86 that, though digital forensics has many definitions, it is generally considered “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data” (Kent, ES-1). Today, though the definition of digital forensics is not definite, the intention is clear: the analysis of digital media through forensically sound means, without alteration of original source evidence.

Anti-forensics is the opposite of digital forensics, but what does that mean? The Grugq, a renowned anti-forensics expert, stated that anti-forensics is the mitigation of the effectiveness of forensic investigation (The Grugq). In comparison with digital forensics, the use of anti-forensics is very similar. Anti-forensics uses tools and techniques to inhibit forensic investigation of digital media, while digital forensics uses tools and techniques to find evidence on digital media during a forensic investigation.

Digital media encompasses an ever-increasing number of sources. This list is determined by a media or device’s ability to transfer or contain digital data and includes standard computer systems, mobile devices, removable media, personal digital assistants (PDAs), networks and networking equipment, and, more recently, cloud computing.

ANTI FORENSIC CATEGORIES

The categories of anti-forensics are as agreed-upon as the definition of digital forensics itself. These categories have been stated in many different ways. In his article about how to control the anti-forensic problem, Harris divided anti-forensics into four categories: (1) destroying evidence (dismantling evidence or otherwise making it unusable to the investigative process), (2) hiding evidence (the act of removing evidence from view), (3) eliminating the source (neutralizing the evidentiary source or the lack of creation of the source), and (4) counterfeiting (creating a version of the evidence to appear as though something else has occurred) (Harris). These four categories can be considered the basic idea of what anti-forensics entails The InfoSec Institute comparatively divided anti-forensics into the following categories: data hiding (concealment of data from forensic analysis), obfuscation and encryption (changing or encrypting data), data forgery (creation of data that is false), data deletion and physical destruction (the attempt to delete or physically destroy data) (De Lucia, Anti-Forensics: Part 0x01), analysis prevention (the ability to infiltrate or work on a system without creating or generating evidence), and online anonymity (inability to associate a specific person with an action) (De Lucia, Anti-Forensics 2). The categories that the InfoSec Institute provided are more specific than the broad categories Ryan Harris defined. The aspects of these categories, though different, cover the same basics and are pertinent to include in the description of anti-forensics. This paper looks at the following categories with regard to anti-forensics: data hiding, data obfuscation, data deletion/destruction, data forgery, and attacking the investigation.
Data Hiding

Data hiding can be defined as the act of hindering an analyst’s ability to locate data. This form of anti-forensics is one of the most widely known within both the civilian and forensic communities. This is because it is all around us: on the television, in the news, and in criminal cases. As data hiding is widely known, it can be accomplished through a variety of means, one of which is steganography.

Steganography, or as Gary Kessler describes it, the art of covered or hidden writing, is used for transferring or hiding information within a seemingly innocent image (Kessler, Overview of Steganography). Digital steganography can hide any form of digital media within another. With steganography, text file data, for example, can be hidden within another text file or an image; an image can be hidden within an mp3 file or another image file. This ability to hide any form of media within another makes forensic analysis difficult. Overlooking inconsistencies within a file or not having the right tools can inhibit or even prevent forensic analysis by an examiner. To employ steganography, many tools have been created and are available online for use or download, including Steghide, JP Hide and Seek, S-Tools (Kessler, Overview of Steganography), Xiao Steganography, Image Steganography, OpenStego (Shankdhar), and mobilefish.com. The numerous types of steganography tools available as both applications and online services make the determination of how the data was hidden even more arduous.

Cryptography is the encryption and decryption of data with the use of a key. This key is used to both encrypt and decrypt a file, folder, partition, or even full digital media itself (though this last option does take time to complete). The key itself can also be protected using a passphrase or by placing it onto removable media, such as a USB. If the key is lost, damaged, or otherwise unavailable, the encrypted data is then considered to be inaccessible, as the key is needed to decrypt the cypher. An example would be protecting the results of vulnerability assessments and penetration tests by using an encryption of the hard drive and keeping the key to the encryption on a USB to preserve the integrity of the data. Tools that can encrypt media include TrueCrypt, WinZip, BitLocker, and SafeBoot (Kessler, Anti-Forensics). Cryptography is also now readily available in many applications; Microsoft Word, as an example, gives the ability to encrypt the document created using a password (Kessler, Anti-Forensics). This is not necessarily a good thing, as criminals can then trade information or hide images or videos from being seen unless a known ‘key’ is entered to decrypt the file.

The generic hiding of data is just as it sounds, hiding of data in an obscure location so that an investigator does not find it. To hide data effectively, there are four main locations that the data can be placed that are not initially analyzed by the investigator: master boot record (MBR), host protected area (HPA), slack space, and the device configuration overlay (DCO). The master boot record is the space at the beginning of a hard drive that contains the code to load the operating system (OS), contains partition tables, and defines the location and size of the partitions. There is a 62-sector gap between the MBR and the first partition table. This is due to digital media, specifically hard drives, creating a track (usually 55 to 62 sectors) of separation between the two types of stored data (Sammes 184). The gap prevents any information from the MBR from unnecessarily being mixed into the next partition, which makes this space a good resource for hiding data.

The most common place to hide data would be the host protected area. This is because the HPA is not accessible by the operating system and requires specific tools to gain access; there are even certain forensic tools to which the HPA is invisible. The HPA is “an area of the disk reserved for booting utilities and diagnostic programs” (Nelson), that also contains vendor information, and therefore has the potential for hiding information and files from the OS. The device configuration overlay is the most beneficial location to hide any incriminating evidence. The DCO is not as well-known as the HPA to forensic analysts and is therefore considered stealthier. This is because the DCO was created to limit the apparent capacity of a drive (Bunting and Wei). This means having a 32 GB USB with only 24 GB of storage available and “seen” by the OS. Another place to hide information is in the unallocated (or slack) space. There are three ways that slack space can be used to hide data: the placement of data within the slack space itself, the placement of data within the last few sectors of data (unable to be seen by the OS), and the modification of good sectors of the hard drive to “bad sectors” to prevent access to this location by the operating system (De Lucia, Anti-Forensics: Part 0x01).

Data Obfuscation

Data obfuscation is the changing of information to hide digital evidence. This means changing the "physical" aspects of files and events. "Physical" in this context pertains to the various identifying data of individual files. This technique of anti-forensics uses various tools to achieve the goal.

Metadata is in every file on digital media, but the presence of metadata can be deceiving. This is because, though a file does contain metadata, not every file will contain the same amount of metadata. For instance, one JPEG file may contain metadata that includes the file name, file type, make and model of the camera used, geographical information, file and pixel sizes, and editing program information, whereas another JPEG file may only contain the file name, file size, and pixel size. Metadata can also include the file’s created, accessed, modified, and edited times, application information (what application was used to create the file), and user information (user or company who created the file). This information is important because it can provide a timeline and confirm user presence on the system.

---

Metadata is in every file on digital media, but the presence of metadata can be deceiving. This is because, though a file does contain metadata, not every file will contain the same amount of metadata. For instance, one JPEG file may contain metadata that includes the file name, file type, make and model of the camera used, geographical information, file and pixel sizes, and editing program information, whereas another JPEG file may only contain the file name, file size, and pixel size. Metadata can also include the file’s created, accessed, modified, and edited times, application information (what application was used to create the file), and user information (user or company who created the file). This information is important because it can provide a timeline and confirm user presence on the system.
The metadata, which can be important, can also be unreliable. This is due to the resourcefulness of criminals changing the metadata using tools. One such tool is Timestamp. Timestamp is a tool created for the purpose of changing or removing the modified, accessed, created, and edited timestamps (also called the MACE) on a file. If done correctly, an investigator will not see these changes at first glance. Another way to overwrite the metadata is to access the files or data in such a way that those changes are not recorded. This can be done by mounting media or partitions as read-only, allowing the files to be accessed without recording the accessed times (Garfinkel). The file type can also be altered, which can, when an attempt is made to open the file, bring up an error window or show unreadable data. The changing of the file type is done by editing the file extension (.docx, .jpg, .txt, etc.) at the end of the filename.

Criminals can also obfuscate data by altering server logs and system event logs (Kessler, Anti-Forensics). Server logs record any activities that the server itself performs, where system event logs record any event that happens on the system (login attempts, application errors, system shutdowns, etc.). Fortunately, it is exceedingly hard to delete or alter server logs and system event logs. This is because the logging applications were created to not remove logs from the system. Though these applications are coded in this way, to prevent changes or deletions to the logs, there have been tools created specifically for this purpose. For example, Winzapper is a tool used to delete server and system event logs from the Windows NT/2000 Operating System.

A computer’s registry contains a mountain of information, if you know where to look. The computer registry is essentially a log of all information that occurs within or on a system; user data, recent documents, browser history, and even program information are a few things that are kept within the registry. Malware and hackers can edit values within the registry to gain access or monitor the system for information. It is important to know where these registry values could be, as criminals can attempt to remove data by removing traces from the registry.

Data Deletion/Destruction
Data deletion and destruction effectively has two meanings with the same potential outcome: the information being no longer available or unable to be found in any way, shape, or form on digital media. The deletion of data is considered the removing of that data from any digital media by any means necessary without compromising the data, whereas the destruction of data is the total annihilation of the data on digital media, even going so far as to physically destroy the media so the data is not readable.

Data deletion anti-forensics is not just removing (or “deleting”) the file from being accessed in the operating system, it is attempting to remove all traces of the file from being accessed using digital forensic means. Data deletion is also known by a few other names as well: overwriting data, artifact wiping, eliminating evidence, scrubbing, and file wiping, to name a few. These names are not just for show; some describe different techniques that criminals can use to remove their unwanted data.

Overwriting data is done by attempting to overwrite individual files, or by attempting to overwrite all previously “deleted” data. Different tools can deploy different techniques to overwrite the data. Simson L. Garfinkel points out that Apple’s Disk Utility overwrites data by passing over the information with a single pass, seven passes, or thirty-five passes of null (or zero) bytes; whereas cipher.exe does multiple passes of varying inputted data (in accordance with DOD standards) (Garfinkel).

Artifact wiping is similar to overwriting data, but it can remove information from groups of data. One type of artifact wiping is to actually use the overwriting technique – it destroys the data using multiple overwrites to render the data irretrievable (Kessler, Anti-Forensics). This can be done with wiping software such as dc3dd, Eraser, Darik’s Boot and Nuke, Disk Wipe, and even CCleaner. Artifact wiping is also done to gain storage space by removing unwanted temporary files. These temporary files can include browser history, cached files, and browser autofill (removed using CCleaner or SecureClean), specific OS files (removed using Window Washer), and even the remnant files in the slack/unallocated space of digital media (removed using Evidence Eliminator).

Artifact wiping is done by using file-specific tools or using open-source tools. A lot of these free open-source tools used for wiping artifacts, can be modified for specialized usage, or additional plugins can be added for more specific applications or file types. Wiping can also eliminate data by wiping digital media completely, depending on the type of media. It is preferable, for example, to completely clear out a USB drive, as opposed to a computer or laptop that is consistently used.

Data destruction, as previously stated, is any means of physically destroying the evidence so a forensic investigator is not able to retrieve any data. Destroying a form of digital media can be done in a variety of ways, including water damage (submerging it into water or running it through the washing machine), smashing it into pieces (with a hammer), trying to flatten it (with a car), electrical damage (overpowering the media with electricity), or even overheating or burning the media (in a fire).

Data Forgery
Data forgery is one of the more difficult anti-forensic measures, as it entails the creation of false evidence to hide or mask the true evidence on a system. This is not to be confused with data obfuscation, which changes the data of an evidence file or system itself. Data forgery can also be considered counterfeiting evidence. This type of anti-forensics is unique, as it requires the creation of new evidence, not just the
changing or removal of evidence. It is also unique because the other categories of anti-forensics can be used in conjunction with data forgery to achieve the intended outcome: the forensic investigator being unable to find the pertinent evidence for the investigation.

The execution of data forgery is done by the creation of different events or files within a system. This can include the use of another user’s account to create false information (Harris) and the creation or removal of files that are not important to the criminal’s task (to throw off the scent).

ATTACKING THE INVESTIGATION

There is also one more category of anti-forensics that has not been covered: the attack on the forensic investigation itself. This attack does not happen in a physical manner, but a logical one within the system. These attacks cannot be anticipated, which makes them extremely surprising and dangerous (depending on the attack). One type of attack on an investigation is the use of a zip bomb. The zip bomb looks like a harmless zipped file, but, when opened, it releases a barrage of files that will immobilize the system. This occurs because a zip bomb consists of a small zip file, that, when expanded, opens four more zip files that open four more zip files each, continuing until the memory is potentially flooded, causing the system or the application used to crash. This crash can be used to inject malware or even corrupt data within the system itself. Figure 1 gives a more visual representation of why a zip bomb can be so dangerous. Another attack is the use of program packers. Program packers are used to hide a malicious program by compressing and/or encrypting it and placing it inside another common executable (Garfinkel). This protects the malicious program from being detected or reverse engineered; reverse engineered in this context means taking the program, file, or executable apart to see how it works and discover any identifying characteristics.

Another way to attack the investigation is to render automated tools unable to analyze specific data. The Metasploit Anti-Forensic Investigation Arsenal (MAFIA) was created by the Metasploit Project to investigate the shortcomings of different forensic tools. This resulted in a set of tools that were created for the sole purpose of hindering forensic tools from accurate analysis: Transmogrify, slacker, TimeStomp, and SAM Juice. For example, Transmogrify is a tool that allows a user to mask and unmask a file’s file type. Though this is considered data obfuscation, it is placed in the “attacking the investigation” category because this tool prevents the forensic suite EnCase from detecting the file type (Kessler, Anti-Forensics).

Attacking the investigation also includes attacking or noting the use of tools used for forensic analysis. Certain types of anti-forensics tools can detect if forensic means are being used on a system. This can be done by using the Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) used in most hard drives (Garfinkel). By accessing these reports, a tool can determine if an image is being made of the system (if there is an increase in power-on minutes) and prevent the tool from opening or reacting in its “natural” way.

ANTI-ANTI-FORENSICS

To react to the anti-forensics threat, there is a group of techniques referred to as anti-anti-forensics. Though a little redundant, the anti-anti-forensics techniques can also be used during a regular forensic investigation. Unfortunately, the amount of techniques for anti-forensics greatly outnumbers the amount of techniques used to thwart criminals’ attempts of hindering an investigation. The techniques used to uncover and “reverse” anti-forensics are as follows: tools, registry logs, data carving, and knowledge.
Tools
When anti-forensics measures have been found on a system, the first thing an investigator should look at are the tools. Knowing the tools used to do anti-forensics and the tools that could be used to retrieve any data is important in an investigation. Once the anti-forensics tools have potentially been identified (and sometimes they will not be identifiable), the investigator can start to try to work around the anti-forensic measures if possible.

Steganography, for example, can be detected due to file size. If a file size looks extremely out of proportion, metadata can be used to see the specifics of the file. Once the file has been identified, as long as it is a known file type, such as an executable, or a has a known file size, the specifics of the file. Once the file has been identified, as long as it is a known file type, such as an executable, or has a known file size, the specifics of the file can be compared to known information to determine if there is a known file type, such as an executable, or has a known file size, the specifics of the file.

One way of looking at cryptography is as a locked door. To open the door, the correct key is needed. This key is the password, passphrase, or encryption key used to encrypt and decrypt the file; if you have the correct key, opening the door is easy. Most of the time, forensic investigators do not have the key needed to open the door. When a key is not available, forensic investigators will use various tools to attempt to crack, or break into, the lock. The tools used are password cracking tools, such as L0phtcrack/Ophcrack, AccessData’s Password Recovery Toolkit, John the Ripper, Cain and Abel, and many others.

Steganography is any anomalous metadata. If steganography is involved, without the tools used to implant the data or the passphrases needed, extraction of the hidden data is impossible. If it is a picture file, however, or a custom file, there may be no way to determine if steganography is involved unless file size is considered, for example, a single image or small group of images that are larger than normal image sizes.

These tools can crack the password using a variety of methods, including brute force (attempting every possible key or combination until it works), dictionary attack (attempting all letters in an organized manner, like words in a dictionary), the use of rainbow tables (like a dictionary attack, but using numbers and other characters in place of letters, as well), or determining the password from a hash value or set (a hash value is an individual algorithmic value given to a string, file, or device). Even with these tools, there are fail-safes that can prevent the cracking of passwords. These fail-safes can be predetermined and are limits on how often passwords can be attempted before the user is locked out or the data gets wiped.

Data Carving
When looking at data on digital media, it is not only represented as binary, but also as a hexadecimal value. This hexadecimal value is a mix of two letters (A through F) and numbers (0 through 9) as a single ASCII character that can be understood. For instance, the hexadecimal value 30 represents the number 0, where the hexadecimal value 6C represents the letter l (lowercase). Figure 2 shows various hexadecimal values with their ASCII counterparts.

These hexadecimal values are what are used to carve out individual files from digital media. This is used because, when a forensic image is taken of digital media, there are still locations (HPA, DCO, slack/unallocated) that contain information unreadable by tools. If this data can be carved out, a file could be re-created, depending upon how much of that file is available. If a criminal hides information within the hidden areas of a hard drive or in the slack/unallocated space of digital media, those files can then be carved out and analyzed. Each type of file has its own signature to mark the beginning and the end of the file. An investigator must determine the signature of the file and carve out as much of the file as possible. It is time-consuming work to carve out data, but there are tools that attempt to carve out files from the unallocated space of digital media. If some hexadecimal values are different from what a program is told to look for, however, it will skip that information. Figure 3 is an image of a JPEG file with a different JPEG hexadecimal value. Because the different value is not the default for JPEGs, some tools will not register the file as a JPEG, but will note it as a “mismatched” file, if it notes anything at all.

Registry Logs
One of the best resources a forensic examiner has is the registry. As stated before, the registry is a log of all information that has been placed, added, or changed on a system. Not all digital media will contain a registry; this storage of information is particular to computer systems, such as tower computers, laptops, and even a few tablets. The registry is easily accessible by users and can be altered by adding or changing a registry key. To use the registry, a user must first know where to look for important information. This is critical in investigations as an investigator can use the registry to find a multitude of information in various places that a criminal may overlook. The following paragraphs detail a few locations where pertinent information can be found in the registry.

User information can be found in both the Security Account Manager (SAM) Hive and the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. The difference between the two is that the SAM file shows accounts that were manually added onto the system by an interactive user.

---

Figure 3. Badheader2.png.

---

Last shutdown/login information can help an investigator determine a timeline of who was on the computer when. The last user to log on can be found in the registry at the following location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon. The last shutdown time is found in the registry at HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows, though the data is in binary format and can be difficult to interpret.

Recently opened documents/files can help an investigator determine what files were opened, and by what user, especially if this information was removed from the recent documents folder in the system or if Timestomp was used. These are found in the location C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Recent Items on a Windows system, and at HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. An investigator can also find the recently opened/saved files (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU) and recently opened/saved folders (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU) in your registry.

Browser history can be useful when trying to determine what a user looked up on their browser. For Internet Explorer, the location for the browser history is at C:\Users\<user name>\AppData\Local\Microsoft\Windows\History. But an investigator can also find various information in the registry, such as typed URLs (HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls), AutoComplete forms (HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1), and even AutoComplete passwords (HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2). Each browser has its own registry key that can hold information in – but whereas the profile list lists the profiles on a system that were made logically, or through a remote process, with no physical user at the system.

Last registry key edited shows the last registry key that was physically altered. This means a user had to open the registry and alter a registry key for this key to be created and retain data. This information can be found at HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit.

A list of some forensically important registry keys can be found in appendix A. The previous list is just a small amount of the information that can be found in the registry. Mounted devices (such as USBs, external hard drives, or SD cards), connected printers, and network connections can also be found in the registry.

**KNOWLEDGE**

When doing a forensic investigation, knowledge is an examiner’s best defense against anti-forensics. The more an examiner knows, the better they can prepare and plan for their investigation. If an investigator knows where hackers like to place their tools, or where certain criminals like to store information or from where they like to remove information, this can be key to finding remnants of any files that may have been removed. Let’s look at data hiding first. In steganography, if an investigator finds a JPEG file that is more than 25 MB large where all the other JPEG files are just a few megabytes, depending upon the resolution, it is a safe bet that there is something odd about the file that requires more investigation. Someone just looking at the images in this case would not take into consideration the file size, therefore ignoring potential evidence.

The generic hiding of data itself requires knowledge about possible places to hide information. HPAs and DCOs are not easy to locate, and therefore require thought as to what a criminal would want to hide and where it would be hidden. This thought process also applies to unallocated/slack space. If data is hidden in the unallocated/slack space, an investigator cannot always rely on their tools to pick up all the data. Because of this, investigators must manually look through this “unused” space and use their knowledge of file systems and file signatures to find missed files and carve them out.

Data obfuscation is uncovered in a similar way. The metadata of a file must be analyzed for anything that looks askew to determine if information has been purposefully changed. In some cases, the metadata that is changed will look completely out of place from the surrounding information, indicating that the file has been tampered with and could be of interest to the case. Server and system event logs can be very helpful in an investigation, but these logs too can also be deleted. This is where one of the most significant advantages of knowledge comes into play. With any system, the lack of information can itself be information. If there are server or event logs missing for a large period of time, or there is data about one event but not about a correlating one (such as startup, logon, logoff, and shutdown), this shows that someone has gone out of their way to change the information on the system itself. When it comes to data deletion or destruction, the best thing that an investigator can do is search
through the data to find if there are possible remnants of files still on the system.

Knowledge is also a key component in creating a timeline of events. An investigator must use their knowledge of the case and the evidence found to create a timeline of events that happened on the digital media. The timeline can indicate who did what, and when, on the system and what data was changed, added, or even removed. The evidence also must be succinct so that there is no inference of the facts. This also ties into data forgery. Investigators should take into consideration all the evidence to make a determination, not just the evidence that was easy to find (which could potentially be forged).

Finally, knowledge can help make or break a case when it comes to attacks on the investigation. If a zip file or an infected file needs to be opened, opening these files in a virtual machine (VM) is the best course of action. This prevents infecting or crashing the host system while still attempting to retrieve data during the investigation. The VM can also be used to mount an image to see how the live system was operating, if the right materials are available (volatile data, such as RAM). Though knowledge of anti-forensics cannot protect an investigator from every actuality, it can be used to help prevent and circumvent the use of anti-forensics against the investigation.

CONCLUSION

The anti-forensic techniques can be used by criminals to hide potential evidence. These techniques include: hiding data through the use of steganography or cryptography, or just plain hiding the information; obfuscating data by attempting to change the metadata of files, deleting server and system logs, and editing the registry; data deletion involving the use of wiping tools to eradicate all traces of data within the media, to the point of even using physical damage to destroy the media itself; data forgery; and, finally, attacking the investigation itself through various means, including zip bombs, packet parsing, and scanning for the use of forensic tools.

Though these anti-forensic measures are daunting, this paper shows that they can be circumvented using different techniques such as tools, data carving, the registry, and knowledge about forensics and anti-forensics. Through the use of counting tools, anti-forensics can be detected or even reversed in rare cases (given the right information is found). Data carving is a skill that is helpful in finding and extracting data that was hidden from or unreadable by automated forensic tools. It is time-consuming, but can lead to important data being recovered. The registry has been shown to contain a large amount of information that can be used during an investigation to help find specific evidence, determine users, and help to create a timeline of events. Though these techniques are important, nothing can replace knowledge. Knowing that anti-forensics is out there and can be used by criminals to impede an investigation can help tremendously.

Unfortunately, the research done on anti-forensics and how to work around it is not as up to date as the anti-forensic techniques and tools themselves. Investigators will always be one step behind the criminals. Hopefully, with more research done, time given, and tools created, the investigators will not be too far behind. Knowledge is power, and as long as investigators maintain and improve their knowledge of anti-forensics, they stand a fighting chance against the criminals who would restrict the investigations.

WORKS CITED


### APPENDIX A: FORENSICALLY INTERESTING WINDOWS REGISTRY KEYS AND LOCATIONS

<table>
<thead>
<tr>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recently opened files from Windows Explorer</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Microsoft\Windows\Recent Items</td>
</tr>
<tr>
<td>Network Shortcuts</td>
<td>C:\Users&lt;user name&gt;\AppData\Roaming\Microsoft\Windows\Network Shortcuts</td>
</tr>
<tr>
<td>Temp folder</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Temp</td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>C:\Recycle.Bin</td>
</tr>
<tr>
<td>Event logs</td>
<td>C:\Windows\System32\config or C:\Windows\System32\wintext\Logs depending on the OS</td>
</tr>
<tr>
<td>SetupAPI Device Log</td>
<td>C:\windows\inf\setupapi.dev.log</td>
</tr>
<tr>
<td>Windows Prefetch</td>
<td>C:\Windows\Prefetch</td>
</tr>
<tr>
<td>Internet Explorer Temp Folder (IE Cache)</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Microsoft\Windows\Temporary Internet Files</td>
</tr>
<tr>
<td>IE Cookies</td>
<td>C:\Users&lt;user name&gt;\AppData\Roaming\Microsoft\Windows\Cookies</td>
</tr>
<tr>
<td>Internet Explorer History</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Microsoft\Windows\History</td>
</tr>
<tr>
<td>Printer spool folder</td>
<td>C:\Windows\System32\spool\PRINTERS</td>
</tr>
<tr>
<td>Recently Opened Office Docs</td>
<td>C:\Users&lt;user name&gt;\AppData\Roaming\Microsoft\Office\Recent</td>
</tr>
<tr>
<td>Offline Outlook Mailbox</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Microsoft\Outlook\outlook.ost</td>
</tr>
<tr>
<td>Temp folder for Outlook attachments</td>
<td>C:\Users&lt;user name&gt;\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook&lt;random value&gt;\</td>
</tr>
<tr>
<td>Flash Cookies Location</td>
<td>C:\Users&lt;user name&gt;\AppData\Roaming\Macromedia\Flash Player#SharedObjects&lt;random value&gt;\</td>
</tr>
<tr>
<td>Items recently ran from the “Run” bar</td>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU</td>
</tr>
<tr>
<td>ComDlg32 recently opened/saved files</td>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU</td>
</tr>
<tr>
<td>ComDlg32 recently opened/saved folders</td>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU</td>
</tr>
<tr>
<td>Recent Docs</td>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs</td>
</tr>
<tr>
<td>User Assist</td>
<td>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist</td>
</tr>
</tbody>
</table>
Description: Last logged on user  
Location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Description: User Profiles  
Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

Description: User Accounts  
Location: HKEY_LOCAL_MACHINE\SAM

Description: Last shutdown  
Location: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

Description: Last key edited by RegEdit  
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

Description: List of Installed USB devices, both connected and unconnected  
Location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

Description: List of installed USB storage devices  
Location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Description: List of Wireless access points the System has connected to  
Location: HKLM\SOFTWARE\Microsoft\WZC3\Parameters\Interfaces

Description: List of all LAN connections made  
Location: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

Description: List of all mounted devices on system  
Location: HKLM\SYSTEM\MountedDevices

Description: Page/Swap file  
Location: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Memory Management

Description: Hibernation file  
Location: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Power

Description: Time Zone of the system  
Location: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

Description: Programs designated to run upon startup  
Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Description: Source OS Updates  
Location: HKEY_LOCAL_MACHINE\SYSTEM\Setup\Source OS\(Date and time of update)

Description: Last Registry Key edited  
Location: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Description: Programs on the system  
Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RegisteredApplications

Description: IE Typed URLs  
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls

Description: Internet Explorer Forms AutoComplete  
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1

Description: Internet Explorer Password AutoComplete  
Location: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Description: List of applications that are allowed 'outside access' by Windows firewall  
Location: HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

Description: Files recently accessed by Windows Media Player  
Location: HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\RecentFileList

ADELINE HEUCHAN

Adeline Heuchan is a Cyber Instructor at Art of Exploitation and a recent graduate of Stevenson University. She has received her Bachelors of Science in Computer Information Systems with a specialty in Computer Forensics, is ACE certified and is working towards her Masters in Forensic Studies.
Authenticating Art
Alisia Alexander

INTRODUCTION

A 2014 documentary film titled Art and Craft, directed by Sam Cullman, Jennifer Grausman, and Mark Becker, recognized the skills and talents of a famous art forger, Mark Landis. The film provided details of Landis’s operation, which allowed him to deceive over 45 museums into showcasing his forgeries in their collections for over 30 years. Using his artistic abilities, Landis would study prints of original artwork and recreate them using basic art materials. He would then contact museums and make appointments to meet with their directors, pretending to be a philanthropist. Using his vast knowledge of art history, Landis would convincingly pass for an art collector, persuading museum directors to accept his artwork for display. Landis would not be caught until 2007, when Matt Leininger, a museum registrar, researched a painting Landis offered for donation to the museum. Leininger discovered that the painting was currently on display in another museum, revealing Landis’s scheme as a forger. Landis would not be arrested or charged with a crime, as he donated, and did not sell, his forged artwork (Blair).

Other forgers have followed the same path as Landis, but differed in their intention to make profits. Landis and other art forgers have made the business of forging art lucrative, gaining the attention of the art community, and, most importantly, alerting the buyers to the necessity of questioning the authenticity of artwork being sold. The art industry, like many others, now bears the cliché “buyer beware” warning. The authenticity of artwork is examined in three parts: provenance, historical context clues from the period, and scientific analysis (Chappell and Hufnagel 90). This paper examines the crime of art forgery and the three steps of authenticating artwork, mainly focusing on techniques used in the scientific analysis phase.

WHAT IS ART FRAUD? AN OVERVIEW OF THE PROBLEM

According to the book Contemporary Perspectives on the Detection, Investigation and Prosecution of Art Crime: Australasian, European and North American Perspectives, “art fraud describes the crime of obtaining benefit (financial) from the deliberate and intentional deception by passing off a work that is not authentic as if it were” (Chappell and Hufnagel 90). Occasionally, art forgery goes unnoticed for years. To identify the crime of forgery, an investigator must prove the intentions of the seller to deceive the buyer. According to Chappell and Hufnagel, members of the art community rely on an assumption of trust. The buyer trusts the seller’s word concerning the artwork’s authenticity and believes the seller has knowledge of the history of the artwork to support the statement of authentication. This trust allows forgers to continue to mask their intentions, as well as their crime (Chappell and Hufnagel 90).

Art forgery has been around since the beginning of humankind. According to Suzanne Bell, author of How to Identify a Forgery: A Guide to Spotting Fake Art, Counterfeit Currencies, and More, the first account of art forgery occurred during the Roman Empire. During that period, Egyptian and Greek art was widely traded. The demand for such art, and specifically Greek art in the case of the Romans, became greater than the resources available, resulting in the establishment of “copy shops” in Rome to fulfill the demand. Modern western art would become the next area of operation for forgers during the fifteenth century, as wealthy people began to buy art and sought-after works produced by famous artists such as Michelangelo and Leonardo da Vinci. Because of Michelangelo and da Vinci’s prestige and the demand for their artwork, some artists would begin to mimic their artwork simply to study their techniques, while others would try to present these copies as authentic works. This practice would continue into the eighteenth century, as Europe’s royalty would create a great demand for art, allowing for the establishment of an art forgery market that would rapidly expand in the nineteenth century to become the blueprint for the art forgery market of today (Bell 23-24). According to Bell, “40 percent of the art on the market are forgeries,” with more works in progress, threatening to overflow the market. Forgers are now “creating libraries of paintings attributed to artists who never actually existed” (Bell 25).

According to Robert Spiel, author of Art Theft and Forgery Investigation: The Complete Field Manual, “art forgery including art theft is roughly estimated to be a $1.3 billion business” (Spiel 33). Problems with statistics, recordkeeping, and underreporting due to the failure to detect forgeries, have hampered the ability to give an exact account of how much money is generated in the illegal business of forgery sales. The estimated wealth generated by the art fraud industry gained the attention of law enforcement, specifically the Federal Bureau of Investigation, prompting the creation of an Art Crime Team dedicated to investigating art crimes and combating the problem (Spiel 33). Nevertheless, law enforcement’s involvement in the dealings of the art market may not deter the sale of forgeries. According to author Gregory Day, the art industry participates in and promotes the secrecy of information regarding the authenticity of the artwork for sale, allowing for the influx of forgeries into the art market. The great demand for artwork produced by historical artists, such as van Gogh and da Vinci, known as the “secondary resale market,” contributes to the art forgery problem, as forgers may be commissioned by sellers to satisfy the market’s need (Day 466, 480). The art industry’s acceptance of art dealers conducting sales of artwork “privately and confidentially” further complicates detecting and preventing the sale of forgeries. These types of art sales do not facilitate a buyer questioning an artwork’s “purchase history, prior owners, and place of origin” (Day 469). Because of these issues, the art market will continue to have problems with art forgeries, as the industry’s current practices allow for and support the existence of forged art (Day 459-469).
ART FORGERY METHODS

According to Spiel, the artwork of a forger is meticulously planned, as forgers ask themselves a series of questions before they begin the creation of a forged masterpiece. The forger first addresses the question concerning what type of artwork he or she wants to create, weighing the cost of materials and the time to be invested, the profitability, and the degree of detectability. “In artwork, the general payoff rank (in ascending order) for artistic media is prints, then cast sculptures, drawings, watercolor paintings, unique sculptures, and oil paintings” (Spiel 83). Once the type of item to be forged is identified, the forger identifies which artist he or she would like to mimic. The artist is selected based on the profitability of works by that artist, as the forged artwork of a more famous artist will have a higher value than that of a lesser-known artist. However, when selecting an artist to mimic, the forger keeps in mind his or her own artistic abilities. Depending on the forger's abilities or level of time available for such a scheme, the forger could decide to only fake a signature. Using his or her knowledge, the forger would search for completed works by an unknown artist whose artwork is similar to that of a known artist and would recreate the well-known artist's signature on the available works. Finally, if the forger possesses excellent skills, he or she needs to decide whether to create a “direct copy” or a “style of” forgery. For a direct copy forgery, the forger attempts to recreate known artwork, while for a style of forgery, the forger uses his or her own artistic abilities to create a new painting that mimics the style of the forger’s choosing. If the forger decides on creating a style of forgery, the remaining questions left to answer are what will the focal point of the painting be and which period will it be mimicked? (Spiel 83-89).

THE PROCESS OF ART AUTHENTICATION

For artwork to be authenticated, a reasonable suspicion must first be brought up by the buyer, or the curator in the case of a museum or business. Once this happens, the provenance is examined. “Provenance is the history of the artwork that exists in documentary form and which provides the evidential chain that links the artist and the work in question” (Chappell and Hufnagel 93). The provenance of a piece of artwork may consist of several documents, as it traces the past movements of the artwork. For example, if a painting was lent to a museum to house in their collection and was later sent to an art institution to be studied and placed into a scholarly catalogue, each movement would be documented with additions to the original provenance. However, there are times when provenance cannot be established or is questionable. Depending on the age of the artwork or how the possessor came into possession of the artwork, the provenance could have been lost or never created. This is the case when authentic artwork is gifted by the artist to family members or friends, and the artwork is further handed down through generations of family members as a family heirloom. At times, the artists themselves did not sign their artwork and began experimenting with other painting styles, not allowing for provenance to be established (Chappell and Hufnagel 93-94).

In 2013, the Van Gogh Museum in Amsterdam, the Netherlands, put on display a long-lost painting of Van Gogh from the year 1888. This painting, “Sunset at Montmajour,” was thought to be a forgery for many years, and was even refused authentication by the Van Gogh Museum. The questioning of this piece’s authenticity resulted from Van Gogh both failing to sign his work and adopting a new painting style in the middle of the artwork's completion. Because of this, the painting had gone through a series of buyers, sometimes without documentation, contributing to the lack of provenance. The painting would finally be authenticated by the museum in 2011 after a request from the most recent buyer. The Van Gogh Museum gained possession of some of Van Gogh’s personal writings that discussed the painting (Associated Press).

Provenance can also be falsified. To reduce the likelihood of forged artwork being detected, forgers can produce fake provenance. Because provenance is merely paperwork, such as “a letter or bill of sale from the gallery representing the artists, which details the artwork, or a statement from the artist” stating the artwork was completed by them (Chappell and Hufnagel 94), the forger could study such documents and recreate them for his or her artwork. Depending on the age of the type of painting the forger is trying to portray, the appearance of the forged documentation can be altered to look older.

Since provenance can be falsified, the next step for authentication is the use of art historical context clues. When assessing artwork for historical context, the examiner must be well educated in the various art movements and artists, and must understand the importance of an art history timeline. At the J. Paul Getty Museum in Los Angeles, California, in its historical context course, students are taught a series of steps to follow in determining historical context (J. Paul Getty Museum Staff). First, they examine the artwork, writing down their initial impressions, what they notice about the painting, and what strikes their attention. From there, the artwork is further observed, objectively. The examiner looks deeper into the artwork, taking note of the painting style or brush strokes, looking for the characteristics of an art movement, or a possible tell-tale sign of an artist. These objective observations are then used to fit the questioned artwork into a movement or period to better date the artwork. At times, the historical examination is accompanied by a visual examination of the artwork. This process is discussed in detail in the scientific analysis portion of this paper. When relying only on historical context clues, there may be challenges, as forgers can use various techniques to age forgeries and/or mimic older artwork. According to Spiel, art forgers have developed many techniques to fake historical contexts. To mimic the appearance of an old canvas, forgers can purchase an older used canvas of an unknown artist to paint over. If the used canvas is not in a good condition, forgers can re-stretch the canvas or stretch a
This technique requires the use of a unique microscope unlike the one examination and detection of elements contained within the artwork. Scanning electron microscopy is a technique that allows for the visual present on the canvas or if the painting was possibly restored. Any other colors used and the different types of paint present layers of the paint, its colors, and its characteristics (Bell 27). The three-dimensional view allows the examiner to identify the various using various methods. The noninvasive techniques do not require any modification of the artwork in question; in fact, the artwork remains completely intact when examined because of the use of enhanced visual techniques. Examples of each technique are described below.

**INVASIVE TECHNIQUES**

The scientific analysis of artwork using invasive methods can range from a simple microscopic examination of paint scrapings to a detailed multi-step process requiring the use of highly powerful and sensitive technical equipment. Depending on the forger’s skills, the materials used, and the time he or she invested to prevent detection, the scientific examination may have to rely on increasingly complex methods. The methods of examination are addressed below in ascending order of complexity.

A visual examination of the paint samples can be completed by the examiner with the use of a stereoscopic microscope. The microscope helps with a “preliminary examination and sorting of particulates” of the material to identify further tests can be done or would be more useful in identifying whether the painting in question is a forgery (Bell 29). This preliminary examination is useful when the sample size is small or if collecting more samples from the painting in question would cause irreparable damage. The use of a stereoscopic microscope allows the paint sample to be viewed as a three-dimensional image on a screen connected to the microscope. This three-dimensional view allows the examiner to identify the various layers of the paint, its colors, and its characteristics (Bell 27). The examiner can differentiate the layers of the paint to possibly identify the age differences between layers based on the discoloration of each layer. Any other colors used and the different types of paint present can be uncovered, revealing whether there is a previous painting present on the canvas or if the painting was possibly restored.

Scanning electron microscopy is a technique that allows for the visual examination and detection of elements contained within the artwork. This technique requires the use of a unique microscope unlike the one described above. This microscope has a greater magnification range and depends on the use of a “beam of electrons” that passes through the paint sample, producing a detailed image based on measurements of the molecules’ reactions to exposure to the electrons. The powerful magnification ability of this microscope allows the examiner to analyze minute structures that would otherwise go undetected by other microscopes. The detailed three-dimensional image produced can be used to identify the layers and the elements contained within them. Scanning electron microscopy can also produce a “backscattered electron image” (Douma). This three-dimensional image allows the examiner to distinguish elemental differences in the paint’s composition by way of light disparity, as “areas with high average atomic number appear light in the image and areas with low average number appear dark” (Douma).

The North Carolina Court System Office of Indigent Defense Services’ Forensic Resources page provides detailed information about the use of chemical analysis tests. Chemical analysis tests can be used on micro-samplings of paint to gain a composition make-up of the paint pigments. When using this method, the examiner will be able to date the pigments. Two types of chemical tests can be run, a solvent test or a reactant test. When using the solvent test, the paint pigment samples are placed in known solvents with specific solubility factors and properties. Depending on the elements present in the paint’s pigment and its solubility factors, the sample may react in many ways. The most notable reactions of paint samples in solvents are “dissolving, swelling, curling, and softening” (North Carolina Department of Justice, “Trace Evidence”). For example, to verify that a forged painting contains acrylic, a small sample of paint is placed in a solution of chloroform or acetone, and if it is acrylic it will dissolve. This reaction allows the examiner to date the painting as having been produced after 1950, as acrylic paints were not available commercially until 1950. The chemical reagent test is similar to the solvent test; however, it only requires a drop of a chemical for a spot test. A paint sample is placed either in a petri dish or on a slide and is tested with a reagent. The reagent that is mainly used is diphenylamine solution. The diphenylamine solution is prepared by mixing one gram of diphenylamine with 40 milliliters of water and 200 milliliters of concentrated sulfuric acid. A drop of the diphenylamine solution is placed onto the paint sample and examined under a microscope to observe any reaction. When subjected to a diphenylamine solution, a paint sample that contains nitrocellulose will present a cobalt blue color. This reaction dates the paint between the late nineteenth century and early twentieth century, when this nitrocellulose compound was used. The diphenylamine solution test can also be used to date the canvas used for a painting in question. Older canvases were made from cotton and/or wool, and a diphenylamine test can be used to identify these materials (North Carolina Department of Justice, “Trace Evidence”).

Dendrochronology is the technique used to identify the age and type of wood. This method allows the examiner to analyze wood panels or
canvas stretchers to identify the age of the materials, authenticating some paintings in the process. Dendrochronology requires the use of a wood sample collected from the center of the wood panel. From the sample, the tree rings are counted, providing "the time at which the tree rings were formed, down to the exact calendar year" (Douma). Identifying the type of wood used for the panel is possible, as this technique was founded on the notion "that certain species of trees produce wide rings during the wet years and narrow rings during dry seasons" (Douma). From this information, the type of tree used can be identified by narrowing the geographical location in which trees of that species are located. The information gathered from this process allows the examiner to confirm or deny the supposed facts about the painting. For example, the authenticity of a painting said to be by a French artist from the 1800s can be confirmed by using the rings. The varying sizes of the ring patterns can be used to confirm whether the wood used for the panel could have been located in France (Douma).

Carbon-14 dating is a technique used to identify an approximate age for items derived from "bone, cloth, wood, and plant fibers" (Douma). Carbon-14 is a radioactive isotope of the carbon atom naturally found in the air, which is created by an interaction between a charged neutron and a nitrogen atom. This technique requires the use of mass spectrometry to measure the half-life of Carbon-14, which is the amount of time it takes for half of the carbon-14 atom to decay. This measurement of the atom's half-life allows the examiner to estimate the age of the canvas used for a painting. Using the general knowledge of the atom's half-life, which is between 5,715 to 5,730 years, a painting on a canvas that is 540 years old would have five percent less carbon atoms when compared to a newer canvas, as one-tenth of the atoms decomposed (Bell 59).

Mass spectrometry is the most complex technique used to analyze questioned artwork. The use of mass spectrometry allows the examiner to gain a detailed breakdown of the tested sample collected from the artwork. The mass spectrometer can analyze the complex structure of the paint sample through a series of internal processes of ion charge changes and bond breaking, causing the separation of each molecule. The presence of certain molecules and the amount in which each molecule exists in the sample is measured through data sets. These data sets are presented as a graph of peaks. From the data set, the examiner can "investigate the biomolecular, organic or inorganic components" of the artwork (Spoto and Grasso 857). The natural physical changes that occur in a painting due to "long-term exposure to the environment" (Spoto and Grasso 857) and the effects that occur as a result of restoration can be identified using mass spectrometry. Mass spectrometry is often paired with another process, chromatography, to aid in the chemical breakdown of the sample before it goes through the mass spectrometer. The chromatography techniques that are used along with mass spectrometry are gas chromatography, laser desorption ionization, and direct temperature (Calvano, et al. 6957 – 6981).

Gas chromatography combined with mass spectrometry is "the most frequently used technique in the characterization of organic constituents in paint layers, ranging from natural varnishes to synthetic pigments" (Calvano, et al. 6958). Gas chromatography requires the examiner to dissolve a paint sample in a solution for testing. Once the sample is dissolved, the sample solution is placed into a gas chromatography machine. Once heated, this machine separates the sample by gas, based on the elements' ability to evaporate. The evaporated elements then float through a tube that is connected to the mass spectrometer. When using gas chromatography, the elements' presence in the "organic materials," as well as the products produced by the gas separation, can be identified (Calvano, et al. 6958). Gas chromatography can be assisted by pyrolysis, allowing the analysis of "both synthetic and natural materials" (Calvano, et al. 6959). When using the pyrolysis method, the elements in the testing sample are heated to create decomposition and separation. These separated molecules are further broken down by the gas chromatography technique. Pyrolysis gas chromatography is considered the "gold standard technique for the characterization of synthetic resins and pigments, and the analysis of traditional binding media and varnishes" (Calvano, et al. 6960).

Direct temperature combined with mass spectrometry is an "effective technique for characterizing mainly organic and some inorganic components present in paint layers" (Calvano, et al. 6971). This technique allows the examiner to analyze a wide range of materials and is sensitive enough to detect small molecules within a sample. The direct temperature technique requires a drop of liquid sample, created using a solvent, that is placed onto a filament wire that separates individual molecules in the sample through heat, while the solvent used to produce the sample is evaporated. This technique is best used for analyzing "natural and synthetic resins and pigments in modern paint materials" (Calvano, et al. 6971).

Matrix-assisted laser desorption ionization, combined with mass spectrometry, allows the analysis of "large, non-volatile, and labile biomolecules such as DNA, proteins, peptides, sugars, and large organic macromolecules" (Calvano, et al. 6962). This method is unique in that large structured elements that would otherwise not be detected or would be destroyed by other techniques can be analyzed. This method's level of sensitivity is also unique, as it can detect very small traces of elements in a sample. The capabilities of this technique are important when analyzing questioned artwork, as "historical paint samples are often available as very small fragments of high complexity typically composed of a heterogeneous mixture of organic and inorganic materials" (Calvano, et al. 6962).

**NONINVASIVE TECHNIQUES**

The scientific analysis of artwork using noninvasive methods involves various techniques that allow for enhanced visual examinations of
the artwork in question. Noninvasive techniques are like invasive techniques in that they can range from a simple microscopic examination to a detailed multi-step process requiring the use of sensitive technical equipment. Nevertheless, noninvasive techniques allow the artwork in question to stay intact. The methods of examination are addressed below in ascending order of complexity.

A detailed visual examination of the questioned artwork’s surface, including the outermost layer of paint, the canvas, and the frame, if present, can be completed by the examiner with the use of a stereoscopic microscope. This surface examination allows for the analysis of any concealed characteristics or defects in the artwork. The three-dimensional image produced by this process allows the examiner to identify the painting style of the artist. The observation of the long or short and soft or hard brush strokes, the use or overuse of a specific color or colors, and the type of paint used can provide tell-tale signs to identify an artist. Further observation of the brush strokes allows for the identification of the type of brush used, which can help with the identification of an artist, and even with dating the painting if the type of brush used was manufactured and available within a specific period. The detailed view of the painting's surface allows the examiner to analyze the characteristics of the paint's condition. The observations of flaky, dry, glossy, rough, smooth, cracking, or discolored paint can help identify the type of paint used and the age of the painting. For example, acrylic can be distinguished from oil paints because of the rough-looking texture created by the retention of brush marks and the greying or discoloration created as acrylic paint ages and is exposed to the particles in the environment. The examination of the canvas allows for identification of the material's fibers and possible age. For example, prior to the early nineteenth century, canvases were made from linen and hemp, so if the canvas fibers match with cotton, the date of origin of the painting would be from 1801 or later. The visual examination of the frame may not result in an identification of the material used if it has been through painting or another process; however, if the frame is wood, the type of wood used can be identified and dated using its rings (Bell 27; Chappell and Hufnagel 95-96).

The implementation of electromagnetic radiation, more commonly known as x-rays, allows for the analysis of the concealed characteristics or defects underneath the artwork's surface that cannot be detected from a visual examination, but may be suspected from the examination. According to Thea Moran, et al., “x-rays have a longstanding role in the forensic examination of cultural properties,” (Moran, et al. 38) as the first painting examined using this technique was examined in the 1890s (Moran, et al. 38). Four types of electromagnetic radiation can be used in the examination of questioned artwork: x-ray radiography, x-ray fluorescence, proton-induced x-ray excitation, and neutron activation (Moran, et al. 38-44).

X-ray radiography (XRR) is the basic x-ray type and the oldest technique used in the analysis of artwork. When using XRR, the painting is placed in a ‘nondependent’ upright position, with the outermost layer facing the image detector. When photographed, the painting is subjected to grenz rays, which possess long, mild wavelengths that pass through the painting to produce a detailed image. From this image, the examiner can detect cracks hidden within the various layers of paint and the presence of holes created by worms eating the wooden supporting structure of the painting. These findings can be used to date the painting. Evidence of previous works, in the case of reused canvases, sketches drawn during the planning of the finished piece, or the process in which each layer of paint was applied can be identified. The analysis of these characteristics can assist in the identification of a well-known artist (Moran, et al. 40).

X-ray florescence (XRF) is a combination of the x-ray and spectrometry techniques. The use of this technique allows the examiner to identify the painting’s composition. The XF technique requires the painting to be x-rayed similar to the XRR process, but it differs in that the image detector is connected to a spectrometer. When the painting is x-rayed, several rays pass through the painting, causing the molecular structure to become unstable. The structure regains stability through bond breaking and charge changes that result in a release of energy by each element. The energy released by each element is detected by the connected spectrometer through two different processes - energy dispersive analysis (EDA) and wavelength dispersive analysis (WDA). The EDA method detects the energies from the elements and “amplifies” them, producing a data set of results displayed as peaks, with variations of each element in each peak. The WDA method detects the energies as wavelengths. These wavelengths are measured to produce a data set similar to that of the EDA, except each element is identified by one peak (Moran, et al. 41-42).

The proton-induced x-ray excitation/emission (PIXE) technique is similar to that of the XRF; however, it differs in that “high energy protons” are passed through the painting as opposed to x-rays. These protons cause instability of the painting’s molecular structure. The structure regains stability through bond breaking and charge changes, resulting in the release of energy by each element, which is measured by the spectrometer using the energy dispersive analysis method discussed above. The equipment for this technique is extremely sensitive and only a small amount of material is necessary for the elements to be identified. While this technique is very useful in helping the examiner identify all the elements present in the paint pigment, the “high energy protons” emitted through this process could possibly damage the painting (Moran, et al. 43-44).

Neutron activation (NA) is the most unusual electromagnetic radiation technique that can be used to analyze artwork for authentication. NA is like the PIXE technique in that it can identify
minute amounts of elements contained within the painting. It differs, however, in that this process reduces the possibility of the painting being damaged. This process requires the use of neutrons to destabilize the molecular structure of the painting and measures the gamma rays and beta particles emitted from each element during the re-stabilizing of the molecules. A data set is produced by the spectrometer based off the gamma readings, while an image is produced using the beta particles. This process must be run several times to have a clear image and a separate data set for each element (Moran, et al. 44).

Attenuated total reflectance Fourier transformation infrared spectroscopic microscopy (ATR-FTIR) is a technique used to analyze the elemental composition of paint in artwork. Extensive research suggested that ATR-FTIR was an invasive technique requiring the use of micro-samples of paint from the artwork in question, as the crystal used for reflecting the light requires evenly flat, direct contact with the artwork. Direct contact on a painting that may not be entirely flat can damage the painting as well as the crystal. Nevertheless, recent case studies have shown that “non-destructive” surface analysis of the paint can be conducted. In one case study, researcher Adriana Rizzo found that “an ATR-FTIR microscope featuring a crystal of optimized geometry and a viewing capability feature allows characterization of individual layers, or areas within layers, of 10 u.m thickness or less in single measurements. A remote aperturing feature with the microscope allowed the analysis of selected area” (Rizzo 47). The technique used in Rizzo’s study allows the examiner to analyze the molecules located in thin layers of paint without having to scrape or separate each layer. The existence of former paint elements from deterioration or damaged paintings can be analyzed. The examiner can also analyze questioned artwork where the forger may have applied only one layer of paint over a used canvas, without contaminating the previous paint layers (Rizzo 48).

Raman microscopy is a technique used to analyze the artwork to identify the molecular structure and elemental components of paint. “Advancements in optics and detector technology” allowed for the development of Raman microscopy (Clark 74). This technique is often used to examine micro-samples of paint taken from artwork; however, recent studies conducted have shown results from an analysis taken from the actual painting without any destruction or sampling. This technique requires the artwork in question to be subjected to a “laser beam” of light. The painting’s exposure to the light results in a reaction in which energy is given off by each element present in the artwork, and this energy is measured by the detector and presented in a graph of peaks and values. When reviewed, this data allows the examiner to identify the elements present (Edwards 14).

Infrared reflectography is a technique that can be used to detect the presence of sketches and other related items underneath the surface of the examined artwork. This technique requires the use of an infrared camera, which is used to take a photograph of the painting. The ray of light from the camera passes through the painting, allowing the camera to capture an image of items that have absorbed the light. This image will allow the examiner to identify possible tell-tale signs of an artist. For example, if an artist failed to sign his or her artwork after completion, but the image captured reveals a signature on an earlier sketch, that could identify the artist. The style of the drawing or the sketching process used can also allow the examiner to identify the artist, as some artists had a tendency to draw pictures of items that aren’t intended to be included in the artwork (Douma).

Ultraviolet fluorescence is a technique that can be used to identify organic paint elements and the presence of natural protective finishes on the painting’s surface. This technique requires the use of an ultraviolet light source that will be shone directly on to a painting at a 45-degree angle, causing a reaction that can be captured as an image using a camera. The light projected is absorbed by the painting and, depending on the elements’ scientific properties, energy is given off by way of fluorescence. The inorganic elements within the painting will not emit light and will remain dark, allowing the examiner to distinguish between the two types of elements present in the painting. The elemental differences allow the examiner to differentiate original pieces from restoration work. Depending on the artwork’s condition, parts of the artwork that are beginning to fade can be identified. This discovery of the artwork’s faded parts can be used to identify an artist known for using materials or techniques that might fade. The usage of organic materials within the painting can aid in dating the painting through further analysis (Douma).

Optical coherence tomography is a recently discovered noninvasive technique that can be used for a comprehensive surface examination of artwork. Prior to this technique’s recognition for scientific analysis in the art world, optical coherence tomography was only considered as a “medical imaging method for detecting eye disease” (King 1248). This technique requires the scanning of an artwork’s surface. During the scanning, the “instrument” exposes the painting to “infrared radiation” of varying strengths and wavelengths, causing a reaction in the elements in the painting (Targowski, et al. 828). The reaction produced causes the elements to reflect light, which is measured by the instrument to produce an image of the different layers. The use of optical coherence tomography allows the examiner to identify the number of layers in the painting without the need for a physical sample from the artwork. The recorded wavelength signals dispersed at the time of scanning can help the examiner to identify the elements present, as all elements have unique reflective properties. The use of wavelengths to identify elements through this technique has not been discussed; however, other techniques illustrate the use of wavelengths in identifying elements in a painting (Targowski, et al. 826-828).
CONCLUSION

The scientific analysis of artwork by means of either invasive or noninvasive techniques for authentication is the last recourse in detecting forgeries. Following the examination of provenance and historical context, these techniques can be used to answer additional questions that surround the painting’s authenticity. The questioning of provenance based on disputed documents or the lack thereof, can be answered using scientific analysis. The identification of synthetic or inorganic material in the painting and canvas may allow the examiner to disprove the supposed date of the artwork, because it’s generally known that the earliest works of art were created using natural materials for paint pigment and canvases. The suggestion of simulated or insufficient historical context clues can be analyzed using scientific techniques. The use of alternative light sources, such as infrared and ultraviolet, allows the examiner to discover sketches and other items that may be tell-tale signs of a particular artist. These signs can be further confirmed by the analysis of paint pigments using either an invasive or noninvasive technique.

Nevertheless, the examiner must evaluate the “risk of damage” versus the information that can possibly be obtained before the implementation of scientific analysis. The assessment for making such decisions must take into consideration the questioned artwork’s current condition. If the painting is distressed or showing signs of deterioration, collecting a sample for testing could cause further damage, diminishing the likelihood of repair. Scientific analysis of artwork would not be justifiable if plausible evidence of authenticity is presented when examining either the provenance or the historical context. Subjecting the artwork to unnecessary tests that could decrease its value if it is damaged and may require restoration would not be recommended. Because of these risks, the examiner’s decision may be to forgo scientific analysis and rely only upon historical context clues (Ortega-Aviles, et al. 165).

Furthermore, the advancements in technology have generated techniques suitable for analyzing artwork for authentication without the need to modify the painting. These noninvasive techniques require only a visual examination of the artwork’s surface to produce data reports to aid in the identification of elements and materials used to create the analyzed painting. The alternative light source techniques allow the “underdrawings” of multiple layers of paint to be discovered without a painstaking process, allowing questionable artwork to be examined for concrete evidence of authenticity without the concern of damaging a potential priceless piece. This benefit, confirmed by research exploring both invasive and noninvasive examinations of artwork for authentication, suggests that noninvasive techniques are as effective as invasive techniques in the detection of forged artwork, with the potential of noninvasive techniques surpassing invasive techniques as the preferred method for scientific analysis.

WORKS CITED


**ALISIA ALEXANDER**

Alisia Alexander, a graduate of Virginia Commonwealth University, with a BS in Criminal Justice. Alisia is currently enrolled in the Forensic Studies graduate program, focusing on the Interdisciplinary track to blend her interest for further learning in criminalistics and investigations. Alisia has served with the Department of Justice since 2010.
Forensic Accounting: 
The Terrorism Explosion
Amber Seibel

The terrorist attacks on September 11, 2001, dramatically influenced the forensic accounting field. The attacks were orchestrated by terrorists seeking to destroy America from inside the country, and were funded through legitimate and illegitimate sources. Part of the job of a forensic accountant is to discover how terrorists obtain funds, trace those funds through both legitimate and illegitimate sources, and present their findings in a court of law. They also serve as the middle man between the books and the law, and do all of this while looking for ways to cut off terrorist funding. Perhaps if forensic accountants had been as prevalent before the attacks as they have been since, the attacks may have been prevented. In the aftermath of the terrorist attacks, the forensic accounting workforce increased a great deal. Based on numerous articles discussing the growth of forensic accounting, the evidence suggests that the growth of forensic accounting within the United States can be attributed to the advancements that have complicated the identification of the money trail associated with terrorism and fraud.

In order to understand the forensic accounting field, a person should understand the role an auditor plays in financial analysis and how the role differs from that of a forensic accountant. Walking the line between the books and the law, a forensic accountant must know both inside and out. They are also responsible for finding irregular transactions by looking at each transaction singularly and in depth. The field requires additional knowledge of laws, business organizations, and patterns to enable the forensic accountant to gather all of the important facts. Forensic accountants must also ensure their investigations and findings are able to be presented in the court system. Presentation and audience are the biggest differences between the forensic accountant and the auditor.

Auditors, on the other hand, study the records of an organization to make a judgement on whether or not the representation, provided by the financial statements, is fair. In the past, auditors have been tasked with the detection of fraud; however, businesses have grown in size and scope, effectively removing the possibility of auditor detection of fraud (Smith 18-19). Material fraud is the only type of fraud remaining in the auditors’ purview because it focuses on significant departures from Generally Accepted Accounting Principles (GAAP). The court system agrees however, that auditors have limited liability when it comes to fraud detection. In 1994, the Supreme Court issued a ruling to limit the liability of auditors and other secondary parties when fraud takes place in a company they have worked for (Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164 (1994)). Evidence suggests that when comparing the job responsibilities of auditors to those delegated to forensic accountants, forensic accountants are more effective than auditors in tracking terrorism and assisting with fraud prevention.

A relatively new responsibility of forensic accountants is assisting with the creation of a system to prevent fraud. Professor of Accounting, Madan Lal Bhasin, mentions that corporations should use a forensic accountant’s knowledge of financial accounting, internal controls, laws, fraud, specific market information, investigational techniques, and relationship skills to create and implement a corporate governance system that works together to stop fraud (7). Since a forensic accountant has knowledge about most aspects of an internal control system, a company needs to implement strong controls as recommended by the accountant. These recommendations include separation of duties, punishments to adequately deter fraud, and methods to monitor, correct, and control failures (9). Overall, the forensic accountant can assist in the prevention of fraud in more ways than just analysis of transactions.

Before discussing how a forensic accountant conducts his or her investigation, it is important to understand how fraud and terrorism are related. The main objective of terrorism is to scare people into acting or not acting, depending on the situation. The attacks of September 11, 2001, were some of the most widely publicized terrorist acts in history and they resulted in widespread fear and confusion. The attacks proved to be what pushed many countries across the globe into what became known as the War on Terror. The countries soon established that the best way to prevent more terrorist attacks would be to cut off funding to terror groups as a whole. If the terrorists had no way to make money, they would not be able to commit these terrible crimes. Fraud and money laundering are just a few of the many ways that terrorists gather funds for their organization. Forensic accountants never complete a terrorism investigation without finding traces of fraud here or there.

Without the added responsibility of determining if the financial statements are fair, forensic accountants are able to focus on transaction analysis and the discovery of inconsistencies. In some cases, forensic accountants must first extract the data they need to analyze from computers, as well as mobile or other electronic devices (Smith 20). As the accounting process is increasingly computerized, technological skills are important to forensic accountants. Once the data is extracted, it can be analyzed in a number of ways, including alter ego, fraudulent transfer or conveyance, solvency, Benford’s Law, expectations-based statement analysis, genograms, proxemics, and timeline analysis. Throughout all stages of the investigation, forensic accountants will need to maintain accurate records documenting their investigation to present at court.

Since forensic accountants are conducting an investigation, they use some of the same techniques that detectives use. According to Dorrell and Gadawski, the authors of Financial Forensics Body of Knowledge, forensic accountants may use the expectations-based statement analysis, genograms, proxemics, and timelines. Expectations-based statement analysis will offer the accountant some insight as to which statements are more apt to be truthful based on the speaker’s word choice (341). Genograms are diagrams showing information
discovered to date, and can include information such as relationships between companies and creditors, as well as personal relationships that could affect company leadership. Proxemics make an investigator aware of how a speaker uses their body within the space around them; it is similar to body language (341). Proxemics are used the most when a forensic accountant is conducting interviews and interrogations of the individuals close to the situation. The technique can provide valuable information as to whether the speaker is telling the truth or if some small detail is more important than it seems. In addition to these general techniques, forensic accountants have many financial analysis techniques available to them: Benford's law, alter ego, fraudulent transfer or conveyance, solvency, the gross profit margin test, the modified net worth method, and the source and use of cash method.

Benford’s law is a recently established tool that requires use of some of the other techniques as support. The financial data is analyzed in four distinct places: the first digit test, the second digit test, the first-two-digit test, and the first-three-digit test. In general, Benford’s law holds that there is an anticipated pattern in the numbers and number sequences provided in financial data (Dorrell and Gadawski 379). If the anticipated pattern is not found, errors, fraud, or irregularities are present in the data. Benford’s law provides an important starting place for more in-depth investigation. In order to establish where the specific problem is, the alter ego, fraudulent transfer, and solvency techniques should be used.

Alter ego is a technique that is used heavily in forensic accounting investigations. According to Dorrell and Gadawski, alter ego can be used to bring owners of companies, which are normally protected by the structure of their organization, to justice (340). This technique also provides the best chance to identify and break terror funding trails (343). The alter ego technique requires many of the bodies of knowledge mentioned earlier, but specific market knowledge is the most important. Alter ego can establish if a parent company oversteps its control over a subsidiary. This is accomplished by looking specifically at whether too much control was exerted, if fraud occurred, and if the subsidiary was harmed by the control and subsequent fraud (344). If it is determined that alter ego exists, intercompany transactions should be viewed to find the fraud that resulted in incorrect figures. Documentation of conducted analyses will allow the forensic accountant to present his or her investigation in court against the suspected terrorist or another criminal.

Another analysis that is typically used by forensic accountants is the fraudulent transfer technique. This technique looks at the debtor-creditor relationships of a company to determine if any transfers have been made incorrectly. Using knowledge of bankruptcy laws, the forensic accountant is looking specifically for incorrect valuations that harm the rights of the creditor (Dorrell and Gadawski 372). Solvency tests can be conducted in combination with the fraudulent transfer technique in order to uncover situations that are possible warning signs for fraud, or to uncover fraud itself. If suspicious transactions are found, solvency tests can establish whether a business is in relatively good standing or has the ability to pay its bills. If a company is found to not be in good standing, fraud may be the cause, and transfers should be scrutinized in more detail (Dorrell and Gadawski 374-375). Findings from these tests can then be presented in court against the suspected terrorists. The aforementioned tests are generally used when investigating company data; however, there are techniques that can be used specifically for an individual suspected of terrorism.

The modified net worth method is a great tool to use against a suspected terrorist. Dorrell and Gadawski describe this method as a way to “[determine] the increase in [the suspect’s] wealth by deriving the year-to-year change in his overall net worth” (409). The accountant would begin by subtracting the previous year’s net worth from the current year. The result represents a portion of the suspect’s income for the year. Living expenses are added to the result, leaving a sum that represents total expenditures during the year. Essentially, the sum represents all income for the entire year. Known income is subtracted from that number to establish the amount of money that has an unknown source. It can then be assumed that the excess was acquired through terrorist financing methods. According to Dorrell and Gadawski, this analysis can be presented in court as circumstantial evidence (409). While the findings can be used as evidence, they can, more importantly, identify connections and suspicious transactions that need to be studied with more focus. The modified net worth method is very similar to the source and use of cash method, which can be used to confirm the net worth findings.

The source and use of cash method can be used as a confirmation of the modified net worth method. This method can provide a way to track terrorists that maintain a very low profile (Dorrell and Gadawski 411). The method begins by totaling the individual known sources of cash and subtracting each expenditure. If expenditures exceed known cash sources, there are unknown sources of cash, most likely related to terrorism. The findings can be used during court proceedings in the same manner as those of the modified net worth method, and can highlight business and individual connections, as well. The use of genograms and timelines, including information found using these financial techniques, can help the investigator recognize connections that would have otherwise been overlooked. Financial techniques are evolving and will continue to do so as reporting requirements change across the globe. When financial techniques are used in conjunction with investigation techniques, the power of these financial tools seems to be limitless.

The generic investigation techniques employed by forensic accountants have been used for many years, but the financial techniques used have only been established more recently. Chancellor Gordon Brown held a role similar to that of the United States
Secretary of the Treasury for the Queen of England. Chancellor Brown has pointed out that the combination of new techniques and existing market knowledge should be able “to create a modern version of Bletchley Park,” a World War II code-breaking installation (Percy 1). Forensic accountants can now use techniques like alter ego, fraudulent transfer, the modified net worth method, and Benford’s law to reach the level Chancellor Brown described. Since these financial techniques are mostly products of changing laws and increasing investigations of terrorists and terrorist organizations, it is clear that the major cause of the growth of the forensic accounting field is unrelated to the number of terrorist acts. The introduction of these new and modified techniques, specifically for use in the detection of terrorism and associated money laundering, has provided for increased detection of fraudulent activities.

There are a few other techniques used to detect fraud and terrorist financing that are generated based off of business and personal requirements. Forensic accountants have established a method of financial profiling that can be used to recognize red flags that can associate an individual or an organization with terrorist financing. Dorrell and Gadawski note three main needs that can be used to profile terrorists: physiological needs, communication needs, and mobility needs. Money trails will be associated with buying items that are similar to the basic needs of all individuals: food, water, clothing, and shelter (392). Shelter may provide the most substantial amount of evidence among the physiological needs of a terrorist because it requires the most amount of paperwork and identification to acquire. Communication is important to a terrorist, mainly for planning purposes (392-393), and most forms of communication, like e-mail or cell phone use, will provide records that a forensic accountant can use to profile and find connections. Mobility is the final need for terrorists that can be tracked; public transportation is preferred over purchasing a vehicle or using airplanes due to the records involved in both methods (393). After analyzing each need, forensic accountants can investigate the financial data left behind.

While the typical citizen is not very concerned with leaving behind records of their transactions, a terrorist is hoping to avoid detection at all costs. It is typical for a terrorist to maintain only a checking account with an associated debit card, leave a post office box as the address of record for the bank, and have small deposits and withdrawals so as not to draw the attention of reporting requirements (Brooks, et al. 16). Each of these methods of reducing detection is a red flag to an investigator, who must be aware of the typical banking habits of a terrorist. An interesting note to mention is that many terrorists are discovered for crimes related to minimizing their personal connection to terrorist financing. In order to minimize involvement, many terrorists steal identities to avoid personal detection. In fact, terrorists can use stolen identities to meet some of their needs, such as using a fake identity to take advantage of the food stamp program.

Governments are just as susceptible to terrorist abuse as any other business. Richard Brooks, Richard Riley, and Jason Thomas wrote an article for the *Journal of Government Financial Management* highlighting how terrorists can take advantage of government assistance programs. Specifically, the article mentions the exploitation of the food stamp program, unemployment benefits, health care programs, workers’ compensation allowances, and other welfare programs (13). Because of the vulnerability of government programs, there is an important role for government accountants in monitoring “suspicious financial relationships and transactions,” as well as “pursuing anomalous observations” to maintain and even increase the integrity of the assistance programs (17). If government accountants take on these responsibilities, they will be able to assist the forensic accountant’s investigation by providing information already on record from any suspicious activity investigation. Since many forensic accountants work for the Federal Bureau of Investigation (FBI) or other governmental bodies, it is important that they work together with government accountants to handle the overlap between their jobs. Terrorists move their money through many different organizations, and the classification of each organization is very important to the investigation process.

Forensic accountants must be sure to record organizations, countries, and financial institutions that the terrorist money travels through as part of the financial profiling. International organizations maintain classifications of organizations based on their involvement with terrorism. The listed organizations may be recognized as part of a terrorist group or as sympathizers to the terrorist cause. The classification of “noncooperative” means that an establishment does not help with discouraging terrorist efforts. The use of organizations labeled with any of these classifications is a clear red flag of terrorist financing. Once the investigator determines whether an organization is found on a flagged list, the focus can shift to analyzing financial data. Organizations provide another level of recordkeeping that is very important to the forensic investigation for fraud or terrorism.

Organizations that operate within the United States are required to meet GAAP standards by creating a set of financial statements at a minimum of once per year. These financial statements can provide indicators of fraud to a forensic accountant. Common-sizing is a method that converts financial data into a percentage of assets when studying the balance sheet, and revenue when studying the income statement. Once these percentages are established, they can be compared to a company’s competitors and to the company itself over time. The gross profit margin comparison test is very similar to common-sizing and can also be used on the financial statements. Once the gross profit margin of a company is calculated, it is compared to itself over time and that of the company’s competitors. Any significant changes in either the common-sizing percentages or the gross profit margin amount can indicate a problem that requires further investigation.
The accounting field is cognizant that the balance sheet and income statement have been around for a long while, and that the cash flow statement, however, is a newer requirement. Dorrell and Gadawski point out that the irreplaceability of the cash flow statement lies in the fact that it starts and ends with cash; it has no room for manipulation because it deals only in cash (403). Any incorrect cash transaction would be extremely noticeable on the cash flow statement, allowing the accountant to immediately flag the transaction and investigate further. As businesses become used to the preparation of the statement of cash flows, they may find methods of hiding fraud that are not easily identifiable to an accountant. Terrorists may find issues navigating around the new rules to begin with, but eventually they will find a method to exploit the new rules. Financial statement analysis and forensic investigation techniques are assisted, however, by the changing legal environment surrounding not only reporting requirements, but terrorism and money laundering laws as well.

The laws that apply to businesses describe the standards that businesses are held to when reporting and record keeping are established. Bhasin points out that the standards in the United States are the most specific and demanding in the entire world. The problem however, is that businesses that are under constant stress to succeed may have employees that are more likely to work around the system to make the company look viable. (5). Many of the standards in the United States can be attributed to the Sarbanes-Oxley Act of 2002. With the passage of the Sarbanes-Oxley Act, the Public Company Accounting Oversight Board (PCAOB) was created, strengthening auditing requirements by providing oversight and monitoring of public company audits (Shim 849). The act also requires that leadership take more responsibility for the company's financial data, and this has added further stress on management to present the company in the best light (890). The reporting environment can only become increasingly more regulated as businesses continue to evolve and investors begin to request more information before investing in a company.

When it comes to terrorism, the legal environment is very specific as well. In early 2000, the United States National Money Laundering Strategy identified financial organizations that were subject to the strategy and called for punishments when a financial crime was discovered (Norton and Shams 106). This strategy provided the basis for the laws that were enacted after the horrors of September 11, 2001. The strategy also proves that laws cannot be the only tool used in the War on Terror. September 11, 2001, occurred only about a year and a half after the new framework was put into place to cut off money sources for terrorism. Leadership in America felt that it was necessary to enact new rules that would provide even more results.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, also known as the USA PATRIOT Act, was one such law established after September 11, 2001. This act's goal is to prevent terrorists from using the American banking system as a way to fund their exploits. Normah Omar, a member of the accounting staff at Universiti Teknologi MARA, describes the subsequent widespread adoption of similar laws all over the world. Omar has found that these laws are affecting the opinion of Islamic Financial Institutions (IFIs) across the globe (166). Due to the relationship between Muslims and the 2001 attacks, it can be difficult for IFIs to gain support and be regarded as beneficial. The opinion of these institutions has the ability to affect how terrorists use IFIs and the complexity of the money trail accountants must follow. A negative opinion could leave IFIs extremely vulnerable to terrorist use, if others begin to avoid using financial institutions backed by Islam.

The World Bank has a significant role to play in the legal environment due to the international nature of terrorism and money laundering. Developing and emerging economies have the most to lose since their economies rely heavily on all transactions. Pierre-Laurent Chatain, a financial sector specialist for the World Bank, describes the bank's efforts to fight terrorist financing and money laundering as "(i) carrying assessments, (ii) granting technical assistance, (iii) conducting research, and (iv) gathering data" (191). Once the World Bank assesses a country's strengths and weaknesses, a plan can be created to intensify efforts to fight against money laundering and terrorist financing. The international scale of terrorism has become common knowledge since the attacks of September 11, 2001, which has led to the demand for an international fight against the problem; the World Bank leads the globe, along with the help of the Financial Action Task Force on Money Laundering (FATF), against terrorism.

The FATF was created for the sole purpose of combating terrorist financing and money laundering internationally. It is with increasing difficulty that the FATF continues the fight. The information age has not only made the discovery of these crimes more difficult, it has challenged the regulatory bodies hoping to issue laws to stop the problem. The FATF has only been able to require that a country assess the risks of adopting new technology instead of making laws that prohibit certain technologies or uses of the technology, according to Rick McDonell, former Executive Secretary of the FATF (para. 7). McDonell also mentions the specific hazard presented by new payment methods, such as Internet payment options and cell phone payments (para. 8). The Internet has caused a shift in accounting and reporting practices that affect forensic accounting investigations immensely.

The Internet reaches all across the globe and has information on every topic known to mankind. When the Internet first became popular, regulations were few and far between because it was a new and unknown tool. In the beginning, terrorists turned to the Internet to gather support, raise money, and pass instructions to other members. The focus however, was on spreading the message, “that supporting
the *jihad* in some fashion was an obligation incumbent upon every Muslim*" (Jacobson 354). Websites helped to fulfill the basic terrorist need for communication. Unfortunately, the need analysis mentioned previously was not established until after the attacks of September 11, 2001. As the Internet spreads, more and more websites have become associated with terrorism. Michael Jacobson, a member of the Stein Program on Counterterrorism and Intelligence, puts the expansion into perspective by quantifying the increase: the number of terrorism-related websites jumped from 12 to 2,600 in the span of eight years (354). During this time, terrorists also worked to increase their usage of the Internet to gather and move funds from all over the globe.

The Internet facilitated the terrorists’ expansion of illegal activities used to fund their organizations. With the world at their fingertips, terrorists were able to steal credit card information from anywhere in the world. False charges to these stolen accounts could be made through the online purchase of supplies, or through gambling websites, from which the winnings could be transferred as legitimate funds (Jacobson 355). The advent of the Internet provided numerous new ways to generate funds and legitimize them: the main goal of any money laundering scheme. The Internet also decreased the ability to recognize terrorist activities; terrorists are able to hide their computer addresses and steal from the other side of the globe with no one the wiser. Levels of technological knowledge differ among countries, allowing the terrorists to take advantage of their different weaknesses. International law must change to address the ease with which terrorists are able to manipulate the Internet for their specific needs.

International bodies have discussed regulation of the Internet, to no avail. Many countries do not have the same capabilities as the United States for Internet regulation (Jacobson 359). Furthermore, many countries cannot rival the United States as far as Internet speed, the manpower needed to monitor Internet activity, and the understanding of technology and programming necessary to correct vulnerabilities. Without having these capabilities, a country would never be able to meet international standards. The debate on free speech has also hindered the creation of international standards (360). While China’s past has shown that leadership has no problem restricting which websites its citizens can access, many other countries have strict rules against inhibiting free speech. Until international agreement is reached on the idea of free speech, there is no hope for a unanimous response to Internet regulation. As the developing and emerging economies industrialize and become more dependent on technology, it is possible that a shift towards agreement may occur.

Limitations exist beyond the technological capabilities across the globe. Internationally, there is no requirement for recordkeeping of specific Internet-based transactions (Jacobson 360). The FATF, already an international organization, has access to the necessary data and the audience to create global requirements for international online record keeping. Once these laws are created, forensic accountants will have another layer of data through which to track terrorist financing. The technological environment is constantly changing, and new technologies are continually being introduced. Until the changes to technology slow down, forensic accountants will always be one step behind. There will always be new methods for terrorists to escape detection, as well as the need for new techniques that forensic accountants must create to identify terrorist activity.

Another relatively new area for the forensic accountant to analyze is the international trade arena. Terrorists use trade not only to purchase supplies, but also to transfer funds between countries. Dr. John Zdanowicz, president of International Trade Alert, Inc., describes how terrorists can undervalue or overvalue exports to launder money; the exporter and the importer must be working together in order to capitalize on the situation (Zdanowicz 54). The Internet plays a huge role in relationship creation between importer and exporter and allows for otherwise unconnected individuals to join together to benefit a terrorist organization.

Once the exporter-importer relationship is secure, the terrorist can begin laundering money. The exporter will purchase goods at market rate and will then sell them to the importer for higher than that market rate. The importer pays the inflated rate and leaves the exporter with the extra money paid over the market value. In order to undervalue the goods, the exporter will purchase goods at the market rate and then sell them to the importer at a lower cost. The importer would pay the lower rate and sell the goods for market value, leaving the importer with the extra money. In order to halt these trading techniques, the United States created a law that requires shipment records be provided to the Customs Agency one full day prior to departure from a port (Zdanowicz 55). The implementation of this law allows for the comparison of current pricing data to the shipment information to determine if any of the products are under or overvalued. If an item is determined to be valued incorrectly, the authorities are notified and the fraud can be thwarted. Unfortunately, it is not clear as to what the repercussions are for the exporter when an item is found to be incorrectly valued. Consequences are an important part of any framework and must be included.

The framework for charities and nonprofit organizations have changed significantly in recent years, as well. Jacobson points out that charities are susceptible to abuse by terrorists because the humanitarian purpose for a charity can be twisted by terrorists to support their organization. A charity can easily be reopened under a new name to escape a terrorist connection to any number of previous names (356). Forensic accountants must recognize the importance of any charity that a suspected terrorist’s money is funneled through. Investigation of a charity may help to bring connections to other terrorists to light by using genograms and timelines.
Forensic accountants can follow a general format for their investigation of charities. In the United States, entities that have been connected to terrorism are maintained in list format by the United States Treasury’s Office of Foreign Assets Control. After viewing the list, the accountant will be able to determine if the charity, or anyone supported by the charity, is associated with terrorism (Romaniuk and Haber 48). The information maintained on this list is very important to the forensic accountant and should be kept up to date at all times. The responsibility for this investigation should not be placed only on a forensic accountant, however. Peter Romaniuk and Jeffry Haber, professors of political science and accounting respectively, describe the practices each charity should complete when deciding to whom they will provide support. First, charities themselves should ensure that their support is not provided to an entity listed by the Office of Foreign Assets Control (49). Any legitimate charity should want to ensure that their support is going to those that need the assistance and will use it to better themselves. Supporting terrorism would go against the nature of any legitimate organizations, and any solution that can be used to prevent the supporting of unknown individuals should be put into place.

After grantees are cross-checked with the list, there is no action to take unless someone is on the list. Romaniuk and Haber stress that when this happens it is important to have documented procedures regarding who to contact and how to prevent further terrorist support (49). Forensic accountants can assist in the creation of procedures to ensure that the correct groups are notified of the problem. In order for charities to remain as transparent as possible, they should strive to meet the best practices published by the Treasury Department (49). Publication of financial statements similar to those of a public, for-profit business can help gain potential donors’ trust, as well as provide investigators a place to begin analysis if terror associations are found. Romaniuk and Haber stress that if charities gather information on those to whom they provide support, choose only the most trustworthy grantees, maintain outside oversight, and publish audited financial statements, they will be well on their way to avoiding ties to terror (49-50). Charities can have a huge international reach and must be proactive when it comes to avoiding terrorism by participating in the best practices outlined by Romaniuk and Haber. Receiving the assistance of an accountant can be beneficial in the long run when creating a system for the charity to avoid supporting terrorism. The forensic accountant’s job is made easier when charities use the prescribed practices and have a solid system in place to investigate and report possible terror connections.

Changes were initiated all over the world, in many different areas, to solve the terrorism issue, which only seemed to be getting worse. Across the globe, the number of terrorist attacks as a whole can be very shocking. According to the Global Terrorism Database, maintained by START, the National Consortium for the Study of Terrorism and Responses to Terrorism, a Center of Excellence of the United States Department of Homeland Security, the occurrences began at a relatively low rate in 1970, around 600 attacks. The number of attacks steadily rose from there until about 1990, when a sharp decline occurred through 1998. Between 1998 and 2004, the number of attacks wavered back and forth, around 1,000 to 2,000. During 2001, when America faced tragedy, the numbers were around the highpoint of 2000. Sadly, since 2004 the global number of terrorist attacks has risen sharply to almost 16,800. The numbers for the United States differ greatly from the occurrences of terrorist attacks globally.

The terrorist attacks of September 11, 2001, placed an even higher importance on terrorism and the need to cut off terrorist funding in the United States. Terrorist attacks occurred around 464 times in the United States in the year 1970. The number of attacks decreased steadily up to 2001, when the occurrence of attacks was only around 40. These numbers have decreased even more up to 2014 where the data stops, at about 19 attacks. Based off of these numbers it seems like America should not have much to worry about. The problem is not the number of attacks that occur within the country, but the number of terrorists that use American businesses, charities, and its banking system to generate money for their organizations to use in attacks on other countries.

Many Middle Eastern countries have experienced a huge spike in attacks. For example, Iraq had relatively no attacks until around 2002, when the country experienced a few attacks. The numbers of 2014 tell a much different story for Iraqi citizens. There were about 3,900 attacks just 12 years after the country began experiencing terror-related attacks. Syria has been in the news lately because of the attacks in their country. Before the year 2010, Syria had only experienced attacks in the years between 1978 and 1983. Other attacks have been few and far between. Attacks rose, however, from practically nothing in 2010 to 325 in 2014. It is amazing that four years can bring about such change. Pakistan has experienced the same spike since 2003; attacks went from almost none to over 2,200 in 2014. These numbers may be different depending on how different agencies define terrorism.

The Global Terrorism Database has a specific definition of terrorism that it describes in the Criteria section. First, an act is required to be politically, economically, religiously, or socially motivated. Next, it must be proven that the victims were not the only people the attack was directed towards. In other words, the terrorists must have been trying to share their message with more than just those harmed by the attack. Another requirement for the database is that the act must not be considered part of a war. If a war was taking place, the casualties would be war-related instead of terror-related; the same would be true for those who were injured. The database also allows uncertain cases
to be included in the count and queries whether the attacks that were attempted but did not succeed should be included (START). Each of these requirements can be selected or not, depending on the aspects of terrorism in question.

Terrorism is a widespread topic that covers not only international actions but also domestic threats. Cutting off the money source for terrorism has always been a general goal of the field and that goal has not been limited to one form of terrorism or another. It seems that all of the methods employed by forensic accountants during a terrorism investigation can be used to uncover any category of terrorism. Stopping terrorist income prevents more than just horrific events like those of September 11, 2001; it has the added benefits of uncovering related crimes and preventing unsuspecting victims from supporting terrorist organizations. When forensic accountants succeed in cutting off terrorist access to funds, there is no way of knowing exactly what attacks have been prevented. There is no possibility for forensic accountants to focus on preventing certain types of attacks. There are many other ways to slow down terrorist organizations; money just seems to be the most direct way to reach the goal.

The attacks of September 11, 2001, set in motion many changes throughout the world. The forensic accounting field was very new when the attacks occurred, and the role of a forensic accountant was primarily presenting evidence in court. The role of the forensic accountant has expanded to include fraud and terrorism investigation, fulfilling a new goal of disrupting terrorist financing. In order to accomplish this new goal, forensic accountants needed to develop techniques to assist in their investigation. Adoption of general investigation techniques was beneficial to these accountants, as they could glean more information from the actions of any potential suspects. Once the accountants had some general ideas about which financial records to begin searching, financial analysis techniques had to be established and/or polished to meet the specific needs of a terror investigation. These techniques, as well as the newly required cash flow statements, provided forensic accountants with wonderful new tools to uncover fraud and money laundering where no one would have thought to look before. These new abilities brought forensic accountants into the forefront of the War on Terror and have caused an explosion of growth in the career field. The changing financial environment characterizes only a small portion of the changes made after the 2001 attacks.

Changes to the legal environment within the United States helped to highlight new areas of investigation for forensic accountants. The Sarbanes-Oxley Act and the creation of the PCAOB required public companies to increase their record keeping for certain types of transactions, providing forensic accountants with more documentation to discover suspicious activities. The USA PATRIOT Act and the creation of the Department of Homeland Security were a few of the legal changes that reduced the terrorists’ ability to exploit U.S. businesses and its financial system. The sweeping changes in the United States also caused international discussion of the problem. International organizations, like the World Bank and FATF, have begun to issue international requirements to lessen the impact of terrorism and reduce the ability of terrorists to exploit monetary systems internationally.

While it is clear that terrorism is on the rise across the globe, the United States has actually experienced a decline in terrorist attacks. This means that the explosion of the forensic accounting field is not in direct relation to the number of terrorist attacks within the country. The combination of new laws and financial analysis techniques has brought the profession into the spotlight by providing many new methods to discover different types of terrorism. With the spotlight on forensic accountants, the field has grown immensely in scope. Forensic accountants must have more knowledge than ever before. The growth in the field is in response to the demand for more knowledge and the need to keep up with advancements in each of the knowledge bases. Advancements in every field important to the forensic accountant will increase the responsibilities of the workers, and, as a result, increase the number of workers needed.

WORKS CITED


AMBER SEIBEL

Amber Seibel is a graduate of Stevenson University, where she received her B.S. in Accounting. Amber has been an employee of the Department of Defense throughout her entire Stevenson education. Amber is currently working towards receiving a M.S. in Forensic Studies at Stevenson University. Amber is using her Stevenson education to expand her career with the Department of Defense.
Mobile Forensics: Current Issues with Third-Party Applications on Mobile Devices and Mobile Device Encryption

Brandon Lee

INTRODUCTION

Forensic science has always been an evolving and ever-changing field. A perfect example of this evolution can be seen in digital forensics expertise and those who study it. In 2008, the American Academy of Forensic Studies (AAFS) formally recognized digital forensics as part of the diverse field of forensic studies (Gordon and Hernandez 310). Digital forensics has brought forth a plethora of unique possibilities for obtaining new evidence that once was unreachable. As digital technologies evolve, so must new ways of collecting important digital evidence. One of these new areas for investigators to study is mobile forensics. Mobile forensics is the dissection and collection of evidence within a mobile device to develop new leads in an open case.

Applications that are developed for mobile devices by companies other than the mobile device developer are known as third-party applications. These third-party applications can lead to new problems in the collection of evidence because current investigative tools either do not properly dissect them or cannot break a mobile device’s encryption. For the investigator, this can cause a loss of information or of data. Based on several mobile applications and forensic software studies, the evidence strongly suggests that current forensic software cannot correctly dissect third-party mobile applications or break mobile device encryption. Current investigative tools would be more effective if the software could be improved to break through mobile device encryption to analyze applications without user input.

HISTORY OF DIGITAL AND MOBILE FORENSICS

Ever since individuals have committed crimes and incorporated technology into those crimes, there has been digital forensics. Digital forensics has developed alongside technology because investigators have realized that important information can be retrieved from digital devices. According to Mark Pollitt in his article, “A History of Digital Forensics,” the study of digital forensics has been around since the first reported digital crime in 1976. By 1995, the International Organization on Computer Evidence (IOCE) was formed for collaboration between countries on computer evidence, and to develop techniques to find digital evidence (Pollitt). The IOCE was formed after the Federal Bureau of Investigation held two conferences in 1993 and 1995. The creation of this organization showed that law enforcement knew the potential for using digital forensics to collect more evidence to convict possible suspects.

Another big leap for digital forensics came in 1991 when Chuck Guzis developed a software known as SafeBack (Pollitt). SafeBack was possibly the first digital forensic software that was commercially sold to investigate digital crimes. SafeBack was the predecessor to similar software used today. Software that investigators use today can be dated back to SafeBack, including EnCase, FTK Imager, Autopsy, and many more (Pollitt). Digital forensics continued to evolve over the years as “[c]omputers became ubiquitous, cell phones became essential and the Internet became the world’s central nervous system” (Pollitt). The reason for this was investigators realizing that a growth in child pornography was related to the use of computers to share pictures and videos. Vital evidence was on these computers, and programs were needed to keep that evidence safe and to locate certain evidence quickly.

Simson Garfinkel is a leading computer scientist who has been at the forefront of digital forensics since the 1980s (Garfinkel, Bio). Garfinkel also appreciated and researched the evolution of digital forensics with the National Institute of Standards and Technology, or NIST. He has helped advance digital forensics to the important science it is today, and is also an accomplished author, having written many books and articles that are used to set standards (Garfinkel, Bio). In one such article, Garfinkel describes forensics and the history of the study of digital forensics, as well as the importance on criminal investigations. Garfinkel states that, “[s]uspects in murder cases routinely have their laptops and cell phones examined for corroborating evidence. Corporate litigation is also dominated by electronic discovery of incriminating material” (Garfinkel, “Digital Forensics”). Thanks to Garfinkel, examiners can see the importance of researching digital forensics and developing ways to investigate new technology like mobile forensics. This technology is still being perfected to glean information from mobile devices that can be used in investigations.

Mobile devices have, themselves, evolved over the years as humans have become dependent on the Internet, and on having contacts and e-mail at our fingertips. The current mobile phone phenomenon started in 2007 when Apple released what some consider to be one of the first smartphones (Brewer and Bowcock). The first-generation iPhone was a new type of technology that bred a whole new way of looking at software. iPhones had software known as “apps” or mobile applications. These applications could do everything from telling the user the weather to running mobile online games. The current trend with smartphones is technology vendors seeing who can develop the next big application or the best smartphone. The forensic response to this expansion in smartphones was to begin to develop ways to investigate these phones to see if evidence could be obtained.

For now, mobile forensics is the latest development in digital forensics. “Some of these services, such as Facebook and Twitter, are changing the way in which people interact. This change is starting to drive how digital evidence is collected” (Pollitt). Even in 2010, it was apparent that the activities performed on mobile devices would be important for digital forensics. Social networking and the use of mobile applications have become a very important part of digital forensics investigations, namely because they lead to consistent activity on a mobile device.
DIGITAL FORENSICS PRACTICES

Digital forensics involves a few different fields, but all of these fields must be discussed to further the conversation on mobile forensics. Digital forensics can be broken down into two different categories of forensics: network and physical forensics (Kent, et al.). Network forensics is the study of cyber-attacks that happen over the Internet, like hacking. Physical digital forensics is the focus of this article, as it pertains to mobile devices. Physical forensics also includes computers, tablets, servers, and any other hardware that might be important to an investigation. The National Institute of Standards and Technology states that, “[t]he most common goal of performing forensics is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event” (Kent, et al).

An investigator acquires the device or physical hardware and looks at the data using a few different software programs that examine raw data bit by bit. EnCase and FTK Imager are both tools that will show an investigator not only what data is available but what has been deleted. One software program, called Autopsy, shows the investigator the files organized by file type to make the investigation easier. These are programs that have taken years to perfect and are widely used to obtain digital evidence.

Digital evidence can be found in many different digital areas and NIST suggests looking through all types of physical devices to obtain the best possible data (Kent, et al.). NIST also suggests that investigators think about acquiring data that may have been corrupted if power was lost to the device first, like Random Access Memory, or RAM (Kent, et al.). These instructions show two things. The first is that there is a good amount of thought that needs to go into the acquisition of digital evidence. The second is that there is useful software that can assist in an investigator’s analysis of raw digital evidence.

MOBILE DEVICE FORENSICS

NIST has designed a set of guidelines for investigators to follow when they acquire a cell phone to examine. The guidelines outline what could be the best possible way to maintain power, how the phone should be handled, and how valuable or potentially relevant data contained on the device should be examined (Jansen and Ayers).

According to William E. Folson, a professor at Stevenson University and a Certified Forensic Examiner, the first thing to do when acquiring a mobile device is to determine the type of mobile device recovered (Folson). The next step is to determine what version has been acquired (Folson). There are three types of phones in general use: Apple iPhone, Android Phone, and Windows Phone. Certain phones are easier to break into than others, according to Folson, and it is important to determine the difference in operating systems between the three devices (Folson).

Another important difference in cell phones is the phone networks. Professor William Folson advised in an interview that the first thing to look at in a cell phone investigation is what carrier the cell phone uses (Folson). The two types of carriers are Code Division Multiple Access, or CDMA, and Global System for Mobile Communications, or GSM. These can be differentiated by observing the presence or lack of a Subscriber Identity Module (SIM) card (Folson; Jansen and Ayers). CDMA cell phones have a SIM card, where GSM phones do not.

Folson confesses that the easiest way to examine a cell phone is if the phone was unlocked before the investigation began (Folson). After checking if the cell phone can be examined without needing to be unlocked, NIST suggests making a backup of the phone. NIST warns that, “[d]igital evidence by its very nature is extremely fragile, especially that found on cell phones. A phone’s contents and the evidence it contains can be affected or even lost any time it is on” (Jansen and Ayers). Much of the current software can handle making a backup, or image, of the cell phone data. Most of the problems come if the phone itself is encrypted. Professor Folson jokes that, “[i]f it’s encrypted, we know we are dealing with a tech-savvy bad guy” (Folson). Most of the time, the easiest way to glean information off the mobile device in question is to simply analyze the data in hand, rather than approaching it in a slow and organized manner.

The last item that Professor Folson suggests an investigator look for is any sort of Secure Digital card that may be in the device with additional data (Folson). A Secure Digital (SD) card can either come in regular size or a smaller size known as Micro SD. These cards can be inserted in some phones to save data like pictures, contacts, application data, and more. These cards can hold vital information and do not need to be examined with the cell phone. An image can be taken of an SD card, and an investigator can independently examine that image.

MOBILE FORENSICS SOFTWARE

There are many different types of software that an investigator can use to dissect a mobile phone and retrieve evidence. It is important to note that in a similar study done by Christopher Tassone, Ben Martini, Kim-Kwang Raymond Choo, and Jill Slay, “they also had a number of less common data types that were not supported across all three tools … further investigation was conducted to determine what data was different and if possible, why the difference occurred between the forensic tools” (Tassone, et al). Not all mobile forensic tools evaluate all important data.

There are three specific software programs that Professor Folson pointed out that he uses every day. Cellebrite, a mobile forensics company that also makes physical tools, has unique software it sells. XRY is a program developed by the digital forensics company MSAB. And the final software program is IEF, developed by Magnet.
Forensics. These three programs, most importantly, meet the Daubert Standard (Daubert v. Merrell Dow Pharmaceuticals, Inc.). The Daubert Standard is a set of rules that determine if an expert and the methodology they use can be considered in court (Daubert v. Merrell Dow Pharmaceuticals, Inc.). The judge decides if the expert is qualified in the forensic study in question. The expert must prove that the software used has been accepted by other courts. All three of these software programs meet the Daubert Standard, making them perfect for use by forensic investigators.

Another area of importance is the internal database or file system that each mobile phone uses to install applications (Folson). These internal databases not only have files of applications that have been installed, but can also contain images, documents, and other important evidence. In the iPhone operating system (iOS), the database is known as a Property List and is set up the same as in Apple computers (Apple Inc.). The Property List, or plist, is used to reinstall deleted applications as well as remember the user and what was done on the application before its deletion. It should be noted that the way iOS stores data on the plist varies depending on the version of the operating system installed.

On an Android device, the file system is a bit more complicated and varies depending on the device. On the newest Android devices, the file system is close to a Linux-based file system, known as Ext4 (Paul). However, the Android devices have changed their file systems somewhat frequently. The file systems have varied depending on what type of device the operating system is on, as well as what version of the Android operating system is installed. Android devices also have a separate database in which to store application data and caches, or application memory. This is known as an SQLite database, and this is where applications on an Android device store information (Yang, et al).

The final type of file system is found on Windows mobile phones. There are two file systems depending on the age and version of operating system on the Windows phone. The older Windows phones use a Transaction Safe-File Allocation Table or TFAT (Grispos, et al.). The newer Windows phones, on the other hand, use the New Technology File System or NTFS, that is also found in the Windows operating system for computers (Grispos, et al).

These file systems are used by mobile forensic investigators to gain knowledge about a device during investigation. The mobile forensic software takes advantage of the file systems to produce text messages, phone calls, and other information that a suspect may think they deleted or hid. Having knowledge of how files are stored on a mobile device is crucial to gathering all evidence pertaining to a specific case.

MOBILE FORENSIC SUCCESS

Mobile forensics has had both successes and failures in important court cases. Many states have now adopted some way of examining mobile evidence. One example would be the recent adaptation of mobile forensics tools in Hartford, Connecticut. And “Providence, R.I., Police Detective Teddy Michael has also seen firsthand the power of mobile data in solving all kinds of crimes, both inside Providence County and out—drug deals, juvenile crime, sexual assault, robberies and murder” (Tidwell). As soon as implemented, mobile forensic software has benefited police forces immensely.

Another example of a case in which mobile evidence was used to convict a criminal was State of Ohio v. Massey. In this case, a mobile forensics expert was able to use photographs found on the suspect’s mobile phone to convict him (State of Ohio v. Massey). Massey was in a relationship with a thirteen-year-old girl, and investigators were having a hard time proving that images found on Massey’s computer were in fact owned by Massey. When the images also appeared on his synced mobile device, the connection was made and Massey was convicted.

There are countless examples of cases that were successfully solved using mobile forensics. However, most of these cases needed only access to images, text messages, call logs, or other information that is not found in third-party applications. Third-party application architecture may hold the key to future cases.

MOBILE FORENSIC FAILURES

Most mobile forensic cases thus far have led to assisting in conviction or aiding an investigation. So far, only a few cases have been documented where mobile forensics was directly at fault for the failure of an investigation. Overall, a case can fail if a mobile device is encrypted so that only the suspect can gain access using a known password. These cases have been known to stop dead in their tracks.

One of the most famous of these cases is the iPhone the FBI seized from the San Bernardino, California, mass shooter, Syed Rizwan Farook: an encrypted iPhone the suspected used (Williams). The FBI had to contract with an outside vendor to gain access to the phone. Even though the phone was opened, it stopped the investigation for weeks (Williams).

Two more cases are prime examples of investigations failing because of encrypted mobile devices. The first was the case of Ray C. Owens, who was robbed and murdered in Illinois in 2015 (Vance, et al.). Next to Owens's body, two encrypted phones were found, “an iPhone 6 running on Apple’s iOS 8 operating system, and a Samsung Galaxy S6 Edge running on Google’s Android operating system” (Vance, et al.). To this day, the case remains unsolved, mainly because investigators cannot crack the encryption on these two devices.
The second case is that of Brittney Mills, a pregnant mother in Louisiana who was murdered by a suspect who is still unknown (Maddox and Ourso). Mills was shot and killed inside her home in Louisiana, and naturally investigators retrieved her phone to search for evidence. However, they met a wall when they discovered her phone was encrypted and could not be used in the investigation. After this, the investigation stalled and the evidence grew cold.

Encrypted devices are becoming a thorn in the sides of device investigation. As technology evolves, so, too, must forensic tools. These are only a few examples of ways that an encrypted device stalls or stops an investigation. If there is no tool created to combat these anti-forensic measures, other crimes could go unsolved.

**CELLEBRITE MOBILE FORENSICS**

The first software company mentioned, Cellebrite, is also, “the leader in mobile forensic extraction, decoding and analysis solutions” (Nazarian). Cellebrite has forensic tools that can even help crack an encrypted iPhone according to some reports (Fox-Brewster). In an article by Thomas Fox-Brewster of Forbes, he claims that Cellebrite was the company helping the Federal Bureau of Investigation crack into a criminal’s iPhone early in 2016 (Fox-Brewster). Cellebrite had to develop a way to crack the iPhone, however, since no other way to crack the mobile device had been invented yet (Fox-Brewster). Cellebrite was able to help the FBI crack into the criminal’s iPhone so the evidence could be obtained.

Cellebrite has an interface that integrates the data in an easy-to-observe format. Cellebrite shows the examiner files that may be of interest, including deleted files, pictures, text messages, phone calls, and more (Cellebrite). This makes the examination of the incriminating data much easier. The one weakness of this software is that it does not show data from deleted third-party applications, or data from currently used third-party applications that may hold information. This data would have to be examined in hand by the examiner, who would run the risk of overlooking data.

Cellebrite is also on the forefront of developing mobile forensic software. Currently, they offer software, which can be downloaded to a computer, that can take an image of a cell phone and divide that image to pick out files that may be important (Cellebrite). They also sell full machines that an investigator can simply plug an unlocked phone into to see the data on the phone (Cellebrite). Along with full machines, Cellebrite also provides tablets that can be taken into the field for quick analysis by someone experienced in forensics. Cellebrite is on the forefront of technology for mobile forensics and continues to work to improve mobile forensics.

Cellebrite’s biggest contribution so far is their ability to crack into a cell phone that is locked or encrypted. When a cell phone is locked, the built-in security settings are the only security in place. Many phones now have a fingerprint lock or a four-digit pin if the user cannot access with their fingerprint. However, Cellebrite has not only designed a command-line software program to unlock a four-number pin, they also have a machine, with a camera securely attached, that is designed specifically to break the device pin in a matter of seconds (Cellebrite). When the phone is encrypted, the process to crack the phone is different and difficult. Cellebrite has also made large strides in this field to break the encrypted mobile devices by combating encryption algorithms.

**XRY BY MSAB**

XRY is another extremely useful mobile investigative tool used by investigators. XRY is a software program and suite of tools very similar to Cellebrite. MSAB offers computer software, machines, and cell phone cracking (MSAB). Unlike Cellebrite, MSAB, the company that creates and improves the mobile examination software, also creates digital forensic tools that can benefit other areas. Cellebrite is only focused on mobile forensics, and has the advantage of leading the industry in that area.

XRY has an easy-to-use integrated interface, which Cellebrite also boasts. The data for XRY is laid out in much the same way as in Cellebrite, making navigating the evidence easy for the examiner. However, the glaring third-party application weakness is evident in this software as well as Cellebrite.

Where Cellebrite has been working on breaking encryption, MSAB has been focused on other types of non-traditional forensics. MSAB has been working to improve on two methods of digital forensics that also affect mobile forensics. MSAB is creating ways to conduct forensic investigations of vehicles and other devices that connect to mobile devices (MSAB). Most newer models of vehicles are built with computers that can do everything from controlling the temperature inside the vehicle, to knowing when the driver is too close to the vehicle in front of them (Yoon and Cho). These smart vehicles also connect automatically to some cell phones when the driver enters the car. Being able to forensically analyze smart cars and their connection with mobile phones will be a large part of mobile forensics in the future.

MSAB has also been working on and successfully implementing a way to examine cloud connections with a mobile phone (MSAB). Most mobile phones connect with a cloud server to back up a client’s data in case the phone gets damaged or data is lost. Whether the connection is to cloud storage that a carrier provides or storage provided by the phone developer, most phones back up automatically. An important aspect of mobile forensics is the ability of an examiner to access this data. MSAB has developed a way to use their XRY software with the mobile phone to retrieve information off of cloud-based services that a criminal may use to hide data (MSAB).
Even though MSAB might not lead the mobile forensic industry, they are worth mentioning because of their work with mobile devices, smart cars, and cloud-based software. The XRY program is still a useful tool in a forensic examination and they maintain an easy-to-navigate interface to help examiners dissect the information on a mobile device.

**IEF BY MAGNET FORENSICS**

IEF, or Internet Evidence Finder, is the third software program a forensic investigator can use to investigate a mobile device (Magnet Forensics). IEF has both strengths and weaknesses that must be talked about when discussing mobile forensics. IEF is the program closest to being able to examine third-party software within an integrated interface, which can benefit an investigator.

IEF does have two glaring weaknesses that should be mentioned due to their competitive disadvantages. Magnet Forensics does not offer any in-field devices or independent machines like Cellebrite and MSAB. IEF is strictly a software program to be downloaded and used (Magnet Forensics). IEF also does not offer any advantages relating to encryption or locked phones like Cellebrite. This weakness makes IEF only usable after the phone is unlocked or unencrypted.

IEF has the strongest interface of all three programs. It has the ability to take an image of a cell phone and distinguish application data that may be important to an investigator (Magnet Forensics). The fact that third-party applications can be seen and labeled properly helps an investigator sort through only the useful data. Investigators can cut time in looking over useless data and can efficiently see important application data.

The other strength that IEF boasts is the ability to analyze cloud-based connections much like XRY can. However, IEF can analyze what documents or data were sent to the cloud without having to connect to the cloud (Magnet Forensics). IEF can see all of the cloud-based services that are connected to the phone and what they were used for.

All three of these tools are powerful in their own way. Combining them can assist an investigator in analyzing mobile data as well as unlocking an encrypted phone; however, the combination of these software programs can be extremely expensive, including the cost of hiring or training investigators who can use them. Most companies use one of the three or another less effective forensic software. Cellebrite, XRY, and IEF are each flawed in their own way, but still remain useful.

**THIRD-PARTY APPLICATIONS**

On a smartphone, there are default applications that are implemented when the phone is designed. These applications are text messaging applications, call making applications, a browser for the Internet, settings to personalize the phone, and many more. Another application that is on smartphones by default is a store that can be accessed to buy other applications that do various other tasks. These are referred to as third-party applications, and have a significant place in the investigation of a mobile device.

Third-party applications increased in popularity in 2008 and 2009 when mobile phones were getting smarter and their usefulness was increasing (Rajput). Mobile applications and games have been around since cell phones could be used for business purposes (Rajput).

With the evolution of the Internet, social media, and smartphones, application development has evolved alongside to make people’s lives both more convenient and easier to access. Since the mobile phone revolution, mobile application development has taken on a mind of its own. Mobile games, social media applications, e-mail services, and messaging applications have taken over the market for third-party applications (Rajput). Most of these applications are harmless, but occasionally these applications can hold valuable forensic evidence.

Third-party applications take advantage of the file systems within mobile phones to save both information about and the architecture of the phone, which the application will pull from for later use (Ntantogian, et al). Most importantly, even if the application is deleted, these files are still available for forensic analysis (Folson). The phone keeps these files around for reinstallation of the application. The application will remember the user, what the user did on the application, and other information, such as what the user may have looked at or been interested in. Things like viewed images and other possible forensic evidence can be found in these file systems.

Forensic examiners can only look at these files if the phone is unlocked and unencrypted (Folson). If the phone is locked or encrypted, then the phone is not accessible until either the lock or encryption is broken or cracked. Once the mobile phone is opened, not all forensic software will look into the mobile applications on the phone. These forensic tools generally look at information such as images, text messages, phone calls, and other default settings and applications. In these programs, the forensic investigator can use the software to look through the file system, but may pass over applications or files that are unknown. IEF is the most useful for evaluating applications, but only looks through installed mobile applications as opposed to deleted information.

There are many mobile applications available for download from an application store that an investigator may not be familiar with. There are also alternative application stores that have applications that a user can download third-party applications from that an investigator can miss. Third-party applications have been extremely popular over the years, and if mobile device investigators do not look for these applications, crucial evidence may be lost.
SOCIAL MEDIA APPLICATIONS

One of the biggest revolutions in mobile phones is the ability to download social media applications from application stores to keep track of friends and family. Social media site applications such as Facebook, Twitter, Snapchat, and Instagram can be found on many individuals’ mobile devices. Even though these social media applications are meant for fun, there have been times when the information or messages were useful evidence for investigators.

In a criminal case in 2012, Darrin Anderson was found guilty of traveling with the intent to engage in illicit sexual conduct (United States v. Anderson). In this case, “between December 2006 and July 2009, Anderson engaged in more than 800 private chats, mostly with adolescent girls” (United v. Anderson). This case shows the significance of social media evidence because Anderson’s Facebook information was found to be fake and used to lure adolescent girls to a hotel room for inappropriate acts (United States v. Anderson). Using social media evidence, the court was able to convict Anderson.

The importance of social media evidence is not only that it is useful for seeing what a person does online, it is also useful for setting up a timeline of the crime. It can also be used to prove whether a suspect was near the scene of a crime or not. Social media provides things like location service information, images that a person has taken throughout a specific day, possible private messages describing where an individual may want to meet someone else, and other useful evidence. The New York Times reported that an average person spends almost an hour a day on Facebook alone (Stewart). With this information, a digital investigator can easily lay out a timeline of what a suspect was doing and when. The investigator can also examine the phone for other social media outlets the suspect may have used.

Another important forensic measure that can be found in the social media SQLite database is the friends and contacts lists (Yang, et al). The mobile investigator can examine the contacts, as well as the conversations that were had between individuals. Only IEF can examine this evidence and make it available for immediate viewing. The other two software programs make the databases available, but the investigator must continuously search for the databases as the investigation progresses.

Snapchat is a newer third-party social media application that should be mentioned. This application allows users to take images and send them to friends. These images are available to the receiving user for only a set amount of time before the application deletes them. Investigators should still consider the SQLite database this application creates. The images that are “deleted” are never actually deleted. This is another example where possible forensic evidence may be lost. If the investigator does not know to look within the SQLite database, they might miss important evidence.

MESSAGING APPLICATIONS

Another type of third-party application that can be found on many consumers’ mobile devices are messaging applications. There are hundreds of applications that mimic text messaging and can be used to contact other individuals. These are applications such as Kik, WhatsApp, and others that can be used to either message other users of the application, or even contact other phone numbers.

Police officers in one town confessed, “[o]ne of Hartford’s biggest challenges involves accessing mobile messaging applications, which are constantly changing and evolving” (Tidwell).

A similar type of messaging application that can be downloaded on a mobile device is Facebook Messenger or Skype Messenger. A study was done by a group of researchers from all over the world on how Facebook and Skype could be examined forensically. This group of researchers examined how Facebook and Skype messengers were installed on a Windows 8.1 machine, and how these applications would save information and memory on a machine (Yang, et al). The process and examination is very similar to how these would be installed and run on a mobile phone. In the study, it is noted how Facebook and Skype messengers save their data in an SQLite database, which looks similar to an Excel spreadsheet when examined (Yang, et al). Though the tools used were not revealed in the study, it is clear how these applications save data and pull information.

If a messaging application is installed on a mobile device, then IEF knows to look for the application and show the investigator what content may be on the application. However, if the application has been deleted, then none of the three available software programs would show the investigator anything about the application. The investigator must go searching to uncover possible evidence in the application. This can lead to evidence being missed or simply overlooked.

CLOUD

Cloud-based software is also vital mobile device evidence that can help an investigator. For most consumers, a computer cloud seems like a strange and hypothetical idea. Most consumers imagine, when talking about cloud computing, their data floating above their head in a real data cloud. The truth is much less fantastic than what is commonly believed. When referring to a cloud, the consumer’s data is simply stored on a server owned by a cloud service. For a forensic investigator, this lack of knowledge can work in their favor if a criminal does not realize their data is accessible.

In a research study done by Information Assurance Research Group, University of South Australia, three investigators looked through popular cloud-based mobile applications. These researchers wanted to see if they would be able to view what a user had taken from their cloud, then looked at, modified, and returned to the cloud.
In this study, the researchers took cloud software like Dropbox and considered how the application stored cached data and information for later (Martini, et al.). They were able to find that most mobile cloud applications created a database with the file extension .db when the user accessed the cloud and viewed data. In the database, other information was saved to the mobile device such as file size, date accessed, file name, location on the server it was stored on, and more (Martini, et al.).

Since their research in 2014, more cloud-based applications have appeared that save more than just documents or images (Martini, et al.). Cloud-based applications, such as Verizon Cloud, have been developed to save contacts, e-mails, text messages, and call logs. These applications can be read the same way Dropbox or other cloud software are read, but these cloud-based programs are not searched for by current forensic software because they assume that the investigator will be able to recover this information from the mobile device. This information can be found by using the current software, however, but only if the investigator looks. These newer cloud-based programs could hold a veritable goldmine of information that has been deleted from a mobile device, and should be thoroughly examined.

XRY and IEF both check if the cloud software is installed and look through the .db files to show an investigator what information the database has. Yet again, however, if the application is deleted, the investigator must search within the software to see if the database files are accessible. This can lead to loss of evidence and overlooked data that might have helped an investigation. Cloud-based applications might hold many valuable images and documents that could be vital to an investigation.

**ENCRYPTION**

Encryption is a growing nuisance to mobile forensics investigators everywhere. Encryption happens when additional protection is put on a mobile device so that others cannot access the mobile device. This is a perfectly acceptable act for law-abiding citizens, but criminals can use this to hide information from investigators and law enforcement agencies. This can cause data to be unrecoverable and can hamper an investigation.

Most recently, the Federal Bureau of Investigation had problems decrypting an iPhone belonging to a potential terrorist (Fox-Brewster). The case of Syed Rizwan Farook, or the San Bernardino shooter, took on a new twist when the shooter’s iPhone was found to be encrypted (Williams). This forced the FBI to request help from Apple, the creator of the iPhone, for assistance with the encrypted device. Apple refused and a large legal battle ensued (Williams). In the end, Cellebrite was able to crack the encryption, providing the FBI with important evidence from the encrypted device (Fox-Brewster).

Cellebrite is on the forefront of battling mobile device encryption. The company has even been able to incorporate their new techniques into the software and machines they sell (Cellebrite). However, encryption changes almost daily and criminals are beginning to use this information to their advantage. If an investigator must fight against an encrypted device, it can stop an investigation cold, like the FBI experienced. Mobile device encryption will be a constant battle, but if Cellebrite works with other mobile forensic companies, the fight may be made easier.

**SOLUTION**

“Acquisition, decoding and presentation of information from mobile devices is complex and challenging … manufacturers have adopted a variety of file systems and formats complicating decoding and presentation” (Grispos, et al.). It is clear that mobile forensics is a difficult and developing process. Fresh and original ideas are needed to keep progressing the study of mobile forensics. As technology evolves, and criminals continue to work against investigators, forensic tools need to evolve alongside.

The first step to solving any problem is recognizing that the problem exists. Mobile forensics is no exception because it deals with ever-evolving technology. Two immediate problems have been identified and can be solved together. The first problem is that the current forensic software does not properly identify third-party applications. The second problem is that, as criminals get more intelligent, they will understand that they need to encrypt their devices to hide what they may have done on them. Both problems can cause investigators to miss vital evidence or to leave a piece of evidence unfound.

The best way to combat these issues is to use the strengths of the existing mobile forensic software as a base, and improving the current software. This improved software would be a combination of Cellebrite’s anti-encryption abilities, XRY’s cloud technology tools, and IEF’s ability to look at third-party applications. It could make an investigator's job as simple as plugging a mobile device into a machine and watching the program run.

An investigator could take a mobile device that was found as evidence, and plug it into a machine on which the improved forensic software was loaded. The interface would then ask the investigator for the make and model of the phone, for example, an iPhone 4. The software would pull from a database that would tell it what operating system was most likely to be on the phone. If an error were found, the investigator would be able to change the operating system selected. The phone would then ask the investigator if the phone was locked, encrypted, or unlocked. The investigator could click an option and the software would attempt to break either the encryption or the simple lock.
The program would then begin to examine the contents of the mobile device. It could compile all of the important application data into one readable interface. On the side of the software, a list of applications, either deleted or installed, would be listed. The investigator could evaluate one application at a time until the investigation was satisfied. This setup would show social media information, data uploaded to cloud storage, messaging applications, and more. Using this setup, neither encryption or third-party application data would be a problem, and reviewing them could be expedited for the investigator.

CONCLUSION

Digital forensics has been evolving and changing as the technology has. The changes in technology lead to new crimes, as well as new ways to commit crimes. The newest technology that has been important forensically is mobile devices and the information individuals load onto their mobile devices. As the ways that individuals use their mobile devices change, so must the ways investigators dissect information from mobile devices.

Investigators currently have three powerful software programs to help them read and interpret what is on a mobile device. Some of this software can be used to break into phones that are locked or encrypted. Even if the investigator combined the software programs, there is a possibility that certain information would be lost or missed. To get the best results, the current software must be evolved, much like the technology it is meant to interpret. Once the software is improved, investigators will have a much easier time reading and understanding the information on mobile devices.

WORKS CITED


BRANDON LEE

Brandon Lee is currently a senior Digital Forensics major at Stevenson University. Brandon is also Stevenson’s Bachelor’s to Master’s program, pursuing his master’s degree in Digital Forensics. After graduation, Brandon plans on working for the United Sates Government in the field of Computer/ Mobile Forensics.
The Addiction Factor in White Collar Crime: New Perspectives on Prevention and Punishment
C. Morgan Little

“Forgetting to include human nature in an equation can be devastating.”
Harry Markopolos, No One Would Listen: A True Financial Thriller

INTRODUCTION

The behavioral sciences have played a significant role in combatting white collar crime. In fact, it was a criminologist, Edward Sutherland, who coined the term “white collar crime” (Wells 12). The fields of psychology, sociology, and criminology are, to an extent, unsung heroes in the fight against white collar crime, as they have laid a foundation of understanding from which strategies for prevention and punishment have emerged, and yet they are often overlooked.

The Association of Certified Fraud Examiners (ACFE) relies on this psychological foundation in the recommendations it provides in its Report to the Nations on Occupational Fraud and Abuse. Attempting to gain understanding and insight into what motivates perpetrators of white collar crime is important, and considering the magnitude of the problem of white collar crime, more needs to be done along those lines to further the understanding that has already been gained, rather than resting on past laurels. Contemporary explorations into the psychological underpinnings of white collar crime are needed in order to hone in on more effective solutions to what has become an ever-growing problem. The stakes have never been higher due to the devastating costs and fallout white collar crime imposes on its victims. Perhaps looking at white collar crime through the lens of addiction can add to that crucial foundation of understanding and contribute new perspectives on prevention and punishment.

AN OVERVIEW OF WHITE COLLAR CRIME

White Collar Crime Defined

White Collar Crime as a concept was first introduced by Edwin Sutherland in 1939 as crime “committed by a person of respectability and high social status in the course of his occupation,” and by “person” he also meant “entities,” including companies (Strader 1). In 1988, however, the United States Department of Justice called white collar crime “one of the most serious problems confronting law enforcement authorities” (Strader 2) and clarified the definition as follows:

Nonviolent crime for financial gain committed by means of deception by persons whose occupational status is entrepreneurial, professional, or semi-professional and utilizing their special occupational skills and opportunities; also, nonviolent crime for financial gain utilizing deception and committed by anyone having special technical and professional knowledge of business and government, irrespective of the person’s occupation (Strader 2).

The ACFE refers to white collar crime as simply “fraud,” and emphasizes deception as the defining characteristic, but also clarifies that white collar crime, or fraud “includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.” (ACFE, What is Fraud?)

Although there is some degree of variation across the spectrum of defining white collar crime, there is enough consensus to have a set of criteria with which to examine the behaviors commonly accepted as white collar crime. The ACFE divides white collar crime into crimes that affect individuals and those that affect companies either from within or from the outside. Some examples of white collar crime include identity theft, embezzlement, corruption, bribery, asset misappropriation, cash larceny, check tampering, financial statement fraud, Ponzi schemes, … and the list goes on. There are so many kinds of fraud that the ACFE, to break down the occupational fraud scheme classifications, developed the “Fraud Tree,” which doesn’t even include fraud schemes against individuals (ACFE, The Fraud Tree).

White Collar Crime: Dealing with the Damages

White collar crime has become an ever-increasing problem over the past few decades, causing widespread destruction that has claimed companies, government agencies, individuals, and small businesses as victims. Although it is difficult to quantify the damage caused by white collar crime because it covers such a vast territory of consequences on so many levels, the ACFE, in its 2016 Report to the Nations, estimated that occupational fraud and abuse contributed to losses of more than $3.7 trillion worldwide in 2014 alone (8). Additionally, the 2010 National Public Survey on White Collar Crime estimated that one in every four homes were affected by white collar crime in 2010, making it more prevalent than “all other types of crime combined.” (AOL) It also estimated that 88 percent of white collar crime was not reported to law enforcement agencies, making it even more likely that any estimates aimed at quantifying the devastation caused by white collar crime are significantly understated (AOL). In its wake, white collar crime has destroyed countless citizens’ lives by draining personal bank accounts, damaged reputations in the financial industry, reduced confidence in the public market system, and bankrupted corporations. It has even reduced national security through its support of the underground economy.

The IRS, FBI, SEC, and other agencies have struggled to keep up with these costly and complex white collar crime cases and their extreme consequences. Efforts to reduce white collar crime have been centered on prevention and punishment. The Sarbanes-Oxley Act and the corporate Federal Sentencing Guidelines were implemented to
increase punishment severity along with requiring increased internal control and accountability, all aimed at deterring white collar crime (Steer 1). This year, Utah became the first state to establish a White Collar Crime Offender Registry, akin to a sex offender registry, in order to publicly shame perpetrators and protect potential victims (Protess). First time offenders will be on the site for 10 years and third time offenders will be on for life (Protess). This is a pioneering action taken by Utah, as the registry is the first of its kind in the nation, and it’s an encouraging example of citizens and government taking action in order to confront the problem of white collar crime with new solutions.

A HISTORY OF PSYCHOLOGICAL RESEARCH IN WHITE COLLAR CRIME

Edwin H. Sutherland

Edwin H. Sutherland has been called the “Freud,” as well as the “Father,” of white collar crime, not only because he coined the term itself, but also because of his pioneering research into the problem. Sutherland’s research in the 1930s and the resulting set of theories is considered by many criminologists to be of paramount importance in the area of white collar crime because it moved the path away from the perception of criminal behavior as a genetically-based characteristic, an idea that had been fully embraced by the field of criminology up to that point; namely, that children of criminal parents will likely be criminals, and so on across generations (Wells 12). This was an important departure on many levels, and opened up the eyes of those in the field to an entirely different point of view. His contribution likely reduced a great deal of prejudice against the children of offender parents. Further, his research illustrated that more research needed to be done in light of rejecting the commonly-held answer to the question of what perpetuates white collar crime.

His theory of differential association claimed that criminal behavior is learned behavior like any other learned behavior, and when an individual is in an environment that exposes him or her to criminal behavior, he or she will be influenced by that behavior and become more likely to engage in the same behavior. However, on the other hand, Sutherland also claimed that good behavior is “contagious” along the same lines (Wells 12). From the perspective of Sutherland’s theory, then, the tone at the top of an organization, internal controls, and staffing choices are critical components of the prevention and prediction aspects of white collar crime.

Donald R Cressey

The Fraud Triangle is a hallmark symbol of psychology in white collar crime and was a theory developed by Donald R. Cressey, who studied under Sutherland’s guidance (Wells 20). His focus was on the psychological factors that contributed to white collar criminals succumbing to the temptation to commit embezzlement. The Fraud Triangle is the hypothesis resulting from his studies. The hypothesis suggests that there are three critical elements that merge in order to contribute to the perpetrator engaging in fraud. The first element, pressure, is generated through some type of financial problem that the perpetrator cannot or will not disclose (Wells 20). A few examples of this pressure include credit card debt, an ill relative or friend in need of expensive medical treatments, or a spouse losing a job. Opportunity is the second component and results from an environment that gives a person the option to commit a crime through a combination of awareness of his or her ability to violate his or her position and the technical skills to be able to take advantage of that access (Wells 20). Opportunities can be found in an environment lacking in internal controls or with poor segregation of duties. If an employee has access to blank checks, for example, ample opportunities for fraud may abound. The third component of the Fraud Triangle is rationalization, which may take many forms, but must allow the perpetrator to continue to perceive himself or herself as justified in his or her actions. A common rationalization for an employee is that he or she isn’t getting paid what he or she deserves and is thus justified to steal in order to compensate the difference. Additionally, employees often frame their rationalization around the fact that they will only be “borrowing” the money and plan to reimburse the company when things settle down. The one requirement of the rationalization component, according to Cressey’s theory, is that the perpetrator must have this rationalization manifested in his or her psyche prior to committing the fraud rather than after the fact (Wells 20).

The Fraud Triangle is commonly seen in textbooks and on websites that advertise fraud prevention. It is a fixture in the fraud and loss prevention community, and a reminder of the importance of the human factor in white collar crime prevention. However, since the development of the Fraud Triangle, a number of professionals suspect that, although the theory may still be useful, it is not perfect and cannot explain all white collar crime cases (Wells 20).

Dr. Steve Albrecht

Dr. Steve Albrecht set out to discover red flags to identify fraud based on categories including personal characteristics and environment. He came up with a list of factors for both categories and from these lists derived the “Fraud Scale,” which focused on “situational pressures, perceived opportunities, and personal integrity” (Wells 23). He found correlations and relationships between various factors in the work environment and personal characteristics of perpetrators that could be used in an effort to predict workplace crime. His research supported the Fraud Triangle in many aspects because the three factors in his fraud scale mirrored the three components of the Fraud Triangle. How he connected those three factors and interpreted how they interacted, however, was different. He also observed some demographic data relationships that are supported by the current demographic statistic correlations found by the ACFE. (Wells 24).
Richard C. Hollinger and John P. Clark
The Hollinger-Clark study was done in 1983 by Richard C. Hollinger and John P. Clark. This study aimed at uncovering the true costs of employee theft, while also explaining the elements of that theft. They concluded that the main driver of employee theft was job dissatisfaction (Wells 20). The concept supports the rationalization portion of Cressey's fraud triangle in that job dissatisfaction is often a rationalization used to commit white collar crime. Additionally, they discovered that the perception of detection, or the feeling that they would be caught, was a significant deterrent of employee theft, a finding that other research has confirmed (Wells 24-29). The finding that the perception of detection can be significantly effective in reducing white collar crime can be seen in the emphasis that is now placed not only on internal control policies, but also in making employees aware that they are being actively monitored.

Hollinger and Clark examined the sense of control in the workplace in depth. Interestingly, they found that "the loss of respect among one’s acquaintances was the single most effective variable in predicting future deviant involvement" (Wells 29). This finding suggests that the threat of being caught and shamed is the most important strategy for prevention and punishment. If a perpetrator feels like the chances are high that he or she will be caught and subsequently exposed, he or she won’t take the chance, regardless of the punishment itself. It implies that the punishment, while necessary and appropriate, is less effective than being caught and exposed and of itself. Utah’s White Collar Offender Registry is a good example of this principle in action.

Cesare Beccaria
Cesare Beccaria introduced another classical theory that has been used to explain white collar crime, the Rational Choice Theory, and although it was introduced in the end of the eighteenth century, it is still relied upon by the behavioral sciences community (Wright 1). The main premise behind the Rational Choice Theory is that a careful measuring of risks, rewards, and associated consequences takes place in the mind of the offender prior to committing any crime. If the punishment is perceived to be likely and severe, the criminal will be less likely to give in to the temptation to commit the crime. This sense of choice may be stronger in the beginning stages of a white collar offense, but will diminish as the crime evolves into a habit and then a dependency. The sense of choice may be dulled by something beyond a sense of “rational” choice—addiction.

WHITE COLLAR CRIME AS AN ADDICTION

Inherent Repetition in White Collar Crime
Before establishing whether or not white collar crime can be addictive, it is important to determine whether there is repetition in white collar crime to begin with. Repetition is at the heart of addiction, as the addict does the same behavior over and over again, usually to his or her detriment or the detriment of others. If examinations into white collar crime indicate that most offenders are not repeat offenders, then it would be reasonable to assume that white collar crime does not appear to be addictive.

However, even without repeat convictions, white collar crime is, by nature, repetitive. On the surface it may not look like one conviction of white collar crime could be indicative of any addiction due to a lack of repeat offenses, but a closer look reveals that there is inherent repetition in white collar crime. One fraud scheme is composed of many transactions. Each transaction is an offense. Essentially every individual fraud scheme is inherently a set of multiple offenses.

By the time Enron hit bottom in late 2002, many choices to offend had been made. Many repeat offenders and many of their prospective repeat offenses contributed to the disaster of the fall of Enron. Jeff Skilling, the President and CEO of Enron in 2001, “believed that greed was the greatest motivator, and he was only too happy to feed it” (McLean 55). Further, according to a former Enron manager, Skilling declared that “all that matters is money” (McLean 55).

The ACFE, in its 2016 Report to the Nations, claimed that the median duration for an occupational fraud scheme is 18 months before detection, and that about 32 percent go on for at least two years before they are detected. This supports the proposition that most white collar criminals are repeat offenders, as their behavior in the scheme indicates that they are offending with each transaction, thereby making deceptive transactions repetitively and frequently. It could be said that they are repeat offenders inherently, or by default, by the time the scheme is uncovered. Additionally, a study done by the Department of Justice supports the concept of repeat offending in a more traditional sense, as it estimated that 40 percent of white collar criminals are already repeat offenders with prior records (Weisburd 3).

Building further on the concept of inherent repetition in white collar crime is the tendency for most fraud schemes to begin with smaller transactions that begin to increase in frequency and intensity in terms of growing fiscal theft amounts per transaction, as illustrated by the case study of Barry Webne, below. As the scheme grows and becomes addictive, it begins to resemble a snowball rolling down the hill, becoming larger and faster until it crashes at the bottom.

Illustration: Case Study Part 1
Barry Webne was a white collar criminal who was convicted of embezzlement. Through falsifying checks and payroll transactions, he stole over one million dollars from the company that employed him. For his crime, he served six months in an “intensive confinement center” and paid back $200,000 in restitution. Ironically, after he left “jail,” he started his own consulting business and called himself a “fraud expert” (Patterson).

The ACFE interviewed Webne about his fraud. During the interview, Webne admitted that he never expected to actually face any jail
time as a white collar criminal, a sentiment that indicates that more severe punishments may be need in order to deter white collar crime. Further, “he took a rational look at his crimes, how he started slowly at first, and then realized that his position of trust within the company—and the seeming lack of any control structure through which he might be caught—led him to steal greater amounts and more frequently” (Patterson). The sense that his thefts grew in quantity and frequency mimic addiction in the sense of a tolerance being developed to the crime. Addicts typically indulge in larger and more frequent doses of whatever it is they are addicted to.

Additionally, “Webne also hinted at something deeper than just greed” (Patterson), and described his experience while committing the crimes as being two-sided; on the one hand he was afraid of being caught, on “the other side [he] was just concerned with getting … that next rush … getting another $20,000.” (Patterson) It is interesting that Webne used the word “rush” to describe and individual offense, as that is precisely how many addicts describe a “high.”

A Common-Sense Perspective
Gone are the days where the stigma of addiction was solely reserved for the stereotypical street drug addict. A new era of addiction has developed over the past few decades. Addiction is now a highly publicized modern day dilemma, and the many different, often competing, theories for explaining and treating addiction make it controversial, as well. A quick google search will pull up addictions to all kinds of things, including substances, behaviors, things, and people. Even the twelve-step programs of Alcoholics Anonymous have branched out to include all types of addictions, including gambling, sex, debt, computer gaming, overeating, and codependency. There is research that points to the fact that any behavior can become addictive, and if that is the case, white collar crime is not exempt.

Many people believe that experiences can become addictive. The brain releases chemicals in response to internal and external stimuli. Stress, lack of sleep, anxiety, fear, excitement, and love all affect the human nervous system and can be chemically identified. Even runners get “high.”

The sense some perpetrators of white collar crime have of becoming addicted to their crime is not unique according to ACFE President James D. Ratley. According to Ratley, “fraud perpetrators tell [him] that it became an addiction for them” (Patterson) and that white collar criminals in general grow more confident with each offense they get away with, fueling their ego (Patterson). Ratley also suspects that the “addiction aspect of the crime [is fueled by] pride over what they’ve accomplished, even after they [are] caught” (Patterson).

It makes sense that white collar crime can become an addiction. Addiction treatment centers can be found all over the country, and new addictions are advertised with their corresponding treatments frequently on television as well as online. Addiction has become a common household concept, used to describe all kinds of habits, both troublesome, such as gambling, and beneficial, such as the runner’s high. Why should white collar crime be excluded from the ever-growing pool of addictions? In fact, if gambling is commonly accepted as being addictive, how is white collar crime any different, aside from the odds of scoring a win being much greater in white collar crime?

There is also the concept of secondary addictions that may fuel white collar criminals to resort to stealing. In order to support any other addiction, whether it be to substances or to other behaviors, the easy money acquired through a white collar crime scheme may be the means that allow the white collar criminal to continue to support his or her primary addiction. This secondary addiction to white collar crime could conceivably be as intense as the direct addiction to the crime itself. It is easy to see how addictions in this sense can become like a web, trapping the criminal in his or her own entanglements.

Another secondary aspect of the addiction may be that the white collar criminal develops additional addictions to what is obtainable through the monetary gains afforded by his or her white collar criminal offenses. This secondary addiction is the same in concept as the one mentioned previously, with the only real difference being the timing and chronology of the series of addictions. Like a web, the addictions become intertwined and connected, one fueling the other and catching the criminal in his or her own crimes.

It is even likely that some white collar criminals may become addicted to the rush and thrill of getting away with the crime itself, regardless of, or perhaps independent from, any other addictions. This common-sense perspective derived from basic analysis of white collar crime in general is a good start in making the case for the addiction factor in white collar crime. While the layman’s common-sense perspective is logical and sound, it is important to examine what experts in the field have to say.

Modern Perspectives on Addiction
In “Behavioral Addiction versus Substance Addiction,” Seyyed Salman Alavi, et al., conducted a research study that examined the consensus views in the field of psychiatry and psychology. Their study showed that

[b]ehavioral science experts believe that all entities capable of stimulating a person can be addictive; and whenever a habit changes into an obligation, it can be considered as an addiction … [and] any source which is capable of stimulating an individual, could become addictive. The change of behaviors such as gambling, drug abuse, computer gaming or chatting and internet browsing from habits into obligatory behavior, can be considered as the development of addiction (Alavi).
White collar criminals are susceptible, then, to becoming addicted to the perpetuation of a fraud scheme, as it becomes an obligation or compulsion. The Alavi study clearly expresses a consensus view that behaviors can become addictive, and from that view it is reasonable to assume that white collar crime as a behavior can also become addictive.

In order to explain the chemical mechanics of this behavioral addiction, Alavi, et al., explain that, "from a neurobiological perspective, behavioral addictions that only indirectly affect the neurotransmitter systems of the brain, can serve as reinforcers comparable to pharmacological substances that directly affect these systems (e.g., dopaminergic system)" What the experts are actually saying, then, is that in response to a behavior, the brain can actually manufacture its own chemicals that are as potent as a street drug! The rush of chemicals flooding the brain during a white collar crime offense could result in the formation of an addiction to white collar crime. That powerful association of the behavior and the chemical experience in the brain in response to the behavior is a learned association that reinforces the development of the addiction.

According to Alavi, et al., the obvious signs of addiction that can be identified in substance abuse are not present in white collar crime. This indicates that appearances are not good indicators of white collar crime, despite the fact that they can be useful in flagging potential addictions to drugs. A heroin addict’s appearance, for example, will, in many cases, deteriorate in a steady and obvious manner over time. In white collar crime, however, other markers will be necessary to identify addiction in its earlier stages.

The study by Alavi, et al., also found that “one of the precursors of behavioral addiction is the presence of psychopathologies such as depression, substance dependence or withdrawal, and social anxiety as well as a lack of social support.” These behavioral issues may be helpful in identifying a perpetrator’s susceptibility to becoming addicted to white collar crime. In fact, these may be red flags to consider in establishing additional controls. Further, the Alavi study also confirmed that there are many similar components of addiction in the “development and maintenance of both behavioral and substance-related addictions,” noting that the following criteria can be found in addiction to both substances as well as behaviors:

1. Salience: Domination of a person’s life by the activity
2. Euphoria: A ‘buzz’ or a ‘high’ is derived from the activity
3. Tolerance: The activity has to be undertaken to a progressively greater extent to achieve the same ‘buzz’
4. Withdrawal Symptoms: Cessation of the activity leads to the occurrence of unpleasant emotions or physical effects
5. Conflict: The activity leads to conflict with others or self-conflict
6. Relapse and Reinstatement: Resumption of the activity with the same vigor subsequent to attempts to abstain [leads to] negative life consequences, and negligence of job, educational or career opportunities (Alavi).

Other Opinions
There are other experts in the behavioral sciences field who disagree with the concept of addiction as a neurobiological process that progresses out of the control of the addict. Some of those experts think that the choice to engage in the behavior in question is purely voluntary, much like the concept of Rational Choice Theory mentioned earlier. According to Edmund Henden in “Addiction: Choice or Compulsion?” addiction involves a certain amount of compulsive behavior but is also tempered with rational choices. He implies that the rational choice still exists in the course of addiction, but the perception of risks and rewards gets skewed and the decision-making process becomes hindered (Henden 4). He describes compulsion as “strongly cue-dependent in the sense that it is regularly triggered by certain situations, places, or people [and] compulsive persons feel repetitively driven to perform the behavior, often in spite of themselves”(Henden 1). Further “if compulsive persons sincerely try to refrain from acting upon their compulsive motivation, achieving success becomes increasingly difficult over time” (Henden 5). Compulsive behavior as described by the Henden study sounds very similar in nature to addiction, so it seems that from either perspective, additional forces may be at play in white collar crime.

An interesting point about the Henden study, however, is that he takes a perspective in the middle of the road between outright neurological addiction and pure free will. Basically, his theory is that there is still a certain amount of choice in the mind of an addict but the addict’s ability to make rational choices dissipates as the compulsive behaviors endure over time. This concept is consistent with the perception that white collar crime can be addictive, but to a less potent extent. This watered-down version of addiction implies that the white collar criminal may lean on the crutch of addiction only to a small extent. Further, it implies a greater degree of personal responsibility than does the perception of addiction as an outright disease of the mind. Even in taking Henden’s perspective into consideration, some useful insight can be gained into prevention and punishment strategies for white collar crime.

WHAT NEXT: NEW PERSPECTIVES IN PREVENTION AND PUNISHMENT

Case Study part 2
After Webne was convicted of embezzlement in the early 1990s, he was ordered to pay restitution and had to serve only six months. Webne only “paid back about $200,000 of the more than $1 million that he stole,” but admitted he was torn between handing over more and hiding the last of what he had. His restitution ended with his sentence and probation (Patterson). However, ACFE President James D. Ratley believes that “serving time and paying what you can doesn’t clear the slate[,] and] one of [his] great complaints is that a lot of fraudsters herald themselves as having
paid their debt to society.” Ratley said that he doesn’t “look at their
debt as being paid until all of their victims have been reimbursed”
(Patterson).

Years later, Webne engaged in another check fraud and payroll
scheme almost identical in nature to his previous scheme, this time
with a new employer, and was subsequently charged with embezzling
another million dollars. His sentence for this second offense was
more severe, and he was sentenced to 63 months in prison and
ordered to pay restitution of the full million that he had stolen
(Roguski). According to Ratley, “it is indeed common for a fraudster
to perpetrate a second fraud when they get in a position of trust.
Based on our knowledge, we feel very strongly that when dealing
with a reformed perpetrator, you should maintain and arm’s-length
relationship, regardless of the circumstances” (Patterson).

Responsibility to Victims
The knowledge that white collar crime can become an addiction,
or at least a compulsion over which a sense of choice is diminished
and a sense of obligation is increased, does not suggest that there
should be any reduction in public contempt for white collar offenders
whose actions have caused such harm to society. The issue of
responsibility still stands and the white collar criminal must still
face his or her consequences.

Responsibility as a concept, however, can be viewed a bit differently
under the light of addiction. To begin with, there is the responsibility
that companies or employers have to ensure that they are creating
the safest atmosphere possible to prevent fraud from festering and
growing under their watch. If it is determined that there was a lapse in
efforts on the part of employers or company owners to create a strong
perception of detection and internal control structure, then they
should bear some of the burden of restitution for victims affected by
individuals who perpetuate fraud on their premises. Along different
lines, the criminal justice system has a responsibility to ensure that
white collar criminals and those who facilitate them, even through
the company but is also directed at preventing the facilitation of
fraud. Punishment strategies can incorporate various
aspects of treatment in their wake. In fact, punishment can be
commingled with treatment. In this sense, restitution and community
service coupled with jail time and public shaming becomes a more
potent punishment strategy in light the addiction factor in white
collar crime.

Further, the red flags of addiction as presented by the Alavi study
indicate that the lack of a strong support system; loneliness, stress,
anger, and depression; and job dissatisfaction can also set the stage
for addiction. Perhaps a component of prevention could incorporate
screening employees for signs of the aforementioned precursors of
addiction.

Perspectives on Punishment
Some experts believe that the recidivism rate in white collar crime is
higher because of the lack of sufficient punishment. The awareness
of the addictive nature of white collar crime can help vulnerable
populations through incorporating more effective punishment
strategies to deter future would-be criminals from starting down
the path of fraud. Punishment strategies can incorporate various
aspects of treatment in their wake. In fact, punishment can be
commingled with treatment. In this sense, restitution and community
service coupled with jail time and public shaming becomes a more
potent punishment strategy in light the addiction factor in white
collar crime.

Based on rational choice theories and the research done by Hollinger
and Clark, getting caught and exposed is a white collar criminal’s
worst fear, and, as such, punishments should include public shaming
to make committing white collar crime that much less attractive.
While punishment itself is important, restitution as a mode of
punishment takes on new meaning under the umbrella of addiction
theory. Restitution is a crucial component of the eighth step of “The
Twelve Steps of Alcoholics Anonymous: “Made a list of all persons
we had harmed, and became willing to make amends to them all.” In
this light, restitution can be perceived as helping not only the victim
of the crime but also the white collar criminal as a victim of his or her
own addiction. It can be viewed as treating him or her by allowing
for growth on a deeper, spiritual level. Along the same lines, service to
others can be part of the treatment/punishment, as it is a twelve-step–style attempt at reformation through spiritual growth away from addiction.

While it is important to mention that addiction treatment usually focuses on overcoming addiction through medical or behavioral treatments, medical treatment would be problematic in white collar crime because of the behavioral nature of the addiction and the high costs of implementation. However, there are many medications advertised publicly that claim to be effective in treating addictive types of behaviors. Behavioral therapies center on various techniques, but group therapy is particularly effective, for example, the twelve-step groups. Addiction treatment through group therapy can present some additional perspective on punishment mixed with treatment. Requiring white collar criminals to sit in group meetings for victims of white collar crime may help to open their eyes to their problem.

CONCLUSION

Not only can the field of forensics benefit from addiction theory, perhaps the treatment of addiction can benefit from investigating the strategies used in confronting the problem of white collar crime. It may be realistic to incorporate the best of both worlds. Because of the addictive nature of white collar crime, the concepts of responsibility and victim are expanded and can present useful insights into prevention and punishment strategies.

It is interesting to note that there has been considerable research done in an attempt to answer the question of who will commit white collar crimes, and from that research there has emerged a commonly accepted general rule of thumb called the 80-10-10 rule, and while anyone can become addicted, this rule indicates initially that 10 percent of people are just plain good and would not commit a crime no matter the circumstances, 10 percent of the population is the opposite and would commit a crime at every chance, while the remaining 80 percent are victims or victimizers of circumstance depending on the situation (Auditor of Public Accounts). This means that a substantial number of potential white collar criminals will be susceptible to various influences in their environment that may have the power to make or break them as white collar criminals. New perspectives on prevention and punishment gained by looking at white collar crime through the lens of addiction may save not only some of the 80 percent mentioned above, but many of their potential victims, as well.

WORKS CITED


C. MORGAN LITTLE

C. Morgan Little is a Stevenson Graduate Student in the Forensic Accounting Program. She currently works for the Department of the Treasury, Office of the Inspector General. She also holds a BA in Psychology from the University of Notre Dame in South Bend, IN.
Correlation Between Occupational Stress, Burnout, and Job Satisfaction in Forensic Scientists
Elizabeth Elliott

ABSTRACT

This research studied the correlation between occupational stress, burnout, and job satisfaction in forensic scientists. The theory was that if a forensic scientist had high levels of occupational stress and burnout, they would have low levels of job satisfaction. To analyze these aspects, three different surveys were used: the Maslach Burnout Inventory-General Survey (MBI-GS), the Perceived Stress Scale (PSS), and the Job Satisfaction Survey (JSS). The final survey was sent out to forensic scientists in four states and Washington D.C., with 60 participants responding. The results showed that forensic scientists have moderate levels of occupational stress, high levels of burnout, and high levels of job satisfaction, which contradicts the original theory.

INTRODUCTION

There are many definitions surrounding the concept of stress. In its basic form, stress occurs when a person is unable to cope with external pressures (Coffey, Stress and Burnout). The extent to which a person copes with stress is dependent on their physiological and psychological state (Coffey and Coleman). According to a survey published by the American Psychological Association in 2010, 44% of Americans said their stress level has increased in the past five years. An increase in stress levels can cause numerous mental and physical health issues such as anger, fatigue, and anxiety (Kirby and Pollock). Many factors lead to increased stress levels, including money, health concerns, and family responsibilities. The one factor that creates the most stress in peoples’ lives, other than money, is stress about work, otherwise known as occupational stress (Clay). Recent studies have shown the effects of occupational stress on burnout and job satisfaction.

Occupational stress can place unnecessary strain on a person’s mental, physical, and emotional well-being. There are many stressors that can cause high levels of occupational stress such as behavioral, attitudinal, emotional, interpersonal, and physical stressors (Carmack and Holm). In addition, occupational stress can be caused by working additional overtime shifts and having extended work schedules (Dembe, et al.). This type of stress not only threatens one’s health, but also has been associated with low levels of job productivity (Väänänen, et al.). Even a short duration of shift work has been known to cause a decrease in job performance and increase in occupational stress (van der Ploeg, et al.). Occupational stress can cause an abundance of negative events in one’s life, including burnout and lower job satisfaction.

Burnout is defined as a state of mental and physical exhaustion due to one’s occupation (Bakker and Costa). In general, burnout is caused by organizational factors such as a lack of resources and high job demand (Happell, et al., Stress and Burnout). If burnout occurs for a long period, a person may become bored or depressed. These psychological emotions can lead to alienation from work, family, and friends (Adderley, et al.). Alienation contributes to lost working days and job turnover, which results in the loss of revenue for businesses (Avanzi, et al.). Burnout not only affects one’s physical and mental state, but also takes a toll on job satisfaction.

Job satisfaction is how satisfied or dissatisfied a person is with their job. If someone has high job satisfaction, they generally enjoy their job. On the other hand, if someone has low job satisfaction, they have negative feelings towards their job (Ozpehlivan and Acar). Job satisfaction can be affected by personal relationships with coworkers, expectations of the work environment, and the organization of the employer (Happell, et al., Burnout and Job Satisfaction). When job satisfaction is low, an employee may not care about their job and may begin to make mistakes. These mistakes can lead to high turnover rates and a loss of revenue for a business. The inverse relationship between burnout and job satisfaction shows that a high level of burnout correlates with a low level of job satisfaction (Bakker and Costa). This correlation is created by the presence of occupational stress.

The correlation between occupational stress, burnout, and job satisfaction has been studied extensively within many professions, such as nursing, teaching, and law enforcement (Coffey and Coleman). Quite a bit of research has been devoted to occupational stress, burnout, and job satisfaction in forensic healthcare workers and nurses. Forensic scientists deal with an enormous amount of stress due to an excessive workload that creates lengthy backlogs and a shortage of staff (Sewell). While occupational stress is an issue in forensic science, little to no research has been conducted on this topic. This research focuses on the correlation between occupational stress, burnout, and job satisfaction among forensic scientists.

METHODS

Participants
The online survey was sent, via e-mail, to various forensic laboratory directors in the states of Maryland, Virginia, Delaware, Pennsylvania, and the District of Columbia. In total, the survey was sent to 18 forensic science laboratories in the above-mentioned states. Once the laboratory directors received the survey, they proceeded to send the survey out to their employees. Since the survey was distributed by the laboratory directors and not by the person giving the survey, it is not possible to determine the response rate. A total of 67 surveys was received, however seven of those surveys were incomplete. Those incomplete surveys were not used in the data analysis; therefore, only 60 responses were included. It can be assumed that the response rate for this survey was low, based on the low number of participants, despite the high number of employees in these forensic science laboratories.
Overall, the sample population consisted of 73.8% (n=47) women and 21.3% men (n=13). Of these participants, 26.6% (n=16) were in the age range of 21 to 29; 40% (n=24) were 30 to 39, 16.7% (n=10) were 40 to 49, 15% (n=9) were 50 to 59, and 1.7% (n=1) were 60 or older. Over half of the sample population, 63.3% (n=38), have a master's degree, while 31.7% (n=19) have a bachelor's degree. The length of time at a current forensic science job was greatest between 0 to 5 years at 56.7% (n=34). In correlation with this statistic, 31.6% (n=19) of the participants have been in the field of forensics for 0 to 5 years, 30% (n=18) for 5 to 10 years, 25% (n=15) for 10 to 20 years, 6.7% (n=4) for 20 to 30 years, and 6.7% (n=4) for 30 to 40 years. Within the realm of forensic science, 33.3% (n=20) work in Chemistry/Toxicology/Drug Chemistry, 28.3% (n=17) work in DNA/Biology, 16.8% (n=10) work in Crime Scene Investigation, 6.7% (n=4) in Management, 5% (n=3) in Latent Prints, and 3.3% (n=2) in Trace Evidence, Firearms, and Tool marks, or other disciplines.

Measures

Three different surveys were combined into one general survey to measure burnout, occupational stress, and job satisfaction. Those surveys are as follows: the Maslach Burnout Inventory- General Survey (MBI-GS), the Perceived Stress Scale (PSS), and the Job Satisfaction Survey (JSS).

The Maslach Burnout Inventory- General Survey was developed by Christina Maslach to measure three different levels of burnout, professional efficacy, exhaustion, and cynicism in occupations with little to no contact with clients. Professional efficacy is having a sense of accomplishment and success in one’s work. Exhaustion is feeling tired and fatigued from the demands of work. Cynicism is when a person develops an indifferent attitude and loses interest in his or her work (Maslach, et al.). The 16-question survey has participants answer each question on a seven-point Likert scale (0=never, 1=almost never, 2=sometimes, 3=fairly often, and 4=very often). Scoring was completed by applying reverse scoring (that is, 0=4, 1=3, 2=2, and 4=0) to the four positively stated items, and scoring the rest of the questions with the normal scale. According to Sheldon Cohen, who developed this survey, the higher the score means the more stress in one’s life; however, there are no definitive ranges for determining a person’s level of stress (Cohen, et al.). For this survey, a scale was created to determine the level of occupational stress. Low occupational stress would have a score between 0 and 13, moderate occupational stress would have a score between 14 and 26, and high occupational stress would have a score between 27 and 40.

The Job Satisfaction Survey was originally used for human service organizations, but it can now be used for all types of organizations and jobs. This 36-item survey measures employees’ attitudes toward and satisfaction with their current job. Within these 36 questions, there are nine subscales (pay, promotion, supervision, fringe benefits, contingent rewards, operating procedures, coworkers, nature of work, and communication) that can affect one’s job satisfaction. Each question is graded on a six-point Likert scale (1=disagree very much, 2=disagree moderately, 3=disagree slightly, 4=agree slightly, 5=agree moderately, and 6=agree very much). All negatively worded questions had reverse scoring applied before finding the sum. Since the original JSS was too long for the purpose of this survey, 14 questions were randomly chosen to be used in this survey. The principle behind the Job Satisfaction Survey is that participants who agree with the positively worded questions and disagree with the negatively worded questions would display a level of satisfaction with their job. However, participants who disagree with positively worded questions and agree with negatively worded questions would display a level of dissatisfaction with their job. In general, a higher score would represent a higher level of job satisfaction (Spector). There is no set numerical scale to determine how satisfied or dissatisfied someone is with their job. For this survey, a scale was created to distinguish the level of job satisfaction in the participant. The maximum score of 84 was divided into three categories: low, moderate, and high job satisfaction. A score of 0 to 28 would demonstrate low job satisfaction. Moderate job satisfaction would be between 27 and 56. A score of 57 to 84 would indicate high job satisfaction. The higher the total score, the greater the level of job satisfaction.

The Perceived Stress Scale is designed to measure the perception of stress in an individual. Questions are geared towards how unpredictable and uncontrollable a subject’s life was during the past month and how these events affect a person’s stress level. For the purpose of this survey, the questions were altered to address occupational stress. For example, the original question would ask “In the past month, how often have you felt nervous or ‘stressed’?” To adapt the question to the needs of this survey, the question was reworded as such: “In the past month, how often have you felt nervous or ‘stressed’ at work?” The ten-question survey had participants rate their stress level at work in the past month on a five-point Likert scale (0=never, 1=almost never, 2=sometimes, 3=fairly often, and 4=very often). Scoring was completed by applying reverse scoring (that is, 0=4, 1=3, 2=2, and 4=0) to the four positively stated items, and scoring the rest of the questions with the normal scale.
RESULTS

Maslach Burnout Inventory- General Survey
For the whole population, the mean score for professional efficiency was 28.7 (SD=6.5), and 56.7% of forensic scientists have a high level of professional efficacy. The mean score for exhaustion was 13.6 (SD=7.9). The exhaustion scores were almost split in half, with 38.3% having a high exhaustion level and 35% having a low exhaustion level. There was a high level of cynicism among forensic scientists, with almost half (46.7%) having high scores, and the mean amount being 11.2 (SD=7.4). Table 2 gives a summary of these findings.

When looking at how long the participants have been in the field of forensic science, the two groups with the largest percentage of highest scores in professional efficacy are those having worked 0 to 5 years at 63.2% (mean=29.6, SD=5.9), and those having worked 30 to 40 years at 75% (mean=31.8, SD=2.2). In addition, forensic scientists who have worked 5 to 10 years have a large percentage of high scores for level of exhaustion at 55.6% (mean=17.8, SD=7.1), and a large percentage of high scores for level of cynicism at 61.1% (mean=13.3, SD=9.1). Table 3 gives a summary of these findings.

Within each discipline of forensic science, most participants have moderate to high levels of professional efficacy. Trace Evidence, Firearms and Tool marks, and other disciplines have 100% high professional efficiency scores; however, this data is based on only two participants working in each of those disciplines. On the other hand, most of the disciplines have moderate to high levels of exhaustion and cynicism. Chemistry/Toxicology/Drug Chemistry had a large percentage of high exhaustion level scores at 50% (mean=16.9, SD=9.7) and a large percentage of high scores for cynicism at 40% (mean=12.6, SD=9.1). Crime Scene Investigation had a large percentage of low scores for exhaustion at 60% (mean=10.6, SD=7.5). Table 4 gives a summary of these findings.
There were three types of labs that participated in this survey: state, municipal, and private. All three types of forensic laboratories have moderate to high scores for professional efficiency, with state laboratories having the highest score, 58% (mean=28.4, SD=7.3). Private forensic laboratories have the largest percentage of high exhaustion level scores at 80% (mean=21, SD=5.0). Municipal laboratories have the highest percentage of low exhaustion levels at 71.4% (mean=9.3, SD=7.0); however, they have the greatest level of high cynicism scores at 57.1% (mean=11.6, SD=7.7). Table 5 has a summary of these findings.

An optional question was asked for participants to disclose which laboratory they currently worked at. Over half of the population (56.6%, n=34) decided to skip this question. However, those who responded to this question were from the following laboratories: Maryland State Police 23.3% (n=14), NMS 8.3% (n=5), Washington DC Department of Forensic Science 6.7% (n=4), Office of the Chief Medical Examiner, Maryland 1.7% (n=1), Pennsylvania 1.7% (n=1), and Western Maryland Regional Crime Laboratory 1.7% (n=1). When looking at burnout, most of these employers have a large percentage of high professional efficacy levels, except for NMS at 60% (mean=30.4, SD=3.1) moderate levels, Pennsylvania at 100% (n=1) moderate levels, and Western Maryland Regional Crime Laboratory at 100% (n=1) moderate levels. Laboratories that scored a large percentage of high levels of exhaustion include NMS at 80% (mean=21.2, SD=6.0) and Pennsylvania at 100%. On the other hand, DC Department of Forensic Science (mean=10.3, SD=9.0),

Table 4: Summary of MBI-GS, Disciplines, continued

<table>
<thead>
<tr>
<th>Crime Scene Investigation</th>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Efficacy</td>
<td>mean=24.5, SD=10.7</td>
<td>30% (n=3)</td>
<td>40% (n=4)</td>
</tr>
<tr>
<td>ExHAustion</td>
<td>mean=10.6, SD=7.5</td>
<td>60% (n=6)</td>
<td>20% (n=2)</td>
</tr>
<tr>
<td>Cynicism</td>
<td>mean=13.8, SD=7.0</td>
<td>20% (n=2)</td>
<td>10% (n=1)</td>
</tr>
</tbody>
</table>

DNA/Biology

| Professional Efficacy     | mean=29.3, SD=5.1 | 11.7% (n=2) | 35.3% (n=6) | 53% (n=9) |
| ExHAustion                | mean=13.8, SD=6.2 | 29.40% (n=5) | 23.50% (n=4) | 47.10% (n=8) |
| Cynicism                  | mean=8.7, SD=5.8 | 29.40% (n=5) | 41.20% (n=7) | 29.40% (n=5) |

Firearms and Tool marks

| Professional Efficacy     | mean=30.5, SD=0.70 | 0% (n=0) | 0% (n=0) | 100% (n=2) |
| ExHAustion                | mean=15.5, SD=14.8 | 50% (n=1) | 0% (n=0) | 50% (n=1) |
| Cynicism                  | mean=10, SD=12.7  | 50% (n=1) | 0% (n=0) | 50% (n=1) |

Latent Prints

| Professional Efficacy     | mean=29.6, SD=5.9 | 0% (n=0) | 66.70% (n=2) | 33.30% (n=1) |
| ExHAustion                | mean=7.3, SD=3.5  | 66.70% (n=2) | 33.30% (n=1) | 0% (n=0) |
| Cynicism                  | mean=12.3, SD=4.7 | 33.30% (n=1) | 0% (n=0) | 66.70% (n=2) |

Management

| Professional Efficacy     | mean=30, SD=3.2  | 0% (n=0) | 50% (n=2) | 50% (n=2) |
| ExHAustion                | mean=10.3, SD=0.95 | 25% (n=1) | 75% (n=3) | 0% (n=0) |
| Cynicism                  | mean=12.3, SD=5.2 | 0% (n=0) | 75% (n=3) | 25% (n=1) |

Trace Evidence

| Professional Efficacy     | mean=33.5, SD=0.70 | 0% (n=0) | 0% (n=0) | 100% (n=2) |
| ExHAustion                | mean=10, SD=1.4   | 50% (n=1) | 50% (n=1) | 0% (n=1) |
| Cynicism                  | mean=10.5, SD=0.70 | 0% (n=0) | 50% (n=1) | 50% (n=1) |

Other

| Professional Efficacy     | mean=35.5, SD=0.70 | 0% (n=0) | 0% (n=0) | 100% (n=2) |
| ExHAustion                | mean=13, SD=8.5    | 50% (n=1) | 0% (n=0) | 50% (n=1) |
| Cynicism                  | mean=8, SD=8.5     | 50% (n=1) | 0% (n=0) | 50% (n=1) |

Table 5: Summary of MBI-GS, Type of Lab

<table>
<thead>
<tr>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional Efficacy</td>
<td>mean=28.4, SD=7.3</td>
<td>21% (n=9)</td>
</tr>
<tr>
<td>ExHAustion</td>
<td>mean=12.6, SD=7.7</td>
<td>39.6% (n=17)</td>
</tr>
<tr>
<td>Cynicism</td>
<td>mean=11.3, SD=7.7</td>
<td>21% (n=9)</td>
</tr>
</tbody>
</table>

Municipal

<table>
<thead>
<tr>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Efficacy</td>
<td>mean=27.9, SD=4.9</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>ExHAustion</td>
<td>mean=9.3, SD=7.0</td>
<td>71.4% (n=5)</td>
</tr>
<tr>
<td>Cynicism</td>
<td>mean=11.6, SD=7.7</td>
<td>28.6% (n=2)</td>
</tr>
</tbody>
</table>

Private

<table>
<thead>
<tr>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Efficacy</td>
<td>mean=30.7, SD=3.0</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>ExHAustion</td>
<td>mean=21, SD=5.0</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Cynicism</td>
<td>mean=10.5, SD=6.5</td>
<td>20% (n=3)</td>
</tr>
</tbody>
</table>
Maryland State Police (mean=13.1, SD=8.3), Office of the Chief Medical Examiner, Maryland (100%), and Western Maryland Regional Crime Laboratory (100%) all scored low levels of exhaustion with larger percentages. Most participating laboratories had large percentages of high to moderate cynicism levels, except for the Office of the Chief Medical Examiner, Maryland, which had a larger percentage of low exhaustion scores (100%). Table 6 gives a summary of these findings.

<table>
<thead>
<tr>
<th>Table 6: Summary of MBI-GS, Employer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Scores</strong></td>
</tr>
<tr>
<td><strong>DC Department of Forensic Science</strong></td>
</tr>
<tr>
<td>Professional Efficacy mean=30.0, SD=5.0</td>
</tr>
<tr>
<td>Exhaustion mean=10.3, SD=9.0</td>
</tr>
<tr>
<td>Cynicism mean=12.3, SD=8.5</td>
</tr>
<tr>
<td><strong>Maryland State Police</strong></td>
</tr>
<tr>
<td>Professional Efficacy mean=29.1, SD=5.7</td>
</tr>
<tr>
<td>Exhaustion mean=13.1, SD=8.3</td>
</tr>
<tr>
<td>Cynicism mean=11.7, SD=8.3</td>
</tr>
<tr>
<td><strong>NMS</strong></td>
</tr>
<tr>
<td>Professional Efficacy mean=30.4, SD=3.1</td>
</tr>
<tr>
<td>Exhaustion mean=21.2, SD=6.0</td>
</tr>
<tr>
<td>Cynicism mean=8.2, SD=7.9</td>
</tr>
<tr>
<td><strong>Office of the Chief Medical Examiner, Maryland</strong></td>
</tr>
<tr>
<td>Professional Efficacy</td>
</tr>
<tr>
<td>Exhaustion</td>
</tr>
<tr>
<td>Cynicism</td>
</tr>
<tr>
<td><strong>Pennsylvania</strong></td>
</tr>
<tr>
<td>Professional Efficacy mean=29.6, SD=5.9</td>
</tr>
<tr>
<td>Exhaustion mean=13.6, SD=7.9</td>
</tr>
<tr>
<td>Cynicism mean=11.2, SD=7.4</td>
</tr>
<tr>
<td><strong>Western Maryland Regional Crime Lab</strong></td>
</tr>
<tr>
<td>Professional Efficacy mean=29.6, SD=5.9</td>
</tr>
<tr>
<td>Exhaustion mean=13.6, SD=7.9</td>
</tr>
<tr>
<td>Cynicism mean=11.2, SD=7.4</td>
</tr>
</tbody>
</table>

PERCEIVED STRESS SCALE

Over half of the forensic science population as a whole, 55% (mean=16.6, SD=6.6), had moderate levels of occupational stress. Low levels of occupational stress were at 37%, while high levels were only at 8% for the overall number of forensic scientists. When looking at the years in forensic science, all age ranges have high percentages of low to moderate occupational stress. The largest percentage of low occupational stress scores comes from the participants who have worked the longest as forensic scientists at 30 to 40 years, 100% (mean=9, SD=4.3). The rest of the ranges have high percentages of moderate occupational stress, with those having worked 0 to 5 years in the field of forensics having the greatest percentage of moderate occupational stress levels at 63.2% (mean=17.2, SD=7.5). Table 7 has a summary of these findings.

<table>
<thead>
<tr>
<th>Table 7: Summary of Perceived Stress Scale, Years in Forensic Science</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Scores</strong></td>
</tr>
<tr>
<td>0-5 years mean=17.2, SD=7.5</td>
</tr>
<tr>
<td>5-10 years mean=18.3, SD=6.1</td>
</tr>
<tr>
<td>10-20 years mean=15.5, SD=5.8</td>
</tr>
<tr>
<td>20-30 years mean=18, SD=4.5</td>
</tr>
<tr>
<td>30-40 years mean=9, SD=4.3</td>
</tr>
</tbody>
</table>

Similar to what was stated above, most disciplines in forensic science had high percentages of low to moderate occupational stress scores. Both Chemistry/Toxicology/Drug Chemistry (mean=18.6, SD=7.6) and Crime Scene Investigation (mean=16.2, SD=3.4) had the highest percentage of moderate occupational stress levels at 70%. Firearms and Tool marks, Management, and Trace Evidence all have high percentages of low occupational stress, which are greater than 50%. Table 8 has a summary of these findings.

<table>
<thead>
<tr>
<th>Table 8: Summary of Perceived Stress Scale, Discipline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Scores</strong></td>
</tr>
<tr>
<td>Chemistry/Toxicology mean=18.6, SD=7.6</td>
</tr>
<tr>
<td>CSI mean=16.2, SD=3.4</td>
</tr>
<tr>
<td>DNA/Biology mean=17, SD=6.6</td>
</tr>
<tr>
<td>Firearms &amp; Tool marks mean=18, SD=4.5</td>
</tr>
</tbody>
</table>

Table 8: Summary of Perceived Stress Scale, Discipline continues on next page.
Table 8: Summary of Perceived Stress Scale, Discipline, continued

<table>
<thead>
<tr>
<th>Discipline</th>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latent Prints</td>
<td>33.3% (n=1)</td>
<td>66.7% (n=2)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Management</td>
<td>75% (n=3)</td>
<td>25% (n=1)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Trace Evidence</td>
<td>100% (n=2)</td>
<td>0% (n=0)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Other</td>
<td>50% (n=1)</td>
<td>0% (n=0)</td>
<td>50% (n=1)</td>
</tr>
</tbody>
</table>

Table 9: Summary of Perceived Stress Scale, Type of Lab

<table>
<thead>
<tr>
<th>Type of Lab</th>
<th>Low Scores</th>
<th>Moderate Scores</th>
<th>High Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>41.9% (n=18)</td>
<td>55.8% (n=24)</td>
<td>2.3% (n=1)</td>
</tr>
<tr>
<td>Municipal</td>
<td>57.1% (n=4)</td>
<td>42.9% (n=3)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Private</td>
<td>0% (n=0)</td>
<td>60% (n=6)</td>
<td>40% (n=4)</td>
</tr>
</tbody>
</table>

Table 10: Summary of Perceived Stress Scale, Employer

<table>
<thead>
<tr>
<th>Employer</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC DFS</td>
<td>50% (n=2)</td>
<td>50% (n=2)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>MSP</td>
<td>57.2% (n=8)</td>
<td>42.8% (n=6)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>NMS</td>
<td>0% (n=0)</td>
<td>60% (n=3)</td>
<td>40% (n=2)</td>
</tr>
<tr>
<td>OCME, Maryland</td>
<td>100% (n=1)</td>
<td>0% (n=0)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>0% (n=0)</td>
<td>100% (n=1)</td>
<td>0% (n=0)</td>
</tr>
<tr>
<td>Western MD</td>
<td>100% (n=1)</td>
<td>0% (n=0)</td>
<td>0% (n=0)</td>
</tr>
</tbody>
</table>

Table 11: Summary of Job Satisfaction Scale, Years in Forensic Science

<table>
<thead>
<tr>
<th>Years</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5 years</td>
<td>0% (n=0)</td>
<td>36.8% (n=7)</td>
<td>63.2% (n=12)</td>
</tr>
<tr>
<td>5-10 years</td>
<td>0% (n=0)</td>
<td>55.6% (n=10)</td>
<td>44.4% (n=8)</td>
</tr>
<tr>
<td>10-20 years</td>
<td>0% (n=0)</td>
<td>33.3% (n=5)</td>
<td>66.7% (n=10)</td>
</tr>
<tr>
<td>20-30 years</td>
<td>0% (n=0)</td>
<td>25% (n=1)</td>
<td>75% (n=3)</td>
</tr>
<tr>
<td>30-40 years</td>
<td>0% (n=0)</td>
<td>25% (n=1)</td>
<td>75% (n=3)</td>
</tr>
</tbody>
</table>

Table 12 summarizes the job satisfaction levels for each forensic science discipline. Both Management and Firearms and Tool marks have the largest percentages of high levels of job satisfaction at 100%, however the low number of participants for those disciplines may affect the results of job satisfaction scoring. Chemistry/Toxicology/Drug Chemistry are each at 50% (mean=57, SD=13.1) for moderate and high levels of job satisfaction. DNA/Biology also had a large percentage of high levels of job satisfaction with 76.5% (mean=59.9, SD=8.9).

Of the participants who disclosed where they worked, none of the laboratories demonstrated large percentages of high levels of occupational stress, except NMS with 40% (n=2). Employers who had high percentages of moderate occupational stress were Washington DC Department of Forensic Science (mean=15.3, SD=3.6), NMS (mean=24.8, SD=5.6), and Pennsylvania (100%, n=1). All other laboratories scored higher percentages for the low range for occupational stress. Table 10 gives a summary of these findings.

**JOB SATISFACTION SURVEY**

Due to the wide response ranges in the Job Satisfaction Survey, none of the participants were categorized as having high percentages of low job satisfaction. This issue will be discussed later in this paper. Overall job satisfaction in the forensic science field is almost split evenly, with 60% of forensic scientists having high job satisfaction and 40% having moderate job satisfaction. All the percentage ranges either had moderate or high job satisfaction. Participants who had worked 20 to 30 years or 30 to 40 years in the field of forensic science had the highest percentage of high job satisfaction at 75%. Forensic scientists who have worked less in this field had high percentages of moderate job satisfaction, with those having worked 5 to 10 years responding at 55.6%. Table 11 shows a summary of these findings.
State forensic science laboratories had the highest level of job satisfaction with 67.4% (mean=60, SD=11.2) of the participants scoring high for job satisfaction. In a private forensic science laboratory, 60% (mean=53.2, SD=7.8) of participants had moderate job satisfaction. The participants who worked in municipal forensic science laboratories scored a high percentage in the moderate range for job satisfaction at 57.1% (mean=58.1, SD=9.8). Table 13 gives a summary of these findings.

Out of the six laboratories that participated in this survey, four of those laboratories had forensic scientists with the largest percentage of high job satisfaction. Those laboratories are the following: Washington DC Department of Forensic Science (mean=59, SD=5.2), Maryland State Police (mean=57.5, SD=9.9), Office of the Chief Medical Examiner, Maryland (100%), and Western Maryland Regional Crime Laboratory (100%). The other laboratories, NMS (mean=54.2, SD=7.2) and Pennsylvania (100%) had larger percentages of high levels of moderate job satisfaction. Table 14 shows a summary of these findings.

DISCUSSION

Studies have shown an inverse relationship between occupational stress, burnout, and job satisfaction. High levels of occupational stress cause high levels of burnout and low levels of job satisfaction. On the other hand, low levels of occupational stress cause low levels of burnout and high levels of job satisfaction (Happell, et al., Burnout and Job Satisfaction). To demonstrate this theory, three surveys were combined to analyze occupational stress, burnout, and job satisfaction in forensic scientists.

Many believe that burnout only occurs in those whose occupations involve caring for others, such as healthcare. However, studies have shown that burnout is not unique to care professions (Smart, et al.). Studies have shown that burnout can be stable and last for five, ten, or even fifteen years (Bakker and Costa). If this theory presents as true, then forensic scientists who work in the field of forensics for a long time will have increased levels of burnout and stress, which would translate to lower levels in job satisfaction. Per the guidelines for burnout defined by the MBI-GS, forensic scientists who have been working from 5 to 10 years have the greatest amount of burnout due to high levels of exhaustion and cynicism and only moderate levels of professional efficacy. Participants who have worked in the forensic science field for 30-40 years show signs of low burnout, having a high professional efficacy, low exhaustion, and moderate cynicism. No matter how long a participant has worked in the field of forensic science, the majority scored a moderate occupational stress level, with those having worked 20 to 30 years having scored the highest percentage of moderate occupational stress, followed by those having worked 0 to 5 years. Participants who have worked 30 to 40 years in forensic science have a low occupational stress level. The majority of participants have high levels of job satisfaction, except for participants who have worked in the field of forensic science for 5 to 10. These participants have a higher percentage of moderate job satisfaction.
satisfaction, rather than high job satisfaction. The data shows that the average participants who have been working in the field of forensic science for 5 to 10 years have a high level of burnout, a moderate level of occupational stress, and a moderate level of job satisfaction. On the other hand, participants who have been working in the field of forensic science for 30 to 40 years have low levels of burnout and occupational stress, and high job satisfaction. This goes against the original theory that the longer a participant works in the field of forensic science, the higher their levels of burnout and occupational stress will be. Participants who have spent fewer years in forensic science could have higher levels of burnout and occupational stress because they are trying to make a name for themselves within their organization. Participants who have worked in the field of forensic science longer may have low levels of burnout and occupational stress because they have already established themselves within the organization, so they experience less pressure.

Some studies show that stress does not randomly occur in an organization, rather there is a system of stress among different roles and different levels within an organization (Kirby and Pollock). Forensic science itself has many different roles within an organization, such as Trace Evidence, DNA/Biology, and Chemistry. In addition, forensic science has many different levels within an organization, including forensic scientists who work in the laboratory, crime scene investigators, and management. These different roles and levels within an organization can have different effects on occupational stress, burnout, and job satisfaction. One would think that those in management roles would have more occupational stress and burnout than those working in the laboratory. The discipline of Chemistry/Toxicology/Drug Chemistry causes a high level of exhaustion and cynicism, which correlates to high levels of burnout. However, those in this discipline also have a high level of professional efficacy, which doesn't exactly agree with the guidelines for burnout. Crime scene investigation has low levels of exhaustion and cynicism and a moderate level of professional efficacy. This would demonstrate that crime scene investigators have a lower level of burnout. Management has moderate levels of professional efficacy, exhaustion, and cynicism, which would show that they have moderate burnout. While management has moderate levels of burnout, they have low levels of occupational stress. Most of the other disciplines have moderate levels of occupational stress, with both Crime Scene Investigation and Chemistry/Toxicology/Drug Chemistry having the highest level of moderate occupational stress. Management has a high level of job satisfaction, while Firearms and Tool marks and Chemistry/Toxicology/Drug Chemistry have moderate job satisfaction. This data shows that management typically has lower levels of occupational stress and burnout in comparison to other disciplines that work in the laboratory; however, all employees in the different roles in forensic science seem to enjoy their job. The amount of occupational stress a person experiences could be based on the type of work they are doing and the type of support they receive at work (Adderley, et al.). It is possible for management to have lower levels of occupational stress and burnout due to the nature of their work and the support they receive from others. Working in a laboratory can produce a stressful work environment due to elevated backlogs and a shortage of staff.

Many believe that there is a correlation between caseload size, levels of stress, and burnout (Happell, et al., Stress and Burnout). In forensic science, there is always a high amount of casework due to backlogs and understaffing (Sewell). In addition, there could be a higher caseload depending on the type of forensic science laboratory one works in, which would cause high levels of occupational stress and burnout. Those working in private laboratories have high levels of exhaustion and cynicism. In addition, private lab employees have a high level of professional efficacy. Municipal laboratory employees have a low level of occupational stress, while those working in state and private laboratories have moderate levels of occupational stress. State laboratory employees have a high level of job satisfaction, while municipal and private laboratory employees have moderate levels of job satisfaction. Those working in private laboratories may have higher levels of stress and burnout because these organizations made up a larger part of the participants in comparison to state and municipal laboratories. Even with the high levels of occupational stress and burnout at private laboratories, it seems participants still are satisfied with their jobs.

Some people in the forensic science community are curious as to how their laboratory compares to others in the categories of occupational stress, burnout, and job satisfaction. Those working in the Washington DC Department of Forensic Science have a moderate to high level of professional efficacy, a low level of exhaustion, a high level of cynicism, a low to moderate level of stress, and moderate to high job satisfaction. The Maryland State Police laboratory employees have a high level of professional efficacy, a low level of exhaustion, a high level of cynicism, a low level of stress, and a high level of job satisfaction. NMS employees have a moderate level of professional efficacy, a high level of exhaustion, a low to moderate level of cynicism, moderate level of stress, and moderate level of job satisfaction. Those in the Office of the Chief Medical Examiner, Maryland have a high level of professional efficacy, low levels of exhaustion and cynicism, low levels of stress, and high levels of job satisfaction. The laboratory employees in Pennsylvania have moderate professional efficacy, high exhaustion and cynicism, moderate stress, and moderate job satisfaction. Finally, the Western Maryland Regional Crime Laboratory employees have moderate professional efficacy, low exhaustion, moderate cynicism, low stress, and high job satisfaction. When comparing all the laboratories, it seems those at NMS and the laboratory in Pennsylvania have a higher level of burnout than the other laboratories. In addition, the participants from NMS have a higher level of occupational stress than the rest of the laboratories, while the Maryland State Police have a lower level of occupational stress. Those at NMS showing a high level of stress
correlates to private laboratory employees displaying a high level of burnout, due to the increased sample size. The Maryland State Police also seemed to have the highest level of job satisfaction among participants.

In general, forensic scientists have a high level of professional efficacy, a high level of exhaustion, and a high level of cynicism. However, it should be noted that almost as many forensic scientists have a low level of exhaustion in comparison to those who have a high level of exhaustion. In relation to stress, 55% of the forensic science population surveyed have moderate occupational stress, 37% have low levels of occupational stress, and 8% have high levels of occupational stress. Job satisfaction was split almost evenly, with 60% of the forensic scientists having a high level of job satisfaction and 40% having moderate job satisfaction. This outcome could be possible because, while forensic science is a stressful job, those in occupations that help people tend to enjoy their job more than other occupations that do not help people to the same extent (Elliott & Daley).

One of the main reasons why workplace environments become toxic is because of decreasing job satisfaction caused by burnout and occupational stress (Özpehlivan & Acar). Burnout and occupational stress can lead not only to physical harm, but professional harm as well. High levels of burnout and occupational stress can cause anxiety, depression, and musculoskeletal problems (Xanthakis). In addition, high levels of burnout and occupational stress can lead to lowered job performance, increased job turnover, and increased lateness to work (Ewers, et al.). This is why it is important to decrease stress and burnout and increase job satisfaction in work environments to reduce stress-related ailments and increase productivity at work (Ito, et al.). One way to correct this problem is to have front-line managers who deal with difficult situations head-on and can resolve problems effectively and efficiently (Newman, et al.). Burnout can also be caused by having a lack of resources (Toppinen-Tanner, et al.). While forensic science may not have an extensive budget, if possible, forensic science laboratories should focus on hiring more staff, acquiring new instrumentation, and making sure that all staff is trained on all instrumentation. By having more employees and more efficient equipment, forensic scientists would not be as stressed about being short-staffed and their job satisfaction would increase. It also should be mentioned that a person can reduce stress and burnout by getting enough sleep, eating the proper diet, and having hobbies outside of the job (Sewell). One of the biggest reasons why employees become dissatisfied with their jobs is because they believe they receive inadequate rewards and compliments for their efforts (Avanzi, et al.). It is important for managers and supervisors to remember to encourage their staff and let them know that their efforts are important to the organization.

While this research evaluates an important issue in forensic science, there are limitations. Since the sample size for this research was only 60 participants, it is difficult to gather an accurate understanding of some of the results. Some of the statistics were based on only a few participants, giving a higher result than expected. This could skew the results and lead to inaccurate conclusions. Another flaw in gathering results was the scales used for the surveys, especially the Job Satisfaction Survey. The JSS has wide ranges for determining job satisfaction. These wide result ranges lead to the assumption that forensic scientists do not suffer from low job satisfaction. It should be noted, when analyzing these results, many participants were on the border between high and moderate job satisfaction. In addition, some participants who scored in the moderate job satisfaction range were on the lower level of that range. When considering these results, it should be mentioned that some participants who scored high in job satisfaction could actually have only moderate job satisfaction and some of the participants who scored as having moderate job satisfaction could actually have low job satisfaction. To produce more accurate job satisfaction results, a new range should be calculated or a different survey for job satisfaction should be used. In addition, a wider range of participation from different laboratories would give a better representation of occupational stress, burnout, and job satisfaction in forensic scientists. About half of the participants declined to reveal where they currently work. Without this information, it was difficult to compare results among local forensic science laboratories. Future work needs to be completed with a larger and more diverse sample size and a more accurate survey system to confirm the results found in this study.

In conclusion, the data shows that forensic scientists don't exactly follow the trend for burnout. While forensic scientists have high levels of exhaustion and cynicism, which are signs of burnout, they also have a high level of professional efficacy, which is the opposite of the signs of high burnout. This shows that, while forensic science causes high levels of exhaustion and cynicism, most people feel a sense of accomplishment and success within their jobs. With the high levels of exhaustion and cynicism, it is natural that stress levels are in the moderate range. This shows that an increase in burnout leads to an increase in occupational stress. However, forensic scientists in general seem to enjoy their jobs and have high job satisfaction, which does not correlate to their high levels of burnout and moderate levels of occupational stress. Many people believe there is a correlation between occupational stress, burnout, and job satisfaction. If someone has high levels of occupational stress and burnout, they will have low levels of job satisfaction. Forensic scientists do have moderate levels of occupational stress and high levels of burnout; however, these high and moderate levels do not translate to a decrease in job satisfaction, rather forensic scientists have a high level of job satisfaction. This information shows that there is not necessarily a correlation between occupational stress, burnout, and job satisfaction in forensic scientists. In addition, this research shows that even in a stressful environment, forensic scientists still enjoy their jobs.
WORKS CITED


**ELIZABETH ELLIOTT**

Ms. Elliott graduated from the University of the Sciences in Philadelphia in 2009 with a bachelor's degree in Medical Technology with a minor in Biology. In 2016, she received her Master's in Forensic Science from Stevenson University. She currently works at the Washington D.C. Medical Examiner's Office as a Forensic Toxicologist.
The Value and Potential of Forensic Models
Jacquelyn A. D. Jones

“The value and potential of forensic models stand in contrast to the familiar case of the death of a child. The Nutshell, a term coined by Mrs. Frances Glessner Lee, is a miniature scene of a death, complete with details of the body and its surroundings. These models provide the opportunity to hone skills in three-dimensional (3D) environments of locations and laboratories. In actuality, a crime scene is available for a short time and then closed.固定 in time, the Nutshells allow intense and repeated study of their details. Investigators by nature work in a physical, three-dimensional (3D) environment of location and laboratory. To have an opportunity to hone those skills with a static model is in concert with the likely learning preferences of those investigators. It may be that the phrase that inspired, and the models that continue to train can provide the simulation needed to draw attention to 3D models in a time of ever-increasing technology.

THE NUTSHELL STUDIES OF UNEXPLAINED DEATH

Corinne May Botz spent many years researching the life of Frances Glessner Lee, culminating in the book The Nutshell Studies of Unexplained Death, a routinely cited source for details on Mrs. Lee’s life. The period in American history from 1878 to the mid-1930s was not a time of considerable independence and autonomy for women, especially women of a high pedigree. There were expectations of motherhood and homemaking, not university and career. Mrs. Lee chose, at least for a time, to fulfill those expectations.

All previous life experience has a potential impact on an individual’s behavior and choices. Frances Glessner’s life experiences were no exception. She grew up in a controlled household, where she learned the domestic arts (such as sewing) and was surrounded by handmade household items, in keeping with her parents’ participation in the Arts and Crafts movement.

The Arts and Crafts Movement began in Europe around 1875. In 1895, The Chalk and Chisel Club became America’s first Arts and Crafts organization, and the movement in America lasted until 1916. According to Gustav Stickley, “the fundamental principles of honesty, simplicity, and usefulness” were the basis for the movement, featuring in homes and furnishings (Lonsinger). This period marked a shift from rural to urban and suburban life. Home ownership became the American dream, and the craftsman sought to furnish that dream with simple, useful, rustic-style furnishings (Lonsinger). Despite the simplicity, the homes and furnishings displayed quality craftsmanship and attention to detail.

It is easy to presume that these influences fostered Lee’s skill with designing and handmaking items. While a student at Harvard, her brother, George Glessner, introduced Lee to classmate George Burgess Magrath. Magrath would later become a medical examiner and muse for Lee’s forensic path. She eventually moved from her parents’ house to a house built by her parents for her and her husband. After having three children, Frances and Blewett Lee divorced in 1914 after several long separations. This family circumstance may have allowed for what would become Mrs. Lee’s legacy. Divorce in the early twentieth century was not necessarily a desirable condition, but it left Mrs. Lee to her own devices. Her children (and grandchildren and great grandchildren) have helped keep the connection to Lee vibrant in the decades following her death.

Mrs. Lee was a woman in her fifties in the 1930s, when the remaining ties that bound her began to fall. By 1938, her brother George, her mother, her daughter, her father, and George Magrath were all deceased, leaving Lee the heir to the International Harvester fortune (Botz 26). Mrs. Lee’s interest in legal medicine began, much to her father’s distaste, with her personal and intellectual connection to George Magrath. Financial freedom allowed Lee the opportunity to continue her pursuits in forensic investigations in earnest. Magrath had expressed his discontent over the lack of consistent training and qualifications for professionals who determined cause of death (Botz 26). By 1936, at Harvard University in Boston, Lee funded a professorship of legal medicine, established the George Burgess Magrath Library of Legal Medicine, and provided the George Burgess Magrath Endowment of Legal Medicine. Lee continued to gain expertise in investigations and manner of death determinations, and supported the revision of the coroner system in many states (Botz 27). After teaching herself about criminal investigation, Lee would come to be described as “a passionate crusader for justice and a tireless lobbyist for reform” (Oswald). Mrs. Lee realized that police or on-site investigators could easily miss clues and, therefore, make errors in identifying a criminal versus non-criminal death (Ramsland, The Truth in a Nutshell 16). In the course of training investigators and medical examiners, having an active scene or some appropriate location to practice was not reliable or feasible. Mrs. Lee saw the need for a tool — for the Nutshells.

Lee had already demonstrated a skill for creating very detailed miniature recreations, her first being a model of the Chicago Symphony Orchestra as a gift for her mother. Now she would turn her talents to design tools to instruct. She used actual crime scenes, police reports, and fiction to develop her scenarios. Lee hired a carpenter, Alton Mosher (and later, his son) to build the structures. She collected furnishings from all manner of sources — dollhouse furniture, charms, and handmade items. The “bodies,” sewn, painted, and positioned by Lee, particularized injury, decomposition, and, perhaps, the manner of death. Each of the 18 Nutshells has a brief description of the scene at the time of discovery, written by Lee and including names, dates, and some witness details.

The scale of the studies is one inch for one foot, making the largest no more than three feet tall. Mrs. Lee’s attention to the smallest detail is astounding. For example, there are likely two dozen or more wooden clothespins, each about one-eighth of an inch long, hand-carved from matchsticks. The scenes are of an array of environments, including
bathrooms, kitchens, a rooming house, a barn, a garage, and a saloon. Primarily, the “deceased” are women of a lower social class and station than Mrs. Lee.

When the Harvard Department of Legal Medicine closed in 1967, former professor Russell Fisher, M.D., then Maryland’s chief medical examiner, gained permission to install the Nutshell Studies in the Office of the Chief Medical Examiner (OCME) in Baltimore. The staff at the OCME is adamant about not characterizing the Nutshells as crime scenes; rather, they are scenes of unexplained death (Goldfarb). It is the job of the investigator, not to solve the crime, but to determine if the death depicted was murder, suicide, or accident by studying Mrs. Lee’s meticulously placed clues.

After completing the first few Nutshell Studies, Mrs. Lee began seminars at Harvard, inviting all manner of police and investigators. The first semi-annual seminars came at a time when police officers did not command much respect or credibility. The week of presentations from speakers and work with the Nutshells also included an elegant well-planned dinner, a certificate of completion, and membership in the Harvard Associates in Police Science (HAPS). Mrs. Lee’s program elevated the status of many police officers and gained immediate respect (Goldfarb).

As of 2016, there is at least one annual seminar (and sometimes a second, depending on demand) conducted in the same manner and for the same purpose as those managed by Mrs. Lee. There is an opportunity for participants to advance their understanding of the investigative topics presented by the speakers using visual aids, and examining the clues in the Nutshells (one per team) to determine how the individual depicted died. The 2016 speaker topics included subjects such as gunshot wounds, shotgun wounds, bloodstains, toxicology, hanging and strangulation, and cause and manner of death. Except for a discussion on tasers, the 19 topics all have a relation to the subject matter of the Nutshells or relevance to Mrs. Lee’s goals for developing expertise in investigators. As always, there is dinner (typically with some of Mrs. Lee’s descendants), a certificate, and HAPS membership.

In 1942, Lee received the honorary rank of Captain in the New Hampshire State Police, including the title of Education Director. This distinction allowed Lee to become the first female member of the International Association of Police Chiefs (Botz 30). In nearly every communication written by friends of Mrs. Lee, they all refer to her as Captain Lee.

There is some limited criticism of Frances Glessner Lee and the Nutshell Studies. The decoration and details are sometimes dated. In at least one of the models, a key item, while it still exists today, looks nothing like it did in the 1940s. However, present day investigators may find themselves in a location that is culturally or socioeconomically out of their circle of understanding. The details, the clues of the death, may not be familiar but are no less important. A reviewer of Ms. Botz’s book commented on the photographs of the Nutshells that, “the bodies are the least convincing … not even Lee could have come up with real tiny corpses,” but admits the close-up photography may be the issue (Gottlieb). There is speculation on Frances Glessner Lee’s motives for getting involved in forensic investigations, for waiting until her fifties before fully engaging, and the mental state of someone who creates scenes of death. The motive for any activity of any human being is obscure at best. Determining the motives for Mrs. Lee’s creation of the Nutshells more than fifty years after her death would be folly. Perhaps anticipating these concerns, Captain Lee stated that she wanted to “do something in my lifetime that should be of significant value to the community” (Botz 27). In 2004, then-Chief Medical Examiner Dr. David Fowler explained reactions to the Nutshells: “People take them as seriously as any other crime scene . . . I’ve never seen anybody make jokes, because of the degree of intricacy and detail. The quality is stunning” (Kahn). That these 18 three-dimensional models still provide insight and education speaks volumes, adding not only to Mrs. Lee’s legacy but also to the learning style they embrace.

THE RELEVANCE OF KINESTHETIC LEARNING

Frances Glessner Lee founded the Harvard Associates in Police Science (HAPS) in 1945. Her purpose was to provide a week-long seminar to improve the skill and reputations of police officers and investigators. By the strength of the organization she created, the seminars continued following Lee’s death and remained popular after the Nutshells moved to Baltimore in 1967. The annual HAPS seminar focuses on death investigations and features speakers, photographs, diagrams, and, of course, the Nutshells (Of Dolls and Murder). Education researchers would likely agree that the popularity and success of the training are due, in part, to the variety of teaching methods and tools used.

During Lee’s lifetime, the education community began thinking about how individuals learn new information. While there are countless learning theory models, most embrace one or more of seven categories: visual (see), aural (hear), physical/kinesthetic (do), verbal (say), logical (reason), social (group), and solitary (self). Of these seven, the first three account for the predominance of research, often know as sensory and perceptive learning.

Perhaps it is obvious that from infancy, people use their senses to get information about the world. Sight, smell, taste, hearing, and touch are how the very young experience their environment. It then would seem reasonable that early research of learning also focused on the senses and classroom activity. It looked at how teachers teach and how students comprehend. Visual, aural, and kinesthetic styles were strong early leaders in preferences.
Sensory learning preference was not a new concept at the time of Neil D. Fleming’s 1995 work, but his name is now nearly synonymous with VARK (Visual, Aural, Read/Write, and Kinesthetic) styles. Visual learners enjoy seeing charts, graphs, and photographs. Aural learners prefer hearing lectures or listening to recordings. The read/write category was a new separation with Fleming’s work. While reading a text, and taking notes have elements of the visual and kinesthetic, Fleming saw them as very different because of the concrete language element. Finally, the kinesthetic learners are the doers—needing to handle, move around, or engage in an activity.

Fleming developed the VARK Questionnaire: 16 questions or circumstances, each with four choices (one related to each of the VARK style preferences). In completing the survey, the test-taker may select one or more than one response that makes him or her most comfortable. The questionnaire, available free online, includes a scoring page to count the selected responses of each preference type.

The questionnaire is easy to use and score, making it a popular tool because, in Fleming’s words, “it avoids diagnostic labelling but provides a basis for selecting practical strategies” (Fleming 308). Since its introduction, the VARK questionnaire has been the subject of considerable scrutiny. The basic purpose of the intensive review was to evaluate if the questionnaire reliably measures what it claims to measure. Walter L. Leite, Marilla Svinicki, and Yuying Shi conducted a psychometric analysis to verify the validity of the questions themselves and the reliability of the results. A sample population of over 14,000, diverse over gender, age, and education, submitted their responses to the VARK questionnaire. The researchers used a four-factor correlated trait—correlated uniqueness model and found that the reliability estimates for the VARK were statistically adequate (Leite, et al. 325). They also noted that the VARK assessment questions, modified over various versions, improved the validity by improving the language (Leite, et al. 325).

The overall distribution of learning preferences is relatively equal when considering a broad range of test subjects, typically university students. Not surprisingly, students in particular interest groups did show strength in different modalities. For example, medical students most often favored kinesthetic learning (Prithishkumar and Michael 186), while music students selected the aural modality most frequently (Prithishkumar and Michael 186). Interestingly, criminal justice students seem to prefer a combination of modalities (Baker 54).

Kinesthetic preference may be either a primary preference or part of a multi-modal preference, and seems to be present in roughly 30 percent of the studied diverse populations (VARK Learn Limited). In either case, it means that the person trying to understand something new responds well to tactile experiences, models, and activity. This type of experiential learning seems to describe the work of the forensic investigator.

It is not a far reach to think that 30 percent of the diverse population involved in the crime-to-court process has, at least, some kinesthetic preference in how they receive information. It would make sense to communicate forensic results in a way that is relevant to both the investigative process and the court participants. Three-dimensional models of crime scenes or scenes of death are not new, as evidenced by the work of Frances Glessner Lee, but as technology advances, they may have greater relevance for the future.

DEFINING THE “CSI EFFECT”

In the early 2000s, television programming took on a new twist. Previously, there were police and medical dramas. Then a new franchise of shows began, CSI: Crime Scene Investigation. The CSI programs take investigations, often inspired by actual events, and show on-site evidence collection and analysis in a state-of-the-art forensics lab. Actual investigators will concede that the equipment is legitimate, and the executive producer of the first CSI series says that most of the television stage equipment is real and fully functioning. The problem for investigators is that no single lab has all the expensive machinery shown on television and the forensic process can take months (or years). All the evidence and investigation done in real life takes longer than a one-hour time slot (Of Dolls and Murder).

Beginning in about 2003, court personnel, prosecutors in particular, speculated on a “CSI effect.” The perception was (and is) that jurors who view television programs that feature forensic evidence are less likely to render a guilty verdict if forensic evidence is not available, and are too heavily reliant on it when it is present (Maeder and Corbett 84). Studies conducted on attorneys, both prosecution and defense, show that the lawyers believe that jurors are strongly influenced by such programming (Maeder and Corbett 86). Since attorneys began believing in the television influence, police noticed a decline in attorneys’ trial use of police reports and non-forensic evidence collected during investigations (Maeder and Corbett 87). Not surprisingly, judges also believe that there has been an increase in wrongful acquittals in cases where there was a lack of forensic evidence (Maeder and Corbett 88). These well-documented concerns have clearly inspired changes in trial presentations, but the validity of those concerns is still under investigation.

Research on whether viewing certain types of programming had an influence on attitudes and behavior often measured the frequency of exposure. One general conclusion, for example, was that frequently viewing programming featuring gay characters does not typically alter the attitude of the viewer to be more tolerant of other sexual orientations. Frequent viewing is more likely evidence of a predisposition for viewing certain types of shows and the existence of an already accepting attitude toward the content (Maeder and Corbett 93). Early research on the CSI effect took the same approach to measure the frequency of exposure to forensic programming and the attitude regarding a sample criminal case. Much like studies on
THE STATUS OF THREE-DIMENSIONAL PRINTING

The recorded beginning of three-dimensional (3D) printing technology is 1986, when Charles Hull received the first patent for the stereolithography apparatus (SLA) for a device he'd invented three years prior. Hull then co-founded 3D Systems Corporation, which continues to be a market leader (The Free Beginner's Guide). Since then, many patents have been filed, and the applications of 3D printing technology cover an array of business sectors, from manufacturing to food production. The development of this technology, up until recently, has focused on industrial and commercial use. As with most new products, the attention was on where there could be the greatest financial return, as the research and development phase of any new product can be costly.

The basic 3D printing process begins with a 3D digital model. That is, the specialized computer software can create or be used to design a new object, or a device like a laser scanner can scan an existing object for reproduction. Printer-compatible computer software then dissects the digital object into layers and the printer uses supplied materials such as plastics, metals, ceramics, and sand to reconstruct the digital image in physical form layer by layer (The Free Beginner’s Guide). The sophistication and quality of the printer, naturally, has a significant impact on the variety of available printer-friendly materials, the product quality, and the level of detail of the item produced.

The process, simplistically described above, requires several key pieces of equipment. Crime-scene reproduction would obviously not involve the creation of any new printed invention, so it would be necessary to have an appropriate, high-quality laser scanner. An example of this class of equipment is the PanoScan. When set up in a central location within the crime scene, it takes a high-resolution, 360-degree panoramic image in generally under 30 minutes.

In 2013, Maryland’s Baltimore County police announced that they purchased the (approximately $40,000) Panoscan camera (WMAR Staff). New York City police have had one since 2009 (“A New Perspective”). The use of the camera allows detectives to revisit the images of the scene, via computer, long after the release of the original site, with no change to the details.

Using 3D scanned images and software to convert the images to a reproducible format, much like that used in architectural design and models, a suitable 3D printer could begin building a model that could take several days to complete. Printers now range from consumer to commercial grade with prices going from several hundred dollars to over a half million dollars.

There are a few general criticisms of 3D printers. First, and probably foremost, being the cost (Gilpin). The good news for most consumers, though not for printer pioneers, is that patents are starting to expire. Removing the patent limitations will likely increase the competitive market and should lead to some price reductions. The second concern is the speed of the printers. Printing speed is primarily an issue concerning manufacturing interests. The 3D printers are still too slow to make any kind of mass production cost-effective (Gilpin). However, in the case of crime-scene reproduction, there would likely...
be only one model produced per scene and, unlike an episode of CSI, it would be acceptable that completion take longer than an hour.

**FORENSIC MODELS GOING FORWARD**

In 1949, Dr. Alan Moritz, who headed the Harvard Department of Legal Medicine, said, "The amazing truth is that, in most localities in the United States, official medical investigation of unexplained deaths is so casual and inexpert that clever murderers often go free" (Martin). Frances Glessner Lee made it her goal to change that reality. As a private citizen, she immersed herself in philanthropic, educational, and creative endeavors to offer investigators a means to improve their skills and become more formal and expert.

By creating the Nutshell Studies of Unexplained Death, Lee gave participants in her seminars tactile, three-dimensional tools to study and evaluate, in addition to speakers on various topics pertaining to the investigation of incidents of death. The cost of each Nutshell to Lee was roughly one thousand dollars, quite the investment in the 1940s, and three months of nearly obsessive labor. The detail makes the Nutshells remarkable, but it is probable that the creation of a model instead of text or diagrams is what makes them valuable. So valuable that there was an investment of an additional fifty thousand dollars to restore and preserve the Nutshells.

Having investigators, whose work is active and tactile by nature, work on refining their skills using models that most closely resemble their work, but in miniature, makes Lee seem a woman ahead of her time. Investigators undisputedly benefit from working with the Nutshell Studies. That being the case, it would seem reasonable for participants in her seminars tactile, three-dimensional tools to study and evaluate, in addition to speakers on various topics pertaining to the investigation of incidents of death. The cost of each Nutshell to Lee was roughly one thousand dollars, quite the investment in the 1940s, and three months of nearly obsessive labor. The detail makes the Nutshells remarkable, but it is probable that the creation of a model instead of text or diagrams is what makes them valuable. So valuable that there was an investment of an additional fifty thousand dollars to restore and preserve the Nutshells.

The Nutshells capture a scene of death at the point of discovery. Several police districts in the United States are already using technology that gives them the same capability. A high-definition panoramic camera placed to operate at a just-secured crime scene allows police to capture every detail of the aftermath of a catastrophic event. The captured images serve not as forensic evidence themselves, but as the measured map for actual evidence. Electronic storage of the digital images is a sort of evidence conservation (Buck, et al. 81). Because physical objects collected as evidence often pass through many hands on their path to trial, it is possible for damage or loss. The virtual record, at least, preserves the knowledge of what should be available.

Work is beginning to evaluate the accuracy of panoramic-type cameras. One area of research tests the accuracy of the height estimate of an individual (the suspect) in a laser-scanned image calculated from the coordinates of the image. Testing done by Monique Johnson and Eugene Liscio used a FARO Focus3D Laser Scanner, and their conclusion was that using subjects of a known height, the height estimates were accurate (Johnson and Liscio 1587). More research of this type, such as analyzing the perceived realism of the models (Ebert, et al. 626), will continue to validate the accuracy of panoramic camera images, making those images more likely to be admissible demonstrations in court.

The images, like all crime scene photography, are not simulations. Computer-generated simulations are a virtual presentation of what actions may have happened just before the crime scene. Data regarding bullet trajectory, angles of falls, and other measurable movements can be entered into specialized computer software to generate an animation of possible circumstances that could result in the crime scene. There is a level of human involvement in the selection of what data is considered. Admissibility of this type of model in a trial is inconsistent.

Panoramic cameras, already in use by some police investigators, may also be useful in other branches of the legal process. It is unlikely that the cameras themselves are of service to attorneys, judges, and juries, but the impact of the collected images could be significant. Scanners often employ software that generates a 3D image from three-dimensional reality. Viewing the resulting images on a computer can be like watching a 3D movie without the special glasses. There would seem to be two options: virtual reality headsets or 3D models.

Virtual reality (VR) headsets enable the wearer to view the panoramic scan as more realistic. There are pros and cons to VR. The headsets have become popular among the computer gaming community. For that reason, the cost of an individual headset is quite reasonable (between 30 and 300 dollars generally). For organizations under budget constraints, individual headsets for anyone wanting to view the scanned crime scene would be far more feasible that a 3D printer capable of sufficient detail. Two significant cons would be the likelihood of “simulator sickness” (Allison 19) and the fact that the images are still a visual experience and not kinesthetic. Simulator sickness is much like motion sickness. The eyes are experiencing movement, but the ears are not, typically resulting in nausea and dizziness. While the visual experience could continue to be useful for investigators, it does not translate well into a courtroom setting. While the cost of the units is appealing, the risk of juror sickness, headset loss or theft, and the ongoing maintenance and sanitizing would make them impractical.

Many would argue that nothing could replace the exquisite detail of Lee's Nutshell Studies, and for their purpose and their history, this argument is entirely valid. However, recognizing that part of what investigators value is their tangible three-dimensional presentation, and understanding that nearly 30 percent of people favor learning by being able to handle and manipulate objects, finding a way to bring models further into the criminal justice system seems a reasonable undertaking.
Jurors typically perceive physical evidence as more accurate, leading to it having a stronger impact on verdicts than testimonial evidence (Daftary-Kapur, et al. 141). It is possible, though currently not confirmed by research, that part of the favored status of physical evidence is that it is physical. While the jurors themselves may not be able to hold DNA evidence or control video surveillance, they are still things that have been measured and analyzed. Reports of the finding of physical evidence, such as a medical examiner’s report, paired with a 3D reconstruction could allow third parties to gain a better understanding of the results (Buck, et al. 82).

The technology exists currently to obtain crime scene images, use software applications to make those images printer-ready, and create a model on printers capable of generating a reproduction. The cost for every crime laboratory to have a high-quality 3D printer is, at least currently, financially irresponsible. There would likely not be enough need to justify a six-figure cost, but perhaps there may be enough interest to collaborate on a printer purchase or outsource the production.

There would have to be protocols in place to determine whether a crime scene goes from digital images to 3D printout. These protocols would likely link to the severity of the offense, at least until pricing becomes less of an obstacle or if a private outside entity assumes the printing cost for a particular case. Whether a case is heading to trial may be another consideration for 3D production. Having a model of the scene available may be enough to start conversations to settle the case. Taking the scanned images could be a standard operating procedure at a crime scene, ensuring that cold case files have images: another ground for making reproductions. The physical image of the scene, viewed from a variety of angles by an entire investigative team, could produce new thoughts about what transpired. Perhaps, like Frances Glessner Lee’s models, the new generation of models may provide instructional value for the next generation of investigators.

All current indicators are that 3D models are not making it to court. Efforts to remove the barriers surrounding this kind of demonstration device seem to be underway. Law enforcement agencies that use panoramic scanners cordon the area and then start the camera. The early start of scanning in the collection protocol nearly eliminates possibilities of contamination before a forensic record is complete. Although the camera, once started, performs without the assistance of a photographer, there would still need to be a trained technician that could testify to the calibration and operation of the camera. Similarly, having a trained computer technician, who could be qualified as an expert witness and speak to the overall functioning and accuracy of the 3D printer in use, would support the inclusion of a crime scene model in a trial. However, since a scan is a crime scene photograph used to generate the model and derived from police-collected evidence, there is a high likelihood of admissibility (Bostanci 8). Further, if there were an eyewitness to the crime, the witness could verify the accuracy of the model, just as witnesses identify photographs, making the model more likely to be admissible.

There are many advantages to models depicting the evidence of a crime and having it available for trial. Often, the presentation of testimony about securing the crime scene is verbal. With a model, especially of a limited-range outdoor area, the first responder could demonstrate, in a more meaningful way for many jurors, how that was accomplished. Sometimes the primary crime scene is a vehicle. While it is possible to keep such a “location” intact following all the investigation, two issues could improve with the use of a model created at the time of discovery. First, jurors could see what the vehicle looked like at the time of the crime rather than after the collection of the evidence that necessarily alters the appearance. Second, there are news reports that jurors sometimes leave the courtroom, albeit under strict supervision, to go to the quarantine location of the vehicle to see it firsthand. Such an excursion was part of the original trial of Officer William Porter regarding the death of Freddie Gray in Baltimore. While this activity is certainly more in keeping with a kinesthetic learning style, it can disrupt the flow of the court proceedings. There have also been instances where dismantled vehicles are brought into the courtroom as evidence. Again, this is keenly kinesthetic-friendly, but it can be unwieldy, whereas a small-scale portable model could serve the same purpose without the disruption.

Another positive feature of a printer-built crime scene model is that it begins with a scanned digital image that can be safely stored. Because of the storage capability, if the model becomes lost or damaged, printing a replacement model is possible. The reproduction, because of the accuracy of the 3D printer, would be identical to the first printed version.

CONCLUSION

From the 1940s, Frances Glessner Lee, not formally trained, but a passionate woman, recognized that the work of police, detectives, and investigators could improve with proper training. That proper training included the use of extraordinarily detailed models of death scenes. Though it is likely she was not aware, the research on sensory learning styles was also beginning. Lee started developing the Nutshell Studies, which were obvious kinesthetic learning tools.

With the Nutshell Studies, Lee was able to create a learning program that included a variety of learning activities. The response to her program continues to be very positive and very beneficial to the community of investigators.

Kinesthetic learning preference touches roughly 30 percent of tested populations. Some groups of learners, such as medical and clinical
It is not surprising that in recent years, some law enforcement organizations have embraced technology that allows alternate approaches to analyzing crime scenes and processing evidence information. The ability to record the visual aftermath of a potential crime allows detectives the opportunity to review the crime scene repeatedly and pair it with the reports of lab results on evidence testing. This multi-style approach has already helped police solve crimes efficiently and more confidently. So, at least to the point of the investigation, police can take advantage of multiple presentations of evidence, thus enhancing their ability to solve the crime.

The next step, with steady improvements to and price reductions of 3D printers, forensic models depicting the relative locations and types of evidence collected are on the horizon. While the technology is currently available, the confidence in the product may not yet be at an acceptable level. However, in support of moving in this direction, if court personnel are concerned that forensic television programming is influencing the public jury pool, then perhaps it is time to offer at least a physical representation of evidence in cases where a tactile element is missing. The 3D model is evidence in the same way that crime scene photographs are evidence. The difference being that the 3D model has a different sensory value than a photograph, the spoken word, documents, and other types of non-forensic evidence. If the influence of television suggested by the cultivation theory, or, at least, the legal professionals’ perception of that influence, is lowered, a more unbiased and fair verdict may result. Technology in the trial system will manage to find a place. Thoughtfully handled 3D forensic models could allow a greater number of very diverse individuals to understand if criminal activity exists in a case.

Once availability improves and 3D models make their way into the courtroom, then research can consider topics including the effectiveness of the models and if there is any CSI effect relationship.

It would be impossible, at least right now, to think any 3D printer could master the intricacies of Frances Glessner Lee’s Nutshell Studies. However, the idea that 3D printing is capable of producing weapons, body parts, and food, makes it reasonable to believe that accurate replication of death scenes is feasible.

It is with thanks to Frances Glessner Lee that advancements continue in improving police work and that the models that she so painstakingly created not only serve today but offer inspiration in a technological future. Improving evidence analysis with scanned 360-degree images and being able to build those images in miniature with the eventuality of taking them all the way through the crime-to-court process, is undoubtedly part of Captain Lee’s legacy. Any improvements in evidence collection, handling, evaluation, and presentation only enhance the likelihood that this and the next generation will “Convict the guilty, clear the innocent, and find the truth in a nutshell” (Botz 27).

WORKS CITED


JACQUELYN A. D. JONES

Ms. Jones’ journey began as Alternate Juror 1 in a criminal trial and quickly moved into Stevenson University’s Forensic Studies, Investigations program. Graduation in December 2017 will give Ms. Jones her third master’s degree, which she hopes to use in combination for a new career in witness preparation or crime scene reproduction. Since learning of the Nutshell Studies, Ms. Jones has taken multiple seminars based on the work of Frances Glessner Lee and became a member of the Harvard Associates in Police Science.
Non-Financial Measures: A Viable and Effective Way of Detecting Fraud in Accounting Records

Kevin McKelvey

The ever-expanding problem of fraud within accounting records continues to spiral out of control. More specifically, an estimated $14 trillion is lost globally every year (Allee, et al. 2). What may be more surprising is that $575 billion of this total is lost in the United States alone (Allee, et al. 2). This astounding figure continues to grow yearly and shows no signs of slowing. Both the public and the U.S. government are becoming increasingly frustrated as to why this problem can’t be solved or, at the very least, addressed in a way that would help decrease this enormous amount. Experts in accounting, finance, and other disciplines have come together to try to determine a course of action that will not only lower this number, but also restore public confidence that companies are not conducting illegal activities.

Fraud within accounting records includes any type of intentional manipulation of the financial statements committed by an individual to conceal the truth or gain an advantage over another individual (Lawrence and Wells). For fraud to have occurred in financial statements, three elements must be present: “a material false statement made with an intent to deceive (scienter), a victim’s reliance on the statement,” and damages resulting from an individual’s reliance on the falsely reported information (Lawrence and Wells). In order to help auditors detect fraud in the financial statements of a company, a relatively new strategy has started to gain momentum as a potentially useful option to help lower the trillions of dollars lost globally. Comparing the financial measurement of revenue growth to the non-financial measures of electricity consumption, employee headcount, and square footage of operations can serve as a viable and unbiased indicator auditors can use to detect fraud and combat this global epidemic.

The idea of detecting fraud using publicly available information not expressed in monetary units was developed around 20 years ago (Meyer). Even with the Public Company Accounting Oversight Board’s endorsement of the use of non-financial measures, the practice has failed to gain popularity among auditors (Allee, et al. 6). It is estimated that about half of all auditors currently use some sort of non-financial measure (Meyer). This number may seem high, but it still means half of all auditors refuse to use non-financial measures. Because of recent major fraud schemes, such as Enron and Lehman Brothers, the outcry from the public for accountants to universally adopt tactics to deter firms from committing fraud is stronger than ever.

Auditors complain that because of tight time constraints and their hectic schedules they cannot afford to perform these additional procedures (Meyer). Auditors fail to understand that, even though it would take more time to perform the audit, using non-financial measures actually makes it easier for them to uncover fraud (Meyer). “[F]raud is easier to detect with nonfinancial measures because this data is disclosed in a public company’s annual filings with the SEC, and companies that commit fraud often fail to hide the nonfinancial evidence of their wrongdoing” (Meyer). If all auditors analyzed this type of information, it would deter companies from even considering falsifying the information in their accounting records. However, not all non-financial measures are completely decisive evidence. With an array of non-financial measures to choose from, accountants have to carefully decide which ones will efficiently help them assess the probability of fraud.

Certain non-financial measures can be influenced or manipulated. Auditors failed to detect the inconsistencies between financial and non-financial measures in Royal Dutch Shell’s accounting records, for example. For years, Royal Dutch Shell deceived investors by overstating their non-financial measure of oil and gas reserves (Brazel, et al., “Using Nonfinancial Measures” 1136). The company was able to manipulate this measure because of the complexity involved in verifying fossil fuel reserves. The top officials at Royal Dutch Shell saw an opportunity and exploited this weakness. Although this may be an argument against the effectiveness of using non-financial measures, it serves as a crucial lesson for auditors. In order for the consideration of non-financial measures to be truly effective, auditors need to take every unique situation into account. When auditors do this, they can determine which non-financial measures will be easily verifiable. The non-financial measures of electricity consumption, employee headcount, and square footage of operations meet this criteria. Not only can non-financial measures be easily verified, but they also maintain a high degree of accuracy.

Every day, businesses find new and innovative ways to conceal fraud within accounting records. The adoption of non-financial measurements would add a higher degree of complexity that businesses would have to navigate (Brazel, et al., “Using Nonfinancial Measures” 1140). Businesses would have to falsify even more data to conceal criminal activity. Not only would it force businesses to tamper with more data, it would also increase the number of employees involved in the fraud scheme. Managers would have to extend their network and include employees from different departments to forge the data. Inevitably, it would require a higher degree of collusion among employees in order to conceal the fraud taking place (Brazel, et al., “Using Nonfinancial Measures 1140). By increasing the number of employees involved in the scheme, the company creates a greater chance that a whistleblower will reveal the financial wrongdoing. Using non-financial measures will never be able to truly stop all fraud, but this strategy will make it significantly more difficult to conceal criminal activity.

Joseph Brazel, a professor at North Carolina State University and one of the leading experts in the accounting field, has been analyzing the usefulness and accuracy of non-financial measures. According to him and his colleagues, auditors absolutely need to consider the idea of adopting non-financial measures (Brazel, et al., “Using
It is estimated that 31.8 percent of all fraud cases take place within money into the company. This is especially true for small businesses. As a result, new and current shareholders will invest more and current shareholders will invest more. The most tampered-with financial measure is simple. By overstating the revenues (Dechow, et al. 27). The reason revenue growth is the key financial measure that must be compared to electricity consumption, employee headcount, and square footage of operations. The most common type of fraud that occurs in the accounting records is overstating revenue growth (Dechow, et al. 27). According to a study that observed over 676 fraudulent firms, the Security and Exchange Commission determined that over 50 percent of all fraudulent cases involved overstating revenue growth (Dechow, et al. 27). The reason revenue growth is the most tampered-with financial measure is simple. By overstating the revenue generated, the company inherently looks more attractive to investors. As a result, new and current shareholders will invest more money into the company. This is especially true for small businesses. It is estimated that 31.8 percent of all fraud cases take place within businesses having fewer than one hundred employees (Smith, et al.). Because small business owners often invest a substantial amount of their personal worth into the business, "[small business owners] lack the resources to implement complete systems of internal controls and properly segregate accounting duties among their limited staffs" (Smith, et al.).

Employee headcount is directly related to revenue generated by a company (Brazel, "Using Financial and Nonfinancial" 5). In order to prove this point, Brazil examined over 110 fraudulent companies and developed a regression model. The result of his model produced an R2 of .62 (Brazel, et al., “Using Nonfinancial Measures” 1157). To put it simply, Brazil’s experiment showed that 62 percent of the companies examined using his model showed a positive correlation between an overstated revenue growth and the number of employees currently employed at the company. The same can be said about square footage of operations. Brazil noted how this other non-financial measure has been used successfully in the past when compared to revenue (Brazel, et al., “Using Nonfinancial Measures” 1142). This proven track record helped Brazil reach his conclusion that square footage of operations is also an effective non-financial measure to use.

When comparing the electricity consumption to revenue growth, encouraging empirical data results have led experts to consider it a useful non-financial measure. In a study that took place from 2006 to 2014, experts tracked the real production activity of an array of different industries. The results showed a direct correlation between revenue growth and electricity consumption (Allee, et al. 36). Not only is there a high correlation between revenue and electricity consumption, this measure is also almost impossible to manipulate. In theory, the non-financial measures of electricity consumption, employee headcount, and square footage of operations should be proportional to the revenue generated in the fiscal year. These non-financial measures are directly correlated to the data that is reported on a company’s annual reports and 10-K filings (Brazel, “Using Financial and Nonfinancial” 5). This, in turn, enables an auditor to establish a benchmark of how the company should perform during any given year. Some non-financial measures, particularly electricity consumption, can be obtained through external independent sources. This adds another level of security because the independent source is highly unlikely to manipulate the numbers. This technique significantly diminishes the chance of a company committing fraud within the accounting records.

If a company under audit does show an inconsistency between the non-financial measure and the revenue growth, it does not necessarily mean that the company is committing fraud. “If financial data and nonfinancial measures are off by about 10%, no big deal. ’But if revenue growth is exceeding the operational data by 20% or more,’ Brazil says, ’our research says that while it may not be
fraud, it is something to look into” (Meyer). As a result, a company showing a large discrepancy will be given what experts call a “red flag” and must be investigated further to determine if the growth in revenue is legitimate (Brazel, et al., “Transparent Disclosure and Fraud” 3).

These three non-financial measures can be applied to any type of business; however, the type of company under audit could determine which specific non-financial measure would be most useful. For certain companies, all three non-financial measures could be useful, but for others, only one may be applicable. Take, for example, a small plumbing company. Most employees are providing a service to a customer at a specific site. It would be nearly impossible for an auditor to use square footage of operations or electricity consumption in this situation. The non-financial measure of employee headcount would still be a practical option in this instance because it would be easy to confirm. Auditors need to be careful when choosing which non-financial measures they compare to the revenue in order to accurately gauge whether a company is tampering with their accounting records.

Finally, after analyzing a company’s questionable revenue growth in relation to the chosen non-financial measures, the results can be compared to competitors’ financial records. This is the last step that can help confirm an auditor’s suspicion. The competitors’ information, in most cases, will give auditors a general understanding of how the industry is performing during current economic conditions. This creates a point of reference auditors can use to determine whether the revenue growth reported is legitimate. If the difference between the non-financial measures and the change in revenue is significantly larger than that of competitors in the industry, fraud may be taking place in the accounting records. Further investigation would be needed to confirm the dramatic growth in sales.

Every business needs energy in order to generate revenue. As such, the electricity a company consumes offers a unique practical technique auditors can use to assess the probability of fraud. The idea of comparing the non-financial measure of electricity consumption to the revenue generated is so new that there is only one study to date that fully analyzes the correlations between the two measures. Because of strict regulations that utility companies face, electricity consumption is nearly impossible to manipulate (Allee, et al. 2). It serves as an extremely reliable non-financial measure that can help confirm an auditor’s suspicion that revenue growth was closely related to the growth in revenue is legitimate (Brazel, et al. 6). The professors sought to further the research on this subject and whether the electricity consumption of a company could be considered an accurate indicator of fraud. The professors conducted an eight-year study, including over 8,000 observations (Allee, et al. 13). After analyzing the amount of electricity consumed by these firms, the professors looked into how strongly this electricity use correlated with changes in revenue. When the growth in revenue was plotted against the growth in electricity consumption, it was clearly evident that these two measures were strongly correlated. As they explain, “[t]he growth in aggregate electricity consumption generally matches the aggregate revenue growth. Specifically, both measures seem to increase and decrease in tandem for the majority of the years” (Allee, et al. 19).

To further test their results, they ran a regression model to mathematically describe how strong the relationship was between the two variables. The regression model resulted in a correlation coefficient of .571, which was described as both “positive and highly significant” (Allee, et al. 20). Furthermore, the professors concluded that this suggested that, “firm-level electricity consumption growth encapsulates a significant amount of information about current firm performance” (Allee, et al. 20). Once the professors confirmed their suspicion that revenue growth was closely related to the growth in electricity consumption, they were able to create a formula to accurately assess the probability of fraud within a company’s records.

The formula developed by these three professors can greatly enhance an auditor’s ability to detect fraud within accounting records. Not only is it easy to understand and use, the input values are all easily attainable. The formula is shown in Figure 1.

\[
GW_{it} = \frac{\text{Revenue}_{t} - \text{Revenue}_{t-1}}{\text{Revenue}_{t-1}} - \frac{\text{Electricity consumption}_{t} - \text{Electricity consumption}_{t-1}}{\text{Electricity consumption}_{t-1}}
\]

Essentially, the formula measures the difference between the revenue growth and the electricity consumption of a company. By comparing these two measures for consecutive years, the final result is what is called a growth wedge. The growth wedge can be used to assess the probability of fraud inside a company (Allee et al. 3). The professors...
determined that when an abnormally large growth wedge is present, it could signal that “a firm’s accounting performance is growing faster than its actual activities [are], hinting at the possibility of firms engaging in income-increasing earnings management” (Allee, et al. 3).

This formula also allowed the professors to pinpoint how much higher the revenue growth should be on average compared to the growth in electricity. “We find that [the growth wedge] has a mean of 3.8 percent, suggesting that the average firm experiences revenue growth 3.8 percent greater than its growth in electricity consumption” (Allee, et al. 3). As stated earlier, the higher the growth wedge, the greater the probability that fraud is taking place somewhere in the accounting records. However, a 3.8 percent growth wedge is normal for a company. A significant deviation from this average is what an auditor should be searching for when conducting their audit. A large discrepancy between the growth in revenue and the growth in electricity could warrant a “red flag” for that company.

The one criticism against electricity consumption being an effective non-financial measure to use is the occurrence of extreme weather (Allee, et al. 5). Events such as heat waves or prolonged periods of severe cold can obviously alter the electricity consumption of a company. Additionally, certain areas experience these temperature swings more than others. The professors acknowledged this criticism and accounted for it accordingly: “[w]e identify firms whose electricity consumption appears sensitive to weather conditions and inferences remain the same after removing the highest [number]” (Allee, et al. 27). To avoid overstating the energy consumption amount, the month in which the company experienced the highest energy consumption can be removed, and the rest of the months averaged. This new number can then be placed in the original formula to calculate a growth wedge that properly accounts for abnormal weather patterns. Allee, Baik, and Roh also noted that auditors should only consider extreme weather as a reason for increased energy consumption when there are five or more occurrences in the year (Allee, et al. 27). Otherwise, the calculated growth wedge can be examined as the true indicator of fraud within the company.

At the end of their eight-year study, Allee, Baik, and Roh were able to conclude that they found “convincing evidence on the incremental predictive power of electricity consumption in detecting financial misreporting. ... Collectively, [their] results suggest that electricity consumption aids in identifying firm financial misreporting” (Allee, et al. 28-29). Because electricity consumption is relatively easy to verify and allows auditors the ability to gain valuable insight into the economic activities taking place inside a firm, this technique can help decrease the total amount lost each year due to fraud. As Allee, Baik, and Roh confirm, “[b]y linking a firm’s real production activities to financial accounting topics, [there are] possible ways in which accounting researchers can draw insights from investigating firm economic indicators such as electricity” (Allee, et al. 29). With the positive regression models, correlation coefficient, and room for adjustment due to weather, electricity consumption can absolutely be considered an authentic non-financial measure that can accurately be used to detect fraud.

Even with these positive results, electricity consumption may be difficult to verify for certain companies or in certain industries. When this problem arises, auditors need to turn to an alternative non-financial measure that is just as accurate as electricity consumption. The number of employees working at a company can serve as that alternative. Not only is employee headcount just as effective, it has also been carefully studied and applied to previous fraud schemes in order to prove its legitimacy.

As previously mentioned, employee headcount has a strong correlation with the amount of revenue generated. Some additional advantages of this non-financial measure is that it can be easily verified by visiting the site of operations and is also disclosed in the 10-K filings of the company. Although it is highly unlikely, managers can manipulate this number by reporting a fictitious number of employees to match the growth in revenue. The fabricated number can easily be identified, however, because it would take only a matter of hours to verify the true employee headcount. This is why employee headcount is as objective and accurate as electricity consumption. It’s an unbiased measurement that accurately assesses the probability of fraud having taken place within the accounting records. Auditors can easily adopt this strategy into their repertoire of analytical procedures.

The non-financial measure of employee headcount is very straightforward. In most cases, more employees are needed in order to keep pace with demand and sustain the higher revenue reported. In contrast, “reductions in the number of employees are likely to occur when there is declining demand for a firm’s product” (Dechow, et al. 5). In this case, the revenue will decline as the number of employees falls. However, as Dechow and her colleagues point out, it is possible for a company to increase revenue by reducing employees because that would naturally reduce payroll costs (Dechow, et al. 5). This increase in revenue is only temporary and would eventually balance out as the year progresses (Dechow, et al. 5). Thus, many experts, including Dechow and her colleagues, believe that when an abnormal reduction in the employee headcount, along with an uncharacteristic growth in revenue, is present, it can be a useful indicator for detecting fraud (Dechow, et al. 5).

Like electricity consumption, employee headcount is calculated by determining the change in employees over consecutive years, then comparing that change to the growth in revenue reported by the company. Not only is this formula elementary, many experts have also agreed that the growth or decline in the number of employees can help an auditor in determining the likelihood of fraud. Ames and his colleagues affirmed Brazel’s regression model and added that, “[t] he results show that the relationship between reported revenue growth and employee headcount for the fraud firms is significantly different
than the relationship for the non-fraud firms” (Ames, et al. C29). Moreover, Dechow and her colleagues conjectured “that managers attempting to mask deteriorating financial performance will reduce employee headcount in order to boost the bottom line” (Dechow, et al. 23). With these kinds of endorsements, employee headcount clearly needs to be used to detect fraud.

To show that employee headcount can be used successfully, Joseph Brazel applied employee headcount to a specific fraudulent company. Brazel’s goal was to confirm whether this non-financial measure could have aided auditors in detecting the fraud scheme years in advance. Del Global Technologies Corporation was an electronic company that produced components for the medical, industrial, and defense fields (Brazel, et al., “Using Nonfinancial Measures” 1141). From 1997 to 2000, the Securities and Exchange Commission alleged that Del Global Technologies was taking part in a fraud scheme and covering it up using the accounting records (Brazel, et al., "Using Nonfinancial Measures" 1141). More specifically, Del Global Technologies was overstating their revenue for these years and prematurely recording sales. Eventually, the corporation was found guilty of fraud, among other charges, but auditors did not uncover the fraud scheme for years. Brazel believes that employee headcount would not only have identified the criminal activity immediately, but would also have deterred the company from even taking part in such fraud.

First, Brazel and his colleagues examined the revenue growth from 1996 to 1997. Del Global Technology’s revenue had grown from $43.7 million to $54.7 million—an increase of 25 percent (Ames, et al. C29). Next, they identified the number of employees that were working in the company. Del Global Technology’s 10-K filing revealed that, in the same year, the number of employees decreased from 440 to 412—a 9 percent decrease (Ames, et al. 29). Even before reviewing the information from competitors in the same field, Brazel and his colleagues noted that, “while a company could increase profits by cutting payroll, it is improbable that the company would double in profitability over a three-year span while laying off employees, and it is even less probable that employee layoffs would correspond with a significant increase in revenue” (Brazel, et al., “Using Nonfinancial Measures” 1141). This massive discrepancy should warrant a “red flag” from any auditor, but it continued for three years. They then compared Del Global Technology’s change in revenue and employee headcount to that of its closest competitor to truly gauge the firm’s financial performance during the prevailing economic conditions.

Brazel and his colleagues identified Del Global Technology’s closest competitor as Fischer Imaging Corporation and analyzed how they performed in the same year. According to their financials, the company reported an accurate 27 percent decrease in revenue along with a 20 percent decrease in employee headcount (Brazel, et al., “Using Nonfinancial Measures 1141). This kind of decline in revenue was legitimate because it was accompanied by a drop in the number of employees. The demand for the company’s products declined significantly, and, as a result, the company had to lay off employees to stay in business. When Del Global Technology’s financials were compared to those of Fischer Imaging Corporation, something illegal was obviously taking place inside the company. As Ames and his colleagues state, “by comparing reported financial results to [employee headcount] for Del Global and Fischer ... Del Global’s auditors could have noted that the [non-financial measures] were inconsistent with the financial results and, therefore, been more aware of the potential for fraud” (Ames, et al. C29). Instead, auditors did not detect the fraud for several years, and millions of dollars were lost because of the scheme.

This experiment helped confirm Brazel’s hypothesis that employee headcount could have helped auditors uncover the fraud taking place with the company’s records. Brazel’s study also revealed another issue. Auditors typically fail to understand the environment their clients have to navigate (Brazel, et al., “Using Nonfinancial Measures” 1161). His study proved that if auditors understood how the economy was affecting the industry that Del Global Technology was operating in, they would have already known that companies were laying off employees. With this in mind, auditors could have reasonably assumed that the revenue reported by these companies should be lower than the previous year. Brazel’s study comparing revenue growth and number of employees further solidified that “[s]ubstantial differences between financial statement data and [non-financial measures] should serve as a red flag to auditors and lead them to ask pointed questions of client management, corroborate and test management’s responses, and, if necessary, serve as a tipping point for assigning forensic specialists to the engagement” (Brazel, et al., “Using Nonfinancial Measures 1161). The number of employees at a business is a solid non-financial measure. It is easy to use and complements the traditional analytical procedures performed during an audit.

The number of employees has one more advantage: it is closely associated with the square feet of a facility. As the number of employees grows, operations have to expand to keep up with the higher demand. Eventually, as revenue continues to grow, additional facilities will need to be opened. This measure is unique because many people do not understand that square footage of operations is directly associated with the amount of revenue generated. For this reason, square footage of operations can also be considered when trying to identify fraud. Auditors can review this figure, identify how much operating facilities have expanded or shrunk, and compare it to the revenue.

As it is similar to employee headcount, square feet of operations is analyzed the same way. The difference between square footage of operations over consecutive years needs to be observed and then compared to the growth or decline of revenue generated. The results should mimic those of the electricity consumption and employee headcount comparisons. For a substantial increase in revenue to be
legitimate, the square feet of a facility must increase, as well (Brazel, et al., “Using Nonfinancial Measures” 1150). This non-financial measure has been labeled a “measure of capacity” because it allows an auditor to statistically determine how much revenue a defined area should generate (Ames, et al. C29). This non-financial measure also has the advantage of being verified through external sources and can be obtained in a short period of time.

The easiest way to verify the square footage of operations is to visit the property tax website of the company’s state of residence. This type of website allows an auditor to research and obtain not only the property taxes, but also the square feet of the facility. The chances of someone manipulating this number are extremely low. However, if an auditor questions the square feet of operations, an independent appraiser can be brought on site to verify the number. This option would most likely occur in rare circumstances. As mentioned earlier, a major advantage of using non-financial measures is that top company officials would have to increase the scope of people involved in order to tamper with these figures. This is especially true for square feet of operations because managers would have to collude with external appraisers in order to report a false number. In the same study that proved the efficiency of using employee headcount, Brazel also attempted to prove that square feet of operations could be just as viable. His experiment was a contributing factor as to why several experts have agreed that square feet of operations comparisons are a useful strategy for revealing fraud.

Brazel pointed to two examples in order to prove his point that square footage is an effective measurement. In his more extensive study, Brazel looked at a company called Anicom. Again, the SEC alleged that from 1998 to 2000 Anicom was taking part in a massive fraud scheme by overstating their revenue (Brazel, et al., “Using Nonfinancial Measures” 1141). Eventually, Anicom was found guilty of falsely reporting millions of sales while also using other illegal techniques to significantly inflate their income (Brazel, et al., “Using Nonfinancial Measures” 1141). Brazel applied the square feet of operations comparison to this company to display how using square footage of operations could have helped auditors expose the illegal activity.

In the first year of fraudulent activity, Anicom reported an astounding $226 million dollar increase in revenue (Ames, et al. C29). The square feet of operations for Anicom also increased 29 percent (Ames, et al., C30). After studying the 10-K filing more thoroughly, it became clear that this relatively small growth in square feet of operations could not possibly have sustained this huge increase in revenue. Anicom’s closest competitor, Graybar Electric Company, reported a legitimate 11 percent increase in revenue, while also expanding the square feet of their facilities by 6 percent (Brazel, et al., “Using Nonfinancial Measures” 1142). This kind of major discrepancy could have been detected if auditors had compared the square feet of Anicom’s operations with the revenue growth. It also could have helped save the millions of shareholder dollars lost when the company filed for bankruptcy shortly after being found guilty of fraud. Brazel acknowledged that external factors could legitimize discrepancies like these, but they still have to be investigated to rule out fraud (Brazel, et al., “Using Nonfinancial Measures” 1142). Unlike electricity consumption and employee headcount, square feet of operations comparisons have been used by the SEC and federal prosecutors to prove that a CEO knowingly committed fraud in the accounting records.

HealthSouth Corporation was federally indicted for a massive fraud scheme that the CEO, Richard Scrushy, knowingly committed (Ames, et al. C30). In court, federal prosecutors examined how the revenue growth continued to increase, but the square feet of the facility decreased (Brazel, et al., “Transparent Disclosure and Fraud” 2). The federal prosecutor, Colleen Conry, asked Scrushy, “[a]nd that’s not a red flag to you?” (Brazel, et al., “Using Nonfinancial Measures” 1136). Conry’s question implied that the major discrepancy between the revenue growth and this non-financial measure should have been a cause for concern for the CEO. Scrushy responded by citing how management never saw the discrepancy and that external auditors also failed to identify the inconsistency (Brazel, et al., “Using Nonfinancial Measures” 1136). Prosecutors used the non-financial measure of square feet of operations to their advantage to help render a guilty verdict.

Square footage of operations, electricity consumption, and employee headcount can be considered as accurate indicators of fraud. It would be advantageous to use as many of these non-financial measures as possible during an audit. By using more than one, an auditor increases the accuracy of the non-financial measures. Multiple “red flags” should give an auditor more reason to believe that fraud may be taking place. It could also warrant an auditor bringing in a forensic accounting expert to help determine where the criminal activity is taking place. Even after proving the efficiency and usefulness of these non-financial measures, they do come with drawbacks. The most glaring drawback is the amount of time needed to retrain accountants to perform these non-financial measures analyses, and how using non-financial measures would affect certain certifications.

Auditors already have tough schedules. With looming deadlines and the amount of work required to finish an audit, there is not a lot of room to add additional work to their schedules. Auditors would have to browse through 50 pages of the 10-K filing to find the relevant non-financial measure (Brazel, “Using Financial and Nonfinancial” 18). Brazel estimated that it would take approximately five to six additional hours to gather the necessary information (Brazel, “Using Financial and Nonfinancial” 18). This is by far one of the major disadvantages of using non-financial measures. Auditors believe their time is used more valuably if they dedicate their undivided attention to other areas of the audit instead of calculating the difference
between a non-financial measure and revenue (Meyer). The amount of time needed to retrain auditors to use this technique is another area of concern. It would be time-consuming for large accounting firms to retrain their accountants. It would take even longer for firms to actually apply this technique to their clients. Although using non-financial measures will require auditors to work longer and require extensive retraining before use in the field, its effectiveness cannot be ignored.

One other question that surfaces is how certifications like Certified Public Accountant and Certified Fraud Examiner could potentially change. The tests to obtain these certifications do change occasionally. For example, the CPA exam is changing at the beginning of quarter two in 2017. The new exam will focus more on critical thinking and applying concepts to real life scenarios. Obviously, the adoption of non-financial measures in the accounting field could change the tests for these certifications. Including non-financial measures on these exams could help resolve the first issue discussed. In the long term, it will help reduce the amount of retraining needed for auditors. Because non-financial measures would be testable material on the exams, it would give newly certified CPAs and CFEs a general understanding of how to use them.

There is no disputing that accountants need to consider other strategies and tactics to decrease the number of businesses that commit fraud in their accounting records. Non-financial measures can truly help this growing problem. When revenue growth is compared to the non-financial measures of electricity consumption, employee headcount, and square footage of operations, it can serve as a tool that auditors can use to immediately identify the illegal scheme. Because these non-financial measures are nearly impossible to manipulate and can be verified relatively easily, it allows them to be true indicators of the company’s performance. The only way to truly manipulate these measures is to commit even more crimes, substantially increasing the probability of being caught. Additionally, the accuracy of these non-financial measures will force businesses to reassess the decision to overstate their revenue. Businesses will realize that the fraud schemes they successfully covered up in previous years will no longer go undetected.

Even though it may take retraining and slight changes to the exams for certain certifications, non-financial measures are a great way to combat fraud. Electricity consumption, employee headcount, and square footage of operations are unquestionably unbiased and should be used to complement the typical analytical procedures performed by auditors. As Franko Milost points out, “[non-financial measures can] reveal a deep crisis in traditional accounting, which does not respond to the challenges and changes of companies’ operations” (Milost, 826). These three specific non-financial measures can indicate “red flags” that traditional analytical procedures would ordinarily fail to recognize. Moreover, these non-financial measures allow both auditors and shareholders to identify characteristics that a fraudulent company may exhibit. Indeed, the three non-financial measures expanded upon in this report may require auditors to perform extra work, but considering how fraud continues to grow at a shocking rate each year, their use needs to be adopted by all accounting firms. When firms finally decide to adopt use of non-financial measures, it will lead to improved financial information, which will ultimately produce renewed public confidence that they are making sound investments.

**WORKS CITED**


Brael, Joseph F. Using Financial and Nonfinancial Measures to Improve Fraud Detection. 3 Nov. 2010.


KEVIN MCKELVEY

Kevin McKelvey graduated from Towson University with a bachelor’s degree in Accounting. He completed a tax internship at RSM U.S. LLP and, soon after, accepted a full time offer with the firm. Currently enrolled in the Stevenson University master’s program for Forensic Studies with a concentration in accounting.
Digital Roads Less Traveled in Criminal Investigations: New Sources of Digital Evidence

MORGAN RONE

INTRODUCTION

The primary goal of forensic investigators is to collect as much information and evidence as possible regarding a criminal case to identify, charge, and convict the correct suspect. The more information that law enforcement officers have access to, the stronger the case will be against the suspect. In recent years, digital evidence has become crucial to the success and accuracy in solving criminal cases and convicting the suspects involved. In February of 2014, a man named Philip Welsh was found murdered in his home in Silver Spring, Maryland (Goodison, et al. 2). During the investigation, law enforcement officials did not have any digital evidence because Welsh avoided using digital devices in his personal life (Goodison, et al. 3). Without any digital evidence available, law enforcement officials were not easily able to determine Welsh’s activities before he was killed or who he met with before his death (Goodison, et al. 3). In this case, digital evidence was the main factor in whether or not law enforcement was going to be able to solve the case.

Digital evidence is any data created by an electronic device or produced due to the interaction between a person and electronic device (Daniel 3). An example of data generated by the device is a log file that records when a user logs on to a specific user account; this data is seamlessly collected in the background while the person is using the device. Data created due to an interaction with a person could be a file created in Microsoft Word and saved on a laptop, or a text message created by the owner and saved on a cell phone. Digital evidence can be obtained from devices such as mobile phones, laptops, desktops, tablets, and external storage devices like USB flash drives or external hard drives. Because digital evidence has become crucial to more accurately solving criminal cases, forensic investigators need to consider including additional sources of digital evidence in the collection, including Smart TVs, wearable devices, and other devices that use cloud storage as their primary method of saving data. The extra information provided by these sources has the potential to provide additional evidence to help solve crimes and strengthen criminal prosecutions.

Presently, law enforcement officers do not include this information in their investigations for various reasons. When technologies like Smart TVs, wearable technology, and cloud storage devices became available to the general public, they were very expensive, so most people were not using these technologies in their everyday lives. As technology continued to evolve, developers began adding more features to these new technologies, like being able to connect to external devices like USB flash drives and cellphones (Boztas, et al. 1). Smart TVs, wearable devices, and cloud storage devices also became affordable to the general public and more people began using them every day. These new features provide new avenues of information for forensic examiners, like Internet browsing history and logs of any connected devices. This kind of information can demonstrate the browsing patterns of a user or confirm that a particular device was plugged in.

Another reason that forensic examiners are not already including these technologies is because search warrants must be very specific when it comes to examining any device involved in a criminal case. In many instances, search warrants must be as specific as listing the exact file directories the examiner is allowed to review, as opposed to the other directories found on the same device, because the warrant is based on probable cause and law enforcement must balance the individual’s privacy rights with law enforcement’s interest in a prosecution. On a device that has multiple user profiles, the search warrant may permit the examiner to search information located under one user’s profile, but not information under another user’s profile.

LEGAL ISSUES REGARDING DIGITAL EVIDENCE

The Fourth Amendment

Although digital evidence has become crucial to solving criminal cases in the recent years, this form of proof has raised many legal issues. The main problem encountered with the recent increase in digital evidence is how the Fourth Amendment should apply to the collection of digital information from devices like cell phones and personal computers. The Fourth Amendment protects citizens from illegal searches and seizures. For a search or seizure to be legal, law enforcement officers must obtain a search warrant based on an appropriate court order (Goodison, et al. 9). The only exceptions to this requirement are searches and seizures performed with the owner’s consent or searches and seizures that occurred due to exigent circumstances or due to the immediate danger of the destruction of the digital evidence (Goodison, et al. 9). Furthermore, law enforcement officials are allowed to conduct limited searches incident to arrest when needed to protect law enforcement officers or to prevent the destruction of evidence (Goodison, et al. 9).

Over the years, Congress has passed numerous laws in an attempt to address the relationship between the Fourth Amendment and digital evidence. The Wiretap Act was enacted in 1968 to protect citizens from the interception of any wire, electronic, and oral communications without consent (Roundy 1). This act was one of the first attempts by Congress to address digital evidence collected through wiretaps, and it remained valid until the 1980s. In the 1980s, e-mail was introduced and electronic communications became standard. The Wiretap Act now failed to adequately regulate communications technology (Roundy 1). In reaction to the realization that the Wiretap Act was no longer effective, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986. The ECPA updated the Wiretap Act in multiple ways to ensure new methods of communication were protected. Title I of the ECPA modified the definition of wire communications by changing the word “communication” to “aural transfer” to limit the communications to anything that included the human voice (Roundy 1). The words aural transfer included the points between the origin of the communication and the reception of it, as well (Roundy 1). Another notable change that the ECPA made was that it
also included electronic communications under the protection of the Wiretap Act, to give these types of communication the same kind of privacy protection as wire communications (Roundy 1). Lastly, the ECPA made it illegal to gain unauthorized access to communications being electronically stored by automated communication services (Roundy 1). Congress also passed the Privacy Protection Act to protect anything created by authors and the products used to create it; therefore, these products aren’t subject to search warrants (Goodison, et al. 10). The Privacy Protection Act applies to digital evidence because authors can now publish their work online through blogs and other social media platforms. The few exceptions to the Privacy Protection Act include scenarios when the published work connects with the commission of a crime, or the collection of the work would prevent serious bodily harm or death (Goodison, et al. 10).

Congressional officials are going to have to re-evaluate how the Fourth Amendment applies to any new device that law enforcement officials could potentially seize and examine to collect evidence in a criminal investigation. Officials have to determine the level of privacy that is expected from citizens for each new device. Depending on the level of privacy expected, the seizure and examination of the device is illegal unless a search warrant is obtained listing the device. In regard to Smart TVs, law enforcement will have to determine if citizens have a reasonable expectation of privacy when using a Smart TV to browse the Internet. When it comes to smart watches, law enforcement must determine whether or not smart watches engender the same level of privacy as a cell phone, since they act as an extension of the cell phone. Cloud devices are a little different because officials are going to have to determine the level of privacy expected by an individual, as well as what is expected on a business level. The same methodology will be applied to new forms of communications that are developed as technology advances.

**Jurisdictional Boundaries**

Jurisdictional boundaries are another legal issue encountered in the collection and examination of digital evidence. Law enforcement officers run into this problem because they often find that the information they are looking for is stored by providers that reside either out of state or out of the country (Goodison, et al. 11). Some states in the United States require law enforcement officers to comply with specific practices since they are operating outside their jurisdiction (Goodison, et al. 11). If the information they are looking for is located outside of the nation, they are required to work through the necessary mutual legal assistance treaty (MLAT) to make sure the laws of that country are satisfied during the collection (Goodison, et al. 11). For instance, there is a website hosting service called 1&1, and the servers that store their client’s data are located in two different locations: the United States and Germany. During a criminal investigation, if law enforcement officers were looking for information located on these servers, and they were not within the jurisdiction of either of the locations, the officers would then have to deal with jurisdictional boundaries. If the information were located in the United States in an area out of the law enforcement officer’s jurisdiction, the officers would have to check and make sure they followed any particular practices of that state to retrieve the information. If the information were located in Germany, then the law enforcement officers would have to go through the right MLAT to collect the information for the investigation.

The issue of jurisdictional boundaries is very apparent when examining devices that use cloud storage as the primary storage solution. Even though jurisdictional issues would be present in many cases involving the examination of information located on cloud storage, more evidence helps solve the crime and strengthen criminal prosecution. Many businesses are switching over to cloud storage to cut down on hardware maintenance costs, as a business using the cloud no longer has to maintain storage servers. The company that is providing the cloud service will be responsible for maintaining the hardware being used. As a result, the business using the cloud service has no control over the physical location of the servers storing their information; that is the decision of the company that is providing the cloud service. For example, Amazon provides a cloud service referred to as Amazon Web Services, which is located in multiple regions, both nationally and internationally. In the United States, they are located in northern Virginia and northern California. If a company outside of these jurisdictions used Amazon Web Services and digital evidence had to be recovered, law enforcement officials would encounter the issue of jurisdictional boundaries.

**The Hearsay Rule**

Many times digital evidence falls under the hearsay statute and therefore cannot be used in court. Hearsay is “an out-of-court ‘statement’ (an oral or written ‘assertion’ or non-verbal conduct intended by the actor as an assertion), other than one made by the declarant while testifying at the trial or hearing, offered to prove the truth of the matter asserted” (Cole 1). Digital evidence can be considered hearsay because text messages are an example of written statements and voicemails are an example of oral statements. Word processing files found on personal computers is another example of a source of written statements. In the case R v Kearley, multiple statements from voicemails left on both the defendant’s cell phone and home phone were used to assert that the defendant was a drug dealer (Hirst 490). The prosecution argued that because multiple callers referred to their ‘usual’ supply, this implied that the caller both knew that the defendant was a drug dealer and the defendant had done business with the caller before (Hirst 490). The court decided that the voicemails were hearsay and thus inadmissible in court. In general, any statements that are taken from the written or oral communications recovered from the digital evidence that are submitted in court to assert the truth of a theory can be argued to be hearsay.
Adding more sources of digital evidence would increase the probability that the communication evidence that is recovered would be considered hearsay, but to defend against this, the written and oral communications recovered from the new and original sources of evidence can be submitted to the court under the exceptions to the hearsay rule. If the prosecution can prove the evidence that was submitted satisfies one of the exceptions to the hearsay rule, that evidence will be considered admissible. Federal Rules of Evidence 803 through 807 provide all the exceptions to the rule against hearsay. Some examples of exceptions to the hearsay rule declared in Rule 803 include statements that refer to the present sense impression of the declarant, statements that describe the then-existing mental, emotional, or physical conditions of the declarant; or documents that are considered business records (Rule 803). In many instances, business e-mails satisfy the business record exception to the hearsay rule, but only if the e-mail is proven to be regular business conduct of the declarant. Overall, for any communication evidence submitted that is considered hearsay, the prosecution has to either apply it to an exception to the hearsay rule or deal with the fact that it cannot be used to prove the fact of the matter asserted.

Admissibility
Since digital evidence can easily be altered, the reliability of this evidence is almost always in question. Federal Rule of Evidence 702 requires that any scientific or expert testimony be reliable based on the methods and principles used by the expert and the application of these techniques and principles to the facts that are testified to in court (Goodison, et al. 12). The testimony provided by the forensic examiners about the evidence they have recovered from the digital devices that were seized is considered expert testimony, but the examiner first has to qualify as an expert in the field. The examiner can be qualified based on his or her education, training, skills, and knowledge (Rule 702). The examiner can demonstrate his or her expertise based on acquired certifications, such as becoming a certified fraud examiner, years of working in the field, degrees obtained related to the field, and published written works.

In many instances, the examiner has to provide scientific evidence along with the digital evidence to help the jury and the court understand what his or her findings mean with regard to the case. Congress determined five criteria to determine the admissibility of scientific evidence. The following has to be satisfied in order for scientific evidence to be admissible: the technique used to collect the evidence has to be tested; the evidence has to go under peer review, there must be a known error rate for the technique used, standards of operation must exist and be maintained, and the technique has to be generally accepted by the scientific community (Goodison, et al. 12). As long as all of these requirements are satisfied, the scientific evidence offered is considered admissible. When a digital forensic examiner presents the findings from an examination of a forensic image of a hard drive, the examiner must demonstrate that the software used to create the image of the device did not alter the data contained on the original hard drive. The software that is used must be widely used by other examiners in the same industry, and tested thoroughly. Otherwise the reliability of the evidence is compromised.

A famous example of examiners failing to thoroughly test their methods is the Casey Anthony case. Anthony was charged with the murder of her two-year-old daughter, and during the investigation law enforcement officials seized her computer. Forensic examiners testified that, based on their examination, Anthony had searched for terms such “chloroform,” “inhalation,” “neck-breaking,” “household weapons,” and “death” using Internet Explorer, with the term “chloroform” being searched for 84 times (Battaglia). Later it was determined that the software used to examine her computer did not give accurate results. After further examination, examiners realized the term “chloroform” was only searched for once, and they missed the browsing history from Firefox, which was Anthony’s default Internet browser (Battaglia). This mistake discredited these examiners and has been one of the main areas for blame as to the reason why Anthony was not convicted of murder. This mistake also discredited the reliability of the rest of the evidence that was submitted by these examiners.

The reliability of digital evidence from Smart TVs, wearable devices, and other devices that use cloud storage can be questioned because examiners in the field do not have a good amount of experience in examining these devices. Also, there are not many standard methods established in the industry regarding the forensic examination of Smart TVs, wearable devices, and other devices that use cloud storage. Because many forensic examiners rely on software to acquire a forensic image of the devices they examine, they have to ensure that the software they are using can acquire the image from that particular device. Once that is determined, examiners must also ensure that the data is not being altered by the software used so they can truthfully testify in court that the data was not altered in any way during the examination. If the data is altered, the evidence presented based on that data is not admissible in court.

Documentation/Authentication
The issue of documentation of digital evidence involves authentication and maintaining the chain of custody (Goodison, et al. 11). Authentication refers to proving that the evidence recovered from the digital devices seized during the investigation is genuine (Goodison, et al. 11). The examiner has to prove that evidence was created by the actual user of the device that was examined. For instance, if a Microsoft Excel spreadsheet was presented in court, the examiner would have to prove that the spreadsheet was created using the device that it is claimed to be from and that it was created by the defendant. To prove that the spreadsheet came from the claimed device, the examiner would have to go through the procedures of
how he or she acquired the data and the precautions that were taken to ensure that the evidence was not altered in any way during the examination. There are multiple ways that the examiner can prove that the defendant created the spreadsheet. One way would be to use the security features that are enabled on the device. If the user account that was used to create the spreadsheet was password protected, the examiner could argue that the only way the defendant did not create this file would be if the defendant shared the password with someone else. The examiner could also test the strength of the password to help prove that the defendant was indeed the person who created the spreadsheet. If the password tests to be weak, that would indicate that someone else could have easily guessed it or hacked the computer using a brute force attack. On the other hand, if the password tests to be strong, it could be argued that the only way another person could gain access would be if the defendant shared the password.

The second aspect of the issue with documentation is maintaining the chain of custody. The chain of custody records who handled evidence, where it was kept, and when it was handled (Goodison, et al. 11). The chain of custody helps ensure that neither the law enforcement officials nor the forensics examiners tampered with the device while it was in their possession. This document details the following: when the evidence was collected, where it was collected from, who owned the device, who had access to the device, how the evidence was collected, how the evidence was stored, who handled the evidence, and who had access to the evidence (Goodison, et al. 12). Each entry written on the chain of custody form is accompanied by a timestamp, a signature of the person who released the device, a signature of the person who received the device, and any necessary comments about the exchange. If the defense finds any time discrepancies in the chain of custody, any evidence submitted from the device listed on the form can be considered to be no longer admissible. This evidence can no longer be admissible because the prosecution can no longer prove that law enforcement officials or forensic examiners did not tamper with the device. For example, the timestamps between the time when the device was collected and when the device was checked into the evidence locker could be logged as 40 minutes. If the defense is able to prove that the distance between the location the device was collected from and the location of the evidence locker was only 20 minutes, this could invalidate all the evidence from this device. Law enforcement officials would have to provide an explanation as to why it took them twice as long to get the device to the evidence locker. If the judge does not feel as though the explanation is sufficient, all the evidence from that device could be inadmissible.

Adding new sources of digital evidence would require forensic examiners to determine different methods of authenticating the evidence collected from Smart TVs, wearable devices, and other devices that use cloud storage. These methods would then have to be thoroughly tested to make sure they won’t alter the original data, as there are not yet any industry-wide accepted methods for the authentication of data from these devices. Examiners also have to make certain that there are not any loopholes in the methods that are used to prove the authenticity of the evidence collected. Admissible evidence must be relevant and reliable, and proving the authentication of the evidence will satisfy the requirement that the evidence being presented is reliable. Without authentication, the evidence is not admissible in court.

CURRENT SOURCES OF DIGITAL EVIDENCE

Currently, the most common sources of digital evidence that are examined in criminal cases are cell phones and personal computers. Cell phones and personal computers are the most used devices in society today; almost everyone has a mobile phone or a personal computer or both. Congress has had the opportunity to address the conflicts between the evidence recovered from these devices and the legal issues encountered by digital evidence in general.

Personal Computers

“Personal computers” refers to both laptops and desktops that are owned for individual or business use. Currently, the general public uses computers for various reasons, such as social networking, online shopping, completing school work, or running a business. Computers have become a part of everyday life, which is why law enforcement officials have included computers as a standard device to examine when conducting a criminal investigation.

Forensically examining a computer starts with retrieving the hard drive and then creating a forensic copy of the hard drive. The examiner uses the forensic copy with a write blocker to conduct the examination (Owen and Thomas). These precautions ensure that the data on both the copy and the original hard drive are not altered in any way. Additional tools, such as different forensic examination software programs, are used to help with the imaging and examination of the hard drive. The most used and industry-accepted forensic examination software programs are EnCase, created by Guidance Software, and Forensic Tool Kit, created by AccessData (Owen and Thomas). These tools help examiners complete examination tasks such as retrieving deleted data, retrieving passwords, providing search functions for files, and data carving. These tools allow the examiner to examine more than one forensic image at a time.

Internet browsing history, user account information, and user-created files are the files that are most commonly collected when a forensic examiner is conducting an examination on a hard drive. The Internet browsing history provides information about the user’s browsing patterns, such as the websites he or she visited often, or common Internet searches that he or she has conducted. For instance, in an Internet gambling case, forensic examiners would look for information such as Internet gambling sites the user has visited and how many times he or she has visited these sites. Proving that the user
has gone to the site once is not enough because it can be argued that the user could have accidentally clicked on the link. If the examiner can prove that the user went to an Internet gambling site more than once on multiple occasions, the examiner can argue that the user was fully aware that it was an internet gambling site and intentionally accessed the site.

When an examiner is examining the user account information, the examiner can tell if the user account is password protected, whether the account is a regular user account or if the account has admin privileges, and the last time that account was logged in to use that device. This information is important because if the user account is password protected, the examiner can prove that the only way someone could access that account is by knowing the password. This point can be further proven by determining the strength of the password. If the password is considered to be strong, this would further enforce the point that the only users that logged on to that account would be users that knew the password. If the password is considered to be weak, then it weakens that point because it can be argued that the password could have been easily guessed by someone close to the device's owner.

Determining if the account had administrative privileges or not provides information on the abilities that the user had while logged in to that particular account. Having admin privileges allows the user to have full control. They are allowed to install and run new programs and may also change many of the general settings of the computer, among other privileges. Using the Internet gambling scenario, if the forensic examiner found a program installed on the computer that was related to Internet gambling, the forensic examiner can argue that the only accounts that would be able to install this program would be user accounts that had administrative privileges. A regular user account would be able to access the same program, but would not be able to install the program because he or she would not have administrative privileges.

User-created files range from word processing files to e-mails sent using the default e-mail program installed on the computer, such as Microsoft Outlook. These kinds of files provide information on how the user used the computer on a regular basis. User-created files related to school would be found if the primary use of the computer was to complete schoolwork. On the other hand, if the primary use was business related, the user-created files located on the hard drive would be business related. Business-related files could be e-mails to and from coworkers or official business documents like articles of incorporation. Proving the general use of the computer in a criminal investigation helps to either reinforce that the intentions of the defendant were in support of the crime for which he or she is charged or help to reinforce that the defendant’s intentions were not in support of the crime he or she is charged with.

The digital evidence gathered from personal computers provides a plethora of information for law enforcement officials to solve the case and for the prosecution to use to build a strong case against the defendant. Furthermore, most legal issues have been resolved to some degree when it comes to digital evidence recovered from a personal computer, but criminals are starting to determine ways to cover their tracks when using these devices. Adding additional sources of digital evidence helps combat this issue and in some cases provide even more information not present on the computer.

Mobile Phones
Mobile phones, just like personal computers, have become a part of everyday society and are used for both personal and business purposes. These devices contain information about the people that the owner interacts with on a regular basis, the owner’s usual activities, and the owner’s main interests. This information can aid criminal investigations in multiple ways, like guiding law enforcement officials in the direction of those they should question. For instance, if law enforcement officials notice that the victim was on the phone minutes before he or she was killed, officers would immediately be signaled to find out who the victim was talking to, and to question that individual in an effort to gain evidence.

Forensically examining a mobile phone is slightly more complicated than examining a hard drive because the data on the cell phone can be altered by simply allowing the phone to lose power. A mobile phone can also be in five different states during the examination. The phone can be in the following five states: (1) off, where the phone is powered off and the battery is removed, (2) in a nascent state where there is no user data present, (3) in a quiescent state where the phone seems to be inactive but there are background functions, such as maintaining network connectivity, being performed, (4) in a semi-active state where the phone is waiting for a certain function like an alarm clock to go off, or (5) in an active state where the phone is on, and a function is currently being performed on it like a telephone call (Owen and Thomas). Determining the state of the phone is important because this determines the method that should be used to conduct the examination of the device. A rule of thumb for mobile device forensic examiners is to put the phone in airplane mode, which stops any network connectivity to and from the phone. Allowing network connectivity presents risks, such as allowing someone to remotely wipe the phone or alter the data on the phone in any way.

Typically, when a forensic examination is done on a cell phone, a report is printed out at the end that details the saved contacts, all of the incoming and outgoing text messages, all the calls from the call log, and any multimedia that was located on the device itself. This information is then used to prove the interactions between certain people that may have been involved in the crime. For instance, the owner of the device denies knowing another suspect that’s involved in the case, but a forensic examiner discovers that not only did the
owner have the suspect’s number, but the number was also saved, and
the two talked to each other on a regular basis. This discrepancy raises
a red flag because if law enforcement officials discover that the owner
of the device is lying, they then have to question everything the owner
has told them.

Mobile phones give both law enforcement officials and the
prosecution information about the suspect’s interactions with people
and everyday activities, which may be used to either prove the
likelihood of the subject’s involvement in the crime or prove that
the subject was not involved at all. Including wearable devices like
smartwatches allows forensic examiners to have another source to
gather similar information about the owner because smartwatches are
completely integrated with the smartphone connected to the watch.
The more digital evidence the prosecution has from these sources of
digital evidence, the stronger the case against the defendant.

NEW SOURCES OF DIGITAL EVIDENCE

Smart TVs
One of the newest technological revolutions has been the invention
of the Smart TV. This television allows the user to access the Internet,
social media apps, and video streaming services like Hulu by using
Wi-Fi, but also incorporates the normal functions of a regular
Television. Users can also connect external devices to the TV such
as his or her mobile phone or an external hard drive. Due to the
available features on a Smart TV, they contain information such
as visited websites, pictures stored on the TV, and the history of
connected devices (Boztas, et al.). Similar to the same information
found on a computer, this information can be used to determine
the Internet browsing pattern of the user. Examiners can tell which
websites the user visited and how many times he or she visited those
websites.

Because the Smart TV is connected to the home network, it can also
provide information about other devices connected to that same
network (Boztas, et al.). Being in possession of the information about
other devices that were connected to the same network as the Smart
TV allows forensic examiners to determine if there are any devices
that law enforcement officials failed to seize from the suspect. These
missing devices could contain digital evidence crucial to solving the
case and in building a strong case the prosecution can use to convict
the correct suspect.

Flash storage memory chips are one of the main methods of storage
used by Smart TVs. Depending on the hardware of the Smart
TV, information from a Smart TV can be recovered using three
methods: the NFI Memory Toolkit II (MTK II), the eMMC five-
wire method, and the application method (Boztas, et al.). The MTK
II is a combination of hardware and software. The hardware is used
to provide power and signals to the memory chip, and the software
is used to run the necessary commands to access the data so the
examiner can collect the necessary digital evidence (Boztas, et al.).
The eMMC five-wire method entails connecting five different
signals to the memory chip, then using a standard SD card reader
with a write-blocker attached to it to access the data and complete
an examination (Boztas, et al.). The application method involves
creating a custom application that takes the data and then writes it to
an external storage device (Boztas, et al.). All three of these methods
prove to be reliable in that they do not alter the data being acquired
in any way, but the application method has proven to be susceptible
to any software updates applied to the TV.

As with any other source of digital evidence, those using evidence
from Smart TVs will encounter some legal issues. The issue of
authentication would be encountered with examining Smart TVs as
there is no way to determine who exactly is using the Smart TV
at a given time. Smart TVs do not have separate user profiles so the
examiner would not be able to differentiate the browsing patterns
between the users and would not be able to narrow the browsing
history down to one user. There are some brands of Smart TVs that
require the owner to create an account, but that is only with certain
brands. Samsung Smart TVs make the user create a Samsung account
to access apps like Netflix and Vudu, which are two different video
streaming services. If the examiner performs an examination on this
particular Smart TV, the examiner could at least narrow it down to
the owner based on the registration information for the account on
the Smart TV.

Congress will also have to determine how the Fourth Amendment
applies to the evidence from Smart TVs. Congress officials will do this
by determining the expected level of privacy, and determining what is
required in the search warrant for the search and seizure of Smart TVs
to be legal, or if a search warrant is required at all. As the technology
of Smart TVs evolves and more information is available to retrieve
through forensic examination, Congress will have to make sure that
Fourth Amendment rights are addressed correctly. This may seem
cumbersome, but the information recovered from Smart TVs can
prove to be very beneficial.

Including Smart TVs as a standard device to examine is recommended
because of the importance of the Internet browsing history, the
history of connected devices, information about devices connected
to the same network, and information stored directly on the
TV’s memory card that is available for examination. Using this
information, forensic examiners and law enforcement officials can
determine other devices they may have missed in the warrant, whether
these devices came from examining the other devices connected
directly to the TV, or those connected through the network. They
can also determine the browsing patterns of the user, but forensic
examiners have to be careful to make sure they can attribute these
browsing patterns to a specific user since there aren’t any user accounts
Wearable Devices
Recently, companies have developed devices that consumers can wear on their wrists that have the ability to connect to the consumer’s mobile phone. The most popular device has been smartwatches, devices that allow the user to have access to his or her e-mails, text messages, calls, voicemails, calendar, and any other notifications from apps the user has authorized. The two biggest competitors in the mobile device industry, Apple Inc. and Samsung, have created their own versions of the smartwatch.

Forensically examining smartwatches has a high potential for providing some very useful evidentiary information. To forensically examine a smartwatch, the forensic examiner has to gain root access to the watch’s operating system, the highest permission level, which lets the examiner access the entire file system of the smartwatch (Baggili, et al. 306). Once that access is gained, the examiner then proceeds to take a forensic image of the device (Baggili, et al. 307). A forensic image is an exact copy of all the data on the device that has not been altered in any way and is protected from any alterations that could occur incidentally during the examination. After examining the forensic copy of the data on the device, multiple database files can be found that contain messages, e-mails, contacts and address book information, and health and fitness data (Baggili, et al. 309). Depending on the make, model, and available features of the smartwatch, the examiner will find different database files. For instance, a Samsung Gear 2 Neo smartwatch contains database files for messages, health and fitness data, e-mails, and contact and address book information (Baggili, et al. 309). On the other hand, the LG G watch only contains database files for events and notifications, contacts and address book information, and health and fitness data (Baggili, et al. 309). The difference in data files could be attributed to the available features for each device or the different operating systems each watch uses.

Essentially, a smartwatch acts as an extension of the mobile phone it is connected to at the time. This connection is beneficial during an investigation because it means additional information that may have been deleted from the mobile phone can be found on the smartwatch; as long as the information examiners are searching for was created while the phone was connected to the watch.

Digital evidence from a smartwatch is not exempt from the legal issues that are encountered with all forms of digital evidence. In the application of the Fourth Amendment to digital evidence from a smartwatch, Congressional officials have to determine if the search and seizure of such a device without a warrant is violating a citizen’s Fourth Amendment rights. One factor to consider in this determination is if a person has a reasonable level of privacy when it comes to using a smartwatch or if the smartwatch should automatically inherit the same level of privacy as a cell phone. If it is determined that there is a reasonable expectation of privacy or that the watch should inherit the same level of privacy as the device it’s connected to, a warrant would be required to search and seize this type of device.

Digital evidence from a smartwatch would also raise the hearsay issue when it comes to using digital evidence in court. The communication information recovered from a smart watch would be treated the same way as communications recovered from a mobile phone. Any of the written and oral communications that are recovered from this device and submitted in court could be considered hearsay and potentially inadmissible in court, but if the prosecution can apply one of the exceptions to hearsay to the evidence, this evidence will no longer be considered inadmissible.

Authentication of the data recovered from smartwatches would be a major issue because the methods that are available to collect the evidence are very new to the industry, and they are not thoroughly tested. The imaging method used for the LG G watch requires that the watch is reset to factory settings to get a clean forensic image of the watch (Baggili, et al. 309). There is some original data lost because the watch has to be reset. Presenting this method in court would raise questions as to the authentication of the submitted evidence derived from this device. The court would question what data is being altered or lost by doing a factory reset and how that data affects the evidence being presented.

Adding wearable devices like smartwatches to the list of standard devices examined during a criminal investigation does encounter some legal issues, but the evidence recovered from these devices can provide essential information. The e-mails, calls, text messages, and calendar events help provide information about the people the device’s owner frequently interacted with and also the usual activities in which the device’s owner partook on a daily basis. Having this information helps law enforcement officers create direction in the criminal investigation as to who to question and how to try to gain additional information regarding the crime. Referring to the Philip Welsh case where Welsh was found murdered in his home, law enforcement officials were missing digital evidence like text messages and phone calls, which lead to them being unable to solve his murder. The law enforcement officials did not have a clue as to who interacted with Welsh right before his murder, so they did not have a clear direction as to with whom they should talk to get additional information about Welsh. The benefits of the information that can be gathered from the digital evidence from wearable devices like smartwatches outweigh the drawbacks presented by the legal issues encountered with this evidence.
Cloud Devices

Additional information not found on the actual device can be recovered from any cloud storage services connected to that same device. Users mainly use cloud storage to store data that they either could not fit on the physical memory of his or her device or to store data they need to be able to access from anywhere. Devices like mobile phones, computers, and tablets can be connected to cloud storage services like Dropbox. Many businesses are starting to convert to using this storage solution because it allows all employees that have been given access the ability to look at documentation from anywhere. Using cloud storage also cuts costs for businesses because they no longer have to maintain any storage hardware; that would be the responsibility of the company providing the cloud storage solution.

Forensically examining cloud-based devices becomes complicated because there are three different models. Cloud services can be offered as software as a service, platform as a service, or infrastructure as a service. With software as a service, the cloud service provider handles everything while the customers just use the cloud as a storage solution (Roussev, et al.). As platform as a service, the customer has control over the application and the data being stored, and as infrastructure as a service, the customer has control over everything except the hardware and virtualization (Roussev, et al.). To accommodate the three different models of cloud storage, a forensic examiner has to use an API-based tool to connect to the cloud and examine the log files that keep track of when files were transferred onto the cloud (Roussev, et al.). With the examination of cloud-based devices, forensic examiners can discover user-created files that couldn’t be found on the physical device. It is possible that users have used cloud storage as a way to hide documents they did not want others to discover or have access to, so having access to the information on the cloud could help to fill some of the potential information gaps created after examining the physical device that was connected to the cloud.

Adding digital evidence from cloud-based devices raises two main legal issues: how the Fourth Amendment applies to this evidence, and jurisdictional boundaries. As with the other new sources of digital evidence, Congress has to determine the expected level of privacy expected for each new device, among other things. Despite the processes that have to be completed when including new sources of digital evidence, it is more beneficial to include them than not because history has shown how crucial digital evidence is in solving a criminal case quickly and accurately and in helping the prosecution build strong cases against defendants.

CONCLUSION

The benefits of having this additional information from Smart TVs, wearable devices like smartwatches, and cloud storage devices during a criminal investigation outweigh the legal issues and obstacles that will be encountered by including this additional evidence. With each new source of digital evidence, law enforcement officials, forensic examiners, and Congressional officials must determine limits. Law enforcement officials have to make sure they include these devices in the warrant, and they have to make sure to handle the device correctly so none of the data is lost between the time it was seized and the time the forensic examiners receive it. The forensic examiners have to make sure the data acquisition methods they are using can hold up in court. These methods have to be thoroughly tested to prove they do not alter the data being examined in any way. Congress has the obligation to ensure that citizen’s rights are not impinged upon by determining the level of privacy expected for each new device, among other things. Despite the processes that have to be completed when including new sources of digital evidence, it is more beneficial to include them than not because history has shown how crucial digital evidence is in solving a criminal case quickly and accurately and in helping the prosecution build strong cases against defendants.

BIBLIOGRAPHY


**MORGAN RONE**

Ms. Rone graduated with a master’s degree in Forensic Studies from Stevenson University in August 2016. She obtained her bachelor’s degree in Business Information Systems from Stevenson University in December 2014. Ms. Rone is currently working as a software engineer for Exceptional Software Strategies developing web applications for the company’s customer.
Walter Pavlo Research Paper
Shaun Madary

Walter Pavlo embezzled more than six million dollars from unsuspecting clients while at Microwave Communications of America, Inc. (MCI). MCI was a long distance telephone company. Subsequently, Pavlo was charged with obstruction of justice, money laundering, and mail fraud (Weinberg). While working at MCI as a collections manager, pressure from management in the middle of the 1990s pushed Pavlo to hide hundreds of millions of dollars in aging bad debts and uncollectable receivables owed to MCI (Weinberg). This was done in order to help MCI avoid bankruptcy. Pavlo said that he “cooked the books to make the numbers look better” (Wickham). Pavlo was then able to transfer company money into his own personal banking account undetected for over a year (Wickham). This article discusses Pavlo’s background, how Pavlo and his conspirator were able to achieve this embezzlement, how the fraud triangle relates to his case, and the lessons Pavlo learned from his experience.

Pavlo appeared an implausible individual to commit a fraud of this magnitude. He grew up near Sistersville, West Virginia, and Savannah, Georgia, with two younger brothers. His father said Walter, Jr. was a hard worker who started as quarterback in high school for one season (Weinberg). Walter “Walt” Pavlo went on to obtain an engineering degree from West Virginia University and received a master’s degree in finance from Mercer University. Equipped with these degrees, he had a bright future ahead. He worked for Goodyear Tire as a financial analyst in the Aerospace division, then went on to work at GEC Ltd. of England as a contract manager. He finally held a senior manager position in MCI’s Telecommunications division (Zeune). Here, he was responsible for billing and collections of MCI customers (Zeune). Pavlo had an honest background in both his schooling and career. What would drive him to commit such a large fraud during his tenure at MCI?

To answer this question, the culture and management pressure at MCI must be examined to understand the whole picture of what was occurring at MCI in the middle of the 1990s. The style of management in these types of companies, particularly in MCI, was imperial. This means that the business strategy was determined by a leader or top management team. The role of top management was to provide direction to the organizational members. In this case, Pavlo obeyed orders from management at MCI (Rao). When employees only obey orders and management has all the power, there is a greater chance for fraud to occur.

In 1995, MCI and Pavlo were handling 650 million dollars in collections per month. Pavlo was in charge of handling high-risk accounts, collecting receivables and coming up with various ways to dispose of these receivables (Weinberg). Many resellers would not pay money owed to MCI because of situations created by MCI’s “ramp-up” contracts, in which the companies were charged a set price for an increasing number of minutes (Weinberg). A reseller in the telecommunication industry is a business entity that purchases communications services from a carrier at wholesale prices then sells them to the public. These resellers do not own transmission facilities.

Based upon these “ramp-up” contracts, resellers eluded paying MCI to avoid bankruptcy. On January 4, 1996, Pavlo sent management a memo stating that there was 88 million dollars or more in reseller receivables for which MCI would be unlikely to collect payments (Weinberg). Management had to figure out what to do to keep the business afloat, or to make it seem like it was afloat.

There were a few schemes attempted by Pavlo and other coworkers to remedy this collection issue, resulting from the pressure from management. Initially, Pavlo did not want to engage in any number falsifying, but was pushed to do so by management. The first scheme was turning some of the unpaid bills into promissory notes. Even though these notes were most likely worthless, MCI told auditors that 75 percent of the face value of the notes was expected to be collected (Weinberg). But this scheme could not keep up with the increasing number of accounts owed to MCI that were over 90 days late. Next, Pavlo and other MCI employees attempted to postdate invoices so the accounts that owed money would look like they hadn’t owed MCI for as long as they actually did. Another scheme they used was “placeholder credits.” This meant that the finance department would credit customer payments up to several million dollars, when MCI had actually never received these payments (Weinberg). Pavlo did not know what else to do; he did not want to lose his job and knew his name was on much of the falsified paperwork. He feared that he would be the scapegoat for management if their schemes were caught.

Pavlo was starting to become upset that he was the only individual in these fraud schemes not becoming rich from the “fudged” financial numbers at MCI (The Fraud Triangle). After drinking one night, Pavlo and a friend came up with a program called “Rapid Advance” and started working with Mark Benveniste, president of Manatee Capital. In this program, Pavlo would collect from MCI clients directly by pocketing payments from the clients that owed money to MCI. (The Fraud Triangle). Pavlo started to see success with this program and wanted to go after some MCI clients that owed a larger amount of money.

One example of a larger client Pavlo “ripped off” was Robert Hilby of Telemedia Networks. Robert was a client of MCI, and Pavlo believed he had no intention of paying. Harold Mann, one of Pavlo’s friends working with him on the scheme, contacted Hilby and offered to have his own firm, Orion Management Services, pay off Telemedia’s MCI debt in exchange for a $200,000 upfront commission, 25 percent of Telemedia, and a promise to pay Orion back over five years (Weinberg). However, Pavlo and Mann never paid MCI because they deposited the $200,000 into a bank account in the Cayman Islands (Weinberg). Pavlo used Orion to divert funds from MCI’s resellers to accounts he and his conspirators controlled in the Cayman Islands,
and then manipulated MCI’s accounting documents to hide the theft (Weinberg). What was the reason behind Pavlo and his conspirators committing this fraud? Did they know they could take advantage of the system? Was it greed? Or did Pavlo want to get revenge on the clients that had never paid back the money they owed to MCI?

The fraud triangle can help to explain why a particular fraud occurred. It is understood that in order for someone to commit a fraud, they almost always possess three elements. These elements are perceived opportunity, perceived pressure, and rationalization. Perceived opportunity is the ability for an individual to commit the fraud. Examples of this element include having the working knowledge to manipulate the accounting system, or being in a position where it is easy to commit the fraud because of easy access to financial documents. Perceived pressures could be financial strain, or a drug addiction or gambling habit. Finally, an individual could rationalize that the fraud would be harmless and not hurt anyone else. Other rationalizations include the company “deserving it,” or that the sum of money stolen wouldn’t be very large. Pavlo has explained how he displayed all three of these elements of the fraud triangle leading up to the commission of his schemes at MCI (The Fraud Triangle).

In this case, Pavlo stated that his perceived pressure, or motivation, was “the desire to support a more affluent lifestyle” (The Fraud Triangle). Many times, individuals wanting that more affluent lifestyle will commit fraud against their better judgement. In many cases where fraud occurs in business, there are observable red flags, such as a change in clothing or vehicle that can point to possible fraud.

Pavlo stated his perceived opportunity was “access to the books he was already doctoring” (The Fraud Triangle). Had Pavlo not been in the position he held at MCI, he would not have had the opportunity to commit the fraud. Finally, Pavlo’s rationalization to commit the fraud was “resentment against his bosses, who he believed were pressuring him into ‘cooking the books in the first place’” (The Fraud Triangle). Pavlo detested his bosses for many reasons, including them compelling him to alter company financial figures, making him feel like he would lose his job, and not rewarding him in any way for “cooking the books” for management. All of these factors made it easier for Pavlo to rationalize that it was acceptable to steal from his company’s management, who he viewed as unethical and only caring about themselves.

Pavlo and Mann ended up stealing six million dollars from MCI customers by the time they were caught (The Fraud Triangle). Pavlo stated that while he was carrying out the fraud against MCI, he felt no remorse for his actions because he believed he was not the only one engaging in fraud schemes (Jacka). Pavlo also said that “These people are doing it, I looked up to them. They’re having to fudge, they’re not going to mind if I do too” (Jacka). This statement shows that managers and leaders of a company are looked up to and respected by their employees. Ethics come from the top of the company. If that ethical behavior or respect is gone, lower level employees are more likely to commit fraud because they are better able to rationalize their unethical behavior.

What were the lessons Pavlo learned from this case and how can white collar crime be better detected in the future? Pavlo’s greatest lesson learned was the magnitude to which his actions affected other individuals, including his coworkers. Pavlo stated that “[tr]ust is a value, and if you lose someone’s trust, you lose value” (Wickham). Many individuals lost their jobs because of Pavlo’s actions at MCI. Pavlo stated that crimes comparable to his will usually end poorly for the individual committing the fraud. During his scheme, Pavlo did not stop to ponder the ramifications of his actions (Wickham). Based on his speeches to students, he hopes that individuals will think twice about committing frauds in the future and will use his story as a cautionary tale.

Finally, there are ways that white collar crimes similar to Pavlo’s can be better detected in the future. There are a few tips Walter Pavlo gave to reduce this type of crime. The first is to consider where opportunities for bribery could occur (Wickham). By looking at weak points in a company, such as procurement or awarding of contracts, there is a better chance to prevent this type of fraud from occurring. He also said that a company’s only protection from fraud is to use data and analytics to create policies and procedures to curtail fraudulent behavior (Wickham). Without policies and procedures enforced by management, there will be more opportunity for employees like Walter Pavlo to commit fraud.

WORK CITED


84
SHAUN MADARY

Shaun Madary has a Bachelor of Science degree in Business Management from York College of Pennsylvania. Currently, at Stevenson University in Owings Mills, Maryland, he is pursuing a Master of Science in Forensic Studies with a concentration in Investigations. He graduated in December of 2016. This program prepares students to gather evidence and relevant case facts, plan and conduct an investigation by learning how to interview individuals important to the case, and develop findings and recommendations based on analysis.
Disaster Response
Joyce Williams, DNP, FAAN

The threat of a disaster is faced daily by someone. Definitions of what a disaster comprises may vary but the fact remains that most disaster situations are ones in which local resources are strained beyond the capacity immediately available. Thomas E. Drabek notes that a disaster is different from an emergency, which may cause an adverse effect but does not require extraordinary use of resources to normalize conditions.

Examining declared disasters in the United States during 2016, the year began with severe storms, tornadoes, and flooding in Mississippi, and severe winter storms in Alabama, Oklahoma, and Oregon, where mudslides added more difficulties for the already strained communities. The mid-Atlantic region had significant snowstorms in March, and the fall brought hurricanes Hermine and Matthew to the southeast.

In the United States, formal emergency management began during the Truman administration and continues to advance. Each mass casualty incident (MCI) provides an impetus to revisit best practices. The Federal Emergency Management Agency (FEMA), as part of the Department of Homeland Security, supports and ensures building, sustaining, and improving capacity within the nation to have robust resilience and preparedness.

Immediately following the 2001 terrorist attacks, efforts were made to eradicate the deficiencies in disaster management in the U.S. using funding from the U.S. Centers for Disease Control and Prevention. This grant became the primary source of funds allocated to address any all-hazards events; without a constant source of revenue, serious risks are possible, from disease outbreaks or bioterrorism to natural disasters such as hurricanes, tornadoes, and floods. In the past 10 years, increased awareness has changed the paradigm to the point where improved preparedness is more common and resources are more readily available, but reports still demonstrate a lack of readiness globally.

A report supported by the Robert Wood Johnson Foundation (RWJF) in 2011 stated that the readiness groundwork in the U.S. is at “risk for elimination” of some key programs due to continued cuts to federal public health emergency preparedness funds. “Preparedness had been on an upward trajectory, but now some of the most elementary capabilities—including the ability to identify and contain outbreaks, provide vaccines and medications during emergencies, and treat people during mass traumas—are experiencing cuts in every state across the country.” Following this scathing report, actions were taken to amend the deficiencies across the nation. This resulted in a compilation of more than 100 different measures to assess the health security and preparedness of the nation, starting the National Health Security Preparedness Index. The 2016 report notes that “the United States scored 6.7 on a 10-point scale for preparedness—an improvement of 3.6 percent since the Index began three years ago.” The progress is ongoing, but disparities remain among the states. Based on the analysis, six categories demonstrate where critical preparedness is best understood: incident and information management, health security surveillance, countermeasure management, environmental and occupational health, community planning and engagement, and healthcare delivery.

A primary tool in the emergency manager’s toolbox is the Hazard Vulnerability Analysis (HVA). It calls for an organization to work toward hazard prevention while simultaneously preparing for the unexpected emergencies and unforeseen situations that inevitably occur. The “all-hazards” approach involves taking the actions necessary to prepare for, respond to, and recover from hazards of all types. It provides one straightforward method to respond to disasters. One cannot underestimate the importance of the planning phase, where protocols and standard operating procedures (SOPs) are compiled, made available, and practiced. Oftentimes, adequate warning is not possible, necessitating immediate access and recall to protect individuals, records, and staff who may be right in the path of a tornado, hurricane, or tsunami. WHO/Europe acknowledges that the all-hazards approach is pivotal to adequately preparing for a natural, technological, or societal event, as the challenges to systems are parallel. Having a comprehensive understanding of risk reduction and using predictive modeling ensures that recovery outcomes are managed appropriately. (http://www.euro.who.int/en/health-topics/disasters/disaster-preparedness-and-response/policy/)

Disasters affect morbidity and mortality due to the combined effects of event intensity during active phases, property destruction, response and recovery efforts, and population displacement. An important component of disaster preparation is the role of healthcare providers. Their expertise is a predominant factor in the response to casualties.

Healthcare awareness can be traced to the efforts of Florence Nightingale during the Crimean War. The beginnings of disaster forensic nursing are notable, as Florence provided support for British soldiers who were not only besieged by battle wounds, but were ravaged by epidemics of cholera and typhus, as well (Williams in Crane, 2013). Because of her intuitiveness, standards improved in sanitation, hospital design, and patient care. Epidemiology became an essential response tool during a disaster event, used to identify trends, infectious components, and biological agents.

Worldwide, it is commonly acknowledged that nurses play an integral role in disaster response. Forensic nurses are instrumental as members of the inter-professional team deployed to assist during a disaster. Specialized education and partnering with governmental and/or non-governmental (NGO) organizations provides knowledge and expertise to prepare, organize, respond, and recover casualties caused by an unexpected event. Despite the call for nurses trained in disaster response, a host of practice, policy, and research challenges limit nurses’ effectiveness in response and recovery efforts.
Many nations and disaster relief organizations invoke history to reiterate to the world a strong message on the need for preparedness. Professionals across the globe encourage learning, using past events to improve future readiness. Risks can be realized from “lessons learned,” conference meetings, focusing on linkages between past events, and connecting current-century events that damaged a region. This expertise is needed when community assets become compromised. Traditionally, there has been limited support for addressing casualty surges, displaced populations, and violence prevention.

Community disaster plans must integrate healthcare providers as primary resources to render immediate care to victims injured during the event. A forensic nurse must be diverse and demonstrate the following clinical capabilities: trauma and emergency nursing, mental health and critical incident stress management, death investigation, addressing infectious disease, syndromic surveillance, and public health nursing. Each aspect poses many challenges.

The role of a forensic nurse trained in emergency management and disaster preparedness is multidimensional. Several potential contributions of forensic nurses can demonstrate how intimately involved the position of a forensic nurse can be: conducting hazard vulnerability analysis; writing disaster plans, orders, and action guides; acting as a key member of emergency operation centers, health departments, and health minister teams; providing administrative and supervisory services pertaining to training and operations; managing resources, rapid response teams, and impact assessments; filling executive positions by creating policy; solving current issues; and leading recovery and restoration teams. However, work is needed to identify the nursing practices that are most effective in improving population outcomes across the disaster life cycle.

Disaster forensic nursing has evolved over the past several years, providing specialized care to populations directly or indirectly affected by a mass casualty event. Expertise is provided in the following areas:

- Trauma care coordinator
- Medico-legal death investigator
- First responder
- Mental health counselor
- Researcher, investigator/epidemiologist
- Forensic nurse examiner
- Incident commander
- Community assessment coordinator
- Decontamination team member
- Manager/coordinator of shelter

Disaster nursing practice incorporates four central concepts of nursing theory: person, environment, health, and nursing. Advanced nursing education focuses on prevention and response following basic and advanced disaster life support core principles. It is significant to note that prevention has become a significant goal, migrating from the traditional pillars of “preparedness, planning, response, and mitigation” of the past.

Communities are positioning themselves to better understand the complexities pertaining to disaster preparedness, including resilience. The forensic nurse is situated to be an integral partner in all phases of disaster management. Advanced practice education has prepared forensic nurses to act during the pre-event, throughout the active periods, and well into the aftermath or post-event. Challenges to the forensic system include:

- Mass evacuations; disorganized exodus
- Limited or unavailable access to care
- Collaborating with outside agencies to provide services
- Reorganizing services in temporary locations
- Loss of evidence and records
- Loss of communication systems
- Immediate ruin of the healthcare system
- Law enforcement overwhelmed/understaffed
- Areas vulnerable and unprotected increasing risk

Disaster executives worldwide continue to establish structures in their respective countries to set policy, disaster relief plans, guidelines, and laws. Working with the healthcare team, including the forensic nurse, is advisable to advance the opportunities for communities to improve preparedness overall. Disasters are complex and place a significant burden on administrators and health officials. Using the services of trained and dedicated professionals with expertise in emergency principles, forensic processes, public health, and medical interventions promotes building the capacity in communities for a more effective response.

**JOYCE WILLIAMS**

Dr. Joyce Williams is an Assistant Professor in higher education instructing graduate students. Dr. Williams primary focus is injury prevention that includes: injury assessment on children, analysis and investigation of death related to mass casualty, including natural disasters, terrorist action and armed conflicts; deaths that occur by violence, suicide, suspicious/unusual manner. Her research includes analysis of combat mortality casework and protective armor and death from non-medicinal inhalants. Her notable contributions to forensic nursing include deployments as a member of the Disaster Mortuary Operational Response Team to United flight 93 following 9/11, in Shanksville, Pennsylvania in 2001 and also to Baton Rouge, LA in 2005 for Hurricane Katrina. Dr. Williams earned her
Bachelor’s in Nursing degree from Antioch University; Masters of Forensic Science Administration from Oklahoma State University; and Doctor of Nursing Practice from the University of Tennessee Health Science Center. She consulted in Malaysia for Normah Medical Specialist Center, a private hospital, evaluating nursing competency and practice. As a professional she is committed to advancing the efforts of advanced practice forensic nurses and volunteers her professional expertise for the International Association of Forensic Nurses Commission on Certification, the American Academy of Forensic Science, and the World Association for Disaster and Emergency Medicine as well as partnering with the American Nurses Credentialing Center in the development of the Advanced Practice Portfolio for certification for forensic nurses. She serves on the Maryland Human Trafficking Task Force Victim Services Committee and is active in the development of medical protocols for victims and the education of emergency department personnel working with trafficked individuals.