2017

Exploring Myths in Digital Forensics: Separating Science From Ritual

Gary C. Kessler
Embry-Riddle Aeronautical University

Gregory H. Carlton
California State Polytechnic University

Scholarly Commons Citation

Kessler, G. C., & Carlton, G. H. (2017). Exploring Myths in Digital Forensics: Separating Science From Ritual. *International Journal of Interdisciplinary Telecommunications and Networking, 9*(4). https://doi.org/10.4018/IJITN.2017100101

Exploring Myths in Digital Forensics:

Separating Science From Ritual

Gary C. Kessler, Embry-Riddle Aeronautical University, USA

Gregory H. Carlton, California State Polytechnic University, USA

ABSTRACT

Digital forensic methodology deviates significantly relative to the methods of other forensic sciences for numerous practical reasons, and it has been largely influenced by factors derived from the inception and evolution of this relatively new and rapidly changing field. Digital forensics methodology was developed more by practitioners in its early days rather than by computer scientists. This led to accepted best practices in the field that may not represent the best or, at least, tested, science. This paper explores some of these differences in the practice and evolution between digital and other forensic sciences, and recommends scientific approaches to apply to many digital forensic practice rituals.

Keywords—Forensic science, computer forensics, digital forensics, best practices, evolution of computer forensics, dogma and ritual

INTRODUCTION

Although now accepted as a recognized forensic science by the American Academy of Forensic Sciences (AAFS), digital forensics is frequently treated differently than other, more traditional forensic sciences. While it is obvious that characteristics of cyberspace are different from those of physical space, the differences between digital forensics and "real-world" forensics are more subtle; the tools have a different relationship to the materials being examined, the results of the processes are different, and the evolution of the disciplines are different.

This paper will explore some of the ways in which the evolution of digital forensics has occurred that demonstrate the differences between it and forensics in the physical world. Section II will describe the basic processes of forensics and how they apply to digital forensics. Section III will describe the practice of digital forensics, again focusing on the differences between cyber and physical world forensics. Section IV discusses the testing of digital evidence and how heretofor "untested" dogmas became industry best practices. Section V provides a summary and conclusion.

THE PROCESS OF DIGITAL FORENSICS

Due to the manner in which the field of digital forensics evolved, many practices that were developed in the early stages during the 1990s remain in common use today without question. The authors contend that some of these practices have risen to the level of ritual and dogma, and while they might have made sense more than twenty years ago, they have not been studied from a scientific perspective to understand their relevance in today's environment.

One of the foundations of forensic science is Locard's Exchange Principle, which says, in essence, "Every contact leaves a trace" (Petherick, Turvey, Ferguson, 2010). Put another way: if two objects come into contact with one another, some part of each object is left on the other. All of the forensic sciences assume that such contacts and exchanges take place during the commission of a crime.

One common model of the forensics process, which applies equally to digital forensics or "physical" forensics, includes the following six phases (Casey and Schatz, 2011; Palmer, 2001):

1. *Identification:* Surveying a crime scene to determine potential sources of evidence that might have a nexus to the crime.
2. *Preservation:* Maintaining the state of potentially probative items to prevent changes, ensuring evidentiary integrity.
3. *Collection:* Assembling potential evidence in a manner so that the items can be forensically examined on-site (as necessary) or transported to a laboratory facility.
4. *Examination:* Testing each evidentiary item to extract probative information, making it available for analysis. This phase is guided by the legal context of the seizure and scope of the search of the items.
5. *Analysis:* Application of the scientific method, systematic processes, and critical thinking to look at the totality of the evidentiary information to answer the fundamental investigative questions: who, what, where, when, why, and how. This phase includes the analysis of both incriminating and exculpatory evidence.
6. *Reporting:* Document the entire forensics process, particularly explaining how the analysis leads to the conclusions about the crime. The type of investigation – i.e., corporate, civil, or criminal – provides the context for this phase.

A. Digital Forensics

Digital forensic practitioners analyze traditional computer systems (e.g., laptops, desktops, and servers), as well as network traffic, mobile devices, and digital media (such as pictures and other images, audio recordings, and videos) (Casey and Schatz, 2011). Locard's Exchange Principle applies in cyberspace as well as it does in physical space. Indeed, it applies so well that there are often hundreds or thousands of contacts that examiners may not be able to detect because of the wealth of devices touched and logs updated as data moves from one place to another on the Internet and other networks.

Digital forensic examiners (DFEs) apply the scientific method to examinations and analysis. DFEs observe, document, and analyze in order to report findings or offer an opinion. This is not an application of science in order to seek greater truths but, instead, to find information, provide a context in which to understand the information, and determine the probative value of the information. Digital forensics uses science to find patterns that are supported by digital evidence, consistent with Cohen's *Fundamental Theorem of Digital Forensic Examination*: "What is inconsistent is not true" (Cohen, 2012).

Although digital forensics generally follows the same six-step forensic process as real-world forensics, the Association of Chief Police Officers (ACPO) has put forward four principles that are particularly relevant to digital evidence (ACPO, 2012):

- ***Principle 1:*** *No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.*
- ***Principle 2:*** *In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*
- ***Principle 3:*** *An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*
- ***Principle 4:*** *The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.*

These principles speak to the fact that those doing digital forensic exams should be expert at their work and perform it with integrity and ethics. The National Institute of Standards and Technology (NIST) addresses the requirement that digital forensics methods and processes be both repeatable and reproducible:

... repeatability is defined as the ability to get the same test results on the same testing environment (same computer, disk, mode of operation, etc.). Reproducibility is defined as the ability to get the same test results on a different testing environment (different PC, hard disk, operator, etc.) (NIST, 2001).

In other words, digital forensics processes should yield the same result when performed multiple times and two DFEs following the same process should be able to obtain the same results.

While the principles of digital forensics might be said to also generically apply to physical world forensics, there are some fundamental differences at the practice level. First, the traditional forensic examiner compares latent evidence found at a crime scene to known samples. For example, a technician finds fingerprints and compares them to a database of fingerprints, looking for a match. The same is true for DNA, blood, bullets, tool marks, tire tracks, shoe prints, hair, typewriters, handwriting, and other forms of physical evidence. Even forensic pathologists compare the signs found in a corpse to known syndromes.

DFEs, however, do not generally conduct the same type of comparing. Instead, DFEs acquire information from a computer, mobile phone, or other digital device, reconstruct a sequence of events that would fit the data, and then attempt to determine whose fingers were on the keyboard at the time of various actions. Indeed, the analysis of a digital device is based upon knowledge of what actions would cause certain traces rather than comparing the traces to a database of actions.[1] This is where science comes into play; a digital forensic examiner is, in essence, creating an experiment to support or refute a theory of what activities occurred. If the experiment contradicts the theory, then the theory is wrong and, possibly, exculpatory evidence has been found; if the experiment supports the theory, however, it only means that the theory is correct insofar as the current set of facts represents the truth (Cohen, 2012). It is because our knowledge of the facts is not perfect that two experts can (properly) disagree on the interpretation of certain digital evidence. As with all forensics examiners that provide expert opinions, our opinions must have a basis in our area of expertise; therefore, we are restricted to providing opinions concerning the state of the data available and the conditions that influence that data.

Second, while the tools of the traditional forensic scientist evolve to become better and more accurate over time, the evidence itself is not in constant flux. Human blood and DNA, for example, have not changed very much in millions of years, although the tools and methods with which to analyze them keep improving

Conversely, both the tools and evidentiary sources of digital forensics are constantly changing. The tools of digital forensics are software and hardware; these are constantly being upgraded with new drivers and software releases. The operating system platforms of the tools – Linux, Mac OS, and Windows – are also frequently updated. In addition, the targets of the examination are also changing, with application software and operating systems frequently being updated and changed with use. In that regard, digital forensics deals with two moving targets.

Third, and perhaps most fundamental, is the different genesis of the forensic sciences. The physical forensic sciences emerged from the relevant sciences; e.g., chemists created procedures for forensic serology and physicians created procedures for forensic pathology. Conversely, computer forensics started in the 1980s with investigations and methodologies developed primarily by law enforcement investigators. While these investigators were very knowledgeable about computer hardware and software, computer forensics did not emerge from the computer science community. The development of computer forensics as a discipline and field of study was very *ad hoc* in the 1980s and 1990s; indeed, there were very few computer forensics examiners that were not in the law enforcement community during that era. The law enforcement community (at least in the U.S.) has had training and professional organizations since the 1990s that are separate from civilian practitioners, and the community even takes specific steps to leave out criminal defense experts. Computer forensics courses in higher education often originated in Criminal Justice programs, further

[1] DFEs do, in fact, use comparative techniques in many circumstances but generally for the purpose of including or excluding materials to be further examined and analyzed. For example, hash values are often used to exclude known operating system files from examination or to find known images of child pornography, malware, or other well-known files. But the comparison in these cases is only to refine or filter the examination and does not replace analysis; lack of hash set detection of malware, for example, does not suggest that malware is not present.

reinforcing the idea that the field was one primarily for law enforcement; indeed, the subject matter did not find its way into Computer Science or Computer Engineering curricula until the very late 1990s and stand-alone degrees in digital forensics did not become widespread until the early 2000s. Even today, computer forensics within the law enforcement community in the U.S. is still primarily practiced by sworn police officers (often on a multi-year duty rotation) rather than civilian professional practitioners.[2]

TESTING DIGITAL EVIDENCE

The *Daubert v. Merrill Dow Pharmaceuticals* ruling (Daubert v. Merril Dow Pharmaceuticals, 1993) spelled out the four-pronged test for the admissibility of expert scientific testimony, further applied to technical experts by *Kumho Tire v. Carmichael* (Kumho Tire v. Carmichael, 1999). The four criteria are whether the procedures and processes that were used to derive the evidence and testimony have:

1. Been tested.
2. Have a known error rate.
3. Been published and subject to peer-review.
4. Been generally accepted by the relevant scientific/technical community.

Many of today's "best practices" in computer forensics are based upon processes and procedures developed by law enforcement practitioners in the 1990s (Forensic Focus, 2010; Henry, 2009; Nelson, Philips & Steuart, 2015; SWGDE, 2006). These old practices are also based upon computer technology from that era. While the procedures may all have solid foundations, they were not based upon published scientific experimentation.

A. Early Dogma of Digital Evidence

Some of the fundamental good practices in computer forensics are:

- Never image (i.e., forensically copy) a running system.
- The destination media for the forensic copy must be sanitized prior to writing the files.
- Hash algorithms are the proof of the integrity of a forensic copy.
- Always use a write-blocker.

Whether these practices make proper sense or not, they have largely not been scientifically tested and validated. Because of the ritual quality of these practices, what might happen if a DFE fails to perform one of these steps? Is it possible that evidence in such an instance might be discarded by an investigator, ignored by a prosecutor, or successfully challenged by opposing counsel solely because the step was skipped? Without testing these guidelines, we do not actually know the true effect of not complying with them. As forensic scientists, it is imperative that we test and understand these guidelines so that we can answer Daubert questions. All of the procedures guiding — and tools employed in — the practice of digital forensics need to stand the test of Daubert scrutiny. For purposes of initial analysis, it is worth looking at the basic policies and procedures listed above.

B. Imaging a Running Computer System

In order to ensure the integrity of digital evidence on a computer, it was common practice in the 1990s through mid-2000s to pull the plug out of the back of the computer immediately upon seizing the system. It is well known that random access memory (RAM) contains usernames, passwords, and other artifacts that might be probative to an investigation. As recently as 10 years ago, many DFEs insisted that imaging RAM

[2] One often-cited reason for the development of this practice is because early computer forensics cases involved images of child sexual assault (i.e., child pornography). While today's cases still largely involve such images, some law enforcement agencies will still not hire civilians as DFEs, as they do for other types of forensics work.

on a running system was a harmful practice. The rationale was that such a step would taint the evidence since the program used to image the memory would reside in memory itself, thus destroying a portion of RAM. Even imaging the hard drive (i.e., physical device) of a running computer was largely frowned upon because of changes that the operating system would make to the data contained within the device during the process, the violation of the "repeatability" principle (since one cannot repeat such a real-time action), and the difficulty in validation by the use of hashing. Eventually, a computer science analysis was employed in order to demonstrate that the imaging software only overwrote a tiny fraction of the RAM and left intact plenty of potential evidence, both incriminating or exculpatory (Nelson, Philips & Steuart, 2015; Casey, 2011). Furthermore, the portion of RAM that is overwritten and the system information, such as Windows registry keys, that is changed when the RAM and disk imaging tools are installed, can be identified. We also know that these changes to RAM and system files do not add or alter user files stored with the physical storage device.

Indeed, we face this very situation with cell phones and other mobile devices. The current state of mobile device forensics requires that the device be in a powered up state during data acquisition in most cases. While we understand that powering on a cell phone, smartphone, or other device alters the state of the device, we also know that the user data most probative to investigations is not modified and, furthermore, that we have no other choice (Kessler and Mislan, 2013; Mislan and Kessler, 2010; Kessler, 2015). This method is an accepted practice based on the best evidence rule.

C. Sanitization of the Destination Media

It has long been a staple of computer forensics practice to sanitize the destination media where the forensic copy, or image files, will be placed. This was a necessary step in a day when a forensic copy of a disk was made directly to another disk with a similar geometry; anything left over from a previous examination or copy operation might be co-mingled with the new information.

Images today, however, are almost invariably made as a set of fully self-contained files with internal integrity controls, such as the use of cyclic redundancy checks (CRCs) (Nelson, Philips & Steuart, 2015; Casey, 2011). In addition, computer forensic examiners frequently make images directly to a networked drive; sanitizing the destination disk is impractical, if not impossible, in that circumstance.

D. The Use and Meaning of Hashes

Cryptographic hashes have long been used to ensure the integrity of files and messages by providing a mathematically strong checksum. Within the computer forensics community, matching hashes have long been the gold standard that a forensic image is a faithful copy of the original data. Hashes have been so important to the process that law enforcement officers since the 1990s have been trained to observe — and testify — that a hash is a "unique identifier" of a file.

The problem with that observation is that it is not, and never was, true. There are a finite number of possible hash values and, theoretically, an infinite number of files. The Message Digest No. 5 (MD5) algorithm, for example, yields a 128-bit hash, meaning that there are 2^{128} possible values. However, $\infty >> 2^{128}$, meaning that a given MD5 hash value does *not* uniquely identify a file; in fact, an infinite number of files can theoretically share a hash value. Thus, training at the time implied a one-to-one relationship between file and hash values without recognizing that while any given file will only have a single MD5 hash value (for example), a given MD5 hash value might apply to multiple files.

This theoretical possibility was shown to be practical as early as 2004 by experiments creating two human-readable files with the same hash value (Wang, Feng, et. al, 2004; Wang and Yu, 2005), causing some practitioners to predict that these *hash collisions* could be fatal to the practice of computer forensics (Burr, 2006); Gutman, Naccache, and Palmer, (2005). By 2004, computer forensics practitioners had spent 15 years telling the court that matching hashes were essential to proving the integrity of the images. If the integrity checking was shown to be faulty, what did that say about the practice?

While hash collisions are still largely a theoretical problem, it remains to be thoroughly tested as to why a *correct* forensic copy might have a different hash than the original (which might be the case if a sector on a disk is near the end of its useful life or after a garbage collection process on a solid state device). Indeed, is it possible that a forensic copy that is not an exact duplicate is sufficient for evidentiary purposes? And lastly, creating two files with the same hash is relatively straightforward when compared to the significantly harder problem of creating a readable file with the same hash value as another, known file.

When a forensic copy of digital media is created, the hash value of each individual file is calculated as well as the hash value of the image itself. Even if a file on the image was overwritten in place with another file of the same size and hash, the hash value of the image file would, by necessity, change. This has been demonstrated in experiments conducted by the first author (Kessler, in press).

E. Use of Write-Blockers

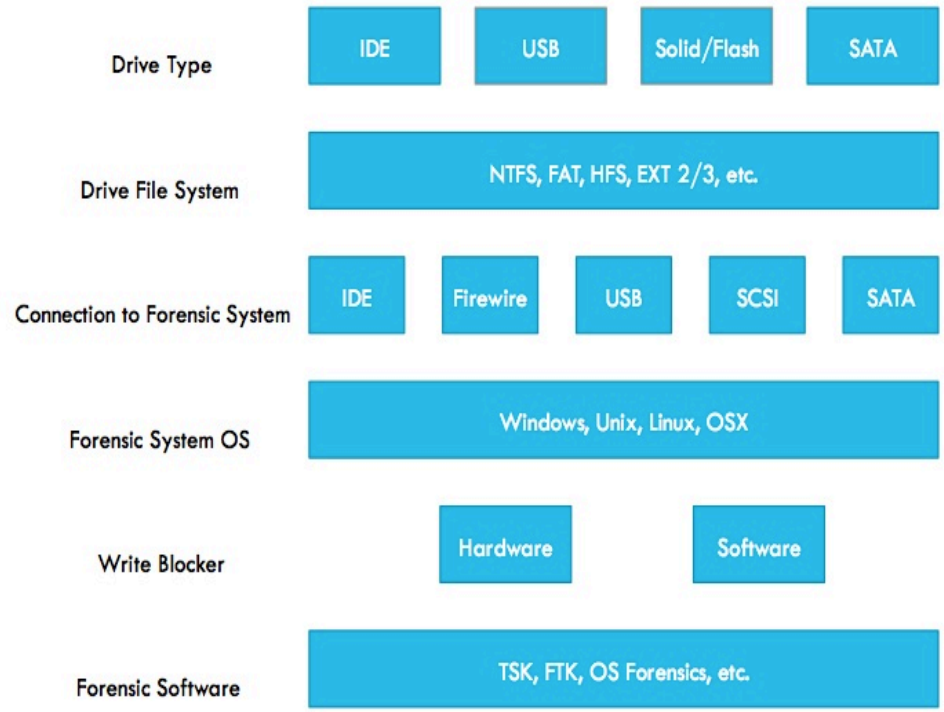
The most fundamental principle of forensics is to maintain the integrity of the source evidence. Thus, a write-blocker must be employed when making a forensic copy to prevent any inadvertent changes to the source hard drive, including adding, deleting, or modifying any information on the media.

Protecting the original data is, indeed, critically important. But where, precisely, does a write-blocker fit into this protection? NIST has tested both hardware and software write-blockers, and confirmed that their tested devices work as they are supposed to; i.e., nothing is written to the target media when attached to a write-blocker (NIST, 2016; NIST, 2014). What has not been tested is to what extent a write-blocker is actually necessary to prevent inadvertent changes.

RESEARCH TESTBED

The authors have initiated a series of experiments in order to identify and examine the practices of computer forensics that are so ingrained as to be ritual and dogma rather than science. The authors are not questioning the need of these practices, per se, but to help establish them based upon the Daubert criteria. We all, as forensics scientists (i.e., practitioners or researchers), must ask the questions, what happens if one of these processes is not followed in a particular case? Is the evidence tainted? If so, what is the significance and extent of any such contamination? Procedurally, should such evidence be challenged by the opposing party on the presumption that the evidence no longer represents the original data? If such a generic objection were raised, how should a judge know whether to sustain or overrule the objection, and how should the party offering such evidence counter the objection and argue for the evidence's inclusion?

Figure 1. Subset of Forensic Imaging Variables (Kessler and Carlton, 2014)



As an example, the authors designed a test framework with which to determine the efficacy of write blockers when creating a forensically correct bit copy, or *image* (Kessler and Carlton, 2014). The test framework was used to identify the universe of possible testing scenarios, including choices of digital media storage technology, file system, interface between the digital media and forensic workstation, forensic workstation operating system, write-blocker type, and the imaging software (not to mention the use of imaging hardware) (Figure 1). The initial tests showed that a thumb drive connected to a Windows forensic workstation without a write blocker had nothing written to it while a disk plugged into a Mac OS X workstation without a write blocker had several system files written to it (Kessler and Carlton, 2014).

The purpose of this experiment was not to suggest that write-blockers are not necessary but to scientifically examine what happens if one is not used. The larger lesson of this small experiment is that the universe of options in digital forensics is huge and a great deal of experimentation will be necessary to complete the catalog of options and results.

Conclusion

Although digital forensics is the youngest of the forensic sciences recognized by the AAFS, it has a quarter-century record as a practice and more than fifteen years as an academic discipline. While the body of digital forensics research literature continues to grow, many of the rituals held over from the earliest days of the field have not been examined or tested as a set of scientific practices. This remains an important activity for future research.

References

ACPO Association of Chief Police Officers (2012). Good practice guide for digital evidence. Version 5. Retrieved February 2, 2016 from http://library.college.police.uk/docs /acpo/digital-evidence-2012.pdf

Burr, W. (2006). Cryptographic hash standards: Where do we go from here? *IEEE Security & Privacy*, vol. 4(2). 88-91.

Casey, E. (2011). *Digital Evidence and Computer Crime*, 3rd ed. Amsterdam: Elsevier.

Casey, E. and Schatz, B. (2011). Conducting digital investigations. *Digital Evidence and Computer Crime*. 3rd ed., pp. 187-225. Amsterdam: Elsevier.

Cohen, F. (2012). Digital Forensic Evidence Examination, 4th ed. Livermore (CA): Fred Cohen & Associates.

Daubert v. Merrill Dow Pharmaceuticals (1993). 509 U.S. 579.

Forensic Focus (2010). Connecting a USB device without a write-blocker. Retrieved February 2, 2016 from http://www.forensicfocus.com/Forums/viewtopic/t=5809/

Gutman, P., Naccache, D. and Palmer, C.C. (2005). When hashes collide, IEEE Security & Privacy, vol. 3(3), 68-71.

Henry, P. (2009). Best practices in digital evidence collection. SANS DFIR. Retrieved February 1, 2016 from http://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/

Kessler, G.C. (in press). The impact of MD5 hash collisions on digital forensic imaging. *Journal of Digital Forensics, Security, and Law*.

Kessler, G.C. (2015). Are mobile device examinations practiced like 'forensics'?, *Digital Evidence and Electronic Signature Law Review*, Issue 12.

Kessler, G.C. and Carlton, G.H. (2014). An analysis of forensic imaging in the absence of write-blockers. *Journal of Digital Forensics, Security and Law*, vol. 9(3), 51-58.

Kessler, G.C. and Mislan, R.P. (2013). Cellular phones. *Encyclopedia of Forensic Sciences*, 2nd ed., J. A. Siegel and P. J. Saukko, Eds. Waltham (MA): Academic Press, 298-302.

Kumho Tire v. Carmichael (1999). 526 U.S. 137.

Mislan, R.P., Casey, E. and Kessler, G.C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation*, vol 6(3-4), 112-124.

Nelson, B., Phillips, A. and Steuart, C. (2015). *Guide to Computer Forensics and Investigations*, 5th ed. Boston: Course Technology.

NIST, National Institute of Standards and Technology (2016). Hardware Write Block Web page, Gaithersburg (MD): U.S. Department of Commerce, Computer Forensics Tool Testing program. Retrieved February 1, 2016 from http://www.cftt.nist.gov/hardware_write_block.htm

NIST, National Institute of Standards and Technology, (2014). Software Write Block Web page, Gaithersburg (MD): U.S. Department of Commerce, Computer Forensics Tool Testing program. Retrieved February 1, 2016 from http://www.cftt.nist.gov/software_write_block.htm

NIST National Institute of Standards and Technology (2001). General Test Methodology for Computer Forensics Tools. Version 1.9. Gaithersburg (MD): U.S. Department of Commerce. Retrieved February 1, 2016 from http://www.cftt.nist.gov/Test Methodology 7.doc

Palmer, G. (2001). "A road map for digital forensic research," DTR-T001-01 Technical Report. Utica (NY): *Digital Forensics Research Workshop (DFRWS)*. http://www.dfrws.org/2001/dfrws-rm-final.pdf

Petherick, W A. Turvey, B E. Ferguson, C E (2010). *Forensic Criminology*. London: Elsevier Academic Press. Retrieved February 2, 2016, from http://aboutforensics.co.uk/edmond-locard

SWGDE Scientific Working Group on Digital Evidence (2006). Best practices for computer forensics. Version 2.1. Retrieved February 1, 2016 from http://www.oas.org/juridico/spanish/cyb_best_pract.pdf

Wang, X., Feng, D., Lai, X. and Yu, H. (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. *International Association for Cryptologic Research*. Retrieved February 1, 2016 from http://eprint.iacr.org/2004/199.pdf

Wang, X. Y. and Yu, H. B. (2005). How to break MD5 and other hash functions. *Advances in Cryptology–Eurocrypt*, 19-35.