THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 11 | Number 2 Article 11

2016

Verification of Recovered Digital Evidence on the Amazon Kindle

Marcus Thompson
Purdue University

Raymond Hansen
Purdue University

Recommended Citation

Thompson, Marcus and Hansen, Raymond (2016) "Verification of Recovered Digital Evidence on the Amazon Kindle," *Journal of Digital Forensics, Security and Law*: Vol. 11 : No. 2 , Article 11.
DOI: https://doi.org/10.15394/jdfsl.2016.1386
Available at: https://commons.erau.edu/jdfsl/vol11/iss2/11

VERIFICATION OF RECOVERED DIGITAL EVIDENCE ON THE AMAZON KINDLE

Marcus Thompson, Raymond Hansen
Purdue University
Computer and Information Technology
West Lafayette, Indiana, 47907
marc@purdue.edu, hansenr@purdue.edu

ABSTRACT

The Amazon Kindle is a popular e-book reader. This popularity will lead criminals to use the Kindle as an accessory to their crime. Very few Kindle publications in the digital forensics domain exist at the time of this writing. Various blogs on the Internet currently provide some of the foundation for Kindle forensics. For this research each fifth generation Kindle was populated with various types of files a typical user may introduce using one method, the USB interface. The Kindle was forensically imaged with AccessData's Forensic Toolkit Imager before and after each Kindle was populated. Each file was deleted through the USB interface. Files were retrieved and recovered through the USB interface before and after file deletion. These two sets of files were compared to the original set of files. All files retrieved before deletion matched their original counterpart. Not all files recovered after deletion matched their original counterpart. These steps and procedures followed a similar adaptation of the NIST General Test Methodology for Computer Forensic Tools developed by Leshney (2008) for virtual machines

Keywords: cyber forensics, amazon kindle, verification, methodology, FAT32

1. INTRODUCTION

According to Garfinkel (2010), digital forensics is about 40 years old with 2007 ending the "Golden Age for digital forensics" (p. S66). The Golden Age included few operating systems, few file formats of investigative interest, and single device investigations. Daniel and Daniel (2011) declare the digital forensics field was created while personal computers were becoming commonplace during the 1980s with the establishment of the Federal Bureau of Investigation's Magnetic Media Program in 1984. Investigations only began using forensic tools such as SafeBack and DIBS to collect unaltered digital evidence in the 1990s (Casey, 2004). Garfinkel (2010) foresees a crisis in the digital forensics community that is in part due to increased use of embedded flash memory, expansion of interest in other file formats, and cross-device analysis (p. S66). In a previous paper from Garfinkel (2006), he states, "[t]oday's forensic examiners have become the victims of their own success. Digital storage devices such as hard drives and flash memory are such valuable sources of information that they are now routinely seized in many investigations" (p. S71). These devices should be seized, but investigators have begun to feel the impact of this crisis as they seize additional digital evidence. This includes seizing smart phones and other digital devices, such as the Amazon Kindle.

The Amazon Kindle synchronizes across a user's devices: Kindle, mobile phone, and computer. This could assist the investigator as multiple sources could point to the user or device as the originator of certain evidence, but it requires correlation of large amounts of evidence from the investigator, which increases "system and human processing time associated with data analysis" with current methods (Beebe & Clark, 2005, 3).

The digital forensics community is very familiar with iPod forensics and mobile device forensics. This is due to some using iPods in manners other than originally intended by the manufacturer. Users can boot into Windows or Linux using their iPods (Marsico & Rogers, 2005). Like many mobile devices, the Kindle contains a Subscriber Identity Module (SIM) card and has 3G network connectivity. In some respects it should be treated as a mobile device, like an iPod.

Investigators know "[c]ell phones can tell you a lot about a person: likes, dislikes, vices, habits, secret fetishes, [and] secret personalities..." (Slovenski, 2012). Many cell phones can outperform computers of yesteryear, facilitating increased complexity of features and functions that will store more data about its user (Daniel & Daniel, 2011). The ability for users to create and store collections may contribute to behavior profiling. Time to Read may be a factor in user attribution. The Amazon Kindle has increased functionality like the iPod or other mobile devices. A user can read books, listen to music, search the Internet, play games, and share content with social media web sites and other users.

Unexpected functionality is a forensic challenge for investigators. Major feature differences between iPods, mobile devices, and the Kindle are narrowing. Mobile device forensic methods should be taken into consideration when encountering these devices. Forensic artifacts remain on computers where iPods have been connected. Investigators should be conscious of these facts to conduct a thorough investigation because many of these ideas may apply to the Kindle as well. Investigators also need to be aware of the differences between operating systems. For example, Windows forensics does not match one to one with Linux forensics (Craiger, 2005). This will affect the appearance of Kindle artifacts on each operating system and other devices. Investigators can extrapolate what they have learned about previous devices such as the iPod, mobile devices, and operating systems to apply forensic practices with the Amazon Kindle.

1.1 The Growing Kindle Problem

The Kindle line of products has extended functionality as it can play music or games, browse the web, and store two to four gigabytes of data. It supports conversion of personal documents through email for the file extensions in Table 1 (Amazon.com, 2011). It also has native support for Portable Document Format (PDF) files and can store any other file much like other storage devices.

Table 1
Supported Formats for Personal Document Conversion

Format	**File Extension**
Microsoft Word Documents	.doc, .docx
Text and Rich Text Format	.txt, .rtf
Structured HyperText Markup Language	.html, .htm
Joint Photographic Expert Group	.jpeg, .jpg
Graphics Interchange Format	.gif
Portable Network Graphics	.png
Bitmap Images	.bmp
Compressed Archive	.zip

The Kindle Development Kit (KDK) is in beta testing providing "rich APIs, tools, and documentation" to allow United States users to develop their own active content, such as games, calendars, or photo galleries (“Kindle Development,” n.d.; “Kindle Active Content,” n.d.). This will give the Kindle even more functionality in the future, narrowing the differences between an e-reader and other devices such as the iPod Touch, PDAs, and mobile devices. According to Marsico and Rogers (2005), as features are added to iPods “to make life more convenient for its users, some decide to use these conveniences to further their criminal trade craft.” These assertions lead the authors to conclude it is a matter of time before Kindles are used as a means of criminal activity and become valuable sources of digital evidence. Without research, documentation and testing of the forensic process for Kindles, examiners may “overlook areas of evidence or may not know how to analyze the information” from a Kindle (Leshney, 2008).

1.2 Significance of the Problem

Jeff Bezos, the founder of Amazon, reports that the Kindle is the bestselling, most wished for, and most gifted product on Amazon.com (Amazon.com, June 15, 2010). He also reported that Kindle books outsold paper books for the first time on Christmas Day 2009 (Amazon.com, December 26, 2009). In addition to over 1.5 million books, hundreds of newspapers, magazines, blogs, and another two million out-of-copyright e-books are available for download. Furthermore, a user can download content in over 100 countries or territories and then synchronize it to other Kindle applications using Amazon’s Whispernet via AT&T’s 3G cellular networks (“Kindle wireless reading device, Wi-Fi,” n.d.).

Research of the Kindle is important for law enforcement investigators who have seized a Kindle and then wish to forensically process the potential digital evidence. Books and other files contained in the Kindle can be considered associative evidence, which can give insight to a suspect, victim, or person of interest and can help build a case in conjunction with other evidence (Horrocks, Coulson, & Walsh, 1998). Since the Kindle can contain more than 3500 books, hundreds of .mp3s, or other files, it may reveal many characteristics of its user(s) (“Kindle wireless reading device, Wi-Fi,” n.d.).

The purpose of this research was to determine the validity of the forensic process on each fifth generation Kindle. Because digital forensics of Kindles is a new research area, other digital forensic processes were considered in order to create a methodology for examining these devices. The National Institute of Standards and Technology has created standards for mobile device forensics. Combined with computers, these devices create the field of digital forensics (Bishop, Hay, & Nance, 2009). This expansion of included devices into the field encompasses many electronics that store data, including the Amazon Kindle. Investigators can reference older devices to learn about and prepare for new sources of evidence like the Amazon Kindle. This research was limited to one technique. The Universal Serial Bus (USB) port was used for each Kindle to access the user partition. These techniques followed standard forensic considerations. Section two references current research on the Kindle platform; section three details the methodology of this study; section four shows the results; and section five highlights our conclusions and directions for future work.

2. LITERATURE REVIEW

2.1 Kindle History

The Amazon Kindle was introduced to the consumer market on November 19, 2007. The Kindle product line includes a tablet family based on the Android operating system. All other Kindle devices have a form of embedded Linux.

The first generation Kindle was introduced as a six-inch display e-reader with the capability of wirelessly downloading content from a selection of over 90,000 books, 250 blogs, and many newspapers (Amazon.com, November 19, 2007; February 9, 2009). Seven years later the Amazon Kindle has entered its eighth generation that includes an expanded content and feature set. Millions of books and hundreds of newspapers and magazines are accessible from each of the eight models: the Kindle Paperwhite with Special Offers (SO), the 3G Kindle Paperwhite with SO, the Kindle 7, and the Kindle 7 with SO, the Kindle Voyage with SO, the 3G Kindle Voyage with SO, the Kindle Oasis with SO, and the 3G Kindle Oasis with SO (Amazon.com, September 6, 2012; Amazon.com, September 6, 2012; Amazon.com, October 25, 2012; Amazon.com, April 28, 2016).

On Christmas Day, 2009, Kindle book purchases surpassed physical book purchases (Amazon.com, December 26, 2009). On December 26, 2009, Amazon announced the Kindle had become the most gifted item in the company's history (Amazon.com, December 26, 2009). In July 2010 Kindle books outsold hardcover books and then paperback books six months later (Amazon.com, May 19, 2011). In April 2011 Kindle books outsold the collective sum of hardcover and paperback books at a rate of 105 to 100 (Amazon.com, May 19, 2011). A timeline of major events in the Kindle's history is shown in Figure 1.

Notable features added since the inception of the Kindle are the experimental web browser, Whispersync, social networking, bookmarks, annotations, highlights, Collections, password protection, native PDF reader, SO, Time to Read, and Parental Controls (Amazon.com, September 6, 2012). Amazon added the ability for the user to access the Kindle's experimental web browser to search Wikipedia through Whispernet (Amazon.com, November 19, 2007). The Kindle featured user added bookmarks, annotations, and highlights to books (Amazon.com, 2007). Amazon's Whispersync technology was introduced the ability to synchronize bookmarks and furthest page read across multiple Kindle devices and future mobile devices (Amazon.com, February 9, 2009; "Wireless, Whispernet," n.d.). Social networks could be connected and associated with the Kindle device allowing the user to post content directly to Facebook or Twitter ("Kindle wireless reading device, free 3G," n.d.). Collections allowed users' books to be able to be organized into categories ("Kindle wireless reading device, free 3G," n.d.); a user can place their books in zero or multiple collections. Users were also given the ability to lock their Kindle with a password ("Kindle wireless reading device, free 3G," n.d.). Adobe Reader Mobile technology was added to natively read more structurally complex .pdf documents (Amazon.com, May 6, 2009). SO places ads and other sponsored screensavers on the home screen and on the Kindle screensaver (Amazon.com, April 11, 2011). Time to Read calculates the user's reading speed (Amazon.com, September 6, 2012). The Kindle Store, archived content, and browser access can be limited with Parental Controls (Amazon.com, September 6, 2012).

2.2 Kindle Content Sources

Content is not limited to the Kindle Store. The Kindle Personal Documents Service allows users to add personal documents to their device, Kindle reading application, or Kindle Library using their Send-to-Kindle email address, the Send to Kindle application, or their computer via USB ("Transferring, downloading," n.d.). This research only studied the USB interface.

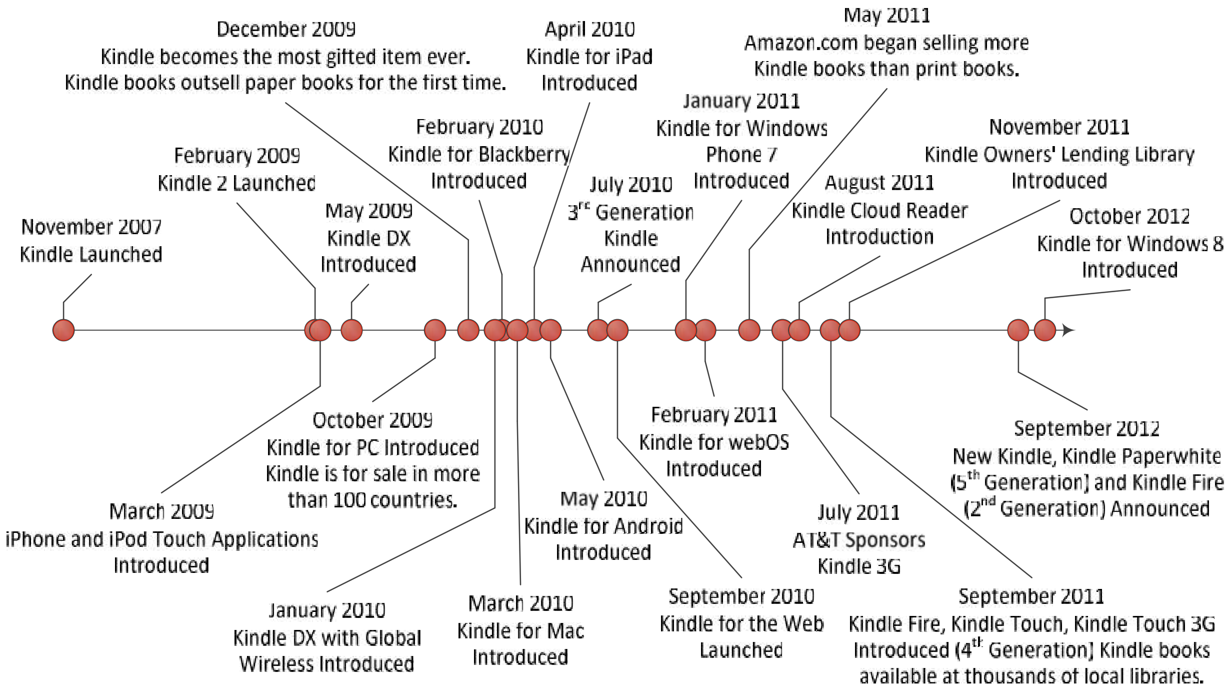
November 2007
Kindle Launched
February 2009
Kindle 2 Launched
March 2009
iPhone and iPod Touch Applications Introduced
May 2009
Kindle DX Introduced
October 2009
Kindle for PC Introduced
Kindle is for sale in more than 100 countries.
December 2009
Kindle becomes the most gifted item ever.
Kindle books outsell paper books for the first time.
January 2010
Kindle DX with Global Wireless Introduced
February 2010
Kindle for Blackberry Introduced
March 2010
Kindle for Mac Introduced
April 2010
Kindle for iPad Introduced
May 2010
Kindle for Android Introduced
July 2010
3rd Generation Kindle Announced
September 2010
Kindle for the Web Launched
January 2011
Kindle for Windows Phone 7 Introduced
February 2011
Kindle for webOS Introduced
May 2011
Amazon.com began selling more Kindle books than print books.
July 2011
AT&T Sponsors Kindle 3G
August 2011
Kindle Cloud Reader Introduction
September 2011
Kindle Fire, Kindle Touch, Kindle Touch 3G Introduced (4th Generation) Kindle books available at thousands of local libraries.
November 2011
Kindle Owners' Lending Library Introduced
September 2012
New Kindle, Kindle Paperwhite (5th Generation) and Kindle Fire (2nd Generation) Announced
October 2012
Kindle for Windows 8 Introduced

Figure 1. Major Events in the History of the Amazon Kindle (Amazon.com Timeline, 2012)

Transferring content via USB is similar to copying files to a flash drive as the Kindle is connected to a computer as a mass storage device. After connecting the Kindle to a computer, it changes to USB drive mode and disables wireless service ("Kindle Personal," n.d.). If the user wishes to transfer content via USB and manage it on their device, they must transfer it into the correct folder ("Kindle Personal," n.d.). According to a Kindle Keyboard support web site the "documents" folder supports Kindle (.azw, .azw1, .azw3), text (.txt), and Mobipocket (.mobi,.prc) files ("Transferring, downloading," n.d.). The "audible" folder supports audio book (.aa, .aax) files ("Transferring, downloading," n.d.). The "music" folder supports .mp3 files ("Transferring, downloading," n.d.). These supported files are shown in Figure 2 in addition to other sources of Kindle content.

Content can be deleted from the Kindle through a few methods. The user can delete content using their Kindle. When the Kindle is confirming the deletion, a message box appears stating the selection will be permanently deleted. This removes it from the device, but it remains in their Kindle Library as archived content and can be replaced. All content including archived content can be deleted from the Kindle in the "Manage Your Kindle" section on Amazon.com of the user's account. The Kindle can be reset to factory defaults within the settings of the device. A computer host can format the Kindle or delete files when the Kindle is USB drive mode. This research is limited to deleting files through the computer host while the Kindle is in USB drive mode.

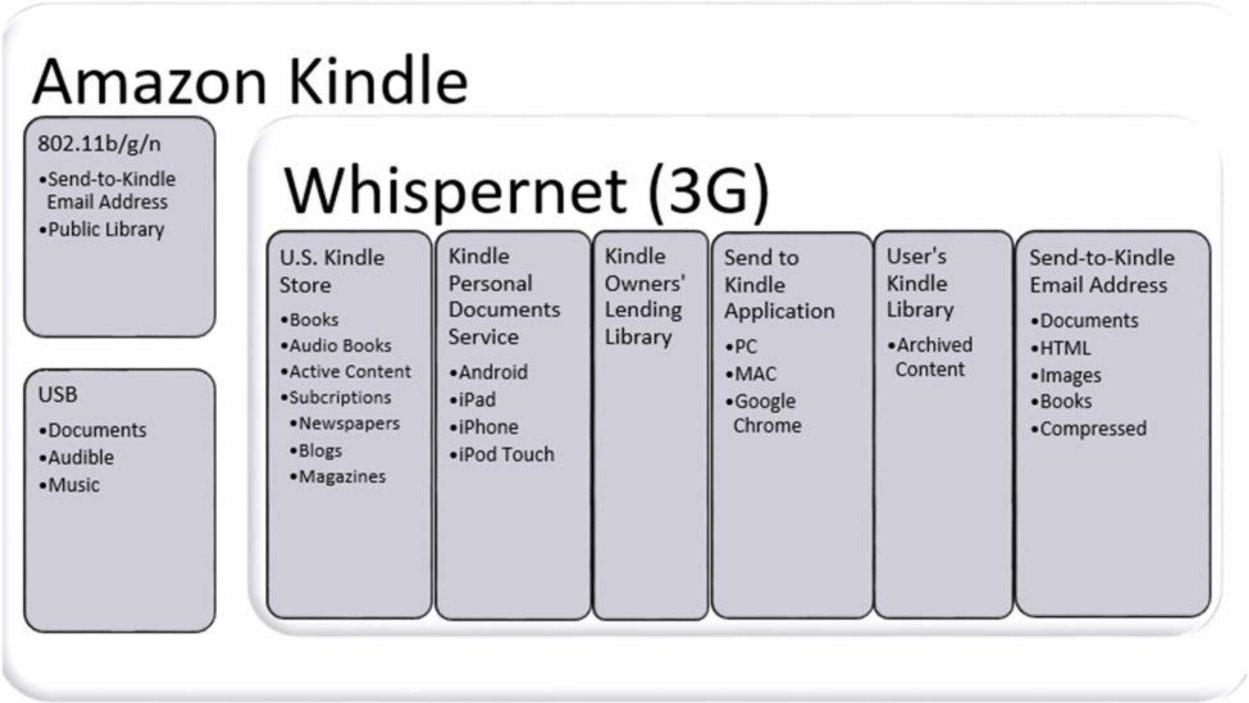

Figure 2. Amazon Kindle Supported Content Sources and Recognized File Types

2.3 Digital Forensics Methodologies

The General Test Methodology for Computer Forensic Tools was published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce in 2001 to evaluate forensic software tools to provide investigators a measure of quality, specifically for the judicial process (National Institute of Standards and Technology, 2001). It includes seven stages in its approach: establish categories of forensic requirements, identify requirements for a specific category, develop test assertions based on requirements, develop test code for assertions, identify relevant test cases, develop testing procedures and method, and report test results (National Institute of Standards and Technology, 2001). Recorded test results are required to be repeatable and reproducible (National Institute of Standards and Technology, 2001).

Some research has been performed using these methods. Leshney (2008) adapted this methodology for his research on digital evidence on virtual machines. Due to the exploratory nature of his work, he did not include all stages of NIST's test methodology and redefined some (Leshney, 2008). Five of the seven stages were included: establish categories of forensic requirements, identify test assertions/variables, develop test cases, develop testing procedures and methods, and report results. Leshney identified three categories of forensic requirements from Burchett: file/directory recovery, file/directory analysis, and log analysis. Leshney divided his research into two phases. In the first phase he identified, recovered, and analyzed evidence, and in the second phase he performed log analysis. This research is based on Leshney's adaptation of the test methodology.

3. METHODOLOGY

This chapter explains the research methodology based on Leshney's research on virtual machines. The sample set included 210 natively supported files for each Kindle. MD5 hashes were calculated throughout the experiment and were compared. The comparison is described in terms of successes and failures and creates the results of this research.

3.1 Research Approach

This was an exploratory study to analyze the effect of individual Amazon Kindles on a known file set during the forensic process. The research followed an experimental design with the Kindle model and file type as the independent variables and the file hashes as the dependent variable. The research included each model of the fifth generation: Kindle Paperwhite 3G, Kindle Paperwhite 3G with SO, Kindle Paperwhite, Kindle Paperwhite with SO, Kindle 5, Kindle 5 with SO, Kindle Keyboard 3G, and Kindle Keyboard 3G with SO. Each model was newly purchased from Amazon.com. The Kindles were populated with a known sample file set with known MD5 hashes as shown in the next section. This process was automated with a script through Windows PowerShell 2.0. The sample file set was acquired from each Kindle for analysis through one technique using the USB interface. The retrieved files were hashed. The sample was deleted from each Kindle through one process: deletion through the computer host in Windows using a PowerShell script. Data was again acquired through the USB interface. The files were hashed a second time resulting in three sets of file hashes. These sets of file hashes were compared and analyzed and comprised the results of this research.

3.2 Sample

The sample included 30 files of each type from each source shown in Table 2. These file types are listed as natively supported in Amazon documentation.

3.3 Forensic Method

The methodology for this study was based on Leshney's (2008) adaptation of the National Institute for Standards and Technology General Test Methodology for Computer Forensic Tools. Leshney's adaptation includes five stages: establish categories of forensic requirements, identify test assertions/variables, develop test cases, develop testing procedures and methods, and report results. Two of the three categories identified by Leshney were considered: file/directory recovery and file/directory analysis (2008). The third category of log analysis was foregone as virtual machines produce vast user accessible logs unlike the Kindle.

3.2.1 Test Cases

Test assertions were developed based on two potential actions a user could perform through the USB interface: adding content and removing content. Amazon supports user added documents, audible books, and music through the USB interface. A user can delete these files through several processes. The USB interface in Windows PowerShell was the only medium used to perform deletion.

The purpose of the first test was to determine differences between files retrieved and the original files. The purpose of the second test was to determine differences between deleted files and the original files. Table 2 displays how many files of each extension were added to each Kindle.

Table 2:
File Types and Count Added to Devices

Physical Medium	File Source	Document Type	File Count
USB	Windows Explorer	.azw	30
		.azw2	30
		.awz3	30
		.txt	30
		.mobi	30
		.prc	30
		.pdf	30

3.2.2 Apparatus and Testing Procedures

The forensic analysis of the Amazon Kindle flash memory can be conducted through a few physical techniques. This research was limited to one technique to access the Kindle flash memory, the USB interface. The technique in this study duplicated the Kindle flash memory with AccessData's Forensic Toolkit (FTK) Imager 3.1.0.1514 using a Tableau T8 Forensic USB Bridge with firmware update 6.87 to prevent tampering of evidence. The duplicates were analyzed using AccessData's Forensic Toolkit 5.1 software on Windows 7 Service Pack 1. These processes followed forensic practices: "data integrity, authentication, reproducibility, non-interference and the ability of proposed techniques to comply with federal minimization requirements" (Garfinkel, 2010, S65).

In phase I, the MD5 hash of each file in the sample was calculated using FTK. This was completed by selecting "Add/Remove..." in the menu bar under "Evidence." The "Add" button was clicked once the "Manage Evidence" window appeared. The source evidence type selected was "Contents of a Directory." The folder containing the sample was chosen. The resulting MD5 hash of each file calculated by FTK. These values were exported from FTK by right-clicking in the file list pane, selecting "Copy Special...," selecting the "All" radio button and clicking "OK." This procedure copied the file list values to the Windows clipboard. The values were pasted into Microsoft Excel for ease of comparison of phase II and phase III results. To conclude phase I each Kindle was imaged in its factory state using a Tableau write blocker and FTK Imager on Windows 7. The Kindles were modified in one way in order for them to mount as an accessible drive in Windows. Each Kindle Paperwhite required a user language be selected before it was able to be mounted and imaged. The research design for phase I is shown visually in Figure 3.

In phase II, each Kindle was populated with files listed in Table 2 through USB with a Windows PowerShell script. There were no failures during the execution of the script, producing no output from the catch block. There was a failure produced in the original procedures of this research. Audio files were included in the sample in the original protocol. The script pointed the copy procedure for those files to the Audio and Music folders. The Kindle Paperwhite does not support audio books or music files and does not include Audio or Music directories. The result of the script was a creation of a flat file of the Audio and Music directory and not the intended file structure. To correct this the research protocol was altered by removing the audio files from the sample. Three Kindles having the original sample were restored to factory defaults. Once each Kindle was populated without audio files, they were imaged a second time with the same steps as in phase I. The MD5 hash of the original files was compared to the MD5 hash of the files retrieved from the second image. The research design for phase II is shown visually in Figure 4.

Phase III deleted all 210 files placed on each Kindle during phase I through the USB interface using a Windows PowerShell script while not deleting any files or directories included in their factory state. There were no failures during the execution of the script, producing no output from the catch block. The script was modified after it was realized the script deleted the Kindle user guide and dictionary. These extraneous deletions did not affect the experiment. Each Kindle was imaged a third and final time with the same steps as in phase I and phase II. The image was opened and processed in FTK in the same manner as phase II. Each file was attempted to be recovered through AccessData's Forensic Toolkit software. The MD5 hashes were exported to Microsoft Excel with the same steps in phase I and phase II. The MD5 hash of the original files was compared to the MD5 hash of the deleted files. The research design for phase III is shown visually in Figure 5.

Results were gathered through the research design process as shown in Figure 4 and Figure 5. The comparisons between file sets created the results for phase II and phase III. The MD5 hashes of the original files were compared to the files retrieved from each Kindle in phase II. The MD5 hashes of the original files were compared to the recovered files from each Kindle in phase III. Matching MD5 hashes were considered a success while conflicting hashes were considered a failure. Missing MD5 hashes in phase III from recovered or non-recovered files were also considered a failure.

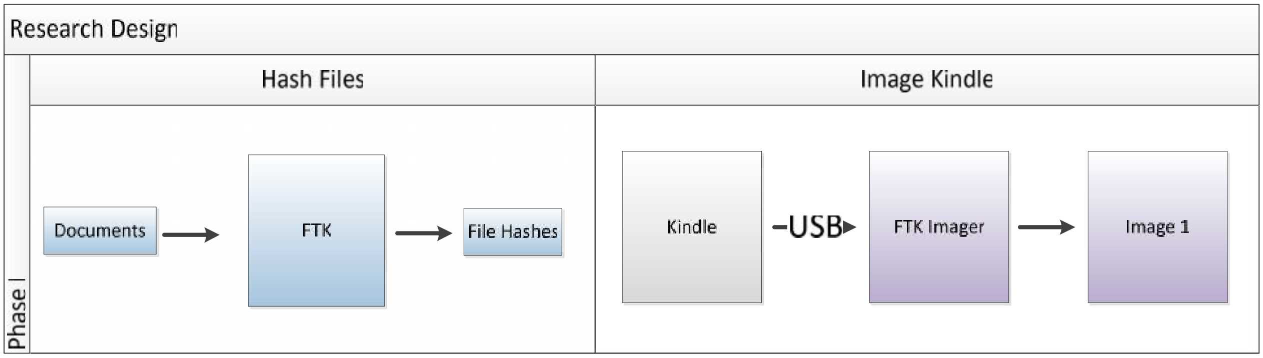

Figure 3. Research Design for Phase I

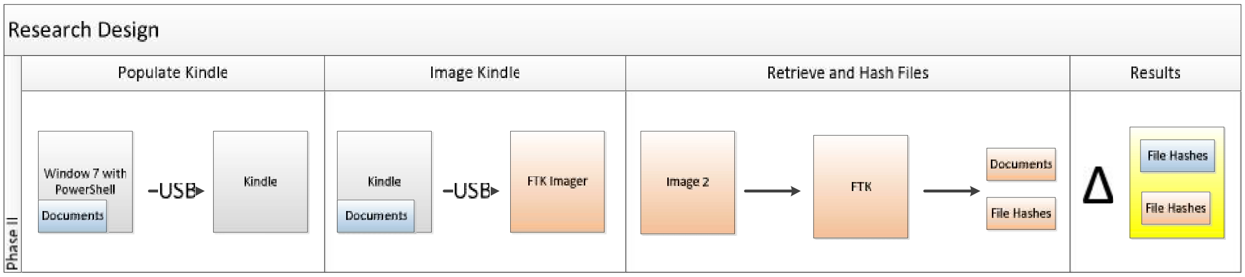

Figure 4. Research Design for Phase II

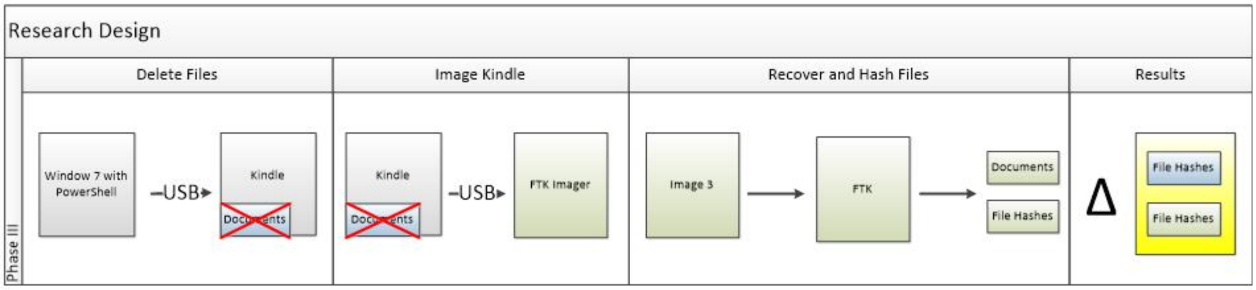

Figure ***5***. Research Design for Phase III

4. RESULTS

This chapter presents the data of the procedures executed in chapter three. It summarizes the raw results, outcomes, and trends. Interpretation, analysis, conclusions, and recommendations are discussed in chapter five.

4.1 Hypothesis One

Each Kindle image was opened and processed in FTK to calculate the MD5 hashes of the sample. The hashes were exported to Microsoft Excel in the same manner as in phase I. The hashes from the original files and the retrieved files were compared. Every MD5 hash of each file retrieved from each Kindle matched the MD5 hash of its original counterpart. The first hypothesis of this study: "There is no difference between the MD5 hashes of the original files and the files retrieved through the forensic process from the Amazon Kindle." In this research, there were no missing MD5 hashes or mismatched MD5 hashes, supporting the first hypothesis. Phase II had a 100% success rate as shown in Table 3.

Table 3
Success Rate in Phase II

Model	**Number of Failures**	**Success Rate**
Kindle Keyboard w/o SO	0	100%
Kindle Keyboard w/ SO	0	100%
Kindle Paperwhite w/ SO	0	100%
Kindle Paperwhite 3G	0	100%
Kindle Paperwhite 3G w/ SO	0	100%
Kindle Paperwhite	0	100%
Kindle 5	0	100%
Kindle 5 w/ SO	0	100%

4.2 Hypothesis Two

The second hypothesis of this study: "There is no difference between the MD5 hashes of the original files and the deleted files retrieved through the forensic process from the Amazon Kindle." 292 of 1680 MD5 hashes in Phase III did not match the original file or was missing altogether, failing to support the second hypothesis of this research. Phase III had an 82.62% success rate. The MD5 hash of B000JML3IW_EBOK.azw was mismatched or missing in every Kindle except the Kindle 5 with SO. The MD5 hash of B000JML7EC_EBOK.azw was mismatched on three Kindle Paperwhites. 25344-h.prc, 26491-h.prc, 29239-h.prc, and 6130-h.prc had mismatched MD5 hashes on every Kindle. An additional ten MD5 hashes of .prc files were mismatched on the Kindle 5. Every MD5 hash of .txt files were mismatched on every Kindle.

A summary of failures per Kindle is shown in Table 4. A summary of failures per file type is shown in Table 5.

Table 4
Success Rate in Phase II by Kindle Model

Model	**Number of Failures**	**Success Rate**
Kindle Keyboard w/o SO	35	83.33%
Kindle Keyboard w/ SO	35	83.33%
Kindle Paperwhite w/ SO	36	82.86%
Kindle Paperwhite 3G	36	82.86%
Kindle Paperwhite 3G w/ SO	36	82.86%
Kindle Paperwhite	35	83.33%
Kindle 5	45	21.43%
Kindle 5 w/ SO	34	83.81%

Table 5
Success Rate in Phase III by File Type

File Extension	**Number of Failures**	**Success Rate**
.azw	10	95.83%
.azw2	0	100%
.azw3	0	100%
.mobi	0	100%
.pdf	0	100%
.prc	42	82.5%
.txt	240	0%

5. CONCLUSIONS

This chapter interprets and draws conclusions from the results as shown in chapter four. Recommendations follow for future related research.

5.1 Research Question

The research question of this study was "Can files from the Amazon Kindle be forensically acquired reliably?" The results of phase II were expected as such. No failures occurred during this phase. The operating system or file system of each Kindle had no effect on files copied to them. Files from the Amazon Kindle can be acquired reliably per procedures in phase II. The results of phase III contained unexpected missing and mismatched MD5 hashes showing that deleted files cannot be forensically acquired reliably from the Amazon Kindle using the procedures of this study. The failures of phase III do not appear to be random and are fairly consistent among each Kindle.

The failures could be an indication of how the Kindle file system and operating system handles the process of deletion. Unexpected changes appeared to have occurred to directory entries after deletion of some files. The file content of the .prc and .txt files on the image created in phase II and the image in phase III were compared. The file content in phase III remained intact in their original phase II sectors. Analysis of the phase II image shows the designated starting cluster in phase III of .prc and .txt files points to preexisting data, meaning new data was not written to the starting clusters of the directory entries in phase III. The directory entry and file allocation table (FAT) may have changed during or after the deletion process. It is expected for the FAT file system to change the allocation status of the directory entry of a file or directory and its entry in the FAT when said file or directory is deleted. Carrier (2005) states:

"When a file is deleted, the first byte of the directory entry is set to 0xe5. Windows does not change any other values in the directory entry but other OSes might. The clusters that were allocated for the file are unallocated by setting their corresponding entries in the FAT structure to 0. Fortunately, Windows keeps the starting cluster of the cluster chain in the directory entry so some file recovery can be performed until the clusters are allocated to new files and overwritten" (p. 172).

It is not expected for the FAT file system to change the starting cluster address of the in the directory entry of a file as well as the FAT when deleting said file. Carrier (2005) later states, "[T]he metadata associated with a file name will not become out of sync after the file is deleted. The metadata associated with an unallocated file name will be accurate until both are overwritten" (p. 177). Contrary to this statement, this seems to have occurred for each .prc and .txt file, which may fall under the caveat Carrier mentioned on page 172: a non-Windows operating system might change other directory entry values. This might explain why even though the files on each Kindle were deleted in a Windows environment, the Kindle operating system may have made further changes upon being unmounted from Windows.

The failures among the .azw files appear to be caused by a similar processes. On the Kindle Keyboard with SO, B000JML3IW_EBOK.azw has 846 bytes prepended to the where the file once began. Unexpectedly, the 846 bytes appears to contain a copy of the user preferences file, reader.pref. On each other Kindle, the sectors where B000JML3IW_EBOK.azw once resided have been written to with new data. On the Kindle Paperwhite with SO, B000JML7EC_EBOK.azw remains mostly intact. Most of the first 200 bytes have been erased. On the Kindle Paperwhite 3G, B000JML7EC_EBOK.azw has been replaced with new data. This same data was located on the phase II image in unallocated space as designated by FTK. The original file content of the .azw files with failed MD5 hashes do not exist elsewhere on the disk. The failures occur at the beginning and ending sectors of the Kindle. No failures occurred in the middle of the sample. Only MD5 hashes of .azw files at the beginning sectors and .prc and .txt files at the ending sectors failed. This shows the Kindle operating system and file system may not have been consistent in how it deleted files.

The results of the research produced six files with a blank hash field. The FTK User Guide (2013) explains "a blank hash field appears for unallocated space files, the same as if the files had not been hashed at all" (p. 102).

More research was conducted after the experiment was completed to investigate the unexpected results further. The author contacted AccessData regarding the possible directory entry changes, conjecturing a possible bug in FTK. AccessData referred the author to their online forums and their sales department for training. Four additional follow up tests were held to determine the cause of the failed MD5 hashes. Possible causes hypothesized included the process of garbage collection on flash based storage, wear leveling processes, the Kindle file system, the Kindle operating system, and the Windows operating system. The Kindle underwent a format through Windows 7 and a factory reset before each test.

In the first test the original experiment was replicated in all aspects on the Kindle Paperwhite 3G with the exception of the order of the files copied to the Kindle. The PowerShell script was modified to copy .azw2 files first and .pdf last. Like the .azw files in the original experiment on the Kindle Paperwhite 3G, the first .azw2 MD5 hash was missing. The last 20 .pdf files MD5 hashes did not match the original files. This behavior was similar to the original experiment where the 30 .txt files, the last files in the sample, had mismatched MD5 hashes. The failures of this follow up test seemed to have the same location and cause of the failures in the original experiment showing the Kindle file system may not be responsible for the changes.

The second test replicated the original experiment in all aspects on the Kindle Paperwhite 3G with the exception of the method of deletion. Each file on the Kindle was individually deleted within the Kindle device rather than through Windows PowerShell. All files recovered from this test matched the original files showing the

Windows operating system is likely responsible for the mismatched MD5 hashes in the original experiment.

A third test replicated the original experiment in all aspects on the Kindle Paperwhite 3G with the alteration of the operating system to Windows XP Service Pack 3 rather than Windows 7. As previously noted, Carrier (2005) stated "Windows does not change any other values in the directory entry" (p. 172). The original protocol of the experiment required Windows 7. The most recent version of the Windows operating system at the time Carrier published his book was Windows XP. The results of this test were the same of the original experiment showing the Windows 7 deletion processes are similar to Windows XP.

A fourth test replicated the original experiment in all aspects on the Kindle Paperwhite 3G with the alteration of the operating system to Windows 8 rather than Windows 7. The results of this test were the same of the original experiment showing the Windows 7 deletion processes are similar to Windows 8.

Directory entries were viewed in DiskExplorer for FAT V4.32 to easily analyze the images from the original experiment and the additional tests at the hexadecimal level. The failed .prc and .txt files were unable to be manually located in the deletion image in phase III or the populated image from phase II. Despite the success of the alternate method of deletion test, the directory entries for all files were not located in the populated image and the deletion image. This shows more research must be conducted in order to understand directory entries on the Amazon Kindle.

5.2 Significance

This research is important for the digital forensics community. The results of phase II confirm standard forensic considerations and practices are applicable to the Amazon Kindle. Researchers and practitioners should be aware of the phase III failure rate of deleted file acquisition from the Amazon Kindle and should not assume a zero failure rate in any future research or investigation until procedures show repeatable successful results. The results of phase III produce many unanswered questions regarding directory entries during file deletion using a Windows environment. The follow up tests show that the forensic process may be reliable if the user deletes files without using a Windows operating system. There is no method to determine what environment or process was used to delete a file resulting in the conclusion deleted files cannot be reliably recovered from the Amazon Kindle.

5.3 Future Work

Future work on the Amazon Kindle may consider extending this research based on the delimitations in chapter one. Artifacts located within the system partitions could be useful in an investigation. The Kindle file population processes in the execution of the research did not include wireless download purchases, wireless download of archived content, or downloaded documents through Amazon's Kindle Personal Document Service. These population processes may yield different results. Hardware deletion, Amazon.com deletion, reset to factory defaults, and formatting through the computer host processes can be studied to understand their effects. The security of the Kindle and identifying and mitigating methods of data obfuscation can be researched. Other obfuscation and security issues should be explored, specifically with files appearing as downloaded books and the security of Whispernet. Other imaging software and analysis software can be compared in future research. A future concern that must be researched is the Kindle Development Kit (KDK).

Other future work may be based on the results and discussion of this research. Directory entries within the Kindle file system and operating system need further analysis and testing because the expected results do not align with the results of this research. Windows may have different effects when using another file system such as NTFS.

REFERENCES

AccessData. (2013, November 12). Forensic Toolkit user guide (v 5.1). Retrieved from http://marketing.accessdata.com/acton/attachment/4390/f-0542/1/-/-/-/-/FTK_UG.pdf

Amazon.com. (2012, July). Amazon.com timeline. Retrieved from http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MTQ2MzQ4fENoaWxkSUQ9LTF8VHlwZT0z&t=1

Amazon.com. (2011). Amazon Kindle user's guide. Retrieved from http://kindle.s3.amazonaws.com/Kindle_User's_Guide_English.pdf

Amazon.com. (2007). Kindle: Amazon's original wireless reading device (1st generation). Retrieved from http://www.amazon.com/dp/B000FI73MA

Amazon.com. (2007, November 19). Introducing Amazon Kindle. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1079388&highlight=

Amazon.com. (2009, February 9). Introducing Amazon Kindle 2. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1254544&highlight=

Amazon.com. (2009, May 6). Introducing Kindle DX – Amazon's large screen addition to the Kindle Family of wireless reading devices. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1285140&highlight=

Amazon.com. (2009, December 26). Amazon Kindle is the most gifted item ever on Amazon.com. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1369429&highlight=

Amazon.com. (2010, June 15). Kindle – Amazon's most wished for and most gifted product – now with free shipping for Father's Day. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1438278&highlight=

Amazon.com. (2011, April 11). Amazon introduces new Kindle family member: Kindle with Special Offers for $114. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1549144&highlight=

Amazon.com. (2011, May 19). Amazon.com now selling more Kindle books than print books. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1565581&highlight=

Amazon.com. (2012, September 6). Amazon takes on the high-end – introducing the new Kindle Fire HD family. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1732546&highlight=

Amazon.com. (2012, September 6). Introducing the new Kindle Paperwhite, the most advanced e-reader ever constructed. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1732545&highlight=

Amazon.com. (2012, October 25). Introducing "Kindle for Windows 8." Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1750157&highlight=

Amazon.com. (n.d.). Connecting your Kindle Keyboard wirelessly. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=200505540

Amazon.com. (n.d.). Free Kindle reading apps. Retrieved from http://www.amazon.com/gp/feature.html?ie=UTF8&docId=1000493771

Amazon.com. (n.d.) Getting started. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_kbbland_stcomp?nodeId=200439170

Amazon.com. (n.d.) Getting started. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=200590080

Amazon.com. (n.d.) Getting started with Kindle Cloud Reader. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_cloudland_start?nodeId=200732260

Amazon.com. (n.d.) Getting started with Kindle for Mac. Retrieved from www.amazon.com/gp/help/customer/display.html/ref=hp_macland_stcomp?nodeId=200443820

Amazon.com. (n.d.). Getting started with Kindle for PC. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_left_cn?ie=UTF8&nodeId=200450200

Amazon.com. (n.d.). Getting started with Kindle for webOS. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_webosland_started?nodeId=200717410

Amazon.com. (n.d.). Getting started with the Kindle app. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_ipland_stcomp?nodeId=200438220

Amazon.com. (n.d.). Kindle active content. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_left_sib?ie=UTF8&nodeId=200505220

Amazon.com. (n.d.). Kindle Cloud Reader. Retrieved from https://read.amazon.com/about

Amazon.com. (n.d.). Kindle Development Kit for active content. Retrieved from http://www.amazon.com/kdk/

Amazon.com. (n.d.). Kindle for the web beta. Retrieved from http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=200528580

Amazon.com. (n.d.). Kindle Owners' Lending Library for Amazon Prime members. Retrieved from https://www.amazon.com/gp/help/customer/display.html/ref=lp_mem_help?ie=UTF8&nodeId=200757120

Amazon.com. (n.d.). Kindle Paperwhite 3G. Retrieved from http://www.amazon.com/gp/product/B008UB7DU6/

Amazon.com. (n.d.). Kindle Personal Documents Service. Retrieved from http://www.amazon.com/gp/help/customer/display.html/?nodeId=200767340

Amazon.com. (n.d.) Kindle for Android phones. Retrieved from http://www.amazon.com/gp/help/custome r/display.html/ref=hp_left_sib?ie=UTF8&nodeId=200495330

Amazon.com. (n.d.) Kindle for Android tablets. Retrieved from www.amazon.com/gp/help/customer/display.html/ref=hp_left_sib?ie=UTF8&nodeId=200683130

Amazon.com. (n.d.). Kindle wireless reading device, Wi-Fi, graphite, 6" display with new E Ink Pearl technology. Retrieved from http://www.amazon.com/dp/B002Y27P3M/ref=btech_kindle_wifi

Amazon.com. (n.d.). Kindle wireless reading device, free 3G, 6" display, white - 2nd generation. Retrieved from http://www.amazon.com/dp/B0015T963C

Amazon.com. (n.d.). Lending Kindle books. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=amb_link_357435222_6?ie=UTF8&nodeId=200549320

Amazon.com. (n.d.). Organizing your Kindle content. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=200375850

Amazon.com. (n.d.). Public library books for Kindle. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_200527380_library?&nodeId=200747550

Amazon.com. (n.d.). Renting Kindle books. Retrieved from http://www.amazon.com/gp/help/customer/display.html/ref=hp_left_sib?ie=UTF8&nodeId=200690040

Amazon.com. (n.d.). Transferring, downloading, and sending files to Kindle Keyboard. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=200505520

Amazon.com. (n.d.). Wireless, Whispernet and Whispersync. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=200375890

Amazon.com. (n.d.). Your Kindle content. Retrieved from http://www.amazon.com/gp/help/customer/display.html/?nodeId=200386160Apple. (n.d.). Kindle – read books, eBooks, magazines, newspapers & textbooks. Retrieved from https://itunes.apple.com/us/app/id302584613

Beebe, N., & Clark, J. (2005). Dealing with terabyte data sets in digital investigations. International Federation for Information Processing, 2005(194), 3-16. doi:10.1007/0-387-31163-7_1

Bezos, J. (2010). Interview by C. Rose [Video recording]. Jeff Bezos, Founder & CEO, Amazon.com. Retrieved from http://www.charlierose.com/view/interview/11138

Bishop, M., Hay, B., & Nance, K. (2009). Digital forensics: Defining a research agenda. Proceedings of the 42nd Hawaii International Conference on System Sciences. doi: 10.1109/HICSS.2009.673

Burchett, J. (2005). Computer forensic data unit layer testing. Unpublished master's thesis, Purdue University, West Lafayette, IN

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. International Journal of Digital Evidence, 1(4), 1-12.

Carrier, B. (2005). File system forensic analysis. Boston: Addison Wesley

Casey, E. (2004). Digital Evidence and Computer Crime, Second Edition. San Diego California: Academic Press.

Craiger, P. (2005). Recovering digital evidence from linux systems. International Federation for Information Processing, 194, 233-244. doi: 10.1007/0-387-31163-7_19

Creswell, J. (2009). Research Design. Thousand Oaks, CA: SAGE Publications, Inc.

Daniel, L., & Daniel, L. (2011) Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom [Kindle Version]. Retrieved from Amazon.com

Garfinkel, S. L. (2006). Forensic feature extraction and cross-drive analysis. Digital Investigation, 3(1), 71-81. doi:10.1016/j.diin.2006.06.007

Garfinkel, S. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7 (August 2010), S64-S73. doi:10.1016/j.diin.2010.05.009

Horrocks, M., Coulson, S., & Walsh, K. (1998). Forensic palynology: Variation in the pollen content of soil surface samples. Journal or Forensic Sciences, 43(2), 320-323.

Leshney, S. (2008). Digital evidence from virtual machines: An exploratory study. (Master's thesis). Retrieved from ProQuest Dissertation and Theses database. (VMI No. 1469702).

Marsico, C., & Rogers, M. (2005). iPod forensics. International Journal of Digital Evidence. 4(2). 1-12.

Microsoft. (n.d.). Amazon Kindle | Windows Phone Apps+Games Store (United States). Retrieved from http://www.windowsphone.com/en-us/store/app/amazon-kindle/48195fb4-ee0e-e011-9264-00237de2db9e

National Institute of Standards and Technology. (November 7, 2001). General test methodology for computer forensic tools version 1.9 (Vol. 2008) (No. June 20 2008).

Slovenski, T. (2012). Cellular Forensics for First Responders [Kindle Version]. Retrieved from Amazon.com

Willassen, S. (2005). Advances in digital forensics. International Federation for Information Processing (Ed.), Forensic analysis of mobile phone internal memory. (pp. 191-204). Boston, MA: Springer. doi: 10.1007/0-387-31163-7_16