

UNIVERSITY OF CENTRAL OKLAHOMA

Edmond, Oklahoma

Jackson College of Graduate Studies

**USE OF FORENSIC CORPORA IN VALIDATION OF
DATA CARVING ON SOLID-STATE DRIVES**

Submitted by

Kristina Y. Hegstrom

Forensic Science Institute

In partial fulfillment of the requirements

For the Degree of Master of Science in Forensic Science

2016

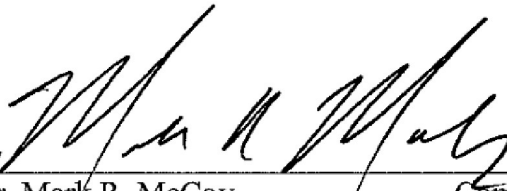
**USE OF FORENSIC CORPORA IN VALIDATION OF
DATA CARVING ON SOLID-STATE DRIVES**

By: Kristina Yvette Hegstrom

A THESIS

APPROVED FOR THE W. ROGER WEBB FORENSIC SCIENCE INSTITUTE

DECEMBER 2016

By 
Dr. Mark R. McCoy Committee Chair


Dr. James Creecy Committee Member


Dr. Wayne B. Lord Committee Member

Acknowledgements

I would first like to thank my thesis advisor, Dr. Mark McCoy of the University of Central Oklahoma, Forensic Science Institute. Dr. McCoy was always available to answer tough questions, provide encouragement, and help me whenever I hit a roadblock throughout this study. He consistently allowed this work to be my own, while providing valuable insight and support.

I would also like to thank Dr. James Creecy and Dr. Wayne Lord for serving as members of my committee. Their insight and commitment to continuing to improve practices within the forensic disciplines served as one of the key motivations in completing this work. In addition to these individuals, I must also thank all the other faculty and staff members at the Forensic Science Institute for their support, especially those who helped ensure I had access to equipment and all the supplies necessary to construct and complete my thesis. Part of this project could also have not been made possible without the help of Dr. Tracy Morris and the Department of Mathematics & Statistics.

Special thanks go to the Comal County Sheriff's Office, Criminal Investigation Division. Thank you to my Captain, my Sergeants, and all the detectives and support staff who welcomed me with open arms and supported the completion of my graduate program.

Finally, I would like to thank my family. To my husband, Charles, thank you for always being supportive and doing everything in your power to help me achieve my goals. And thank for seeing my potential. To my parents, Jimmy & Kelli, and my in-laws, Steve & Mary Jo, thank you to all of you for encouraging me when times became hard, and for always having faith in me, and helping me reaffirm my faith in God.

Abstract

The need for greater focus on the validation and verification of tools has become more evident in recent years. The research in this area has been minimal. Continued research regarding the validation of digital forensics tools is necessary to help meet demands from both the law enforcement and scientific communities and to bring digital forensics in line with other forensic disciplines (as cited in Guo, et al., 2009). One of the most effective ways to perform validation and verification of digital forensics tools is to enlist the use of standardized data sets, also known as *forensic corpora*. This study focused on the use of forensic corpora to validate the file carving function of a common digital forensics tool, Access Data's Forensic Tool Kit (FTK). The study centers specifically on FTK's ability to recover data on solid-state drives (SSDs). The goal of this study was to both evaluate the use of forensic corpora in the validation and verification of digital forensic tools, as well as a serve as a validation study of FTK's carving function on solid-state drives.

**USE OF FORENSIC CORPORA IN VALIDATION OF
DATA CARVING ON SOLID STATE DRIVES**

Acknowledgements.....	3
Abstract.....	4
Table of Contents.....	5
List of Tables.....	7
List of Figures.....	8
List of Appendices.....	9
Chapter 1: Introduction.....	10
Statement of the Problem.....	12
Lack of Research in Digital Forensics.....	13
Forensic Corpora Use and Availability.....	13
New Technologies in Digital Forensics.....	14
Background and Need.....	15
Purpose of the Study.....	16
Research Questions.....	18
Significance to the Field.....	18
Definition of Terms.....	19
Limitations.....	20
Chapter 2: Literature Review.....	22
Validation Techniques Through File Carving.....	22
Forensic Corpora in Tool Testing.....	26
Solid-state Drives.....	30
Summary.....	32
Chapter 3: Methodology.....	33
Setting.....	34
Sample.....	34
Materials.....	36
Measurement.....	38
Data Collection.....	39

Data Analysis.....	41
Chapter 4: Results.....	42
File Carving Analysis.....	44
File Carving Results by Solid-state Drive Size.....	45
File Carving Results by Test Image Level.....	45
File Carving Results by File Type.....	46
Chapter 5: Discussion.....	49
Discussion.....	50
Limitations.....	53
Recommendations for Future Research.....	55
Conclusion.....	56
References.....	58

List of Tables

Table 1: <i>CFTT Test Image Data Levels and Descriptions</i>	35
Table 2: <i>CFTT Test Image Types and File Types</i>	36
Table 3: <i>File Carving Results Measurement Scale</i>	40

List of Figures

Figure 1: <i>FTK File Carving Example.</i>	38
Figure 2: <i>Image Layouts Example.</i>	39
Figure 3: <i>Recorded File Carving Results.</i>	41
Figure 4: <i>Summary statistics of data carved by SSD Size.</i>	42
Figure 5: <i>Summary statistics of data carved by test image level.</i>	43
Figure 6: <i>Summary statistics of data carved by file type.</i>	43
Figure 7: <i>Percentage of files carved correctly by solid-state drive size.</i>	45
Figure 8: <i>Percentage of files carved correctly by file level.</i>	46
Figure 9: <i>Percentage of files carved correctly by file type.</i>	47

List of Appendices

Appendix A: File Carving Test Images 60

Appendix B: Recorded File Carving Results 62

CHAPTER 1

Introduction

In recent years, the field of forensic science has begun to face continued scrutiny from government bodies, law enforcement, and the public. In September of 2016, the President's Council of Advisors on Science and Technology (PCAST) recommended actions to strengthen forensic science and promote its more rigorous use in the courtroom (President's Council of Advisors on Science and Technology, 2016). This council, comprised of individuals in academia and law enforcement, released a report titled, "Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods." In this report, advisors discuss and consider the role of scientific validity within the legal system. While some on the council went so far as to recommend some forensic disciplines be thrown out of court, they recommended others be subject to larger scale validation of techniques. Such scrutiny has been long standing in the forensic community. In fact, this report comes in the aftermath of the scathing 2009 National Research Council Report, "Strengthening Forensic Science in the United States: A Path Forward," which called for major reforms to the criminal justice system and charged those in the forensic community to move forward in establishing national forensics scientific standards (National Research Council, 2009).

The digital forensics discipline has been no stranger to scrutiny in the scientific world. Digital forensics first emerged as an established discipline in the late 1980s, following the emergence of the personal computer and a rise in computer related crimes (Guo, Slay, and Beckett, 2009). Digital forensics is not only young in comparison to other forensic disciplines, but also faces a set of problems rarely encountered in other areas. While digital forensics investigations initially focused on computer related crimes, this field has grown to encompass a

variety of digital devices. In turn, as the quantity and diversity of digital devices available has increased, technology has only continued to evolve (Wilsdon & Slay, 2005, p. 1). In other disciplines, the examiner is often presented with opportunities for comparative analysis, wherein they are provided access to an evidentiary “known” sample that can then be compared to an unknown for investigative purposes. Digital forensic examiners however, rarely work under the same conditions. In conducting their analysis, they must rely heavily on their forensic tools in recovering evidence. This frequently requires searching through large amounts of information for evidence based on statements or other known details about the case in question.

Due the nature of digital forensics investigations and the similar methodology utilized by examiners, a large percentage of their analysis relies heavily on the availability and use of various digital forensics tools. Tools such as Access Data’s Forensic Tool Kit (FTK) and Guidance Software’s EnCase Forensic come equipped with features including file carving, password recovery capabilities, and other functions, enabling examiners to locate specific types of data based on particular characteristics and perform complex analysis. Digital forensics tools can also aid examiners in recovering deleted and corrupted files. Understanding the role digital forensics tools play in analysis is essential for not only examiners, but also for those involved in the prosecutorial phase- be it jurors, judges, or attorneys. Digital forensics tools are used from the collection phase, throughout analysis, and into the reporting process thereafter. Because these tools are an absolute necessity in effective forensic analysis, they must be confirmed to function both properly and as intended.

To ensure the reliability of these tools, greater research is required in the area of digital tool validation and verification. Commonly used forensic tools need to undergo testing in order to confirm that they are indeed performing a true forensic function. Examiners must also be

assured that the tools are performing appropriately, recovering data correctly, and in turn reporting true and accurate results as well as performing a true forensic function (Beckett & Slay, 2007, p.3). Studies such as these, however, have continued to prove difficult in the research community due to lack of resources, time, and communication. Added to this challenge are the continuous advances in technology across a wide range of devices, often times making it difficult for forensic tools to keep up with device functions. As a result of these changes, more research is required in the area of digital forensics, focusing on tool performance in various settings to gain a better understanding of functionality and reliability during forensic analysis.

Statement of the Problem

In his 2010 work, Garfinkel analyzed current and future trends in digital forensics research, noting the need to make digital forensics research practices more efficient through data representation (Garfinkel, 2010, p.S-68). There has been significantly less research in the field of digital forensics in comparison to other disciplines. However, rapid changes in technology and their increased presence in the commission of crime warrant the need for further study in the area. Researchers and examiners in the field have reached a consensus that one of the greatest issues faced when attempting to advance digital research has been lack of standardization. Much of this relates to limited availability to standardized data sets, or *digital corpora*, which is necessary in order for similarly structured studies to be conducted effectively by different examiners and across a variety of tools.

Lack of Research in Digital Forensics.

Digital forensics differs in comparison to other forensic disciplines in that it was born out of necessity. The committee on “A Path Forward” (2009) reminds us that unlike other disciplines, digital forensics did not start in forensic laboratories. In turn, it has been forced to mature while subsequently facing the “rigors and expectations of other fields of forensic science” (p. 181). This background has sadly contributed to the lack of research in this area. Although digital forensics now involves a greater number of scholars, it is still intertwined with the world of law enforcement, where much of the analysis is still seen as investigative, rather than a true forensic function. Lack of agreed upon certification and various level of training also lend to difficulties in conducting comprehensive, collaborative studies (p.182). In continuing to move forward increasing reliability and trustworthiness of results, the digital forensics community must direct its effort toward better understanding one of the key methods used in the majority of digital forensics analysis- file carving. File carving, also known as data carving, involves recovering data based on file signatures and headers, often from unallocated space (Yoo, Park, Lim, Bang, & Lee, 2012, p. 244). Focus in this area will require validation studies measuring the tools’ capabilities. To effectively study the functionality of carving tools, there is a need for widespread development and availability of standardized data sets, known as forensic corpora.

Forensic Corpora Use and Availability.

Forensic corpora, also referred to as digital corpora, have served as another necessary piece of the puzzle in the effort to increase research and practice regarding validation and verification of forensic tools. A principle element of most scientific disciplines, and the basis of research, is the ability to perform controlled experiments that can be reproduced, and often

expanded upon, by others in the field. In order for examiners and researchers to be able to conduct repeatable experiments using digital tools, forensic corpora must be available. Garfinkel, Farrell, Roussev, and Dinolt (2009) state that the availability and use of forensic corpora allows for the establishment of a baseline. This in turn provides results that can help improve both current and future tools. Currently, examiners have been met with difficulty in acquiring reliable forensic corpora. Much of this is due to lack of availability of broad standardized data sets. Correspondingly, examiners and researchers alike have often been left to rely on accuracy rates as disclosed by vendors.

New Technologies in Digital Forensics.

Dating back to the emergence of early computers, the digital world has experienced variability among electronic storage media. The need for portable and accessible media quickly became evident as computers expanded into the realm of personal use and continued to advance in function and capability. Solutions to the need for various storage options came to fruition as early as the 1950s and 1960s, with the availability of hard disk drives (HDD) and later, floppy disks. While some types of media, like floppy disks, eventually dwindled, storage devices such as hard disk drives were kept alive by vendors thanks to increases in capacity and speed (Pierce, 2010, p. 12). While hard disk drives are still alive and well today, technology has continued to evolve in an effort to meet consumer needs. As a result, we have witnessed innovations in digital media that have slowly become essential in the production of digital devices—from personal computers, to cellular phones, to external storage. Although there have been rapid advanced in the types of media used in common digital devices, much of the research done on file carving to date has focused on traditional hard disk drives. With this, it is evident there is a need for digital

examiners and researchers to not only study carving functions and capabilities, but to expand these studies to include media similar to those that become more prevalent in the types of devices often examined during criminal investigations.

Background and Need

There has been little research focused on file carving reliability on digital media outside of traditional hard disk drives. From its conception, digital forensics has expanded outside of criminal justice into both the public and private sectors. Because of this expansion, it has faced problems growing into an established, reliable discipline. As a result, it has struggled to maintain the standards met by other forensic disciplines. Due to lack of research to support a scientific basis, courts and the media have questioned as to whether or not the results of digital analysis are truly trustworthy.

In order to improve the “trustworthiness” of digital forensics analysis and reaffirm the discipline’s scientific, more studies must be developed with a focus on file carving and how it relates to overall analysis. Previous research has shown that both current and future digital forensics research needs to become dramatically more efficient and better coordinated to meet expectations (Garfinkel, 2010, p. S-69). Achieving this task requires the use of forensic corpora. In addition, although efforts have been made previously within the digital forensics community to create corpora that could be used on a broad scale, there has still been very little standardization. While collaborative efforts among researchers to create usable data sets remains an attainable goal in the future, currently available corpora should be considered to continue to move digital forensic research forward.

Organizations such as the National Institute of Standards and Technology (NIST) and the Scientific Working Group on Digital Evidence (SWGDE) have begun to take steps toward validation and verification of digital tools. NIST has established the Computer Forensic Tool Testing (CFTT) project to better study the specific functions of the tools used in today's field, while SWGDE has recommended guidelines for validation testing (Guo, Slay, and Beckett, 2009). The use of forensic corpora within the scientific community available from reputable research bodies can prove useful in conducting file carving studies on various tools, that are in turn easily reproducible by examiners, providing both training and a basis for future research. Once again, these studies must expand outside of traditional media. In striving to create studies that will prove beneficial in laboratory analysis, research should begin to focus on a drive that has become more commonplace in computer and mobile devices-solid-state drives (SSDs). The structure, reliability, and speed of solid-state drives has contributed to its utilization across an expansive range of devices, and due to continued increase in affordability, some researchers in the digital community predict that it will eventually replace the hard disk drive altogether (Pierce, 2010, p. 12).

Purpose of the Study

The purpose of this study was to validate the data carving function of a common tool utilized in digital forensics labs, Access Data's Forensic Tool Kit (FTK), using forensic corpora on solid-state drives (SSDs), and to review the application of standardized corpora in validation and verification of digital forensics tools. There is a need for updated practices in the field when working with digital forensic tools in order to improve on both current and future methodology (Editorial, 2006, p. 2).

With the discovery that evidence in other disciplines has at times proven inaccurate or unreliable, as seen in overturned convictions due to analysis error, forensic science continues to face increased scrutiny. While many have begun to question the reliability of forensic testimony as a whole, other efforts have been put forth in continuing to reinforce the importance of forensic evidence in the law enforcement. As such, there have been unrelenting calls for foundational validity, in which the methods executed by forensic examiners have been subjected to empirical testing by various outlets (PCAST, 2016, p. 5). For digital forensics to remain relevant as a discipline and increase trustworthiness among the courts and the public, more extensive research must be carried out to support the reliability of findings as well as contribute to the effective analysis of future technology.

The increased availability and prevalence of solid-state drives in digital devices supports the need for research geared toward measuring the functionality of carving tools when recovering data from SSDs. In this study, forensic corpora, used in a previous file carving study conducted by NIST (2014) on HDDs, will be restored to SSDs of various sizes. The corpora will consist of different levels, and each data set will be carved from its respective drive using the Forensic Tool Kit (FTK) carving function.

While the carving rate of FTK is presumed amongst examiners to be high on hard disks drives, around 100%, there have been few studies to confirm a similar carving rate on solid-state drives. In conducting this research, it was expected that FTK would carve data from solid-state drives at a rate similar to the presumed industry rate. The accuracy rate could vary depending on the type of files being carved. For contiguous files, the tool is expected to recover at a rate close to 100%; while with non-contiguous, or fragmented, files, the rate may be significantly lower. It must also be noted that SSDs are structured somewhat differently than HDDs, and as such, the

possibility exist that while data may be carved from the SSDs, the reported data itself may either be incorrect or the correct data carved from the wrong location.

Research Questions

This research looked to answer the following questions. First, does FTK's data carving function perform as intended and recover all possible data when used on solid-state drives? We also wanted to explore whether FTK's data carving function ability varies significantly when carving is carried out on solid-state drives of various sizes, file types, and file structures.

Significance to the Field

This study sought to add to the current standards in place for executing file carving using Access Data Forensic Tool Kit (FTK), and other similar tools utilized in digital forensics investigations. This research also hoped to shed light on the significance of standardized forensic corpora in digital research and its practicality in contributing to more widespread, reproducible studies. In turn, it is our anticipation that more researchers and nationally established scientific organizations will continue to contribute towards building reliable corpora available for use in the scientific community. This research also sought to serve as a starting point for similar studies, as well as spur more exploration on carving capabilities in regard to solid-state drives.

In the long term, studies such as this one will help contribute to larger scale studies with a greater focus on emerging technologies. Continuing to develop research that focuses on tool testing will help to establish baselines for reliability across a broad range of tools, and ultimately lend to increasing trustworthiness of results. Working to better understand these tools will also continue to urge examiners to reevaluate current standards as new tools arise. Lastly, increasing

research studies in general in digital forensics will ultimately subsidize training practices among departments.

Definition of Terms

- Computer Forensics Tool Testing Program (CFTT)- A joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology (NIST) Law Enforcement Standards Office (OLES) and Information Technology Laboratory (ITL), whose objective is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results.
- Contiguous File- A file on disk that is not broken apart. All sectors are adjacent to each other.
- FAT32- (File Allocation Table32) The 32-bit version of the FAT file system, widely used for USB drives, flash memory cards, and external hard drives for compatibility on all platforms.
- File Carving- The process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values.
- File Extension- A file type that is appended to the end of a file name (ex. .DOC, .JPEG).
- File Footer- A small amount of data at the end of a file that denotes the end of the file.
- File Header/Signature- A small amount of data at the beginning of a file which generally defines the content of the file and list specific file attributes.
- Forensic Corpora/digital corpora- A standardized, representative reference data set; can contain various file types, file sizes, and file systems.
- Forensic Image- A bit stream copy of the available data. The result may be encapsulated in a proprietary format (e.g., E01, 001, etc.).
- Forensic Wipe- Completely erasing the data in disk sectors.
- Fragmented File- Storing data in non-contiguous areas on a disk.

- Hash or Hash Value- Numerical values, generated by hashing functions, used to substantiate the integrity of digital evidence and/or for inclusion /exclusion comparisons against known value sets.
- Hashing Function- An established mathematical calculation that generates a numerical value based on input data. This numerical value is referred to as the hash or hash value.
- National Institute of Standards and Technology (NIST)- A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.
- Offset- The distance from a starting point, either the start of a file or the start of a memory address. An offset into a file is simply the character location within that file, usually starting with 0.
- Sector- The smallest unit of data that is written to and read from a storage drive.
- Wear-leveling- A technique for prolonging the service life of storage media (such as flash memory), where data is arranged so that erasures and re-writes of data are distributed evenly across the medium.

Limitations

The focus of this study is to utilize previously proposed methods to further explore the practicality of forensic corpora in validation and verification of digital forensics tools. This study is limited in that it focused on the function of only one tool. With that, although the procedures used in this study may be similar to those used in other validation studies, the results are likely to vary when used with a different tool.

A second issue is that this study will be conducted with limited data samples. As stated previously, forensic corpora is beneficial in conducting validation studies of digital tools. However, building corpora is time consuming and access to multiple sets of corpora is limited. Another point worth noting is that, even with an extensive set of corpora, it is nearly impossible to fully encompass an example of every case scenario a practitioner would encounter in the field.

This study was conducted under a specific set of conditions, with all settings and test results recorded. As a result, this study should be capable of being replicated by another researcher, assuming the same version of FTK and same corpora sets are used. Once again though, differing software conditions and hardware configurations, as well as other lab factors, could possibly yield results different than those obtained in this study.

CHAPTER 2

Literature Review

Digital forensics has struggled to meet and maintain the standards held by other forensic disciplines. Much of this has been due to lack of research in the field, resulting in digital evidence being called into question when evaluating its reliability in criminal investigations. In reviewing current practices, digital forensics has been identified by law enforcement and researchers as a field requiring greater standardization and reproducibility. There is also a clear need for researchers to continue to develop studies with an emphasis on newer technology in order to better understand the components necessary to improve tools for future research and analysis, and avoid current techniques becoming completely irrelevant (Garfinkel, 2007, p. S66). This research focuses on the utilization of forensic corpora in evaluating the reliability of file carving when used on solid-state drives (SSDs).

The literature review will address three areas of research related to the use of forensic corpora in conducting file carving on solid-state drives. In the first section, research related to previous studies and their contributions to the field will be addressed. The second section will discuss the components needed for reliable forensic corpora, as well as the benefits of incorporating corpora into current and future studies. Finally, the last section will focus on the emergence of solid-state drives, and their role in the future of digital media and digital forensics.

Validation Techniques Through File Carving

While forensic science disciplines have continued to receive widespread criticism, it should be noted that much of this dismay is due to lack of standardization in many fields. Particularly in the area of digital forensics, there is not solely one universal standard concerning

assessing the reliability of digital forensics tools (Wilsdon & Slay, 2005, p. 5). As a result, this weakens the discipline in several ways. Forensic experts, while often prepared witnesses, present testimony with minimal scientific foundation. Lack of standardization has also led to fewer forensic labs holding accreditation in digital forensics, as well as examiners having little knowledge of how the tools used during analysis truly function on a scientific level.

In moving away from a sole focus on the investigative side of digital forensics, examiners and researchers across the board have pushed recommendations for developing a framework surrounding validation and verification techniques. ISO (International Organization for Standardization) 17025 serves as a starting point for many labs. This standard specifies the general requirements to be deemed competent and in turn, receive accreditation for that specific discipline (ISO, 2010). The question must be explored as to whether the tools being used are actually performing a true forensic function. From this, we see the rise in demand for validation and verification (VV) of common digital forensics tools from law enforcement and research organizations.

Wilsdon and Slay (2005) define validation as “the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies requirements,” satisfying intended use and user needs (p. 2-3). To simplify, validation is conducted to determine if a tool functions correctly as it was intended to function. They go on to define verification, citing this process as “evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase” (p. 3). Verification focuses on whether the product is built correctly. Validation is confirmed through verification, with the application of different tools and techniques. The end

results can provide answer as to whether or not tools are actually performing a true forensic function.

In establishing VV techniques, many researchers' concentrated efforts toward file carving studies in testing the reliability of commonly used forensic tools on a variety of digital devices. Data recovery is a significant part of digital investigation, often including recovery from various types of media. However, the term has become synonymous with forensic recovery over the years. Forensic recovery is often conducted through file carving. File carving is accomplished by "extracting" (or copying) all the bytes to a file from an image (Cohen, 2007, p. 120). Some common file carving tools used in today's market include EnCase and Access Data Forensic Tool Kit (FTK). The usefulness of file carving in forensic investigations points to another issue discussed later in this text.

Original file carving tools were simple, relying on Start of File/End of File (SOF/EOF) carvers. These types of programs would search for file headers and footers (p.120) of commonly known file types (i.e. PDF, WordDoc, etc.). While this method worked well initially, as technology continued to improve, file-carving techniques became faced with a constant need to advance. The complexity of data sets encountered in investigations has evolved from structured, contiguous files to large volumes of fragmented and intertwined bytes of data consisting of various file types. Carving serves as a significant, essential tool in forensic investigation, as it often allows examiners to recover data when the information has been deleted or a file system is not present (p. 127).

In moving forward, it is recommended that a centralized, well-recognized scientific body serve at the helm of laying the groundwork for file carving methodology and research (Wilsdon & Slay, 2005, p. 6). Over the last decade, a variety of research organizations-the Scientific

Working Group on Digital Evidence (SWGDE), the Department of Defense, and the National Institute of Standards and Technology (NIST)-have spearheaded research projects and moved to provide more guidelines for digital forensics studies. In 2014, the Computer Forensics Tool Testing (CFTT) program conducted an extensive file carving test-utilizing Version 4.1 of Access Data Forensic Toolkit (FTK).

In this study, the CFTT reviewed how the carving function of Version 4.1 of FTK performed when carving raw disembodied “dd” graphics images, or forensic corpora (NIST, 2014). These graphics images varied in content. A total of seven levels were developed, identifying the content contained within each forensic image. Some images were complete and contiguous, while others were only partially complete or fragmented. The images used also varied in file type, including jpeg, bmp, png, tiff, etc. Using the default settings in FTK, the researchers directed the file-carving tool to carve files from each data set. The reported data was then recorded and the recovery rate reviewed. The study noted that this version of FTK was most successful at carving bmp, png, and jpg. It was also noted that the majority of gif files were incomplete, and tiff files could not be carved (p. 2).

While this study was significant in adding to currently established file carving research, it contains several limitations. First, the study focuses only on the file carving function’s performance when recovering graphics files. Given the broad range of file types utilized in digital communications, file carving capabilities should be tested and measured on a variety of file types, specifically those most likely to be encountered by an examiner during an investigation. These include documents, audio, video, and more. Next, as stated previously, technology is constantly evolving- often times faster than digital forensics tools are able to keep pace. When this study was conducted in 2014, Access Data FTK was on Version 4.0. As of

October 2015, FTK currently functions under Version 6.0. Rapid updates and changes to common software such as this point to a clear need for testing to not only be conducted on these tools, but for this to be done so on a regular basis as so to keep up with current technological advances. Lastly, this study was conducted on traditional media, such as hard disk drives (HDD). Again, progressions in technology, often as a result of consumer demand, support the idea that testing must not only be conducted regularly, but also developed around new devices as they become more widespread.

Forensic Corpora

One of the most significant components in the success of the previously described CFTT file carving study was the availability of a broad, diverse set of forensic corpora. This data supports the argument for standardization across digital forensics studies. Alluded to briefly in the introduction, in order for new validation and verification approaches to be able to be applied in digital forensics research, the issue of forensic corpora must be tackled. Forensic corpora are essentially standardized, representative sets of data. The content within corpora sets is known prior to conducting the study. This can include the use of image layouts which indicate the number of known files in each corpora set, their size, and location. In regard to their role in digital forensics research, they work to support studies on various scales in terms of size and content. Garfinkel et al. (2009) explain that “representative corpora enhances scientific evaluation of forensic methods beyond the obvious benefits of providing ready test data and enabling direct comparison of different approaches” (p. 2). To reiterate, the authors acknowledge that the use of corpora in research ultimately helps establish a baseline for the tools being tested.

Reproducibility is a widespread issue across the discipline due to lack of standardization. Although there have been several studies over the last ten years examining data sets using similar tools, the results have done less than desired to spur larger scale and more frequent tool studies. In much of the current literature on file carving, different researchers have tested the same or similar tools. In the majority of these cases, however, the data sets utilized to measure file carving rates varied from study to study. The issue arises that, while one set of results may report a high level of accuracy with a specific tool, another may report low accuracy. All the same, the results are still not comparable because the same data sets were not used (Garfinkel et al., 2009, p. 4). The availability of common corpora accepted by the research community would level comparability in digital forensics and allow for improvements to tool functions. Standardized corpora would also benefit academia, providing greater opportunities for file carving studies on the academic level, as well as garnering a better comprehension of the components necessary for strong corpora that can be utilized on both old and new, emerging technology.

While forensic corpora is clearly desirable in improving digital research as a whole, the sheer availability of these data sets is not enough and can prove useless without being constructed with certain goals in mind. For corpora to be effective, a large and diverse sample must be available. Although not every scenario that digital examiners may face in an investigation can be predicted, it must still include a representative enough sample of the common issues and data regularly encountered in the field. This requires the inclusion of both sensitive and non-sensitive data, generated from frequent use of human subjects.

In their study, Garfinkel et al. (2009) focus on building a variety of corpora sets. They note the inclusion of disk images, memory images, and files among other types of data. In tackling this project, they span a broad range of data types- utilizing disk images, which are the

most fundamental to forensic corpora, to network packages, an area still fairly young in comparison to traditional computer forensics. The corpora sets ultimately constructed for further research use contained various file types, were built with different media types in mind, and took into consideration the size of the final image. In conclusions however, the researchers noted that the study proved much more difficult than they had initially perceived. They noted size being the most difficult part, wherein they experienced difficulties transferring files and an image could be anywhere between 10 Gigabytes to 100 Gigabytes in range. The researchers also encountered another common issues experienced by examiners working to build corpora-privacy.

A representative corpus requires real and relevant data. This often requires data used in corpora sets to be generated by average users. Use of such data though raises the question of privacy when utilizing an individual's data for other research. While researchers can generate their own data for studies, this proves grossly time consuming. Garnering data from volunteers and the "wild" however yield a different set of problems. Roux and Falgoust (2012) review the ethical concerns when procuring data media from outside sources. The authors note that many of the ethical procedures have little standing in influencing examiners and no true board to oversee them. However, as technology has become more ingrained as a fixture in everyday life, more emphasis has been placed on digital privacy. In retaining data for their study, devices were purchased from third party sites such as eBay. In their findings, it was noted that other parties who may not always be the data owner sell many devices. Roux & Falgoust compared going through data acquired through these means to "going through someone's trash," wherein, if a person does not want something found, it is their responsibility to destroy it (p. 53). However, researchers still run the risk of ethical violations when examining data not previously known to them.

These studies point toward important considerations for future file carving tests. For future studies to continue to yield useful results for examiners, forensic corpora must span in all possible directions. Data sets must include various file types, sizes, and states. Levels should be considered, and include fragmented and non-fragmented files, as well as files that fluctuate in contiguity. While enlisting the use of data generated by real individuals is beneficial, the risk of violating an individual's privacy as well as the discovery of illegal material is currently too great. Building corpora is ideal, in that it allows examiners to be aware of what file types and data are already present, as well as where these files are located and what is needed for them to be successfully carved. As noted previously however, building a broad range of corpora is painstakingly time consuming, even for a group of researchers.

Keeping these issues in mind, steps can be taken toward the application of specific aspects of each these types of studies that will ultimately yield effective and more easily reproducible research. First, studies should initially be developed on smaller scales. Utilizing pre-constructed corpora will yield greater efficiency in file carving. Although corpora built by examiners is ideal in continuing to expand research across labs, this has proven repeatedly to be time consuming, spanning anywhere from several months to several years. The use of currently established corpora constructed by a reputable scientific body, such as NIST, will allow for a greater number of carving studies to be conducted, as well as more opportunities for researchers to compare results. Lastly, in developing smaller scale studies, researchers should always take into account size, focusing on a select type of media in a small range upon which to conduct studies.

Solid-state Drives

Improved validation and verification techniques must not only grow, but also expand outside of testing on traditional media. While studies on traditional hard disk drives (HDDs) are still relevant, HDDs are slowly becoming obsolete. Consequently, they are gradually being replaced by another form of media-solid-state drives (SSDs). The hard disk drive has been around since the early days of computing (Pierce, 2010, p. 1). Due to the uniqueness of its storage capabilities, in regard to capacity and speed when compared to earlier storage devices, it has managed to keep pace with evolving industry standards up to now. As consumers' needs have continued to change, there has been a constant demand for faster, smaller, more reliable storage devices. This is where the solid-state drive (SSD) comes into play. The main difference between SSDs and HDDs is the parts contained therein.

While there are many things that distinguish SSDs and HDDs from one another, the most noticeable is the lack of moving parts among solid-state drives. HDDs enlist the use of a head mounted on an actuator arm to access rotating magnetic storage media (Cornwell, 2012, p. 59). While the platters spin, digital data is being written and read. Data on hard disk drives is typically stored sequentially and accessed in any order. Because of this, individual blocks of data stored on hard disk drives can be retrieved in any order. Although HDDs provide a wealth of storage space, these moving parts have rendered them more and more unreliable among the years. Often times when consumers complain of devices having "crashed," it is a mechanical failure. These can include the actuator arm coming in contact with the platters, the alignment being off, or the circuitry wearing out over time.

As a result, many people believe it is time for the industry to direct their efforts toward a more reliable mass storage media, such as solid-state drives (Pierce, 2010, p. 1). With solid-state

drives, there are no moving parts; hence the “solid-state” title. They employ the use of flash memory for data storage. Flash memory is non-volatile, often performing with the use of NAND flash, where power is not required to retain data. Flash memory can also be written byte for byte and must be erased several blocks at a time before it can be re-written. Most multimedia devices used today-cell phones, digital cameras, laptops, and more- use NAND flash (Breeuwsma, de Jongh, Klaver, van der Knijff, and Roeloffs, 2007, p. 1).

As demand for SSDs continues to increase, so must testing on these types of devices. SSDs have already begun to appear as evidence in forensic labs and have proven to be an entirely new set of problems for examiners. One such example is the wear leveling feature found among SSDs. Wear leveling is used in solid-state drives to determine what block data will be written to next, different from hard disk drives in which data is written sequentially. Wear leveling involves constantly rearranging pages and blocks of data in order to extend the flash lifetime of the drive (p. 2).

Garbage collection is another feature common to SSDs. Solid-state drives are structured to write new information to available blocks rather than in sequential order. Since data can only be written to empty blocks, the drive is tasked with maintaining these empty segments (Conwell, 2012, p. 62). Flash memory is divided into blocks, and those blocks are subsequently divided into pages. As a result, only entire blocks can be erased. In turn, if that space is needed, the data in those blocks must first be copied and moved to new blocks and pages. This results in the drive, rather than the user moving data from one location to another, which is essential for examiners to understand when analyzing SSDs through file carving techniques. Research surrounding SSDs and their functions has increased, but there is still little known on the rate and frequency these tasks occur on SSDs. Breeuwsma et al. (2007) note that there are similar affects

when mobile devices are powered on and off, resulting in changes in data. From this they advise, as a rule of thumb, to keep the number of power cycles to a minimum when utilizing SSDs in data recovery studies.

Summary

These studies show there is a need to continue to direct efforts toward greater research on SSDs. Technology has no signs of slowing down, and while examiners may still encounter a larger number of HDDs in the lab today, it is clear that the industry is continuing to make a gradual shift toward the enlistment of SSDs to meet consumer demand. Accordingly, developing file-carving studies that utilize forensic corpora on solid-state drives will contribute to current knowledge on SSD analysis, as well as encourage increased studies and training. This will require collaborative efforts in building reliable corpora, pushes for standardization across the discipline, and an essential understanding of how our current tools function as well as how they can improve.

Chapter 3

Methodology

This study focused on the application of file-carving using Access Data Forensic Tool Kit (FTK) v. 6.0 in carving forensic corpora on solid-state drives (SSDs). The following research questions were addressed in the study:

1. Does FTK's data carving function perform as intended and recover all possible data when used on SSDs?
2. Does FTK's data carving function ability vary depending on the size of the drive?
3. Does FTK's data carving function ability vary depending on file type?

This study utilized the process section from the Scientific Working Group on Digital Evidence (SWGDE) Recommended Guidelines for Validation Testing, Version 2.0 (2014). Forensic corpora were obtained from NIST's CFTT project, consisting of graphic, document, archive, audio, and video files. Of the corpora obtained from NIST, four levels were utilized, ranging from Level 0 (L0) to Level 3 (L3). The levels of corpora each varied in structure and status (i.e. complete, partial, fragmented, etc.). Prior to the corpora being placed on the drives, each solid-state drive was forensically wiped, ensuring no residual data remained on the drive. Each data set was then restored to each of three SSDs in the study and subsequently carved using FTK. FTK's carving function was directed to carve for the specific file types and recover each item within the respective image. In measuring the recovery rate, the tool was graded on a pass/fail scale, in which the recovery of the data in full from the correct location warranted a pass, and all other results warranted a fail. The occurrence of false negatives and positives was also noted during the course of the study.

Setting

The solid-state drives were forensically wiped using a freestanding forensic duplicator in the University of Central Oklahoma Digital Forensics classroom. Once wiped, a “blank check” was performed using the same tool to ensure that all data had been wiped from each drive, wherein the result yielded a sum of zero. The corpora sets were then restored to each SSD using a hex editor tool located on the classroom computers. Once restored, each drive was then imaged using a disk-imaging program and saved to be used later for carving.

Sample

The sampling procedure used by the researcher in this study was convenience sampling. The forensic corpora test images used in this study was limited to corpora sets previously developed by the CFTT project and made available for use by other researchers. A total of 30 test images were developed. This included five file types and six different levels. For this specific study, a total of 20 images were selected for use. These still included all five file types, but only levels zero through four. These test images were selected given they were highly representative of the type of data encountered during digital forensics investigations.

Each test image contained no more than 10 files of a specific file type. An image layout was provided for each test image, detailing the file size, starting sector, and ending sector. The naming convention for the test images were FILESYSTEM_LEVEL_FILETYPE.dd.bz2. For example, FAT_L0_Graphic.dd.bz2 identifies a Level 0, Graphic test image with a FAT 32 file system. This means the test image was developed using a file allocation table (FAT) file system, contains non-fragmented graphic files (Level 0), and contains JPG, PNG, BMP, GIF, TIF, and PCX file types. The levels enlisted are described below (Table 1):

Table 1

CFTT Test Image Data Levels and Descriptions

Level	Description	Content
Level 0	Cluster padded	contiguous files with assorted levels of content ranging in size from 1, 2, 4, 8, 16, ...128 sectors
Level 1	Fragmented in order	contiguous and sequential fragmented files with content separating the files
Level 2	Fragmented out of order	contiguous and disordered fragmented files separated by other content
Level 3	Incomplete	contiguous and partial (i.e., only a portion of the file is present) files

The test image categories and the file extensions of the file items contained therein are listed in Table 2. The file signatures for each of the listed extensions are utilized by FTK in locating and carving their respective data. See Appendix A for a complete list of all test images utilized, including file system information, file types, and descriptions).

Table 2

CFTT Test Image Types and File Types

Image Type	Images	File Types
Graphic	FAT_L0_Graphic.dd.bz2 FAT_L1_Graphic.dd.bz2 FAT_L2_Graphic.dd.bz2 FAT_L3_Graphic.dd.bz2	JPG,PNG,BMP,GIF,TIF,PCX
Document	FAT_L0_Document.dd.bz2 FAT_L1_Document.dd.bz2 FAT_L2_Document.dd.bz2 FAT_L3_Document.dd.bz2	DOC, XLS, PPT, PDF
Archive	FAT_L0_Archive.dd.bz2 FAT_L1_Archive.dd.bz2 FAT_L2_Archive.dd.bz2 FAT_L3_Archive.dd.bz2	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
Video	FAT_L0_Audio.dd.bz2 FAT_L1_Audio.dd.bz2 FAT_L2_Audio.dd.bz2 FAT_L3_Audio.dd.bz2	MP4,AVI,MOV,FLV,MPG,WMV
Audio	FAT_L0_Video.dd.bz2 FAT_L1_Video.dd.bz2 FAT_L2_Video.dd.bz2 FAT_L3_Video.dd.bz2	MP3,WAV,AU,WMA

Materials

The independent variables measured by this study consisted of size, level, and file type. A total of three Samsung 850 EVO solid-state drives were used, including a 120 GB, 250 GB, and 500 GB size drive. The component of size variation was included to assess FTK's carving ability when carving the same file across drives of different sizes. Test image levels zero through three involved FTK carving similar files, but in different states; where some files were contiguous and complete, more representative of what would normally be encountered during

analysis, while others were partial and fragmented, illustrative of data recovery in cases where files may have been intentionally deleted or destroyed. Lastly, the inclusion of assorted file types allows for comparison of the carving success rate across common file categories.

The dependent variable measured by this study consisted of FTK's carving function and whether it carved or did not carve the data in question.

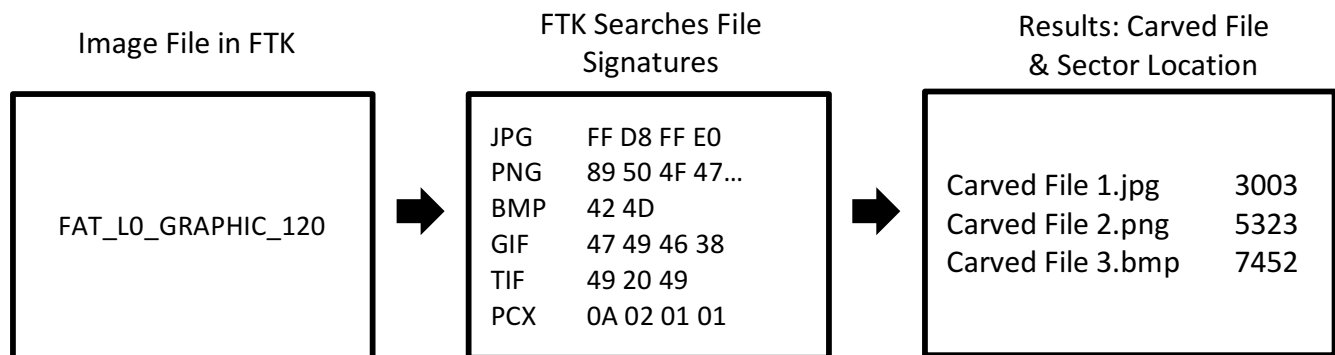
A Tableau TD2 Forensic Duplicator was used to forensically wipe each hard drive prior to data being placed on them. The duplicator was also used to hash the device to ensure that no data was left on the device. Any result greater than one indicated that the drive was not blank, which would be confirmed by a return of zero. Once the drives were confirmed to be blank, the test image in question was restored to the drive. During restoration, the image was copied to the drive in the same format as its original structure. This was completed using WinHex v. 16.5, a disk editor tool. The image was opened and restored to the drive in its original format, wherein the imaging process started at offset zero on the blank drive, and each sector consisted of 512 Megabytes. Images were restored one at a time. Once complete, the drive to which the test image was restored was connected to a Tableau Forensic SATA/IDE Bridge [T35u] to prevent data from being written to the drive while connected to the forensic class computer. The drive was forensically imaged through Access Data FTK Imager v 3.4.2.6, a standalone disk-imaging program included in the FTK tool suite. In addition to imaging the drives, Imager was also directed to verify each image, providing a hash value at the end of the imaging process to ensure the contents of the test image had not been changed or altered following restoration. Image files were saved using the naming convention FILESYSTEM_LEVEL_FILETYPE_DRIVESIZE.dd and processed as raw "dd" files. The steps listed were repeated for each test image on each of the three SSDs. Images were restored one at a time and saved to an external hard drive until carving

was performed. It should also be noted that during restoration and imaging, each drive underwent an average of two to three power cycles.

Measurement

Once all test image files were restored and imaged to each of the three solid-state drives used in this study, the images were prepared for carving. A case file was created for each image file in Access Data FTK v. 6.0 on a Digital Intelligence Forensic Recovery of Evidence (F.R.E.D.) computer. Once the case file was created, the image file was added as evidence into FTK. After the image file was loaded, the automatic carving function of FTK was directed to carve for the respective file types. If the extension types were not present when initiating automatic carving, a custom carver was created. The custom carver function is a pre-installed feature in FTK, in which, custom carvers can be created using file signatures. Carvers that were not initially available were added into FTK. The carving function then searched the image file for the file signatures of each carver and returned the carved results. The returned results were assigned an item number, a name (typically Carved [#]), and the location from which the specific data was carved. A stepwise example is listed below (Figure 1).

Figure 1. FTK File Carving Example.



Among examiners across the discipline, the efficiency of FTK's carving function is presumed to be very high. The accuracy rate will vary depending on file. Such behavior was noted in the 2014 CFTT project study, where the tool was only able to retrieve certain graphics files. Differences in accuracy may also be witnessed when comparing files of different structures, i.e. complete versus partial, or fragmented versus non-fragmented. Lastly, some studies have noted that FTK has been known to report false positives (Laurenson, 2013).

Data Collection

The data was collected and recorded based on the items carved by FTK during each case. The image layouts displayed the files within each test image. Since the data used was standardized corpora, each test image layout provided the file name, file size, starting and ending sector (see example, Figure 2).

Figure 2. Image Layouts Example.

FAT_L0_Graphic.dd drive layout			
File	File Size	Start Sector	End Sector
Fill	5 120 000	303	10 302
000_0021.png	12 966 639	10 303	35 628
Fill	5 120 000	35 631	45 630
02010025.pcx	806 664	45 631	47 206
Fill	5 120 000	47 207	57 206
02010026.jpg	61 038	57 207	57 326
09260002.jpg	60 716	57 327	57 445

Once carving was completed for the file, the results were recorded for each file item. The carving function was graded on a pass/fail scale for each item within each test image with regard to whether the data was accurate and carved from the correct sector (location). The scale ranged from 0 to 2 (Table 3), in which a pass was noted as 0 and all other numbers were noted as a fail.

Table 3

File Carving Results Measurement Scale

Score	Response
0	No data was carved in relation to the specific file item
1	Data was correct, carved from correct location
2	Correct data was carved from wrong location

A spreadsheet was created for recording purposes. Each tab was representative of a different test image file, listed in Table 2. Results were recorded for each carving test in separate columns in correspondence to their respective SSDs. While conducting carving, several instances arose where FTK reported false positives. With these particular false positive cases, FTK reported files that were not the original files and did not correspond to a specific sector listed in the test image layouts, but were identified by FTK with a specific file extension. In these cases, the overall file carving were results were still recorded using the scale described in Table 3. False positives however, were noted with a 1 in parentheses next to the corresponding file signature (see example, Figure 3). Following the completion of file carving, the results were reformatted into one spreadsheet for quantitative purposes (see Appendix B for a complete list of recorded file carving results).

Figure 3. Recorded File Carving Results.

File	120 GB	250 GB	500 GB
000_0021.png	1	1	0
02010025.pcx	1	1	0
02010026.jpg	1	1	0
09260002.jpg	1	1	0
100_0304crop.bmp	0	0	0
100_0018.tif	0	0	0 (1)
100_0183.gif	0	0	0

Data Analysis

The file carving results were categorized in terms of the research questions. The data was recorded noting size, file type, and level. The results were summarized, where the percentages of carved, non-carved, and incorrectly carved data were calculated and analyzed by drive size, file type, and file level. Chi-square tests were also performed to test for the differences in the percentages of files carved correctly in regard to SSD size, file level, and file type.

CHAPTER 4

Results

Three sizes of solid-state drives (120 GB, 250 GB, 500 GB), four levels of files (cluster padded, fragmented in order, fragmented out of order, incomplete), and five types of forensic images (archive, audio, document, graphic, video) were considered in this experiment. In all, data carving was attempted for 690 files. For each file there were three possible outcomes (carved data correctly, carved data but not the correct file, did not carve data). Summary statistics for size, level, and type are presented in Figures 4 through 5.

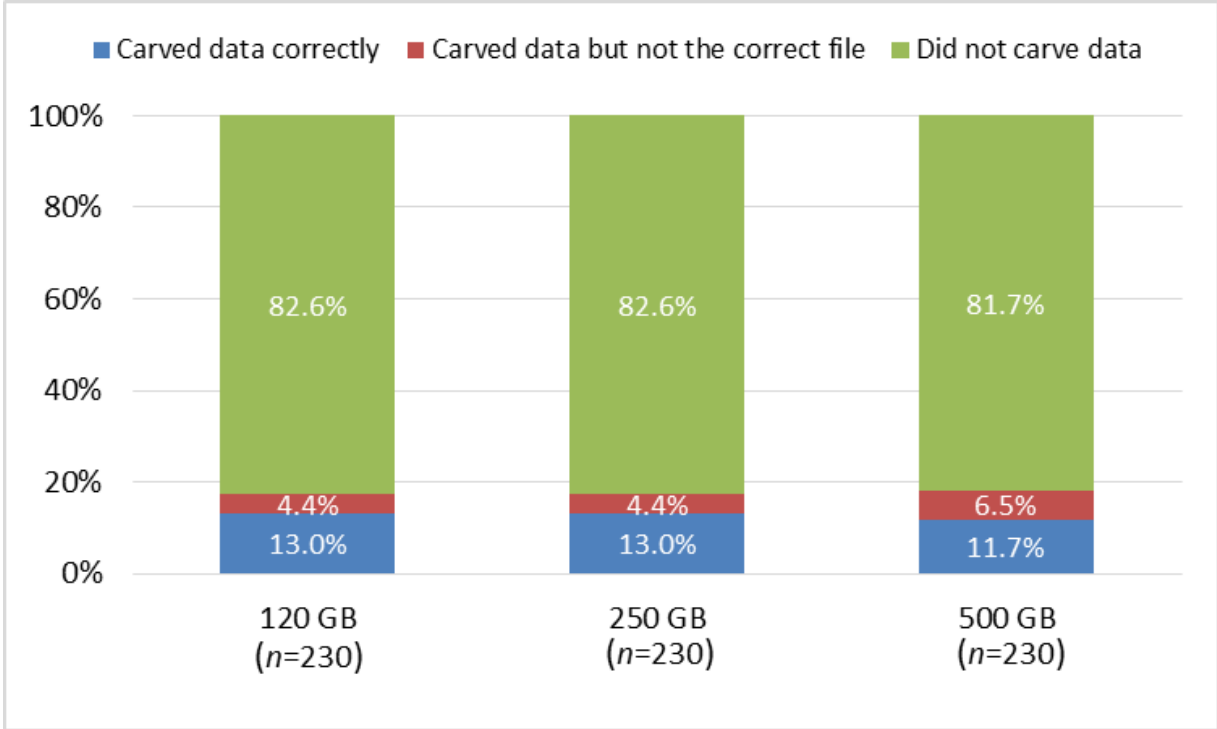


Figure 4. Summary statistics of data carved by SSD Size.

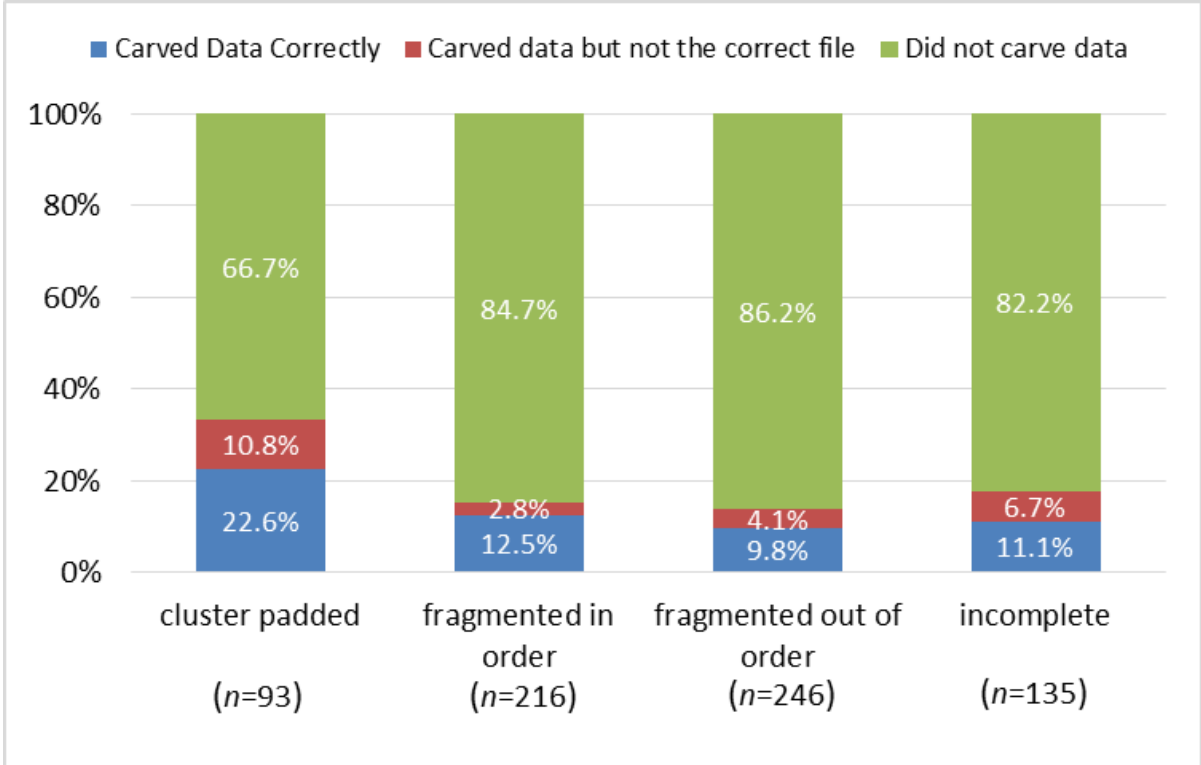


Figure 5. Summary statistics of data carved by test image level.

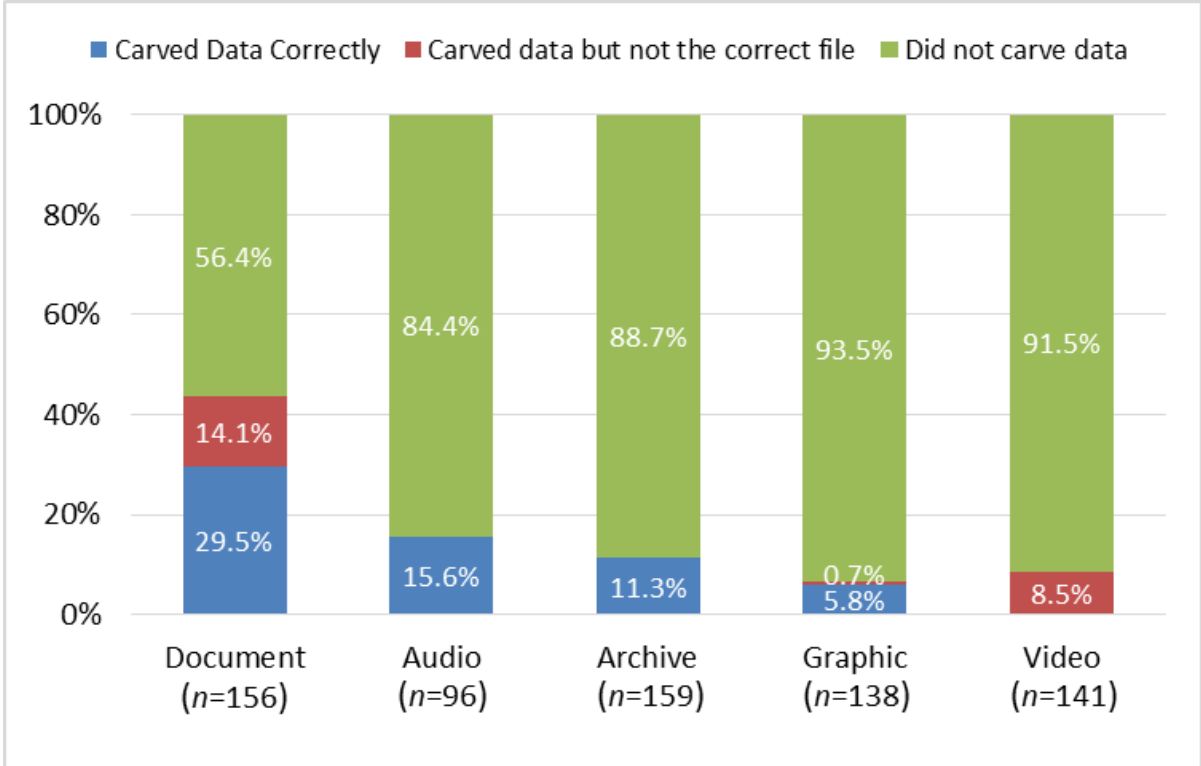


Figure 6. Summary statistics of data carved by file type.

File Carving Analysis

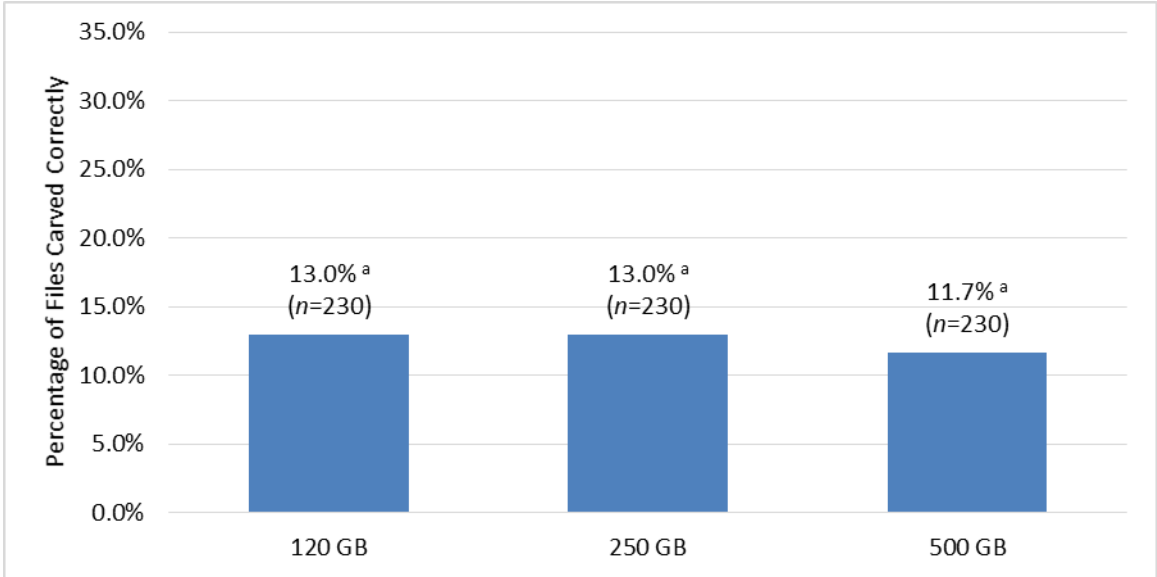
The following statistical analysis focused primarily on the test image files which were carved correctly. Chi-square tests were utilized given that the expected results in this study, where it was expected that FTK would recover data at a relatively high rate, were in turn compared to the actual outcomes of the files carved, which lacked a normal distribution and presented the need for non-parametric testing. Chi-square tests were performed to test for differences in the percentages of files carved correctly for the different sizes, levels, and types. P-values less than 0.05 were considered to be significant. Significant chi-square tests were followed by pairwise chi-square tests (with no adjustment for multiplicity) to determine specifically which size(s), level(s), and/or type(s) was significantly different.

The file types were further broken down by file extension. Within each file type, chi-square tests were performed to test for differences in the percentages of files carved correctly for the different file extensions.

For any chi-square test, if the sample size was too small for a valid test, Fisher's exact test was performed instead. P-values marked with an (F) indicate the use of Fisher's exact test rather than the chi-square test. All statistical tests were performed in SAS v. 9.4.

File Carving Results by Solid-state Drive Size

There were no significant differences in the percentages of files carved correctly for the different solid-state drive sizes ($\chi^2 = 0.24$, $p = 0.888$). The results of the chi-square test for size are displayed in Figure 7.

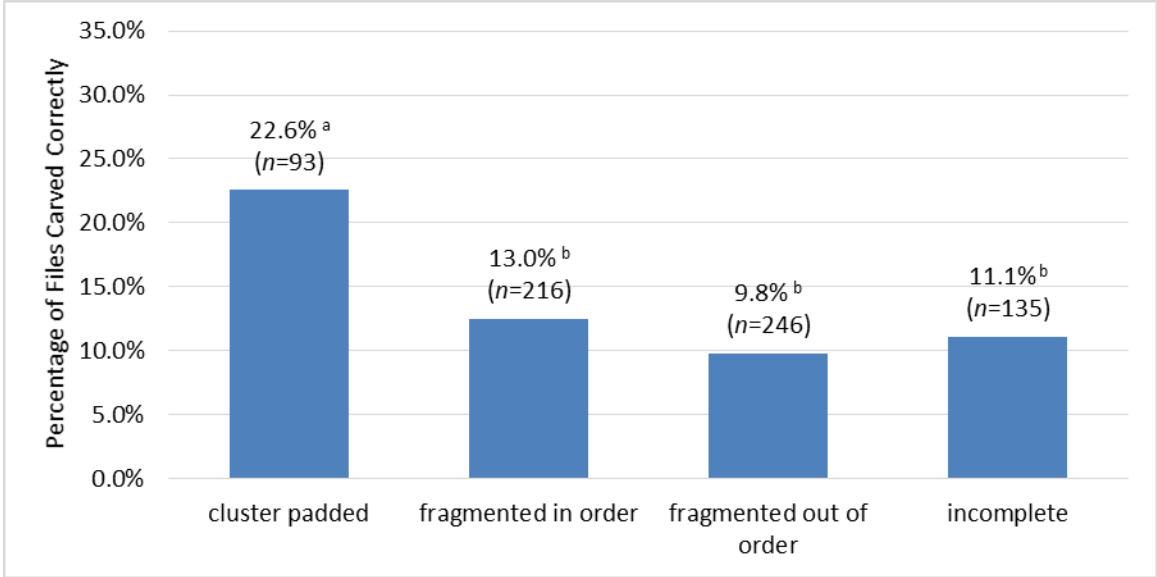


^a Percentages marked with the same letter are not significantly different at the 0.05 level.

Figure 7. Percentage of files carved correctly by solid-state drive size.

File Carving Results by Test Image Level

There was a significant difference in the percentages of files carved correctly for the different levels of files ($\chi^2 = 10.49$, $p = 0.015$). The results of the chi-square test for level are displayed in Figure 8. Specifically, the odds of correctly carving a cluster padded file are 2.35 (95% CI: 1.35, 4.06) times greater than the odds of correctly carving any of the other file levels. There were no other significant differences among the levels.

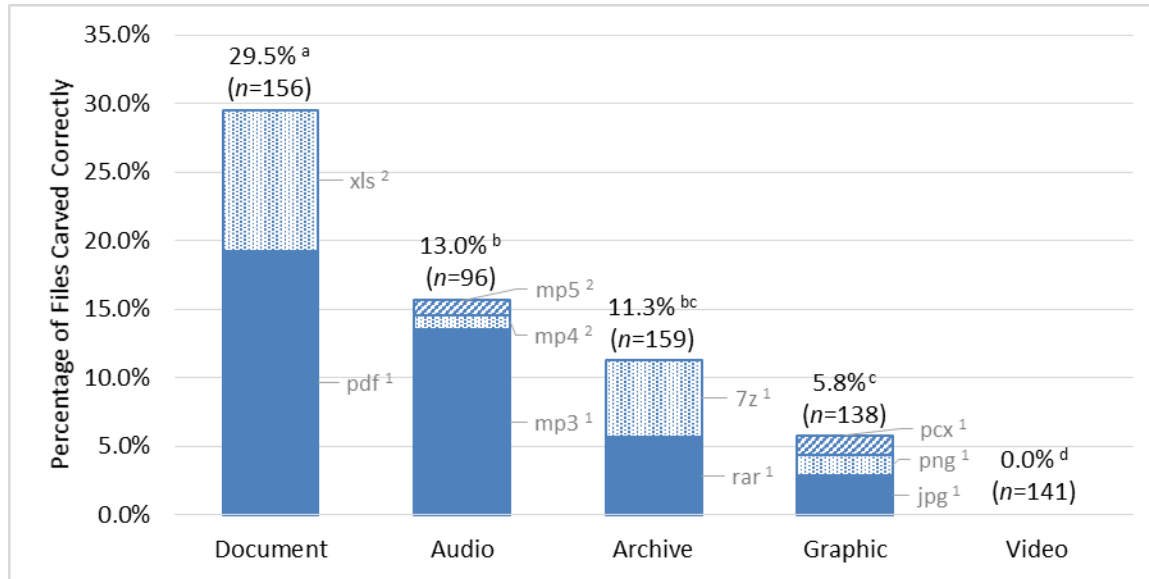


^{a,b} Percentages marked with the same letter are not significantly different at the 0.05 level.

Figure 8. Percentage of files carved correctly by file level.

File Carving Results by File Type

There was a significant difference in the percentages of files carved correctly for the different file types ($\chi^2_4 = 67.52, p < 0.001$). The results of the chi-square test for file type, as well as file extension, are displayed in Figure 9. Specifically, the odds of correctly carving a document file are 5.03 (95% CI: 3.15, 8.04) times greater than the odds of correctly carving any of the other file types.



^{a,b,c,d} Percentages marked with the same letter are not significantly different at the 0.05 level.

^{1,2} File extensions, within the same bar, marked with the same number are not significantly different at the 0.05 level.

Figure 9. Percentage of files carved correctly by file type.

The file types were further broken down by file extension. For document files, there was a significant difference in the percentages of pdf and xls files that were carved correctly ($\chi^2_1 = 3.96$, $p = 0.047$). Specifically, the odds of correctly carving a pdf file are 2.32 (95% CI: 1.01, 5.36) times greater than the odds of correctly carving an xls file. None of the doc and ppt files were carved correctly.

For audio files, there was a significant difference in the percentages of mp3, mp4, and mp5 files that were carved correctly ($\chi^2_2 = 26.94$, $p < 0.001(F)$). Specifically, the odds of correctly carving an mp3 file were 47.17 (95% CI: 7.65, 294.12) times greater than the odds of correctly carving an mp4 or mp5 file. None of the au, wav, and wma files were carved correctly. For archive files, there was no significant difference in the percentages of rar and 7z files that were carved correctly ($\chi^2_1 = 0.14$, $p = 0.714$). None of the bz2, gz, tar, wim, and zip files were carved correctly.

For graphic files, there was no significant difference in the percentages of jpg, png, and pcx files that were carved correctly ($\chi^2 = 1.07$, $p = 0.579(F)$). None of the bmp, gif, and tif files were carved correctly.

CHAPTER 5

Discussion

Government bodies and scientific committees alike have continued to push for improvements within forensic science. Digital forensics has been no exception, in that it has been noted as a discipline in which many of the practitioners are undertrained (National Research Council, 2009) and a great deal of emphasis is placed more so on investigative procedure rather than science. In strengthening digital forensics, there has become a clear need for greater research to bring the discipline in line with other areas of forensics. This challenge requires not only research that focuses on current problems, but studies geared toward standardization and improving tools in the future.

Various bodies have begun laying the groundwork for future research in an attempt to acquire a better picture of the reliability of commonly used forensic tools. As discussed earlier, there has been minimal research surrounding standardization methods in the field. This has influenced researchers to explore the possibilities of forensic corpora and how it can be utilized to expand on current digital research. More specifically, we have begun to enlist forensic corpora in validating common tools.

The purpose of this quantitative study was to extend the research on file carving, focusing particularly on Access Data FTK's file carving function through the application of forensic corpora. This study also sought to test file-carving reliability when used on solid-state drives, in comparison to accuracy rates on traditional hard disk drives. Lastly, this study looked to review the usefulness of standardized corpora in research studies and the ways in which it could possibly contribute to further progression in the field. Previous research in relation to file carving with the use of forensic corpora on solid-state drives is limited; therefore, this study was

to fill a gap and provide a foundation for future studies on file carving validation and its relation to SSDs.

Discussion

Overall, FTK's file carving function performed poorly when carving the test images from the solid-state drives. A large number of false negatives were experienced across every category. In these cases, the data was sets were present in the test image, but FTK did not carve the particular file item. When analyzing the carved data in regard to size, the percentage of false negatives was slightly lower (approx. 0.9%) on the 500 GB drive than on the other drives, but not significant. However, the 500 GB drive did experience a higher percentage of false positives in comparison to the 120 GB and 250 GB drives, where data was carved, but the data was not the correct file.

In regard to level, FTK's carving function performed most efficiently when carving data from Level 0 (cluster padded, contiguous) test images. The tool recovered the most data when carving on this level, with at least a 10% difference between Level 0 and the remaining levels. Level 0 also resulted in the highest number of false positives, and the lowest number of false negatives. Finally, the carving results varied across file type. The document test images produced the highest number of correctly carved test images, but also the highest number of false positives. The audio and archive test images yielded no false positives, but also yielded correctly recovered files at a lower rate than the document test images. In reviewing all the file types, the tool performed exceptionally poor on the video test images, recovering no files at all.

The percentage of correctly carved files were also analyzed individually based on drive size, test image level, and file type. The carving function performed marginally better when

applied to the 120 GB and 250 GB drives than when assigned to carve on the 500 GB. This resulted in only a 1.3% difference between the SSDs. Similar to the summary statistics touched on in the previous paragraph, the tool was most effective when carving cluster padded, contiguous (Level 0) files. Lastly, when viewing file type, it was noted that the odds of correctly carving a document file are a little over 5 times greater than the odds of correctly carving other file types. When further broken down by file extension, some file items showed a higher percentage of being carved than others. Testing found that the odds of correctly carving a pdf file was 2 times greater than the odds of correctly carving an xls file. Most significant was among audio files, where the odds of correctly carving an mp3 file was 47 times greater than the odds of carving an mp4 or mp5.

From these results, it is evident that FTKs carving function performs well below the presumed accuracy rate (100%) when utilized on solid-state drives. The results also display that the tool's overall accuracy does not vary across drive size. The tool does however, perform more efficiently on contiguous, non-fragmented files as well as with document files.

During the file carving process, we failed to witness any false positives in which the correct data/file was carved from the wrong location. We initially expected this to be the case with various files across all the solid-state drives given that SSDs enlist the use of garbage collection, in which files are deleted and moved by the drive to save space and ultimately increase write performance. This may have been the result of several contributing factors.

It was noted that garbage collection occurs across power cycles. As such, researchers have recommended keeping the total number of power cycles low when conducting carving on SSDs. In this study, the drive experienced an average of two to three power cycles between restoration and imaging. In addition, once the test image had been restored to the solid-state

drive, forensic imaging was started almost immediately. While being imaged, the SSDs were connected to a write blocker, rather than the computer itself. This would have prevented any new data from being written to the drive. In reviewing these steps, the drives simply may not have been presented with an opportunity to interact with other files and experience an above average number of power cycles. As a result, there may not have been a need for the drive to utilize the built in garbage collection feature, and as a result, no files were moved from their original location.

One unexpected occurrence experienced during testing was a somewhat high number of false positives. While FTK had been noted in other studies as reporting some false positives, we initially expected to receive a higher number of false positives similar to those discussed in the previous paragraph. Again, the false positives that were recorded in this study were reported by FTK as a file with a specific file extension. Upon opening these files and reviewing the Hex data, they did not contain any of the file signatures that corresponded with the extension assigned by FTK. For example, if FTK presented a carved file with a Bitmap (.bmp) extension, the file signature *0x 42 4D* would be present within the file. However, when files like these were opened and searched, the file signature would not be present within the carved data at all. Typically, in cases such as these, the data contained in the carved file would be all zeros. As of now, we have been unable to determine exactly what contributed to such poor results.

Overall, using the corpora provided by the NIST's CFTT project was straightforward. The data sets were easy to access via the CFTT website. The test image files fit easily onto smaller drives, which made moving and restoring the images from different devices much smoother. The provision of image contents and layouts for each of the image files also helped in data analysis. Having access to the size and locations of the files prior to and during testing made

the process of carving and subsequently recording results much more streamlined. The ease of use and accessibility of these data sets ultimately support forensic corpora's usefulness in conducting digital forensics studies. It also supports the need for the development of further forensic corpora that can in turn be made available to the scientific community, leading to increased standardization and greater reproducibility.

Limitations

Several limitations to this study were noted early on. Again, this study is limited in that it only focuses on the function of FTK's file carving tool. While other studies may garner similar results, there is a strong possibility results will differ from those obtained in this study due to changes in programs, operating system, and tools used. The issue of limited data has also been addressed. It is essentially impossible to create a data set that incorporates every scenario an examiner may encounter, therefore, extensive and representative corpora must be relied upon.

While this study included a large range of tests, it proved to be extremely time consuming. This was previously identified as an issue experienced by other examiners. The imaging times following the restoration of the test images to the drives varied, dependent upon both content and drive size. The majority of the time, the largest drive, the 500 GB SSD, took the greatest amount of time for imaging and verification to be completed. The longest imaging and verification time in the study was recorded around a total of 28 hours.

Issues were also experienced restoring the test images to the drives at the beginning of the study. Initially, we attempted to complete both the restoration and imaging processes through FTK Imager. Imager would not recognize the drives if there was no data or the drive was not formatted. However, early on, it was decided to restore the test images to drives without file

systems already present to prevent any data being present on the drive prior to restoration, and possibly interfering with file carving. Imager also would not allow the disk to physically be edited. As a result, WinHex was used to restore each test image to the drives, ensuring the image structures were formatted the same as the original image files.

Space was another issue faced during this study. While the image files themselves were small, once restored to the drives, more space was needed. The forensic images of the drives were saved as raw/dd images. These are essentially “flat” images where no compression is performed. Consequently, each image that was created was around the same size as the source SSD (ex. 500 GB SSD= 465 GB.dd image). Following the first several rounds of imaging, the computers to which the drives were being imaged quickly ran out of space. To free up space for further imaging, all images were compressed (following imaging completion). This added yet more time to the overall imaging process. A five Terabyte external hard drive was later invested in, to which the images were saved until later decompressed for carving purposes.

Collecting the data in FTK was also tedious. Prior to executing file carving, the image must be loaded into the FTK case file. This process alone took anywhere between four and eight hours. Once the image was loaded, the completion of file carving by FTK took an average of four to eight hours as well. In total, 20 test images were restored to each of the three SSDs, and a total of 60 forensic images were created. The results yielded a total of 690 files to be recorded following file carving. Lastly, a total 17,400 GB (17.4 TB) of data were utilized throughout the course of this research. In summary, this study involved massive amounts of data, which if expanded upon to include more files and drives, could prove overwhelming for one individual. The same can be said of forensic corpora, where the development of data sets would prove most effective when produced through collaborative efforts.

Recommendations for Future Research

In future studies, it is recommended that researchers be aware of the amount of data that will ultimately be analyzed prior to developing their research plan. For students and others on the university level, smaller scale studies may serve as a more effective starting point. Focusing on specific features and smaller sets of data may provide more time to complete analysis and better understand improvements that can be made to future studies.

For those that wish to expand on this study, it is suggested that different drives be used. The field could benefit from studies such as this one being performed on larger solid-state drives, as well as drives of different brands. This would continue to support the development of a baseline in understanding file-carving capabilities on solid-state drives, as well as if these capabilities are impacted by other factors such as brand and size. It is also recommended that researchers allow the drives used in their study to experience multiple power cycles and interact with other file systems and file types. This would prove more representative of the state of SSDs received for analysis in the lab and possibly allow those in the field to more closely analyze the garbage collection and wear leveling functions enabled in SSDs.

Concerning time consumption in studies such as these, researchers would benefit from using a forensic computer similar to F.R.E.D. While the images in this study were created using standard classroom computers, the carving was conducted using F.R.E.D. The use of such computers would most likely yield lower imaging times, as these machines often possess faster processors and are built for the specific purpose of running forensic programs such as FTK. A forensic machine may also solve the issue of space, as most are built at a much larger capacity than regular desktop computers and can hold numerous terabytes of data. Lastly, the field can

also benefit from direct comparison studies, in which the same images and carving techniques are applied to both traditional hard disk drives and solid-state drives and the results compared.

Conclusion

Three major conclusions can be drawn from this study. The first conclusion is that this particular file-carving tool does vary in performance across devices. Second, the file carving function, when applied to SSDs, is somewhat influenced by both file type and level. Lastly, forensic corpora can serve as a useful tool in effectively conducting a file carving study.

The first conclusion is that Access Data FTK's file carving function performs significantly worse on solid-state drives than on traditional hard disk drives. While the results may not be desirable, this data shows there is a need for vendors to improve upon current file carving tools and features. It further reaffirms the indication that the handling and analysis of SSDs must be approached differently than that of traditional HDDs. Once again, SSDs have become more prevalent and are slated to eventually replace HDDs altogether. Continuing to develop studies, which focus on SSD analysis, will eventually contribute to the development of better training and a greater understanding of SSD structure and function by practitioners.

Next, the results of this study provide further details as to whether the carving tool is influenced by varying factors, including drive size, file type, and file level. Being that the carving function recovered more files depending on file type and level, this is another factor that should be taken into consideration when examiners are conducting analysis. The areas in which the tool performed poorly (fragmented files, partial files, images, etc.) are strongly representative of the type of evidence that may be received during an investigation. The fact that solid-state drives continue to become more prevalent displays that, while file carving tools such as FTK are

useful, examiners should continue to supplement these tools with their own analysis in order to recover all possible data. Doing so requires physically looking through data, and carving evidence items manually.

This study ultimately supports the need for more forensic corpora. The data sets utilized during testing truly allowed for the analysis of a broad range of factors, helping identify current gaps in FTK's carving function and better understand the areas in which the tool can improve. The use of established bodies of corpora can also prove beneficial in the future for researchers who wish to expand on studies similar to this one. While building corpora is a tedious and time consuming task for researchers, the benefits of making these data sets available to the research community can contribute to increases in validation studies, greater collaborative efforts among examiners and scientific organizations, and improved trustworthiness in digital evidence.

In conclusion, while the tool used in this research was able to perform, the results showed that examiners relying solely on these functions could potentially be missing significant evidence. This is of great concern, given that a great deal of digital forensics investigations involve analysis during criminal cases. It is not enough to assume that a tool is functioning as intended, citing the need for validation and verification studies. In order to deliver the best possible report, examiners may have to continue to rely on manual carving and see the tool as a supplement. Accordingly, examiners must continue to reaffirm the discipline's basis in science, understanding their tools' limitations and also continuing to push for improved practices in digital forensics. Establishing large scale change can often be a slow-moving process, but beginning to hold each other accountable as practitioners through advanced research practices is an excellent place to start.

References

- Breeuwsma, M., de Jongh, M., Klaver, C., van der Knijff, R., & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory. *Small Scale Digital Device Forensics Journal*, 1 (1), 1-17.
- Cohen, M.I. (2007). Advanced carving techniques. *Digital Investigation*, 4, 119-128.
- Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council (2009). *Strengthening Forensic Science in the United States: A Path Forward*.
- Cornwell, M. (2012). Anatomy of a Solid-State Drive. *Communications of the ACM*, 55 (12), 59-63.
- Editorial. (2006). Moving forward in a changing landscape. *Digital Investigation*, 3, 1-2.
- Executive Office of the President, President's Council of Advisors on Science and Technology (2016). *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods*, 1-160.
- Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7S, S64-S73.
- Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, 6, S2-S11.
- Guo, Y., Slay, J., Beckett, J. (2009). Validation and verification of computer forensic software tools-Searching Function. *Digital Investigation*, 6, S12-S22.
- International Organization for Standards. (2010). ISO Catalogue. ISO 17025.
- Laurenson, T. (2013). Performance Analysis of File Carving Tools. *IFIP Advances in Information and Communication Technology*, 405, 419-433.
- National Institute of Science and Technology. (2014). *FTK v4.1: Test Results for Graphic File Carving Tool*, 1-12.
- Pierce, A. The Emergence of the Solid-State Drive. *Tech Directions*, 19 (8), 12-13.
- Yoo, B., Park, J., Lim, S., Bang, J., & Lee, S. (2012). A study on multimedia file carving method. *Multimedia Tools Appl*, 61(1), 243-261.
- Roux, B., & Falgoust, M. (2012). Ethical Issues Raised by Data Acquisition Methods in Digital Forensics Research. *Journal of Information Ethics*, 21(1), 40-60.

Scientific Working Group on Digital Evidence. (2014). *SWGDE recommended guidelines for validation testing* (Version 2.0). 1-22.

Wilsdon, T., Slay, J. (2005). Digital Forensics: Exploring Validation, Verification & Certification. *SADFE '05*, 1-8.

Appendix A: File Carving Test Images

- **NIST /CFTT Test Images**

Table 1: File Carving Test Images

Image	Description	File Types	File System
FAT_L0_Graphic.dd.bz2	Non-fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX	FAT32
FAT_L1_Graphic.dd.bz2	Sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX	FAT32
FAT_L2_Graphic.dd.bz2	Non-sequentially fragmented graphics files	JPG,PNG,BMP,GIF,TIF,PCX	FAT32
FAT_L3_Graphic.dd.bz2	Graphics files with missing fragments	JPG,PNG,BMP,GIF,TIF,PCX	FAT32
FAT_L0_Document.dd.bz2	Non-fragmented document files	DOC, XLS, PPT, PDF	FAT32
FAT_L1_Document.dd.bz2	Sequentially fragmented document files	DOC, XLS, PPT, PDF	FAT32
FAT_L2_Document.dd.bz2	Non-sequentially fragmented document files	DOC, XLS, PPT, PDF	FAT32
FAT_L3_Document.dd.bz2	Document files with missing fragments	DOC, XLS, PPT, PDF	FAT32
FAT_L0_Archive.dd.bz2	Non-fragmented archive files	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP	FAT32
FAT_L1_Archive.dd.bz2	Sequentially fragmented archive files	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP	FAT32
FAT_L2_Archive.dd.bz2	Non-Sequentially fragmented archive files	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP	FAT32
FAT_L3_Archive.dd.bz2	Archive files with missing fragments	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP	FAT32
FAT_L0_Audio.dd.bz2	Non-Fragmented audio files	MP3,WAV,AU,WMA	FAT32

Image	Description	File Types	File System
FAT_L1_Audio.dd.bz2	Sequentially fragmented audio files	MP3,WAV,AU,WMA	FAT32
FAT_L2_Audio.dd.bz2	Non-Sequentially fragmented audio files	MP3,WAV,AU,WMA	FAT32
FAT_L3_Audio.dd.bz2	Audio files with missing fragments	MP3,WAV,AU,WMA	FAT32
FAT_L0_Video.dd.bz2	Non-Fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV	FAT32
FAT_L1_Video.dd.bz2	Sequentially fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV	FAT32
FAT_L2_Video.dd.bz2	Non-sequentially fragmented video files	MP4,AVI,MOV,FLV,MPG,WMV	FAT32
FAT_L3_Video.dd.bz2	Video files with missing fragments	MP4,AVI,MOV,FLV,MPG,WMV	FAT32

Appendix B: Recorded File Carving Results

- **Recorded Results Key**
- **Recorded File Carving Results**

Table 1: Recorded Results Key

KEY
<u>File Extension</u> -File extension for the corresponding file name (Ex. 000_021.png)
<u>Size</u> -Sizes are represented in Gigabytes (GB). Each size represents the size of the solid state drive used in that carving test.
<u>Level</u> -Level 0 (Cluster Padded): Non-fragmented, contiguous files with assorted levels of content ranging in size from 1,2,4, 8,16...128 sectors -Level 1 (Fragmented in Order): Contiguous and sequential fragmented files with content separating files (Ex. Part 1 of File-01234-Part 2- of File-01234) -Level 2 (Fragmented Out of Order): Contiguous and disordered fragmented files separated by other content (Ex. Part 3 of File-01234-Part 1 of File-01234) -Level 3 (Incomplete): Contiguous and partial (i.e. only a portion of the file is present) files
<u>Type</u> -Type of forensic image examined (i.e. Document, Video, etc.)
<u>*Carved 1</u> 1=Carved data, correct file (pass) 0= Did not carve data (fail)
<u>Carved 2</u> (Questionable file carving) 1= Carved data, but data carved was not the correct file 0= Did not carve data
<small>*File extension is not necessary to represent carved data. Grouped data is not carved data.</small>

Table 2: Recorded File Carving Results

File Name	ext	Size	Level	Type	Carved 1	Carved 2
000_021	png	120	0	Graphic	1	0
000_021	png	250	0	Graphic	1	0
000_021	png	500	0	Graphic	0	0
02010025	pcx	120	0	Graphic	1	0
02010025	pcx	250	0	Graphic	1	0
02010025	pcx	500	0	Graphic	0	0
02010026	jpg	120	0	Graphic	1	0
02010026	jpg	250	0	Graphic	1	0
02010026	jpg	500	0	Graphic	0	0
09260002	jpg	120	0	Graphic	1	0
09260002	jpg	250	0	Graphic	1	0
09260002	jpg	500	0	Graphic	0	0
100_0304crop	bmp	120	0	Graphic	0	0
100_0304crop	bmp	250	0	Graphic	0	0
100_0304crop	bmp	500	0	Graphic	0	0
100_0018	tif	120	0	Graphic	0	0
100_0018	tif	250	0	Graphic	0	0
100_0018	tif	500	0	Graphic	0	1
100_0183	gif	120	0	Graphic	0	0
100_0183	gif	250	0	Graphic	0	0
100_0183	gif	500	0	Graphic	0	0
09260002 (1)	jpg	120	1	Graphic	0	0
09260002 (1)	jpg	250	1	Graphic	0	0
09260002 (1)	jpg	500	1	Graphic	0	0
09260002 (2)	jpg	120	1	Graphic	0	0
09260002 (2)	jpg	250	1	Graphic	0	0
09260002 (2)	jpg	500	1	Graphic	0	0
100_0018 (1)	tif	120	1	Graphic	0	0
100_0018 (1)	tif	250	1	Graphic	0	0
100_0018 (1)	tif	500	1	Graphic	0	0
100_0018 (2)	tif	120	1	Graphic	0	0
100_0018 (2)	tif	250	1	Graphic	0	0
100_0018 (2)	tif	500	1	Graphic	0	0
100_0018 (3)	tif	120	1	Graphic	0	0
100_0018 (3)	tif	250	1	Graphic	0	0
100_0018 (3)	tif	500	1	Graphic	0	0
100_0304crop (1)	bmp	120	1	Graphic	0	0
100_0304crop (1)	bmp	250	1	Graphic	0	0

Running head: USE OF FORENSIC CORPORA IN VALIDATION

File Name	ext	Size	Level	Type	Carved 1	Carved 2
100_0304crop (1)	bmp	500	1	Graphic	0	0
100_0304crop (2)	bmp	120	1	Graphic	0	0
100_0304crop (2)	bmp	250	1	Graphic	0	0
100_0304crop (2)	bmp	500	1	Graphic	0	0
02010025 (1)	pcx	120	1	Graphic	0	0
02010025 (1)	pcx	250	1	Graphic	0	0
02010025 (1)	pcx	500	1	Graphic	0	0
02010025 (2)	pcx	120	1	Graphic	0	0
02010025 (2)	pcx	250	1	Graphic	0	0
02010025 (2)	pcx	500	1	Graphic	0	0
02010025 (3)	pcx	120	1	Graphic	0	0
02010025 (3)	pcx	250	1	Graphic	0	0
02010025 (3)	pcx	500	1	Graphic	0	0
100_0183 (1)	gif	120	1	Graphic	0	0
100_0183 (1)	gif	250	1	Graphic	0	0
100_0183 (1)	gif	500	1	Graphic	0	0
100_0183 (2)	gif	120	1	Graphic	0	0
100_0183 (2)	gif	250	1	Graphic	0	0
100_0183 (2)	gif	500	1	Graphic	0	0
000_021 (1)	png	120	1	Graphic	0	0
000_021 (1)	png	250	1	Graphic	0	0
000_021 (1)	png	500	1	Graphic	0	0
000_021 (2)	png	120	1	Graphic	0	0
000_021 (2)	png	250	1	Graphic	0	0
000_021 (2)	png	500	1	Graphic	0	0
100_0018 (1)	tif	120	2	Graphic	0	0
100_0018 (1)	tif	250	2	Graphic	0	0
100_0018 (1)	tif	500	2	Graphic	0	0
100_0018 (3)	tif	120	2	Graphic	0	0
100_0018 (3)	tif	250	2	Graphic	0	0
100_0018 (3)	tif	500	2	Graphic	0	0
100_0018 (2)	tif	120	2	Graphic	0	0
100_0018 (2)	tif	250	2	Graphic	0	0
100_0018 (2)	tif	500	2	Graphic	0	0
09260002 (1)	jpg	120	2	Graphic	0	0
09260002 (1)	jpg	250	2	Graphic	0	0
09260002 (1)	jpg	500	2	Graphic	0	0
09260002 (3)	jpg	120	2	Graphic	0	0
09260002 (3)	jpg	250	2	Graphic	0	0
09260002 (3)	jpg	500	2	Graphic	0	0

Running head: USE OF FORENSIC CORPORA IN VALIDATION

File Name	ext	Size	Level	Type	Carved 1	Carved 2
09260002 (2)	jpg	120	2	Graphic	0	0
09260002 (2)	jpg	250	2	Graphic	0	0
09260002 (2)	jpg	500	2	Graphic	0	0
100_0304crop (2)	bmp	120	2	Graphic	0	0
100_0304crop (2)	bmp	250	2	Graphic	0	0
100_0304crop (2)	bmp	500	2	Graphic	0	0
100_0304crop (1)	bmp	120	2	Graphic	0	0
100_0304crop (1)	bmp	250	2	Graphic	0	0
100_0304crop (1)	bmp	500	2	Graphic	0	0
02010025 (1)	pcx	120	2	Graphic	0	0
02010025 (1)	pcx	250	2	Graphic	0	0
02010025 (1)	pcx	500	2	Graphic	0	0
02010025 (3)	pcx	120	2	Graphic	0	0
02010025 (3)	pcx	250	2	Graphic	0	0
02010025 (3)	pcx	500	2	Graphic	0	0
02010025 (2)	pcx	120	2	Graphic	0	0
02010025 (2)	pcx	250	2	Graphic	0	0
02010025 (2)	pcx	500	2	Graphic	0	0
100_0183 (3)	gif	120	2	Graphic	0	0
100_0183 (3)	gif	250	2	Graphic	0	0
100_0183 (3)	gif	500	2	Graphic	0	0
100_0183 (1)	gif	120	2	Graphic	0	0
100_0183 (1)	gif	250	2	Graphic	0	0
100_0183 (1)	gif	500	2	Graphic	0	0
100_0183 (2)	gif	120	2	Graphic	0	0
100_0183 (2)	gif	250	2	Graphic	0	0
100_0183 (2)	gif	500	2	Graphic	0	0
000_021 (2)	png	120	2	Graphic	0	0
000_021 (2)	png	250	2	Graphic	0	0
000_021 (2)	png	500	2	Graphic	0	0
000_021 (1)	png	120	2	Graphic	0	0
000_021 (1)	png	250	2	Graphic	0	0
000_021 (1)	png	500	2	Graphic	0	0
09260002 (1)	jpg	120	3	Graphic	0	0
09260002 (1)	jpg	250	3	Graphic	0	0
09260002 (1)	jpg	500	3	Graphic	0	0
100_0018 (1)	tif	120	3	Graphic	0	0
100_0018 (1)	tif	250	3	Graphic	0	0
100_0018 (1)	tif	500	3	Graphic	0	0
100_0018 (2)	tif	120	3	Graphic	0	0

Running head: USE OF FORENSIC CORPORA IN VALIDATION

File Name	ext	Size	Level	Type	Carved 1	Carved 2
100_0018 (2)	tif	250	3	Graphic	0	0
100_0018 (2)	tif	500	3	Graphic	0	0
100_0304crop (2)	bmp	120	3	Graphic	0	0
100_0304crop (2)	bmp	250	3	Graphic	0	0
100_0304crop (2)	bmp	500	3	Graphic	0	0
02010025 (1)	pcx	120	3	Graphic	0	0
02010025 (1)	pcx	250	3	Graphic	0	0
02010025 (1)	pcx	500	3	Graphic	0	0
02010025 (3)	pcx	120	3	Graphic	0	0
02010025 (3)	pcx	250	3	Graphic	0	0
02010025 (3)	pcx	500	3	Graphic	0	0
100_0018 (2)	tif	120	3	Graphic	0	0
100_0018 (2)	tif	250	3	Graphic	0	0
100_0018 (2)	tif	500	3	Graphic	0	0
100_0183 (3)	gif	120	3	Graphic	0	0
100_0183 (3)	gif	250	3	Graphic	0	0
100_0183 (3)	gif	500	3	Graphic	0	0
000_021 (3)	png	120	3	Graphic	0	0
000_021 (3)	png	250	3	Graphic	0	0
000_021 (3)	png	500	3	Graphic	0	0
D1	pdf	120	0	Document	0	0
D1	pdf	250	0	Document	0	0
D1	pdf	500	0	Document	1	0
D2	pdf	120	0	Document	1	0
D2	pdf	250	0	Document	1	0
D2	pdf	500	0	Document	1	0
D3	xlsx	120	0	Document	1	0
D3	xlsx	250	0	Document	1	0
D3	xlsx	500	0	Document	1	0
D4	xlsx	120	0	Document	0	0
D4	xlsx	250	0	Document	0	0
D4	xlsx	500	0	Document	0	1
D5	docx	120	0	Document	0	1
D5	docx	250	0	Document	0	1
D5	docx	500	0	Document	0	1
D6	docx	120	0	Document	0	0
D6	docx	250	0	Document	0	0
D6	docx	500	0	Document	0	1
D7	pptx	120	0	Document	0	0
D7	pptx	250	0	Document	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
D7	pptx	500	0	Document	0	1
D1 (1)	pdf	120	1	Document	1	0
D1 (1)	pdf	250	1	Document	1	0
D1 (1)	pdf	500	1	Document	1	0
D1 (2)	pdf	120	1	Document	0	0
D1 (2)	pdf	250	1	Document	0	0
D1 (2)	pdf	500	1	Document	0	0
D2 (1)	pdf	120	1	Document	1	0
D2 (1)	pdf	250	1	Document	1	0
D2 (1)	pdf	500	1	Document	1	0
D2 (2)	pdf	120	1	Document	1	0
D2 (2)	pdf	250	1	Document	1	0
D2 (2)	pdf	500	1	Document	0	0
D2 (3)	pdf	120	1	Document	1	0
D2 (3)	pdf	250	1	Document	1	0
D2 (3)	pdf	500	1	Document	0	0
D3 (1)	xlsx	120	1	Document	1	0
D3 (1)	xlsx	250	1	Document	1	0
D3 (1)	xlsx	500	1	Document	1	0
D3 (2,3)	xlsx	120	1	Document	1	0
D3 (2,3)	xlsx	250	1	Document	1	0
D3 (2,3)	xlsx	500	1	Document	0	0
D4 (1,2)	xlsx	120	1	Document	0	0
D4 (1,2)	xlsx	250	1	Document	0	0
D4 (1,2)	xlsx	500	1	Document	0	0
D4 (3)	xlsx	120	1	Document	0	0
D4 (3)	xlsx	250	1	Document	0	0
D4 (3)	xlsx	500	1	Document	0	0
D5 (1)	docx	120	1	Document	0	0
D5 (1)	docx	250	1	Document	0	0
D5 (1)	docx	500	1	Document	0	0
D5 (2)	docx	120	1	Document	0	0
D5 (2)	docx	250	1	Document	0	0
D5 (2)	docx	500	1	Document	0	0
D5 (3)	docx	120	1	Document	0	0
D5 (3)	docx	250	1	Document	0	0
D5 (3)	docx	500	1	Document	0	0
D6 (1)	docx	120	1	Document	0	0
D6 (1)	docx	250	1	Document	0	0
D6 (1)	docx	500	1	Document	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
D6 (2)	docx	120	1	Document	0	0
D6 (2)	docx	250	1	Document	0	0
D6 (2)	docx	500	1	Document	0	0
D7 (1)	pptx	120	1	Document	0	1
D7 (1)	pptx	250	1	Document	0	1
D7 (1)	pptx	500	1	Document	0	1
D7 (2,3)	pptx	120	1	Document	0	0
D7 (2,3)	pptx	250	1	Document	0	0
D7 (2,3)	pptx	500	1	Document	0	0
D1 (3)	pdf	120	2	Document	0	0
D1 (3)	pdf	250	2	Document	0	0
D1 (3)	pdf	500	2	Document	0	0
D1 (1)	pdf	120	2	Document	0	0
D1 (1)	pdf	250	2	Document	0	0
D1 (1)	pdf	500	2	Document	1	0
D1 (2)	pdf	120	2	Document	0	0
D1 (2)	pdf	250	2	Document	0	0
D1 (2)	pdf	500	2	Document	0	0
D2 (2)	pdf	120	2	Document	1	0
D2 (2)	pdf	250	2	Document	1	0
D2 (2)	pdf	500	2	Document	1	0
D2 (3)	pdf	120	2	Document	1	0
D2 (3)	pdf	250	2	Document	1	0
D2 (3)	pdf	500	2	Document	1	0
D2 (1)	pdf	120	2	Document	1	0
D2 (1)	pdf	250	2	Document	1	0
D2 (1)	pdf	500	2	Document	1	0
D3 (2)	xlsx	120	2	Document	1	0
D3 (2)	xlsx	250	2	Document	1	0
D3 (2)	xlsx	500	2	Document	0	0
D3 (1)	xlsx	120	2	Document	1	0
D3 (1)	xlsx	250	2	Document	1	0
D3 (1)	xlsx	500	2	Document	1	0
D4 (2)	xlsx	120	2	Document	0	1
D4 (2)	xlsx	250	2	Document	0	1
D4 (2)	xlsx	500	2	Document	0	0
D4 (1)	xlsx	120	2	Document	0	0
D4 (1)	xlsx	250	2	Document	0	0
D4 (1)	xlsx	500	2	Document	0	1
D4 (3)	xlsx	120	2	Document	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
D4 (3)	xlsx	250	2	Document	0	0
D4 (3)	xlsx	500	2	Document	0	0
D5 (1)	docx	120	2	Document	0	0
D5 (1)	docx	250	2	Document	0	0
D5 (1)	docx	500	2	Document	0	1
D5 (3)	docx	120	2	Document	0	0
D5 (3)	docx	250	2	Document	0	0
D5 (3)	docx	500	2	Document	0	0
D5 (2)	docx	120	2	Document	0	0
D5 (2)	docx	250	2	Document	0	0
D5 (2)	docx	500	2	Document	0	0
D6 (2,3)	docx	120	2	Document	0	0
D6 (2,3)	docx	250	2	Document	0	0
D6 (2,3)	docx	500	2	Document	0	0
D6 (1)	docx	120	2	Document	0	0
D6 (1)	docx	250	2	Document	0	0
D6 (1)	docx	500	2	Document	0	0
D7 (3)	pptx	120	2	Document	0	0
D7 (3)	pptx	250	2	Document	0	0
D7 (3)	pptx	500	2	Document	0	0
D7 (2)	pptx	120	2	Document	0	0
D7 (2)	pptx	250	2	Document	0	0
D7 (2)	pptx	500	2	Document	0	0
D7 (1)	pptx	120	2	Document	0	1
D7 (1)	pptx	250	2	Document	0	1
D7 (1)	pptx	500	2	Document	0	1
D1 (1)	pdf	120	3	Document	0	0
D1 (1)	pdf	250	3	Document	0	0
D1 (1)	pdf	500	3	Document	1	0
D1 (2,3)	pdf	120	3	Document	0	0
D1 (2,3)	pdf	250	3	Document	0	0
D1 (2,3)	pdf	500	3	Document	1	0
D2 (1)	pdf	120	3	Document	1	0
D2 (1)	pdf	250	3	Document	1	0
D2 (1)	pdf	500	3	Document	1	0
D2 (3)	pdf	120	3	Document	0	0
D2 (3)	pdf	250	3	Document	0	0
D2 (3)	pdf	500	3	Document	1	0
D3 (2)	xlsx	120	3	Document	0	0
D3 (2)	xlsx	250	3	Document	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
D3 (2)	xlsx	500	3	Document	0	0
D3 (3)	xlsx	120	3	Document	1	0
D3 (3)	xlsx	250	3	Document	1	0
D3 (3)	xlsx	500	3	Document	1	0
D4 (2)	xlsx	120	3	Document	0	0
D4 (2)	xlsx	250	3	Document	0	0
D4 (2)	xlsx	500	3	Document	0	0
D5 (1)	docx	120	3	Document	0	1
D5 (1)	docx	250	3	Document	0	1
D5 (1)	docx	500	3	Document	0	1
D6 (2,3)	docx	120	3	Document	0	0
D6 (2,3)	docx	250	3	Document	0	0
D6 (2,3)	docx	500	3	Document	0	0
D7 (3)	pptx	120	3	Document	0	1
D7 (3)	pptx	250	3	Document	0	1
D7 (3)	pptx	500	3	Document	0	1
arc1	7z	120	0	Archive	1	0
arc1	7z	250	0	Archive	1	0
arc1	7z	500	0	Archive	1	0
arc2	bz2	120	0	Archive	0	0
arc2	bz2	250	0	Archive	0	0
arc2	bz2	500	0	Archive	0	0
arc3	gz	120	0	Archive	0	0
arc3	gz	250	0	Archive	0	0
arc3	gz	500	0	Archive	0	0
arc4	tar	120	0	Archive	0	0
arc4	tar	250	0	Archive	0	0
arc4	tar	500	0	Archive	0	0
arc5	wim	120	0	Archive	0	0
arc5	wim	250	0	Archive	0	0
arc5	wim	500	0	Archive	0	0
arc6	rar	120	0	Archive	0	0
arc6	rar	250	0	Archive	0	0
arc6	rar	500	0	Archive	0	0
arc7	zip	120	0	Archive	0	0
arc7	zip	250	0	Archive	0	0
arc7	zip	500	0	Archive	0	0
arc1 (1)	7z	120	1	Archive	1	0
arc1 (1)	7z	250	1	Archive	1	0
arc1 (1)	7z	500	1	Archive	1	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
arc1 (2)	7z	120	1	Archive	1	0
arc1 (2)	7z	250	1	Archive	1	0
arc1 (2)	7z	500	1	Archive	1	0
arc2 (1)	bz2	120	1	Archive	0	0
arc2 (1)	bz2	250	1	Archive	0	0
arc2 (1)	bz2	500	1	Archive	0	0
arc2 (2)	bz2	120	1	Archive	0	0
arc2 (2)	bz2	250	1	Archive	0	0
arc2 (2)	bz2	500	1	Archive	0	0
arc2 (3)	bz2	120	1	Archive	0	0
arc2 (3)	bz2	250	1	Archive	0	0
arc2 (3)	bz2	500	1	Archive	0	0
arc3 (1)	gz	120	1	Archive	0	0
arc3 (1)	gz	250	1	Archive	0	0
arc3 (1)	gz	500	1	Archive	0	0
arc3 (2)	gz	120	1	Archive	0	0
arc3 (2)	gz	250	1	Archive	0	0
arc3 (2)	gz	500	1	Archive	0	0
arc4 (1)	tar	120	1	Archive	0	0
arc4 (1)	tar	250	1	Archive	0	0
arc4 (1)	tar	500	1	Archive	0	0
arc4 (2)	tar	120	1	Archive	0	0
arc4 (2)	tar	250	1	Archive	0	0
arc4 (2)	tar	500	1	Archive	0	0
arc4 (3)	tar	120	1	Archive	0	0
arc4 (3)	tar	250	1	Archive	0	0
arc4 (3)	tar	500	1	Archive	0	0
arc5 (1)	wim	120	1	Archive	0	0
arc5 (1)	wim	250	1	Archive	0	0
arc5 (1)	wim	500	1	Archive	0	0
arc5 (2)	wim	120	1	Archive	0	0
arc5 (2)	wim	250	1	Archive	0	0
arc5 (2)	wim	500	1	Archive	0	0
arc6 (1)	rar	120	1	Archive	0	0
arc6 (1)	rar	250	1	Archive	0	0
arc6 (1)	rar	500	1	Archive	0	0
arc6 (2)	rar	120	1	Archive	0	0
arc6 (2)	rar	250	1	Archive	0	0
arc6 (2)	rar	500	1	Archive	0	0
arc6 (3)	rar	120	1	Archive	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
arc6 (3)	rar	250	1	Archive	0	0
arc6 (3)	rar	500	1	Archive	0	0
arc7 (1)	zip	120	1	Archive	0	0
arc7 (1)	zip	250	1	Archive	0	0
arc7 (1)	zip	500	1	Archive	0	0
arc7 (2)	zip	120	1	Archive	0	0
arc7 (2)	zip	250	1	Archive	0	0
arc7 (2)	zip	500	1	Archive	0	0
arc6 (2)	rar	120	2	Archive	1	0
arc6 (2)	rar	250	2	Archive	1	0
arc6 (2)	rar	500	2	Archive	1	0
arc6 (1)	rar	120	2	Archive	1	0
arc6 (1)	rar	250	2	Archive	1	0
arc6 (1)	rar	500	2	Archive	1	0
arc7 (1)	zip	120	2	Archive	0	0
arc7 (1)	zip	250	2	Archive	0	0
arc7 (1)	zip	500	2	Archive	0	0
arc7 (3)	zip	120	2	Archive	0	0
arc7 (3)	zip	250	2	Archive	0	0
arc7 (3)	zip	500	2	Archive	0	0
arc7 (2)	zip	120	2	Archive	0	0
arc7 (2)	zip	250	2	Archive	0	0
arc7 (2)	zip	500	2	Archive	0	0
arc1 (2)	7z	120	2	Archive	0	0
arc1 (2)	7z	250	2	Archive	0	0
arc1 (2)	7z	500	2	Archive	0	0
arc1 (1)	7z	120	2	Archive	0	0
arc1 (1)	7z	250	2	Archive	0	0
arc1 (1)	7z	500	2	Archive	0	0
arc1 (3)	7z	120	2	Archive	0	0
arc1 (3)	7z	250	2	Archive	0	0
arc1 (3)	7z	500	2	Archive	0	0
arc2 (2)	bz2	120	2	Archive	0	0
arc2 (2)	bz2	250	2	Archive	0	0
arc2 (2)	bz2	500	2	Archive	0	0
arc2 (3)	bz2	120	2	Archive	0	0
arc2 (3)	bz2	250	2	Archive	0	0
arc2 (3)	bz2	500	2	Archive	0	0
arc2 (1)	bz2	120	2	Archive	0	0
arc2 (1)	bz2	250	2	Archive	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
arc2 (1)	bz2	500	2	Archive	0	0
arc4 (3)	tar	120	2	Archive	0	0
arc4 (3)	tar	250	2	Archive	0	0
arc4 (3)	tar	500	2	Archive	0	0
arc4 (1)	tar	120	2	Archive	0	0
arc4 (1)	tar	250	2	Archive	0	0
arc4 (1)	tar	500	2	Archive	0	0
arc4 (2)	tar	120	2	Archive	0	0
arc4 (2)	tar	250	2	Archive	0	0
arc4 (2)	tar	500	2	Archive	0	0
arc5 (3)	wim	120	2	Archive	0	0
arc5 (3)	wim	250	2	Archive	0	0
arc5 (3)	wim	500	2	Archive	0	0
arc5 (2)	wim	120	2	Archive	0	0
arc5 (2)	wim	250	2	Archive	0	0
arc5 (2)	wim	500	2	Archive	0	0
arc5 (1)	wim	120	2	Archive	0	0
arc5 (1)	wim	250	2	Archive	0	0
arc5 (1)	wim	500	2	Archive	0	0
arc3 (2,3)	gz	120	2	Archive	0	0
arc3 (2,3)	gz	250	2	Archive	0	0
arc3 (2,3)	gz	500	2	Archive	0	0
arc3 (1)	gz	120	2	Archive	0	0
arc3 (1)	gz	250	2	Archive	0	0
arc3 (1)	gz	500	2	Archive	0	0
arc6 (1)	rar	120	3	Archive	1	0
arc6 (1)	rar	250	3	Archive	1	0
arc6 (1)	rar	500	3	Archive	1	0
arc7 (2)	zip	120	3	Archive	0	0
arc7 (2)	zip	250	3	Archive	0	0
arc7 (2)	zip	500	3	Archive	0	0
arc3 (1)	gz	120	3	Archive	0	0
arc3 (1)	gz	250	3	Archive	0	0
arc3 (1)	gz	500	3	Archive	0	0
arc3 (2)	gz	120	3	Archive	0	0
arc3 (2)	gz	250	3	Archive	0	0
arc3 (2)	gz	500	3	Archive	0	0
arc2 (1)	bz2	120	3	Archive	0	0
arc2 (1)	bz2	250	3	Archive	0	0
arc2 (1)	bz2	500	3	Archive	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
arc2 (3)	bz2	120	3	Archive	0	0
arc2 (3)	bz2	250	3	Archive	0	0
arc2 (3)	bz2	500	3	Archive	0	0
arc1 (2)	7z	120	3	Archive	0	0
arc1 (2)	7z	250	3	Archive	0	0
arc1 (2)	7z	500	3	Archive	0	0
arc1 (3)	7z	120	3	Archive	0	0
arc1 (3)	7z	250	3	Archive	0	0
arc1 (3)	7z	500	3	Archive	0	0
arc4 (3)	tar	120	3	Archive	0	0
arc4 (3)	tar	250	3	Archive	0	0
arc4 (3)	tar	500	3	Archive	0	0
arc5 (2,3)	wim	120	3	Archive	0	0
arc5 (2,3)	wim	250	3	Archive	0	0
arc5 (2,3)	wim	500	3	Archive	0	0
Audio1	mp3	120	0	Audio	1	0
Audio1	mp3	250	0	Audio	1	0
Audio1	mp3	500	0	Audio	1	0
Audio2	wav	120	0	Audio	0	0
Audio2	wav	250	0	Audio	0	0
Audio2	wav	500	0	Audio	0	0
Audio3	au	120	0	Audio	0	0
Audio3	au	250	0	Audio	0	0
Audio3	au	500	0	Audio	0	0
Audio4	wma	120	0	Audio	0	0
Audio5	wma	250	0	Audio	0	0
Audio6	wma	500	0	Audio	0	0
Audio1 (1)	mp3	120	1	Audio	1	0
Audio1 (1)	mp3	250	1	Audio	1	0
Audio1 (1)	mp3	500	1	Audio	1	0
Audio1 (2)	mp3	120	1	Audio	1	0
Audio1 (2)	mp4	250	1	Audio	1	0
Audio1 (2)	mp5	500	1	Audio	1	0
Audio2 (1)	wav	120	1	Audio	0	0
Audio2 (1)	wav	250	1	Audio	0	0
Audio2 (1)	wav	500	1	Audio	0	0
Audio2 (2)	wav	120	1	Audio	0	0
Audio2 (2)	wav	250	1	Audio	0	0
Audio2 (2)	wav	500	1	Audio	0	0
Audio2 (3)	wav	120	1	Audio	0	0

Running head: USE OF FORENSIC CORPORA IN VALIDATION

File Name	ext	Size	Level	Type	Carved 1	Carved 2
Audio2 (3)	wav	250	1	Audio	0	0
Audio2 (3)	wav	500	1	Audio	0	0
Audio3 (1)	au	120	1	Audio	0	0
Audio3 (1)	au	250	1	Audio	0	0
Audio3 (1)	au	500	1	Audio	0	0
Audio3 (2)	au	120	1	Audio	0	0
Audio3 (2)	au	250	1	Audio	0	0
Audio3 (2)	au	500	1	Audio	0	0
Audio4 (1)	wma	120	1	Audio	0	0
Audio4 (1)	wma	250	1	Audio	0	0
Audio4 (1)	wma	500	1	Audio	0	0
Audio4 (2)	wma	120	1	Audio	0	0
Audio4 (2)	wma	250	1	Audio	0	0
Audio4 (2)	wma	500	1	Audio	0	0
Audio4 (3)	wma	120	1	Audio	0	0
Audio4 (3)	wma	250	1	Audio	0	0
Audio4 (3)	wma	500	1	Audio	0	0
Audio1 (2)	mp3	120	2	Audio	0	0
Audio1 (2)	mp3	250	2	Audio	0	0
Audio1 (2)	mp3	500	2	Audio	0	0
Audio1 (1)	mp3	120	2	Audio	1	0
Audio1 (1)	mp3	250	2	Audio	1	0
Audio1 (1)	mp3	500	2	Audio	1	0
Audio2 (1)	wav	120	2	Audio	0	0
Audio2 (1)	wav	250	2	Audio	0	0
Audio2 (1)	wav	500	2	Audio	0	0
Audio2 (3)	wav	120	2	Audio	0	0
Audio2 (3)	wav	250	2	Audio	0	0
Audio2 (3)	wav	500	2	Audio	0	0
Audio2 (2)	wav	120	2	Audio	0	0
Audio2 (2)	wav	250	2	Audio	0	0
Audio2 (2)	wav	500	2	Audio	0	0
Audio3 (2)	au	120	2	Audio	0	0
Audio3 (2)	au	250	2	Audio	0	0
Audio3 (2)	au	500	2	Audio	0	0
Audio3 (1)	au	120	2	Audio	0	0
Audio3 (1)	au	250	2	Audio	0	0
Audio3 (1)	au	500	2	Audio	0	0
Audio3 (3)	au	120	2	Audio	0	0
Audio3 (3)	au	250	2	Audio	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
Audio3 (3)	au	500	2	Audio	0	0
Audio4 (3)	wma	120	2	Audio	0	0
Audio4 (3)	wma	250	2	Audio	0	0
Audio4 (3)	wma	500	2	Audio	0	0
Audio4 (2)	wma	120	2	Audio	0	0
Audio4 (2)	wma	250	2	Audio	0	0
Audio4 (2)	wma	500	2	Audio	0	0
Audio4 (1)	wma	120	2	Audio	0	0
Audio4 (1)	wma	250	2	Audio	0	0
Audio4 (1)	wma	500	2	Audio	0	0
Audio1 (1)	mp3	120	3	Audio	1	0
Audio1 (1)	mp3	250	3	Audio	1	0
Audio1 (1)	mp3	500	3	Audio	1	0
Audio1 (3)	mp3	120	3	Audio	0	0
Audio1 (3)	mp4	250	3	Audio	0	0
Audio1 (3)	mp5	500	3	Audio	0	0
Audio2 (1)	wav	120	3	Audio	0	0
Audio2 (1)	wav	250	3	Audio	0	0
Audio2 (1)	wav	500	3	Audio	0	0
Audio3 (2)	au	120	3	Audio	0	0
Audio3 (2)	au	250	3	Audio	0	0
Audio3 (2)	au	500	3	Audio	0	0
Audio3 (3)	au	120	3	Audio	0	0
Audio3 (3)	au	250	3	Audio	0	0
Audio3 (3)	au	500	3	Audio	0	0
Audio4 (1)	wma	120	3	Audio	0	0
Audio4 (1)	wma	250	3	Audio	0	0
Audio4 (1)	wma	500	3	Audio	0	0
Audio4 (2)	wma	120	3	Audio	0	0
Audio4 (2)	wma	250	3	Audio	0	0
Audio4 (2)	wma	500	3	Audio	0	0
vid1	mp4	120	0	Video	0	0
vid1	mp4	250	0	Video	0	0
vid1	mp4	500	0	Video	0	0
vid2	avi	120	0	Video	0	0
vid2	avi	250	0	Video	0	0
vid2	avi	500	0	Video	0	0
vid3	mov	120	0	Video	0	0
vid3	mov	250	0	Video	0	0
vid3	mov	500	0	Video	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
vid4	flv	120	0	Video	0	1
vid4	flv	250	0	Video	0	1
vid4	flv	500	0	Video	0	1
vid5	mpg	120	0	Video	0	0
vid5	mpg	250	0	Video	0	0
vid5	mpg	500	0	Video	0	0
vid6	wmv	120	0	Video	0	0
vid6	wmv	250	0	Video	0	0
vid6	wmv	500	0	Video	0	0
vid1 (1)	mp4	120	1	Video	0	0
vid1 (1)	mp4	250	1	Video	0	0
vid1 (1)	mp4	500	1	Video	0	0
vid1 (2)	mp4	120	1	Video	0	0
vid1 (2)	mp4	250	1	Video	0	0
vid1 (2)	mp4	500	1	Video	0	0
vid1 (3)	mp4	120	1	Video	0	0
vid1 (3)	mp4	250	1	Video	0	0
vid1 (3)	mp4	500	1	Video	0	0
vid2 (1)	avi	120	1	Video	0	0
vid2 (1)	avi	250	1	Video	0	0
vid2 (1)	avi	500	1	Video	0	0
vid2 (2)	avi	120	1	Video	0	0
vid2 (2)	avi	250	1	Video	0	0
vid2 (2)	avi	500	1	Video	0	0
vid3 (1)	mov	120	1	Video	0	0
vid3 (1)	mov	250	1	Video	0	0
vid3 (1)	mov	500	1	Video	0	0
vid3 (2)	mov	120	1	Video	0	0
vid3 (2)	mov	250	1	Video	0	0
vid3 (2)	mov	500	1	Video	0	0
vid3 (3)	mov	120	1	Video	0	0
vid3 (3)	mov	250	1	Video	0	0
vid3 (3)	mov	500	1	Video	0	0
vid4 (1)	flv	120	1	Video	0	1
vid4 (1)	flv	250	1	Video	0	1
vid4 (1)	flv	500	1	Video	0	1
vid4 (2)	flv	120	1	Video	0	0
vid4 (2)	flv	250	1	Video	0	0
vid4 (2)	flv	500	1	Video	0	0
vid5 (1)	mpg	120	1	Video	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
vid5 (1)	mpg	250	1	Video	0	0
vid5 (1)	mpg	500	1	Video	0	0
vid5 (2)	mpg	120	1	Video	0	0
vid5 (2)	mpg	250	1	Video	0	0
vid5 (2)	mpg	500	1	Video	0	0
vid5 (3)	mpg	120	1	Video	0	0
vid5 (3)	mpg	250	1	Video	0	0
vid5 (3)	mpg	500	1	Video	0	0
vid6 (1)	wmv	120	1	Video	0	0
vid6 (1)	wmv	250	1	Video	0	0
vid6 (1)	wmv	500	1	Video	0	0
vid6 (2)	wmv	120	1	Video	0	0
vid6 (2)	wmv	250	1	Video	0	0
vid6 (2)	wmv	500	1	Video	0	0
vid2 (2)	avi	120	2	Video	0	0
vid2 (2)	avi	250	2	Video	0	0
vid2 (2)	avi	500	2	Video	0	0
vid2 (1)	avi	120	2	Video	0	0
vid2 (1)	avi	250	2	Video	0	0
vid2 (1)	avi	500	2	Video	0	0
vid6 (1)	wmv	120	2	Video	0	0
vid6 (1)	wmv	250	2	Video	0	0
vid6 (1)	wmv	500	2	Video	0	0
vid6 (3)	wmv	120	2	Video	0	0
vid6 (3)	wmv	250	2	Video	0	0
vid6 (3)	wmv	500	2	Video	0	0
vid6 (2)	wmv	120	2	Video	0	0
vid6 (2)	wmv	250	2	Video	0	0
vid6 (2)	wmv	500	2	Video	0	0
vid1 (2)	mp4	120	2	Video	0	0
vid1 (2)	mp4	250	2	Video	0	0
vid1 (2)	mp4	500	2	Video	0	0
vid1 (1)	mp4	120	2	Video	0	0
vid1 (1)	mp4	250	2	Video	0	0
vid1 (1)	mp4	500	2	Video	0	0
vid1 (3)	mp4	120	2	Video	0	0
vid1 (3)	mp4	250	2	Video	0	0
vid1 (3)	mp4	500	2	Video	0	0
vid3 (2)	mov	120	2	Video	0	0
vid3 (2)	mov	250	2	Video	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
vid3 (2)	mov	500	2	Video	0	0
vid3 (3)	mov	120	2	Video	0	0
vid3 (3)	mov	250	2	Video	0	0
vid3 (3)	mov	500	2	Video	0	0
vid3 (1)	mov	120	2	Video	0	0
vid3 (1)	mov	250	2	Video	0	0
vid3 (1)	mov	500	2	Video	0	0
vid5 (3)	mpg	120	2	Video	0	0
vid5 (3)	mpg	250	2	Video	0	0
vid5 (3)	mpg	500	2	Video	0	0
vid5 (1)	mpg	120	2	Video	0	0
vid5 (1)	mpg	250	2	Video	0	0
vid5 (1)	mpg	500	2	Video	0	0
vid5 (2)	mpg	120	2	Video	0	0
vid5 (2)	mpg	250	2	Video	0	0
vid5 (2)	mpg	500	2	Video	0	0
vid4 (3)	flv	120	2	Video	0	0
vid4 (3)	flv	250	2	Video	0	0
vid4 (3)	flv	500	2	Video	0	0
vid4 (2)	flv	120	2	Video	0	0
vid4 (2)	flv	250	2	Video	0	0
vid4 (2)	flv	500	2	Video	0	0
vid4 (1)	flv	120	2	Video	0	1
vid4 (1)	flv	250	2	Video	0	1
vid4 (1)	flv	500	2	Video	0	1
vid4 (1)	flv	120	3	Video	0	1
vid4 (1)	flv	250	3	Video	0	1
vid4 (1)	flv	500	3	Video	0	1
vid2 (2)	avi	120	3	Video	0	0
vid2 (2)	avi	250	3	Video	0	0
vid2 (2)	avi	500	3	Video	0	0
vid1 (1)	mp4	120	3	Video	0	0
vid1 (1)	mp4	250	3	Video	0	0
vid1 (1)	mp4	500	3	Video	0	0
vid1 (2)	mp4	120	3	Video	0	0
vid1 (2)	mp4	250	3	Video	0	0
vid1 (2)	mp4	500	3	Video	0	0
vid5 (1)	mpg	120	3	Video	0	0
vid5 (1)	mpg	250	3	Video	0	0
vid5 (1)	mpg	500	3	Video	0	0

File Name	ext	Size	Level	Type	Carved 1	Carved 2
vid5 (3)	mpg	120	3	Video	0	0
vid5 (3)	mpg	250	3	Video	0	0
vid5 (3)	mpg	500	3	Video	0	0
vid6 (2)	wmv	120	3	Video	0	0
vid6 (2)	wmv	250	3	Video	0	0
vid6 (2)	wmv	500	3	Video	0	0
vid6 (3)	wmv	120	3	Video	0	0
vid6 (3)	wmv	250	3	Video	0	0
vid6 (3)	wmv	500	3	Video	0	0
vid3 (3)	mov	120	3	Video	0	0
vid3 (3)	mov	250	3	Video	0	0
vid3 (3)	mov	500	3	Video	0	0