Spring 2015

# Xbox one file system data storage: A forensic analysis

Caitlin Elizabeth Gravel
*Purdue University*

*Graduate School Form 30*
*Updated 1/15/2015*

**PURDUE UNIVERSITY**
**GRADUATE SCHOOL**
**Thesis/Dissertation Acceptance**

This is to certify that the thesis/dissertation prepared

By Caitlin Elizabeth Gravel

Entitled

XBOX ONE FILE SYSTEM DATA STORAGE: A FORENSIC ANALYSIS

For the degree of Master of Science

Is approved by the final examining committee:

Marcus Rogers
Chair

Raymond Hansen

James Eric Dietz

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Marcus Rogers

Approved by: Jeffery Whitten 4/15/2015

Head of the Departmental Graduate Program Date

# XBOX ONE FILE SYSTEM DATA STORAGE: A FORENSIC ANALYSIS

A Thesis

Submitted to the Faculty

of

Purdue University

by

Caitlin Elizabeth Gravel

In Partial Fulfilment of the

Requirements for the Degree

of

Masters of Science

May 2015

Purdue University

West Lafayette, Indiana

To my parents, Liz and Mark, for always supporting and believing in me. To my brothers, Patrick and Sammy, for being there for me. To Katja for never letting me give up and always making me smile when I needed it.

# ACKNOWLEDGEMENTS

This research was inspired by Sam Liles, Marcus Rogers, Brian Carrier, and Steven Bolt. Their teachings and previous research allowed me to find what I love in digital forensics. Thank you to Eric Dietz and Ray Hansen for helping me find my voice in this research. Thank you to Microsoft's Xbox team to produce the Xbox One. Finally, thank you to all of my friends and family who helped me throughout this process. I truly owe this to you all.

# TABLE OF CONTENTS

Page

Page

Page

Page

# LIST OF TABLES

Table Page

Table Page

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| BIOS | Basic Input/Output System |
| FAT | File Allocation Table |
| FTK | Forensic Took Kit |
| GPT | GUID Partition Table |
| GUID | Global Unique Identifier |
| HDD | Hard drive |
| LBA | Logical Block Address |
| MBR | Master Boot Record |
| MD5 | Message Digest 5 |
| MFT | Master File Table |
| MSDOS | Microsoft Disk Operating System |
| NIST | National Institute of Standards and Technology |
| NTFS | New Technology File System |
| OS | Operating System |
| PC | Personal Computer |
| PS# | PlayStation # |
| PFS | PlayStation File System |

| | |
|---|---|
| RAM | Random Access Memory |
| ReFS | Resilient File System |
| SATA | Serial ATA |
| SHA1 | Secure Hash Algorithm 1 |
| TC1 | Test Case One |
| TC2 | Test Case Two |
| TC3 | Test Case Three |
| TD1 | Test Drive One |
| UEFI | Unified Extensible Firmware Interface |
| USB | Universal Serial Bus |

# GLOSSARY

*Data* – "A subset of information in an electronic format that allows it to be retrieved or transmitted" (NIST, 2013 p.83).

*Data Integrity* – "The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit" (NIST, 2013 p. 59).

*Decryption* – "The process of transforming ciphertext into plain text" (NIST, 2013 p.60).

*Digital Evidence* – "a digital object that contains reliable information that supports or refutes a hypothesis" (Carrier, 2005).

*Digital Forensics* – "the use of an expert to preserve, analyze, and produce data from volatile and non-volatile media storage" (Meyers, 2004).

*Digital Investigation* – "a process where we develop and test hypothesis that answer questions about digital events" (Carrier, 2005 p.12).

*Encryption* – "Conversion of plaintext to ciphertext through the use of a cryptographic algorithm" (NIST, 2013 p.69).

*File Sytem* – Computers method for the long-term storage and retreival of data. File systems provide a mechanism for users to store data in a hierarchy of files and directories. A flie system consists of structural and user data that are organized such that the computer knows where to find them" (Carrier, 2005).

*Firmware* – "The programs and data components of a crytographic module that are stored in hardware within the cryptographic boundry and cannot be dynamically written or modified during execution" (NIST, 2013 p.79).

*Forensically Sound* – "The application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law" (McKemmish, 2008 p. 3).

*Game Console* – "Computer devices dedicated to (or primarily used for) playing video games" (Henderson, 2009 p. 205).

*Hard Drive/Hard Disk (magnetic) (aka HDD)* – "The primary means of fast data storage and retrieval in computer systems of all sizes. The disk itself consists of a rigid aluminum alloy platter coated with a magnetic oxide material. The platter can be rotated at speeds of more than 10,000 rpm. A typical drive consists of a stack of such platters mounted on a rotaating spindle, with a read/write head mounted above each platter" (Henderson, 2009 p.222).

*Hardware* – "The physical components of an information system" (NIST, 2013 p.84).

*Hash Function* – "A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions are specific in FIPS 180 and are designed to satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input that maps to any new prespecified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output" (NIST, 2013 p.84).

*Hash Total* – "Value computed on data to detect error or manipulation" (NIST, 2013 p.84).

*Hashing* – "The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data" (NIST, 2013 p.85).

*Hypervisor* – "A layer of software that sits between the hardware and one or more operating systems. Its primary job is to provide isolated execution environments called partitions." (Microsoft, 2014).

*Operating System (OS)* – "An overreaching program that manages the resources of the computer. It runs programs and provices them with access to memory (RAM), input/output devices, a file system, and other services. It provides application programmers with a way to invoke system services, and gives users a way to control programs and organize files" (Henderson, 2009 p.352-353).

*Software* – "Computer programs and associated data that may be dynamically written or modified during execution" (NIST, 2013 p.185).

*Virtual Machine* – "Software that allows a single host to run one or more guest operating systems" (NIST, 2013 p. 211).

*Write-Blocker* – "A device that allows investigators to examine media while preventing data writes from occurring on the subject media" (NIST, 2013 p. 215).

# ABSTRACT

Gravel, Caitlin Elizabeth, M.S., Purdue University, May 2015. Xbox One File System Data Storage: A Forensic Analysis. Major Professor: Marcus K. Rogers.

The purpose of this research was to answer the question, how does the file system of the Xbox One store data on its hard disk? This question is the main focus of the exploratory research and results sought. The research is focused on digital forensic investigators and experts. An out of the box Xbox One gaming console was used in the research. Three test cases were created as viable scenarios an investigator could come across in a search and seizure of evidence. The three test cases were then analyzed individually and cross analyzed with each other for differing digital artifacts. It was found that the Xbox One works off of a UEFI/GPT system with NTFS within each of the five partitions. MD5 and SHA1 hash checksums were used as to view altered, added, and removed files for both integrity checking and test case comparison.

# CHAPTER 1. INTRODUCTION

Technology is constantly evolving in the world. Digital forensic investigators have to overcome the challenge of researching brand new devices every year. Microsoft's Xbox One is among these new devices and was released on November 22nd, 2013 (Microsoft, 2014). To help forensic investigators understand the Xbox One system the following research explored the gaming consoles file system.

The Xbox One console has many new features than simply allowing users to play video games, including allowing users to download music, pictures, and videos, browse the internet, Skype, backup data in the cloud, sign on to the Xbox Live network, voice command, Kinect camera motion tracking, SmartGlass, cloud storage, ability to run cable box through console, and of course play video games. With these new features users have the ability to do innocent and devious behavior with the Xbox One. It is up to forensic investigators to conclude which is which. This research allows the forensic investigators to know more about the gaming console so they can make their conclusion an accurate one.

The default specifications of the Xbox One are: an eight core processor, eight gigabytes of RAM, one 500GB magnetic hard drive, Blu-ray/DVD optical drive, Wi-Fi, and Ethernet capabilities (Microsoft, 2014).

The Xbox One has three operating systems working together for the overall end user experience (Rubin, 2013). The operating systems are listed as the Xbox OS, an OS based on Windows 8 and RT, and a Hyper-V like operating system to talk between the other two operating systems (Sakr, 2013). The Xbox OS is used as the main gaming engine for video gaming. The stripped down Windows OS is based off of the Windows kernel and is primarily used for the apps to be used on the system (Sakr, 2013).

These operating systems, working together simultaneously, allow the ability of Microsoft's SmartGlass to work where the end-user can see two different screens at the same time. Examples of these features include, but are not limited to, playing a video game while Skyping with friends and family, or watching a movie and browsing the internet or downloading more games.

The forensic significance of researching the Xbox One is that the console can be used to commit illegal crimes. An Xbox One can be used either as a target, tool, or data storage unit for malicious intent. The Xbox One has the potential to be included in crimes such as computer fraud, child abuse and pornography, network intrusion, homicide, domestic violence, financial fraud and counterfeiting, e-mail threats, harassment and stalking, narcotics, software privacy, telecommunications fraud, and identity theft (USA DHS, 2007, p. 13).

By researching the Xbox One investigators have the ability to better know how the console works to get to the data they need to better help liberate or incarcerate a suspect. Each digital device is customized to its owner's specifications and can be modified further to enable illegal acts. If investigators have a better grasp on the ways in

which owners can modify their Xbox One then they have the ability to enter the digital investigation with proper knowledge and understanding of the Xbox One's full capabilities. Just like behavioral profiling of a suspect, an investigator can profile a digital device.

## 1.1 Statement of the Problem

This research is important for forensic investigators due to the challenge of technologies being pushed into the market at high speeds while digital forensic tools and investigators struggle to play catch-up. This research acts as a stepping stone for investigators to understand further how the Xbox One file system(s) structure stores data.

Digital forensic investigators are strongly encouraged to understand how the technology that they are investigating works down to the most technical level so they are aware of errors, the potential for anti-forensics, and the ability to prove their competence (Wedge, 2013). There is little published work on how the Xbox One interacts with its file system. This research is able to provide some of the answers for current investigators and provide direction for later research.

The investigators, researchers, and those in charge of creating, modifying, and replacing standards in the digital forensic field are all stakeholders in this research. The Xbox One is but a single device to be examined but with the number of features, the Xbox One has the ability to execute, makes it very personalized to its owner and could contain valuable digital evidence.

## 1.2 Research Question

The question to be answered is: How do the file system(s) of the Xbox One store data on its hard disk?

## 1.3 Statement of Purpose

Research on the newest devices allows current and future digital forensic investigators to understand how the system works. Carrier (2005) states that by understanding how a system works the examiner has the ability to know the full potential of the device leading to quicker and smarter investigations. This also allows digital forensic investigators to save time, money, and resources because the foundational research is already done. They can then allocate these resources to other priorities. By understanding how the Xbox One stores data on its hard disk investigators are closer to understand the device's potential for anti-forensics and also have the ability to prove competence and understanding of the Xbox One.

## 1.4 Assumptions

The assumptions inherit to this project include:

- The Xbox One chosen for this research has not been altered in any way before unboxing.
- The Xbox One is working within tolerable error in the way Microsoft meant it to.

- The Xbox One has three operating systems which meant there was a possibility it had multiple file systems.

## 1.5 Limitations

The limitations inherit to this project include:

- The research conducted was by interacting with the Xbox One gaming console following the methodology taken from NIST General Test Methodology for Computer Forensic Tools
- The hardware that was forensically imaged in this research was the hard drive.
- Tested the tools with a different internal hard drive. Being a different hard drive from the Xbox One's drive for these tests is a low risk understood by the researcher.

## 1.6 Delimitations

The delimitations inherit to this project include:

- The embedded memory was not looked at in this research.
- Interaction with Microsoft's SkyDrive, or cloud, was not be looked at in this research.
- Error rate was not examined.
- The encrypted blocks on the hard drive were not decrypted.

# CHAPTER 2. REVIEW OF LITERATURE

## 2.1 The PlayStation 2

The PlayStation 2 (PS2) is a gaming console created by Sony and released on March 4th, 2000 (Tyson, 2012). The PS2 has the option to have an external 40GB hard drive attached and the option to connect to the internet via Ethernet. Sony used the PlayStation File System (PFS) for the PS2 hard disk (Wiki, 2014). This file system is a proprietary file system created and used by Sony. It was also found that the file system of the memory cards used for the PS2 closely resemble MSDOS FAT (Ridge, 2000).

## 2.2 The PlayStation 3

The PlayStation 3 (PS3) was the third generation of the PlayStation systems, which was released in November 2006 (Conrad, 2010). The PS3 was used in a crime involving Anthony Scott Oshea, 24 years old, who was storing pictures of child pornography on his PS3 gaming console (Conrad, 2010). Investigators were able to identify the girl in the photos as "an 11-year-old from Houston, Texas" (Conrad, 2010 p.1). Oshea was able to convince the girl to send him the nude photos of herself over the PlayStation Network via email from her PS3 to his PS3 and then also sent the illegal photos to "people in at least 5 other states" (Potter, 2009).

The Xbox systems and the PlayStation systems are very different in their software technologies as Sony and Microsoft have been avid competitors in the gaming realm for years. Nintendo was also in that race but has been taking more of a back seat in the dueling company wars. As for the actual capabilities of the PS3, Sony allows its users on the PS3 to partition the hard drive themselves, which allows users to add their own operating systems as well as potentially hiding partitions and other questionable and illegal materials (Conrad, 2010).

The PS3 has a single operating system, an internal magnetic hard disk storage, and internet accessibility through Ethernet cable and Wi-Fi. The file system of the PS3 is difficult to identify like its predecessor the PS2. The research found discusses the file system of the PS3 as FAT32 but studies show that the FAT32 file system is just a file system that the PS3 supports, not necessarily one of which it runs. The actual file system of the PS3 is actually a proprietary file system that can cause issues for investigators as Sony has not been the most forthcoming with information on its set up (PS3FAQ, 2013).

## 2.3 The Xbox

The Xbox was released November 15th, 2001 and "largely relies on stock PC hardware modified for use as a game console" (Burke, 2007 p.2). Having simply been modified from stock hardware from PC's, the Xbox was a popular gaming console to be altered by its users for non-gaming uses and projects. The file system Microsoft used for the hard drive of the Xbox was an altered version of FAT32, which they began to call

FATX. Forensic tools that could read FAT32 had difficulties reading anything in FATX after this change until research was done and updates were pushed out (Burke, 2007 p.2).

Burke and Craiger (2007) conducted research to explore the Xbox for forensic investigators. They found that the hard drive of the Xbox was difficult to image as errors would occur if Windows or Linux programs attempted to access the stored data. The data on the hard drive locks unless the hard drive gets a 32-byte password generated from the Xbox's ROM, serial number, and model number (p.2). Burke and Craiger (2007) created a work around this problem by connecting to the Xbox as root through SSH and imaging each partition (p.5).

Rabaiotti and Hargreaves (2010) also showed alternative ways to image data stored on the Xbox. The storage being imaged was the Xbox's RAM by using a buffer overflow exploit to push out any data being stored creating a raw image (p.97).

## 2.4 The Xbox 360

The Xbox 360 was released on November 22nd, 2005. This console has one operating system and a custom volume handler working together to better handle data stored on its hard disk (Nelson, 2014 p. S49). The Xbox 360's hard disk file system is XTAF, which is said to be similar to FAT by Alex J. Nelson, Erik Q. Steggall, and Darrell D. E. Long (2014):

> File allocations are still handled with block chains in a File Allocation Table. Directory entries and inodes are a single, conflated concept. The superblock is also a simple structure… The most significant changes in interpreting the directory entry data are how timestamps and names are handled. Timestamps use one format for modification, access, and creation times, with a granularity of two seconds. Names are a single 42-byte field, that are only designed to store ASCII characters (p. S49).

These differences between FAT and XTAF allow forensic investigators to get a better idea on what they are looking at. Without the knowledge of what file system they were looking at on an Xbox 360, the investigators could potentially interpret data improperly (such as the file system header and modified/created/accessed times), which would then alter the timeline they were attempting to create or even cause the investigator to not understand what they were really looking at inevitably allowing data to fall through the cracks (Nelson, 2014 p. S49). One can also see that XTAF is FATX backwards which should be a huge indicator to the relationship between the two file systems.

According to Bolt (2011), was called an "application-specific computer… the machine is designed to run one specific type of application: video games" (p.12). The Xbox 360 was designed simply to run games at the beginning of its creation but had the additional feature of network connectivity to include chatting and interaction with multiplayer and Xbox Live friendly games. This allowed for chat sessions between people over the internet and offered a whole new type of communication for crime to take part in under law enforcement's nose, but not for long. According to Bolt (2011) the

Xbox 360, along with the PS3 and Wii, were examined for forensic evidence in various criminal and civil cases and then the view on digital evidence identification began to focus in on gaming consoles of all types (p.4).

In 2006 a Ronnie Brendan Watts, 26, met a 14-year-old boy through the Xbox Live network (LiveJournal, 2006). Watts persuaded the boy to meet with him in a Santa Rosa park after talking and Watts sending multiple e-mails and pornographic videos. Watts molested the boy at the meeting point (LiveJournal, 2006). There have been similar cases like this across the country. In response to happenings like this, in 2012 the state of New York banned around 3,580 known sex offenders from online gaming due to the potential for them to use the anonymity of certain games (Good, 2012).

## 2.5 The PlayStation 4

The PlayStation 4 (PS4) was released November 15th, 2013 as the Xbox One's competition. In hardware they are almost identical. The biggest differences between the two consoles are the file system and the operating system. The PS4 uses a single operating system named Orbis OS, which is a modified version of FreeBSD 9.0 (Humphries, 2014). The file system of the PS4 has not been identified in publications, which leads some to believe that Sony stuck with or modified their PS3 proprietary file system for the PS4 but this is just an assumption based on Sony's previous pattern with the PS3 and PS2.At the time of this research there were no articles to be found currently on digital forensic analysis of the PS4, which is not surprising as the file system is also

still unknown. It is still worth noting though in this literature review as this is the Xbox One's main competitor in the gaming console realm.

## 2.6 The Xbox One

### 2.6.1 Previous Studies

In the summer of 2014 Digital Investigation published an article titled *Preliminary Forensic Analysis of the Xbox One*. The researchers looked at an Xbox One to create a preliminary forensic analysis by answering the questions: what is the file structure of the Xbox One console system, and what forensically valuable information is available on the console, and where is that information located? The researchers were able to get some of these answers through three different phases in their research(Moore, 2014). Each of these phases had forensically sound images produced and each image was then analyzed and compared to each other. In phase 1 their Xbox One was reset to factory settings and imaged while using a write blocker. Phase 2 was to get the hard drive reinstalled in the console, install various games, importing data for the examination, connecting the console to a cable box, signing in with facial recognition and without, and viewing friend's gameplay. Phase 3 included connecting the console to the internet and visiting various applications and playing games using the Xbox Live network(Moore, 2014).

The researchers also were able to gain network packet captures to view what kind of information the Xbox One uses to communicate over the Xbox Live network. Through

this research they were able to determine that the Xbox One has five partitions: Temp Content, User Content, System Support, System Update, and System Update 2. The researchers also found what areas of the hard drive were being kept encrypted, different file types the Xbox One comes with, changes in time zone and time stamp records, what changes on the system when the console connects to the Xbox Live network, and entropy scores completed for all files. The research team also released the images taken along with obtainable data for the public to view and analyze (Moore, 2014).

### 2.6.2 Xbox One Technical Specifications

The console's internal hardware consists of an 8-core x86 AMD Jaguar CPU combined with an AMD Radeon graphics GPU, 8GB of DDR3 SDRAM, 8GB SK Hynix H2M42003GMR eMMC NAND flash memory, and a 500GB hard drive (via SATA connection) (iFixit, 2014). The input/output methods of the console are: a power connection, HDMI out, HDMI in, digital optical audio out, three USB 3.0 ports, one Kinect port, infrared output, one Ethernet port, one Blu-ray/DVD/CD drive (via SATA connection), and a touch activated power sensor, Wi-Fi 802.11ac, NFC (iFixit, 2014).

The 8-core processor allows the user to switch in-between their game and the applications used on the system, including web browsing(Microsoft, 2014). The user is also able to use certain apps at the same time as playing a game or watching TV with the use of Microsoft's application SmartGlass. The Xbox has an HDMI pass-through as well, to allow the user to pass the Xbox One through their TV to ease switching inputs of devices connected to the TV. The Xbox One has the option to be purchased with a Kinect

2.0 sensor bar. This additional accessory allows the Xbox One to view gesture controls, hear voice commands, and automatically log a known user into their Xbox Live account based on facial recognition software (Microsoft, 2014).

Two other interesting features of the Xbox One is its Game DVR and voice command. The Game DVR feature allows users to have "a continuously recording backlog of the last 5 minutes (of game play)" (Stein, 2013). This could prove to be interesting for forensic investigators to assist in creating a timeline of events. The voice command feature is another feature to should stand out for forensic investigators. If the Xbox One is off and so is the TV the user can walk into a room and say "Xbox On" and the system turns on as well as turns on the TV. In order for this to happen that means that the Xbox One is always on, even if just in a lower power state, in order to hear and react to the voice commands (Stein, 2013).

The site iFixit.com proves to be useful, as they have videos, pictures, and descriptions as how best to extract the hard drive disk of the Xbox One safely without causing harm to the console itself (iFixit, 2014). According to iFixit's Xbox One teardown, when connecting the Xbox One's hard drive disk to their test computer they found five New Technology File System (NTFS) partitions (iFixit, 2014).

Due to the research done by Moore, Baggili, Marrington, and Rodrigues the partitions have been identified to have the file system as some form of NTFS. This is important to know as the researcher knows now that there is some element in the Xbox One that is signaling to other tools that it is NTFS. By identifying certain elements of the operating system and how it interacts with an NT file system, there are certain flags used

with file structures and metadata structures that showed what is happening which allowed the researcher to answer the research question.

Carrier (2005) states by knowing how a file system works on a device, the investigator can conduct a smarter investigation which in turn "reduces the time needed to conduct an investigation" (p.12). The investigator also is more aware of how the tools they are using work when they understand file system structures According to Carrier (2005):

> An NTFS file system does not have a specific layout like other file systems do. The entire file system is considered a data area, and any sector can be allocated to a file. The only consistent layout is that the first sector of the volume contain the boot sector and boot code (p.199).

Carrier (2005) also points out that the Master File Table (MFT) is a huge give away for NTFS because it is what keeps track of all the files in the file system. The MFT stores meta-data on every file within the file system and because everything within NTFS is a file that means the MFT is a gold mine of data for investigators (p.199).The Xbox One has three different operating systems working simultaneously so the researcher is curious to know if the console is using a true NTFS, hybrid version, or an updated version and if so what are the changes it has done to data storage on the hard disk to answer the main research question.

Mentioned as well in a publication testing metadata verification on the Xbox 360, Nelson mentions how the Xbox 360's file system is XTAF but that file system seems to be abandoned by the Xbox team and they have been integrating NTFS within the Xbox

One (Nelson, 2014). Microsoft has also been dealing with the creation of Resilient File System (ReFS) for Windows Server 2012 but there has not been any mention of possible overlap between changes in the Xbox One NTFS version and ReFS (Microsoft, 2013).Since the Xbox One has been released to the public there have been 11 updates to the operating system of the Xbox One. The update "6.2.11511.0 (xb_rel_1409.140829-1829) fre" (Xbox Support, 2014) is the most recent update released September 2nd, 2014 by Xbox Support.

# CHAPTER 3. METHODOLOGY

The researcher analyzed the Xbox One with a methodology that was adapted from the National Institute of Standards and Technology (NIST). This NIST methodology has been used and adapted in the past for similar research by Leshney (2008) and Gillam (2007). The methodology has been reviewed directly from NIST and adapted to meet the demands and stay within the scope of the research conducted.

The researcher used a write-blocker and hash functions to check the integrity of the data stored on the Xbox One's hard disk as well as each individual file. The researcher used a hardware write blocker to keep the original device's data from being altered by disabling the hard drives write ability when being forensically imaged.

Kit #4 contains the Digital Intelligence UltraKit. The Tableau Firewire 800 + USB 2.0 SATA Bridge (firmware v5.20 ) was used for write blocking to connect the test hard drive (TD1) and Xbox One hard drive (TC1, TC2, TC3) to the computer when imaging. The write blocker is crucial in the imaging process as it blocks the possibility of the computer and imaging program from writing data on the test case hard drive. If the program were allowed to write data, on the hard drive being investigated, then it has the potential to alter results making the research flawed. A hash function was used to show that the data from each forensic image has not been altered in any way shape or form upon analysis. The hash functions used were the MD5 and SHA1 hash functions. Each

image hash check sum was compared with the hard drive hash check sum value after the image is first created and after the analysis of that image is completed as to show that no data was altered before, during, or after imaging and analysis.

## 3.1 Method

The method used is from NIST's General Test Methodology for Computer Forensic Tools are under the approach section which asks for the following (NIST, 2001):

1. Develop test assertions based on requirements
2. Identify relevant test cases
3. Develop testing procedures and method
4. Report test results

### 3.1.1 Test Assertions

Within the research conducted "develop test assertions based on requirements" (NIST, 2001)is the first step in the methodology. This beginning step allows the researcher to stay on track and within the scope of the research. The test assertions developed within the scope of the proposed research are shown in Table 3.1.

*Table 3.1* Test Assertions to Test Cases

| Test Assertions | | Test Cases |
|---|---|---|
| Unboxed Data | → | Case #1 |
| Updated System Data | → | Case #2 |
| User Data Interaction | → | Case #3 |

These test assertions work in relation to the test cases developed. Within each test case the test assertions are imposed as the defining data variable when the researcher interacts with the Xbox One. This is the first step in changing data between the test cases.

### 3.1.2 Test Cases

The second step in the researcher's methodology is to "identify relevant test cases" (NIST, 2001). Three test cases are created based upon states that the gaming console's hard disk could be under in a search and seizure event, as shown in Table 3.2. The test cases were compared with each other to determine any major changes in data storage such as file slack, deleted files, and orphan folders.

*Table 3.2* Xbox One Test Cases

| Test Case | Test Assertion | Data Change |
|---|---|---|
| TC1 | Unboxed Data | Out of the box Xbox One. Acts as base line test case. |
| TC2 | Updated System Data | Xbox One updated to v6.2.12130.0 (xb_rel_1502.150209-1738) fre |
| TC3 | User Data Interaction | Top 25 most popular applications installed& accesses, 2 games installed and accessed, & user profile created. |

#### 3.1.2.1 Test Case #1

The first test case is to look at an Xbox One's hard disk after the gaming system has been first taken out of the box. This test case acted as the state of the Xbox One as if it has not been played on or touched by a user. This was used as a control test case for the research, as no test data has been created on the hard disk. Refer to Appendix A for the Test Case Creation Procedure for details.

#### 3.1.2.2 Test Case #2

The second test case looks at the TC1 hard disk after it was updated to OS version.2.12130.0 (xb_rel_1502.150209-1738) fre (Xbox Support, 2014). Hard drive retrieval and imaging follows the same procedures as TC1. Refer to the Appendix A for the Test Case Creation Procedure for details.

#### 3.1.2.3 Test Case #3

The third test case looked at the TC2 hard disk after it had been altered with user data generated by the researcher thus creating TC3. The top 25 most popular applications were downloaded and installed on the Xbox One as well as two games. The applications were chosen because they are currently the most popular downloaded apps listed in the Xbox Store. The games were chosen as they were launch titles for the Xbox One when it was first released. These games help showcase the features of the Xbox One. To gauge a baseline of how the Xbox One saves popular file types on its hard disk a variety of data files were attempted to be copied onto the Xbox One's hard disk. Refer to the Appendix

A for the Test Case Creation Procedures and Data Files List for details. The files were taken from NIST resources of test files (CFReDS, 2013).

Once the Xbox One had application and game play data generated, the TC3 hard drive was imaged in the same way TC1 and TC2 were. The images taken from TC3 was compared to the images taken from TC1 and TC2 to look for any changes in the way the Xbox One's file system has been saving data.

### 3.1.3 Procedures and Methods

The third step in the researcher's methodology is to "develop testing procedures and method" (NIST, 2001). The procedures identified are, to create a bit-copy of an Xbox One's hard drive for each test case with the use of a hardware write blocker, MD5 & SHA1 hash functions, and FTK Imager 3.1.4.6 (or newest version). Duplicates of the bit-copy images were stored as a back-up; one as a working copy and one as a library backup. By the use of the tools FTK Imager 3.1.4.6, and Autopsy 3.1.1were used to analyze the bit-copy image to determine how the file system of the Xbox One stores data by interpreting the hex within the copies.

Each test case involves the researcher to ground self, apply the test case changes to the Xbox One, removal of the Xbox One's hard disk from the console, imaging, relocating the hard disk to the Xbox One, and analysis of the bit-copy image. A final comparison was done as to note the changes occurring with the data between each imaging process. Refer to the Appendix A for Steps of the Process for handling the Xbox

One hard disk and images. If at any point the researcher feels the need to reimage the Xbox One hard disk, these steps were followed starting from the Test Stage.

### 3.1.4 Results

The fourth and final step in the researcher's methodology is to "report test results" (NIST, 2001). After the analysis stage is complete, within the steps of the process, the researcher began to report results found.

## 3.2 Validity

The research is exploratory by nature. Validity is met within this research when the research question is answered by explaining what was found within the Xbox One's file system. The researcher is following a similar methodology that was followed by Leshney (2008). Leshney borrowed methodology steps from NIST's General Test Methodology for Computer Forensic Tools in their study which was also exploratory (Leshney, 2008). The details to each step within this research are different because they are tailored to help answer a different research question.

# CHAPTER 4. RESULTS

TC1, TC2, and TC3 were compared to each other. The test cases were used to determine any major changes in data storage on the Xbox One; such as deleted, changed, or added files and folders. The test cases are three possible states an unmodified Xbox One could be in if an investigator had to forensically investigate the gaming console. The Xbox One underwent various updates and data changes and because of this the researcher needed the three test cases to make sure that the file system would not change. It is not normal for the file system to change under an update but because the system uses three OS's simultaneously, which within itself is new to gaming systems, the researcher had to be sure of what was happening to the file system during these test case changes. Reference Appendix A for the test case creation procedures.

Note that throughout the results there is a directory listed as "[orphan]" parallel to the root directory. This does not reside on the Xbox One's hard drive this is simply a directory that one of the tools, FTK Imager 3.1.4.6, adds into the evidence tree to display items that no longer have a parent directory.

## 4.1 Test Case #1

Reference Appendix C-D for the TC1 imaging and analysis process. The first thing noticed was the Xbox One has 5 partitions with unpartitioned space as seen in Table 4.1.

*Table 4.1* Xbox One Partitions

| # | Name | Size | Reported File System |
|---|---|---|---|
| 1 | Temp Content | 41984MB | NTFS |
| 2 | User Content | 373760MB | NTFS |
| 3 | System Support | 40960MB | NTFS |
| 4 | System Update | 12288MB | NTFS |
| 5 | System Update 2 | 7168MB | NTFS |
| - | Unpartitioned Space | - | GPT |

The tools (FTK Imager and Autopsy) reported NTFS as the file system. To double check if this is actually true the researcher went to the MBR to check the partition table. Instead of a traditional MBR there was a Protected MBR located at Logical Block Address (LBA) 0. Figure 4.1 shows a screen shot of the Xbox One Protected MBR.

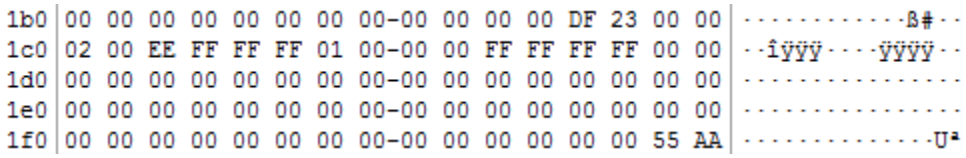



*Figure 4.1* Protected MBR

Understanding the partition table of the Xbox One allows the investigator to know how the partitions are broken up on the hard disk of the console which also allows for better knowledge on what file system and probability of the file system version. The type of file system and its version gives the researcher a structural understanding of how data

is stored on the Xbox One. The researcher was able to identify this MBR as a Protected MBR which is different from a legacy MBR.

The legacy MBR would have a partition table beginning at offset “1ce” but there are no entries for active partitions here because this is a Protected MBR. This is causing the entire disk to be protected by legacy OS’s so the GUID Partition Table (GPT) layout can reside on the entire disk (UEFI Inc, 2014, p. 163). This means that the whole hard drive of the Xbox One uses GPT with a set file system within each partition. The Protected MBR is acting as a way for legacy systems to be used with the Xbox One’s system as well as protecting the MBR as not to disrupt the newer system that has been implemented on the gaming console. This is why in Table 4.1 it shows GPT as the reported file system in the unpartitioned space.

This Protected MBR looks standard and follows the UEFI Inc. standards (UEFI Inc, 2014, p. 163). This Protected MBR is showing that it is unbootable, the partitions begin at C0, H0, S2 which is where the Primary Partition Entry Array is located, and that there is one sector before the partitions. The only item that was not represented was at offset 0x1c3 and 0x1ca. According to UEFI Inc. (2014), these values can be 0xFFFFFF and 0xFFFFFFFF if the values are too large to represent. This is slightly odd because the Xbox One’s hard drive is only 500GB which is under the UEFI/GPT limit. This is discussed further in section 5.3 Future Research. Table 4.2 gives the meaning of each hex entry within the Xbox One Protected MBR.

*Table 4.2* Xbox One Protected MBR Hex Meanings

| Hex | Offset | Meaning |
|---|---|---|
| 00 00 00 00 | 1b8 | Unique MBR Disk Signature (Unused by UEFI and set blank here) |
| DF 23 | 1bc | Unknown (unused by UEFI) |
| 00 | 1be | BootIndicator: Stating not bootable |
| 00 02 00 | 1bf | Starting CHS: Stating that the partitions begin at Cylinder 0, Head 0, Sector 2 |
| EE | 1c2 | OSType: Stating the partition type is GPT partitioned disk. |
| FF FFFF | 1c3 | EndingCHS: Is set to 0xFFFFFF because it was not possible to represent the value. |
| 01 00 00 00 | 1c6 | StartingLBA: Stating that there is 1 sector preceding the partitions, which is the MBR here. |
| FF FFFFFF | 1ca | SizeInLBA: Normally "set to the size of the disk minus one" (UEFI Inc, 2014, p. 104) but is 0xFFFFFFFF because the disk was too large to be represented. |
| 55 AA | 1fe | End Signature |

Note. Adapted from *Unified Extensible Firmware Interface Specification v2.4 Errata B, p.103.* By Unified EFI, Inc 2014.

Since the Xbox One is using GPT, it was assumed that it is also working off of a Unified Extensible Firmware Interface (UEFI) at this point (Nikkel, 2009). This assumption was checked by viewing LBA 1 to find the GPT Header. The GPT Header had information about the Xbox One system including where the partition table is, the

version of GPT header, and the Disk Globally Unique Identifier (GUID or UUID). See Figure 4.2 for a screen shot of the Xbox One GPT Header.

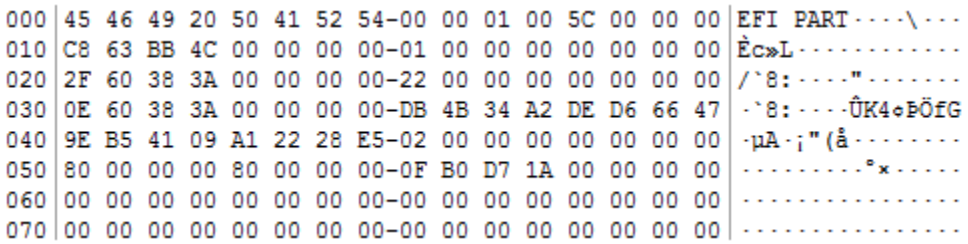



*Figure 4.2* Xbox One GPT Header

From Figure 4.2, the Xbox One reveals itself as a UEFI/GPT system. This is different from the legacy BIOS/MBR system found on legacy Microsoft systems. The UEFI/GPT system was created for larger systems so they could handle more data and features. A difference is that the MBR was limited to 32 bits wide, 3 primary partitions and an extra partition entry for logical partitions. This limits the maximum disk size that the BIOS/MBR can handle to 2 Terabyte. The UEFI/GPT system can have 128 partitions with 64 bit wide which means it can handle disk sizes up to 8 Zettabytes (which is 8,000,000,000TB) (Nikkel, 2009).

The GPT header also contains a Cyclic Redundancy Check (CRC) to check the integrity of the GPT Header (Microsoft, 2015). The GPT Header has a CRC32. This checksum acts as an error check function and is only for GPT Header errors. Table 4.3 describes the meanings of the Xbox One GPT Header hex.

*Table 4.3* Xbox One GPT Header Hex Meanings

| Hex | Offset | Meaning |
|---|---|---|
| 45 46 49 20 50 41 52 54 | 000 | "EFI PART" |
| 00 00 01 00 | 008 | GPT Header version 1.00 |
| 5C 00 00 00 | 00C | Each logical block is 92 bytes |
| C8 63 BB 4C | 010 | CRC32 of the GPT Header checksum is "4CBB635C" |
| 00 00 00 00 | 014 | Reserved space (blank) |
| 01 00 00 00 00 00 00 00 | 018 | "LBA location of the GPT Header" at 0x0000000000000001. |
| 2F 60 38 3A 00 00 00 00 | 020 | LBA address of the backup copy GPT Header which is at sector 976773167 |
| 22 00 00 00 00 00 00 00 | 028 | "First usable LBA sector for any partition" which is at sector 34. |
| 0E 60 38 3A 00 00 00 00 | 030 | "Last usable LBA sector for any partition" which is at sector 976773134. |
| DB 4B 34 A2 DE D6 66 47 9E B5 41 09 A1 22 28 E5 | 038 | This is the Disk Globally Unique Identifier (UUID) which is 0xE52822A10941B59E4766D6DEA2344BDB |
| 02 00 00 00 00 00 00 00 | 048 | Sector 2 is the starting LBA of the GPT array. |
| 80 00 00 00 | 050 | "Stating the number of partition entries" which is 128 here. |
| 80 00 00 00 | 054 | Each partition entry size which is 128 bytes here. |
| 0F B0 D7 1A | 058 | Partition Entry Array CRC32. Number of partition entries * size of the partition entries = 0x1AD7B00F. |
| 00... | 060 | Reserved |

By following the GPT Header we see that the Primary Partition Entry Array is at LBA 2. The Primary Partition Entry Array is the GPT version of the legacy MBR partition table. There is more data as well as data integrity checking within a Primary Partition Entry Array. Figure 4.3 shows a screen shot of the Primary Partition Entry Array.

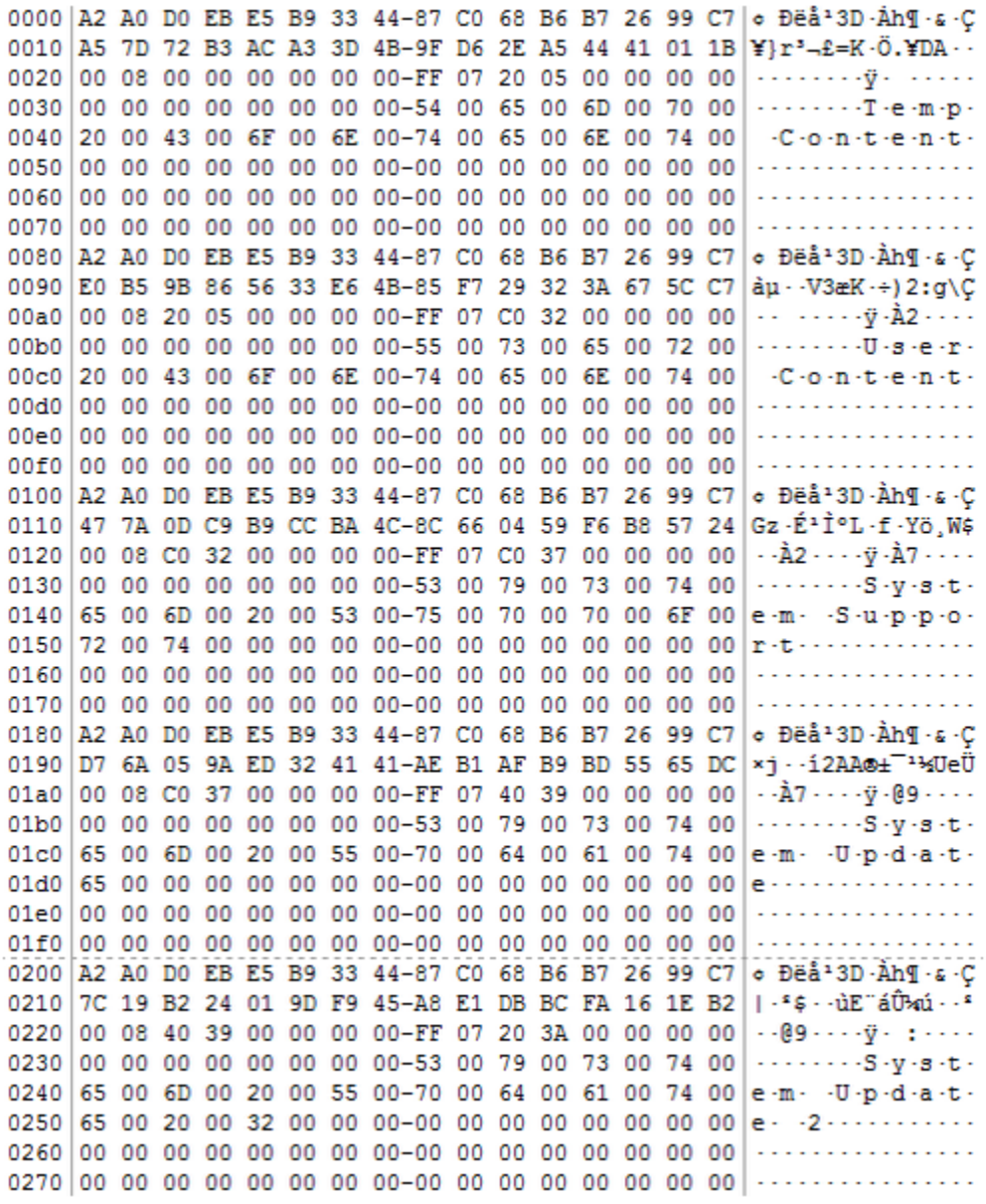



*Figure 4.3* Xbox One Primary Partition Entry Array

The Primary Partition Entry Array shows similar information that would be saved in a regular MBR partition table but the GPT partition table holds more information such as a partition GUID, the partition type GUID, and each partition's full name which is limited to a 36 character Unicode string (Nikkel, 2009). Table 4.4 shows the hex meanings for the Primary Partition Entry Array.

*Table 4.4* Xbox One Primary Partition Entry Array

| Hex | Offset | Meaning |
|---|---|---|
| A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7 | 000 | Partition Type GUID: (Windows basic data partition) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 |
| A5 7D 72 B3 AC A3 3D 4B 9F D6 2E A5 44 41 01 1B | 010 | Partition GUID: B3727DA5-A3AC-4B3D-9FD6-2EA54441011B |
| 00 08 00 00 00 00 00 00 | 020 | Partition starting LBA: sector 2048 |
| FF 07 20 05 00 00 00 00 | 0028 | Partition ending LBA: 85985279 |
| 00 00 00 00 00 00 00 00 | 0030 | Partition attributes: empty |
| 54 00 65 00 6D 00 70 00 20 00 43 00 6F 00 6E 00 74 00 65 00 6E 00 74 00 | 0038 | Partition Name: T.e.m.p. .C.o.n.t.e.n.t. |
| A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7 | 0080 | Partition Type GUID: (Windows basic data partition) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 |
| E0 B5 9B 86 56 33 E6 4B 85 F7 29 32 3A 67 5C C7 | 0090 | Partition GUID: 869BB5E0-3356-4BE6-85F7-29323A675CC7 |

*Table 4.4 (Continued)*

| Hex | Offset | Meaning |
|---|---|---|
| 00 08 20 05 00 00 00 00 | 00a0 | Partition starting LBA: 85985280 |
| FF 07 C0 32 00 00 00 00 | 00a8 | Partition ending LBA: 851445759 |
| 00 00 00 00 00 00 00 00 | 00b0 | Partition attributes: empty |
| 55 00 73 00 65 00 72 00 20 00 43 00 6F 00 6E 00 74 00 65 00 6E 00 74 00 | 00b8 | Partition Name: U.s.e.r. .C.o.n.t.e.n.t. |
| A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7 | 0100 | Partition Type GUID: (Windows basic data partition) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 |
| 47 7A 0D C9 B9 CC BA 4C 8C 66 04 59 F6 B8 57 24 | 0110 | Partition GUID: C90D7A47-CCB9-4cBA-8C66-0459F6B85724 |
| 00 08 C0 32 00 00 00 00 | 0120 | Partition starting LBA: 851445760 |
| FF 07 C0 37 00 00 00 00 | 0128 | Partition ending LBA: 935331839 |
| 00 00 00 00 00 00 00 00 | 0130 | Partition attributes: empty |
| 53 00 79 00 73 00 74 00 65 00 6D 00 20 00 53 00 75 00 70 00 70 00 6F 00 72 00 74 | 0138 | Partition Name: S.y.s.t.e.m. .S.u.p.p.o.r.t. |
| A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7 | 0180 | Partition Type GUID: (Windows basic data partition) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 |
| D7 6A 05 9A ED 32 41 41 AE B1 AF B9 BD 55 65 DC | 0190 | Partition GUID: 9A056AD7-32ED-4141-AEB1-AFB9BD5565DC |

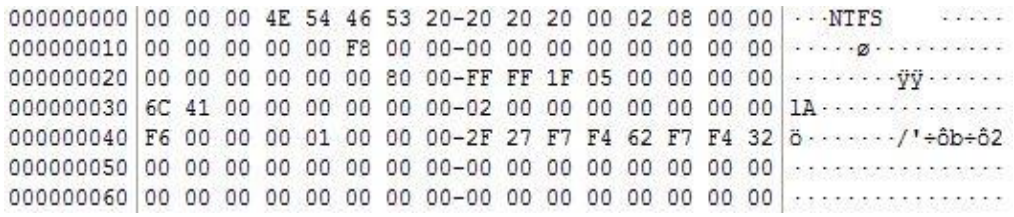
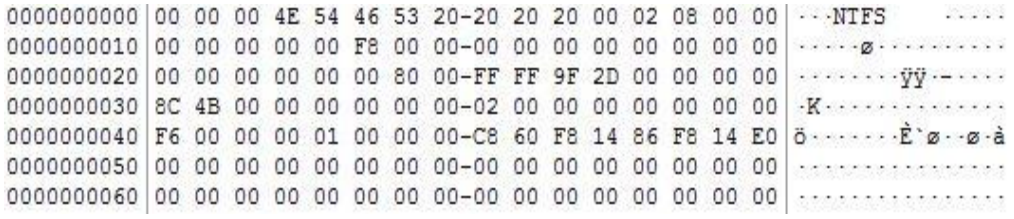
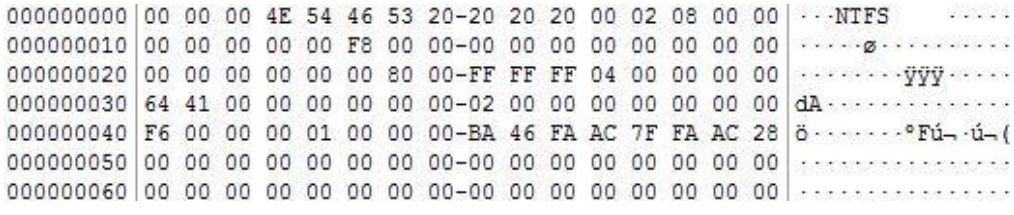
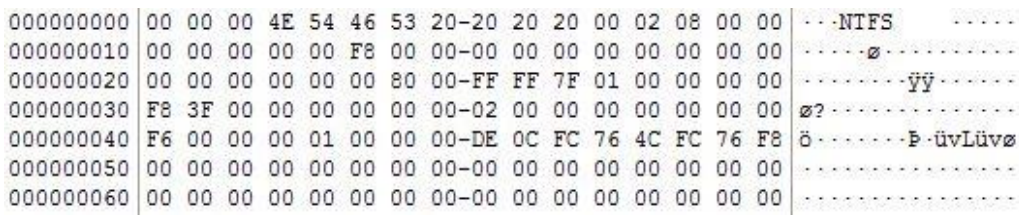
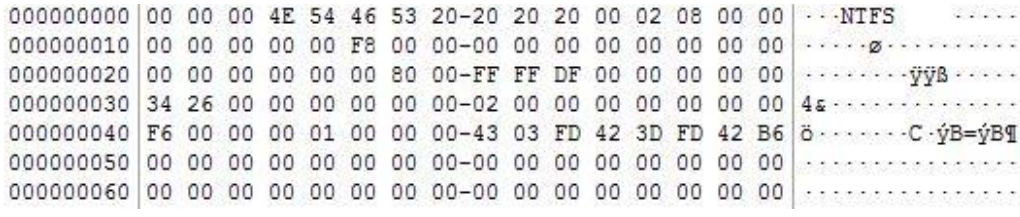
*Table 4.4 (Continued)*

| Hex | Offset | Meaning |
|---|---|---|
| 00 08 C0 37 00 00 00 00 | 01a0 | Partition starting LBA: 935331840 |
| FF 07 40 39 00 00 00 00 | 01a8 | Partition ending LBA: 960497663 |
| 00 00 00 00 00 00 00 00 | 01b0 | Partition attributes: empty |
| 53 00 79 00 73 00 74 00 65 00 6D 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 | 01b8 | Partition Name: S.y.s.t.e.m. .U.p.d.a.t.e. |
| A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7 | 0200 | Partition Type GUID: (Windows basic data partition) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 |
| 7C 19 B2 24 01 9D F9 45 A8 E1 DB BC FA 16 1E B2 | 0210 | Partition GUID: 24B2197C-9D01-45F9-A8E1-DBBCFA161EB2 |
| 00 08 40 39 00 00 00 00 | 0220 | Partition starting LBA: 960497664 |
| FF 07 20 3A 00 00 00 00 | 0228 | Partition ending LBA: 975177727 |
| 00 00 00 00 00 00 00 00 | 0230 | Partition attributes: empty |
| 53 00 79 00 73 00 74 00 65 00 6D 00 20 00 55 00 70 00 64 00 61 00 74 00 65 00 20 00 32 00 | 0238 | Partition Name: S.y.s.t.e.m. .U.p.d.a.t.e. .2 |

Here the Primary Partition Entry Array shows the partition type for each section as a basic data partition. According to Microsoft their UEFI/GPT systems must have an NTFS file system. Some differences between MBR partition tables to a GPT partition

table is that an MBR partition table has beginning and ending H/C/S where the GPT has beginning and ending sectors. By taking this information one can go to the beginning of each partition to check what file system is listed for each. Table 4.5 shows a screen shot of each of the Xbox One's partition headers, also known as the boot sector ($Boot).

*Table 4.5* Xbox One Partition Boot Sectors

| Partition | Boot Sector Screen Shot |
|---|---|
| Temp Content |  |
| User Content |  |
| System Support |  |
| System Update |  |
| System Update 2 |  |

Throughout each test case each partition's boot sector stayed the same. Notice in Table 4.5 that from offset 0x00 to 0x29 everything is the same, then the hex values begin to change beginning at offset 0x2a. Table 4.6 shows the boot sector hex meanings for each partition. Note that the table is sectioned off to have different partition entries after offset 0x28 so show the different hex meanings.

*Table 4.6* Xbox One Partition Boot Sector Hex Meaning

| Partition | Hex | Offset | Meaning |
|---|---|---|---|
| 1-5 | 00 00 00 | 000 | Jump Instruction: (none here) |
| 1-5 | 4E 54 46 53 20 20 20 | 003 | OEM ID: NTFS (no version listed) |
| 1-5 | 00 02 | 00b | Bytes per sector: 512 |
| 1-5 | 08 | 00d | Sectors per cluster: 8 |
| 1-5 | 00 00 | 00e | Reserved sectors (must be zero by Microsoft specifications) |
| 1-5 | 00 00 00 00 | 010 | Unused |
| 1-5 | F8 | 015 | Media descriptor: Hard disk |
| 1-5 | 00 00 | 016 | Unused (must be 0) |
| 1-5 | 00 00 00 00 00 00 00 00 | 018 | Unused (must not be checked) |
| 1-5 | 00 00 00 00 | 020 | Unused (must be 0) |
| 1-5 | 00 00 80 00 | 024 | Unused (must not be checked): is checked |
| 1 | FF FF 1F 05 00 00 00 00 | 028 | Total sectors in file system: 85,983,231 |

*Table 4.6 (Continued)*

| Partition | Hex | Offset | Meaning |
|---|---|---|---|
| 1 | 6C 41 00 00 00 00 00 00 | 030 | Starting cluster address of MFT: 16748 |
| 1 | 02 00 00 00 00 00 00 00 | 038 | Starting cluster address of MFT Mirror $DATA attribute: 2 |
| 1 | F6 | 040 | Size of MFT entry: 246 sectors |
| 1 | 00 00 00 | 041 | Unused |
| 1 | 01 | 044 | Size of index record: 1 sector |
| 1 | 00 00 00 | 045 | Unused |
| 1 | 2F 27 F7 F4 62 F7 F4 32 | 048 | Serial number |
| 2 | FF FF 9F 2D 00 00 00 00 | 028 | Total sectors in file system: 765,460,479 |
| 2 | 8C 4B 00 00 00 00 00 00 | 030 | Starting cluster address of MFT: 19340 |
| 2 | 02 00 00 00 00 00 00 00 | 038 | Starting cluster address of MFT Mirror $DATA attribute: 2 |
| 2 | F6 | 040 | Size of MFT entry: 246 sectors |
| 2 | 00 00 00 | 041 | Unused |
| 2 | 01 | 044 | Size of index record: 1 sector |
| 2 | 00 00 00 | 045 | Unused |
| 2 | C8 60 F8 14 86 F8 14 E0 | 048 | Serial number |
| 3 | FF FFFF 04 00 00 00 00 | 028 | Total sectors in file system: 83,886,079 |
| 3 | 64 41 00 00 00 00 00 00 | 030 | Starting cluster address of MFT: 16740 |

*Table 4.6 (Continued )*

| Partition | Hex | Offset | Meaning |
|---|---|---|---|
| 3 | 02 00 00 00 00 00 00 00 | 038 | Starting cluster address of MFT Mirror $DATA attribute: 2 |
| 3 | F6 | 040 | Size of MFT entry: 246 sectors |
| 3 | 00 00 00 | 041 | Unused |
| 3 | 01 | 044 | Size of index record: 1 sector |
| 3 | 00 00 00 | 045 | Unused |
| 3 | BA 46 FA AC 7F FA AC 28 | 048 | Serial number |
| 4 | FF FF 7F 01 00 00 00 00 | 028 | Total sectors in file system: 25,165,823 |
| 4 | F8 3F 00 00 00 00 00 00 | 030 | Starting cluster address of MFT: 16376 |
| 4 | 02 00 00 00 00 00 00 00 | 038 | Starting cluster address of MFT Mirror $DATA attribute: 2 |
| 4 | F6 | 040 | Size of MFT entry: 246 sectors |
| 4 | 00 00 00 | 041 | Unused |
| 4 | 01 | 044 | Size of index record: 1 sector |
| 4 | 00 00 00 | 045 | Unused |
| 4 | DE 0C FC 76 4C FC 76 F8 | 048 | Serial number |
| 5 | FF FF DF 00 00 00 00 00 | 028 | Total sectors in file system: 14,680,063 |
| 5 | 34 26 00 00 00 00 00 00 | 030 | Starting cluster address of MFT: 9780 |
| 5 | 02 00 00 00 00 00 00 00 | 038 | Starting cluster address of MFT Mirror $DATA attribute: 2 |

*Table 4.6 (Continued )*

| Partition | Hex | Offset | Meaning |
|---|---|---|---|
| 5 | F6 | 040 | Size of MFT entry: 246 sectors |
| 5 | 00 00 00 | 041 | Unused |
| 5 | 01 | 044 | Size of index record: 1 sector |
| 5 | 00 00 00 | 045 | Unused |
| 5 | 43 03 FD 42 3D FD 42 B6 | 048 | Serial number |

TC1 had 4693 total files throughout the entire image. Out of those 4693 files there were only 154 total unique hashes. Reference Table D.1 in Appendix D for TC1 Hash List. This test case is only specific for an Xbox One that is out of the box and has no unique user data on it but it is still good information to know because it is a baseline for what the Xbox One has on its system already.

## 4.2 Test Case #2

Reference Appendix E-G for creation, imaging, and comparison from TC2. From TC1 to TC2 it was found that the Protected MBR, GPT Header, the Primary Partition Entry Array, and Partition Boot Sectors had not changed at all.

What had changed between TC1 and TC2 was there were 4,679 total items (14 less than TC1), and 164 total unique hashes (10 more than TC1). Of the items from TC1 to TC2, 2 had been removed, 12 had been added, and 26 had been altered. The researcher is stating the changes as ‘items’ because there was a mix of file types, clusters, and meaningful sectors that were looked at for alterations, additions, and removals. There

were a plethora of clusters that had been added /removed/altered to and from the unpartitioned space within each partition including the unallocated space. This is discussed further in section 5.3 Future Research. Reference Table G.2, G.3, and G.4 within Appendix G for the full list of altered, added, and removed items.

The majority of altered files were within Temp Content. The majority of added files were within System Update, which is not surprising as this is the updating test case. For a forensic investigator this test case is good to know what it would look like because it shows that the user has not really done a whole lot with the system yet and so there may not be much forensic value in exploring further unless with probable cause to do so.

## 4.3 Test Case #3

Reference Appendix H-J for creation, imaging, and comparison from TC3. Like TC2 it was found that the Protected MBR, GPT Header, the Primary Partition Entry Array, and Partition Boot Sectors had not changed at all from TC2 to TC3. This is great information to know because it means that from out of the box to user generated data the file system and boot sequence of the Xbox One stays the same. This is important for a forensic investigator to be aware of because it lets them know if the Xbox One has been modified by the user if these items are not the same as Microsoft's specifications.

TC3 had 3,869 total items (810 less than TC2), and 185 unique hashes (19 more than TC2). Of the items from TC2 to TC3, 49 had been removed, 79 had been added, and 25 had been altered. Just like TC2, there were a plethora of clusters that had been added /removed/altered to and from the unpartitioned space within each partition including the

unallocated space. This is discussed further in section 5.3 Future Research. Reference Table J.2, J.3, and J.4 within Appendix J for the altered, added, and removed items.

A very important issue for forensic investigators found within TC3 is that within the partition User Content, there are huge blocks of data that are encrypted. The file names are in the form of GUIDs and the research assumes that these files are the applications and game data created by in the test case creation.

# CHAPTER 5.CONCLUSIONS AND DISCUSSION

The research question to answer was how do the file system(s) of the Xbox One store data on its hard disk? To answer this question the researcher also asked: is the console is using a true NTFS/hybrid version/an updated version, and what changes are there to data storage on the hard disk? The answer to these questions is that the Xbox One uses UEFI/GPT for its partitions and uses the file system NTFS for data storage.

## 5.1 Conclusions

The researcher was able to determine that the Xbox One works off of a basic disk utilizing UEFI/GPT. From Microsoft's specifications this system must have an NTFS file system, can have up to 128 partitions, has no need for extended or logical partitions, each partition can be larger than 2TB (if given a single large enough disk), the ability to support other operating systems, other partition types, and independent software vendors (Microsoft, 2015).

One of the fundamental elements of the UEFI design is the system partition which allows cross partition sharing to maximize the value of the platform "without significantly growing the need for nonvolatile platform memory" (UEFI Inc, 2014, p. 8). This could be how all three operating systems of the Xbox One are able to optimize the system while interacting with each other in addition to the Hyper-V ability.

The file system is confirmed as NTFS as well and the hierarchy of the system is simplified within the partitions as they each hold similar structures. Reference Figure M.1 in Appendix M.

## 5.2 Issues encountered

The first real issue encountered was within TC3 when data creation was happening. There were some applications that needed a credit card to be created. Due to the fact that the Xbox One was connected to an open network on a University Campus the network wasn't fully secure to use that sort of information. Upon finding that this type of data is encrypted when stored on the hard drive this issue was a moot point for the researcher.

The other issue encountered was when the data files, taken from NIST and listed in Table A.1 within Appendix A, to be placed on the hard drive were not being allowed to be copy and pasted. The researcher would need to create another test case that could alter the Xbox One system in order to force these files to reside on the hard disk for analysis. This was outside of the scope of the research and forfeited this task.

## 5.3 Future Research

The Xbox One offers a plethora of features that could assist forensic investigators with an investigation. Other areas of research to be explored include but are not limited to testing the full extent of the potential for anti-forensics, Kinect facial recognition error rate (including logon differences such as manual logon, facial recognition logon, or

automatic logon), in-depth network forensics, and user gesture profiles for behavioral analysis. All of these topics could assist investigators to better understand the workings of the Xbox One along with assisting in profiling their suspect based on their behaviors on this gaming system.

An unanswered question is why were the EndingCHS and SizeInLBA set to unknown values (0xFFFFFF and 0xFFFFFFFF) when the disk size was under the UEFI/GPT disk size limit? These values could be set to unknown values if the operating systems were booted from virtual machines. This also would allow for all three operating systems to work simultaneously. This was a speculation so this would be another area for future research as testing these hypothesis were outside the scope of this research.

One last item was that within the Xbox One's unpartitioned space of each partition, including the unallocated space, both FTK Imager and Autopsy were listing a plethora of clusters. Each time the test case changes these clusters would get new names. Each cluster name was the cluster ID. Most of the clusters had no data and a few had data within them. There was uncertainty as to what the clusters within the unallocated space of each partition represented. This would be another area for future research as testing this was once again outside the scope of this research.

In closing, this research provides test cases for scientists to see the technological advancements companies are using within their digital systems within the last year. Understanding what the file system is for the Xbox One allows digital forensic investigators to enter an investigation on this device without a blind fold that would force them to create similar redundant research that would cost them money and time that they

cannot spare. The researcher also welcomes any other researcher to recreate these test cases and see if they find differing results or further answers. Digital forensics is a growing field that relies on collaborative research to flourish. Never stop hunting for the right answers.

# LIST OF REFERENCES

# LIST OF REFERENCES


Bolt, S. (2011). *Xbox 360 forensics.* Burlington, MA: Elsevier.

Burke, P. &. (2007). Xbox forensics. *Journal of Digital Forensic Practice 1*, 1-8.

Carrier, B. (2005). *File system forensic analysis.* Upper Saddle River, NJ: Pearson Education, Inc.

CFReDS. (2013, March 1). *Computer forensics reference data sets: The CFReDS project*. Retrieved February 16, 2015, from CFReDS: www.cfreds.nist.gov

Conrad, S. D. (2010). Forensic analysis of a Playstation 3 console. In I. &. Ray, *Advances in Digital Forensics IV* (pp. 65-76). New York, NY: IFIP International Federation for Information Processing.

Gillam, W. B. (2007). *Macintosh forensic tool testing.* West Lafayette, IN: Purdue University.

Good, O. (2012, 12 9). *New York bans another 2,000 sex offenders from online gaming*. Retrieved from Kinja: http://kotaku.com/5969781/another-2000-sex-offenders-are-kicked-off-online-gaming-services

Henderson, H. (2009). *Encyclopedia of computer science and technology.* New York, NY: Facts On File, Inc, an imprint of Infobase Publishing.

Humphries, M. (2014, June 24). *PS4 runs modified version of the FreeBSD 9.0 operating system*. Retrieved October 5, 2014, from Geek: http://www.geek.com/games/ps4-runs-modified-version-of-the-freebsd-9-0-operating-system-1559866/

iFixit. (2014). *Xbox One teardown*. Retrieved October 3, 2014, from iFixit: http://www.ifixit.com/Teardown/Xbox+One+Teardown/19718

Leshney, S. (2008). *Discovered digital evidence from virtual machines: An exploritory study.* West Lafayette, IN: Purdue University.

LiveJournal. (2006, January 5). *Justice files: Accused molester met victim thru Xbox live*. Retrieved October 29, 2014, from LiveJournal: http://gamepolitics.livejournal.com/171996.html

McKemmish, R. (2008). When is digital evidence forensically sound? In S. S. Indrajit Ray, *Advances in Digital Forensics IV* (Vol. 285, pp. 3-15). Boston, MA: IFIP International Federation for Information Processing.

Meyers, M. R. (2004). *Computer Forensics: Meeting the challanges of scientific evidence.* West Lafayette, IN: CERIAS Purdue University.

Microsoft. (2013, November 1). *Resilient file system overview*. Retrieved September 15, 2014, from Windows Server: http://technet.microsoft.com/en-us/library/hh831724.aspx

Microsoft. (2014). *Developer network*. Retrieved October 29, 2014, from Hyper-V Architecture: http://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx

Microsoft. (2014). *Xbox One*. Retrieved February 28, 2014, from Xbox: http://www.xbox.com/en-US/xbox-one/meet-xbox-one#adrenalinejunkie

Microsoft. (2014). *Xbox One + Kinect*. Retrieved September 24, 2014, from Microsoft: http://www.microsoftstore.com/store/msusa/en_US/pdp/Xbox-One-+-Kinect/productID.285169400

Microsoft. (2015). *Windows and GPT FAQ*. Retrieved March 7, 2015, from Windows Dev Center - Hardware: https://msdn.microsoft.com/en-us/library/windows/hardware/dn640535(v=vs.85).aspx#ELD

Moore, J. B. (2014). Preliminary forensic analysis of the xbox one. *The International Journal of Digital Investigation & Incident Response 11*, S57-S65.

Nelson, A. S. (2014). Cooperative mode: Comparative storage metadata verification applied to the Xbox 360. *The International Journal of Digital Investigation & Incident Response 11*, S46-S56.

Nielsen. (2014). *An era of growth: The cross-platform report.* New York, NY: The Nielson Company.

Nikkel, B. (2009). Forensic analysis of GPT disks and GUID partition tables. *Elsevier in Digital Investigation: The International Journal of Digital Forensics and Incident Response, 6*(1-2), 1-18. doi:10.1016/j.diin.2009.07.001

NIST. (2001). *NIST test methodology for computer forensic tools.* National Institute for Standards and Technology.

NIST. (2013). *NIST IR 7298 revision 2, glossary of key information security terms.* Gaithersburg, MD: National Institue of Standards and Technology.

Potter, N. (2009, March 13). *PlayStation sex crime: Criminal used video game to get girl's naked pictures*. Retrieved October 29, 2014, from ABC News: http://abcnews.go.com/technology/story?id=7009977&page=1

PS3FAQ. (2013). *PlayStation 3 HDD FAQ*. Retrieved October 5, 2014, from Whirlpool: http://whirlpool.net.au/wiki/ps3_hdd

Rabaiotti, J. &. (2010). Using a software exploit to image RAM on an embedded system. *Digital Investigation 6*, 95-103.

Ridge, R. (2000). *PlayStation 2 memory card file system*. Retrieved October 26, 2014, from CSClub.Uwaterloo: http://www.csclub.uwaterloo.ca:11068/mymc/ps2mcfs.html

Rubin, P. (2013, April). *Wired exclusive Xbox One revealed*. Retrieved October 5, 2014, from Wired: http://www.wired.com/2013/05/xbox-one/

Sakr, S. (2013, May 21). *Xbox One runs three operating systems, including cut-down Windows for apps*. Retrieved March 1, 2014, from Engadget: http://www.engadget.com/2013/05/21/xbox-one-runs-three-operating-systems/

Stein, S. (2013, November 21). *Xbox One: 20 things you need to know.* Retrieved October 6, 2014, from Cnet: http://www.cnet.com/news/xbox-one-20-things-you-need-to-know/

Tyson, J. (2012). *How PlayStation 2 works*. Retrieved October 26, 2014, from How Stuff Works: http://electronics.howstuffworks.com/ps22.htm

UEFI Inc. (2014). *Unified extensible firmware interface specification v2.4 errata B.* Unified EFI, Inc.

USA DHS. (2007). *Best practices for seizing electronic evidence v.3: A pocket guide for first responders.* Washington, DC: NCJRS.

Wedge, T. (2013, May 28). *Training is not enough: A case for education over training*. Retrieved December 29, 2014, from Forensic: Magazine: On the scene and in the lab: http://www.forensicmag.com/articles/2013/05/training-not-enough-case-education-over-training

Wiki. (2014, March 29). *Playstation file system*. Retrieved October 26, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Playstation_File_System

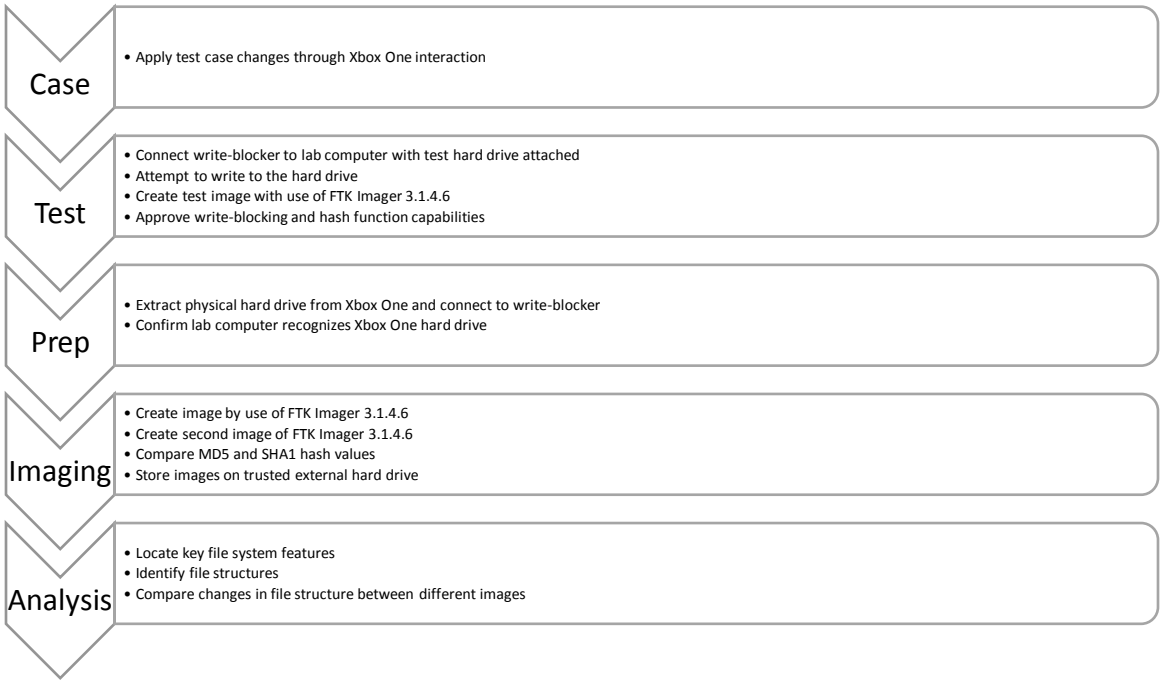
Xbox Support. (2014, September 2). *Xbox one operating system versions and system updates*. Retrieved October 5, 2014, from Xbox One: http://support.xbox.com/en-US/xbox-one/system/system-update-operating-system

Xynos, K. H. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *The International Journal of Digital Investigation & Incident Response*, 104-111.

# APPENDICES

# Appendix A. Test Case Creation Procedures

*Figure 0.1* Test Case Procedures



TC1 Steps of the Process

1. The Xbox One taken apart safely
2. Test case one hard disk (TC1) safely removed
3. TC1 connected to the SATA hardware write blocker
4. TC1 imaged (bit-copy image) using Access Data's Forensic Tool Kit (FTK) 3.1.4.6.
5. TC1_(date) .001 saved.
6. TC1 reconnected to the Xbox One

TC2Steps of the Process

1. The Xbox One connected to an Ethernet cable and turned on.
2. Create a test account through the Xbox Live network.
3. Begin the update and wait for the most recent update to complete.
4. Turned Xbox One off.
7. Once the Xbox One has been updated Xbox One taken apart safely.
8. Test case one hard disk (TC2) safely removed.
9. TC2 connected to the SATA hardware write blocker.
10. TC2 imaged (bit-copy image) using Access Data's Forensic Tool Kit (FTK) 3.1.4.6.
11. TC2_(date) .001 saved.
12. TC2 reconnected to the Xbox One.

TC3 Steps of the Process

1. Xbox One turned on and connected to an Ethernet cable to access the Xbox Live network and log in.
2. Install applications .
    a. Netflix, YouTube, Blu-ray Disc, Twitch, Xbox Video, Hulu Plus, Skype, Media Player, Amazon Instant Video, Pandora, Xbox Music, HBO Go, Upload Studio, Uplay, WWE Network, Halo Channel, EA Access Hub, Forza Hub, Crunchyroll, VUDU Movies & TV, ESPN, Plex, MLG, Audio CD Player, and Crackle.
3. Interaction with each application.
4. Data transfer from EX2 USB. Table A1 shows files and hashes.
5. Install games.
    a. Ryse: Sons of Rome&Forza Motorsport 5
6. Interact with game for 30 minutes each.
7. Turn off Xbox One
8. The Xbox One taken apart safely
9. Test case one hard disk (TC3) safely removed
10. TC3 connected to the SATA hardware write blocker
13. TC1 imaged (bit-copy image) using Access Data's Forensic Tool Kit (FTK) 3.1.4.6.
14. TC3_(date) .001 saved.
15. TC3 reconnected to the Xbox One

*Table 0.1* Files for Transfer to Xbox One

| File Name | File Type | Use | Size KB | MD5 | SHA1 |
|---|---|---|---|---|---|
| 000_0021 | .png | Graphic | 12663 | b1bdd6f22c1a622b6acf68ba95d6ad64 | 8f244b50a7ac8129f455b1e9c6ca74cf06a23640 |
| 100_0018 | .tiff | Graphic | 14619 | 70ea373e3b686f6ef295fd9a49fe1a13 | 1c4402f777440f15d8f5896156ddb647f8747208 |
| 100_0183 | .gif | Graphic | 130 | 0b910d6c21828e0b8be06322168fbd60 | eefd2bb644efb6d0ee57814992f8108834f8c0b2 |
| 100_0304crop | .bmp | Graphic | 4993 | a4f1f6095d8117aa00737f4b7f79c094 | 98b43081a49c83ca4e00e36e3e08bcab071ff01b |
| 02010025 | .pcx | Graphic | 788 | 1e846d0506d21dd8a08a0cd784ce4f19 | 76f8ad6854448c76c2b127cb5a1a5486ee3ba5b3 |
| 02010026 | .jpg | Graphic | 60 | 20f34a3f571d394ab9342ac21588e96e | 57cc6a1d54280f77674388ec31c1710bb8836ba3 |
| 09260002 | .jpg | Graphic | 60 | bb1e236cf935815e5bb714760b23f549 | 395e50118bc92973049709 56c2241059eabe7f8d |
| arc1 | .7z | Archive | 1104 | d1051cae37c82c24a019d03902c2d0c2 | 32f913fe68601e999baf77b92fe7ba934db99c83 |
| arc2 | .bz2 | Archive | 552 | 7e50af1887d7b39c3a900d99924ae521 | 4161f3045fc93bdfd22c34bf8aa0ea41967ab776 |
| arc3 | .gz | Archive | 50 | 2b2ac3fd281e2f1ff94257f47780ad9a | bf6ae4537bf5bf11f14f57d41812bda52637f86c |
| arc4 | .tar | Archive | 1185 | c52408fbba699fff0f6ea62ba86ab33d | e2f0d19d235d42ba34e8b5e643930f10ae12f21f |
| arc5 | .wim | Archive | 920 | 3fb5f789ab0d9693a9e11333fac463ef | c0934bb2668fe45d79c5606f033d749f8343c5c6 |
| arc6 | .rar | Archive | 849 | 15ccca7548228668d1fe8eead2ff10fc | ac892b4584fefd06712e9a530147f7ca8ac447dc |
| arc7 | .zip | Archive | 629 | 4c514453204a0eca1d8e46765ecaa4ce | 7b0ac44b60adabc3cfabb6929042e50c7e954529 |
| audio1 | .mp3 | Audio | 1029 | 4906f2b94eb7a95591396dca7fb9ef67 | 7f80f691ba21efdaf99df0e7381a5de7a16db3f6 |
| audio2 | .wav | Audio | 4505 | 5124c9db0a4c3269e8562b8ed2e85f66 | ddc5e2b60a59f2d3ef47340f4b224588a8ed628d |
| audio3 | .au | Audio | 9028 | ad0c2d9fd8ef051e6b3bfecfee780a44 | cac33b6d61c4b59252149f5a28e0abcb86a31340 |
| audio4 | wma | Audio | 1050 | 1e1eaa07418813407a3e12e685008570 | 7f2301958fb8024b702df1ed7a55bc26bdc299b4 |
| D1 | .pdf | Document | 3102 | 624eb29686b0b13974a804d66a6779d8 | ed7cfb2161941c474bf4beba65abb735bcbcddb7 |
| D2 | .pdf | Document | 2467 | d8b3bd66e9c38ce0af69658df3de8c78 | ca9b313594c4ab7986f1c75f42ac5505bdcf1777 |
| D3 | .xlsx | Document | 23 | 21f5ae676b06893a1ad7e7fc9da8a141 | a8798e9fa76f22e87c1602afebad5bb1e1f98682 |
| D4 | .xlsx | Document | 14 | d5a11e93b5bd2a6e7735fee921c0a6ea | da1b444a230350dc13cc46a72ccf96b77131e116 |
| D5 | .docx | Document | 5 | 038bc8f9138cc281ee9def3edadec4bd | aa97a1d5ee7befb60e370565c74e075a7125440a |
| D6 | .docx | Document | 4 | 00a289fca326a78e40420f33dfe77eac | 08f62b9f5bdaaecc48c4cc8fc8fbd981d3ef4223 |
| D7 | .pptx | Document | 882 | 3bb602b8f96c56a10bbc97a5e210678d | b7780bec19f40d2b06690b9e860dc801a4f0be14 |
| vid1 | .mp4 | Video | 1110 | d3bf39fa2f30b5acf644523d1a92ac82 | 49a35bb85084da324d393b1916559cbca5d4dd7b |
| vid2 | .avi | Video | 1436 | 20ca4356a2f152bae77c30f98f7e381f | e7cb37ede3bfc1c9594f07a0dcdeb391a7aa3eb6 |
| vid3 | .mov | Video | 486 | 074ce15293e30b338d5a0c5fe8cf5d88 | a961343baf828c5363e99907bed97c5b033e947a |
| vid4 | .flv | Video | 3627 | c57611b8e3052bd853d79e2de932aa3d | 7ba95033fd83d8013fc5cb3fba6834c0eb635677 |
| vid5 | .mpg | Video | 22050 | 57586384eb1f286ef9c2325b521dca4c | ed12faaa09ffffbca7682529c44b013c7bfb4f4b |
| vid6 | .wmv | Video | 2404 | abb8ca304b17d645aee1c46786361fe0 | 8e3cf8a8f0fe65e5d598b9e012f8a0291e72084e |

# Appendix B. Tool Test

Date: Wednesday February 11th, 2015 beginning at 12:04 pm
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228
Computer: CFLWIN15

- Windows 7 sp1 64-bit
- 8GB RAM
- Intel Core i5-2400S CPU @ 2.50GHz
- domain cit.lcl
- Time Zone Set:(UTS-05:00) Indiana (East) date set to Wednesday February 11th, 2015

Test Hard Drive: (TD1)

- Manufacturer: Toshiba
- Model: mq01abd050
- S/N: Y4CQTIBHTSB1
- P/N: PH2050U-1|54 593851-A0
- Size: 500GB 5400APM 8MB Cashe
- Physical: 2.5 SATA 3Gb/s
- Cylinders: 16,383
- Heads: 16
- Sectors: 63
- LBA: 976,773,168

External Hard Drive: (EX1)

- Manufacturer: Western Digital
- Model: N3565A
- S/N: WXF1A7221875
- P/N: WDBY8L0020BBK-01
- Size: 2TB

Tools:

- Disk Manager (Logical Disk Manager)
- FTK Imager 3.1.4.6
- Tableau Firewire 800 + USB 2.0 SATA Bridge

Steps of the Process:

1. Took SATA bridge and connected power cord, USB cord, SATA data, and SATA power to power cable. Connected USB to Computer, and connected TD1 to bridge. Turned on at 12:03:00. Computer detected hard drive as “USB Mass Storage Device” and “TOSHIBA MQ01ABD050 USB Device”.
2. Accessed disk management and found TD1 as “Disk 3 Unknown 465.76GB”. Prompted to “initialize a disk before Logical Disk Manager can access it”. Clicked OK. Got a message stating that the device was write protected.
3. Opened FTK Imager 3.1.4.6
    a. Create Disk Image
    b. Physical Drive
    c. \\PHYSICALDRIVE3 - TOSHIBA MQ01ABD050 USB DEVICE [500GB USB] → Finish → Add
    d. Raw (dd)
    e. Skipped case info entry
    f. Named image “TD1_2-11-15.001” and saved it on external hard drive EX1. Also changed Image Fragment Size to 0 so the image would not be broken up.
    g. Began imaging at 12:04 pm.
    h. Forced stop at 1:37pm. Tools proved to be imaging fine and write blocking. Turned off tools and disconnected TD1.

# Appendix C. Test Case 1 (TC1) Imaging

Date: Wednesday February 11th, 2015 beginning at 13:40
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228
Computer: CFLWIN15

- Windows 7 sp1 64-bit
- 8GB RAM
- Intel Core i5-2400S CPU @ 2.50GHz
- domain cit.lcl
- Time Zone Set:(UTS-05:00) Indiana (East) date set to Wednesday February 11th, 2015

Xbox One TC1 Hard Drive: (TC1)

- Manufacturer: Seagate
- Model: ST500VT000
- S/N: W3PA4MEL
- P/N: 1DK142-120
- FW: 0001MBC1
- Size: 500GB
- Physical: SATA 2.5”
- CHS and LBA not listed

External Hard Drive: (EX1)

- Manufacturer: Western Digital
- Model: N3565A
- S/N: WXF1A7221875
- P/N: WDBY8L0020BBK-01
- Size: 2TB

Tools:

- Windows Explorer
- Disk Manager (Logical Disk Manager)
- FTK Imager 3.1.4.6
- Tableau Firewire 800 + USB 2.0 SATA Bridge

Steps of the Process:

1. Tested tools again on TD1. Reference Appendix B for tool testing steps of the procedure.
2. Grounded self.
3. Took Xbox One from its box and unwrapped. Took tools and followed instructions from iFixit opened Xbox One to get access to the hard drive.
    a. There were no screws to take the outer casing off, just plastic clips along the inner sides of the Xbox One. Start on the back left corner using pressure points to lift the top off. Note that there is a ribbon attached to the front of the case to the inner hardware, removed with caution. Top section of case successfully removed.
    b. There were 8 64mm Torx screws to get out to release the top inner protective covering. All but one screw was showing. C3 was under the Wi-Fi board. Carefully removed Wi-Fi board as it was attached to a connector with an 11 pin connection.
4. Found hard drive, TC1. Grounded self again before touching.
5. Disconnected TC1 from Xbox One (4 Torx9 screws connected to supports). Placed TC1 on antistatic pad.
6. Connected TC1 to Tableau Firewire 800 + USB 2.0 SATA Bridge and turned on at 13:40.
    a. NOTE: when TC1 was turned on 5 windows opened titled “System Support (I:)”, “Temp Content (J:)”, “User Content (K:)”, “System Update (L:)”, and “System Update 2 (M:)”. Did not engage with pop-ups and closed them.
7. Attempted to write on each partition by creating a text document named “TxtTest1.txt” with “TxtTest” written in the document through Windows Explorer. All partitions showed that the device was write protected and could not create the text document.
8. Accessed disk management and found TC1 listed as “Disk 3 Basic 465.76GB Read Only” with 5 partitions in use and unallocated space:

*Table 0.1* TC1 Partitions

| Name | Size | Partition Type | Reported File System |
|---|---|---|---|
| Temp Content | 41GB | Primary | NTFS |
| User Content | 365GB | Primary | NTFS |
| System Support | 40GB | Primary | NTFS |
| System Update | 12GB | Primary | NTFS |
| System Update 2 | 7GB | Primary | NTFS |
| Unallocated | 779MB | - | - |

7. Proceeded to create the TC1 image.
8. Opened FTK Imager 3.1.4.6
    a. Create Disk Image
    b. Physical Drive
    c. \\.\PHYSICALDRIVE3 - ST500VT0 00-1DK142 USB Device [500GB USB] → Finish → Add
    d. Raw (dd)
    e. Skipped case info entry
    f. Named image "TC1_2-11-15
    g. 5.001" and saved it on external hard drive EX1. Also changed Image Fragment Size to 0 so the image would not be broken up.
    h. Began imaging at 14:01:18, ended at 21:48:44.
        i. MD5 checksum: f6518a28cd6d9325a1c9e1153d54d5ef
        ii. SHA1 checksum: f675c832b865158760b2cf7ef11dee546a01cbd3
        iii. Sector Count: 976773168
        iv. Source data size: 476940 MB
        v. Cylinders: 60,801
        vi. Tracks per Cylinder: 255
        vii. Sectors per Track: 63
        viii. Bytes per Sector: 512
9. Disconnected TC1 and reconnected to Xbox One. Put all equipment back where found and left lab.

# Appendix D. Test Case 1 (TC1) Analysis

Image File: TC1_2-11-15.001

MD5 checksum: f6518a28cd6d9325a1c9e1153d54d5ef
SHA1 checksum: f675c832b865158760b2cf7ef11dee546a01cbd3
Cylinders: 60,801
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Source data size: 476940 MB
Sector Count: 976,773,168
Drive Model: ST500VT0 00-1DK142 USB Device
Drive Serial Number: W3PA4MEL

Software:

Windows Explorer
FTK Imager 3.1.4.6
Autopsy 3.1.1

Total file count: 4693
154 total unique hashes

*Table 0.1* TC1 Unique File Hash List and Amounts

| MD5 | SHA1 | Amt. |
|---|---|---|
| 00c1c00a63e5b5b661520bfa8c49d137 | 6f2a3ce1078214d921ca4ee2fdb482163d3af3cb | 1 |
| 046ab916388bcb86384203d19e244324 | 5414390643ea5e6e1b4724107e25911f0e9340d7 | 1 |
| 04a3207844460ceb816475f4fce40993 | 8bf96ea97b3946252ec45d5c1866baec9f140f10 | 1 |
| 0546597403c3844850c60ae78cd5edb4 | 20b2955bffc2c19c1ec3afe82aa3d76c43c9d306 | 1 |
| 063c648b6dac91ff704e1e2f0b6341d2 | 002365d3c2ab3cce12da3024a27f7d560b08ef5b | 1 |
| 09ed73e70b3d012fd44c2e5131e8f2dc | 022b57f89f30e73b174e9035419312a03c75bfcd | 1 |
| 0c6dd58f92ba24f89de8035f124c81ce | af62999cd86dd361600c8583af6da13319e2803b | 1 |
| 0e8182d48fa55d3826e8326baa896069 | ca6219651ff48945ec5e8d57cd7f6713490b9290 | 1 |
| 111a4fc1939438e30f1703f139f86a65 | 5c09403e69aa821fe79a15f63225aa41e6556ee2 | 1 |
| 122dd294e44b50559f1769a877c8e753 | d35553f49273d92e28fef92988de61d53f8ea2b7 | 1 |
| 128d96428f6a38fde18795e41b1e5484 | 0bfcc909783c63ef45fb5d7db9eb83d324f740ea | 1 |
| 141bface6cf6fa22ee616eb8ebbcc2ec | cdad43ff107fffa8c0858f9bffc6279c124e3ff6 | 1 |
| 167913465360d336cf2c0bc7efb2b61d | c1f978cef7de559c231bb5ae8d99a898f89529bd | 1 |

*Table D.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 18f40283e94415cae928d4216654f653 | ddfbf2c59cc1c1a559f1156c749fac0c4b5ae23e | 1 |
| 19366f3ebb206606cc3f8d073eb7c2b7 | 4b71522ada21d131764338ecd0230f55ce109123 | 1 |
| 19af014284d561a89087252bb17a8812 | bfbdccfe11b7d634fb853fe0843d6e635ed842e6 | 1 |
| 1ab7adc6e6e6ee7e339bc3ea49cf2198 | 2bc3013440673173841eff04eff3875b0f0ea348 | 1 |
| 1b5d03ae790f7f7af1dc172574033c35 | 044c0c253e60d625cc585a0edb1811deb1c357eb | 1 |
| 1cc4c3f7d02459aed30512ada20f8cfa | 8020692270b4dfad9ef6cc047e904de24b436cc6 | 1 |
| 1d748d6235553d44a2c2903812abdc06 | f222502bf4d54cfb1019fe45f343582478b0aa4b | 1 |
| 1f53d222546c48bceb8b81585e475500 | 1159a288756247dfb9f1f5980e2cfb4fb1ea7a98 | 1 |
| 1f7f61d2bd3456aaee7e56193bdf8a7f | 93248290392c2e5f99f75e49a66d900f713d92dd | 1 |
| 1ff5e07de590894222c3622492d1f874 | 7468c2ae22674764b1f293b351ed65b9ba63e659 | 1 |
| 209c81a16cccb6936901ea78ee530571 | e9b0d7d775be88ef07eef03aa520a063652d2d4a | 1 |
| 20b38aa5c071c0a36f67c8c127af4106 | d2aa44e759db5639ead6f1e4bdd640eab5ecde2e | 1 |
| 22ffb13a63dbb2a0f583664f8ea5ae7c | 363a5c888349b471b0391b88ccec3e85e9f4e575 | 1 |
| 23b5793757b5db5d26744a56ffa1e3f1 | 6034b085137733020818a543819567d5c10a71ed | 1 |
| 24b7f3c819fab262a83a9e683a402be3 | 0f86db156cfd0d06745720d08455d5a5ed41336b | 1 |
| 2b51a57a938b93b203f74ca6fdbe2d0b | f10bcda35f6a8131e15dc5ec4ca56c581f4eb522 | 1 |
| 2bc496adfeb69f722f3de20693a22fd0 | 6f9f4c44b13550c0575848749b39568438d50f15 | 1 |
| 2d0a8a3d8447bc8154c3e2dc1f3db9ac | 43803812cbf81f22b7bba4ef576093d84b178bb3 | 1 |
| 2f282b84e7e608d5852449ed940bfc51 | 2c2ceccb5ec5574f791d45b63c940cff20550f9a | 4159 |
| 2f550fa2e03eccfed53223fe5ce2f3b6 | 952a0bb80cc6cf0140839c97c599d87ff32fa757 | 1 |
| 30f3fb693759b623bd468523068db4b5 | ef75b37d170403700369ac0afee53ea4ab442dd1 | 1 |
| 35843e6d7ff00fecb23c7dc36eafabe1 | aaf3d72e47b345a42cac7cfcf47c399563e3dfff | 2 |
| 358afb2be5387086a1be7da04a6150db | 2374bff0efa8fbe322c5e0e29f657848704e1665 | 2 |
| 35d8d747df8bedc2e2c9ac404a85b671 | f0db40f7a03c27f8e085aa29481c49e438fad3b0 | 1 |
| 366db0e7c30f245721d116a1aad6bfa5 | e425547a0d4adf4983d32c04076447e0a51483da | 1 |
| 36d7c154f7bcd854cfdc26174406b848 | 9e8710c92f79e64fe0535db1af7bdfcbf6e44384 | 2 |
| 3766dd2e8b80f5a9f3c75cde67e042bc | 200c8eac9b8c29562fec4d548c21ffb043480bd6 | 1 |
| 397e01f35a5c162a600b16b6cb8f25b8 | cae2d2eea396f3137bb209f31adabf2e7a65276c | 1 |
| 3c8197cf20e7f199f9a24a6b785c1604 | 231b46bb6b9fa81cff0fc94ef06e5d04854cbbcd | 1 |
| 3dae037a4cdcb10684501b6d31d65a20 | 106aa5f2158c5f50f80b9e52639755dca3d74606 | 1 |
| 3e7bf0de7afe72ff80be10cb4f86fd9a | a47f8f20b99976c835ce7589923af2729ea56397 | 1 |
| 3f35779fca79720f75f00b9f5b6bde03 | e1f210de9519ccd71fcd276f48fce7ace88c43e4 | 1 |
| 3f7c39e0e2e3b7248e7d219cd6988572 | c2d5ab34e58cdd2f7ea4c59e88f50a0b602dc9b6 | 1 |
| 401797918103f25aacd7bf703e26912b | 67db4accd91426953a54becf1fb44dc5a0cd6ded | 1 |
| 438fa532fbde3200d7eb7639a6ae034c | 855827d861f3576a4774761cc59b7d4a5c623217 | 1 |
| 44eca22626fa607c99d9f94bd9b6c0d8 | 0dfd75954d661dead1a78959caca1650224448d1 | 1 |
| 45b9ceebfe8cf0d8fdca816c4d438787 | 0f259f90da24c5e827ce1a92802198b5cffe40f2 | 1 |
| 464379cc355b512c78788d323b87ff25 | 62f7398b85d58478548f981b64eb4cb486e8de10 | 1 |
| 474e0085d3b2e9916d35fd47ca18ee38 | ca7fc995ba2d3ed5d084e258ae486ebeba94a73b | 1 |
| 4781df8adc61e16eb4adcb0301749613 | db4d5476c3b2d2aadd0b0d6e3296c547f1653c03 | 1 |
| 489606cb5c87f29ce4541a3b0262b88f | 56d34531d73304bbf2ac24a606c4e0c6fc0663e9 | 1 |
| 49caba25f2de87b7917392b8c63aec4c | edfa5c8dd12148ef633fd43626542e2ab97974ad | 1 |
| 515c0d931d58160810db9f1a583e8d34 | 984aa74038a19d0c5e0812981e3a5c24769ebbd3 | 1 |
| 51f03672d2152c11f0ff3f399e272922 | abb5dcb132358e0df5add93887379562af7e44a9 | 10 |
| 521a6ebf3468eff686f388e4eb405bd5 | f8f0982d594c267a5ea26c5decdecbf0befbd7d1 | 1 |
| 52693c359c8a13f8817c3931d2d8a8a2 | 555e6405a5ffd95ce2b303abeb119566a0a740c8 | 1 |

*Table D.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 5a48c2eb9fbd45d420b5a794c5672de5 | e48bad554ae6ff5f07b644f36143334cf593705b | 2 |
| 5abd611446f9e8e9c2fe6baab91e3df2 | cb7aca18264b724f8a9490460f29ae6c3635387f | 1 |
| 5d0ff95229281d3c3b0596746538c445 | c9b699eba930c46eed95aa8378036e9f76a249aa | 1 |
| 60677a6bd61fa68beb18aa91153ed2ae | 682d44df56b82dc00158769e63c383fa05b44a74 | 1 |
| 60c0688147f715a7ab0940286e7dc927 | 32fdf5d888d2d32883282063354bab77e11c5813 | 1 |
| 6404c73e103c4c90eb1b3e8317d0e44c | 40f2daa9b39a260852f97da16d9e04d3d6f99c4d | 1 |
| 6c768abe7517044afcd418e6c8a18a33 | eef231ee80882665317ecbd819703425ca03d3ca | 5 |
| 6dff3a49046b0f8c2949e7661cb53753 | 4dad28cc5bcf4af4b0d5a3bc5750594d1860d61a | 1 |
| 710a811fb3679f5701a8494b00729106 | 76f211ba32c2c035d34630d651e0750fd3c233e2 | 1 |
| 7165d94359886c0cb0f29504f5c11467 | 9a8070d17c81d629a3a00a0f3b6cff84204ff944 | 2 |
| 72161653662ff0afdc29bb4458004618 | 96809fb60612c5169da8ffa38e8e38c9d9b806b6 | 1 |
| 72678dd19efebfdd1fe989ba5048f6c4 | c53bb67862d14155d566c4985bd8f0b71fdee2f8 | 1 |
| 78df7d13538aa76aca97b8866347ed84 | e91e524a5fe21cad756cfc89546a87e87bfa4cfa | 2 |
| 790742fa73920dbf2f7bcb8a171243a8 | 5bf7219a9074a2429cb28fed8a746906b74d44c9 | 1 |
| 79de6e5cbb286c47048761bf01a387ef | 895cacb945011b3c4bf0809bcba087aaaafd2ca2 | 1 |
| 7c1ec3cf185afb99bbc70925748fae72 | d148e882f73707fee834226a09e4e7d191d3403f | 1 |
| 7df03c94e79e4dda462dd276eea6fc44 | 3978be682abd094e8b6e8ffb81f3e5f5a6dd75c0 | 1 |
| 7ff498a44e45e77374cc7c962b1b92f2 | 5161a18e27b9ca9f5d04f2154576bf1ffb1121e8 | 5 |
| 800cd991ba91f9d14fc70aefe870e48d | 6a676fd61c469d3d897acce68a3a12928e2ab2ae | 1 |
| 8010d4683006b5dd7ac2b5ac27ad050d | b0cde380832992aae356a0db713a391dcab6af5d | 1 |
| 8274dc8683724b52651766b2dd089b42 | 2bb0be460de913213dd2d4668f94917864ccc5a6 | 1 |
| 82ae862e8b7d3e883d054d951a51c993 | 5906fb34e435d35c9f8efdc11a0f7c8f48a92bb7 | 1 |
| 856e334ad8b7835c41bd91ee305f83d4 | b6f737a8d59a42a2858e325b39e55715d04a7982 | 1 |
| 8b7bdf67970ed38a7bff8d58ef435936 | 9b2efab8d9471a4b0760f5080c1da448098099ff | 1 |
| 8bb09d218c62d77d23c5fafce3649d3f | 691ca96d12f11db6ecc00f5aef2a7c267bc1e555 | 1 |
| 8bb91cc072005f033bdb37e1eb77d0d5 | 251ce0775e2cff87380252fcda16ffb72713efef | 1 |
| 8e90f3f16cc1fd4ba3f5a4d918181f7b | cab36f1deb571fbc50b3ff939a1f11e1cf158311 | 2 |
| 9127d4b76ccd3ef715576cb478e7d630 | 7619b5e9095d9edeb627a4d0083df066330a9284 | 1 |
| 916d600863fc424010372e2c031737f6 | f6e57e756b64041690ccb4794bb116c5925a82a2 | 2 |
| 92f409f797b858544a1ce6f795f2eb1e | ef8b56ff4d8737c0023bf3df6f3a1faf48408df7 | 1 |
| 95fe8cf0ea7a88154e1523a60280488b | df737753bcd2abf701dd916424eae9294a567d9f | 1 |
| 9608501875f7e7c9ef9459fa0439b714 | 2bc765cce8c5339cd7f16e21130e1c3cf65c84bd | 1 |
| 97dc490ac9723fd995d68f514dd458d2 | 23d72f7774037e9ad32b6802889616ebae3a89fd | 1 |
| 9948d222b8ddd10eea5fd27e43c96a7a | cfafe8def0bad81e99da11592240fefff09d4a52 | 1 |
| 99e462d40c3bb1fb0736ec75fc7f0164 | 984a17257a606225860de5ad8730903d9ae73a41 | 1 |
| 9cdbab9bba51624d6309daad3e817011 | 38474cfba7c623b8bcbc07d9648f7c7857bd0d1f | 1 |
| 9d8bb6cb1247ee8c254cbcfccc016f1a | 3dcedd819a91b7380f2567c9c97dce382d624238 | 1 |
| 9f0a88928e5d5c0736737e032b3fbbdb | 540e3cd6a5df4aaf2613072d19206b67c43a34f8 | 1 |
| a0923df212bf9a4189cb2a15dc4626af | b04d94dd04f2415edaee5547b1210b7190d0a1aa | 1 |
| a0b1512cea6286fdb5db65018849489e | 4ace8815abad5d9ef6d840c8beb7d95895d838bf | 1 |
| a6dcb8041f7a2e9d236527994ff0f3e2 | 809fafd115128f7126a4c34d80dc5e0214379024 | 1 |
| a75c836e8ed090d6065c2e0043c5fba4 | d0c8bffe35cb031f282b8517fd95d19f397cdf4b | 1 |
| a9b4ea855f46fa7da9d975173078ffd6 | fd9c344c2205d39fab1b174e44ed23ee6d096fa2 | 1 |
| aab9a8c0d3ba44ddd0b069b74d72c638 | da799991f31b9b8fdda33e41aef8f7d9ab8133cf | 1 |
| ab981967d9f545695c396db3787f8a49 | 2497adcb05fe54ad8a55c8fd2c145951ea039237 | 5 |
| ad617ac3906958de35eacc3d90d31043 | b49d7f48300701235231f6b6fc3d92a5630f9e70 | 5 |

*Table D.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| af9648fb762b69314cbf19cb1e37e976 | 0092a991194babb338d156eaabf041ab7229df51 | 1 |
| b29f58cfde2c25d89c47abc1dd0029ab | 4677fb679acb30b3ec9833353e4e219a79c15a77 | 1 |
| b31ff39de9cacf82e654a8d1a374fe07 | df9384ba90f3b7e51717d5979f501b51c5246065 | 1 |
| b4202f7fe985b9648b4676e6f70832bd | d37c2b3927946ed617455b3c5913fcab0bc1af52 | 5 |
| b4f0f0aa21e50f6d4d704d734b8d4d34 | a6dbb19a063be57fd63b3ffeeaaa9378e77b92e5 | 1 |
| b501432bddf91ae5d7ed16b496f298ff | 9ac41b155deda4dc8cb5dcceca27e85da82406a6 | 1 |
| b64d1ea9751245ffd169b598aa0dd60d | 7cf09ade47e16babb369262d2308bbeb74095c8d | 1 |
| b836143231c4eda0e4fd4765a741ec18 | 466bb52a38153071e22ae0c42c426cd6b8846e7c | 1 |
| bc6ee59591d5007c78f1b64c25f0404c | 96d671198b381a39b57cdebd94db89bd8b33856c | 1 |
| bed6ab23b0e4a4f2f903a87afbec4b3b | 53f475644e4ca0daeba0c59a18df804da1233310 | 1 |
| c0a01e9c9296748e2761bf6b1d6d202a | 9a9a348c0136385572f6d46646541190b91649cc | 1 |
| c2115c88466fd2148bfbb4f9b7a6aaca | 2043af89dbec10180005f1e1a721b342de526aea | 1 |
| c30b4d73be49df3d5950ba49e3ebe0ee | e821ef789b6fb72a4eba0ef205e52c42cc04ba2f | 1 |
| c37b911194bf81da064cbb49d767d308 | 3fc3a3970b1a78848656ac7743ce0fa303482c8f | 1 |
| c93a7fdc2ecba8b65c4c5ee5e7dcd1a1 | b71f43c05952e4f5debe6cd12f600534e3d1f509 | 1 |
| ccc7677b0a8d066efb0026d05fc2d8ce | 014311aed6137cb46edeec2da597c9e9fb51c0fb | 1 |
| d2389a74d9784cc5aeaca86f6ce50993 | 623c0330e86dd7ce07dc20665d6e225cc514f362 | 1 |
| d3c35273db55dcda916db3b3f3a998d9 | 8fe086fd8fc2bda28b304cc38ccddfa55819e98d | 1 |
| d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | 20 |
| d4213280274d39a03eba7b5cd99c8e9f | 88a395ac835da687cc806988590471227cd45191 | 1 |
| d6fdfa460e2538caef7bf574453d7894 | 2d24c6762d6ec8575fc70f17f88a4f599043931f | 1 |
| d887a17cc43887d799fca62319d051db | cf6e8e0e96636477f1746bf8aa0ca9c3f5fa4c9f | 1 |
| d892d0820768c96bc521c1318efcfa9d | b830e94e6a37e6c95859a2279976ee780f713e8f | 1 |
| db511d02c1be9792fbdf4bea7c5fd3ca | 43a98d5a2e7aa411d0ca184d8382572e323f3165 | 1 |
| dc2784e32e79706ac09df198ec8835ed | 52b6a6caf32bfbb061436b7e710a5cc4625e5d9a | 1 |
| deb5c30cf4e8a2bfab38992264b1756c | 51106b2af57081242ab2c27dcc547e3c9b378630 | 4 |
| df97e5cfdb6a5e84b230d61536d9ac3e | e354da81e30913cda2f8ee813742631a091884f5 | 1 |
| e0777a146f0eeaaa587c283faaa19bf3 | 39c683ea038a60740c518645a386228f64576019 | 1 |
| e0b1a957b1a0efc909fb2e64960968ac | bac35ed86cd09ce1c64770b565ce4a6ffe17c1ef | 1 |
| e2da72071b15025127156f3ce6e5cca7 | b47ae4e38370d4d0a40ce73cfb507168344c5f23 | 1 |
| e7301356d96583bbd713667c56ca6f82 | 1559df29b3625ac3c687f5160e57874f8125fd12 | 1 |
| e81ecc08fd743d071619f226cb9715c8 | 3a7df03a12853503a0212379cc4e1f17c87c978c | 4 |
| e94f97f8f0d4dfbc11c487c98b88f58d | 4c17d3a67e6c384f8d7259b7562d2687f8e2db0f | 1 |
| ea5ba8a90735e40978eac5e9da75a94a | f100f255996de20aadcf708047ca4f734065e674 | 1 |
| eb349055b5eac7c0503ecf711f6fbca3 | fd04c3376f10a1a0b628d9ad163b9d263e014a3e | 1 |
| ecb6749289cd3277e5cdb970a36ae18d | d4f794dc10a472355c50727ba4cede94e4f92955 | 1 |
| edc4c3de71636089cd395e4773c79e19 | 1dcc88152fc1492520b3e26f54a98a5abdfa6c58 | 1 |
| edcd503951b8676ec401a3df89ee4df0 | 606fcae96a65dd92ee44e32aeb0090f8174a230e | 1 |
| f4152b0992dbb28a19e4447ef6a7b195 | 67dffc8090b19b96e86c6486402b3f8a38792c18 | 1 |
| f4d2127084a2277d9b0911714111849c | e745a76dedd998715f7197f697afca681de8a8d6 | 1 |
| f77eb69c26e1f279329bf19c735d116c | 872517d323ea780c61153239bea1c35caefc756c | 1 |
| fa1daa970ba3560c1314dff313653157 | 47eaa934af5497fd010f941edb04c30bf7ac6788 | 1 |
| fb4a1dad2dcf9a38e84a0c38c642357a | bae9f94196b7d2d539dbf3351e10b20dbc3b6069 | 1 |
| fbb7abadb02632161176e7cefdb874d5 | 0cb9b4bb73c4bdd0c4286e8b0777a27337c52905 | 1 |
| fc0567da64a9842ca71e73dfebda99fd | f38a9f6bfd411dd7d87055e65e92c290cd9e72de | 1 |
| fc3e8322d0bb5d1dc5f643dea86ab359 | e0c0134b207dce519bbe5213fea176d90dae898a | 5 |

*Table D.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| fece24feb630ae23b9171380c3116685 | ac0625c334905c8a543f3b4e0aa31438a1c22f04 | 1 |
| ff2339aaf556aa414f8f241726b1d3b4 | fcf786eccdfd566ac1a952d9c30237fa5affc5f4 | 1 |
| ff63cd5358364dfacc3cd95d5ebb01af | a93d6a93f12f8bc78f1f6bf2ba984277258fc59c | 1 |

# Appendix E. Test Case 2 (TC2) Creation

Date: Monday February 16th, 2015 beginning at 6:00 am
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228

Steps of the process:

1. Took Xbox One (reassembled since TC1 Imaging) and connected it to a TV in the lab via HDMI connection. Note at this time the researcher had acquired a Kinect and also connected that to the Xbox One for TC2 creation.
2. Connected Ethernet cable to Xbox One.
3. Turned on the TV.
4. Turned on the Xbox One with the controller it came with at 6:08 am.
5. Pressed Continue at 6:11:20.
6. Chose English as main language.
7. Xbox One asked if 1080p or 740p would work for the TV resolution but neither worked. Chose option "None of these work" and continued through to a screen saying the resolution was at 640 x 480 and continued through.
8. The Xbox One stated that it was connected to the internet at 6:13:35 am.
9. Chose United States as location country and continued through.
10. Stated the Xbox One needed an update. Began update at 6:14:15. An automatic reboot happened at 6:17:53, then booted back up again at 6:18:26. Update completely finished at 6:21:20. Continued through.
    a. NOTE: At this time the update should be 6.2.12130.0 (xb_rel_1502.150209-1738) fre which was released 2-13-15 (Xbox Support, 2015).
11. Set time zone to (UTC -05:00) Indiana. Kept the option checked to automatically update for daylight savings time and continued through at 6:22:40.
12. Began Kinect sensor set up. The Kinect could see me, and then checked audio. The volume was at 45 for the check (louder than normal as prompted). Continued through.
13. Created a Microsoft account on Xbox One. Account is FrankOX@outlook.com (Frank OX) at 6:30:05-6:31:50. Password is "Digital!" which was entered at 6:33:00-6:33:20. Birthday was set for May 17th, 1987. The external email was set to FrankieXman@yahoo.com at 6:40:40. This email was created by the researcher.
    a. Yahoo account: Frank OX. Fake Phone: (765) 223-1828. Birthday: 05-17-1987. Password: Digital!
14. Accepted Terms of Use.
15. Chose the privacy control to be "Make it Fast, Make it Magic". This option states "Step in front of Kinect and you're signed in, ready to play. On this Xbox, people

can sign you in, change your settings, and buy things without extra steps." Continued through and the Kinect found my face again. Stated that was me and continued through again.

16. Chose the light blue color for the profile and continued through.
17. Chose "No Thanks" to signing up for Xbox Live for now as this is a part of creating TC3. Continued through to the Xbox One Home screen. Turned off by holding the X button on controller and selecting "Turn of Console" at 6:45:30.
18. Turned off TV and disconnected Xbox One from TV. Put all power cables to TV where found.
19. Took Xbox One to imaging workstation to begin imaging process.

# Appendix F. Test Case 2 (TC2) Imaging

Date: Monday February 16th, 2015 beginning at 7:00 am
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228
Computer: CFLWIN15

- Windows 7 sp1 64-bit
- 8GB RAM
- Intel Core i5-2400S CPU @ 2.50GHz
- domain cit.lcl
- Time Zone Set:(UTS-05:00) Indiana (East) date set to Wednesday February 16th, 2015

Xbox One TC2 Hard Drive: (TC2)

- Manufacturer: Seagate
- Model: ST500VT000
- S/N: W3PA4MEL
- P/N: 1DK142-120
- FW: 0001MBC1
- Size: 500GB
- Physical: SATA 2.5”
- CHS and LBA not listed

External Hard Drive: (EX1)

- Manufacturer: Western Digital
- Model: N3565A
- S/N: WXF1A7221875
- P/N: WDBY8L0020BBK-01
- Size: 2TB

Tools:

- Windows Explorer
- Disk Manager (Logical Disk Manager)
- FTK Imager 3.1.4.6
- Tableau Firewire 800 + USB 2.0 SATA Bridge

Steps of the Process:

1. Took Xbox One apart to access the hard drive just as when accessing TC1.
2. Connected TC2 drive to tools and turned on at 7:10 am. Note when the write blocker was turned on messages popped up for all 5 partitions: "You need to format the disk in drive (I:, J:, K:, L:, M:) before you can use it." Canceled format to all.
3. Attempted to write on each of the volumes but Windows Explorer would not even let me access the partitions to TC2 stating "(I:, J:, K:, L:, M:) is not accessible. The media is write protected".
4. Accessed disk management and found TC2 listed as "Disk 3 Basic 465.76GB Read Only" with 5 partitions in use and unallocated space only the partitions did not have any names this time and the reported file system was listed as "RAW":

*Table 0.1* TC2 Partitions

| Name | Size | Partition Type | Reported File System |
|---|---|---|---|
| (K:) | 41GB | Primary | RAW |
| (J:) | 365GB | Primary | RAW |
| (I:) | 40GB | Primary | RAW |
| (L:) | 12GB | Primary | RAW |
| (M:) | 7GB | Primary | RAW |
| - | 779MB | - | - |

5. Proceeded to create the TC2 image.
6. Opened FTK Imager 3.1.4.6
    a. Create Disk Image
    b. Physical Drive
    c. \\.\PHYSICALDRIVE3 - ST500VT0 00-1DK142 USB Device [500GB USB] → Finish → Add
    d. Raw (dd)
    e. Skipped case info entry
    f. Named image "TC2_2-16-15.001" and saved it on external hard drive EX1. Also changed Image Fragment Size to 0 so the image would not be broken up.
    g. Left "Verify images after they are created checked".
    h. Began imaging at 7:27:10, ended at 15:42:57
        i. MD5 checksum: e5ba73896e6698fcfe90e2f29b35d01f
        ii. SHA1 checksum: 9daf045689c847e6f4f432571b8f238628946945
        iii. Sector Count: 976773168
        iv. Source data size: 476940 MB
        v. Cylinders: 60,801
        vi. Tracks per Cylinder: 255

vii. Sectors per Track: 63
viii. Bytes per Sector: 512

7. Disconnected TC2 and reconnected to Xbox One. Put all equipment back where found and left lab.

# Appendix G. Test Case 2 (TC2) Analysis

Image File: TC2_2-16-15.001

- MD5 checksum: e5ba73896e6698fcfe90e2f29b35d01f
- SHA1 checksum: 9daf045689c847e6f4f432571b8f238628946945
- Cylinders: 60,801
- Tracks per Cylinder: 255
- Sectors per Track: 63
- Bytes per Sector: 512
- Sector Count: 976,773,168
- Drive Model: ST500VT0 00-1DK142 USB Device
- Drive Serial Number: W3PA4MEL

Software:

- Windows Explorer
- FTK Imager 3.1.4.6
- Autopsy 3.1.1

Total file count: 4679 (14 less than TC1)

164 total unique hashes

*Table 0.1* TC2 Unique Hash List

| MD5 | SHA1 | Amt. |
|---|---|---|
| 0546597403c3844850c60ae78cd5edb4 | 20b2955bffc2c19c1ec3afe82aa3d76c43c9d306 | 1 |
| 09ed73e70b3d012fd44c2e5131e8f2dc | 022b57f89f30e73b174e9035419312a03c75bfcd | 1 |
| 0bb15da434440c0572eac837ad847f9a | 3676fa9cce3b3aee499fdf9dab1ff5325b16415e | 1 |
| 0cb1099ee088093a5cbb4c8cc0fd1556 | 95693181a5792da022a4f151ca40d3399a03cfd9 | 1 |
| 0e7a8b19c7c02ed2e0161ffe81071673 | d851fe0993baecda42cd71ce29be0a8d144db75f | 1 |
| 111a4fc1939438e30f1703f139f86a65 | 5c09403e69aa821fe79a15f63225aa41e6556ee2 | 1 |
| 122dd294e44b50559f1769a877c8e753 | d35553f49273d92e28fef92988de61d53f8ea2b7 | 1 |
| 128d96428f6a38fde18795e41b1e5484 | 0bfcc909783c63ef45fb5d7db9eb83d324f740ea | 1 |
| 167913465360d336cf2c0bc7efb2b61d | c1f978cef7de559c231bb5ae8d99a898f89529bd | 1 |
| 18f40283e94415cae928d4216654f653 | ddfbf2c59cc1c1a559f1156c749fac0c4b5ae23e | 1 |
| 19af014284d561a89087252bb17a8812 | bfbdccfe11b7d634fb853fe0843d6e635ed842e6 | 1 |
| 1ab7adc6e6e6ee7e339bc3ea49cf2198 | 2bc3013440673173841eff04eff3875b0f0ea348 | 1 |
| 1d748d6235553d44a2c2903812abdc06 | f222502bf4d54cfb1019fe45f343582478b0aa4b | 1 |
| 1f53d222546c48bceb8b81585e475500 | 1159a288756247dfb9f1f5980e2cfb4fb1ea7a98 | 1 |
| 209c81a16cccb6936901ea78ee530571 | e9b0d7d775be88ef07eef03aa520a063652d2d4a | 1 |

*Table G.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 20b38aa5c071c0a36f67c8c127af4106 | d2aa44e759db5639ead6f1e4bdd640eab5ecde2e | 1 |
| 22ffb13a63dbb2a0f583664f8ea5ae7c | 363a5c888349b471b0391b88ccec3e85e9f4e575 | 1 |
| 23b5793757b5db5d26744a56ffa1e3f1 | 6034b085137733020818a543819567d5c10a71ed | 1 |
| 296e94da77b6b827a885a3572d1db539 | c9bfa2e235f5f4d576ebda41b0d09256752333f0 | 1 |
| 2a5a0f9c27aab78550042c6e2d35a49f | 4b2ea7cbb857732420a02a2006cf166f46e9df8a | 1 |
| 2b51a57a938b93b203f74ca6fdbe2d0b | f10bcda35f6a8131e15dc5ec4ca56c581f4eb522 | 1 |
| 2b76f46a6c00947779ac55f0a5b98068 | ec42e6a4027c0590c378ddda2c4708c0d4c39527 | 1 |
| 2bc496adfeb69f722f3de20693a22fd0 | 6f9f4c44b13550c0575848749b39568438d50f15 | 1 |
| 2e1459c0273ade852dbf7369172b1dd8 | 158af0658367584c4bd64e5fa4c933fa92fef472 | 1 |
| 2f282b84e7e608d5852449ed940bfc51 | 2c2ceccb5ec5574f791d45b63c940cff20550f9a | 4416 |
| 2f550fa2e03eccfed53223fe5ce2f3b6 | 952a0bb80cc6cf0140839c97c599d87ff32fa757 | 1 |
| 2f8b78c0afa0dd910042ce51ddfc27fd | 4d9c0089b59ce4087d223b99f5c33a168064e230 | 1 |
| 30f3fb693759b623bd468523068db4b5 | ef75b37d170403700369ac0afee53ea4ab442dd1 | 1 |
| 32f887d5b2a059839397ff7f9a34b9a6 | eaf86283eb470a2a37c3420ed505b4d82434b544 | 1 |
| 358afb2be5387086a1be7da04a6150db | 2374bff0efa8fbe322c5e0e29f657848704e1665 | 2 |
| 36d7c154f7bcd854cfdc26174406b848 | 9e8710c92f79e64fe0535db1af7bdfcbf6e44384 | 2 |
| 397e01f35a5c162a600b16b6cb8f25b8 | cae2d2eea396f3137bb209f31adabf2e7a65276c | 1 |
| 3996bf6b970dda7688c1c2373f6d5406 | 984b84258bbc01a09d695a9df9bb354cd7990933 | 1 |
| 3c8197cf20e7f199f9a24a6b785c1604 | 231b46bb6b9fa81cff0fc94ef06e5d04854cbbcd | 1 |
| 3d62dd60999d5e06ddb2f00ea523ffe6 | da6fdb58a93df3a57562b47d62cf1472dd50b191 | 1 |
| 3dae037a4cdcb10684501b6d31d65a20 | 106aa5f2158c5f50f80b9e52639755dca3d74606 | 1 |
| 3e7bf0de7afe72ff80be10cb4f86fd9a | a47f8f20b99976c835ce7589923af2729ea56397 | 1 |
| 3f35779fca79720f75f00b9f5b6bde03 | e1f210de9519ccd71fcd276f48fce7ace88c43e4 | 1 |
| 410f2d06fb03b594a17c5a067711648c | 90afa71a0e397f526dea055c7c438685a26f2f62 | 1 |
| 438fa532fbde3200d7eb7639a6ae034c | 855827d861f3576a4774761cc59b7d4a5c623217 | 1 |
| 44b65b6e3ce4169ea99365a1413e04b4 | 94b729497d653086764c1f54dd9f8eeb330d5708 | 1 |
| 464379cc355b512c78788d323b87ff25 | 62f7398b85d58478548f981b64eb4cb486e8de10 | 1 |
| 4781df8adc61e16eb4adcb0301749613 | db4d5476c3b2d2aadd0b0d6e3296c547f1653c03 | 1 |
| 489606cb5c87f29ce4541a3b0262b88f | 56d34531d73304bbf2ac24a606c4e0c6fc0663e9 | 1 |
| 49caba25f2de87b7917392b8c63aec4c | edfa5c8dd12148ef633fd43626542e2ab97974ad | 1 |
| 4b33951b65ba1451ed8a16bebad154f3 | 206d35d2248dda8c4bd1584ad8790ba28f773dbf | 1 |
| 4d8f577de833ccf4713fd85e60b7167a | 6782f051e208e541f1e214376829a55a6a0f8aee | 1 |
| 4e1159971f10b57ec7de45bf14e2ae34 | 4f1af59708e791ee208d356da708a3bffbb761da | 1 |
| 4f3c847cabe9542dc748a7ff08021496 | 6710dd9626cc4a2a71ffc670ffd929459dbf3f26 | 1 |
| 51f03672d2152c11f0ff3f399e272922 | abb5dcb132358e0df5add93887379562af7e44a9 | 10 |
| 521a6ebf3468eff686f388e4eb405bd5 | f8f0982d594c267a5ea26c5decdecbf0befbd7d1 | 1 |
| 523565888e1178c984ad673cda163b9d | 595c55f5b3b6a2151ff828548e5b3f8385dc8ce3 | 1 |
| 57c156ada7dcb2105e212e9c081f27ec | 60995d6b003dc718a8c727d661e19f8763fafb3b | 1 |
| 5a48c2eb9fbd45d420b5a794c5672de5 | e48bad554ae6ff5f07b644f36143334cf593705b | 2 |
| 5abd611446f9e8e9c2fe6baab91e3df2 | cb7aca18264b724f8a9490460f29ae6c3635387f | 1 |
| 5e58d6d766454f2e7aa304f26bcda97e | 89065f45d646f24accc77dc707f75b2cc4bf2ff5 | 1 |
| 60c0688147f715a7ab0940286e7dc927 | 32fdf5d888d2d32883282063354bab77e11c5813 | 1 |
| 62244af3c96842f764ecc9cbbfed5417 | 490c5f83df1eb0372f8f1bc4275a38282e482c55 | 1 |
| 6404c73e103c4c90eb1b3e8317d0e44c | 40f2daa9b39a260852f97da16d9e04d3d6f99c4d | 1 |
| 687985620e9bcea4865953c79eed183b | 5f9e7f0675605a5d58751d960c2f541354eb4e14 | 1 |
| 6c768abe7517044afcd418e6c8a18a33 | eef231ee80882665317ecbd819703425ca03d3ca | 5 |

*Table G.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 6cf4216366dfead41858352db690cbd1 | 82f96583af5f8df4a84dc4ee1fad64161c81634a | 1 |
| 6d1340e58f7bf2f2db660f1dc7d1da43 | d55c36f8276aa69c658f665b6823f858c02f6989 | 1 |
| 710a811fb3679f5701a8494b00729106 | 76f211ba32c2c035d34630d651e0750fd3c233e2 | 2 |
| 7147a7f3dbeee702202e0a74f88f1530 | 14e5ee5ca6e574077d0ecffcda8597f14e3a3956 | 1 |
| 7165d94359886c0cb0f29504f5c11467 | 9a8070d17c81d629a3a00a0f3b6cff84204ff944 | 1 |
| 77457113512eeb29b981a0fc6b94e336 | f8781ca90285e81f445bf6bee45ea1dc536c39c2 | 1 |
| 78df7d13538aa76aca97b8866347ed84 | e91e524a5fe21cad756cfc89546a87e87bfa4cfa | 2 |
| 790742fa73920dbf2f7bcb8a171243a8 | 5bf7219a9074a2429cb28fed8a746906b74d44c9 | 1 |
| 796f01508b47a95ac217e3ce8021f442 | 8599485f5df223fd050aa3d869ee069bdf329a30 | 1 |
| 79bc93165b22865dab0799f55f83eab3 | 6b44ce69f3ac4ae9160a5c690d6f28a31849096b | 1 |
| 7b400915c05deeb86a175af6a8f20400 | 4401f8d259bf599c28dd62e7c17a930af7687430 | 1 |
| 7b802e9d49c916b0f9bc8400ad1436f3 | 6f8f70ae08a6800278e2c483d585d9e200f53141 | 1 |
| 7c1ec3cf185afb99bbc70925748fae72 | d148e882f73707fee834226a09e4e7d191d3403f | 2 |
| 7df03c94e79e4dda462dd276eea6fc44 | 3978be682abd094e8b6e8ffb81f3e5f5a6dd75c0 | 1 |
| 7e85c536816811126fc8f0512561c19e | 5ba19850e6505aa6692b1e2c6a3f3b838338b7ea | 1 |
| 7ff498a44e45e77374cc7c962b1b92f2 | 5161a18e27b9ca9f5d04f2154576bf1ffb1121e8 | 5 |
| 8010d4683006b5dd7ac2b5ac27ad050d | b0cde380832992aae356a0db713a391dcab6af5d | 1 |
| 8215b3d8187e427a16628505de16c298 | bb1711f203dedbcf0c36595e2bb46f66af82cfd7 | 1 |
| 8274dc8683724b52651766b2dd089b42 | 2bb0be460de913213dd2d4668f94917864ccc5a6 | 1 |
| 82ae862e8b7d3e883d054d951a51c993 | 5906fb34e435d35c9f8efdc11a0f7c8f48a92bb7 | 1 |
| 868578814c1d61a3f84fd546a1e064a8 | 877c69b83aa60491e0e7bc7b6ab396b6e02c5f42 | 1 |
| 892a474648e191a875ca4fb6c9a74a8c | d92cf32e5ea100dd99ca7713ce32b7831948af87 | 1 |
| 8b7bdf67970ed38a7bff8d58ef435936 | 9b2efab8d9471a4b0760f5080c1da448098099ff | 1 |
| 8e90f3f16cc1fd4ba3f5a4d918181f7b | cab36f1deb571fbc50b3ff939a1f11e1cf158311 | 2 |
| 9127d4b76ccd3ef715576cb478e7d630 | 7619b5e9095d9edeb627a4d0083df066330a9284 | 1 |
| 916d600863fc424010372e2c031737f6 | f6e57e756b64041690ccb4794bb116c5925a82a2 | 2 |
| 92f409f797b858544a1ce6f795f2eb1e | ef8b56ff4d8737c0023bf3df6f3a1faf48408df7 | 1 |
| 95fe8cf0ea7a88154e1523a60280488b | df737753bcd2abf701dd916424eae9294a567d9f | 1 |
| 9608501875f7e7c9ef9459fa0439b714 | 2bc765cce8c5339cd7f16e21130e1c3cf65c84bd | 1 |
| 97f9ef13a1aa24f4e5dd226057249ed1 | d17a20dd25fc238bbe5547f1c06abd9303d3d60b | 1 |
| 9948d222b8ddd10eea5fd27e43c96a7a | cfafe8def0bad81e99da11592240fefff09d4a52 | 1 |
| 9cdbab9bba51624d6309daad3e817011 | 38474cfba7c623b8bcbc07d9648f7c7857bd0d1f | 1 |
| 9d8bb6cb1247ee8c254cbcfccc016f1a | 3dcedd819a91b7380f2567c9c97dce382d624238 | 1 |
| 9dce8f75aee0d59aea168b98598844d1 | 6dda93f60858c3ffdb17a81e99b99606b543ab57 | 1 |
| 9eda4e5252c089fe9390eb4879a183f1 | 249fd4e8a153860170eb36d8e59590aead188a84 | 1 |
| 9f0a88928e5d5c0736737e032b3fbbdb | 540e3cd6a5df4aaf2613072d19206b67c43a34f8 | 1 |
| a04e45f8538613c10372faa3179552e0 | bea0067fa554dda7ddf129d0bccafed1372e6d79 | 1 |
| a0923df212bf9a4189cb2a15dc4626af | b04d94dd04f2415edaee5547b1210b7190d0a1aa | 1 |
| a0b1512cea6286fdb5db65018849489e | 4ace8815abad5d9ef6d840c8beb7d95895d838bf | 1 |
| a220e732919d636f1bf269c8ffa794e1 | 69c3945d071da28e3639271c0eb98cf7a096607c | 1 |
| a6dcb8041f7a2e9d236527994ff0f3e2 | 809fafd115128f7126a4c34d80dc5e0214379024 | 1 |
| a75c836e8ed090d6065c2e0043c5fba4 | d0c8bffe35cb031f282b8517fd95d19f397cdf4b | 1 |
| a835df07c953fd918606e4aaa11367ea | 526ae7867a9fd64c4be0a54b81cea0fd5c88b99d | 1 |
| ab981967d9f545695c396db3787f8a49 | 2497adcb05fe54ad8a55c8fd2c145951ea039237 | 5 |
| acf026ca14cce268fe40621c1fd787ad | b1558802b2f4334734b2dbfd9cd9a3ace4c49b9e | 1 |
| ad617ac3906958de35eacc3d90d31043 | b49d7f48300701235231f6b6fc3d92a5630f9e70 | 5 |

*Table G.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| ae53ce28325bfc0482ca90d005d1bab5 | f3c711d17c34c4b0a28a61c2e523952fbf5c4f5b | 1 |
| af9648fb762b69314cbf19cb1e37e976 | 0092a991194babb338d156eaabf041ab7229df51 | 1 |
| b3bc476292e8056db03d87b88a7e82c7 | 44a1d8e05f52300da748ea18edc00f5b1e2274c6 | 1 |
| b4202f7fe985b9648b4676e6f70832bd | d37c2b3927946ed617455b3c5913fcab0bc1af52 | 5 |
| b4f0f0aa21e50f6d4d704d734b8d4d34 | a6dbb19a063be57fd63b3ffeeaaa9378e77b92e5 | 1 |
| b501432bddf91ae5d7ed16b496f298ff | 9ac41b155deda4dc8cb5dcceca27e85da82406a6 | 1 |
| b5f13a73f7f681be6e8f2e6310387bd6 | 16e8cfa23688f441a5ac548091207e49a56bd1fa | 1 |
| b64d1ea9751245ffd169b598aa0dd60d | 7cf09ade47e16babb369262d2308bbeb74095c8d | 1 |
| ba4fa6f08f8431c94115b55bc589123b | d3e3121c8677140b5bbd3bf1fa861846a038ed31 | 1 |
| bed6ab23b0e4a4f2f903a87afbec4b3b | 53f475644e4ca0daeba0c59a18df804da1233310 | 1 |
| c0a01e9c9296748e2761bf6b1d6d202a | 9a9a348c0136385572f6d46646541190b91649cc | 1 |
| c1915798b2c80eeee4e10ff7ddc40bcd | d030e154b71d07681fb7c358cdac089bbf53772b | 1 |
| c2115c88466fd2148bfbb4f9b7a6aaca | 2043af89dbec10180005f1e1a721b342de526aea | 1 |
| c30b4d73be49df3d5950ba49e3ebe0ee | e821ef789b6fb72a4eba0ef205e52c42cc04ba2f | 1 |
| c37b911194bf81da064cbb49d767d308 | 3fc3a3970b1a78848656ac7743ce0fa303482c8f | 1 |
| c81601b97f1a4095366b51fa8d0620ab | 67751b58b290f6bcd5ec054d02ca9b98c229990d | 1 |
| c8505390f82e20e2a623d1205b1e3ea8 | b6fa4e367eaa23dd3e8eeff8f3972cb2c153967e | 1 |
| c93a7fdc2ecba8b65c4c5ee5e7dcd1a1 | b71f43c05952e4f5debe6cd12f600534e3d1f509 | 1 |
| ccc7677b0a8d066efb0026d05fc2d8ce | 014311aed6137cb46edeec2da597c9e9fb51c0fb | 1 |
| cfcd208495d565ef66e7dff9f98764da | b6589fc6ab0dc82cf12099d1c2d40ab994e8410c | 1 |
| d2389a74d9784cc5aeaca86f6ce50993 | 623c0330e86dd7ce07dc20665d6e225cc514f362 | 1 |
| d308cbaf2024821a8c08a68fe790fb7a | 3f01db556e043ad37a5bb602b485781b5199baca | 1 |
| d3656d96011f4604a8e9d8a32af4f500 | 0b367314ae8ecc42fceea20b7d98b9361789f2d9 | 1 |
| d3c35273db55dcda916db3b3f3a998d9 | 8fe086fd8fc2bda28b304cc38ccddfa55819e98d | 1 |
| d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | 20 |
| d46ca434e2518cd2ae05068f8579821c | 00c43af3a98dbd48248e4530375ab67f8b9c7a29 | 1 |
| d6fdfa460e2538caef7bf574453d7894 | 2d24c6762d6ec8575fc70f17f88a4f599043931f | 1 |
| d73ddac86b5f91f06043a66cd16fa35f | 91f8d883d7fd1d6678be04693f182fc5c1c68113 | 1 |
| d887a17cc43887d799fca62319d051db | cf6e8e0e96636477f1746bf8aa0ca9c3f5fa4c9f | 1 |
| d9df5b2e2927a94735c6c1c3112a9a5d | 0fe35373c0020995623ed3f7372d15d4d7d2eb86 | 1 |
| db511d02c1be9792fbdf4bea7c5fd3ca | 43a98d5a2e7aa411d0ca184d8382572e323f3165 | 1 |
| dc2784e32e79706ac09df198ec8835ed | 52b6a6caf32bfbb061436b7e710a5cc4625e5d9a | 1 |
| dc7acf30aacc4e0fcd40a903827f004b | a9bb13387a1e856f1b29c62a84bbdb0d3109781d | 1 |
| deb5c30cf4e8a2bfab38992264b1756c | 51106b2af57081242ab2c27dcc547e3c9b378630 | 4 |
| df97e5cfdb6a5e84b230d61536d9ac3e | e354da81e30913cda2f8ee813742631a091884f5 | 1 |
| e2da72071b15025127156f3ce6e5cca7 | b47ae4e38370d4d0a40ce73cfb507168344c5f23 | 1 |
| e7301356d96583bbd713667c56ca6f82 | 1559df29b3625ac3c687f5160e57874f8125fd12 | 1 |
| e81ecc08fd743d071619f226cb9715c8 | 3a7df03a12853503a0212379cc4e1f17c87c978c | 4 |
| e86ad85283c81dfa99acf8e7e47c0a0c | 0361e246ea05cefd4b0ae4bd8c1dfa6db82ae4b7 | 1 |
| e94f97f8f0d4dfbc11c487c98b88f58d | 4c17d3a67e6c384f8d7259b7562d2687f8e2db0f | 1 |
| eb349055b5eac7c0503ecf711f6fbca3 | fd04c3376f10a1a0b628d9ad163b9d263e014a3e | 1 |
| ecb6749289cd3277e5cdb970a36ae18d | d4f794dc10a472355c50727ba4cede94e4f92955 | 1 |
| edcd503951b8676ec401a3df89ee4df0 | 606fcae96a65dd92ee44e32aeb0090f8174a230e | 1 |
| f2b16423939a53598ac2ddd44a8cbf93 | d095bb8a1bca8c222ec81b5f8ee21535b692805e | 1 |
| f4152b0992dbb28a19e4447ef6a7b195 | 67dffc8090b19b96e86c6486402b3f8a38792c18 | 1 |
| f4d2127084a2277d9b0911714111849c | e745a76dedd998715f7197f697afca681de8a8d6 | 1 |

*Table G.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| f67552881bc13163f2b3abe2c9efb283 | 7ca1a295eebf4704ae6be060985bafc6d059fa05 | 1 |
| f77eb69c26e1f279329bf19c735d116c | 872517d323ea780c61153239bea1c35caefc756c | 1 |
| f8ff33c019580b3e4c8437d3ddaabfd7 | edd6b21f0dfb25146ea9e8db90a349ea1680e750 | 1 |
| fa70b0482ca9f558affc52d8576cd62e | 7efb058f0a9ce9a52e71869a2dc78dbd68230061 | 1 |
| fb4a1dad2dcf9a38e84a0c38c642357a | bae9f94196b7d2d539dbf3351e10b20dbc3b6069 | 1 |
| fbb7abadb02632161176e7cefdb874d5 | 0cb9b4bb73c4bdd0c4286e8b0777a27337c52905 | 1 |
| fc0567da64a9842ca71e73dfebda99fd | f38a9f6bfd411dd7d87055e65e92c290cd9e72de | 1 |
| fc3e8322d0bb5d1dc5f643dea86ab359 | e0c0134b207dce519bbe5213fea176d90dae898a | 5 |
| fece24feb630ae23b9171380c3116685 | ac0625c334905c8a543f3b4e0aa31438a1c22f04 | 1 |
| ff2339aaf556aa414f8f241726b1d3b4 | fcf786eccdfd566ac1a952d9c30237fa5affc5f4 | 1 |
| ffaaa451dd79de906024098fd4cf3614 | 7641ee9c335df770fea00aebf03af88778e2f1bf | 1 |

Compared TC1 hash lists to TC2 hash lists. NOTE: No changes to the Protected MBR, Primary GPT Header, or the Primary Partition Entry Array.

*Table 0.2* TC2 Changed Items

| # | Changed Location |
|---|---|
| 1 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$Bitmap |
| 2 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$I30 |
| 3 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$LogFile |
| 4 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$MFT |
| 5 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$sosrst.xvd |
| 6 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\appswapfile.xvd |
| 7 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\AppTempStorage |
| 8 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\AppUserStorage |
| 9 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\ConnectedStorage-retail |
| 10 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\GDVRIndex.xvd |
| 11 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$I30 |
| 12 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$LogFile |
| 13 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$MFT |
| 14 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$Bitmap |
| 15 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$I30 |
| 16 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$LogFile |
| 17 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$MFT |
| 18 | System Support (3) [40960MB]\System Support [NTFS]\[root]\cms.xvd |
| 19 | System Support (3) [40960MB]\System Support [NTFS]\[root]\controllers\cache0.cfg |
| 20 | System Support (3) [40960MB]\System Support [NTFS]\[root]\DataCollectionUploader_0 |
| 21 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$Bitmap |
| 22 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$I30 |
| 23 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$LogFile |
| 24 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$MFT |
| 25 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$I30 |
| 26 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$LogFile |

*Table 0.3* TC2 Added Locations

| # | Added Location |
|---|---|
| 1 | User Content (2)\User Content [NTFS]\[root]\PLS\ |
| 2 | System Support (3)\System Support [NTFS]\[root]\oddfwupd\ |
| 3 | System Support (3)\System Support [NTFS]\[root]\SharedStorage\ |
| 4 | System Support (3)\System Support [NTFS]\[root]\oddfwupd\0.log |
| 5 | System Support (3)\System Support [NTFS]\[root]\oddfwupd\sequence.txt |
| 6 | System Update (4)\System Update [NTFS]\[root]\updater.xvd |
| 7 | System Update (4)\System Update [NTFS]\[root]\A\systemaux.xvd |
| 8 | System Update (4)\System Update [NTFS]\[root]\A\system.xvd |
| 9 | System Update (4)\System Update [NTFS]\[root]\A\deltas.xvd |
| 10 | System Update (4)\System Update [NTFS]\[root]\A\sosinit.xvd |
| 11 | System Update (4)\System Update [NTFS]\[root]\A\SettingsTemplate.xvd |
| 12 | System Update (4)\System Update [NTFS]\[root]\A\sostmpl.xvd |
| + | Overabundance of numbered clusters in Unpartitioned Space |

*Table 0.4* TC2 Removed Location

| # | Removed Location |
|---|---|
| 1 | User Content (2)\User Content [NTFS]\[root]\246d3k |
| 2 | System Update (4)\System Update [NTFS]\[root]\2x42ir |
| + | Overabundance of numbered clusters in Unpartitioned Space |

# Appendix H. Test Case 3 (TC3) Creation

Date: Wednesday February 18th, 2015 beginning at 14:00
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228

Steps of the Process:

1. Connected Xbox One to TV.
2. Powered on Xbox One at 14:02
3. Signed in without network connection to Frank. NOTE: gamer tag had not been created yet but showed a gamer tag named "MoltenRhombus35" for Frank. Double checked to make sure this was the correct account and it was. Logged out.
4. Connected Ethernet to Xbox One and signed on with network connection as Frank. NOTE: gamer tag still showed as "MoltenRhombus35". Found out that Xbox Live automatically assigns a gamer tag when user first signs up profile. The user can change this tag once for free.
5. Changed gamer tag to FrankieXman at 14:29.
6. Created custom avatar for Frank at 14:33.
7. Made Avatar the gamer pic at 14:44.
8. Created Xbox Live Account at 14:49:40. Xbox Live Membership entered "R3D3Y-KBFBX-XF3K4-PP4J6-HP3BD".
9. Went to Microsoft Store/apps and began downloading top 25 most popular applications at 14:50. Ended downloads at 14:59.
10. Accessed Internet Explorer (IE) between 15:00-15:02.
    a. Opened
    b. Accepted default privacy settings
    c. Closed before entering any information
11. Accessed Netflix between 15:07-15:18.
. Signed-in
    a. Accepted new terms of service
    b. Watched the first thing that came up which was "Mr. Peabody & Sherman" for 5 minutes.
12. Accessed YouTube between 15:23-15:42.
    a. Opened
    b. Dismissed the guide
    c. Searched and typed "epic" then selected the auto finish option "Epic Rap Battles of History"
    d. Selected option "ERB"
    e. Played "Romeo and Juliet vs. Bonnie and Clyde Epic Rap Battles of-"
    f. Let ad load and play
    g. Watched video then went back by pressing "O"
    h. Played "Artist vs. TMNT Epic Rap Battles of History Season 3"

i. Went back with O to the search option.
j. Searched “game grumps” and selected “Best of Game Grumps – Jan. 2015”
k. Watched video for 5 minutes.
l. Exited YouTube

13. Accessed Blu-Ray Disk between 3:43-3:43
    a. Opened
    b. Forgot my blue-ray disk. Got an error message reading “We’re having trouble reading this. Make sure it’s a Blu-ray or DVD. If it’s a game, launch it from your games & apps instead. (0x91d70000)”
    c. Exited.
14. Accessed Twitch between 15:45-16:09
    a. Opened
    b. Selected Log-In
    c. Stated to “1) head to http://twitch.tv/activate on a mobile device or computer. 2) On the website, enter the 6-digit code to start broadcasting for free!” 6-digit code is “ECD5D9”.
    d. Went to IE on the Xbox One and followed site
    e. Selected sign-up
    f. Entered “FrankieXman” as user name, “diggs23” as password, 05-17-1987 as birthday, and FrankieXman@yahoo.com for email
    g. Signed up
    h. Entered code
    i. Went back to Twitch and selected “Channels”
    j. Selected “Captain5parklez”
    k. Followed Captain5parklez
    l. Entered chat option for channel and entered “lol”
    m. Exited Channel
    n. Entered channel FACEITTV
    o. Followed FACEITTV
    p. Entered chat option for channel and entered “pizza time”
    q. Exited channel and exited Twitch.
15. Plugged EX1 into Xbox One.
    a. Found at Settings\System\Manage Storage\External 3.7GB
    b. Could not access items on EX1
16. Accessed Xbox Video between 17:28-17:45
    a. Opened
    b. Browsed movies
    c. Added the following to my wish list:
    d. Guardians of the Galaxy
    e. Big Hero 6
    f. Birdman
    g. Dumb and Dumber to
    h. John Wick

i. Warren Miller's Playground
j. Ride: World Elements
k. Lucy
l. The Interview
m. Let's be cops
n. Game of Thrones
o. Inuyasha Season 7
p. Played the movie "Atari: Game Over" for 5 minutes.
q. Exited

17. Accessed Hulu Plus between 17:46-17:55
    a. Opened
    b. Start Your Free Trial
    c. "Please visit www.huluplus.com/xboxone on your computer and sign up with this code to start your 1 week free trial: GDX3M5J".
    d. Went to IE on the Xbox and followed the link.
    e. Pinned IE to home and opened
    f. Start your free week trial
    g. Entered: Frank OX 05-17-1987 frankiexman@yahoo.com diggs23 and continued
    h. Asked for credit card information. Due to not being on fully secure network the researcher decided to skip this and end the interaction with Hulu plus.
    i. Exited IE and Hulu Plus.
18. Accessed Skype between 17:55-19:15
    a. Opened
    b. Join
    c. Agreed to terms and conditions. Skype detected my Xbox profile and created an account with the information I already had attached to the account.
    d. Saw that the account was with frankox2015@outlook.com and the name that pops up for this account is FrankOX.
    e. Added account photo by taking a photo with the Kinect.
    f. Allowed Skype to send notifications to user,
    g. Got started and made a skype call to a bogus created account to Ted Lolly, password: lollieteddy85.
    h. Exited skype.
19. Accessed Media Player
    a. Accidentally accessed when attempting to get USB to work.
    b. Connected EX2 to Xbox One.
    c. Media Player open
    d. Found USB: EX2
    e. No access to this location.
    f. Went to settings/system/manage storage
    g. Did not see EX2.

h. Disconnected EX2, connected to lab computer and put DataSets on EX2 then reconnected to Xbox One.
i. Xbox One could now see EX2 in Media Player.
j. Opened Data Sets and played what Xbox One recognized as music. Files audio1, audio2, and "." played.
k. Went back and hit play all for videos and photos. 6 photo's played (rose, pizzeria, Idaho, bamboo, sunflower, & Stonehenge), 5 videos played (vid1.mp4, vid2.avi, vid3.mov, vid5.mpg, vid6.wmv).
l. When viewing the following items are the only that show in Media Player:
    i. 000_0021
    ii. 09260002
    iii. 100_0183
    iv. 02010026
    v. 100_0018
    vi. 100_0304crop
    vii. Audio1
    viii. Audio2
    ix. Audio4
    x. Vid1
    xi. Vid2
    xii. Vid3
    xiii. Vid5
    xiv. Vid6
m. Media is not giving an option to copy and paste items to Xbox One's hard drive (TC3) or transfer directories. Will have to force data on hard drive when outside the Xbox One. This is outside the scope of this research.
n. Exit.

20. Accessed Amazon Instant Video between 19:16-19:26.
    a. Opened
    b. No thanks, start browsing (not signed in and browsing, did not attempt to make an account)
    c. Watched trailer for Jack Ryan: Shadow Recruit
    d. Watched trailer for The Captive
    e. Watched trailer for Snatch
    f. Exited
21. Accessed Pandora between 19:26-19:37.
    a. Opened
    b. I am new to Pandora
    c. FrankieXman@yahoo.com, diggs23, 1987, 47906
    d. Searched for artist "Childish Gambino" and selected that artist to play.
    e. Liked the song Lights Turned On by Childish Gambino
    f. Went back and searched the artist "Kend" and selected "Kendrick Lemar".
    g. Liked the song Swimming Pool (Drank) (Extended Version) by Kendrick Lemar.

h. Searched for the artist “Girl Talk” and chose that option.
i. Disliked the song “Too Deep” and “Non-Stop Party Now” by Girl Talk
j. Went back and Exited
k. Xbox Music:
l. Opened
m. Selected Playlists
n. Created a new playlist named “This is it”
o. Went to add songs to the playlist by browsing the catalog
p. Played the album “If you’re reading this it’s too late” by Drake. Only played the first song “Legend”
q. Played the album “Birdman (Original Motion Picture Soundtrack)”. Only played the first song Get Ready.
r. Played the album “In the lonely hour” by Sam Smith. Only played the first song Money on My Mind.
s. Played the album “Hail to the King: Deathbat” by Avenged Sevenfold. Only played the first song “AndronikosTheme”
t. Exited.

22. Accessed HBO Go between 19:45-21:17.
    a. Opened
    b. Went to Collections
    c. Selected Kids
    d. Played Scooby Doo the movie but was prompted to activate an account by going to www.hbogo.com/activate and enter the code below: TP927K.
    e. Opened IE and followed site
    f. Activate Device: Xbox One
    g. Signed in
    h. Pin TP927K
    i. Went back to HBO Go and started Scooby Doo The Movie for 5 minutes.
    j. Exited
23. Accessed Uplay between 21:17-21:25.
    a. Opened
    b. Created account with autofill Frank’s info
    c. Selected an avatar for Frank
    d. Accepted terms and policy
    e. Went to games
    f. Selected Child of Light
    g. Went to video’s and played “Child of Light”
    h. Exited Uplay as games have not been played yet
24. Accessed WWE Network between 21:25-21:32.
    a. Opened
    b. Prompted to sign up at wwe.com and create an account but wanted credit card info. Researcher decided not to as it was on an unsecure network.
    c. Exited

25. Accessed Upload Studio between 21:32-21:35.
    a. Opened
    b. Selected to add a new clip
    c. Showed nothing in my box
    d. Need to play games to access more in this. Will return.
    e. Exited.
26. Accessed Halo Channel between 21:36-21:49.
    a. Opened
    b. Selected featured
    c. Selected view episodes
    d. Selected add to queue
    e. Played the first episode "Second Story Seed of Honor".
    f. Added Red vs. Blue Season 12 to Queue and played first episode.
    g. Exited.
27. Accessed EA Access Hub between 21:49-21:59
    a. Opened
    b. Connected to server
    c. Auto completed with Frank's profile info and had me create a password for the account: Digital!3. User name FrankieXman. Favorite pet: bird
    d. All items in this app require purchase, exited.
28. Accessed Crunchyroll between 22:00-22:15.
    a. Opened
    b. Played first video option to come up with Ads (no trial): Episode 1 Testimiate of sister new devil.
    c. Played 5 minutes of Yona of the Dawn.
    d. Exited.
29. Accessed Vudu Movies & TV between 22:16-22:18.
    a. Opened
    b. Chose to create account
    c. Entered email address
    d. Accepted terms
    e. Signed in.
    f. Browsed Most Watched
    g. Everything required purchase. Exited
30. Accessed Forza Hub between 22:19-22:27.
    a. Opened
    b. Selected News
    c. Selected Weekly Summary
    d. Watched video "My New Ferrari" and "Dubai Police Fleet"
    e. Exited
31. Accessed ESPN between 22:27-22:35.
    a. When opening ESPN app got the Achievement "Off the Bench"
    b. Went to most recent news and went to NHL
    c. Watched the video "Predators Rout Sharks"

    d. Watched the video “Panthers Edge Maple Leafs”
    e. Exited
32. Accessed MLG TV between 22:35-22:43.
    a. Opened
    b. Watched live video from “KYRSP33DY” for 2 minutes.
    c. Watched live video from “jahova” for 2 minutes.
    d. Exited
33. Accessed Plex between 22:43-22:47.
    a. Opened
    b. Prompted to sign in
    c. Signed in with FrankieXman, Digital!
    d. Need to purchase Plex Pass.
    e. Exited.
34. Accessed Audio CD Player 22:47-22:47.
    a. Opened
    b. Exited
35. Accessed Crackle between 22:48-22:59.
    a. Opened
    b. Went to featured
    c. Pinned The Throwaways to home and attempted to play but image would not come through, only audio.
    d. Pinned Hot Fuzz to home and watched 5 minutes of movie.
    e. Exited
36. Accidentally turned off system at 23:00, immediately turned back on.
    a. Turned off system again at 23:01.
    b. Turned back on at 23:11.
37. Put in Inglorious Bastards DVD and played for 10 minutes.
    a. Tried manual cd eject but wouldn’t work
    b. Put Xbox One’s case top back on and attached ribbon. Got DVD out with touch eject button.
38. Put in Ryze and started install and update
39. Started game with 11% done at 23:42.
    a. Started a new timeline as a recruit
    b. Started another install
    c. Stopped Ryze at 24:34am
40. Started Forza at 24:35am
    a. Started a new game as a single player.
    b. Played through introduction race.
    c. Selected local multiplayer (not networked multiplayer) and raced two courses.
    d. Stopped Forza.
41. Turned off Xbox One.

# Appendix I. Test Case 3 (TC3) Imaging

Date: Monday February 19th, 2015 beginning at 1:50 am
Examiner: Caitlin Gravel
Location: Purdue University Knoy Lab 228
Computer: CFLWIN15

- Windows 7 sp1 64-bit
- 8GB RAM
- Intel Core i5-2400S CPU @ 2.50GHz
- domain cit.lcl
- Time Zone Set: (UTS-05:00) Indiana (East) date set to Wednesday February 19th, 2015

Xbox One TC3 Hard Drive: (TC3)

- Manufacturer: Seagate
- Model: ST500VT000
- S/N: W3PA4MEL
- P/N: 1DK142-120
- FW: 0001MBC1
- Size: 500GB
- Physical: SATA 2.5”
- CHS and LBA not listed

External Hard Drive: (EX1)

- Manufacturer: Western Digital
- Model: N3565A
- S/N: WXF1A7221875
- P/N: WDBY8L0020BBK-01
- Size: 2TB

Tools:

- Windows Explorer
- Disk Manager (Logical Disk Manager)
- FTK Imager 3.1.4.6
- Tableau Firewire 800 + USB 2.0 SATA Bridge

Steps of the Process:

1. Took Xbox One apart to access the hard drive just as when accessing TC1 & TC2.
2. Connected TC3 drive to tools and turned on at 1:50 am. Note once again when the write blocker was turned on messages popped up for all 5 partitions: "You need to format the disk in drive (I:, J:, K:, L:, M:) before you can use it." Canceled format to all.
3. Once again attempted to write on each of the volumes but Windows Explorer would not even let me access the partitions to TC3 stating "(I:, J:, K:, L:, M:) is not accessible. The media is write protected".
4. Accessed disk management and again found TC3 listed as "Disk 3 Basic 465.76GB Read Only" with 5 partitions in use and unallocated space, the partitions did not have any names, and the reported file system was still listed as "RAW":

*Table 0.1* TC3 Partitions

| Name | Size | Partition Type | Reported File System |
|---|---|---|---|
| (J:) | 41GB | Primary | RAW |
| (I:) | 365GB | Primary | RAW |
| (K:) | 40GB | Primary | RAW |
| (L:) | 12GB | Primary | RAW |
| (M:) | 7GB | Primary | RAW |
| - | 779MB | - | - |

5. Proceeded to create the TC3 image.
6. Opened FTK Imager 3.1.4.6
    a. Create Disk Image
    b. Physical Drive
    c. \\.\PHYSICALDRIVE3 - ST500VT0 00-1DK142 USB Device [500GB USB] → Finish → Add
    d. Raw (dd)
    e. Skipped case info entry
    f. Named image "TC3_2-19-15.001" and saved it on external hard drive EX1. Also changed Image Fragment Size to 0 so the image would not be broken up.
    g. Left "Verify images after they are created checked".
    h. Began imaging at 1:54:24 am, ended at 10:16:40
        i. MD5 checksum: e5ba73896e6698fcfe90e2f29b35d01f
        ii. SHA1 checksum: 9daf045689c847e6f4f432571b8f238628946945
        iii. Sector Count: 976773168
        iv. Source data size: 476940 MB
        v. Cylinders: 60,801
        vi. Tracks per Cylinder: 255
        vii. Sectors per Track: 63

viii. Bytes per Sector: 512

7. Disconnected TC3 and reconnected to Xbox One. Put all equipment back where found and left lab.

# Appendix J. Test Case 3 (TC3) Analysis

Image File: TC3_2-19-15.001

MD5 checksum: d77a90737303fccaf9ca2acb8143351e

SHA1 checksum: 55cdba10adc62b20941136f011043c33e55a5afe

Cylinders: 60,801

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 976,773,168

Drive Model: ST500VT0 00-1DK142 USB Device

Drive Serial Number: W3PA4MEL

Software:

Windows Explorer

FTK Imager 3.1.4.6

Autopsy 3.1.1

Total file count: 3869 (810 less than TC2)

185 total unique file hashes

*Table 0.1* TC3 Unique Hash List

| MD5 | SHA1 | Amt. |
|---|---|---|
| 0546597403c3844850c60ae78cd5edb4 | 20b2955bffc2c19c1ec3afe82aa3d76c43c9d306 | 1 |
| 06319cc3693aa9b16d94dd60e0b4e168 | f73121ca022fc7cf72e56ae4f4fc822f06c99a03 | 1 |
| 0796567f38c0d7fa2d402ed9ac575b10 | 09a54e30f4f850d4765c6e08e4ce20e6fe552148 | 1 |
| 080386bcb0c58c0bf1618d2d7ffc7525 | 35b398213c6b4bd9550594b6f6e18ccc463fe992 | 1 |
| 0805bc6281e0c28ae12b37bad0cbb627 | ec1e1d62f25e8b410c4d47008ee9ff400e8e704b | 2 |
| 0cb1099ee088093a5cbb4c8cc0fd1556 | 95693181a5792da022a4f151ca40d3399a03cfd9 | 1 |
| 122dd294e44b50559f1769a877c8e753 | d35553f49273d92e28fef92988de61d53f8ea2b7 | 1 |
| 136684549d26b21ccf81729d43e897d1 | 9e12f64d5c4fbac507729570275c6b52a2c2efac | 1 |
| 166fc4b9722b8047b707e7c646c76a75 | 49101f0816a6c17fd5863e77c9bdcbe2fa77cd02 | 1 |
| 183fd4099b5aa63e9bbccbcc3bcfb303 | 8391f29df80eaf3c0fcce8b4ce8a73e8d904f646 | 1 |
| 18f40283e94415cae928d4216654f653 | ddfbf2c59cc1c1a559f1156c749fac0c4b5ae23e | 1 |
| 1cdaefd37fc83464b29aafbc7f754916 | c0eb1fea4495c8c49647c582c9ba65ab4d7e0908 | 1 |
| 1ce79b10ed92aa06c8fbd605f8b83ecc | 506d6e02dec736fbefbe5707c8a1df0edf8d3e0b | 1 |
| 1d748d6235553d44a2c2903812abdc06 | f222502bf4d54cfb1019fe45f343582478b0aa4b | 1 |

*Table J.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 1e361430258da7f9d2553293e3ac723b | 78445fc491d8e23b3812f3d6a26f7af986abbde4 | 1 |
| 1fa02b90bcb02ce56e22a0805ec9fd2a | c96b8167d3ce937aa5ba47b077f16df96a40f0dd | 1 |
| 1ffb17510d3c389d8963bb3fbcae740f | 68d9121caa09e9f314f1f1630e128a6e5ba9794f | 1 |
| 209c81a16cccb6936901ea78ee530571 | e9b0d7d775be88ef07eef03aa520a063652d2d4a | 1 |
| 20d718307730690062ee6b7281ae5742 | 263d69259efd2b5cbf9b48b12b3515a8781378da | 1 |
| 23b5793757b5db5d26744a56ffa1e3f1 | 6034b085137733020818a543819567d5c10a71ed | 1 |
| 2b65b29b4133274492e247726071b35b | 392088180a0337da6dace7a093558f25e4e2baee | 1 |
| 2cfcac52c1bab63906b5fe86d94861f7 | dae30fc275ea3c835d97b5e992e627b7cddad993 | 1 |
| 2e1459c0273ade852dbf7369172b1dd8 | 158af0658367584c4bd64e5fa4c933fa92fef472 | 1 |
| 2f282b84e7e608d5852449ed940bfc51 | 2c2ceccb5ec5574f791d45b63c940cff20550f9a | 3587 |
| 2f550fa2e03eccfed53223fe5ce2f3b6 | 952a0bb80cc6cf0140839c97c599d87ff32fa757 | 1 |
| 2f8b78c0afa0dd910042ce51ddfc27fd | 4d9c0089b59ce4087d223b99f5c33a168064e230 | 1 |
| 30f3fb693759b623bd468523068db4b5 | ef75b37d170403700369ac0afee53ea4ab442dd1 | 1 |
| 314e60c4b98c4a0f95caaec6685fdd59 | 62af8cae07a27699888dbd533eb4ded5a741cd8a | 1 |
| 352340aaa26350f176f67ebed22e9468 | 7f6c65c3912ef60ce211f631c83d9f08c8358821 | 1 |
| 358afb2be5387086a1be7da04a6150db | 2374bff0efa8fbe322c5e0e29f657848704e1665 | 1 |
| 36d7c154f7bcd854cfdc26174406b848 | 9e8710c92f79e64fe0535db1af7bdfcbf6e44384 | 2 |
| 397e01f35a5c162a600b16b6cb8f25b8 | cae2d2eea396f3137bb209f31adabf2e7a65276c | 1 |
| 3b9d715e82946b3f6545dc9ce8bbe517 | 8081c1e6cf361d07f8bb28fa5a7dd1cc785d1928 | 1 |
| 3c8197cf20e7f199f9a24a6b785c1604 | 231b46bb6b9fa81cff0fc94ef06e5d04854cbbcd | 1 |
| 3dae037a4cdcb10684501b6d31d65a20 | 106aa5f2158c5f50f80b9e52639755dca3d74606 | 1 |
| 3f35779fca79720f75f00b9f5b6bde03 | e1f210de9519ccd71fcd276f48fce7ace88c43e4 | 1 |
| 3f8d746a91e101f887a8e2984026e2aa | 72fd9d960ff0eeb834c370d18b38db092de67f8d | 1 |
| 41d1de316a765c3804e63b0d82ddfb2d | 4d29dfd1b2051af06bffec4eaf5f78d50bfb0123 | 1 |
| 464379cc355b512c78788d323b87ff25 | 62f7398b85d58478548f981b64eb4cb486e8de10 | 1 |
| 4721c82200624f82a4ae426e092454f6 | bad8eefbabeb355161c1590a7346a2a9a45b8a1e | 1 |
| 4781df8adc61e16eb4adcb0301749613 | db4d5476c3b2d2aadd0b0d6e3296c547f1653c03 | 1 |
| 48784b65e7c932baff5b5693d84466cd | 6c76c02acfc449a5b3f439fc9e1d5939dc1cc62a | 1 |
| 4942faa946adef562b39d12b1534c9c3 | 9adb291f7c039284fb376687d3e47166d08b9cf8 | 1 |
| 49caba25f2de87b7917392b8c63aec4c | edfa5c8dd12148ef633fd43626542e2ab97974ad | 1 |
| 4af824a16fee99ab67b1b47f94353aa2 | 10d7d4ce1949371201d2e6ad52b5fc1af4ea2c47 | 1 |
| 4d1b61ea5d69d4bfdd53b814820c2fca | 02ea96b7fa6e871e8bbf9e14afa178a335daef47 | 1 |
| 4d390d4862e880154aed02df9432d80f | 152666e40fe49c73a9fb0cfefffe0b9890426688 | 1 |
| 4eb7f4984baa00a80d0123b181822a1b | 1bf1049727ff1e52bba9aafb104231198c9dd05c | 1 |
| 5191ab5a6ddf692f24e137ccd2634328 | 6aa5dc83d799f863b5477ebfa1fb22805ba5cd05 | 1 |
| 51f03672d2152c11f0ff3f399e272922 | abb5dcb132358e0df5add93887379562af7e44a9 | 10 |
| 5315235fc500ab10521f0d92610ee4d5 | e7d97834ba9210dba17de4886d857be22d6e4adf | 1 |
| 586ad722b35e66ec9508cbdd054d82c9 | 43b7dc9f0c1fe1db9aea932e3133a1b5b962e06e | 1 |
| 5a48c2eb9fbd45d420b5a794c5672de5 | e48bad554ae6ff5f07b644f36143334cf593705b | 2 |
| 5abd611446f9e8e9c2fe6baab91e3df2 | cb7aca18264b724f8a9490460f29ae6c3635387f | 1 |
| 5c5d38f6d2a7d5af20d6cbaa3acf3060 | 9afc1b7acc9053d7a28ee1c62fe34388925eada7 | 1 |
| 5e58d6d766454f2e7aa304f26bcda97e | 89065f45d646f24accc77dc707f75b2cc4bf2ff5 | 1 |
| 62244af3c96842f764ecc9cbbfed5417 | 490c5f83df1eb0372f8f1bc4275a38282e482c55 | 1 |
| 656d004649be5160508a3f9eb78386ec | 75cc5015cff3bb930fdc0d5b8061ed750e7db5ac | 1 |
| 675055b71fead63af48c389190eed3d6 | 4d6e3e14315a80a241a1a309104376d3385346c3 | 1 |
| 687985620e9bcea4865953c79eed183b | 5f9e7f0675605a5d58751d960c2f541354eb4e14 | 1 |

*Table J.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| 68fec310b994f254701a4d6b26537ee6 | 56581b457040db04171b53183075b09e3bfaa1c2 | 1 |
| 693bd78f0b3f7ab6806cd39d49f1e148 | 06460da63d4ab717686eaf3ea2e07c70a5c0e004 | 1 |
| 6947a1ff3354a1b6aafe118924abc6ac | a69c5e8878d3a2cdc22e3951363513a2303ce3a2 | 1 |
| 69767357bd3136222ad1f274954d7a82 | b5309b623ab288157585a530a77d71537af94b87 | 1 |
| 6b66429e970f481027e84fcbef88e38d | ce12bc48154869f192bbf69fc85807a1e7ef5900 | 1 |
| 6bb149afa324ce2b2aabcb2c3a70f6a9 | 1a888029ca94b4ead7ada483b60bcdb41105c4a7 | 1 |
| 6c20f7343d677aab0e8764d002765c01 | 5615e0bfd40a2a8c81c4d0073d83b73a9cfaac9b | 1 |
| 6c768abe7517044afcd418e6c8a18a33 | eef231ee80882665317ecbd819703425ca03d3ca | 5 |
| 6cda3ab3e6c5fa5cd606f07fddfdbeec | 046f017bc290a78fde66b6d0f07d53e500f20f92 | 1 |
| 6df25890719229603a4ee00c21adaf07 | bc1c7d9fcb5316fab4895456f169c12d0d1e9aaf | 1 |
| 710a811fb3679f5701a8494b00729106 | 76f211ba32c2c035d34630d651e0750fd3c233e2 | 1 |
| 7147a7f3dbeee702202e0a74f88f1530 | 14e5ee5ca6e574077d0ecffcda8597f14e3a3956 | 1 |
| 7165d94359886c0cb0f29504f5c11467 | 9a8070d17c81d629a3a00a0f3b6cff84204ff944 | 1 |
| 727294268d73a090a3ba58ae2ab672cb | bbf52e9282bf9c8c23a58c8a6bf872f2b76308a9 | 1 |
| 727694f0465e86f739d1b83235c31548 | 8a41c1d5f5939fcc19331a63556eecd5864b7333 | 1 |
| 73c2bd65ac0e1e73e435937eb181cf60 | c35573f2dbd0cd284d2fd5bac26b74309397b66b | 1 |
| 73d8bd2371cec53d2faf4f036fc65e22 | e29b0e7ae8d9ef6e2b2dbe482eb21caadab39929 | 1 |
| 766c36a65e48b9b83a4052210388184c | 23c82069eecc5fde6df5da69325408504565792d | 1 |
| 78df7d13538aa76aca97b8866347ed84 | e91e524a5fe21cad756cfc89546a87e87bfa4cfa | 2 |
| 790742fa73920dbf2f7bcb8a171243a8 | 5bf7219a9074a2429cb28fed8a746906b74d44c9 | 1 |
| 7c1ec3cf185afb99bbc70925748fae72 | d148e882f73707fee834226a09e4e7d191d3403f | 1 |
| 7cb729cf9ada1fc358b37c0b8b5b7ce7 | 532aa868f19043ebecf8c9a10899bfa3147e32f9 | 1 |
| 7d68e5880964810a63e0913f0489bbf0 | 8911ee35b48e176de0cc43bab640f9707f07cc1a | 1 |
| 7df03c94e79e4dda462dd276eea6fc44 | 3978be682abd094e8b6e8ffb81f3e5f5a6dd75c0 | 1 |
| 7e85c536816811126fc8f0512561c19e | 5ba19850e6505aa6692b1e2c6a3f3b838338b7ea | 1 |
| 7ff498a44e45e77374cc7c962b1b92f2 | 5161a18e27b9ca9f5d04f2154576bf1ffb1121e8 | 5 |
| 8010d4683006b5dd7ac2b5ac27ad050d | b0cde380832992aae356a0db713a391dcab6af5d | 1 |
| 8265922f61653dc1892ccb4d8f701a8e | 601f932e417e130edd99b6285196e9bc886ca031 | 1 |
| 8274dc8683724b52651766b2dd089b42 | 2bb0be460de913213dd2d4668f94917864ccc5a6 | 1 |
| 83a34aa0a3b783fc229b78bd6d48d254 | b23f42c5a2ce3ebd396daa1f8416ec502f5c7edf | 1 |
| 846dd3c05b166896a5af3ea74b3ad680 | c0620f2c514dae5433324c4cdbb7b1216f2dfdcd | 1 |
| 89a87953c8cec4193274f83b92feec44 | ca161f0d88cba1a340fb4fc90d6091b9897d9ac5 | 1 |
| 8a31d95f63af54967d42a3b9b5f9a408 | 1ba3a832bd111adbb48208a86098e00755ea88ea | 1 |
| 8a7a85db98e91004b149fdcdeed5f054 | 54218ef7f1b88d6a4996be04037c9ef4b4ff5eb5 | 1 |
| 8ce20ce49936eb3879328968f729e880 | 3066118919777fdc4f5354618192997c74b0cd43 | 1 |
| 8dff116fa589af347cd0c206cdc2ef27 | 3aa2a0fdef25ad857501a8a370f0939dc3d49406 | 1 |
| 8e90f3f16cc1fd4ba3f5a4d918181f7b | cab36f1deb571fbc50b3ff939a1f11e1cf158311 | 1 |
| 9127d4b76ccd3ef715576cb478e7d630 | 7619b5e9095d9edeb627a4d0083df066330a9284 | 1 |
| 91d68cfd6ffeb894d70acb4d211d9dfa | d61087632564b3529e7b841bd98ba23535b4525b | 1 |
| 95fe8cf0ea7a88154e1523a60280488b | df737753bcd2abf701dd916424eae9294a567d9f | 1 |
| 9699fdc561f554ac9c0f022834a4dcea | 535a22cfcd512fe2eda9e4d9c1d5067bb8fa017d | 1 |
| 97f9ef13a1aa24f4e5dd226057249ed1 | d17a20dd25fc238bbe5547f1c06abd9303d3d60b | 1 |
| 9a907739909f1e8e9927d1def1231689 | 794d8725f6d0688f09892aee235fb955f09d6070 | 1 |
| 9e1be64a753cf001a4bc5ce74752346f | 1319fcf802798d26b7071ae88716c07207eea150 | 1 |
| a0923df212bf9a4189cb2a15dc4626af | b04d94dd04f2415edaee5547b1210b7190d0a1aa | 1 |
| a0b1512cea6286fdb5db65018849489e | 4ace8815abad5d9ef6d840c8beb7d95895d838bf | 1 |

*Table J.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| a120cf12517ffa1fdbe292ee506d3bed | 6aea1ce93700d894c83ca5e6e870baf5c5712e7f | 1 |
| a3465c3ba79bd2631da72df1c2a40898 | 5baa321db97bb9806b7dd2a39dc525b5087d5fc0 | 1 |
| a42dd0428bc3dd190dd50df6b2a81700 | a4ddf8f5854fa5fe1d11a883c0338175c6d9c178 | 1 |
| a6dcb8041f7a2e9d236527994ff0f3e2 | 809fafd115128f7126a4c34d80dc5e0214379024 | 1 |
| a8c6767f5a450c9b49899f287452eefa | c50f8b22094be95fa2fa2ba1887160dfbfe92c5e | 1 |
| aa0858eea994d6b99affd94304ac635d | 17b9433b504eea95de619a1abcc380d570b90d14 | 1 |
| ab981967d9f545695c396db3787f8a49 | 2497adcb05fe54ad8a55c8fd2c145951ea039237 | 5 |
| acfe8314fd109f0be892bd3fab51e2ed | ebc414d490df3b1ff2c59b57e6ae4daecd5dba27 | 1 |
| ad617ac3906958de35eacc3d90d31043 | b49d7f48300701235231f6b6fc3d92a5630f9e70 | 5 |
| aee4247a1fe04cd6f7e1501f919e42b4 | 1bc3d127d5f35fdca4b253699e616ea56035410c | 1 |
| af164022602e83c7586afd92c802b2f8 | ac5da3f770c5eba43bfdd9f78004f4bb5201c7d0 | 1 |
| b0d06d53d7d5491acf6a7cda1579b224 | c6fc579929187826e4f8896b1a2d4e92b7029f88 | 1 |
| b4202f7fe985b9648b4676e6f70832bd | d37c2b3927946ed617455b3c5913fcab0bc1af52 | 5 |
| b48aab0739c6786030ad3b39f4f090e4 | 4d6ce185f5da7b2456de6e0729c604a32f26fff4 | 1 |
| bc8617576815910180d1eb604a0bcdd9 | 474c039e27345412b0d8c871669263e2963592ba | 1 |
| bed6ab23b0e4a4f2f903a87afbec4b3b | 53f475644e4ca0daeba0c59a18df804da1233310 | 1 |
| c0d7cca8dfe3966a3023c30ce3cfebda | e2752ae08e2019212def6763ea138bc636466dec | 1 |
| c2c244b10d9fc7f6f48ed1ea5cc4999e | 1fd09283c4a4681930778b95ce85706eeb7106b9 | 1 |
| c44f26b77ce61a95a487765916c95a4a | 427d4f6596c29338c458b8b03b36032461a39ac6 | 1 |
| c54d16984503f206bf56f5fa5731f581 | 4155c198ff821b2dcd026fc4dfd023961fbcccae | 1 |
| c62367558e59b7e1249ae427369d102a | ded4c083c88245a37e3b38395ae0f0814fcc7ece | 1 |
| c6f32cdb0612efaa422911f3be9dca6a | 4e07f85ed718a42a4f02dce5cc714782b88085fc | 1 |
| c8c158b10df60d2a147053985127e766 | 8f9fc5bc71c58a71ecc3de28876c9d7746dbfa00 | 1 |
| c9616c056c5247a7f4a821fd2a255ae6 | 730e6ab9859af48b7619c6f57d1d558329eeacbd | 1 |
| cfcd208495d565ef66e7dff9f98764da | b6589fc6ab0dc82cf12099d1c2d40ab994e8410c | 1 |
| d0a8194a9b11f8d89d073016c06e76d3 | ee9b733edb8928458ebe97becdacbec48f5c2a24 | 1 |
| d0d75577042a8848c13860450e0adbeb | a240a99aa21a2ad44f0ffc01a2e8532db2fd50eb | 1 |
| d0e8abd769fa4d66b7a622e8d0c0fb49 | 4aa0bfa399fdd31d09731ba3f534b4e382f16246 | 1 |
| d2389a74d9784cc5aeaca86f6ce50993 | 623c0330e86dd7ce07dc20665d6e225cc514f362 | 1 |
| d3c35273db55dcda916db3b3f3a998d9 | 8fe086fd8fc2bda28b304cc38ccddfa55819e98d | 1 |
| d3de3450bf82a8fd46074c0e07ae381b | 662c0e8b7e38d81aea51f4fdbb564cb0a54c02af | 1 |
| d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | 20 |
| d44cac632ed017fd40c4e89695c5d325 | 7a8373fd2f4eebae30fbbf12d01d2a0024f97690 | 1 |
| d5e4ed7d12bd084e0bf64c8fc7dac6eb | 1f6c528e66b5b5ba4bb6be01489e0e5959b6b55d | 1 |
| d730c03e674f79d3d5aef7a344c26a8e | fdb8a6b397bb6369d8eb3c7dac47c7cebb67b2a3 | 1 |
| d7c438a0f84fe20d98c289909f7178b8 | 3501313d66cc7f58567c0f8e4122104e33cd00c8 | 1 |
| d9df5b2e2927a94735c6c1c3112a9a5d | 0fe35373c0020995623ed3f7372d15d4d7d2eb86 | 1 |
| da9c64d014ca514e7d8c68eadd9bda99 | 02551c45074e8453453ea9d707d4e97beedae6d2 | 1 |
| dbbe162825e7b9e58e37c8c46ebb7052 | 8b6e8619958d19f97051c05bdcd5231b176df283 | 1 |
| dc2784e32e79706ac09df198ec8835ed | 52b6a6caf32bfbb061436b7e710a5cc4625e5d9a | 1 |
| dcce2ae90ee1b34b167bb065e4a108b5 | 912e524cdaa8e8f5caad76cbb76e8044b1587583 | 1 |
| deb5c30cf4e8a2bfab38992264b1756c | 51106b2af57081242ab2c27dcc547e3c9b378630 | 4 |
| e17053b5f91c937302cde3cc045be980 | 088f06ae0d12fa6b6217d34b5286a1a89a3e9814 | 1 |
| e2da72071b15025127156f3ce6e5cca7 | b47ae4e38370d4d0a40ce73cfb507168344c5f23 | 1 |
| e2fbc3860bc16fbf97ab6ae86b9ae8b4 | aed9ea7953f2a5b1a20d8404b81a3ab8c179f502 | 1 |
| e483b2c4ea0785e6fa71d13ba94a355c | 538f135525d166ff160804bf87d3eed6f2784e17 | 1 |

*Table J.1 (Continued)*

| MD5 | SHA1 | Amt. |
|---|---|---|
| e52b61ca908384e86c52a40085ef55fa | 53e6337a086a96fb37f11be84ada1c39e0807e67 | 1 |
| e7301356d96583bbd713667c56ca6f82 | 1559df29b3625ac3c687f5160e57874f8125fd12 | 1 |
| e81ecc08fd743d071619f226cb9715c8 | 3a7df03a12853503a0212379cc4e1f17c87c978c | 4 |
| e86ad85283c81dfa99acf8e7e47c0a0c | 0361e246ea05cefd4b0ae4bd8c1dfa6db82ae4b7 | 1 |
| e94f97f8f0d4dfbc11c487c98b88f58d | 4c17d3a67e6c384f8d7259b7562d2687f8e2db0f | 1 |
| ea2204d97754ecb4c29af5d7bfab61aa | 142b9773b70b27a692c75022c79aad8659cebee8 | 1 |
| eb349055b5eac7c0503ecf711f6fbca3 | fd04c3376f10a1a0b628d9ad163b9d263e014a3e | 1 |
| eb8cbf7032a6ab9c73afb496fda8747a | 3f89cbf9bfcfd0c6315f58553aeb28816453df16 | 1 |
| ec7af7386bc25fda768a7853aa6dcd3f | f2ccba3fc871d710037d9ec3262a6896052d230e | 1 |
| edcd503951b8676ec401a3df89ee4df0 | 606fcae96a65dd92ee44e32aeb0090f8174a230e | 1 |
| f03a632623bfcec005f1ba26d3375937 | 88aa3948648bca5765d208d4c604d3e604f3e851 | 1 |
| f086fd72ba16681a0c620eb80b133ee0 | decd0cf818111492a29bd96ddd4f2a9c6eb2c1b6 | 1 |
| f0a55a130ea18ec612878aba617efe84 | f948b56ea7d60cec4873baa03a26ec69c5014970 | 1 |
| f21164d554d650a831f01018068e7897 | d9373f41e92744f409db8bda525f4b803a70773c | 1 |
| f4152b0992dbb28a19e4447ef6a7b195 | 67dffc8090b19b96e86c6486402b3f8a38792c18 | 1 |
| f43ff879d89093f96dde472cf0b1f426 | 336a3c9b4d2de88d6d6e17f7b9674c282b98417b | 1 |
| f4d2127084a2277d9b0911714111849c | e745a76dedd998715f7197f697afca681de8a8d6 | 1 |
| f572a951486b04ee032d32955b8f8cda | 75874124d575bf0e4fedafd8b566580efae4c5ed | 1 |
| f6a1dc7578a99f4bffd97861d2b35889 | b7da46b3cf71e7c35bf55915a8ed34dcb9311c4f | 1 |
| f77eb69c26e1f279329bf19c735d116c | 872517d323ea780c61153239bea1c35caefc756c | 1 |
| f9228f09ce436260fc4f282025c88502 | 03391334922e38eeb3e53b439bde34582669b412 | 1 |
| fa70b0482ca9f558affc52d8576cd62e | 7efb058f0a9ce9a52e71869a2dc78dbd68230061 | 1 |
| fa9cdbd6c7bb38a9b8c1c7112447509e | c7ee21b6d8b7107c8d69edfd021c3258d162bd4f | 1 |
| fb4a1dad2dcf9a38e84a0c38c642357a | bae9f94196b7d2d539dbf3351e10b20dbc3b6069 | 1 |
| fbbf311ade5c8fbffbf83c7e5d4cc0b1 | 3ad5e14379a8ec6a75b1e4e0151626c81deeaf27 | 1 |
| fc061ed3c383dbf3ca9e765df335583b | 077de28c9df4d71933d201421dcf25db641b2a88 | 1 |
| fc3e8322d0bb5d1dc5f643dea86ab359 | e0c0134b207dce519bbe5213fea176d90dae898a | 5 |
| fc3f8cfe7e7ad49317311d4aed65b921 | ad0bb72a68d29f9e8844f4d77008f9137aef6c08 | 1 |
| fde1cd7e515b4ac2aca92db1e930505a | 750b7f20784406f841902adae144c935224fa223 | 1 |
| fe21fcce87647dc359f6576442baa1ee | f13cb031619967aed398e53c9bbb7300f0717a6f | 1 |
| fe8fc85a9efbcede081436cf65efcd6c | 61ba65ee69f765507f9339b5bafd8de5e52e358e | 1 |
| fece24feb630ae23b9171380c3116685 | ac0625c334905c8a543f3b4e0aa31438a1c22f04 | 1 |
| ffb14422313e7ad74aad8a79cb239191 | 9f95284746d2fa7c79793a8166455edd793e753b | 1 |

Compared TC2 hash lists to TC3 hash lists. NOTE: No changes to the Protected MBR, Primary GPT Header, or the Primary Partition Entry Array.

*Table 0.2* TC3 Changed Locations

| # | Changed Location |
|---|---|
| 1 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$Bitmap |
| 2 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$I30 |
| 3 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$LogFile |
| 4 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$MFT |
| 5 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\$sosrst.xvd |
| 6 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\appswapfile.xvd |
| 7 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\AppTempStorage |
| 8 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\AppUserStorage |
| 9 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\ConnectedStorage-retail |
| 10 | Temp Content (1) [41984MB]\Temp Content [NTFS]\[root]\GDVRIndex.xvd |
| 11 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$Bitmap |
| 12 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$I30 |
| 13 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$LogFile |
| 14 | User Content (2) [373760MB]\User Content [NTFS]\[root]\$MFT |
| 15 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$Bitmap |
| 16 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$I30 |
| 17 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$LogFile |
| 18 | System Support (3) [40960MB]\System Support [NTFS]\[root]\$MFT |
| 19 | System Support (3) [40960MB]\System Support [NTFS]\[root]\cms.xvd |
| 20 | System Support (3) [40960MB]\System Support [NTFS]\[root]\controllers\cache0.cfg |
| 21 | System Support (3) [40960MB]\System Support [NTFS]\[root]\DataCollectionUploader_0 |
| 22 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$I30 |
| 23 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$LogFile |
| 24 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$I30 |
| 25 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$LogFile |

*Table 0.3* TC3 Added Locations

| # | Added Location |
|---|---|
| 1 | Temp Content (1)\Temp Content [NTFS]\[root]\temp01 |
| 2 | Temp Content (1)\Temp Content [NTFS]\[root]\temp00 |
| 3 | User Content (2)\User Content [NTFS]\[root]\F706F390-A956-4C2C-8D4B-67196C3A2C92 |
| 4 | User Content (2)\User Content [NTFS]\[root]\F3DBA358-AC97-4882-8E4E-8219FAE8FF1B |
| 5 | User Content (2)\User Content [NTFS]\[root]\478C0B29-148A-4814-AA63-3D759ED4A459 |
| 6 | User Content (2)\User Content [NTFS]\[root]\F1C16E8E-594A-4282-B5B4-4E3EF93AC8F4 |
| 7 | User Content (2)\User Content [NTFS]\[root]\5516852A-9F51-453C-84AC-A2B02F5023A2 |
| 8 | User Content (2)\User Content [NTFS]\[root]\7F1327EB-FA14-4A27-B72A-FDF3393DBB5E |
| 9 | User Content (2)\User Content [NTFS]\[root]\466E2035-64EF-47D8-A7B7-DC8EE810DB64 |
| 10 | User Content (2)\User Content [NTFS]\[root]\79BB07B5-F533-4E6E-AC74-94595DB47CF9 |
| 11 | User Content (2)\User Content [NTFS]\[root]\116AE68B-3CEE-462C-AF8A-57D5525AA40E |
| 12 | User Content (2)\User Content [NTFS]\[root]\E07277CC-7AFF-4F81-9990-5EDF0F7B073D |
| 13 | User Content (2)\User Content [NTFS]\[root]\F5022706-83BB-4AC2-B425-4FBA4D78D82D |
| 14 | User Content (2)\User Content [NTFS]\[root]\12F8A6D0-CB0B-4860-981B-D546278985F2 |
| 15 | User Content (2)\User Content [NTFS]\[root]\265C6BAD-C47C-4A63-A192-5818037FAC97 |
| 16 | User Content (2)\User Content [NTFS]\[root]\47EDE6D3-AF95-4B45-904A-228E39EEAB3D |
| 17 | User Content (2)\User Content [NTFS]\[root]\068D245A-11BC-479B-8769-033BEB60208D |
| 18 | User Content (2)\User Content [NTFS]\[root]\4431298F-71B0-4FA0-9566-A981A2B6AE45 |
| 19 | User Content (2)\User Content [NTFS]\[root]\B72D5AA7-6941-472A-8A5C-8BACE4D0B6DF |
| 20 | User Content (2)\User Content [NTFS]\[root]\F33D08D8-73E9-4897-9BBF-8736A32E34D9 |
| 21 | User Content (2)\User Content [NTFS]\[root]\02BBDA9B-E4D2-400A-BA6E-84E7DEA4F2BE |

*Table J.3 (Continued)*

| # | Added Location |
|---|---|
| 22 | User Content (2)\User Content [NTFS]\[root]\05D64F3E-9E29-47CE-A23C-4E86F2AFB09A |
| 23 | User Content (2)\User Content [NTFS]\[root]\242BF9CE-DA7C-4872-805E-E873ADB32C07 |
| 24 | User Content (2)\User Content [NTFS]\[root]\0EE0F048-4608-4CB4-AC16-BD285CB6A3B0 |
| 25 | User Content (2)\User Content [NTFS]\[root]\B0655109-C128-4519-9E36-0D370809CD0E |
| 26 | User Content (2)\User Content [NTFS]\[root]\D0134385-33C0-4382-BE31-58C4CF4F453E |
| 27 | User Content (2)\User Content [NTFS]\[root]\AppSpecificStorageXvd1 |
| 28 | User Content (2)\User Content [NTFS]\[root]\72354F8E-9A35-4148-811D-0E36CA95C64C |
| 29 | User Content (2)\User Content [NTFS]\[root]\13096BD0-8237-47FA-80BE-29A3563CF0BF |
| 30 | User Content (2)\User Content [NTFS]\[root]\FB4C8FF5-ED19-48FE-A462-851A076663C0 |
| 31 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00687733 |
| 32 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00713333 |
| 33 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00738933 |
| 34 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00763133 |
| 35 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00788733 |
| 36 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00882170 |
| 37 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00907770 |
| 38 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00923541 |
| 39 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00924068 |
| 40 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00926186 |
| 41 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\02032935 |
| 42 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\02111483 |

*Table J.3 (Continued)*

| # | Added Location |
|---|---|
| 43 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\03831553 |
| 44 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\09699303 |
| 45 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\47840587 |
| 46 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\95662081 |
| 47 | System Support (3)\System Support [NTFS]\[root]\F706F390-A956-4C2C-8D4B-67196C3A2C92.xvi |
| 48 | System Support (3)\System Support [NTFS]\[root]\esram.bin |
| 49 | System Support (3)\System Support [NTFS]\[root]\F3DBA358-AC97-4882-8E4E-8219FAE8FF1B.xvi |
| 50 | System Support (3)\System Support [NTFS]\[root]\478C0B29-148A-4814-AA63-3D759ED4A459.xvi |
| 51 | System Support (3)\System Support [NTFS]\[root]\F1C16E8E-594A-4282-B5B4-4E3EF93AC8F4.xvi |
| 52 | System Support (3)\System Support [NTFS]\[root]\5516852A-9F51-453C-84AC-A2B02F5023A2.xvi |
| 53 | System Support (3)\System Support [NTFS]\[root]\7F1327EB-FA14-4A27-B72A-FDF3393DBB5E.xvi |
| 54 | System Support (3)\System Support [NTFS]\[root]\466E2035-64EF-47D8-A7B7-DC8EE810DB64.xvi |
| 55 | System Support (3)\System Support [NTFS]\[root]\79BB07B5-F533-4E6E-AC74-94595DB47CF9.xvi |
| 56 | System Support (3)\System Support [NTFS]\[root]\116AE68B-3CEE-462C-AF8A-57D5525AA40E.xvi |
| 57 | System Support (3)\System Support [NTFS]\[root]\E07277CC-7AFF-4F81-9990-5EDF0F7B073D.xvi |
| 58 | System Support (3)\System Support [NTFS]\[root]\F5022706-83BB-4AC2-B425-4FBA4D78D82D.xvi |
| 59 | System Support (3)\System Support [NTFS]\[root]\12F8A6D0-CB0B-4860-981B-D546278985F2.xvi |
| 60 | System Support (3)\System Support [NTFS]\[root]\265C6BAD-C47C-4A63-A192-5818037FAC97.xvi |
| 61 | System Support (3)\System Support [NTFS]\[root]\47EDE6D3-AF95-4B45-904A-228E39EEAB3D.xvi |
| 62 | System Support (3)\System Support [NTFS]\[root]\068D245A-11BC-479B-8769-033BEB60208D.xvi |
| 63 | System Support (3)\System Support [NTFS]\[root]\4431298F-71B0-4FA0-9566-A981A2B6AE45.xvi |

*Table J.3 (Continued)*

| # | Added Location |
|---|---|
| 64 | System Support (3)\System Support [NTFS]\[root]\B72D5AA7-6941-472A-8A5C-8BACE4D0B6DF.xvi |
| 65 | System Support (3)\System Support [NTFS]\[root]\F33D08D8-73E9-4897-9BBF-8736A32E34D9.xvi |
| 66 | System Support (3)\System Support [NTFS]\[root]\02BBDA9B-E4D2-400A-BA6E-84E7DEA4F2BE.xvi |
| 67 | System Support (3)\System Support [NTFS]\[root]\05D64F3E-9E29-47CE-A23C-4E86F2AFB09A.xvi |
| 68 | System Support (3)\System Support [NTFS]\[root]\242BF9CE-DA7C-4872-805E-E873ADB32C07.xvi |
| 69 | System Support (3)\System Support [NTFS]\[root]\0EE0F048-4608-4CB4-AC16-BD285CB6A3B0.xvi |
| 70 | System Support (3)\System Support [NTFS]\[root]\B0655109-C128-4519-9E36-0D370809CD0E.xvi |
| 71 | System Support (3)\System Support [NTFS]\[root]\D0134385-33C0-4382-BE31-58C4CF4F453E.xvi |
| 72 | System Support (3)\System Support [NTFS]\[root]\72354F8E-9A35-4148-811D-0E36CA95C64C.xvi |
| 73 | System Support (3)\System Support [NTFS]\[root]\13096BD0-8237-47FA-80BE-29A3563CF0BF.xvi |
| 74 | System Support (3)\System Support [NTFS]\[root]\FB4C8FF5-ED19-48FE-A462-851A076663C0.xvi |
| 75 | System Support (3)\System Support [NTFS]\[root]\controllers\cache1.cfg |
| 76 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$I30 |
| 77 | System Update (4) [12288MB]\System Update [NTFS]\[root]\$LogFile |
| 78 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$I30 |
| 79 | System Update 2 (5) [7168MB]\System Update 2 [NTFS]\[root]\$LogFile |
| + | Overabundance of numbered clusters in Unpartitioned Space |

*Table 0.4* TC3 Removed Locations

| # | Removed Location |
|---|---|
| 1 | Temp Content (1)\Temp Content [NTFS]\[root]\qzfwSy |
| 2 | User Content (2)\User Content [NTFS]\[orphan]\ |
| 3 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\1smcbl_gb_dev.bin |
| 4 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\1smcbl_gb_rtlA.bin |
| 5 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\1smcbl_gb_rtlB.bin |
| 6 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootanim.dat |
| 7 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootkbe.green.bin |
| 8 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootkbmse.green.bin |
| 9 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootkbsse.green.bin |
| 10 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootmbe.green.bin |
| 11 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootmbmse.green.bin |
| 12 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\bootmbsse.green.bin |
| 13 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\ExtHost.green.xvd |
| 14 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\Header_a.bin |
| 15 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\Header_b.bin |
| 16 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_113_dev.mng |
| 17 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_113_rtlA.mng |
| 18 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_113_rtlB.mng |
| 19 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_123_dev.mng |
| 20 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_124_dev.mng |
| 21 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\smcfw_124_rtlB.mng |
| 22 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\SystemAux.green.xvd |
| 23 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\SystemExt.green.xvd |
| 24 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\Template.green.xvd |
| 25 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\Template2.green.xvd |
| 26 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\update.ini |
| 27 | User Content (2) [373760MB]\User Content [NTFS]\[orphan]\XosInitExt.green.xvd |
| 28 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00079843 |
| 29 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00105443 |
| 30 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00131043 |
| 31 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00156643 |
| 32 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00182243 |
| 33 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00207843 |
| 34 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00233443 |
| 35 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00259043 |
| 36 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00284643 |
| 37 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00310243 |
| 38 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00335843 |
| 39 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00361443 |
| 40 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00387043 |
| 41 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00412643 |
| 42 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00438243 |
| 43 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00463843 |
| 44 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00489443 |

*Table J.4 (Continued)*

| # | Removed Location |
|---|---|
| 45 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00515043 |
| 46 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00540643 |
| 47 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\00566243 |
| 48 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\47823843 |
| 49 | User Content (2) [373760MB]\User Content [NTFS]\[unallocated space]\95662080 |
| + | Overabundance of numbered clusters in Unpartitioned Space |

# Appendix K. Digital Storage Devices Used

Xbox One Hard Drive:
- Manufacturer: Seagate
- Model: ST500VT000
- S/N: W3PA4MEL
- P/N: 1DK142-120
- FW: 0001MBC1
- Size: 500GB
- Physical: SATA 2.5”
- CHS and LBA not listed

Image Storage:
- EX1:
  - Manufacturer: Western Digital
  - Model: 1213B
  - S/N: WXF1A7221875
  - P/N: WDBY8L0020BBK-01
  - Size: 2TB
- EXLibrary:
  - Manufacturer: Western Digital
  - Model: 2515B
  - S/N: WX41AB415L4A
  - P/N: WDBMWV0020BBK-04
  - Size: 2TB

File Transfer:
- EX2:
  - Manufacturer: SanDisk
  - Model: Cruzer
  - S/N: NG04G2308005789DMI
  - Size: 4GB
- EX3:
  - Manufacturer: Western Digital
  - Model: 0515B
  - S/N: WX21e54mz410
  - P/N: WDBZFP0010BBK-94
  - Size: 1TB

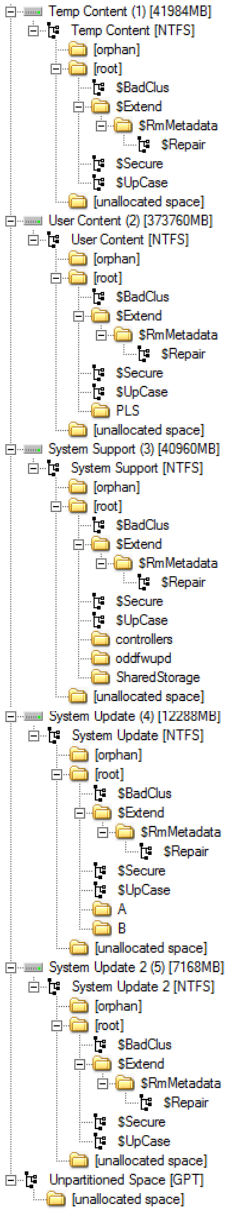
# Appendix L. Test Case Image Hashes

*Table 0.1* Test Case Image Hashes

| Test Case | MD5 | SHA1 |
|---|---|---|
| TC1 | f6518a28cd6d9325a1c9e1153d54d5ef | f675c832b865158760b2cf7ef11dee546a01cbd3 |
| TC2 | e5ba73896e6698fcfe90e2f29b35d01f | 9daf045689c847e6f4f432571b8f238628946945 |
| TC3 | d77a90737303fccaf9ca2acb8143351e | 55cdba10adc62b20941136f011043c33e55a5afe |

# Appendix M. Xbox One Directory Tree

*Figure 0.1* Xbox One Directory Tree.




NOTE: The "[orphan]" folder in each partition is not an actual folder located within the Xbox One directory, FTK Imager creates the folder as to show items that have no parent directory.