May 25th, 11:00 AM

A Practitioners Guide to the Forensic Investigation of Xbox 360 Gaming Consoles

Ashley L. Podhradsky
Drexel University

Rob D'Ovidio
Drexel University

Cindy Casey
Drexel University

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL

A PRACTITIONERS GUIDE TO THE FORENSIC INVESTIGATION OF XBOX 360 GAMING CONSOLES

Dr. Ashley L Podhradsky
Drexel University

Dr. Rob D'Ovidio
Drexel University

Cindy Casey
Drexel University

ABSTRACT

Given the ubiquitous nature of computing, individuals now have nearly 24-7 access to the internet. People are not just going online through traditional means with a PC anymore, they are now frequently using nontraditional devices such as cell phones, smart phones, and gaming consoles. Given the increased use of gaming consoles for online access, there is also an increased use of gaming consoles to commit criminal activity. The digital forensic community has been tasked with creating new approaches for forensically analyzing gaming consoles. In this research paper the authors demonstrate different tools, both commercial and open source, available to forensically analyzing gaming consoles, specifically the Xbox 360. Used Xbox 360 gaming consoles were purchased online through popular auction sites for the purpose of this research.

Keywords: Digital Forensics, Identity Theft, Xbox 360 Gaming Console, Cyber Crime

1. INTRODUCTION

Technology has introduced new mediums for criminal and misuse activity. While the crimes and misuse are not new, the medium they are carried out on is. Therefore, the digital forensic community has to work to create new standards, tools, and approaches to investigating gaming consoles.

While many gaming consoles exist, Microsoft's Xbox 360 is the most popular among American consumers, selling over thirty-nine million consoles, six million more than their top competitor the PS3. (Bloomberg Businessweek, 2010). With this rise in popularity, the Xbox 360 has also become a popular medium for criminals. When Bill Gates first announced his plans for the Xbox 360 gaming system in January 2000, at the International Electronic Consumers Show in Las Vegas, some critics proclaimed that this new console was nothing more than a "...PC in a black box (Official Xbox Magazine staff , 2005)." These critics were not too far off the mark. The Xbox 360 is not only similar to a personal computer - it is actually *more* powerful than most average personal computers. The hardware and technical specifications found in today's Xbox 360 console includes a detachable 250GB hard drive, an IBM customized power –PC based CPU containing three symmetrical cores each capable of running 3.2 GHz, a 512 MB GDDR3 RAM (which reduces the heat dispersal burden and is capable of transferring 4 bits of data per pin in 2 clock cycles for increased throughput), and 700 MHz DDR (theoretically supplying a swift 1400 MB per second maximum bandwidth) memory (Berardini, 2005).

Given the advanced hardware, high storage capacities and online access, the Xbox 360 has become a favorite medium for cybercrimes.

2. CRIMINAL ACTIVITY ON GAMING CONSOLES

The latest gaming consoles by Microsoft, Sony, and Nintendo provide users with computing and Internet functionality that is similar to the functionality offered to users of traditional computing

devices (i.e. desktop and laptop computers running Windows, Macintosh, and Linux operating systems). The Xbox 360, for example, allows users to access social networking services such as Facebook and Twitter, stream Internet radio through Last.fm, and watch movies via Netflix. The PS3 allows users to send instant messages and create chat rooms to banter with other users over the PlayStation Network. It also allows users to access web-based email (e.g. Hotmail, Gmail, Yahoo! Mail) and websites through its proprietary browser. The Nintendo Wii allows users to send email messages, including messages that contain picture attachments, to other Wii users and users of third-party email services. The Wii, PS3, and Xbox 360 all offer users the ability to store media files on a hard drive or in flash memory.

The functionality of the PS3, Wii, and Xbox 360 provide offenders with a powerful tool to use for committing and supporting criminal activity. The communication options available through these gaming consoles are particularly helpful to criminals. Text, voice, and video communication options within gaming environments and through consoles menus provide offenders with easy access to a population of suitable targets for victimization for crimes that produce economic and social harms.

Criminal activity that produces economic harm is expressed in terms of monetary damages (Criminal Intelligence Service Canada, 2007). These damages can be borne by individuals, communities, businesses, and governments and can be committed by a single person or an organized criminal group. Subscriber data (e.g. name, address, phone number, credit card number, gaming network ID, and gaming network password) connected to an account for an online video game console community can be exploited by criminals for direct financial gain or sold to third-parties for their misuse. Virtual currencies and virtual goods amassed by a game player can, at times, be converted into real-world currency through in-game transactions or third-party services (e.g. EBay, PlayersAuctions, and IGE) and are, thus, attractive targets for economic fraud.

Media reports document the involvement of gaming consoles in a variety of crimes aimed at illicit financial gain, including video game piracy (McHugh, 2011), cracking/hacking (Rivington, 2007; McMillan, 2011), identity theft (Lemos, 2007), credit card fraud (Evers, 2007), and phishing (Fried, 2005; Deleon, 2008; Constantin, 2010). For example, Harris (2009) reports on the theft and, subsequent, sale of more than 500,000 Xbox Live account credentials. He also notes that the credentials sold for approximately £5 per account.

Unlike crimes that produce economic harm, crimes that produce social harm are not expressed in terms of monetary damages (Criminal Intelligence Service Canada, 2007). Instead, criminal activity involving social harm is expressed in terms of the physical and psychological damages to the victim.

Children who use gaming consoles and respective online networks are particularly vulnerable to crimes producing social harm. When playing games with other people over the Internet, children often find themselves immersed in environments devoid of the traditional guardians (e.g. parents and teachers) who serve to protect them in the physical world. Media reports have linked gaming consoles to the victimization of children in cases of rape (Hill, 2009), child pornography (Bush, 2008; Weinstein, 2009; Peterson, 2010), online harassment/bullying (Snow, 2007; Fujji, 2010), and child sexual solicitation (Bullock, 2009; Cavalli, 2009; Potter, 2009). Hitt (2011), for example, details a case in which a 36-year old woman traveled from Florida to Maryland to meet a 13-year old boy she met in an Xbox Live chat room. During her visit, the woman engaged in sexual activity with the boy. She was subsequently charged with rape and child molestation. Chat transcripts discovered during the investigation also showed that the offender exchanged sexually explicit images and videos with her victim.

3. XBOX 360 GAMING CONSOLE

The file data format used on the Xbox 360 is FATX, which is an offshoot of the more familiar FAT32, found on older computers and storage devices (Paul K. Burkea P. C., 2006). In fact, the two possess virtually identical format and file data layouts. Unlike the FAT32 however, the FATX does not

contain the backup boot or file system information sectors found in FAT32. Additionally, FATX does not support Unicode, which is often utilized by examiners when performing forensic analyses (World Lingo , 2010). The reasoning behind these variations in the file format is that the Xbox 360 was designed primarily for entertainment as opposed to productivity. Thus, redundancy and legacy are apparently forfeited in order to increase the system's speed.

Some of the identifying data which can potentially be retrieved from consoles include, but are not limited to, a user's name, address, telephone number, and credit card information. Credit cards are used to purchase games through the Live Arcade, pay for Xbox 360 Live membership, and buy merchandise such as gamer icons and console themes at Xbox 360's Live Marketplace. One popular movie subscription service, Netflix (Netflix, 2011), even permits its members to rent movies using credit cards directly though their Xbox 360 consoles. Other personal information includes profile data, chat transcripts, blog files and online history. In fact, the Xbox 360 is even capable of keeping a gamers' blog for the user by monitoring the account and automatically generating blog entries about their daily gaming activities.

In addition to gaming consoles becoming incidental to a crime, such as with identity theft, they are also increasingly becoming the actual *instrument* of the crime (i.e.: using the Xbox 360 to transfer and store child pornography).

Given the abundance of data that is retrievable on Xbox 360 consoles, there is an increasing demand to learn more about what tools and approaches are favorable in acquiring data on game consoles. While many tools exist, as with traditional computer forensics, not all tools are created equal.

For this research, two Xbox 360 gaming consoles were purchased randomly from an online auction site and a popular classified forum respectively. An additional Xbox 360 hard drive was retrieved after being discarded, bringing the total tested drives to three. The researchers acknowledge the sample size is small, however they feel it is appropriate due to the fact the major testing is on the software, not the drives.

4. THE INVESTIGATIVE PROCESS

Once removed from the consoles (if applicable), the drives were extracted using T10 and T4 Torx wrenches. Although some forensic examiners report problems accessing data due to locked drives, we did not encounter any difficulties. A variety of open source and commercial tools were utilized to examine the drives. Also, before each tool was used both pre and post Md5 and SHA-1 hashes were recorded for validation purposes utilizing EnCase**.** Direct checksums were also obtained using Linux to curtail dependency and maintain objectivity on the software being tested. The reasoning for utilizing such a wide array of tools was twofold. First, there is not a great deal of information available to date regarding the structure and forensic examination of gaming consoles. This is not because gaming consoles are new per se, but rather that they have evolved so rapidly over the past decade. Secondly, no one tool was capable of presenting the drives in their entirety. The software used to examine the Xbox 360 drives included the following:

- *XPlorer360-* Freeware tool that allows access to three Xbox partitions and memory cards. Xplorer360 allows access to both physical and logical areas of the drive
- *FTK 3.0-* Forensic Toolkit (FTK), produced by AccessData is a commercial suite of applications for forensic analysis of digital media, including Xbox consoles
- *FTK Imager-* Freeware tool from AccessData which allows users to forensically image and analyze drives
- *Modio-* Freeware modding tool that allows Xbox users open their system to allow for customized use of their console

- *wxPirs-* Freeware tool that allows extraction of access to PIRS (themes or gamertags), LIVE (content downloaded from Xbox Live), or CON (internal files specific to Xbox) container files on Xbox 360's
- *ProDiscover Basic-* Freeware tool based on the commercial ProDiscover- allows viewing of each sector to determine data storage locations
- *Digital Forensic Framework* (DFF)- Is an open source tool that aids in the collection and analysis of digital evidence
- *Hex Editor XV132* – Freeware hex editing tool that runs on memory and doesn't need to be installed on the host system, incorporate a built in hex to string and allows bookmarks
- *XFT 2.0- C*ommercial Xbox toolkit developed by Protowise Labs that allows for access to configuration, modification, and user files, included recovering deleted files
- *Data Rescue's DD (DrDD)-* Freeware tool that recovers deleted files off of corrupted storage devices or partitions, while not designed for gaming consoles, it was used to determine functionality
- EnCase Forensic v6 – Commercial forensic analysis tool by Guidance Software (Guidance Software , 2011)

In addition to the above software, several operating systems were also employed during our analysis. This was done to not only to eliminate the possibility that any of the software limitations encountered were the direct result of an incompatible OS, but also to gain a clearer understanding of the FATX file structure. The operating systems utilized for this study were:

- Windows XP
- WIN 7 (Ultimate)
- Red Hat Fedora 14
- Ubuntu 10.10

Determining which operating system to use created somewhat of a dichotomy at times. While the majority of the tools available only operate in a Windows environment, the Linux operating system appeared to be the most compatible with the actual gaming console itself.   In fact, gamers seeking to download and play unsigned copies of Xbox 360 games, or elicit superior gaming and dashboard options, can modify their console using Linux. This is referred to as soft-modding or simply modding. Microsoft discourages these types of system changes, which if executed will void the system's warranty. (Microsoft, 2010)

In a recent effort to discourage console modifications, Microsoft released an Xbox 360360 update in early August 2009. This was referred to as the "homebrew lockout" by the Free60 Project, an organization which both promotes and supports users running homebrew applications and Linux operating systems on their Xbox 360360 gaming consoles. The update overwrote the first stage boot loader (responsible for starting the system when it is turned on) thus causing any updates or modifications made by the user to render their system useless. (Free60 Project, 2009)   This information can be of significant importance to digital examiners who are seeking to establish or understand the system's bootstrapping process and subsequent drive structure,particularly given how thorny this task can be.

Because the Xbox 360 does not contain the same type of BIOS found in a PC, it should not be expected to boot like the typical PC. In fact, as early as 2002, MIT researcher, Andrew Huang, noted in his detailed study of the Xbox 360's structure that the Xbox 360 contains a "secret boot block"

(Huang, 2001). Perhaps this was an attempt by Microsoft to deter tampering and possibly initially, although not very successfully, as a security mechanism. This information is pertinent because if the boot block is a decoy – then what else might be a red herring?

An example of this ambiguity was found upon examination of the hard drive's partitions. Partition 1, the second partition encountered when opening an Xbox 360 drive, appears to be empty – that is, when it can be found. There could be several reasons for this. It might be reserved for future use or simply just not accessible. Another option is that it could be a lure – a hard drive honey pot of sorts to deflect, and possibly detect, unauthorized access or changes.

Partition 1 was only viewable on two of the hard drives examined, including one sample containing a second or merged set of files. These integrated or legacy files were located on Partition 3, as seen in the capture below using the open source utility, Modio. (Image 1)
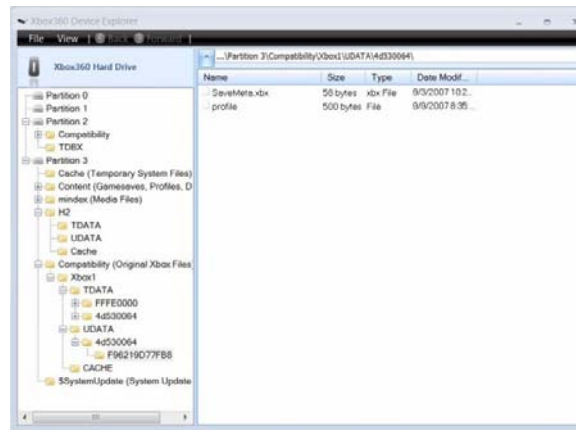

Image 1- Partitions as viewed in Modio

Modio is a modding utility that allows Xbox 360 users to manipulate their consoles. It is also handy for viewing image files on the fly without needing to export them first into another program. (Image 2) However, the option to extract files is also available. Although not yet tested by NIST, further evaluation of this utility might prove valuable to law enforcement agencies.
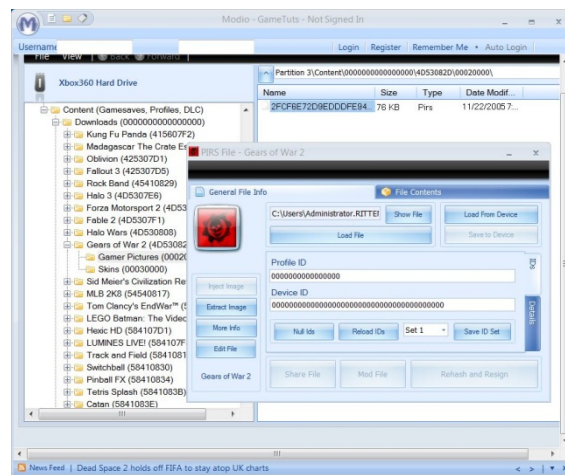

Image 2 – Image viewed in Modio

The hard drives were accessed using a USB 2.0 to SATA adaptor with a 50/60 Hz power supply cable. Writing access to USB adaptors was disabled via the registry in Windows and driver-level write

blocking in Linux. Imaging with Access Data's Forensic Toolkit 3.0 (FTK) was a timely process which did not yield extremely productive results. The limited results obtained could be attributed to the FATX file structure of the Xbox 360. The extracted files were inspected by examining the raw data to determine if the drives were intact, deleted, or reformatted.

All three of the drives exhibited signs of being overwritten as evidenced by large sections of zeros in non-program specific files. It would be difficult at best however to declaratively state the drives were reformatted without further studies as each operating system has its own unique way of performing this process and while the Xbox 360 does share some similarities with a PC, it cannot truly be measured using the same criteria. (Computer Gyaan, 2010)

Xplorer360

One of the more useful tools employed was a utility called Xplorer360. Xplorer360 is an open source program that enables gamers to open and view, edit, or export data from their Xbox 360 hard drives through their PC. The results were very swift with the hard drive opening in under a minute. Partitions and their subsequent subfolders are displayed in the left hand pane. More detailed information about a selected file or directory is displayed in the right pane. Although earlier studies of the Xbox 360 drive found that Partition 0 was an empty partition (Bolt, 2011), our analysis found two drives that did exhibit files on Partition 0. (Image 3) The empty partition was initially attributed to the extra file mentioned earlier on Partition 3, Xbox 3601 (Partition 3\Compatibility\Xbox 3601), which when observed using traditional forensic tools such as FTK 3.0, appeared to be on the only drive in our study that possessed an empty partition 0. However, after utilizing popular modding tools such as Modio and Explorer360, we were able to ascertain that the two drives containing data in partition 0 *included* the drive with the additional Xbox360 folder. The drive which *did not* contain viewable data in Partition 0 was the newer of the three drives as ascertained from sector 4 (07-02-09). This indicates that the empty Partition 0 may be the result of the August 2009 update which as mentioned earlier, reportedly overwrote the first stage boot loader.
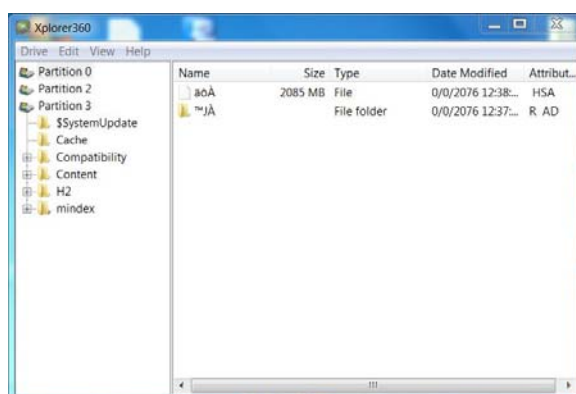

Image 3 - Partition 0, Viewed in Xplorer360 showing a JA folder and an aoA file

Ironically, although FTK 3.0 did not generate any remarkable user data independently, additional data was revealed later using FTK Imager. After the drive's contents were opened and dumped using Xplorer360, the extracted files were opened in FTK Imager for analysis. One test drive produced a file containing a user's name. This file, which contained profile saved data, was identified as Partition3\Content\0000000000000000\4D5707D4\00000001\BTLsave, last modified on 8/28/2007. (Image 4) Other personal data obtained from the same drive included a user's first name and a partial or abbreviated city name. This was later confirmed by comparing the name discovered with the name and location of the individual who originally owned the console.
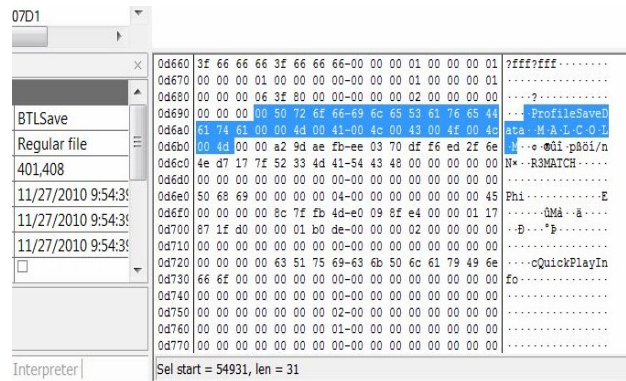
Image 4 – Profile saved data revealing a user's name as seen in FTK Imager

In partition 3, under system update files (Partition3\$SystemUpdate) was a 6.96 MB Pirs file named su20076000_00000000. Extracting this file and opening it with wxPirs revealed a list of xexp files (Image 5). WxPirs is another open source utility commonly used by gamers seeking to modify their gaming consoles. It enables users to open PIRS, CON, and LIVE files - commonly found on the Xbox 360360 drive.
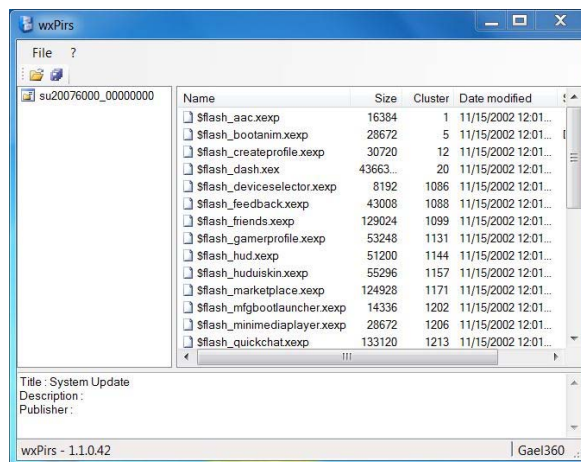

Image 5 - Partition3\$SystemUpdate\ su20076000_00000000 extracted from Modio as viewed in wxPirs.

The xexp files were then extracted from wxPir and opened further with a Hex Editor (XV132). Once opened in the Hex Editor we could see that the files contained symbol table data - most likely used for linking programs to other programs. Xexp files are software development files that store information about a program and that program's functions. (Microsoft, 2005) This particular system update was found on all three of the hard drives. (Image 6)

Image 6 - $flash_bootanim.xexp file extracted from wxPirs as viewed in XV132

These system update files were identified as belonging to an update released by Microsoft in January 2007. (Billo, 2007) Apparently, similar to the August 2009 update discussed earlier, this was possibly another attempt to keep gamers from modifying their consoles. It is also interesting to note that the August 2009 update was not found in the system update folder on any of the drives examined.

A closer inspection of the sectors on each drive was performed using ProDiscover Basic and Digital Forensic Framework (DFF). ProDiscover Basic is the demo-freeware version of Technology Pathway's ProDiscover Forensics. It enables digital examiners to scrutinize a hard drive's clusters and files hidden in slack space. Digital Forensic Framework (DFF) is an open source cross-platform tool for examining digital media. It is a rather efficient utility which enables the user to find hidden data. While ProDiscover was not useful for drive acquisition, DFF was. Once the drives were extracted using DataRescue's DD (DrDD) however, ProDiscover was very instrumental in our research.

On two of the drives, including the one with the assimilated systems, the first piece of data observed was found on sector two - ©Axb (programming code belonging to Microsoft. In the other drive, the first sector containing data was sector four. All three drives had a rather interesting find in sector four, the name JOSH, followed by some digits and a date, as indicated in image 7 and table 1.

Drive	Name	Digits	Date
001	JOSH	97-001	03-19-07
002	JOSH	49-001	07-02-09
003	JOSH	78-001	08-07-08

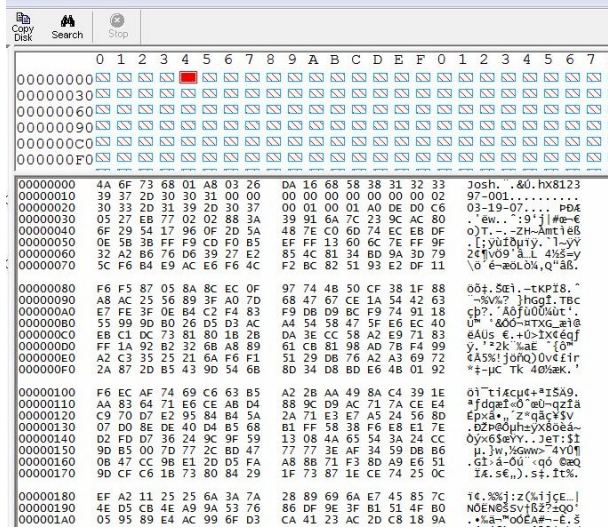*Table 1 – Sector 4 data found*

Image 7 – Sector 4 in ProDiscover Basic

This could signify a number of things including a digital ID, some type of Microsoft numbering or cataloging scheme, or the developer's signature (i.e.; Joshua Gilpatrick, Microsoft Xbox 360 Program Manager). Later, we encountered files with a similar structure (i.e.:CON hx8123 97-001 03-19-07). Information regarding the hard drive itself was located in sector ten. (Image 8)
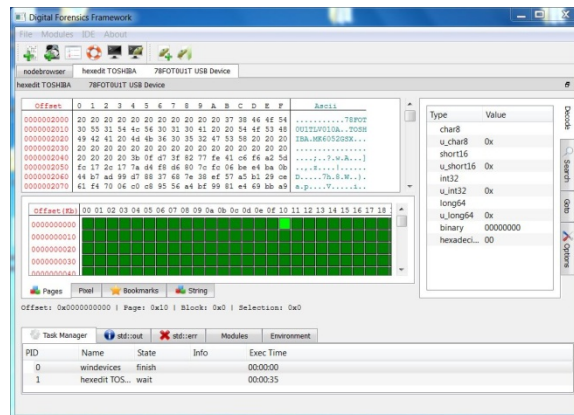

Image 8 – Sector 10, Hard Drive Information as seen in DFF

Examining the Xbox 360 drive using EnCase can be extremely productive - depending on what you are looking for. Image 9 shows some of the data obtained on one of the drives imaged with EnCase. In this particular instance, we can see NAT (Network Address Translation) rules for a site called Bungle.net, where Halo players can have their stats tracked or purchase games and merchandise. (Bungie, 2011)

Microsoft defines three categories of Nat on their consoles- open, moderate, and closed. These attributes, or policies, control the amount of user access to Live services. The ports used are UDP (User Datagram Protocol) ports 3074, 5060, and 5061. (OAI Networks, 2011) Considering that UDP is a connectionless protocol, this could present a considerable vulnerability (ie: UDP 5060 and weak SIP or Brute Force Attack) of which users are not warned about. Thus, when gamers who are not familiar with NAT or VoIP weaknesses elect to change their settings in an effort to host games or communicate with other players, they are also unknowingly introducing more vulnerabilities into their system.
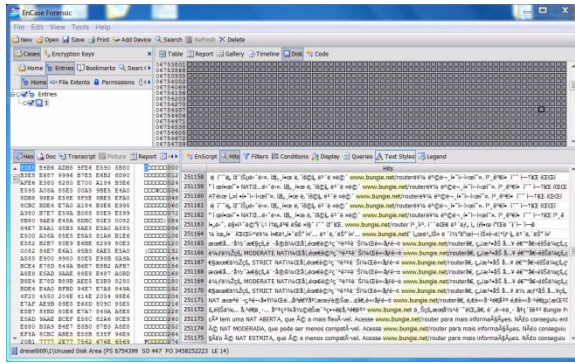
Image 9 –Microsoft's defined NAT as viewed in EnCase

Another benefit of utilizing EnCase is its ability to discover credit card information on a hard drive by looking for numbers encoded with ASCII digit characters that match valid credit card company identifiers. These numbers are then run against the Luhr formula (an algorithm used to validate credit cards, social security numbers, and other identification numbers). (University of Michigan, 2008) Performing a fast scan on one of the drives resulted in a possible credit card hit. (Image 10) Although this does not definitively prove there are any credit card numbers on the hard drive, it is highly probable given the results obtained. The Bank Identification Number in this hit identifies this as a Bank of America Discover Card. (BinBD, 2011)
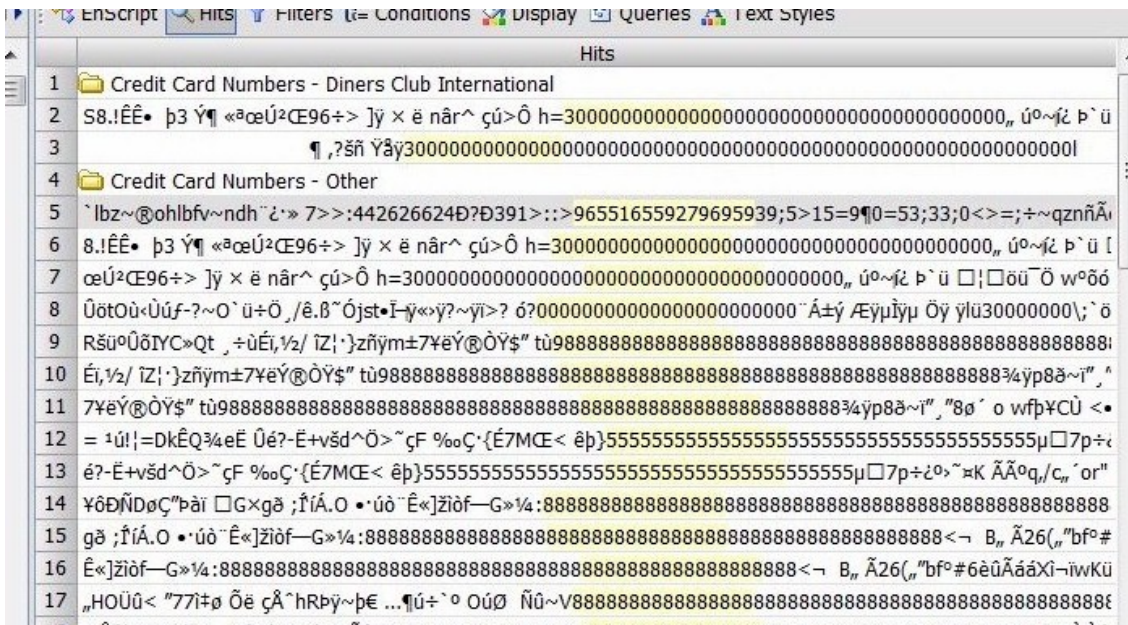
Image 10 – EnCase credit card hit

A new tool recently developed to address the need for forensic software capable of obtaining information from nontraditional devices is XFT 2.0 Game Console Forensic Toolkit, developed by David Collins, a computer scientist at Sam Hoston State University in Texas and distributed by Protowise Labs. (Protowise Labs, 2011) XFT 2.0 features both FATX and XTAF (derived from MS-DOS) file system mounting and preview, file hashing, recovery of deleted files, and file type identification. It is designed to run on Windows operating systems and features a user-friendly interface, although when tested on both Windows XP and WIN 7, the utility did not run as smoothly on WIN 7.

While we were able to see the names of deleted files, we were unable to actually view their contents. When attempting to view deleted files the message "XFT cannot currently display deleted files. Right click and choose "properties" for disk offset and starting cluster" was obtained, as seen ini mage 11. By right-clicking on a selected deleted file, the user is given the option to export, hash, or view the properties of that file (Image 12). This information can prove very useful for law enforcement agencies in cases involving child sexual exploitation where the hash values obtained can be compared against known values from the CVIP (Child Victim Identification Program) database (FBI, 2011). Although other forensic tools tested performed hashes, XFT was the only tool which showed the deleted files from the Xbox 360 drives.
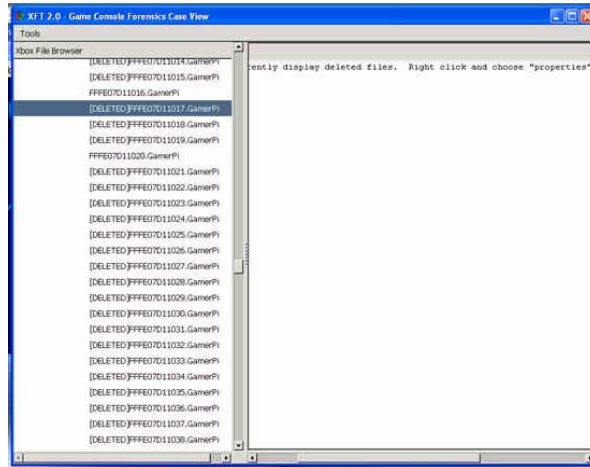
Image 11 – XFT message – "…cannot currently display dleted files."
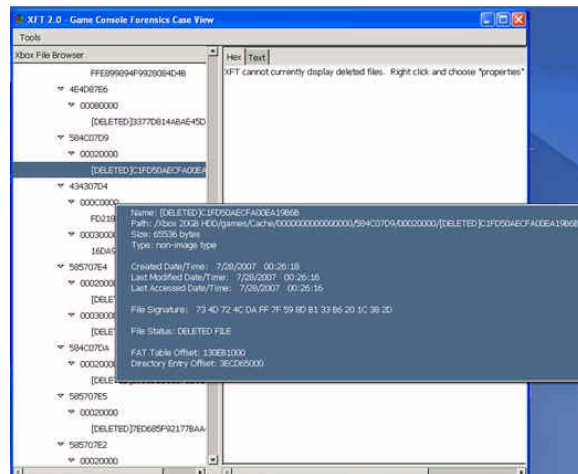
Image 12 – Viewing the properties of a deleted file in XFT

Other information discovered with XFT 2.0 included user names (Image 13) and the user's player list containing the gamer tags of other Xbox 360 players. (Image 14) This finding is extremely significant because it can not only aid law enforcement seeking to establish a connection between users, but it can also pose a risk to anyone who has been in contact with a user whose system has been compromised. Gamer tags can be searched through any number of gamer databases or social networking sites to gain additional information about a player.
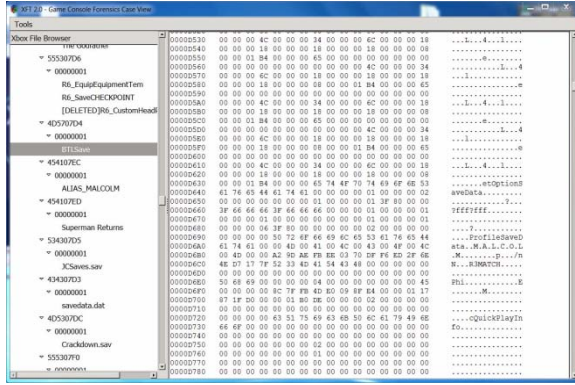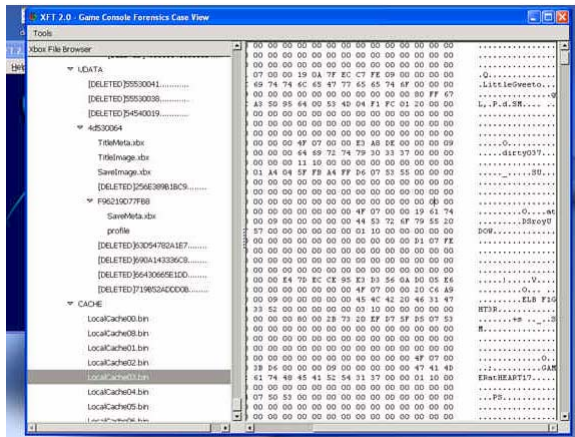
Image 13 – User name viewed in XFT

Image 14 – Cache showing a player's list in XFT

While XFT does not enable users to read larger files such as databases, it does enable the option to export the data. In one example, we exported the marketplace database for closer examination using notepad. After a quick look through the file, we came to the text "Purchase History Items", and decided to take a closer look in DFF. Once in DFF, strings of text in German, Italian, and French were discovered. (Table 2) (Image 15)

Item	Language	Information
per maggiori informazion**.**	Italian	for greater information
ore dopo aver selezionato	Italian	hours after to have selected
inhalt ist zur zeit nicht	German	contents are at present not
dejouer les	French	to thwart them

Table 2 – Example of foreign languages found in marketplace.dat file

Because Xbox 360 is an international platform, one might expect to see multiple languages in the marketplace data file. However, it presents forensic examiners with another challenge and should be kept in mind when examining the contents of the drive.
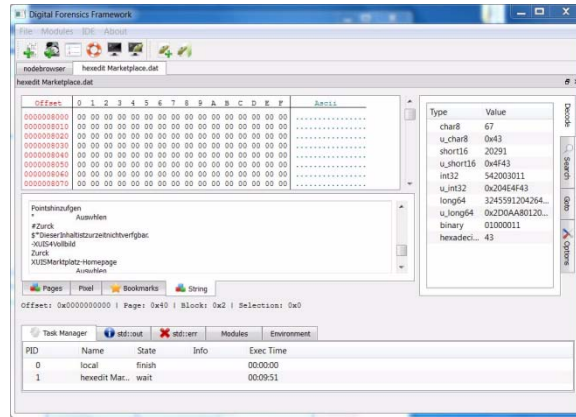
184

Image 15 – Marketplace database in DFF

Although XFT was designed specifically to examine Xbox 360 drives, we were unable to acquire the drive through the program without first extracting the data using DrDD. While the drives were tested both before and after acquisition, it is problematic at best to claim with any certainly that the extracted data was not altered during the extraction because we were transferring FATX data using tools, which even if tested and given a green light by NIST, were not designed to acquire or examine FATX files. This can create quite a quagmire when working within a legal framework. One feature of XFT which addresses this dilemma is its ability to keep an electronic "chain of custody" of the data being examined. Each time data is accessed through the program, it is logged in a file until the case is manually is closed. (Images 16 and 17)
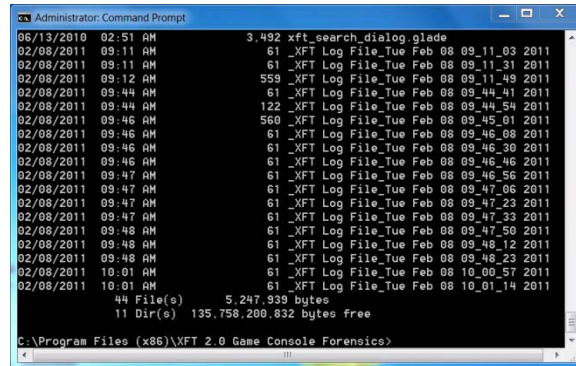

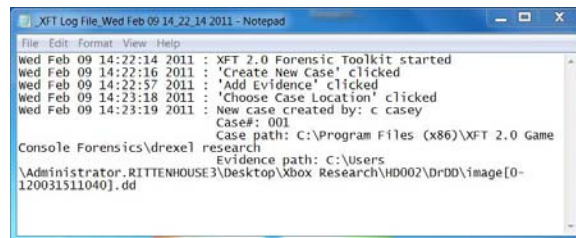*Image 16 – XFT access log as viewed in DOS*

Image 17 – Example of an XFT access log

Up until this point, we looked exclusively at Windows based tools. However, when examining an Xbox 360 drive, investigators can also obtain valuable information using Linux. Upon initial assessment, examiners can try to boot the console with Linux to determine if the system has been modified. Drives mounted to a computer running Linux (or machines booted with a Linux CD or bootable USB) can be searched using common Linux commands such as grep to look for files, or a

defined string of text. The abundance of gamer sites and forums dedicated to Xbox 360 modding with Linux may also prove a valuable resource. If the budget is available, an analysis workstation can be built and dedicated to examining Xbox 360 drives. It is recommended however that the hardware of the machine being deployed for this workstation is compatible with the latest Linux kernel (2.6). (Paul K. Burkea P. C., 2006) During our research, we encountered repeated kernel errors while trying to examine the test drives in Linux.

5. CONCLUSION

Although many of the tools tested discovered the same or identical data, there was no single tool adept enough to perform the task independently. Furthermore, with the exception of XFT, evidence obtained from these tools may not necessarily be admissible in a court of law.

It is no longer feasible to examine devices such as gaming consoles, smart phones, and iPods using *"electronic ethnocentricity"*. Using computers to measure where data is, and how it should be structured or stored, will simply no longer suffice. As devices evolve, so must the examiner's methodologies. Technology has passed the age where we can use one or two tools, and by pushing a few buttons, have all of our evidence appear before our eyes and arranged automatically into neat little reports. This is not to suggest that program developers should not continue to create software to address these new needs, but rather that digital investigators may need to think outside the "box" when examining devices like gaming consoles.

By looking at a small sampling of drives using multiple tools and operating systems, we were slowly able to begin constructing a model of the Xbox 360 gaming console structure. While this was just a sampling of Microsoft's Xbox 360 architecture, it enabled us to find two user names, city, a user profile, a cache containing a player's list, and a credit card number. When we reference the seller address from eBay we are able to have a name, address, and credit card number; a complete identity. If the investigators had stuck exclusively to conventional techniques, or tools designed to acquire data from computer hard drives, they would have missed some of this data.

Given the increase of crimes using gaming consoles such as the Xbox 360, there needs to be more research conducted to help determine appropriate tools and approaches for forensically sound data identification and acquisition.

6. FUTURE WORK

Future work includes testing additional tools to determine the best acquisition method for gaming consoles, specifically the Xbox 360. Furthermore, the researchers aim to establish and verify date/time stamps on Xbox 360 data. For example, the researchers were able to recover "buddy lists," and if you are able to cross reference actions with the "buddy lists" and data/time stamps you would be able to build activity and communication timelines. This would be extremely helpful in criminal cases such as child exploitation, fraud or other criminal activities.

The researchers will also continue to work on developing best acquisition methods for emerging, non-traditional devices such as smart phones and other internet capable devices.

7. ABOUT THE AUTHORS

Dr. Podhradsky is an Assistant Professor of Computing and Security Technology at Drexel University. Dr. D'Ovidio is a Professor of Criminal Justice at Drexel University, and Cindy Casey is a student in the Computing and Security Technology program at Drexel University.

8. REFERENCES:

Becker, D. (2001, 1 6). *Microsoft got game: Xbox 360 unveiled*. Retrieved 11 17, 2010, from CNET News :
http://news.cnet.com/Microsoft-got-game-Xbox 360-unveiled/2100-1040_3-
250632.html?tag=untagged

Berardini, C. (2005, 12 5). *The Xbox 360 360 System Specifications* . Retrieved 11 17, 2010, from Team Xbox 360: http://hardware.teamXbox 360.com/articles/Xbox 360/1144/The-Xbox 360-360-System-Specifications/p1

Billo, J. (2007, 1 23). *Xbox 360 360 dashboard update and efuses* . Retrieved 1 22, 2011, from Jake Billo's weblog: http://jakebillo.com/Xbox 360-360-dashboard-update-and-efuses

BinBD. (2011). *Bin Checker*. Retrieved 2 7, 2011, from Bin Database Search - Bin Checker: http://www.bindb.com/bin-database.html

Bloomberg Businessweek. (2010, 3 11). *Microsoft's Xbox 360 Sales Beat Wii, PS3 in February on "BioShock"*. Retrieved 11 17, 2010, from Bloomsberg.com:
http://www.businessweek.com/news/2010-03-11/microsoft-s-Xbox   360-sales-beat-wii-ps3-in-february-on-bioshock-.html

Bolt, S. (2011). *Xbox 360 360 Forensics; A Digital Foresnics Guide to Examining Artifacts.* Burlington : Syngress.

Bungie. (2011, 2 4). *Halo*. Retrieved 2 7, 2011, from Bungie.net: http://www.bungiestore.com/

Bullock, H. (2009, 2 6). *Accused Sexual Predator Edward Stout Met Victim Through Xbox*. Retrieved 2 18, 2011, from KSFN-TV: http://abclocal.go.com/kfsn/story?section=news/local&id=6643907

Bush, E. (2008, 10 24). *Virginia Man Arrested for Child Pornography over Xbox Live*. Retrieved 2, 18, 2011, from Planet Xbox 360:
http://www.planetxbox360.com/article_5559/Virginia_Man_Arrested_for_Child_Pornography_o

Carmody, T. (2010, 11 3). *How Motion Detection Works in Xbox 360 Kinect*. Retrieved 11 17, 2010, from Wired: http://www.wired.com/gadgetlab/2010/11/tonights-release-Xbox 360-kinect-how-does-it-work/all/1

Cavalli, E. (2009, 3 17). *Animal Crossing is Pedophile Haven*. Retrieved 2 18, 2011, from Wired: http://www.wired.com/gamelife/2009/03/missouri-police/

Computer Gyaan. (2010, 11 2). *Disk formatting and Data recovery*. Retrieved 1 14, 2011, from Computer Gyaan:
http://www.muamat.com/classifieds/174/events/2010-12-
30/11663_Disk_formatting_and_Data_recovery.html

craigslist. (2010). *Offical Site*. Retrieved 12 23, 2010, from craigslist: http://www.craigslist.org

Constantin, L. (2010, 10 19). *Phishers Target Xbox Players Via Fake Gamertag Changer*. Retrieved 2 18, 2011, from Softpedia: http://news.softpedia.com/news/Phishers-Target-Xbox-Players-via-Fake-Gamertag-Changer-161812.shtml

Criminal Intelligence Service Canada (2007). *Integrated Threat Assessment Methodology*.

Ottowa, Ontario: Criminal Intelligence Service Canada.

Deleon, N. (2008, 8 5). *Be Careful, There's a Phishing Scam Going Around Xbox Live*. Retrieved 2 18, 2011, from CrunchGear: http://www.crunchgear.com/2008/08/05/be-careful-theres-a-phishing-scam-going-around-xbox-live/

Ebay. (2010). *Xbox 360 Console Listings*. Retrieved 11 30, 2010, from Ebay Online Auction : http://video-games.shop.ebay.com/Systems-/139971/i.html?_nkw=Xbox 360+console&_catref=1&_fln=1&_trksid=p3286.c0.m282

Evers, J. (2007, 3 20). *Microsoft Probes Possible Xbox Live Fraud*. Retrieved 2 16, 2011, from CNet News: http://news.cnet.com/2100-7349_3-6169060.html

FBI. (2011). *Child Victim Identification Program (CVIP)*. Retrieved 2 8, 2011, from Department of Justice/Federal Bureau of Investigation: http://foia.fbi.gov/cvip.htm

Federal Trade Commission . (2007). *2006 Identity Theft Survey Report.* McLean: Synovate.

Free60 Project. (2009, 8 11). *849x System Update*. Retrieved 1 4, 2011, from Free60 Project Achieves: http://free60.org/old/849x_System_Update.html

Fried, I. (2005, 5 25). *Microsoft Plugs Phishing Hole in Xbox Site*. Retrieved 2 18 2011, from CNet News: http://news.cnet.com/Microsoft-plugs-phishing-hole-in-Xbox-site/2100-1029_3-5720241.html

Fujji, M. (2010, 4 15). *Man Arrested for Intimidating Witness Over Xbox Live*. Retrieved 2 18, 2011, from College News: http://www.collegenews.com/index.php?/article/witness_intimidated_over_xbox_live_041520101235235/

Harris, M. (2009, 1 23). *Online Games Open Door to ID Theft*. Retrieved 2 17, 2011, from Tech Radar: http://www.techradar.com/news/internet/online-games-open-door-to-id-theft-610380

Hill, C. (2009, 1 29). *Teenage Boy Accused of Repeatedly Raping 12-Year Old He Met on Xbox Live*. Retrieved 2 18, 2011, from NY Daily News: http://www.nydailynews.com/money/2009/01/29/2009-01-29_teenage_boy_accused_of_repeatedly_raping.html

Hitt, B. (2011, 1 8). *Women Raped Boy, 13, She Met Playing Xbox Online*. Retrieved 2 19, 2011, from KTLA: http://www.ktla.com/news/landing/ktla-xbox-mom-rape,0,2120242.story

Huang, A. ". (2001, 5 26). *Keeping Secrets in Hardware: the Microsoft Xbox 360 Case Study.* Retrieved 1 7, 2011, from Massachusetts Institute of Technology - Artificial Intelligence Laboratory: http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf

Javelin Strategy and Research. (2010, 10 2). *2010 Identity Fraud Survey Report: Identity Fraud Continues to Rise.* Retrieved 11 16, 2010, from Javelin Strategy and Research Library: https://www.javelinstrategy.com/research/brochures/Brochure-170

Lemos, R. (2007, 3 23). *Account Pretexters Plague Xbox Live*. Retrieved 2 18, 2011, from The Register: http://www.theregister.co.uk/2007/03/23/xbox_live_pretexting/

McHugh, M. (2011, 2 4). *Pirated Microsoft Software Funded Mexican Drug Cartel*. Retrived 2 18, 2011, from Digital Trends: http://www.digitaltrends.com/computing/pirated-microsoft-software-funded-mexican-drug-cartel/

McMillan, R. (2011 2 14). *Spanish Police Arrest Alleged Nintendo Hacker*. Retrieved 2 18, 2011, from PCWorld: http://www.pcworld.com/businesscenter/article/219598/spanish_police_arrest_alleged_nintendo_hacker.html

Microsoft . (2010, 10 20). *Article ID: 906502 - How to format an Xbox 360 360 Hard Drive or Memory Unit*. Retrieved 12 23, 2010, from Microsoft Support : http://support.microsoft.com/kb/906502

Microsoft. (2005). *.exp Files as Linker Input*. Retrieved 1 5, 2011, from MSDN Library, Link Input Files: http://msdn.microsoft.com/en-us/library/se8y7dcs(v=vs.80).aspx

Microsoft. (2010, 10 20). *How to format an Xbox 360 360 Hard Drive or Memory Unit*. Retrieved 11 30, 2010, from Microsoft Support Search Microsoft SupportSearch Microsoft.comSearch the web : http://support.microsoft.com/kb/906502

Microsoft. (2010, 10). *Xbox 360 LIVE and Games for Windows LIVE Terms of Use*. Retrieved 1 12, 2011, from Microsoft Xbox 360: http://www.Xbox 360.com/en-US/Legal/livetou

Netflix. (2011). *How does Netflix work?* Retrieved 2 7, 2011, from NetFlix: http://www.netflix.com/Default?mqso=80012928

OAI Networks. (2011). *Strict, Moderate, and Open NAT - Load balancing Xbox 360 Game Servers* . Retrieved 2 7, 2011, from Tech Tips: http://www.cainetworks.com/support/how-to-NAT-strict-open.html

Official Xbox 360 Magazine staff . (2005, 12 13). *The Complete Hisotry of Xbox 360*. Retrieved 11 17, 2010, from CVG Gaming : http://www.computerandvideogames.com/article.php?id=131066

Paul K. Burkea, P. C. (2006). *Xbox 360 Forensics.* Retrieved 11 18, 2010, from Journal of Digital Forensic Practice: http://dx.doi.org/10.1080/15567280701417991

Paul K. Burkea, P. C. (2006). *Xbox 360 Forensics.* Retrieved 2 9, 2011, from Journal of Digital Forensic Practice, Volume 1, Issue 4 December 2006 , pages 275 - 282 : http://www.informaworld.com/smpp/section?content=a779635437&fulltext=713240928

Peterson, D. (2010, 8 30). *Former Walt Disnet World Employee Arrested on Xbox Child Porn Charges*. Retrieved 2 17, 2011, from Examiner: http://www.examiner.com/disney-travel-in-national/former-walt-disney-world-employee-arrested-on-xbox-child-porn-charges

Potter, N. (2009, 3 13). *PlayStation Sex Crime: Criminal Used Video Game to Get Girl's Naked Pictures*. Retrieved 2 18, 2011, from ABC News: http://abcnews.go.com/print?id=7009977

Protowise Labs. (2011). *XFT 2.0 Game Console Forensics is Released*. Retrieved 2 8, 2011, from XFT 2.0 Game Console: http://protowise.com/?tag=xft-Xbox 360-forensics

Rivington, J. (2007, 8 20). *Wii and PS3 Vulnerable to Hacks and Phishing*. Retrieved 2 18 2011, from Tech Radar: http://www.techradar.com/news/gaming/consoles/wii-and-ps3-vulnerable-to-hacks-and-phishing-161313

Snow, B. (2009, 12 13). *Gamer Arrested for Shooting Threats on Xbox Live*. Retrieved 2 18, 2011, from GamePro: http://www.gamepro.com/article/news/152848/gamer-arrested-for-shooting-threats-on-xbox-live/

Team Xbox 360. (2005, 9 8). *Xbox 360 Live Facts 'n Stats.* Retrieved 11 30, 2010, from Team Xbox 360: http://news.teamXbox 360.com/Xbox 360/9194/Xbox 360-Live-Facts-n-Stats/

Technology Pathways. (2011). *ProDiscover Demo Download*. Retrieved 2 7, 2011, from Technology Pathways: http://www.techpathways.com/Demo.htm

The President's Identity Theft Task Force. (2007). *Combating Identity Theft: A Strategic Plan.* Washington: U.S. Government.

University of Michigan. (2008, 6 20). *Tools for Discovering Credit Card and Social Security.* Retrieved 2 7, 2011, from Information Technology Security Services : http://www.safecomputing.umich.edu/tools/download/ccn-ssn_discovery_tools.pdf

Weinstein, N. (2009, 3 14). *Man Charged with Alleged Child Porn Via PS3*. Retrieved 2 18, 2011, from CNet News: http://news.cnet.com/8301-10797_3-10196553-235.html

Wells, E. C. (2008, 1). *Sustaining Gen Y's Interests*. Retrieved 11 30, 2010, from Today's Garden Center: http://www.todaysgardencenter.com/trends/sustainability/?storyid=340

World Lingo . (2010). *Comparison of file systems* . Retrieved 11 18, 2010, from World Lingo : http://www.worldlingo.com/ma/enwiki/en/Comparison_of_file_systems

9. BIBLIOGRAPHY

DataRescue. (2010). Retrieved 2011, from DrDD- DataRescue's DD freeware: http://www.datarescue.com/photorescue/v3/drdd.htm

Digital Forensics Framework. (2009). Retrieved 2010, from Digital Forensics: http://www.digital-forensic.org/digital-forensics-framework/community/

EnCase. (2011). Retrieved 2011, from Guidance Software: http://www.guidancesoftware.com/

Hex Editor XVI32. (2009). Retrieved 2001, from Freeware Hex Editor XVI32: http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

Modio. (2010). Retrieved 2011, from Game-Tuts: http://www.game-tuts.com/community/index.php?pageid=modio

Prodiscover. (2010). Retrieved 2011, from Technology Pathways: http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14

wxPirs . (2010). Retrieved 2011, from Xbox-Scene : http://www.xbox-scene.com/xbox360-tools/wxPirs.php

Xbox-Scene. (2009). Retrieved 2011, from Xbox 360 PC Tools: http://www.xbox-scene.com/xbox360-tools/xplorer360.php

XFT 2.0 Game Console Toolkit Released. (2009). Retrieved 2011, from Video Game Device Forensics: http://consoleforensics.com/xft-2-0-game-console-toolkit-released/