Identity Theft and Used Gaming Consoles: Recovering Personal Information from Xbox 360 Hard Drives

Dr. Asley L. Podhradsky  
Drexel University

Dr. Rob D'Ovidio  
Drexel University

Cindy Casey  
Drexel University

Follow this and additional works at: http://aisel.aisnet.org/amcis2011_submissions

Recommended Citation
Podhradsky, Dr. Asley L.; D'Ovidio, Dr. Rob; and Casey, Cindy, "Identity Theft and Used Gaming Consoles: Recovering Personal Information from Xbox 360 Hard Drives" (2011). AMCIS 2011 Proceedings - All Submissions. 54.
http://aisel.aisnet.org/amcis2011_submissions/54

This material is brought to you by AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2011 Proceedings - All Submissions by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Identity Theft and Used Gaming Consoles: Recovering Personal Information from Xbox 360 Hard Drives

Dr. Ashley L. Podhradsky, Drexel University
Dr. Rob D’Ovidio, Drexel University
Cindy Casey, Drexel University

Keywords: Digital Forensics, Identity Theft, Xbox Gaming Console, Data Sanitization

Abstract
Traditionally, when individuals wanted online access they connected their PCs to the internet. Now, non-traditional devices such as cell phones, smart phones, and gaming consoles serve as common means of online access. Gaming consoles, just like PCs need proper sanitization processes to help fight identity theft. Individuals understand you cannot simply throw away a computer that has your personal data on it without some sort of sanitization process; gaming consoles are no different. Simply returning your console back to “factory state” will not do the trick, you need to take things one step further.

In this research paper the authors aim to bring awareness to the gaming public, researchers and practitioners that improperly discarding used consoles without proper sanitization practices can inadvertently release personal data which can result in identity theft. The researchers will demonstrate through a case study how easy it is to steal an identity through a discarded Xbox. Finally, the researchers will demonstrate how gamers can sanitize their game consoles when upgrading their systems to ensure their identity is not at risk when the used device is retired.

1. Introduction
Identity theft occurs when an individual’s personal data is obtained and fraudulently used by another, typically for monetary profit [1]. With as little as a person’s name, social security number, or date of birth, a thief can cause major damage [1]. Although the most common type of identity theft is credit card theft, stolen identities can be used for immigration, tax, medical, residential, and social security fraud to name a few [2]. As reported by the President’s Identity Theft Task Force, what makes identity crime so successful and lucrative is that the victims typically do not know they have been victimized until late into the life cycle of the theft [2]. By the time a victim finds out his identity has been stolen, usually via a bad credit report or a rejected credit application, the thief has already enjoyed the spoils of his crime and has moved on to the next victim [2].

In their 2010 Identity Theft Report, Javelin Strategies, a research firm that analyzes trends in identity theft, revealed that identity theft increased a staggering 11% percent between 2008 and 2009 [3]. According to the Federal Trade Commission’s most recent survey, approximately one out of every four Americans is at risk of being victimized
each year. With an identity stolen every three seconds in the United States, fraud has reached epidemic proportions [4]. It is important to note that these numbers do not include those who do not report, or are not even aware, that they have had their identities stolen. Therefore, the researches hypnotize this staggering statistic to be even higher.

Due to their tendency to engage in riskier activities such as sharing computers, utilizing unprotected wireless access points, and uploading videos, younger adults tend to be the most vulnerable of the populace. However, securing computers and advocating online safety are not the only countermeasures that can curtail these escalating statistics. Personal data used in identity theft can be obtained through a multiplicity of means, many of which are not even considered by the general public as posing a potential threat.

In addition to computers, other devices such as cell phones, smart phones and gaming systems also store copious amounts of personal or confidential data. Most individuals do not realize when using these devices that their personal information is being copied and stored. Even when the device is considered data-free using conventionally practiced sanitation methods such as erasing or over-writing the hard drive, sensitive data can still be retrieved [5]. Any device over which personal information is sent or stored and then is not sanitized correctly creates the perfect storm for identity theft. Instead of going through the trouble of hacking into someone’s Bluetooth device or peering over the shoulder of a laptop in public – the criminal merely has to purchase a used gaming system at an online auction site, and the identity comes to him.

The researchers acquired three used gaming consoles for the purpose of this paper and research. Two consoles were purchased from eBay and a popular online classified forum, and one was retrieved after being discarded.

2. Xbox Gaming Console

While personal data can be extracted from Sony’s PS3 and Nintendo’s Wii gaming systems, Microsoft’s Xbox is the most popular among American consumers, selling over thirty-nine million consoles, six million more than their top competitor, the PS3 [6]. When Bill Gates first announced his plans for the Xbox 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 [7].” These critics proved to be correct.

The Xbox console is not only similar to a personal computer - it is actually more powerful than the average personal computer. The hardware and technical specifications found in today’s Xbox 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 [8].

The file data format used in Xbox is the FATX which is an offshoot of the more
familiar FAT32 found on computers and flash media [9]. 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 [10]. The reasoning behind these variations in file formatting is that the Xbox was designed primarily for entertainment as opposed to productivity. Thus, redundancy and legacy are apparently forfeited in order to increase the system’s speed [33].

Some of the personal data which can potentially be retrieved from consoles include, but are not limited to the following:

- User’s name
- Address
- Telephone number
- Credit card information
- Personal chat logs
- Personal blog records

Credit cards are used to purchase games through the Live Arcade, pay for Xbox Live membership, and buy merchandise such as gamer icons and console themes at Xbox’s Live Marketplace. One popular movie subscription service, Netflix, even permits its members to rent movies using credit cards directly though their Xbox consoles [20]. Other personal information is used to create profiles, chat, and blog. In fact, the Xbox is even capable of keeping a gamers’ blog for the user by monitoring the account and automatically generating blog entries about their daily activities. However, as is true with any technology, these advancements also create more vulnerabilities.

Recently Microsoft released the Kinect motion-sensing peripheral for Xbox 360. Kinect relies on biometrics, thus enabling players to turn on their console with a wave of the hand or palm scan [11]. With body movements and voice recognition, users can control their characters in the game. If trying to reestablish credit and other finances destroyed due identity theft is not complex enough, imagine how difficult it may be to recover a palm, fingerprint, or even a retina scan. While this may sound like something out of a science fiction novel, it is not that implausible.

With the emergence of the Kinect gaming bundle, more users will be selling or trading their current consoles either because they are outmoded or to financially offset the cost of acquiring a newer system. In addition to selling the system in its entirety, some users may elect to sell or swap the hard drive independent of the console. Oftentimes, after acquiring numerous games, storing countless television shows, or amassing a plethora of other data, the user may seek to change a drive out of necessity because a larger drive is required.

Not all Xbox consoles are sold for profit or to upgrade to a better system. According to demographics, the majority of Xbox users are young males between the ages of eighteen and thirty [12]. These statistics correlate with the medium age of Americans who embrace or practice green living [13,14]. Thus, a considerable number of Xbox users may choose to recycle their gaming systems and its components in lieu of destroying them or tossing them into a landfill.
A quick look on eBay provides a small snapshot of how many systems are sold daily. At the date of this study, there were over 1,500 Xbox gaming systems for sale in the United States alone [15]. It is relative to note that these listings are subject to change by the minute and do not include Xbox hard drives being sold devoid of a console.

Thus, the probability that more Xbox devices will fall into the hands of unscrupulous individuals can be expected to increase in light of the following occurrences:

- Emergence of newer (next generation) gaming consoles and bundles
- More users seeking to offset gaming costs due to the recession
- Increasing conservation awareness and recycling efforts
- Gaining popularity of cloud gaming

Typically, when an individual decides to sell or trade their Xbox console or hard drive they delete, or erase their personal data and history believing the information is permanently gone. However, this common practice does not remove data from the console at all, it merely alters it [5]. When data is deleted, it is not really erased; in fact, it is not even necessarily moved. In most cases, the information or file stays exactly where it was. What changes is the path and filename of the data known as the directory entry. The first letter of the file is modified and marked with a character indicating it is available to be rewritten. There it will stay intact until new data is written over the existing data (overwriting).

More savvy Xbox users may opt to reformat the console’s hard drive in order to destroy sensitive information. Theoretically, when an Xbox drive is reformatted, every available block of space is filled with zeros, or ASCII NUL bytes (0x00). Successfully overwriting a drive is not only contingent upon both the logical and physical condition of the drive, but the methodology utilized as well. It would be problematic at best to say, with any degree of certainty, that all information can be eradicated.

According to Microsoft’s Online Xbox Support tutorials, once the Xbox console is reformatted, “…all of the information saved on that device is erased and cannot be recovered [16].” This information was reiterated by Microsoft via email after we contacted Xbox’s customer support inquiring how to securely and permanently remove personal data from the system. One of the objectives of this project is to ascertain exactly how accurate this consumer directed information actually is.

3. The Investigation

Two Xbox gaming consoles were purchased randomly from an online auction site and a popular classified forum respectively. An additional hard drive was retrieved after being discarded by the original user. Once removed from the consoles (if applicable), the drives were extracted using T10 and T4 Torx wrenches. To preserve objectivity, each drive was randomly numbered (001 through 003). It is relevant to note, that when purchasing used gaming systems from online auction sites, identity thieves have somewhat of an advantage – the seller’s name and mailing address appears right on the package when it arrives. Likewise, if acquired from a classified forum such as craigslist [17]
unscrupulous individuals can amass the seller’s name, telephone number or email address, and various other tidbits of information by way of social engineering.

A variety of tools were utilized to examine the drives. The reasoning for this 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. Some of the software used to examine the Xbox drives included, but was not limited to:

- **XPlored360** - Freeware tool that allows access to all discoverable Xbox partitions and memory cards. XPlored360 allows access to both physical and logical areas of the drive [18]
- **FTK 3.0** - Forensic Toolkit (FTK), produced by AccessData is a commercial suite of applications for forensic analysis of digital media, including Xbox consoles [19]
- **FTK Imager** - Freeware tool from AccessData which allows users to forensically image and analyze drives [20]
- **Modio** - Freeware modding tool that allows Xbox users to open their system to allow for customized use of their console [21]
- **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 [22]
- **ProDiscover Basic** - Freeware tool based on the commercial ProDiscover allows viewing of each sector to determine data storage locations [23]
- **Digital Forensic Framework (DFF)** - Is an open source tool that aids in the collection and analysis of digital evidence [24]
- **Hex Editor XV132** – Freeware hex editing tool that runs in memory and doesn’t need to be installed on the host system, incorporates a built in hex to string, and allows bookmarks [25]
- **XFT 2.0** - Commercial Xbox toolkit developed by Protowise Labs that allows for access to configuration, modification, and user files, included recovering deleted files [26]
- **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 [27]
- **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 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 [28].

In a recent effort to discourage console modifications, Microsoft released an Xbox360 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 Xbox360 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 [29]. 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.

Since the Xbox 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’s structure that the Xbox contains a “secret boot block [30]”. 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 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, as indicated in image 1.

Modio is a modding utility that allows Xbox 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, as demonstrated in 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.

The hard drives were accessed using a USB 2.0 to SATA adaptor with a 50/60 Hz power supply cable. 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. 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 does share some similarities with a PC, it cannot truly be measured using the same criteria [31].

**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 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 drive found that Partition 0 was an empty partition [32], our analysis found two drives that did exhibit files on Partition 0, as demonstrated

*Image 2- Viewing files in Modio*
in image 3. This empty partition was initially attributed to the extra file mentioned earlier on Partition 3, Xbox1 (Partition 3\Compatibility\Xbox1), 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 Xbox1 folder. The drive which did not contain viewable data in Partition 0 was the newest of the three drives as ascertained from sector 4 (7-02-09). 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.

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 EXplorer360, 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\4D5 707D4\00000001\BTL save, and last modified on 8/28/2007, as demonstrated in Image 4. Other personal data obtained from the same drive included a user’s first name and a partial or abbreviated city name.

Image 3 - Partition 0, Viewed in EXplorer360 showing a JA folder and an aoA file

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, as demonstrated in 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 Xbox360 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 [16]. This particular system update was found on all three of the hard drives, as demonstrated in Image 6.

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

These particular system update files were identified as belonging to an update released by Microsoft in January 2007 [34]. 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 of 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 neither ProDiscover Basic nor DFF were useful for drive acquisition, once the drives were extracted using DataRescue’s DD (DrDD), they were 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-Microsoft proprietary programming code. 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.

<table>
<thead>
<tr>
<th>Drive</th>
<th>Name</th>
<th>Digits</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>JOSH</td>
<td>97-001</td>
<td>03-19-07</td>
</tr>
<tr>
<td>002</td>
<td>JOSH</td>
<td>49-001</td>
<td>07-02-09</td>
</tr>
<tr>
<td>003</td>
<td>JOSH</td>
<td>78-001</td>
<td>08-07-08</td>
</tr>
</tbody>
</table>

Table 1 – Sector 4 data found
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 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, as demonstrated in Image 8.

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 (i.e.: UDP 5060 and weak SIP or Brute Force Attack) of which the user is not informed 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.

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) [27]. Performing a fast scan on one of the drives resulted in a possible credit card hit as demonstrated in 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 [37].

![Image 10 – EnCase credit card hit](image10.png)

Utilizing a new tool, XFT 2.0, developed by David Collins, a computer scientist at Sam Houston State University and distributed by Protowise Labs, (Protowise Labs, 2011), files which were deleted on the drives were discovered however, the file’s contents were not retrievable.

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. Because Xbox is an international platform, one might expect to see multiple languages in the marketplace data file. The real red flag here is that while we could not locate the boot loader in or around the partition one would expect to find it, we were able to locate the user’s purchase history where we would expect to – in the marketplace. This suggests that the system information is more secure than the user’s personal data.
Of equal significance is that while Microsoft’s proprietary files and databases were encrypted, multiple instances of user data was in plain text. This practice is apparently not exclusive to Microsoft. In a recent class action suit filed against Sony Computer Entertainment America LLC, in response to the much publicized PS3 Security breach of April 2011, SONY allegedly failed to encrypt user data. This unencrypted information included, but was not limited to, credit card data, names, birth dates, and passwords of a staggering 77 million console users [40].

While the researchers acknowledge that the average thief may not utilize all of the tools or methodologies performed in this project, it doesn’t take all of the information we discovered to steal someone’s identity. Through social engineering and the internet, a thief can construct a full profile of their victim rather easily. Additionally, the majority of the information discovered can be found using open-source tools readily available for download on the internet.

4. Steps Consumers Should Take

When consumers sell or dispose of their used Xbox 360’s they need to take more steps than simply returning the device back to “factory settings.” During this project researchers were able to recover personal identifying information from an Xbox 360 that had in fact been returned back to the original “factory setting.” The original eBay posting coupled with investigative tools such as ProDiscover, showed the media was indeed written with 0’s. However, it is the opinion of the researchers that not all of the partitions are overwritten during the factory setting process.

When consumers are upgrading to a new Xbox and need to sanitize their old device, it is the opinion of the researchers that users should physically remove the HD from the console (as indicated in section 2), and run a software sanitizer on the drive.

There are several options available for both open source and commercial data sanitization tools. Table 2, Open Source and Commercial Sanitization Tools, highlights popular sanitization tools.

When selecting a tool, the authors note it is important to select a tool that emphasizes patterns in write fill in addition to passes. This is imperative to making sure that slack and unallocated space is overwritten.

Book and Nuke, by DBAN is a free tool downloadable online. The researchers tested Boot and Nuke by sanitizing a drive with the tool then attempted to recover residual data. The drive was searched and forensically analyzed, however no residual data could be recovered. The process included acquiring a new drive, forensically imaging the drive with FTK Imager, acquiring an MD5 and SHA-1 hash, placing data on the drive,
running Boot and Nuke on the drive, forensically imaging with FTK imager, and obtaining a final hash. The hash files were the same and no data was found, therefore the researchers can infer that the drives are indeed sanitized [8].

Given the simple process of using Book and Nuke, the researches pose the question why there is not better sanitization process in any of the key industries studied with the DFDR study?

<table>
<thead>
<tr>
<th>Tool</th>
<th>Price</th>
<th>Platform</th>
<th>Where to Find the Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Darik’s Boot &amp; Nuke</td>
<td>Free</td>
<td>Unix/Linux, Mac, Windows</td>
<td>Tool can be found at <a href="http://www.dband.sourceforge.net">http://www.dband.sourceforge.net</a></td>
</tr>
<tr>
<td>SecureClean</td>
<td>$39.95</td>
<td>Windows</td>
<td>Tool can be found at <a href="http://www.whitecanyon.com/secureclean-clean-hard-drive.php">http://www.whitecanyon.com/secureclean-clean-hard-drive.php</a></td>
</tr>
<tr>
<td>Erase</td>
<td>Free</td>
<td>Windows</td>
<td>Tool can be found at <a href="http://eraser.heidi.ie/">http://eraser.heidi.ie/</a></td>
</tr>
<tr>
<td>Wipe</td>
<td>Free</td>
<td>Unix</td>
<td>Tool can be found at <a href="http://www.wipe.sourceforge.net">http://www.wipe.sourceforge.net</a></td>
</tr>
</tbody>
</table>

Table 2: Available Sanitization Tools
5. Conclusion

Identity theft is a very serious problem that every year continues to surpass the previous year’s record. Each year more individuals have their identity stolen, most through emerging techniques. Five years from now, identities will be stolen on devices and technology that do not yet exist. Given the increased use of technology and digital records, and the introduction of more non-traditional devices such as the Xbox gaming console that hosts personal identifying information, individuals have a multitude of devices that house their data.

Consumers have to be extremely vigilant when it comes to their own data. Relying on 3rd parties to protect their personal information is not recommended.

The researchers found that Microsoft protected their proprietary system files well; however, they did not do a sufficient job in protecting their customer’s data. Consumers need to be diligent about protecting their own data, and not assume their technology is going to do it for them. Section 4 highlighted tools and approaches consumers should take when discarding any used device, especially an Xbox 360. Data Sanitization is even more pressing when the device is sold to another consumer. Returning your Xbox back to factory settings is only effective for the Xbox and Microsoft proprietary data, not the user data.

Future work will include analyzing the Microsoft Xbox Kinect motion system.

6. 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.
7. References:


