

available at www.sciencedirect.comDigital
Investigationjournal homepage: www.elsevier.com/locate/diin

Xbox 360: A digital forensic investigation of the hard disk drive

Konstantinos Xynos*, Simon Harries, Iain Sutherland, Gareth Davies, Andrew Blyth

University of Glamorgan, Faculty of Advanced Technology, Pontypridd CF371DL, United Kingdom

ARTICLE INFO

Article history:

Received 16 December 2009

Received in revised form

15 February 2010

Accepted 16 February 2010

Keywords index:

Digital Forensics

Hard Disk Drive

Microsoft Xbox 360

Residual Data

Games

ABSTRACT

In recent years an increase in the complexity of games has subsequently demanded an upscale of the hardware in the consoles required to run them. It is not uncommon for games consoles to now feature many pieces of hardware similar to those found in a standard personal computer.

In terms of forensics the most significant inclusion in today's games consoles is the storage media, whether they are flash based memory cards, or electro-mechanical hard disk drives. When combined with networks, particularly the internet, this inbuilt storage gives games consoles a host of new features, including the downloading of games, updating of console software/firmware, streaming media from different network locations, activities centred around social networking and usually involving user specific content being saved on the consoles storage media.

This paper will look at analyzing the SATA hard disk drive contained in Microsoft's Xbox 360 games console. We present our findings and provide suggested basic guidelines for future investigations to be able to recover stored remnants of information from the drive.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

The increased complexity of games over recent years has resulted in games consoles now containing more advanced sophisticated hardware. Multiple CPUs and high-end graphic cards are just a few basic requirements. These systems still rely on some form of local storage media, be that flash based or hard disk drive based. From a digital forensics perspective these storage devices can contain an amount of information that could prove useful in digital investigations.

Additional functionality in newer consoles includes the ability to install and run other operating systems (OS) alongside the native host OS, connect to networks, in particular the

Internet and in combination with the inbuilt storage this gives games consoles a whole host of new capabilities, including the downloading of games, updating console software/firmware and streaming media from different network locations. This functionality is ever increasing as manufactures produce many hardware add-ons for these systems such as cameras with the ability to take and view photos and record digital video. Some of these activities involve user specific content being saved on the consoles storage media. The ability to use consoles in this fashion increases the potential of the device's storage media containing data of forensic value. A malicious user could potentially use these games consoles to commit or facilitate criminal acts and thus should be researched and examined.

* Corresponding author. Tel.: +44 1443 483246; fax: +44 1443 482715.

E-mail address: kxynos@glam.ac.uk (K. Xynos).

1742-2876/\$ – see front matter © 2010 Elsevier Ltd. All rights reserved.

doi:10.1016/j.diin.2010.02.004

The most recent and popular games consoles (i.e., based on total amount of sales up to 25/02/2009 (gamezine.co.uk, 2009)) include, Nintendo Wii, Microsoft's Xbox 360 and the Sony Playstation 3. This paper examines one of these consoles, the Xbox 360, the leader in hardware sales in recent years, which currently ships with a standard 2.5" SATA hard disk drive. This paper is an initial look into the console and examines the type of data of forensic value that might be contained on the system and outlines the steps required to recover information from an Xbox 360 Hard Disk Drive, as suggested basic guidelines for future investigations.

2. Games consoles and forensics: the XBOX 360

2.1. Review stage

The volume of digital material submitted for forensic analysis now provides a serious challenge to investigative agencies. In addition to storage media contained in the more common laptop and desktop computing platforms, investigators are now expected to examine PDAs, cellular phones, satellite navigation systems and now games consoles ([Lim and Lee, 2008](http://gamezine.co.uk)). The increase in the number of games consoles (gamezine.co.uk, 2009) has provided yet another potential source of information for forensic analysis. Games consoles now pose a problem on a number of possible levels:

They now commonly include some form of storage media that can include user preferences, settings and game related information, these storage devices could be modified and misused to conceal additional information. A number of these systems are also able to connect to a network, often via the Internet to enable online gaming and other forms of social interaction exchanging messages and information.

Despite Microsoft's protection mechanisms, hacking communities have already found code exploits/loopholes, which allow the Xbox 360 to execute unsigned code and software. With the right knowledge and firmware revision on the Xbox 360, Linux can now be booted up, allowing the console to be used much like any other Linux box or computer. Once the Xbox 360 is running Linux, it can be used for a greatly expanded range of purposes, including malicious ones (e.g., illegal file storage). The Xbox 360s predecessor, the Xbox, also succumbed to a thriving hacking community, and was running Linux within a few months of its release.

Therefore games consoles have the potential ability to store a variety of information of potential forensic value. To enhance the efficiency and speed of access to potential evidence, procedures which highlight the locations with the storage device are essential.

This paper aims to highlight the types of material that can be retrieved from the Xbox 360 and the particular locations of data held within the file system. It should be possible to retrieve forensic evidence from an official, unmodified, Xbox 360 examining the normal use of the game console and then forensically imaging the hard disk drive and analysing it with legally acceptable computer forensic tools. The results should produce evidence that is possible to trace or retrieve useful information from the everyday usage of an unmodified Xbox

360. In particular this paper presents what has previously been unknown. Game manufacturers store specific information about a game when it is saved, on the hard disk drives. Inevitably users, by playing and saving games, unknowingly generate a wealth of information waiting to be mined.

3. Related work

A number of papers have considered the forensic value of the Xbox 360 in particular [Vaughan \(2004\)](#) and [Burke and Craiger \(2006, 2007\)](#) highlight the use of Linux to access essential locations of evidential value. On the older Xbox, due to the limitations caused with the existence of the ATA password protection and the limited amount of personal information stored on the consoles, the actual drives did not contain as much information as is common with more recent gaming consoles. The existence of tampering, mod chipping and/or Xbox versions of Linux meant that the system had been expanded in some way therefore the drive was of interest to the forensic examiner. Community work at xbox-linux.org ([Xbox Linux Project, 2009](#)) focused on getting open-source operating systems (e.g., GNU/Linux, BSD, etc.) on the Xbox. This meant decoding and finally leading to the creation of Linux tools, like XFT ([Collins, 2007](#)), that extract data from the FATX file system (i.e., in the Xbox). Similar work is being conducted at free60.org ([Free60 Project, 2009](#)) who focus on adapting and installing open-source operating systems on the Xbox 360. This inevitably means that the current file system, known as XTAF, has to first be decoded ([Free60 Project, 2009](#); [Ladan, 2008a,b](#)), besides finding a way to circumvent certain security features (e.g., digitally signed executables etc.).

[Ladan \(2008c\)](#) also created FreeBSD drivers that will allow a user to mount a drive or image on the FreeBSD system.

Other literature ([Reyes et al., 2007](#)) mentions the possibility and importance of considering game consoles during the seizure process as a potential source of useful information. Especially if it has been modified (e.g., mod chip, running a modified version of the Linux kernel) in any way that extends the capabilities of the device. Work conducted in the area of embedded systems ([Lim and Lee, 2008](#)) mentions that systems like the Xbox 360 should be looked at closely since they could be used to conceal information with the use of hidden partitions on the disk drive. They go on to provide details on what should be examined and how a default system should be compared to that of a suspect's in order to detect any discrepancies. While detecting hidden partitions with the right forensic tools can be a fairly trivial task, conducting a comparison to a default file system is not an easy task as details about the proprietary file system remain unknown. Alternative methods are also looked at, and this involves making use of specialised hardware that looks at low-level hard drive AT commands.

Related work has looked at modified systems that usually meant that either the device's hard disk drive would be altered by installing or booting to a new operating system or unknown coding could be running, in the background, on a rogue system or mod chip.

None of the related work has provided evidence that would enhance a forensic investigation by providing the investigator

with clues such as usertags, date and timestamps, an online presence, multiplayer gameplay and other saved game details.

3.1. File structure and community tools

3.1.1. Drive XTAF structure

The Xbox 360 file system is based on the older FAT implementations (e.g., MS-DOS) with some slight modifications to enhance/improve its use and to make it more suitable for a newer system like the Xbox 360. It is called XTAF and consists of 4 parts (Free60 Project, 2009):

- The Header (Equivalent to the BOOT sector on FAT file systems)
- The File Allocation Table
- The ROOT directory cluster
- The rest of the file system (Directories and files)

The Xbox 360 hard drive is split up into 4 partitions. They are as follows:

- Cache Partition
- Unknown Usage
- Xbox Backwards Compatibility drive
- Main Xbox 360 Partition

Details on the hard drive are written near the beginning of the disk, including the serial number, manufacturer and drive model (Table 1).

A basic overview of the Xbox 360 hard drive contents is presented in Table 2. This may be of interest to a forensic investigator validating the integrity of an Xbox 360 hard drive.

During the first inspection of the drive an index file was found, believed to list all the files used by the console on the drive, along with CRC checksums.

Throughout the examination of the drive, references to storage mediums were made by the device ids. (i.e., \Device\Harddisk0\Partition1\).

The tool Xplorer360 (Xbox-Scene, 2009) makes use of the XTAF details as published by the Free60 Project (2009) and the authors shied away from any immediate reference to it, in order to provide a forensically sound alternative. In a similar fashion XTAF mounting is also possible through a FreeBSD system with drivers provided by Ladan (2008c). This approach was not used either and could be considered in future work. Once again a detailed verification process will be required to ensure that the information extracted with the use of the drivers is correct and coherent.

Table 1 – Xbox 360 HDD Information Structure.

Address	Length (bytes)	Contains
0x2000	0x14	Drive serial # padded with spaces
0x2014	0x08	Firmware revision
0x201C	0x28	Drive model, padded with spaces

Derived from (Free60 Project, 2009).

Table 2 – Xbox 360 HDD Header Structure.

Address	Length (bytes)	Contains
0x0000	8192	Null (0x00)
0x2000	68	Plain text hard disk info
0x2044	24	Static binary info (doesn't change from console to console)
0x205C	256	Dynamic binary data (changes from console to console)
0x2202	2	Size of the following PNG file
0x2204	2754	MS logo in PNG format, made with Macromedia Fireworks MX 2004 on the 19th of July 2005

Derived from (Free60 Project, 2009).

After close inspection of the hard disk drive contents, we have come to the understanding that the dashboard (the console operating system), and system configuration including TCP/IP settings and display/TV settings might be stored on the Xbox 360s embedded flash chip/device.

3.1.2. Xplorer360

Xplorer360 (Xbox-Scene, 2009) is a Microsoft Windows application which reads the Xbox 360s proprietary file system (i.e., XTAF). The program was designed for copying game saves from one drive to the other, so the program has write access to the drive. This makes the program unsuitable for forensic analysis if the program is accessing the drive. It is possible to create a dd version of the forensic image and import that into the program. The program then parses the drive and data carves the file structure and potential file contents. These can only be used as a reference point when conducting an analysis.

The only way to ensure that the program does not make any changes to the dd image is to put the dd image through a cryptographic hashing function (e.g., SHA1, SHA256, etc) and ensure the digests (i.e., footprints) are consistent.

4. Analytical procedures

Any tool or methodology developed to examine the Xbox System has to comply with a sound forensic practise. This is summarised in the UK in the Association of Chief Police Officer (ACPO) guidelines version 4 on digital evidence (ACPO, 2009). This investigation focuses solely on the console hard disk drive as this is seen as the main data repository for the system. Contrary to the flexibility provided by the ACPO guidelines the analysis information provided in the paper demonstrates how information can be extracted from a games console hard disk drive by using a forensically sound methodology.

4.1. Analysis of the console

A forensically sound analytical procedure was devised to enable the patterns of use left by a user on the game console to be identified. The analysis of the drive was performed in a number of stages as outlined in Fig. 1. At each stage, paper based documentation was kept about any changes, modifications and interactions with the Xbox360. This then followed an imaging process after each consecutive game play stage.

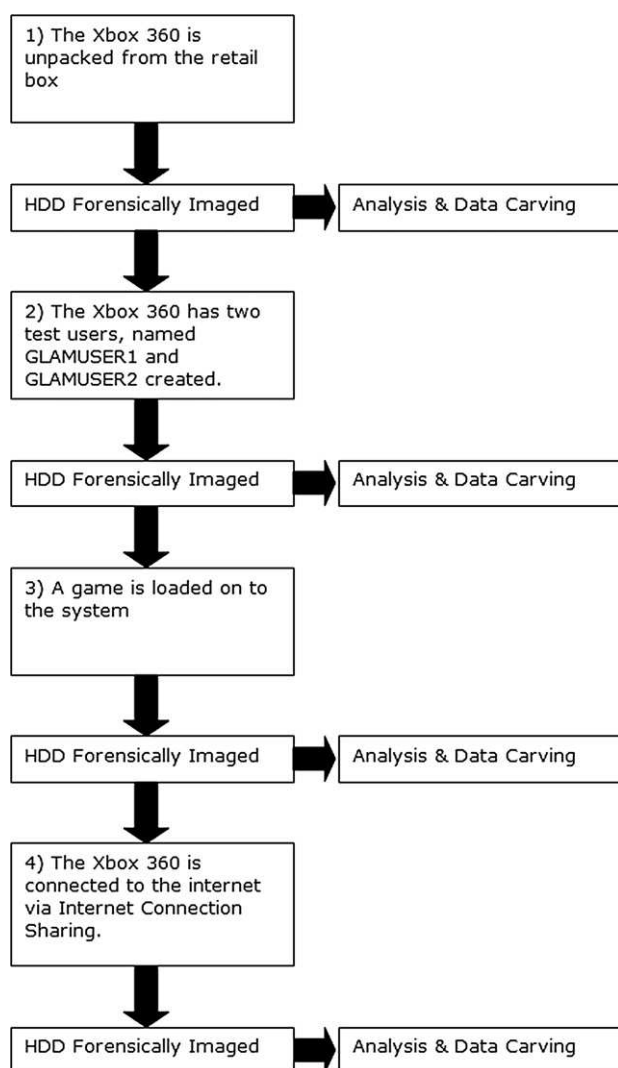


Fig. 1 – Analytical process for the Xbox 360.

Therefore providing with small increments of data accumulation, which helped in the comparison and elimination process during the analysis stage.

4.2. Hard disk drive imaging process

In accordance with the ACPO guidelines copies of the source drive must be taken in a manner not to alter any potential evidence present on the system. Powering on the system will impact on the forensic value of the data therefore in virtually all cases a forensic copy of the disk must be taken to preserve the original media. The Xbox 360 comes with a Serial ATA hard disk drive that is housed in an external sealed drive casing mounted on the top of the console and attached with proprietary connector. See Fig. 2.

It would be possible to construct a cable to attach the drive to a computer system without breaching the casing however to obtain direct access to the SATA interface the disk casing needs to be opened, voiding any warranty. Once achieving access to the drive it is then connected to a write blocker. The authors used a USB 2.0 to SATA Bridge from Tableau T35U (Tableau Software, 2009) and created a forensically sound



Fig. 2 – External view of the Xbox 360.

image of the hard disk using AccessData FTK Imager (AccessData, 2009). All the images are standard E01 formatted disk drive images. These can then be imported into a forensic analysis tool (like AccessData Forensic ToolKit (AccessData, 2009), Guidance Software Encase (Guidance Software, 2009), The Sleuth Kit etc.) for further analysis. AccessData FTK was used to analyse the images taken from the Xbox 360.

4.3. Data carving

Analysis was conducted with the AccessData FTK version 1.8 which is a recognised industry standard tool for the analysis of forensic data. When a case is created, a disk drive image is added to the case in AccessData FTK, the program will automatically index any available file system structure it recognises along with text strings found within the image data. Indexing text strings is a very useful process and aids the forensic analyst in searching for indexed items much quicker, compared to a live search. Since there is no official support for analysing the Xbox's file system, data carving was employed to extract any useful files. Data carving relies on the fact that certain application files contain signature bytes at the beginning and end of the file which can be used to identify the file and extract the file for analysis. Data carving also relies on the fact that the operating system does not mix the fragments.

Another method which is not currently forensically acceptable is the transformation of the image to a dd image and importation of that image into the Xplorer360 tool (Xbox-Scene, 2009). The tool makes use of the detailed analysis of the Xbox 360 file system provided by the free60.org community (Free60 Project, 2009). It is widely used to transfer files (e.g., game saves) from one Xbox360 hard disk drive to another. The inner workings of Xplorer360 are not known to the wider public, as it is freeware and closed source. Therefore, it is not an appropriate tool for using when conducting a forensic investigation. Although it is possible to extract files that contain specific information to a game (e.g., game data is grouped in a single file), it was not used in this paper to confirm any of the findings.

4.4. Network analysis

Since the Xbox 360 will be inevitably connected to the Internet, we deemed it a requirement to connect to the Internet. Therefore, in order to understand further the way the Xbox 360 interacts and communicates with the Internet and a series of controlled live tests were run. These included the following:

- Downloading system updates/patches
- Registering on Xbox Live with a gamertag
- Browsing and downloading game demos
- Playing online multiplayer gaming sessions with other users of the Xbox Live service

As mentioned in Section 4, the hard disk drive was imaged at the end of each of these processes and the findings discussed in Section 6.

5. Digital forensic importance of games

The main purpose of a games console is to run games software. Although the Xbox 360 was designed to work without a hard disk drive, consumer and technological requirements have driven the market in a different direction. The hard disk drive provides a perfect place for games to store saved games, game settings and even whole or parts of the actual game CD in order to reduce reading times, which consequently reduces game loading time.

Although there is an Arcade version which comes without a hard disk drive, all other versions include a hard disk drive. It is believed that sales of the Xbox 360 with a drive would be more sought out, as games depend on them so much and the fact that Xbox 360 hard disk drives are scarce, on the high street and online market places demonstrates an increased need for the accessory.

6. Analysis

6.1. Games results

For this paper two games were analysed, Halo 3 and FIFA 2008 (aka. FIFA 08), in single player, co-operative multiplayer and online multiplayer (i.e., Xbox Live), respectively.

6.1.1. Single player

Analysing the contents of the Xbox 360 hard drive after the aforementioned games had been played showed that the console logs a certain amount of data pertaining to each game and each session spent playing that game. This data correlated with the paper logs kept during the data generation stage. An example of this can be seen in Fig. 3 where FIFA 2008, in single player mode, was played and the time the game settings were saved.

As can be seen in the following two categories (Multiplayer and Xbox Live) Halo 3 demonstrates the same timestamp formats and positioning of the usertags.

```
FIFA 08
00000001
:MqQ:MqQ:MqQ
Settings0 20090213152757
J9X814562-001
UVeo
    4 P8CQ92TO
PERSONAL SETTINGS 1
FIFA 08
```

Fig. 3 – Shows the user of the console had saved settings on FIFA 08 on Friday the 13th of February 2009 at 15:27:57.

6.1.2. Multiplayer

After playing a multiplayer co-operative mode of Halo 3 there were indications of the gamer profiles that had been playing together and at the time and date the activity occurred (See Fig. 4).

Although there is a file path present in Fig. 4 it is unclear how it relates to the game console. It could probably be part of the development stage. There is a high possibility that the other strings (i.e., halo3_ship) might relate to the stage being played by the users.

```
Fri_02132009_160750@pn@GLAMUSER1
d:\maps\020_base
GLAMUSER1
GLAMUSER1
GLAMUSER2
GLAMUSER2
86265EEF2354
10478626
fimd
levels\solo\020_base\020_base
11855.07.08.20.2317.halo3_ship
d:\maps\020_base
```

Fig. 4 – Users ‘GLAMUSER1’ and ‘GLAMUSER2’ playing co-operatively on the ‘020_base’ level of Halo 3, on Friday the 13th of February 2009 at 16:07:50.

6.1.3. Xbox Live

After playing multiplayer co-operative mode, the final test was to try Halo 3 online (i.e., Xbox Live). Once playing a stage online with other users, it was possible to discover remnants of online gamertags (Xbox Live usernames) of all the Xbox Live players who had been present in the online session, Fig. 5. Once again the usertag of the gamer and the date and timestamp have all been recorded. For privacy reasons, the online gamertags cannot be published in this paper.

```
isrguser1
athr
/612070.08.09.05.2031.halo3_s
fimd
12070.08.09.05.2031.halo3_ship
Wed_02182009_130601@pn@isrguser1
jd:mags\isolation
Social Skirmish
One Bomb
Only one team has a base to defend. 4 rounds, teams take turns defending.
Isolation
Containment protocols are almost impervious to pre-Gravemind infestations. What could possibly go wrong? 2-10 players
```

Fig. 5 – Looking at the data logged by the game, it can be ascertained the user ‘isrguser1’ was playing online in a ‘Social Skirmish’ game with other Xbox Live users on the 18th of February 2009, at 13:06:01.

6.1.4. Time stamps

The logs found that the details of game play on the Xbox 360 hard drive contained strings ascertained to include time/date stamps specific to the games analysed. It has been noted that different game developers appear to use slightly different formats for their time strings.

Translating the strings into a time and date was generally straightforward. Although specific to each game, Fig. 6 demonstrates how the timestamp can be translated when FIFA 08 has been played and Fig. 7 for Halo 3 respectively.

It is believed the amount of game data logged is dependant on how the game developers have constructed the software.

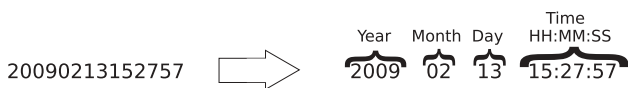


Fig. 6 – Conversion of the FIFA 08 time string.



Fig. 7 – Conversion of Halo 3 time string.

6.2. USB plugging into Xbox 360 and bus doctor results

The authors wanted to examine the user material deposited on the drive as a result of the insertion of a USB device into the Xbox 360. This was done with the help of specialised equipment from Finisar (Finisar, 2009) that analyses hard disk drive activity. The analysis of this activity will demonstrate if the insertion of the USB device creates any events that require the Xbox 360 to write any information on to the hard disk drive. The capturing process is a very intense process creating thousands of events a second when the drive is activated in any way. The hardware has a limit on the amount of ‘stores’ or events it can capture.

The Finisar Bus Doctor Rx was used in conjunction with the Finisar DR-SATA 3000 to capture data going back and forth from the Xbox 360 and the hard disk drive’s SATA interface. The Finisar Bus Doctor CE communicates with the Finisar Bus Doctor Rx and traces and logs all the information in ‘stores’.

The information is the low-level hard disk drive AT commands sent and received by the hard disk drive.

The Bus Doctor was used to see what information is stored on the Xbox 360 when a USB drive is plugged in, as shown in Fig. 8. Contrary to usual practise which involves plugging in the USB device, imaging the drive and searching for changes made to it and then comparing it to a previous image of the same drive, intercepting the low-level commands can yield better and faster results.

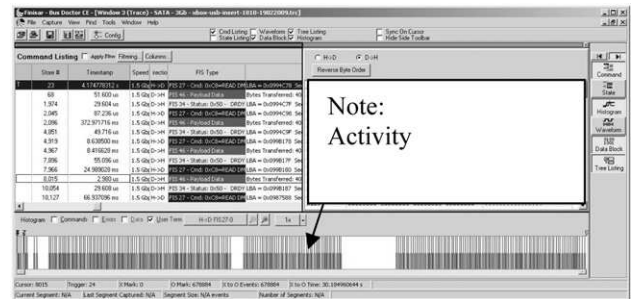


Fig. 8 – Bus Doctor CE – Read DMA.

Due to the vast amounts of events captured (i.e., 678,884), the authors made use of the Histogram and its filtering options. Specific commands are of interest at this stage. When the Event Type FIS 27 frame command flag is set to 0xC8 (hexadecimal value) then it is set to READ DMA, where if it is set to 0xCA then it means that the command is set to WRITE DMA. The Histogram was then set to filter through just the 0xC8 command in Fig. 8. The filtering results can be seen at the bottom section of the window, in waves. The window on the left is the Command Listing and the store number 8015 is selected and its total Payload Data is displayed on the right in the Data Block section.

When the filtering option was set to the 0xCA command, to detect if any Write commands were issued it is clear from Fig. 9 that there are no write commands, since there are no purple indicators.

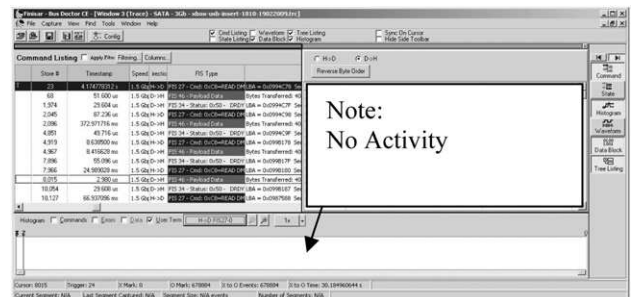


Fig. 9 – Bus Doctor CE – Write DMA.

The Finisar Bus Doctor setup is a much better way of making sure, what information is accessed and stored on a hard drive especially with closed systems like the Xbox 360. It is seamless and not as intrusive as mod chipping or installing

other operating systems and it provides analysts with a better understanding of how and why the system accesses the hard disk drive.

Unfortunately the system's buffers tend to fill up quite quickly when the hard disk drive is accessed. Further research into the area will be needed in order to produce any conclusive results.

6.3. Networking and system update

Using Wireshark on a shared Internet connection, it was possible to trace the network activity. When connecting to the Microsoft Live services the overall communications are encrypted.

Although the system update did alter certain areas of the file system these were not taken into consideration as they did not contain any user specific information that would be deemed useful at this point. The fact that imaging was conducted at the end of each stage helps compare changes done to the system. This could be taken into consideration in future analysis.

7. Future considerations

There is still much work to be conducted on the Xbox 360. The results from analysing the information stored on the Xbox 360 hard disk drive is truly unexpected since the Xbox 360 Hard disk drive was never meant to save detailed amounts of information. The fact that games developers make use of the drive and store what has now being deemed as forensically useful information is a interesting find. Since this information is unique for each game, further analysis will be required on the top 10 most popular games and a constant review of newer games as they come out. The authors also believe that co-operative games could possibly provide an investigator with very interesting information as it places two people in front of the games console. The findings could then feed into a project that would create pattern-matching algorithms or regular expressions that could consequently be fed into numerous forensic tools (e.g., Encase, AccessData FTK, etc).

Further analysis can be conducted in the use of Xplorer360 and the information extracted by it, in conjunction with the data found specific to a game. This could in turn provide with better-grouped information compared to the unified binary seen in AccessData FTK.

With the expansion of the online communities further work needs to be conducted in the online Microsoft Live system and the streaming of digital media from PCs and streaming services.

Further research is also required at analysing the embedded flash chip. This will probably involve removing, imaging and analysing the embedded flash chip.

The authors believe that it is imperative that investigating officers take and image games consoles as there is a high possibility that there may be information of value to their investigation. If these devices are not being taken into consideration then there is a high possibility that a cunning perpetrator would store information on that drive to avoid prosecution.

8. Conclusions

The volume and range of devices submitted for analysis will only increase and provide a serious challenge to investigative agencies who are now required to deal with PDAs, cellular phones and satellite navigation systems. The fact that games consoles also include hard disk drives provides another analysis source with even more potential information.

This paper has considered the forensic value of material which may be present on one of these consoles, the Xbox 360.

The paper has highlighted the fact that game saves and games in general can provide interesting digital forensic artefacts. These artefacts can provide details like if the game was in single player mode, multiplayer co-operative mode or even online multiplayer mode and date and timestamps usually in association with a usertag or usertags.

Finally, the communications channel between the Xbox 360 and the hard disk drive were analysed and it has been proven that nothing is written to the drive when a USB flash drive is plugged into the Xbox 360.

Overall, it is believed that officers should acquire and analyse these types of media as the information stored on them could possibly be very fruitful.

Acknowledgements

The authors would like to thank the Information Security Research Group (ISRG) at the University of Glamorgan for the various supports given, including time and funding in completing this project. Special thanks go to Huw Read and Nick Pringle.

Appendix.

Software tools used:

- Xbox 360 dashboard version is: D:2.0.7363.0-K:2.0.7363.0 (BK:2.0.1888.0) X:020D-BD94-9E8B-700D
- AccessData FTK Imager 2.5.4.16
- AccessData Forensic ToolKit 1.81
- Finisar Bus Doctor CE V5.0.0
- Wireshark
- Xplorer360 Beta 6 Xtreme
- Windows 2000 Advanced Server SP4
- Windows XP Professional SP3

Hardware tools used:

- Xbox 360 Elite with a 120 GB hard disk drive
- USB 2.0 to SATA Bridge from Tableau T35U
- Finisar Bus Doctor Rx
- Finisar DR-SATA 3000
- Custom Male to Female SATA cable

REFERENCES

- AccessData [Online]. Available: <http://www.accessdata.com>; 2009 (last accessed 26.02.09).

- ACPO. [Online], Good practise guidelines for computer-based electronic evidence, Version 4. Available at, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf; 2009 (accessed 02.11.09).
- Burke P, Craiger P. Forensic analysis of Xbox consoles. In: Craiger P, Shenoi S, editors. *Advances in digital forensics III*. IFIP international federation of information processing, vol. 242. Boston: Springer; 2007. p. 269–80.
- Burke PK, Craiger P. Xbox forensics. *Journal of Digital Forensic Practice* 2006;1(4):275–82.
- Collins D. XFT – a forensic analysis tool for the Microsoft Xbox game console. In: *Proceedings of the 6th annual security conference*. Las Vegas, USA: CD Proceedings, ISBN 0-9772107-5-8; April 11–12, 2007.
- Finisar [Online]. Available, <http://www.finisar.com>; 2009 (last accessed 25.02.09).
- Free60 Project [Online]. Available, <http://www.free60.org>; 2009 (last accessed 26.02.09).
- gamezine.co.uk. PlayStation 3 and Xbox 360 worldwide sales equal in 2008 [Online]. Available, [http://www.gamezine.co.uk/news/ps3-and-360-sales-equal-in-2008-\\$1264624.htm](http://www.gamezine.co.uk/news/ps3-and-360-sales-equal-in-2008-$1264624.htm); 2009 (last accessed 26.02.09).
- Guidence Software [Online]. Available, <http://www.guidencesoftware.com>; 2009 (Last Accessed 26.02.09).
- Ladan R [Online]. Python tool to extract typical Xbox 360 files. Available <ftp://rene-ladan.nl/pub/distfiles/extract360.py>; 2008a (last accessed 25.02.09).
- Ladan R [Online]. xtaf tool in C. Available <ftp://rene-ladan.nl/pub/distfiles/uxtaf.c>; 2008b (last accessed 26.02.09) and <ftp://rene-ladan.nl/pub/distfiles/uxtaf.txt>; 2008b (last accessed 26.02.09)
- Ladan R. Geom_xbox360 and a preliminary driver for the Xbox 360 file system (xtaf) [Online]. Available, <http://wiki.freebsd.org/ReneLadan>; 2008c (last accessed 26.02.09).
- Lim K, Lee S. A methodology for forensic analysis of embedded systems. In: *Second international conference on future generation communication and networking*; 2008, p. 283–86.
- Reyes A, O'Shea K, Steele J, Hansen JR, Jean BR, Ralph T. *Digital forensics and analyzing data*. In: *Cyber crime investigations*. Burlington: Syngress, ISBN 978-1-59-749133-4. doi:10.1016/B978-159749133-4/50010-3. 2007 p. 219–59.
- Tableau Software [Online]. Available, <http://www.tableau.com>; 2009 (last accessed 26.02.09).
- Vaughan C. Xbox security issues and forensic recovery methodology (utilizing Linux). *Digital Investigation* 2004;1(3):165–72.
- Xbox Linux Project [Online]. Available, <http://www.xbox-linux.org>; 2009 (last accessed 26.02.09).
- Xbox-Scene, Xplorer360 [Online]. Available, <http://www.xbox-scene.com/xbox360-tools/Xplorer360.php>; 2009 (last accessed 25.02.09).