Investigating an Xbox Game Console for Potential Forensic Evidence

Game consoles are gaining their popularity not only as simple gaming machines, but also as media centres, multimedia players and media servers. The fine line between the game consoles and personnel computers blurred at early two thousands, especially with the launch of Xbox game console, because of its striking similarity to the PC architecture. Because of this striking resemblance of the PC like architecture, Hobbyists, enthusiasts, hackers and homebrew developers could develop and install 3rd party software on to the Xbox with little to none modification to the console and to the software.

Unlike the earlier game consoles, the Sixth generation game consoles (Ex: Xbox, PS2 and GameCube) can be easily modified to support any PC like functionality because of the straight out of the box PC hardware installed on them. Out of the Sixth Generation game consoles, Xbox in particularly consists of standard PC hardware as opposed to GameCube and PlayStation 2 using PowerPC processors, custom optical drives and custom gamepad connectors (Steil 2005).

Therefore Mod chips and exploits for the Xbox game console are widely available, low-priced and require little technical knowledge to install. Once modified, the Xbox can be used to perform any functionality of a standard computer and also it can be used to store Gigabytes of non game related files. Because of this, there is a high possibility that a suspect's Xbox game console could hold valuable forensic evidence. But still the forensic investigators seem to oversight the forensic importance of these devices.

As a remedy, this paper tries to discuss and to lay due stress on; the forensic value of an Xbox game console, the ways and means of conducting an investigation and the limitations of those approaches.

This paper is organised as follows: In section 1, paper would provide a brief discussion of Xbox and its internal hardware. In section 2, the paper would critically discuss the security mechanisms used in the Xbox and how the security mechanisms have been exploited by the hackers to run non-Microsoft codes. Section 4 would discuss the Partition structure of the Xbox and provide a brief discussion on FATX, the native file system of the Xbox. Section 5 would provide a detailed discussion of step-by-step procedures for a forensic investigation of an Xbox and would briefly point-out some of the limitations of the current Xbox investigation mechanisms. Finally the paper would draw the conclusions and provide the grounds for future work.

1: The Xbox Game Console

Microsoft Xbox game console was released in year 2001 as a direct competitor for PS2 and GameCube. Except for the fact that it is only authorized to run executables signed by Microsoft, the Xbox game console is indeed a low end personnel computer.

The Xbox consists of a Pentium III Celeron mobile 733 MHz CPU, 64 MB of RAM, GeForce 3 MX Graphics processing unit with a TV out, 10 GB IDE hard disk (8GB on earlier models), an IDE DVD drive, Fast Ethernet Port and USB ports for Game Controllers. In addition, as the software solution, the Xbox uses ripped down version of Microsoft Windows 2000 kernel as its operating system and a altered version of DirectX interface (Steil 2005).

2: Xbox Security mechanism

Because of the more than passing similarity of the Xbox to a PC, the need for a hacker proof security system was of utmost important for the Xbox than for the other two game consoles. The Xbox uses a security mechanism that refuses any software that is not authentic or any software that is not on the intended medium.

This is achieved by a chain of trust that triggers at the start-up of the Xbox and expands up to the execution of a game. Upon the start-up of the Xbox, the CPU is booted by a non-replaceable secret ROM (it is important that the ROM is non-replaceable and non-reprogrammable as otherwise hackers could change the whole verification process) embedded in the Southbridge. Then, a virtual machine embedded in the secret ROM verifies the contents of the encrypted Second Boot Loader inside the flash memory using RC4 hash algorithm (the decryption key is stored in the secret ROM and is sent to the flash memory using a very fast HyperTransport bus which Microsoft thought is impossible to sniff). The virtual machine confirms the authenticity of the Second Boot Loader by comparing the last 32 bits of the decrypted value with the constant of 0x7854794A (Steil 2005).

If the flash memory is changed, overridden, replaced, or reprogrammed by a hacker, the last 32 bits of the hash would change and the Xbox would enter the ‘Panic mode’. Once in the ‘Panic mode’, the Xbox is designed to automatically switch off its secret ROM to stop hackers from dumping the contents of it.

If the verification process confirms the originality of the Second Boot Loader, then the Second Boot Loader decrypts the kernel (operating system of the Xbox) which is also stored in the flash memory. If the verification of the kernel is successful, then the kernel verifies the contents of the Xbox Dashboard (the GUI of the Xbox).All files, except the font files and audio files, of the Xbox Dashboard are signed by Microsoft and hashed. So the kernel verifies the Dashboard files by comparing them with a known hash list. If all of these steps are completed successfully, then only the Xbox would boot up (Steil 2005).

2.1: Xbox Security Mechanism Exploits

Despite of all the above mentioned security mechanisms, hackers have found various workarounds to bypass the security of the Xbox and to install custom software and operating systems in it.

Hackers have found two main methods to bypass the security system of the Xbox, the hard modifying and soft modifying.

2.1.1: Hard Modifying an Xbox

As already mentioned under 'Xbox security mechanism', Microsoft assumed that the RC4 cipher key, that gets transferred from the secret ROM to the flash memory during the decryption of the Second Boot Loader, is impossible to sniff because of the high speed of the HyperTransport bus. But a hacker named Andrew Huang was able to successfully sniff RC4 key using a custom build packet sniffer (Steil 2005).

Another defect in the Xbox security system is, only checking the last 32 bits of the decrypted data of the RC4 algorithm for the verification of the Second Boot Loader. Unfortunately RC4 is not a cipher. It decrypts data bit by bit; it cannot be used as a hash algorithm. With RC4, even if the first few bits are altered by a hacker, the last few bits would decrypt correctly. Therefore the hackers could reprogram the Second Boot Loader (up to last 32 bits) to patch the kernel to accept games without proper RSA signature, games on DVD-R and custom software (Steil 2005).

As the RC4 key is known and as there was no proper hashing for the Second Boot Loader, numerous Modchips emerged to replace the Second Boot Loader. These Modchips enabled copying games from the CD to the hard drive, playing games from the hard drive, installing 3rd party software including the operating system and installing larger hard drives.

2.1.2: Soft Modifying an Xbox

As already mentioned, before executing a game, the Xbox kernel checks the RSA signature of the disk and the medium of the game. This makes it impossible for hackers to alter the contents of the game and to use them against the security system of the Xbox.

But most, if not all, Xbox games support loading save game files from the Xbox memory cards. Some of the Xbox games like 'Splinter Cell', 'MechAssault', '007 Agent under Fire' have buffer vulnerabilities in their save game handlers. This enables the hackers to change the contents of the save games in a way that over floors the memory stack of Xbox and jumps to the code the hacker inserted in the save game (Steil 2005).

So users only have to launch the game with the buffer vulnerability, and load the exploited save game to get the full control of the Xbox. Once the user gets the full control of the Xbox kernel, he has the ability to access the Dashboard files that resides on the Xbox hard drive which is by default locked by an ATA password protection mechanism.

As already mentioned under 'Xbox Security Mechanism', all the Dashboard files, with the exception of font files and audio files, are hashed, thus preventing hackers from modifying them. But there is an integer vulnerability in the font handlers. Since the font files are not hashed, once a hacker has the access to the Dashboard files (by using save game exploitation), he can replace the font files with faulty fonts which would exploit the integer vulnerability to cause the Xbox Dashboard to crash and to load a alternative dashboard that is embedded in the secondary fonts (Steil 2005).

Alternative dashboards act like small operating systems. They provide basic functionalities like FTP, Telnet, Media playing and image viewing.

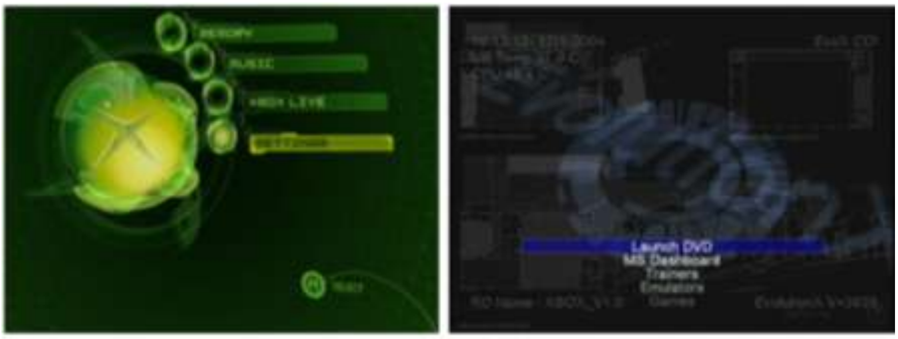


Figure 1: Microsoft Dashboard vs. an alternative (Evolution-X) Dashboard

If a user wants the full functionality of a PC, he can then install a Linux Distribution such as Xebian, Xdsl, Xubuntu or GentooX.

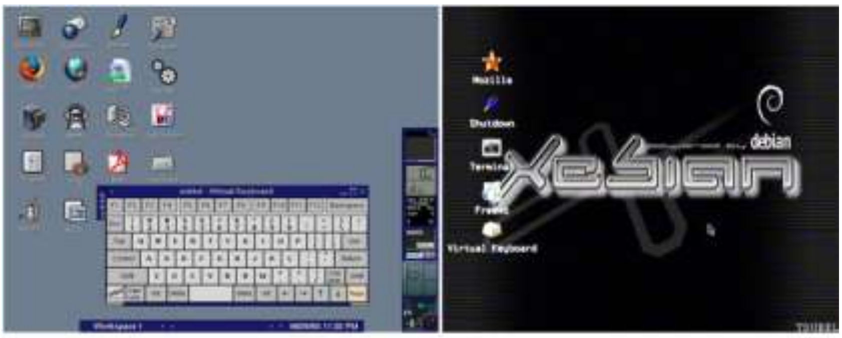


Figure 2: XDSL installed on an Xbox

Xebian Installed on an Xbox

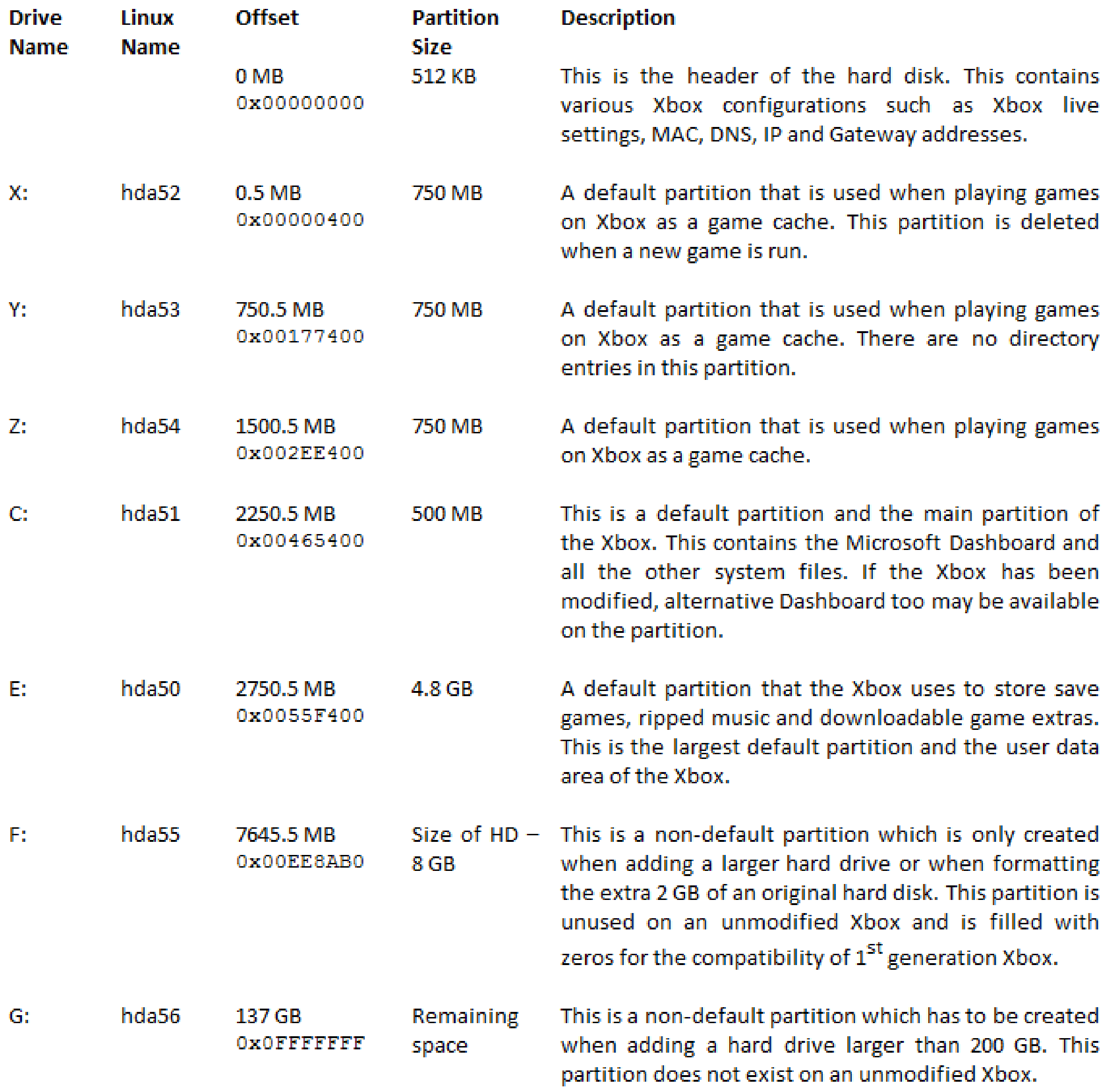
Criminals may find soft modifying more attractive than the hard modifying for several reasons. Soft modifying does not need to open the casing of the Xbox; thus effectively reducing the chances of detection. In addition it would further reduces the chance of detection as switching on a soft modified Xbox would boot up to the Microsoft Dashboard if the exploited game disk is not in the drive, as oppose to hard modified Xbox always login to alternative dash boards. So without the game disk with the vulnerability and the hacked save file, a soft modified Xbox is un-modified at the first glance (Collins 2007).

3: Xbox Hard drive and Partition Structure

Xbox hard drive is by default locked by an ATA password protection mechanism. The 32 byte password that is required to unlock the Xbox hard drive is dependent on the eeprom data of the Xbox, serial number of the hard drive and the model of the hard drive. So the password is unique to the hard drive and to the Xbox that the hard drive is installed on (SpeedBump 2002). Once the Xbox passes all the security checks would the hard disk be unlocked.

3.1: The Partition Structure

Once a user compromises the Microsoft security system by occupying one of the above two methods, he has the total control of the Xbox. Once the security is breached, not only the user can access all the partition of the Xbox hard disk, but also he can replace the entire hard disk with a bigger hard drive. Because of this, a criminal can save or hide his files in any of the following hard drive partitions and it is important to have a thorough understanding of partition structure of an Xbox for a proper forensic investigation.



Drive Name	Linux Name	Offset	Partition Size	Description
		0 MB 0x00000000	512 KB	This is the header of the hard disk. This contains various Xbox configurations such as Xbox live settings, MAC, DNS, IP and Gateway addresses.
X:	hda52	0.5 MB 0x00000400	750 MB	A default partition that is used when playing games on Xbox as a game cache. This partition is deleted when a new game is run.
Y:	hda53	750.5 MB 0x00177400	750 MB	A default partition that is used when playing games on Xbox as a game cache. There are no directory entries in this partition.
Z:	hda54	1500.5 MB 0x002EE400	750 MB	A default partition that is used when playing games on Xbox as a game cache.
C:	hda51	2250.5 MB 0x00465400	500 MB	This is a default partition and the main partition of the Xbox. This contains the Microsoft Dashboard and all the other system files. If the Xbox has been modified, alternative Dashboard too may be available on the partition.
E:	hda50	2750.5 MB 0x0055F400	4.8 GB	A default partition that the Xbox uses to store save games, ripped music and downloadable game extras. This is the largest default partition and the user data area of the Xbox.
F:	hda55	7645.5 MB 0x00EE8AB0	Size of HD – 8 GB	This is a non-default partition which is only created when adding a larger hard drive or when formatting the extra 2 GB of an original hard disk. This partition is unused on an unmodified Xbox and is filled with zeros for the compatibility of 1st generation Xbox.
G:	hda56	137 GB 0x0FFFFFFF	Remaining space	This is a non-default partition which has to be created when adding a hard drive larger than 200 GB. This partition does not exist on an unmodified Xbox.

3.2: File System of the Xbox

Xbox uses FATX as its file system. FATX is a derivate of the FAT32 file system with some of the redundant fields dropped in order to avoid inconsistencies and security issues (Steil 2003). FATX is largely an undocumented file system and therefore is not supported by the most of the leading Forensic Investigation tools.

According to Steil, just like FAT32, FATX consists of a super block, a File allocation table and directory entries in addition to the actual data. The File allocation table in FATX is identical to FAT32 and FAT16. Similar to FAT32, in FATX, the File allocation table for partitions less than 1 GB is formatted in FATX16 and for other partitions in FATX32 (Steil 2003). Therefore, as the partitions X, Y, Z and C are less than 1GB, they are formatted in FATX16 while the partition E is formatted in FATX32.

In addition to the File allocation table, the Directory entries in FATX are also similar to FAT32, but with the exception of long file names up to 42 characters. A directory entry in FATX is 64 bytes long and since the cluster size of FATX is 16 KB, a cluster can hold up to 256 directory entries (Steil 2003).

The 64 bytes of a directory entry are distributed as follows:

Offset	**Size**	**Description**
0	1	Size of filename (max. 42)
1	1	Attribute as on FAT
2	42	Filename in ASCII, padded with 0xff (not zero-terminated)
44	4	First cluster
48	4	File size in bytes
52	2	Modification time
54	2	Modification date
56	2	Creation time
58	2	Creation date
60	2	Last access time
62	2	Last access date

Upon the deletion of a file, the pointer to the file is removed and the filename size field is marked with the value of ‘0xe5’. Though the pointer is removed, the file still resides on the hard disk until it gets overwritten by another file (Steil 2003).

So searching for the value ‘0xe5’ using a Hex editor would reveal any deleted files in FATX which comes handy in a forensic investigation of such disk.

4: Forensic Investigation of an Xbox Game Console

This section of the paper discusses the procedures involved in a forensic investigation of an Xbox game console. These procedures are categorized into three main sections, ‘Initial assessment’, ‘Imaging and Mounting the Xbox hard disk’ and ‘Forensic Analysis of the hard disk’. The initial assessment section would focus on how to identify a modified Xbox and the precautions that have to be taken when seizing an Xbox. ‘Imaging and Mounting the Xbox hard disk’ section would discuss how to set up the forensic workstation and various methods of imaging the Xbox hard drive. Final section, Forensic Analysis of the hard disk, would discuss various analyses methods and tools that can be used for the investigation.

4.1: Initial assessment

This section describes various methods that can be occupied to identify a modified Xbox and various precautions that have to be exercised during the initial stage of an investigation.

Burke and Craiger, in their paper ‘Xbox Forensics’ describe various methods that can be used to identify both hard modified and soft modified Xbox. According to them, a hard modified Xbox can be identified by physically examining the stickers and rubber pads that conceal the six screws of the Xbox. Any tampering of the sticker or rubber pads would evident a hard modification, since hard modification require the case of the Xbox to be opened (Burke & Craiger 2006).

Furthermore, they also suggest observing the environment around the Xbox. If the Xbox is not connected to a TV but to an Ethernet cable, then chances are the Xbox is being used as a terminal PC (to remotely SSH) or as a server. In addition, the presence of a ‘USB XBOX adapter’ implies that the Xbox is being used as a personnel computer as the ‘USB XBOX adapter’ is only used to connect USB keyboards and mice to an Xbox. Presence of keyboards and mice around the Xbox is also suspicious.

According to Burke and Craiger, the best method to identify a modified Xbox, hard modified or soft modified, is by switching it up with a Linux Boot CD inside the CD tray. If the Xbox boots into Linux successfully, that means the Xbox is being modified (Burke and Craiger confirms that booting an Xbox with a Linux CD wont alter the contents of the hard drive in any way). Otherwise the Xbox would prompt an error message saying that it can’t recognise the disk. However, even if such error message is prompted, the Xbox has to be tried with several Linux Boot mediums (CD-RW, DVD-R, DVD-RW) because some Xboxes have difficulties in identifying some CDs because of an inherent fault in the XBOX CD head. As a general guide, according to Xbox-Linux group, it is always advisable to try with DVD-R disks.

If the Xbox is unplugged from it power source for a long time (more than an hour), then at the first attempt, the Xbox would not boot into Linux even if it is modified. In such a case, a dialog box would appear asking to set the date and time of the Xbox, and once they are set the default MS Dashboard will appear even the Xbox is modified. In such a sitiation, the Xbox has to be restarted to see if it loads Linux.

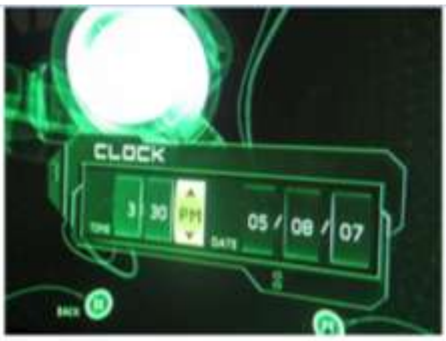


Figure 3: The dialog box that appears upon the reset of the internal clock

4.1.1: Precautions

- ✓ Prior switching on the Xbox with a Linux Boot CD, any memory cards connected to it has to be removed. This is because; the Xbox formats any memory cards which does not contain game related data. A criminal could use this behaviour to intentionally delete his data in case someone else switches on the console (Burke & Craiger 2006).
- ✓ As already mentioned, if the Xbox is unplugged for a long time, the internal clock would reset. Therefore, according to Burke and Craiger, in case the Xbox has to be moved during a seizure, it has to be connected to a power source immediately. At the same time, they also state that a reset of the internal clock would not modify the disk contents anyway (Burke & Craiger 2006).

Once an Xbox is confirmed to be modified, it has to be seized and transported to a Forensic laboratory for further investigations in a similar fashion as any other personnel computer.

4.2: Imaging and Mounting the Xbox hard disk

This section focuses on the procedures involved in duplicating and mounting an Xbox hard drive. This section is two fold. The first part describes various methods that could be used to duplicate an Xbox hard drive. The later describes the preparation of the Forensic Workstation as an Xbox image cannot be mounted on a normal PC straight away.

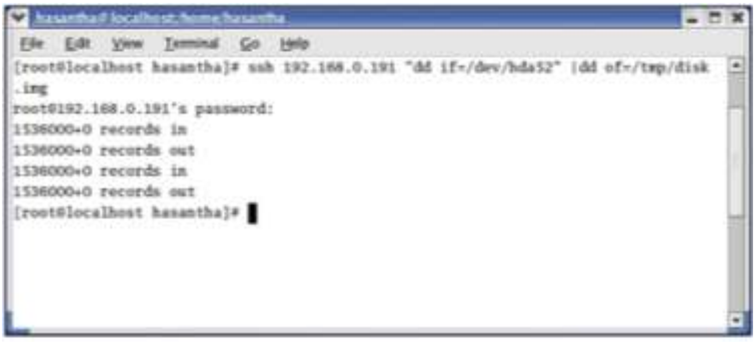
4.2.1: Imaging an Xbox Hard Disk

As already mentioned under 'Xbox Hard Drive and Partition Structure', the Xbox hard disk is locked by an ATA password protection mechanism. Because of that, without the correct password or without that specific Xbox, the hard drive is locked and would not be identified by any traditional imaging software. This poses a significant challenge to forensic investigators.

Vaughan, however, proposes several workarounds to this problem. The first of them is 'hotswap'. In hot swapping, the Xbox is switched on and waited till it boots to the Dashboard. Once the Xbox boots to the Dashboard, as already mentioned, it unlocks the hard disk. Once unlocked, the Xbox IDE cable is replaced on the fly with a running computer's IDE cable (Vaughan 2004). This method however is a least forensically sound mechanism as there is a high possibility of data corruption.

He then suggests another solution which unlocks the hard drive using the 'Unlock Harddisk' feature of an 'Evox' (an alternative dashboard- Evolution X) disk and then using that hard drive as any other normal disk. Another alternative he proposes is that, obtaining the ATA password using an 'Evox' CD, connecting the hard disk to the computer, unlocking that hard disk through software such as 'unlockhdd' using the obtained password and then imaging it (Vaughan 2004). With the exception of the first method, the last two are forensically sound. But all those methods require physical extraction of the hard disk from the Xbox and some require changing the state of hard disk such as permanently unlocking it.

Burke and Craiger introduce a less intrusive method for imaging hard disk that does not require any low-level physical interaction with the Xbox. In this method, the Xbox is booted with a Linux CD and then connected to the Forensic Workstation using a crossover cable. Then, using the Workstation, the partitions of the Xbox are imaged through a secure shell (SSH).


hasantha@localhost:/home/hasantha
File Edit View Terminal Go Help

```
[root@localhost hasantha]# ssh 192.168.0.191 "dd if=/dev/hda52" |dd of=/tmp/disk
.img
root@192.168.0.191's password:
1536000+0 records in
1536000+0 records out
1536000+0 records in
1536000+0 records out
[root@localhost hasantha]#
```

Figure 4: Disk dumping through SSH

Despite of the method used for imaging the hard disk, it is recommended to image individual partitions (‘sfdisk’ command can be used to obtain partition information) instead of the disk as a whole, because Linux does not support mounting partitions embedded inside an image. Once imaged, the hash of the acquired images has to be checked against the original drives to ensure the integrity.

4.2.2: Mounting the Images

None of the current operating system provides native FATX support and therefore the acquired images can not be mounted straight away. There are some Windows tools for mounting and viewing FATX partition such as Xplorer360, but they are unstable and lack the logical level support needed for a forensic investigation.

Therefore, Burke and Craiger propose to use Linux with the FATX kernel patch applied (The FATX patch is a modified version of the FAT32 driver for Linux). In their paper, they provide a step-by-step guide for compiling a Linux kernel with FATX support. Once the corresponding patch for the kernel is applied, the compilation process is identical to the traditional Linux kernel compiling, but it is essential to modularize or to add built in kernel support for FATX, Xbox partitions and Loopback devices. The patches for 2.6 kernels are very unstable and therefore sometimes do not properly identify FATX partitions (Burke & Craiger 2006). It is advisable to use an older Linux distribution which comes with a 2.4 kernel as downgraded kernels are not supported by the FATX patch.

Once the new kernel is compiled with the FATX support, the following command can be used to mount the partitions as read-only:

```
mount -t fatx -o ro,loop /tmp/ hda52.img /mnt/xbox-52
```

David Collins offers XFT as an alternative to the above approach. XFT, a software currently under development, is a command line tool that can be used to mount FATX partitions, browse FATX directories, open files, view files in hex mode and generate directory trees, using Linux shell commands (Collins 2007).

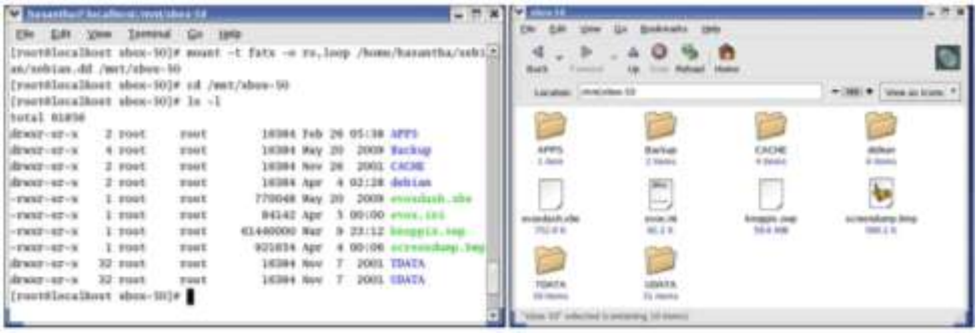
Regardless of the method used for mounting the partitions, the images have to be always protected by 'root', set as 'read-only' and analysed through a standard user account to avoid accidently writing to the partitions.

4.3: Forensic Analysis of the hard disk

At the time of writing this paper, no major Forensic utility provides support for FATX file system and therefore there is no simple method for extracting evidence from an Xbox hard disk in all instances. However, because of the similarity between FAT32 and FATX file system, some components of existing forensic suits can be used to a certain extent to extract information from such disks. This section of the paper discusses such tools and methods that can be used for extracting information.

4.3.1: Traversing the Hard disk

Once the partitions are mounted using the FATX patch, they can be treated as local file systems and can be traversed using the X-window interface or using standard Linux shell commands. If XFT is used to mount the partitions, the XFT commands can be used to browse through the file system.



```
[root@localhost xbox-50]# mount -t fatx -o ro,loop /home/hasantha/xebi
an/xebian.dd /mnt/xbox-50
[root@localhost xbox-50]# cd /mnt/xbox-50
[root@localhost xbox-50]# ls -l
total 81856
drwxr-xr-x   2 root     root        16384 Feb 26 05:38 APPS
drwxr-xr-x   4 root     root        16384 May 20  2009 Backup
drwxr-xr-x   2 root     root        16384 Nov 28  2001 CACHE
drwxr-xr-x   2 root     root        16384 Apr  4 02:28 debian
-rwxr-xr-x   1 root     root       770048 May 20  2009 evoxdash.xbe
-rwxr-xr-x   1 root     root        84142 Apr  3 00:00 evox.ini
-rwxr-xr-x   1 root     root     61440000 Mar  9 23:12 knoppix.swp
-rwxr-xr-x   1 root     root       921654 Apr  4 00:06 screendump.bmp
drwxr-xr-x  32 root     root        16384 Nov  7  2001 TDATA
drwxr-xr-x  32 root     root        16384 Nov  7  2001 UDATA
[root@localhost xbox-50]#
```

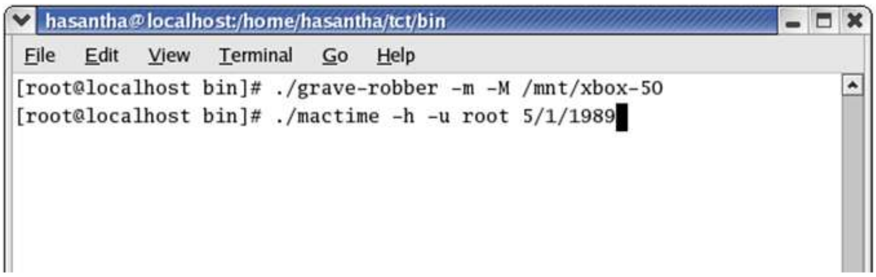
Figure 5: Traversing the Disk Using Linux Shell and X-Window Interface

4.3.2: Time Stamp Analysis

Because of the similarity between FAT32 and FATX, the 'Sleuth Kit' or 'The Coroner's Toolkit (TCT)' can be used to generate time line information.

Burke and Craiger provide a step by step guide for using Sleuth kit and an explanation of the results that are generated from it. Therefore, this paper would provide a brief description on using the TCT to generate time line information.

When using TCT, as the first step, 'gave-robber' utility has to be used in order to extract MAC time information from the file system. Grave-robber extracts MAC information and stores them in a database. When executing grave-robber it is important to run as 'root' as grave-robber will then be able to capture file and process information that are not available for normal users (Jeffris 2002).

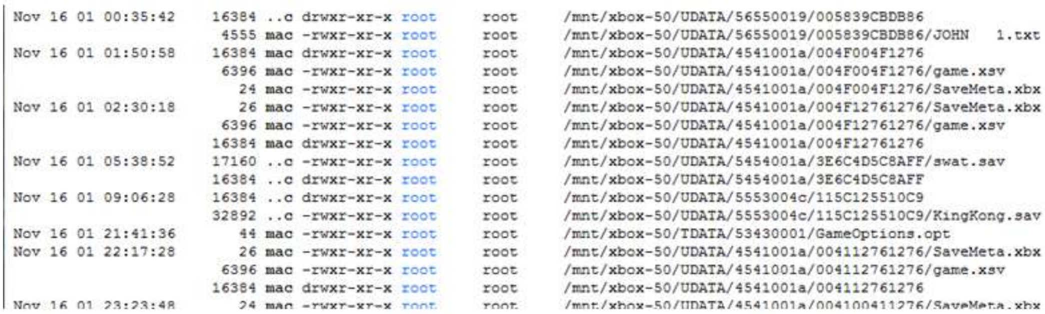


hasantha@localhost:/home/hasantha/tct/bin
File Edit View Terminal Go Help

```
[root@localhost bin]# ./grave-robber -m -M /mnt/xbox-50
[root@localhost bin]# ./mactime -h -u root 5/1/1989
```

Figure 6: Using Mactime utility for Time stamp analysis of files after 5/1/1989
(-h tag would present the output in a HTML page, -u tag would highlight the activities of that user in a different colour)

After the grave-robber is done with the file system walk and after the database is created, the 'mactime' utility can be used to extract information from the database and to present them in a human readable manner.



```
Nov 16 01 00:35:42     16384 ..c drwxr-xr-x root      root      /mnt/xbox-50/UDATA/56550019/005839CBDB86
                        4555 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/56550019/005839CBDB86/JOHN   1.txt
Nov 16 01 01:50:58     16384 mac drwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F004F1276
                        6396 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F004F1276/game.xsv
                          24 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F004F1276/SaveMeta.xbx
Nov 16 01 02:30:18        26 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F12761276/SaveMeta.xbx
                        6396 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F12761276/game.xsv
                       16384 mac drwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004F12761276
Nov 16 01 05:38:52     17160 ..c -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/5454001a/3E6C4D5C8AFF/swat.sav
                       16384 ..c drwxr-xr-x root      root      /mnt/xbox-50/UDATA/5454001a/3E6C4D5C8AFF
Nov 16 01 09:06:28     16384 ..c drwxr-xr-x root      root      /mnt/xbox-50/UDATA/5553004c/115C125510C9
                       32892 ..c -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/5553004c/115C125510C9/KingKong.sav
Nov 16 01 21:41:36        44 mac -rwxr-xr-x root      root      /mnt/xbox-50/TDATA/53430001/GameOptions.opt
Nov 16 01 22:17:28        26 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004112761276/SaveMeta.xbx
                        6396 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004112761276/game.xsv
                       16384 mac drwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004112761276
Nov 16 01 23:23:48        24 mac -rwxr-xr-x root      root      /mnt/xbox-50/UDATA/4541001a/004100411276/SaveMeta.xbx
```

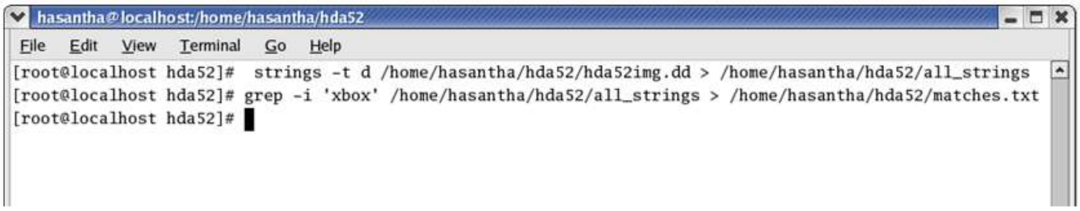
Figure 7: The output of the Mactime utility
(1st column shows the date and time of the last activity, 2nd column shows the file size, 3rd column shows whether the file is being modified, accessed and/or created, the final column shows the location)

'-m' flag requests grave-robber to extract MAC times while the '-M' flag requests grave-robber to calculate MD5 values of all the files. Storing MD5 values along with their MAC times is useful because then it is possible to remove the known-good files from future analysis by comparing those extracted MD5 values with the set of trusted MD5 list published by ncfs.org (Burke & Craiger 2006).

4.3.3: Text Analysis

Valuable forensic information can reside on the Xbox hard disk in the form of text since data can be entered into an Xbox using the on-screen keyboard, a USB keyboard, FTP, CD/DVD or as an email. Therefore a keyword search has the potential to reveal forensic evidence that would support an investigation.

Vaughan suggests using Linux utilities 'String' and 'grep' to find any evidence left in ASCII form. First, the texts have to be extracted from the raw image using the 'String' command. Once extracted, the 'grep' command can be used to find specific expressions from the extracted strings (however, grep won't find strings that spans across several lines). If the keyword is found, grep writes the line which contains that keyword along with the file offset. By travelling to those offsets using a hex editor, it is then possible to find the area of the file where the string occurred (Vaughan 2004).



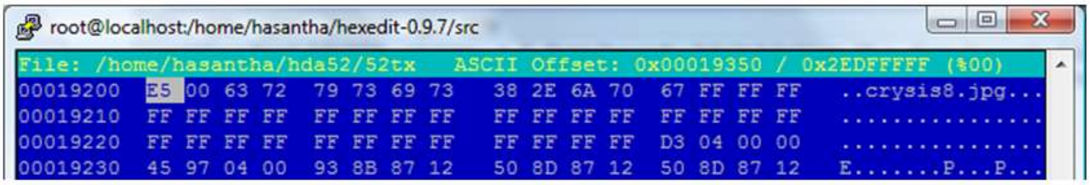
hasantha@localhost:/home/hasantha/hda52
File Edit View Terminal Go Help

```
[root@localhost hda52]#  strings -t d /home/hasantha/hda52/hda52img.dd > /home/hasantha/hda52/all_strings
[root@localhost hda52]# grep -i 'xbox' /home/hasantha/hda52/all_strings > /home/hasantha/hda52/matches.txt
[root@localhost hda52]# 
```

Figure 8: Text Analysis
(-t requests for the offset of the string, d specifies the offset to be in Decimal notation, -i flag requests to ignore the case of the regular expression)

4.3.4: Recovering Deleted Files

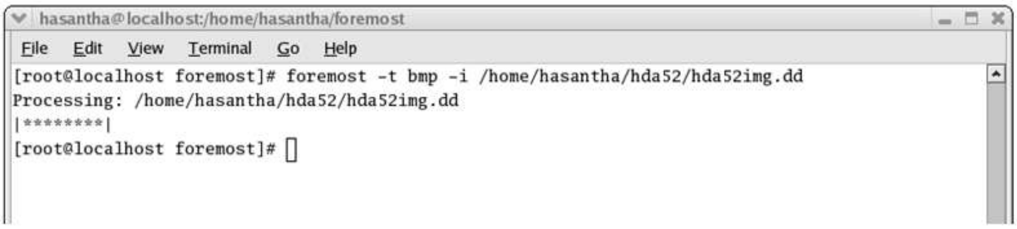
As already mentioned under 'File System of the Xbox', FATX marks deleted files with the value '0xE5' and removes the file pointer. But the file resides on the hard disk till it gets overwritten by another file. Therefore searching for the value ‘0xe5’ using a Hex editor would reveal any deleted files in FATX.



```
File: /home/hasantha/hda52/52tx   ASCII Offset: 0x00019350 / 0x2EDFFFFF (%00)
00019200  E5 00 63 72  79 73 69 73   38 2E 6A 70  67 FF FF FF   ..crysis8.jpg...
00019210  FF FF FF FF  FF FF FF FF   FF FF FF FF  FF FF FF FF   ................
00019220  FF FF FF FF  FF FF FF FF   FF FF FF FF  D3 04 00 00   ................
00019230  45 97 04 00  93 8B 87 12   50 8D 87 12  50 8D 87 12   E.......P...P...
```

Figure 9: Searching for the value '0xE5' using a hex editor would reveal any deleted files

As the FATX file system is not supported by the current Forensic suits, recovering the deleted files in terms of recovering their FAT information is not possible. Therefore file system independent data carving tools that recover deleted files using their file signatures (based on header and footer information) have to be occupied in order to recover any deleted files in an Xbox hard disk. Data carvers such as Scalpel, Foremost and Lazarus can be used for this purpose (Vaughan 2004).



```
[root@localhost foremost]# foremost -t bmp -i /home/hasantha/hda52/hda52img.dd
Processing: /home/hasantha/hda52/hda52img.dd
|********|
[root@localhost foremost]# 
```

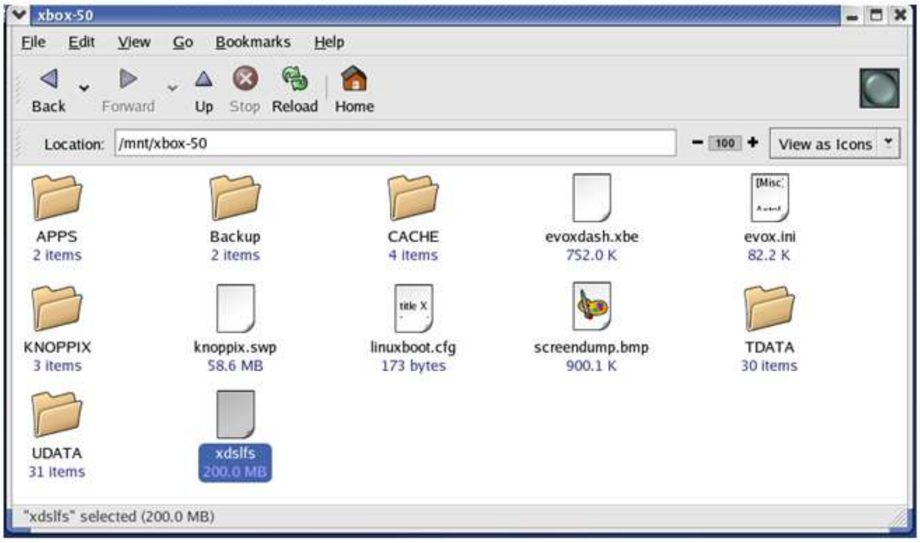
Figure 10: Using Foremost to recover deleted BMP files

4.4: Limitations of Xbox Forensics

This section would briefly point out the main limitations and drawbacks of the current approaches practiced in Xbox Forensics. In addition to the obvious limitations such as absence of ACPO guidelines for game consoles, yet alone for Xbox and lack of Microsoft support regarding FATX file system, the following limitations can be laid down:

- There is no proper forensic investigation suit that supports FATX file system. Therefore investigators have to conduct the analysis manually, not to mention that they have to rely on standard Linux commands such as String, Grep, Find, etc… and other low level tools such as hex editors to hunt for evidences.
- There is no forensically sound mechanism to image an Xbox memory unit as to yet. The Xbox memory units are not identified as standard USB devices by computers. As Burke and Craiger point out, one way to image an Xbox memory unit is by using a modified Xbox, but for that the memory unit has to be connected to the Xbox prior booting. But as already mentioned the Xbox would format any memory unit that does not contain game information while booting. Though the formatted data can be recovered using a data carver, it breaks the data integrity (Burke & Craiger 2006).
- During the installation of a Linux distribution, the installer prompts the user for the amount of disk space that he would like to allocate for Linux. Once the user specifies an amount, the installer creates a logical partition (or a file system) inside the actual Xbox partition. During an investigation, after mounting the Xbox partition, an investigator can browse through the whole file system, except through the logical partition that was created inside the actual partition. The logical file system appears as a one big file (instead as a directory structure). Therefore, if a criminal stores all his files inside this logical file system, the investigator

would not be able to access them. Despite of the author's best effort to mount this logical file system as a separate partition, the kernel does not identify it as a file system. Though this issue was not identified in any of the existing literature, this could prove to be fatal in real world investigations.



Location: /mnt/xbox-50

"xdslfs" selected (200.0 MB)

Figure 11: xdslfs is the logical file system created when installing XDSL Linux distribution. Once the user is in Linux, he is by default working inside this file system. But once mounted, xdslfs appears as a single file as oppose to a directory tree.

5: Conclusion

Not only the Modchips and exploits for the Xbox are inexpensive, but also they require very little technical knowledge to install. There are so many web sites who sells Modchips and provides all the exploited save game files and step-by-step guidance for modifying an Xbox. Once modified, the Xbox can be used to perform any PC like functionality. Therefore it is vital to treat an Xbox game console similar to a PC during an investigation of a crime.

But the Xbox forensic mechanisms and tools are still in their infancy. There are no clear published guidelines for Xbox forensics and even the available guides are based on information gathered from reverse engineering FAXT file system, rather than on direct information published by Microsoft. The available literature on Xbox forensics are mostly limited to specific versions of Soft modified Xboxes and there is a high possibility that those mechanisms may not work as intended on Hard modified Xbox and other Xbox versions.

As to yet, none of the current forensic utilities provides native FATX support. Therefore the current Xbox forensic approaches heavily rely on low level tools such as hex editors and standard Linux commands which can be very time consuming, not to mention their significant drawbacks such as inability to image memory units and to access the logical file system.

Xbox forensic still being in its infancy and new consoles such as Xbox 360 and PS3, who provide those PC like functionalities straight out of the box, coming into the market would undoubtedly provide additional pressure to the investigators. It is of utmost importance that the authorities, who currently seem to oversight the forensic value of these consoles, take prompt actions to develop frameworks and forensic tools to cater the FATX file system.

6: References

Burke, PK & Craiger, P 2006, ‘Xbox Forensics’, Journal of Digital Forensic Practice, National Center for Forensic Science, University of Central Florid, USA.

Burke, PK & Craiger, P 2006, ‘Xbox Media MD5 Hash List’. Retrived March 24, 2009, from http://www.ncfs.org/burke.craiger-xbox-media-hashlist.md5

Collins, D 2007, ‘XFT-A Forensic Tool for the Microsoft Xbox Game Console’, Proceedings of the 6th Annual Security Conference, The center of Excellence in Digital Forensics, Las Vegas, NV. Retrieved March 20, 2009, from www.security-conferece.org

SpeedBump 2002, ‘Xbox Hard Drive Locking Mechanism’. Retrieved March 22, 2009, from http://www.xbox-linux.org/wiki/Xbox_Hard_Drive_Locking_Mechanism

Steil, M 2005, ‘17 Mistakes Microsoft Made in the Xbox Security System’. Retrieved April 2, 2009, from http://events.ccc.de/congress/2005/fahrplan/attachments/591-paper_xbox.pdf

Steil, M 2003, ‘Difference between Xbox FATX and MS-DOS FAT’, Retrieved April 4, 2009, http://www.xbox-linux.org/wiki/Differences_between_Xbox_FATX_and_MS-DOS_FAT

Jeffris, CL 2002, ‘The Coroner’s Toolkit- in depth’, SANS Institute. Retrieved March 24, 2009, from http://www.sans.org/reading_room/whitepapers/incident/the_coroners_toolkit_in_depth_651?show=651.php&cat=incident

Vaughan, C 2004, ‘Xbox security issues and forensic recovery methodology (utilising Linux)’, Digital Investigation, Elsevier, UK.