

Forensic Analysis of a Sony Play Station 3 Gaming Console

Scott Conrad
conrad.scott@gmail.com

Greg Dorn
cg.dorn@gmail.com

J. Philip Craiger
philip@craiger.net

National Center for Forensic Science
12354 Research Parkway
Orlando, FL 32826

University of Central Florida

**Paper submitted for the 6th Annual Conference of the International Federation of
Information Processing**

Abstract

The Sony Playstation 3 (PS3) is a powerful gaming console that is expected to sell 75 million units by 2010. It provides much the same functionality as a typical desktop computer, and additionally provides the capability of playing Blu-ray movie disks, allows users to partition the hard drive and install a secondary operating system, and forces encryption for the primary hard drive that contains the gaming software. There are important forensic implications for the PS3 because of its ability to serve as a desktop computer, including its capability of accessing the Internet. In fact, a suspect in a criminal case involving child pornography has already used the PS3 for criminal intent. Unfortunately, little is known from a forensic perspective regarding the procedures for imaging and analysis of the PS3 and its media. In this paper we describe our exploratory research into the PS3 console. We describe several procedures, developed as a results of several dozen tests conducted on the PS3, that we believe would be valuable for a forensic examiner faced with examining a PS3 console.

Keywords

Sony Playstation 3, PS3, Gaming Console, forensic analysis, digital forensics

Introduction

The Sony PS3 was introduced to the Japanese and North American retail markets in November of 2006 (March 2007 for Europe) (1). It is estimated that 75 million consoles will be sold by 2010 (2). The PS3 marked Sony's entry into the seventh generation of game consoles, which also consists of the Nintendo Wii and the Microsoft Xbox 360. Each of these gaming consoles possesses many of the traits of a basic home computer; all are designed with internal storage, on-board memory, and multimedia capabilities and are Internet-ready. Furthermore, many game consoles are able to run operating systems (Linux-based) that are not native to their intended design, allowing them to additionally capabilities than originally conceived by their manufacturers (4, 5).

The latest game consoles are able to function much the same as a desktop computer. As such it is important to understand – as forensic scientists – forensically sound procedures available to support a forensic analysis on a game console that has been used for illegal purposes. Anecdotally we are aware of a few instances of game consoles being used for criminal purposes. Perhaps the most detailed incident involved a PS3. In early 2009, Anthony Scott Oshea of Somerset, Kentucky was arrested and charged with possessing child pornography after being tracked down by prosecutors in Houston, Texas (8). Oshea had received nude pictures of an 11-year-old girl that lived Houston, and thus was guilty of possessing child pornography (12). The pictures themselves were actually taken and e-mailed to Oshea by the little girl after he persuaded and manipulated her to do so. What made this case very unusual, though, was that Oshea did not own a desktop computer; rather, he perpetrated his crimes using a PS3.

The instance above demonstrates how seemingly benign devices like gaming consoles can be used for criminal purposes. It also highlights the need for forensically sound procedures for the imaging and forensic analysis of game consoles. Research has been performed and

published on the forensic analysis of game consoles including Xboxes (6, 10), the Nintendo Wii (9) and the Play Station Portable (7). For instance, research has been conducted on the Microsoft Xbox (6) as it relates to a forensic investigation or examination. In concept, the Xbox console is very similar to the PS3; both are gaming consoles with much of the same functionality as describe above. The Xbox, however, lacks the highly advanced structure and security of the PS3 (described below), making any forensic procedures created for the Xbox virtually useless as forensic procedures for he PS3. Unlike desktop computer technology, which is fairly standardized across manufacturers, game console technology tends to vary greatly in the components and software used. This makes it extremely difficult for the ‘typical’ (as of 2009) forensic examiner who may have no training or experience in dealing with novel devices such as game consoles. Interestingly, we have found no publication that describes research on forensic analysis of the PS3.

PS3 Architecture Overview

The PS3 is the most technically advanced system in the seventh generation of gaming consoles (17). The PS3 has undergone several changes since its initial release; as of late 2009 there have been a total of nine different Playstation models since its initial release. Each model change is reflected in its configuration of available USB ports, flash card readers, Super-Audio CD support, and hard drive size (11). The PS3 also contains a number of advanced components including Blu-ray disc drive for movie and game play, an extremely powerful CPU, the cell processor, and an Nvidia RSA graphics processing unit (GPU) (3).

Interestingly, Sony engineers designed the PS3 to allow users to partition the internal hard drive and install a secondary OS, typically a distribution of Linux (citation). This feature

was part of the standard architecture and did not require any modification of the device by the user as in other consoles; the Xbox and Wii have to be modified in order to place any other OS on the console (18, 19). Sony realized that end users would want this functionality and therefore provided this option to discourage modifying the console in ways that could divulge propriety information and lead to the overall ‘breaking’ of the system. Thus, a PS3 console may have two operating systems on it, the ‘Game OS’ (native OS) by Sony and a second, ‘Other OS’ (non native OS) installed by the user. Sony, however, restricts the Other OS partition size as well as limiting access to certain components. For instance, Sony limits the Other OS partition size to either 10GB large or [size of the hard drive – 10GB] large (5).

Impediments to Forensic Analysis of the PS3

There are several impediments to developing forensic procedures for the PS3. First, the game OS and file system for the PS3 are both proprietary, and it is unlikely that the technical details to the OS and file system will ever be publically released. Second, the largest obstacles to forensically analyzing the PS3 comes from the security measures, which Sony introduced to keep users from reverse engineering the console (as many users had done with other gaming consoles). The most notable of these measures is the encryption used for the hard drives. Each hard drive is encrypted specific to each console; this means that a hard drive from one console will not work if it is connected to another console (as described below). In many of the other gaming consoles such as Xbox and Wii, the OS or files system have been broken or hacked (modified) by end users (18, 19). As of late 2009 we know of no instances of a PS3 being modified in a similar manner. The combination of the hard drive encryption, proprietary OS, and file system make the task of decrypting a PS3 either problematic or perhaps impossible. This is

in stark contrast with normal hard drive encryption, where details about NTFS, EXT, or other files systems are widely known and thus an unencrypted hard drive is easily recognizable.

Although the Game OS partition is encrypted, the PS3 does not encrypt the Other OS partition (as described below). This means that files can be easily carved from the Other OS partition using forensic software. However, attempts to use forensic software (e.g., Encase or FTK) to identify the Other OS partition as containing a legitimate file system have not been successful (as described below). Specifically, the software is able to recognize the partition as an EXT file system, however, it is unable to read the EXT file system and provide the folder structure so the software shows it as unpartitioned space. Furthermore, Sony made it impossible to gain access to the Game OS partition from the Other OS running on the second partition, most likely prevented by security measures in the kernel or hypervisor.

Test Methodology

In the following section we describe our efforts to identify and establish best practices for forensically analyzing a PS3. All testing was performed with an 80GB PS3; model CECHK, purchased through an online retail store. No modifications of any kind were made to the console. The only an additional items used for the testing of the PS3 were a SATA extension cable, an additional 2.5" 120GB hard drive, a USB mouse and a USB keyboard. The PS3 was connected per instructions to an LCD HDTV via HDMI cable. Internet access was provided via Category 5 Ethernet cable connected to the Gigabit Ethernet port on the PS3 and attached to the Lab network. Additional PS3 consoles were brought in to compare and contrast results between console models; specific tests will note the additional PS3 and its model number. All tests involving an installation of Linux was done with Ubuntu Linux Desktop v. 8.10, with the default

configuration. We used a Knoppix bootable CD to zero out all hard drives prior to each test as an experimental control. We used a write blocker (Digital Intelligence UltraBlock (16)) for all imaging.

Encryption Test

This test was run to determine whether or not it would be possible to manually find a picture after it had been copied onto the PS3 (Game OS).

- Copied a JPEG picture onto a removable flash drive.
- Plugged the flash drive into the PS3, and copied the picture to the PS3's hard drive.
- Removed flash drive, shutdown the PS3, and removed the console's hard drive, subsequently we imaged the hard drive.
- Test Result: We used FTK's data carving tool to attempt to carve the JPEG from the image. FTK was unsuccessful in identifying files or folders on the partition.
- We then opened the JPEG on the lab computer using a hex editor. It was noted that the first 16 bytes of the picture was "FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 64". We used a hex editor to search for this string on the hard drive image, but it was unsuccessful.
- For redundancy, we also search for 16 bytes starting at offset 0x2000 in the picture (1C 7D 53 CB 45 C3 9F B5 6F 8E CC 9C 55 48 80 80). Again, no matches were found.
- Test results: This test suggests that files copied to the 'Game OS' partition are automatically encrypted when saved to the hard drive.

Timestamp Test

We conducted this test to determine if the PS3's hard drive is altered by simply turning the console on.

- The clean hard drive was removed and imaged.
- The hard drive was replaced into the PS3.
- The PS3 was turned on using the power switch on the back of the console was turn on and the power button on the front of the console was pressed.
- After 3 minutes, we used the power switch on the back to turn the console off.
- The hard drive was again removed and reimaged.
- Test results: We compared the two images. We found were numerous differences occurred in block-sized chunks randomly throughout the hard drive. The differences, however, were much more numerous in the beginning of the hard drive and became much more sparse farther down the hard drive. This test suggests that the console writes some kind of time stamp and/or random data to the hard drive every time it is powered on.

Write Blocker Test

We conducted this test to determine if the PS3's hard drive could be placed behind a write blocker before connecting it to the console.

- We removed the hard drive from the console, placed it behind a write blocker, and the write blocker was then plugged into the console.
- We turned on the system using the power switch. We found that the PS3 would “power up”, but it would not “boot up”. The console was clearly on and running, but the OS would never start up.
- We turned off the console and removed the write blocker, replacing it with a bridge that would allow writing. The PS3 would power up, boot up, and run normally.
- Test results: This test suggests that the console must be able to write to the hard drive before it will “boot up”, though it also shows that the hard drive does not need to be

directly connected to the console. Another security measure introduced by Sony is that a write blocker cannot be placed in-between the hard drive and the console; simply, the console must be able to write to the hard drive before it will boot properly.

Other OS Installation Test

We conducted this test determine any changes to the Game OS (native partition) when Linux is installed on the Other OS (non native partition).

- We created an image of the PS3 hard drive.
- We then partitioned the hard drive, making the Other OS partition to 10GB. We subsequently installed Linux on the Other OS partition.

We created a second image of the PS3 hard drive, which allowed us to compare the first and second images for any changes.

- Test results: We found that the start of the Linux partition is marked by a standard partition table. A search for '0x00000055aa' should always find the partition table The Other OS partition was located at the end of the hard drive, as one would expect. These results suggest that the Linux (or any other OS) can be easily located due to the fact that the Other OS partition, along with the partition table, is unencrypted.

Netcat Image Test

We conducted this test determine if the entire unencrypted hard drive image could be obtained by using the Linux commands *netcat* and *dd* to create and copy a forensic duplicate over the network while in the 'Other OS' is running.

- Installed Linux as the Other OS in the 10GB Other OS partition.
- Booted a second computer with a live Knoppix CD (20).

- We used *netcat* and *dd* to image the hard drive (called ps3da) while the PS3 was running the Other OS. We streamed the bits over the network to the lab computer.
 - The command used on the PS3 was ‘dd if=/dev/ps3da | nc [ip address of lab computer] [port number].’
 - The command used on the lab machine was ‘nc -l -p [port number] > [image name].’
- Shutdown the PS3, removed the hard drive, and imaged it.
- Compared the image obtained over the network and the image obtained by removing the hard drive.
- Test results: The results showed that the network image was only of the Linux partition and not of the whole hard drive. This test further suggests that the Game OS partition is inaccessible from the OS running on the Other OS partition.

Game OS Reinstallation Test

We conducted this test to determine changes when reinstalling the Game OS.

- We created a user account on the Game OS.
- We zeroed the hard drive.
- We attempted to reinstall the Game OS.
 - Note: In the CECHK model (newer PS3 model), the hard drive had to be reformatted, the Game OS had to be reinstalled, and the user account had to be recreated
 - Note: In the CECHE model, the hard drive had to be reformatted, but the gaming OS did not have to be reinstalled and the user accounts did not have to be recreated

- Test results: This test suggests that between the two different models of the PS3, the OS and user data is stored in different places. In the CECHK model (a newer model) it is stored on the hard drive, in the CECHE model (an older model) it is stored in memory on the motherboard.

Backup Utility Test

We conducted this test to determine what happens when the backup utility is used.

- Download several pictures and bookmarked several websites using the built in PS3 web browser.
- Zeroed a second hard drive and formatted it with FAT32 file system.
- Connected the FAT32 hard drive to the PS3 via a USB port
- We then used the PS3 backup utility to back up the data from the PS3 hard drive to the FAT32 hard drive. The backup data was about 4GB in size, and the file names of the backup were the date/time of the backup
- We created an image of the FAT32 hard drive was taken and the image was uploaded into FTK. FTK was unable to carve any picture files, but it did find the backup files.
- We loaded the image into a hex editor and searched for website URLs.
- Test results: The searches were unsuccessful, and no bookmarks were located. This test suggests that no relevant data that can be manually carved from the backup files. It is unknown whether this is because the backup files are encrypted in the same way the hard drive is, or if the backup files use a propriety format that only the PS3 can decipher.

VM Test

We conducted this test to determine if the Linux partition could be manually carved out, placed within a virtual machine, and then run normally within the VM.

- Installed Linux on the 10GB Other OS partition.
- Imaged the hard drive.
- Used a hex editor to carve the Linux partition from the image.
- We then used ProDiscover 5, Live View, and VMWare converter to convert the carved image into a format that would be bootable with VMWare.
- Test results: Unfortunately, all attempts to boot the carved partition from within VMWare were unsuccessful. FTK (v1.7) and Encase (v5) were unable to recognize the file system of the Linux partition; therefore this test is ultimately inconclusive. We are conducting further research to determine if and how the Other OS partition can be carved out so that it can be placed in a virtual machine to be run on a standard computer and/or be recognized by forensic software.

Browser Test

We conducted this test was used to determine the number of websites URLs kept in the PS3's built-in browser history.

- Started the built-in web browser and randomly visited websites
- After each website visit we checked the history to identify changes
- Test results: We found that the web browser keeps the last 100 unique websites in its history. Websites at the top of the list are the most recently visited sites and websites at the bottom of the list are the least recently visited. If the same site is visited more than once there will not be multiple entries, but instead the same entry will simply move up in the list. Once the 101st website is visited it will be placed into the history (at the very beginning), but the very last website in the history will not be removed until the 101st

website has fully loaded; thus it is possible for there to be 101 websites in the history if the web browser was forced to close before the 101st website was fully loaded.

Hard Drive Swap Test

We conducted this test to determine if we could swap two PS3s hard drives between two PS3 consoles, and allow us to boot into Linux on both.

- We installed Linux on both hard drives (10GB Other OS partition)
- We set both drives to boot into the Linux partition by default
- We shut down the consoles and switched the hard drives.
- Test results: Neither console was able to boot. Both consoles prompted us to reformat the unrecognized hard drives. This test suggests that even though a PS3 can be set to boot directly into the Linux partition without having to boot into the Game partition first and that the Linux partition is not encrypted like the Game partition is, the hard drive will still be checked to make sure that it belongs to that specific console before the PS3 will boot into either OS.

Hard Drive Decryption Test

We conducted this test to determine if a PS3 hard drive could be plugged into a PS3 running Linux and have its hard drive automatically decrypted.

- We prepared two hard drives, one was set aside while the other was repartitioned (10GB Other OS partition) and had Linux installed onto it.
- We placed the Linux hard drive into the PS3 and booted the console into Linux.
- Connected the second drive using a bridge to the PS3's USB port.
- Test results: The PS3, while running Linux, was able to see the other hard drive (connected though the bridge), but was unable to read its contents because it was not

automatically decrypted. The theory behind this test was that if an encrypted hard drive was plugged into the PS3 that encrypted it, the console would recognize the encryption and automatically decrypt the hard drive. This was unfortunately not the case.

Results

Our test results suggest that Sony has successfully locked-down the PS3 to the point where no normal or standard forensic methods would work properly. The hard drive is encrypted; the Other OS can be carved out, but no software can read the file system; the Game OS is completely inaccessible from the Other OS; and hard drives can only be read by their respective consoles. No method of attack that was tested managed to break the security measures developed by Sony.

Proposed Forensics Methods

Following the results of the aforementioned tests we proposed the following process as a suitable substitution for traditional forensics methods used when obtaining digital evidence during an investigation of a PS3. Our research suggests that the only means to view the encrypted data of the PS3 is to view it natively through the device in which it was obtained.

This process requires both the original PS3 and the hard drive to that specific PS3

1. Take the original hard drive and while using a write blocker, hash the hard drive and then copy it at the bit level to a blank hard drive of the same size.
2. Set the original hard drive aside (it won't be used) and hash the copy hard drive to ensure it is a perfect copy
3. Plug the copy hard drive back into the PS3

4. Use the PS3 natively to record all setting information and to search through the Game OS for any files, including in the web browser. Ensure that each step is carefully documented. The use of video capturing software/ applications is suggested so that all steps used during the examination can be captured in real-time (14).

This process allows for the evidence (the original hard drive) to be preserved while also allows for the forensic investigation to be repeatable. Furthermore, the video capturing software/applications provides accountability towards the investigator by showing that no steps taken during the investigation could have manipulated the data in a way that would compromise the integrity of the case.

Future work

Sony has provided several updates to the PS3 firmware. These updates increase the functionality the PS3 numerous ways, from enhanced game play to added features in file sharing (13). Therefore, the PS3 becomes a dynamic machine, providing forensic examiners with increasing challenges to face in recovering data from the console.

As the PS3 becomes more commonplace in homes, it is likely that attempts will be made to create viruses or attacks geared toward the architecture of the console. At this time, there are no known viruses for the Game OS of the PS3, though companies such as Trend Micro have released software to protect the PS3 from harmful and inappropriate content (15). It is not known whether the Linux (or Other) OS can become infected with a virus, though due to the PS3's unique underlying architecture, it would be very unlikely that such viruses exist.

Because current forensic software is unable to read the file system of a PS3 (both the Game OS and Other OS), additional research will be needed so that this functionality can be

provided in a manner that is forensically sound and accepted. Current methods, manually carving out the data, can only go so far in recovering needed data from the console.

Conclusion

The PS3 is a powerful and adaptive gaming console that can be used for a variety of tasks outside of playing games. To that end, a forensic analysis of this console has become a necessity in order to provide agencies involved with investigations or examinations of the PS3 with as much information as possible. The research has shown that the PS3 to be extremely well designed to prevent any of its proprietary material from being accessed by anyone other than Sony. The inability to access any data from the PS3 through traditional forensic methods has forced the development of alternative means to access this data. Furthermore, agencies could possibly find themselves working with Sony directly in order to obtain data from the PS3 when all other approaches have been unsuccessful.

References

1. Wikipedia. PlayStation 3. http://en.wikipedia.org/wiki/PlayStation_3. (Last accessed: January, 2009)
2. Surette, Tim. Research firm: 75 million PS3s sold by 2010. <http://www.gamespot.com/news/6163625.html>. January 2, 2007. (Last accessed: July, 2009)
3. Sony. PLAYSTATION®3 80GB System. <http://www.us.playstation.com/PS3/Systems/TechSpecs/default.html>. (Last accessed: February, 2009)
4. Sony. Install Other OS. <http://manuals.playstation.net/document/en/ps3/current/settings/osinstall.html>. (Last accessed: February, 2009)

5. Sony. Overview of the Open Platform for the PLAYSTATION®3 system.
<http://www.playstation.com/ps3-openplatform/index.html>. (Last accessed: January, 2009)
6. Burke, Paul K. and Craiger, Philip, 'Xbox Forensics', Journal of Digital Forensic Practice, 1:4, 275 – 282. 2007.
7. Conrad, Scott, Rodriguez, Carlos, Marberry, Chris, and Craiger, Philip. 'PSP Forensics', Advances in Digital Forensics V.
8. Potter, N. Playstation sex crime: Criminal used video game to get naked girl's pictures.
<http://abcnews.go.com/Technology/Story?id=7009977&page=1>. March 13, 2009. (Last accessed: August 4, 2009).
9. Turnbull, Benjamin. Forensic Investigation of the Nintendo Wii: A First Glance.
http://www.ssddfj.org/papers/SSDDFJ_V2_1_Turnbull.pdf. June, 2008. (Last accessed: March, 2009)
10. Vaughan, Chris. Xbox security issues and forensic recovery methodology (utilising Linux).
http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B7CW4-4D6364M-4&_user=2139851&_rdoc=1&_fmt=&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=973837661&_rerunOrigin=google&_acct=C000054275&_version=1&_urlVersion=0&_userid=2139851&md5=5cfe674211c476e8c263539c7fcf962d. August 27, 2004. (Last accessed: July, 2009)
11. Sony. PLAYSTATION®3 System Frequently Asked Questions.
<http://www.us.playstation.com/PS3/Systems/FAQs>. (Last accessed: February, 2009)
12. Penal Code. Title 9. Offenses Against Public Order And Decency Chapter 43. Public Indecency. <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.43.htm#43.26>. (Last accessed: July, 2009)

13. Sony. PLAYSTATION®3 System Software Update. <http://www.us.playstation.com/Support/SystemUpdates/PS3>. (Last accessed: February, 2009)
14. Pinnacle Systems. Dazzle Video Creator Plus. http://www.amazon.com/Pinnacle-Systems-82301006461-Dazzle-Creator/dp/B001C5DOWI/ref=sr_1_1?ie=UTF8&s=software&qid=1247674193&sr=8-1. (Last accessed: April, 2009)
15. Chalk, Andy. PlayStation 3 Anti-Virus Software Released. <http://www.escapistmagazine.com/news/view/79054-PlayStation-3-Anti-Virus-Software-Released>. November 16, 2007. (Last accessed: May, 2009)
16. Digital Intelligence. UltraBlock eSATA IDE-SATA Write Blocker. http://www.digitalintelligence.com/products/ultrablock_esata_ide-sata_ro/. (Last accessed: August, 2009)
17. Wikipedia. History of video game consoles (seventh generation). [http://en.wikipedia.org/wiki/History_of_video_game_consoles_\(seventh_generation\)](http://en.wikipedia.org/wiki/History_of_video_game_consoles_(seventh_generation)). (Last accessed: January, 2009)
18. Huang, Andrew. Hacking the Xbox. <http://hackingthexbox.com/>. 2003. (Last accessed: May, 2009)
19. Five Things to Know Before You Modify Your Wii. http://www.associatedcontent.com/article/776395/five_things_to_know_before_you_modify.html?cat=15. May 28, 2008. (Last accessed: August, 2009)
20. Knoppix. <http://www.knoppix.net/>. (Last accessed: July, 2009)