Forensic Analysis of a PlayStation 3 Console

Scott Conrad, Greg Dorn, Philip Craiger

Chapter 5

FORENSIC ANALYSIS OF A PLAYSTATION 3 CONSOLE

Scott Conrad, Greg Dorn and Philip Craiger

Abstract The Sony PlayStation 3 (PS3) is a powerful gaming console that supports Internet-related activities, local file storage and the playing of Blu-ray movies. The PS3 also allows users to partition and install a secondary operating system on the hard drive. This "desktop-like" functionality along with the encryption of the primary hard drive containing the gaming software raises significant issues related to the forensic analysis of PS3 systems. This paper discusses the PS3 architecture and behavior, and provides recommendations for conducting forensic investigations of PS3 systems.

Keywords: Sony PlayStation 3, gaming console, forensic analysis

1. Introduction

The Sony PlayStation 3 (PS3) hit the Japanese and North American retail markets in November 2006 (March 2007 in Europe) [13]. It is estimated that 75 million consoles will be sold by 2010 [14]. The PS3 marked Sony's entry into the seventh generation of game consoles, which also includes the Nintendo Wii and Microsoft Xbox 360. These gaming consoles possess many of the traits of an Internet-ready home computer; all are designed with internal storage, on-board memory and multimedia capabilities. Furthermore, many of the game consoles can run non-native operating systems (typically Linux-based operating systems), providing them with capabilities beyond those conceived by their manufacturers [8, 10].

Because game consoles provide the same functionality as desktop computers, it should come as no surprise that they have been used in the commission of crimes. An example is the 2009 case of Anthony Scott Oshea of Somerset, Kentucky, who was arrested and charged with pos-

sessing child pornography [6]. Investigators discovered that Mr. Oshea's PS3 contained nude pictures of an 11-year-old girl from Houston, Texas; he was eventually convicted of the child pornography charge.

This case and others underscore the need for forensically-sound procedures for the imaging and forensic analysis of (seemingly benign) game consoles with advanced capabilities. Other researchers have focused on the forensic analysis of seventh generation game consoles, including the Xbox [1, 17], Nintendo Wii [16] and PlayStation Portable [3]. The Xbox console has similar functionality as the PS3. However, it lacks the advanced structure and security features of the PS3. Thus, the forensic procedures developed for the Xbox have little, if any, applicability to the PS3.

Another complication is that, unlike desktop computers, game consoles tend to vary greatly in their hardware and software components. This makes it extremely difficult for most forensic examiners to analyze game consoles. Indeed, as of late 2009, no published research exists related to the forensic analysis of the PS3. This paper describes our research on the PS3 system with a focus on developing forensically-sound imaging and analysis procedures.

2. PlayStation 3 Architecture

The PS3 is the most technically advanced system in the seventh generation of gaming consoles [7]. From its initial release in 2006 to 2009, there have been nine different PlayStation models. Each model differs in the configuration of its USB ports, flash card readers, Super-Audio CD support and hard drive size [11]. Each of these differences has potential implications for forensic analysis. The PS3 also incorporates several advanced components, including a Blu-ray disc drive for movies and games, an extremely powerful cell processor (CPU), and an Nvidia RSA graphics processing unit (GPU) [11].

Interestingly, Sony engineers designed the PS3 to allow users to partition the internal hard drive and install a secondary operating system (OS) – typically a distribution of Linux [10] – as long as the OS is capable of supporting the PowerPC architecture. This feature is part of the original design and does not require any modification of the device by the user. In contrast, the Xbox and Wii have to be modified (hacked) in order to install a different OS [5, 15]. Sony's design rationale was that users would desire this feature and providing it would discourage users from modifying the PS3 console in a manner that would release proprietary information or software.

In general, a PS3 console may contain two operating systems: Sony's "Game OS" (native OS) and a second "Other OS" (non-native OS) installed by the user. Note, however, that the PS3 design restricts the size of the Other OS partition to either 10 GB or the difference between the hard drive size and 10 GB [10]; access to certain components is also limited. The ability to install a secondary operating system has been eliminated in the latest (CECH-2000) version of the PS3 [9].

3. Impediments to Forensic Analysis

There are two main impediments to developing forensic procedures for the PS3. First, the PS3 Game OS and file system are proprietary, and it is unlikely that their technical details will be released. Second, security-related measures, such as the mandatory encryption of the Game OS partition, increase the difficulty of recovering evidence.

Some users have modified (hacked) gaming consoles such as the Xbox and Wii [5, 15]; however, these consoles do not use encryption like the PS3. The combination of hard drive encryption and proprietary OS and file system make the task of decrypting a PS3 hard drive problematic, if not impossible. As of late 2009, we know of no case involving the modification of a PS3 system. However, the PS3 does not encrypt the Other OS partition. This means that files located on the non-native OS partition may be identified and recovered.

4. Test Methodology

The forensic tests were performed on an 80 GB CECHK PS3 model purchased from a retail outlet. Several console models were investigated to compare and contrast the results. No modifications of any kind were made to the consoles. The other items used in the tests were a SATA extension cable, an additional 2.5 inch 120 GB hard drive, a USB mouse and a USB keyboard.

The PS3 was connected as stipulated in the instruction manual to an LCD HDTV using an HDMI cable. Internet access was provided via a Category 5 Ethernet cable connected to the Gigabit Ethernet port on the PS3 and attached to the laboratory network. The Other OS was a Ubuntu Linux Desktop v. 8.10. A Knoppix bootable CD was used to zero out the hard drives prior to each test as an experimental control. A Digital Intelligence UltraBlock write blocker was used during imaging.

4.1 Control Boot Test

The first test was conducted to determine if merely turning on (i.e., booting) the PS3 would write to the hard drive. A zeroed hard drive was

set up using the PS3; the drive was then removed and imaged. Next, the hard drive was placed back in the PS3 and the console powered up. After approximately three minutes, the console was powered down and the hard drive was removed and imaged. A hex editor was used to compare the two hard drive images.

We found numerous differences between the two images. The differences appeared to occur randomly in block-sized chunks throughout the image. However, they were more numerous towards the beginning of the hard drive and much sparser farther down the drive. Thus, the console writes to the hard drive every time it is powered up. From a forensic standpoint, it is, therefore, important that the hard drive always be removed and imaged using a write blocker. Of course, this is standard operating procedure for traditional laptops and desktop computers.

4.2 Write Blocker Test

This test was conducted to determine if the PS3 software could be executed when a write blocker is placed on the hard drive. The hard drive was removed from the console and placed behind a write blocker. The write blocker was then connected to the console and the system powered up.

We discovered that the PS3 would power up, but not boot up. We turned off the console and removed the write blocker, replacing it with a bridge, the UltraDock Drive Dock (version 4), which would allow writing. The PS3 was then able to power up, boot up and run normally.

The test results suggest that the console must be able to write to the hard drive in order to boot properly (possibly a security measure introduced by Sony). The results also show that the hard drive does not have to be connected directly to the console in order for the PS3 to run.

4.3 Other OS Installation Test

This test was conducted to track the changes that occur to the hard drive when Linux is installed in the Other OS (non-native) partition. A zeroed hard drive was set up using the PS3, and then removed and imaged. Next, the hard drive was inserted back into the PS3 and a 10 GB Other OS partition was created; Linux was immediately installed on this new partition. The hard drive was then removed and imaged, and the two images were compared using a hex editor.

We discovered that the start of the Linux partition is marked by a standard partition table (searching for `0x00000055aa` finds the partition table). Also, as one would expect, the Other OS partition is located at the end of the hard drive. The results suggest that the Linux (or other)

OS is easily located because the Other OS partition and its partition table are not encrypted.

4.4 Imaging over a Network Test

This test was conducted to determine if an unencrypted hard drive image could be obtained. The PS3 was booted into Linux, and `netcat` (a networking service for reading from and writing to network connections) and `dd` (a program for low-level copying and conversion of raw data) were used to create and copy a bit-for-bit image of the hard drive over the network. Next, a second computer (Dell Optiplex 755) was booted using a Knoppix Live CD. The `fdisk` command was used to identify hard disk and partition information.

We discovered that the Linux OS is installed and runs in a partition named `ps3da`. Furthermore, there are only three available partitions (all Linux) with `ps3da` as the boot partition.

Next, `netcat` and `dd` were used to image the hard drive with the PS3 running under Linux. The bits were streamed over the network to the Dell 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 Dell computer was:

```
nc -l -p [port number] | [image name]
```

The PS3 was powered down after the imaging was completed, and the hard drive was removed and imaged. Comparison of the two images showed that the image obtained over the network is only of the Linux partition and not of the entire drive. The test results suggest that the Game OS partition is inaccessible from an OS running on the Other OS partition.

4.5 Game OS Reinstallation Test

This test was conducted to identify the differences between two PS3 models, CECHK (2008) and CECHE (2007). Changes in the architecture, functionality and behavior of a game console can have significant implications with regard to forensic imaging and analysis. It is, therefore, very important to understand the differences across models.

For this test, the same user account was created on the two PS3s. The hard drives in the two consoles were removed and zeroed, and then replaced in their respective consoles. Upon powering up the systems, we discovered that the newer CECHK model requires the hard drive to be reformatted, the Game OS to be reinstalled and the user account to be recreated (Figure 1). On the other hand, the older CECHE model only requires the hard drive to be reformatted.

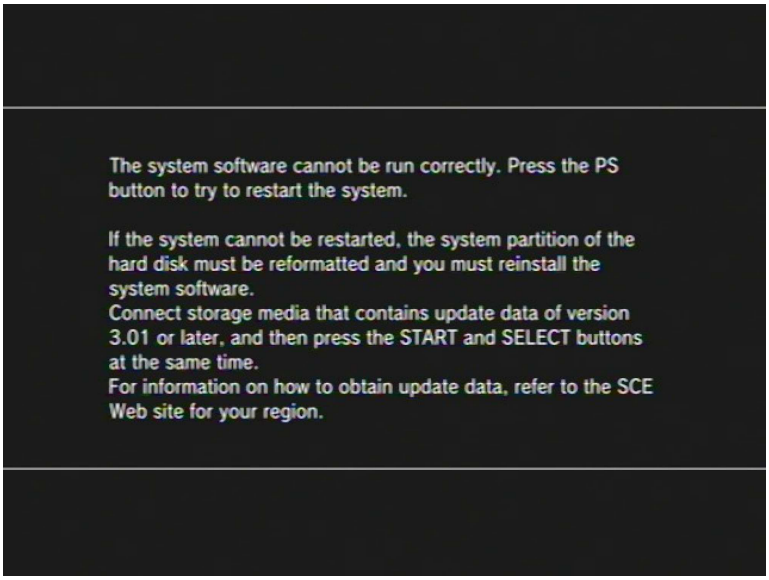

Figure 1. Error message to reformat drive.

The results suggest that significant differences in PS3 architecture and behavior may exist between models. Also, the OS and user data are stored in different locations in different models. The newer CECHK model stores data on the hard drive while the older CECHE model stores data in memory on the motherboard.

4.6 Backup Utility Test

This test was conducted to determine what happens when the PS3 backup utility is used to backup the hard drive to a secondary location. The built-in PS3 web browser was used to download several images and bookmark several websites. A second external hard drive was zeroed and formatted with the FAT32 file system. The external hard drive was then connected to the PS3 via a USB port and the PS3 backup utility was used to save the data from the PS3 to the FAT32 hard drive.

Our analysis revealed that the backup has a folder/file structure whose size depends on the amount of data saved on the current hard drive. The name of the folder in the backup is based on the date/time of the backup (e.g., 200910201325). The files contained in the backup are titled "archive" and numbered to differentiate between them; all the files have the `.dat` extension corresponding to data files [4].

The external hard drive was subsequently imaged and examined using AccessData's FTK suite (version 1.80). However, FTK was unable

to identify or recover any images from the backup files. Next, a hex editor was used to search for website URLs in the image, but none were located. These results suggest that data cannot be manually recovered from a PS3 backup file (at least for the model tested). It is possible that this is because the backup files are encrypted like the hard drive. Alternatively, the backup files may use a propriety format that only the PS3 can decipher.

4.7 Hard Drive Swap Test 1

This test was performed to determine if the hard drives of two different PS3 consoles (CECHK and CECHE models) can be swapped. A zeroed hard drive was installed in the CECHK console, the system was powered up and the hard drive was formatted using the PS3. The PS3 was then shut down, and the newly formatted hard drive was removed from the CECHK console and installed in the CECHE console. Although the CECHE console did power up, it required the hard drive to be formatted before use.

The test was then reversed. The CECHE console was used to format a zeroed hard drive, which was installed in the CECHK console. Once again, the hard drive had to be formatted before it could be used. The results suggest that a PS3 checks that the hard drive belongs to the specific console before it will boot.

4.8 Hard Drive Swap Test 2

This test was conducted to determine if the hard drives of two different PS3 consoles (CECHK and CECHE models) can be swapped and booted under Linux. A hard drive was zeroed and installed in the CECHK console, the system was powered up and the hard drive was formatted using the PS3. Linux was installed in the Other OS partition of the drive.

The system was restarted to boot under Linux instead of the Game OS. The CECHK console was then powered down and the hard drive removed. Next, the hard drive was installed in the CECHE console and the system was powered up. As in the case of the Hard Drive Swap Test 1, the hard drive had to be formatted before use.

The test was then reversed. The CECHE console was used to format a zeroed hard drive, which was installed and tested in the CECHK console. Once again, the hard drive required formatting before use.

The results suggest that although a PS3 can be set to boot directly into the Linux partition without having to boot into the Game OS partition and that the Linux partition (unlike the Game OS partition) is

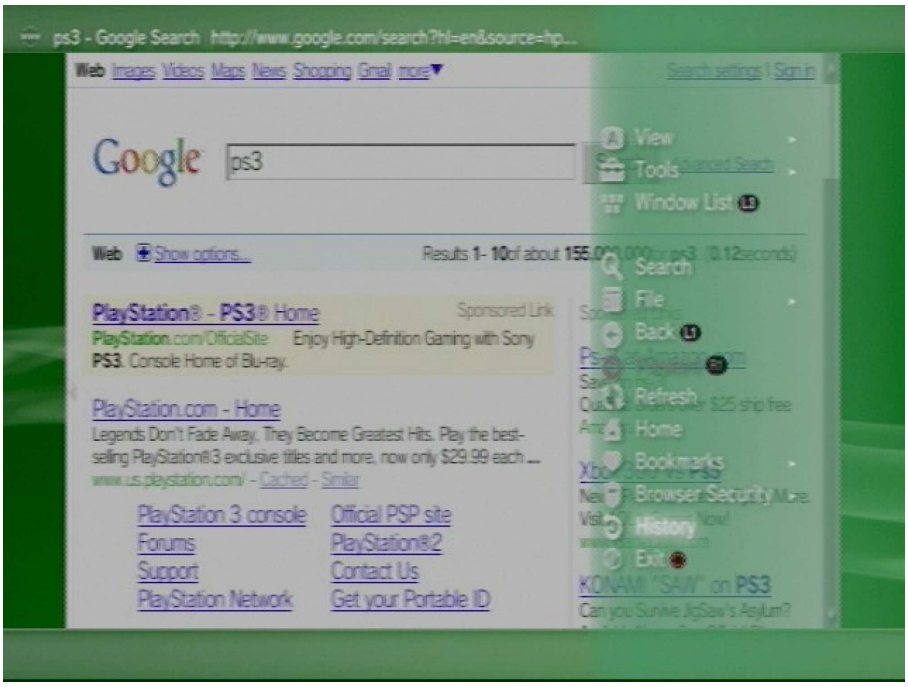

Figure 2. Accessing the browser history.

not encrypted, the hard drive is nevertheless checked to ensure that it belongs to the specific console before the PS3 will boot.

4.9 Browser Test

This test was performed to determine the number of website URLs that are maintained in the browser history. The browser was used to visit random websites and the browser history was checked to identify the changes after each website was visited (Figure 2).

The results indicate that the browser maintains the last 100 unique websites in its history with the most recently visited URLs at the top of the list (Figure 3). Only one entry is maintained for a site that is visited multiple times; however, the entry moves up the list each time it is accessed. At interesting quirk is that 101 URLs can sometimes be maintained in the browser history. This occurs because each newly-visited URL is added to the history list at the time the website is accessed, but the least recent URL is not deleted until the website has loaded completely. Thus, the browser history can contain 101 URLs if the browser is forced to close before the 101st website is loaded.

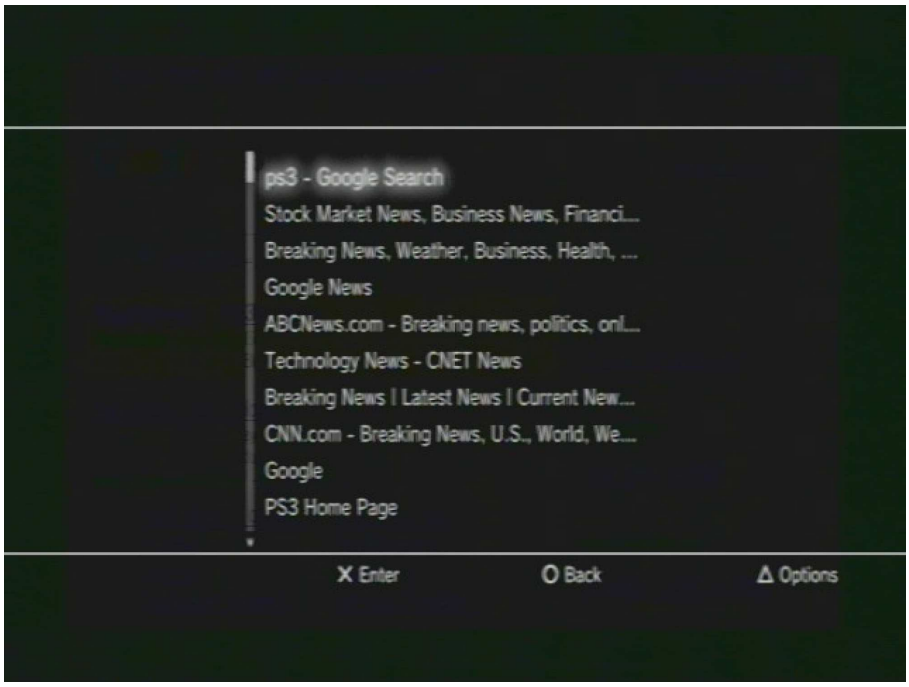

Figure 3. Browser history list.

4.10 Hard Drive Decryption Test

This test was performed to determine if an encrypted PS3 hard drive can be decrypted or read by attaching it externally to the same PS3 that originally encrypted it. Essentially, the goal of the test was to see if a PS3 could read its own hard drive.

The test used two hard drives, one formatted with only the Game OS and the other formatted with a 10 GB Other OS partition containing Linux. The Linux hard drive was inserted into the PS3 and the console was booted into Linux. The second hard drive was then attached to the UltraDock and connected to the PS3 via a USB port. The PS3 running Linux attempted to mount the newly attached drive, but failed every time. The hard drive contents could not be read and, thus, the drive was very likely not automatically decrypted.

5. Evidence Recovery Procedure

The test results suggest that Sony has locked down the PS3 to the point where standard forensic methods do not work. The hard drive is encrypted; the Other OS can be carved out, but the file system cannot

be read. The Game OS is completely inaccessible from the Other OS and hard drives can only be read by their respective consoles.

None of the techniques employed were able circumvent the security measures. This does not mean that the PS3 is impenetrable; it is just that the information available at this time is insufficient to defeat the security measures.

Based on the test results, the only means to view encrypted data on a PS3 is to view it natively using the same device. This is the basis of a procedure for obtaining digital evidence from a PS3, which is a reasonable substitute for a traditional forensic method. The evidence recovery procedure, which requires the original PS3 and the hard drive specific to the PS3, involves the following steps:

- Connect a write blocker to the original hard drive. Compute a hash of the hard drive and make a bit-for-bit copy of the drive to a zeroed hard drive of the same size.
- Secure the original hard drive in an evidence locker because it will not be used again. Compute a hash of the copied hard drive in order to check that it is a perfect copy.
- Install the copied hard drive in the PS3.
- Use the PS3 natively to record all settings and to search through the Game OS for files (including in the web browser). Document each step carefully using a video capturing device or application.

This procedure allows for the evidence (original hard drive) to be preserved while allowing its contents to be viewed. The investigation is repeatable because there is no limit to the number of copies that can be made. Capturing the entire procedure on video provides documentation and accountability. This is important because it is inevitable that the copied hard drive will be changed in some manner as demonstrated by the Control Boot Test (Section 4.1), and this cannot be prevented as demonstrated by the Write Blocker Test (Section 4.2).

6. Conclusions

The procedure for obtaining digital evidence from a PS3 serves as a reasonable substitute for a traditional forensic method. Because commercially-available forensic software is unable to read the Game OS and Other OS file systems, additional research is needed to develop a more comprehensive procedure. Traditional methods, such manually carving the data, can only go so far in recovering data from the PS3.

Currently, the PS3 is primarily used for gaming. However, Sony is constantly updating the PS3 firmware to provide new features ranging from enhanced game playing to file sharing and online access [12]. It is certain that attempts will be made to create PS3 viruses and develop attacks that exploit PS3 vulnerabilities. To our knowledge, no viruses exist that target the Game OS and Other OS; however, companies such as Trend Micro have released software to protect PS3s from harmful and inappropriate content [2].

The constant upgrades to the Sony PS3 functionality will only increase the likelihood that these devices will be used in the commission of crimes. Forensic investigators need sophisticated techniques and tools to analyze PS3s and other game consoles. We hope that our research stimulates will renewed efforts in this direction.

References

[1] P. Burke and P. Craiger, Xbox forensics, *Journal of Digital Forensic Practice*, vol. 1(4), pp. 275–282, 2006.

[2] A. Chalk, PlayStation 3 anti-virus software released, *The Escapist*, November 16, 2007.

[3] S. Conrad, C. Rodriguez, C. Marberry and P. Craiger, Forensic analysis of the Sony PlayStation Portable, in *Advances in Digital Forensics V*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 119–129, 2009.

[4] FileInfo.com, `.dat` file extension (www.fileinfo.com/extension/dat).

[5] A. Huang, Hacking the Xbox (hackingthexbox.com), 2003.

[6] N. Potter, PlayStation sex crime: Criminal used video game to get girl's naked pictures, ABCNews.com, New York (abcnews.go.com /Technology/Story?id=7009977&page=1), March 13, 2009.

[7] Seeking Alpha, Seventh generation gaming consoles: Thinking outside the Box (seekingalpha.com/article/22075-seventh-generation-gaming-consoles-thinking-outside-the-box), December 11, 2006.

[8] Sony Computer Entertainment, Install other OS, Foster City, California (manuals.playstation.net/document/en/ps3/current/settings/osinstall.html).

[9] Sony Computer Entertainment, New slimmer and lighter PlayStation 3 to hit worldwide market this September, Foster City, California (www.us.playstation.com/News/PressReleases/525), 2009.

[10] Sony Computer Entertainment, Open platform for PlayStation 3, Foster City, California (www.playstation.com/ps3-openplatform /index.html).

[11] Sony Computer Entertainment, PlayStation 3 80 GB system, Foster City, California (www.us.playstation.com/PS3/Systems/TechSpecs/default.html).

[12] Sony Computer Entertainment, PlayStation 3 system software update, Foster City, California (www.us.playstation.com/Support/SystemUpdates/PS3).

[13] Sony Computer Entertainment, Support: Knowledge Center, Foster City, California (playstation.custhelp.com/app/answers/detail/a_id/232).

[14] T. Surette, Research firm: 75 million PS3s sold by 2010, GameSpot, CBS Interactive, San Francisco, California (www.gamespot.com/news/6163625.html), January 2, 2007.

[15] TechTips, Five things to know before you modify your Wii, Associated Content, New York (www.associatedcontent.com/article/776395/five_things_to_know_before_you_modify.html?cat=15), May 28, 2008.

[16] B. Turnbull, Forensic investigation of the Nintendo Wii: A first glance, *Small Scale Digital Forensics Journal*, vol. 2(1), pp. 1–7, 2008.

[17] C. Vaughan, Xbox security issues and forensic recovery methodology (utilizing Linux), *Digital Investigation*, vol. 1(3), pp. 165–172, 2004.