Exploring the Effectiveness of Digital Forensics Tools on the Sony PlayStation Vita

Karolina Alvarez and Masooda Bashir(✉)

University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
karolina.a.alvarez@gmail.com, mnb@illinois.edu

Abstract. As gaming consoles become more advanced, their capabilities increase and they can store more information on the users. Because of this, they are becoming viable sources of forensic evidence. This research contributes to the little-explored and growing field of video game console forensics through the examination of current forensic tools on the Sony PlayStation Vita. These tools were used to analyze backups created by the device to better understand the new file types, and what data are stored in them and how. Although most of the files were encrypted, valuable metadata could be acquired from them.

Keywords: Digital forensics · Sony PlayStation Vita · PS Vita · Video game console forensics

1 Introduction

Modern gaming systems are becoming more and more like personal computers. Their functionality and the type of data they store make them potential sources of evidence for criminal investigations. Such data include not only game logs with timestamps, but also personal information, internet history, credit card information, location, pictures, and videos. There have been several instances where gaming consoles have been used for criminal purposes, and became sources of incriminating evidence, especially for child pornography cases. There have been cases where young children were contacted through messaging services on video game consoles and bribed into sending nude pictures [1]. In one case, the only evidence of the crime existed on the gaming console [11]. There have been other cases where gaming logs were used to undermine an alibi or shed new light on a case [2]. However, despite the multitude of information available in gaming systems, investigators have difficulty finding and extracting it in a forensically sound manner. Accessing the contents directly through the console may tamper with the evidence, and typical digital forensics analysis is difficult due to the differences between gaming consoles and regular computers. As a result, investigators typically turn to online forums for advice. They may use community-created tools to view the content, but even those are unable to unveil everything [2]. Because gaming console forensics is still a new field, there is much to learn about how data are stored on these systems. The purpose of this research is to perform preliminary forensics analysis on the Sony PlayStation

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 200–206, 2015.
DOI: 10.1007/978-3-319-25512-5_14

Vita (PS Vita) in order to understand what can be read and accessed using current digital forensic tools.

2 Device Information

From its release in December 2011 to January 2013, over 4 million PS Vitas have been sold worldwide [15]. As with most video game consoles, the technical detail about the operating system and file system of the PS Vita are not publicly released, but various other information is available. As of 2015, there have been 3 models of the PS Vita. The first generation consisted of two models: one with 3G and Wi-Fi support, and one with only Wi-Fi. This research focused on the second generation model, commonly referred to as the PS Vita Slim. All versions use a removable PS Vita Memory Card, but the Slim model has 1 GB of internal storage memory, which is only usable if no card is inserted [17]. In addition to playing games from PS Vita game cards, the PS Vita is also able to stream games from previous PlayStation consoles and connect to a PlayStation 4 through Remote Play. Through Remote Play, the PS Vita can be used as a second screen and controller for the game or can give players the ability to continue to play PlayStation 4 games remotely [10]. PS Vita has proven to be very difficult to mod, as only certain games on a certain firmware can be exploited, and Sony works quickly to fix known security exploits [12]. In this research, firmware version 3.36 was running on a new, unmodified PS Vita Slim.

3 Related Research

As gaming console forensics is relatively new, there are very few papers published on the subject. Most of the research done in this field is on home gaming consoles rather than mobile ones, as the hard drives are simpler to remove and image, and while the effectiveness of traditional forensic analysis is limited, much was learned about these systems. For example, although they produced new file types, the hard drive of the Xbox One used NTFS partitions [7], and the file system of the Xbox 360 was based off an older implementation of the FAT file system. [19], which facilitated analysis of the extracted data. Sony, however, has taken extra measures to prevent reverse engineering on the PlayStation 3, so alternative means had to be found to store and access the data [3]. Some information about the file system of PlayStation Portable, the predecessor of the PS Vita, was found [9], but much of the technology used has been changed, so it is unlikely to be the same for the PS Vita. No other research related to PS Vita forensics could be found. Thus, this research will lay a foundation for future research in PS Vita forensics.

4 Methodology

Because the hard drive of the PS Vita could not be removed, it was connected directly to a computer by the USB cable. However, the device could not be detected without the Content Manager Assistant for PlayStation (CMA). The CMA is an application required to enable data transfer between the device and the PC [10]. Therefore, in order to capture all files on the PS Vita for imaging, the CMA was used to create backups of the system files, saved data, and application data on the computer. Also, to prevent anything from accidentally being written onto the PS Vita, a USB software write blocker by DSi was enabled. This write blocker was tested by attempting to write to another USB device while active.

4.1 Creating Backup Files

To facilitate isolating events, the actions performed on the PS Vita were split into nine phases. After each stage, the system was backed up. By default, the CMA creates a new folder for the backup with a name consisting of the date and time the backup was created. This name was used to keep track of when each backup was made (Table 1).

Table 1. Actions performed in each phase.

Phase I	Initial startup (settings system updates)
Phase II	Connect to WiFi and sign in to PlayStation Network account
Phase III	Insert memory card and transfer data from internal memory
Phase IV	Download Borderlands 2 from PlayStation Store
Phase V	Play Borderlands 2 in single player mode locally
Phase VI	Play Borderlands 2 in multi player mode online
Phase VII	Download Youtube, Facebook, and Skype applications
Phase VIII	Perform regular tasks on each application
Phase IX	Take pictures and videos with and without location enabled

4.2 Acquiring Images of Backups

In order to analyze the image with multiple forensics tools, the file type of the images needed to be compatible with the tools. One such file type is the Encase Image File. However, to create this type of image file using AccessData’s Forensic Toolkit Imager, the entire drive where the PS Vita backups were located needed to be imaged.

4.3 Analyzing the Images

Five tools were used to analyze the images: The Forensic Toolkit (FTK) Imager v3.4.0.1, Autopsy v3.1.2, EnCase v7.09.06, Digital Forensic Framework (DFF) v1.3, and Bulk Extractor v1.5.5. Since it was likely that there would be new and unknown file types in the backup, it was uncertain what data each tool would be able to extract. Therefore, multiple tools were used to compare the effectiveness of current digital forensics tools on the PS Vita files.

The examinations in this research were run on 64-bit Windows 7 machine, so the tools selected were those compatible with the machine and widely used by forensic researchers and professionals. FTK Imager is an important component of the Forensic Toolkit, which is a highly regarded forensic analysis tool [8], and Autopsy is a popular open-source tool due to all the modules available [16]. EnCase is a widely accepted tool in the industry and is used in many investigations [14]. DFF is a relatively new open-source tool that has gained popularity due to its capabilities and customizability with modules and scripts [4]. Bulk Extractor has a strong reputation as an open-source forensic tool capable of data carving [7]. Autopsy, DFF, and Bulk Extractor are all packages include in the SANS Investigative Forensics Toolkit (SIFT) [5]. SIFT is a VMware image with multiple open-source forensic tools pre-installed and is widely used for forensic examinations [14].

4.4 Qualitative Measures

In each tool, after adding the image as an evidence file, we navigated to the folder containing the backups. Once there, the folder with the final backup from Phase IX was opened. For each of the files in the backup, several questions were posed, which are listed in Table 2. The results were later compared with the files from other phases.

Table 2. Set of questions for the Phase IX image.

1. What files are in the backup?
2. What are the sizes of the files?
3. What type are these files?
4. What are the timestamps of the files?
5. What are the contents of each of these files?
6. Does the tool recognize anything in terms of file carving?

5 Results

All four tools were able to find three files in the backup folder: 201501262046-01.psvimg, 201501262046-01.psvinf, and 201501262046-01.psvmd. All other images contain these files, with the name of the backup it belongs to as their names. In FTK, another file named $I30 was found as well, which is the Windows NTFS Index Attribute [5]. In Encase, a file called 201501262046-01.psvimg·Attribute List was found instead. This file is created by the NTFS and holds the location of attribute records that do not fit in the MFT record [13].

The tools were also able to find the size of each of these files. The PSVIMG file was 3,483,839,744B, the PSVINF file was 15B, and the PSVMD file was 208B. Additionally, both Encase and FTK provided the physical size of the files. The sizes of the $I30 file and $Attribute List file were 4096B and 1760B, respectively.

In FTK, there is an entry in the metadata table for file type. While $I30 was listed as an NTFS Index Allocation, the PSV* files were listed as Regular Files. In Encase, the “File Type” entry for all files, including $Attribute List, was blank. There was also an entry for “Category”, but it was listed as “Unknown” for $Attribute List and “None” for the others. Autopsy and DFF did not have an entry for this information.

All three tools indicated the last accessed, created, and last modified timestamps in each image. All these times matched for each file, after taking into account the time zone. The PSVIMG file was created first and was last modified a few seconds afterwards. Then, the PSVINF and PSVMD files were created. The timestamps from DFF were more detailed. They revealed that the PSVMD files were created before the PSVINF files by about one ten-thousandth of a second. The $I30 file was created at the same time as the PSVIMG file and was last modified at the same time as the other two. There were no timestamps for the $Attribute List file.

In both Autopsy and FTK, the contents of the files could be read in hex and text format. However, the contents of the PSVIMG and PSVMD files were illegible and are possibly encrypted. Future tests will be done to calculate the entropy values to determine if the files are encrypted. The PSVINF file, however, was stored in plaintext, which DFF recognized as ASCII text, and simply contained the name of the backup it belonged to. The $I30 file also contained some encrypted data, but it also held the names of the files in the folder as well as the 8.3 short filenames: 201501~1.PSV, 201501~2.PSV, and 201501~3.PSV.

It was difficult to isolate the backup files from the PS Vita when Bulk Extractor was used on the image. Instead, the original backup folder was used for this test. Bulk Extractor was run with all possible scanners, excluding hashdb and sceadan. The outputted report was empty, except for a file called wordlist.txt. Typically, this file would contain a list of the “words” that were extracted from the folder, but in this case, the only word found was the backup name from the PSVINF file. Other than that, no useful information was found.

6 Conclusion and Future Work

From the results above, much can be learned about the new PSV* file types in each backup. Very little is known about these files, as the system software used by the PS Vita is closed source, and most information posted in forums has yet to be confirmed.

For each phase, the PSVINF file simply contained the name of the backup, most likely for bookkeeping. Since this file type seems more straightforward, most of the discussion in the community is about the other two types. These files are encrypted [17], which the results affirm, possibly through the CMA so that the decrypted data can only be read by the PS Vita that created the backup [18]. The PSVMD files for each phase are different, but they are all the same size. There is speculation in the community that this file contains metadata, “MD,” and is stored as an XML file [18]. The PSVIMG file should then be where all the actual data is stored. In each phase, the size of the PSVIMG file grew by relatively small amounts. It should be noted that prior to Phase IV, when Borderlands 2 was downloaded, the backup folders did not include an $Attribute List file, probably because there was enough room for the records to be stored in the MFT. After the game was downloaded, the size of the PSVIMG file grew over 1000 times its size, from 3,208 KB to 3,423,876 KB.

Although the metadata collected from the tools do not match the extent of the data stored on the PS Vita, and may not seem to provide sufficient forensic evidence alone, it can be useful for timelining. At the time the backup was created, the same user would need to be in possession of the PS Vita and the computer where the backup was stored. Therefore, actions performed on the PS Vita around that time are most likely done by the same user. If the identity of the console's user can be found, so can the identity of the computer's user.

The goal of this research was to follow a standard procedure for multiple existing tools in order to find what information could be extracted from the PS Vita in a forensically sound manner, and it is clear that these tools provide limited data. Ideally, a specialized tool will need to be made to properly analyze all the stored data. In order to create more effective tools, more needs to be learned about the system. For example, in future research, we can physically take apart the system and attempt to extract unencrypted data directly from the device. Several members in the community have successfully taken apart a PS Vita [6] and have identified what appears to be a JTAG port on the CPU [18]. Another possibility is to extract the data directly from the PS Vita memory cards and examine how the data are stored in it. A more challenging direction could be to reverse engineer the CMA to attempt to decrypt the files found.

References

1. 10-year-old victimized through Xbox. The Folsom Telegraph (27 August 2010)
2. Anderson, N.: CSI: Xbox - how cops perform Xbox live stakeouts and console searches. Ars Technica (10 January 2012). http://arstechnica.com
3. Conrad, S., Dorn, G., Craiger, P.: Forensics analysis of a PlayStation 3 console. In: Chow, K., Shenoi, S. (eds.) IFIP WG 2010. IFIP AICT, vol. 337, pp. 65–76. Springer, Heidelberg (2010)
4. Digital Forensics Framework. http://www.digital-forensic.org
5. Digital Forensics Training | Incident Response Training | SANS. http://digital-forensics.sans.org
6. Gadget Teardowns | iFixit. https://www.ifixit.com/Teardown/
7. Moore, J., Baggili, I., Marrington, A., Rodrigues, A.: Preliminary forensic analysis of the Xbox One. In: Fourteenth Annual DFRWS Conference. Digital Investigation, vol. 11, supplement 2, pp. S57–S65 (August 2014)
8. Liang, J.: Evaluating a selection of tools for extraction of forensic data: disk imaging. Thesis, Auckland University of Technology (2010)
9. Pancoast, S.: The play station portable: background and forensics analysis of the file system and standard files on the play station portable (2008)
10. PlayStation. http://www.playstation.com
11. Potter, N.: PlayStation sex crime: criminal used video game to get girl's naked pictures. ABC News (13 March 2009)
12. PS Vita Hacks | PS Vita eCFW. https://vitahax.wordpress.com
13. Resources and Tools for IT Professionals | TechNet. https://technet.microsoft.com
14. Shah, M., Paradise, D.: Tool comparison. Research, Champlain College (2013)

15. Stuart, K.: PlayStation 2 manufacture ends after 12 years. The Guardian (4 January 2013)
16. The Sleuth Kit (TSK) and Autopsy: Open Source Digital Forensic Tools. http://www.sleuthkit.org
17. Vita Dev Wiki. http://www.vitadevwiki.com
18. Wololo.net - PS4, PS Vita, PSP Programming, security and homebrews. http://wololo.net
19. Xynos, K., Harries, S., Sutherland, I., Davies, G., Blyth, A.: Xbox 360: a digital forensics investigation of the hard disk drive. Embedded systems forensics: smart phones, GPS devices, and gaming consoles. Digit. Invest. **6**(3–4), 104–111 (2010)