Digital Investigation 12 (2015) S81–S89

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2015 Europe

Forensic analysis of a Sony PlayStation 4: A first look

Matthew Davies [a], Huw Read [b, c, *], Konstantinos Xynos [b], Iain Sutherland [c, d]

[a] Sytech Digital Forensics, PO Box 3471, Stoke-on-Trent, ST4 9JS, UK
[b] University of South Wales, Pontypridd, CF37 1DL, UK
[c] Noroff University College, 4608 Kristiansand S, Vest-Agder, Norway
[d] Security Research Institute, Edith Cowan University, Perth, Australia

Keywords:
PlayStation 4
Games console
Online investigation
Small scale digital device
Embedded system

A B S T R A C T

The primary function of a games console is that of an entertainment system. However the latest iteration of these consoles has added a number of new interactive features that may prove of value to the digital investigator. This paper highlights the value of these consoles, in particular Sony's latest version of their PlayStation. This console provides a number of features including web browsing, downloading of material and chat functionality; all communication features that will be of interest to forensic investigators. In this paper we undertake an initial investigation of the PlayStation 4 games console. This paper identifies potential information sources of forensic value with the PlayStation 4 and provides a method for acquiring information in a forensically sound manner. In particular issues with the online and offline investigative process are also identified.

Introduction

Gone are the days of games consoles being regarded as mere entertainment systems. Games console technologies are advancing at a far greater rate than that of game console forensics. This is evident from devices like the PlayStation 3, relatively little is known of this console in terms of forensic analysis, yet the PlayStation 4 has been released. It has been identified by several authors including, (Xynos et al., 2010), (Conrad et al., 2009), and (Turnbull, 2008) that the distinction between games consoles and personal computers is becoming increasingly blurred. Modern gaming consoles possess far greater functionality and processing speed, and connectivity features similar to standard PCs. Game console forensics will continue to become a specialist area, with its own bespoke challenges to the digital investigator.

Currently there are over 10 million Sony PlayStation 4 games consoles in worldwide circulation (Peckham, 2014). At present there is little information available offering forensic investigators an insight into what information of interest is stored on this device, or how to acquire data in a forensically sound fashion. This paper seeks to provide a greater insight into the PlayStation 4 in relation to a digital investigation, and to present a methodology that can provide guidance to investigators working with such a system.

The rest of this paper is arranged as follows. Section 2 highlights literature that has helped shape our investigation, Section 3 presents the forensic challenges an analyst may encounter, Section 4 describes the empirical experiment methodology we undertook to discover what data is of importance, Section 5 describes the forensic analysis of the PlayStation 4, Section 6 presents our methodology for extracting useful information, Section 7 and Section 8 highlight conclusions and future considerations.

* Corresponding author. University of South Wales, Pontypridd, CF37 1DL, UK. Tel.: +44 (0)1443 654287; fax: +44 (0)1443 654050.
E-mail address: huw.read@southwales.ac.uk (H. Read).

http://dx.doi.org/10.1016/j.diin.2015.01.013

Literature review

Games platforms present a number of challenges in terms of accessing and interpreting data, as each system is a proprietary platform with a unique operating system. While there has been work on the forensic analysis and acquisition of data from other game platforms, there has been little work to date on the Sony PlayStation 4. However we can learn of the types of challenges we are likely to face with such a device by reviewing recent work in similar embedded systems.

Microsoft Xbox One

Previous work (Moore et al., 2014) has provided a preliminary analysis of an Xbox One, using initial exploratory methods such as file carving, keyword searches, network forensics and file system analysis. The greatest challenge faced by Moore et al. (2014) appears to be the encrypted and/or compressed nature of the files and game network traffic, thus making extraction and analysis somewhat difficult. However, an analysis of the NTFS filesystem did allow for file timestamps to be recovered, and some encrypted network traffic could be related back to which game was played.

Sony PlayStation 3

The analysis conducted by Conrad et al. (2009) was of particular interest as we were presented with similar challenges to those posed by the Sony PlayStation 4. A series of experiments was conducted by Conrad et al. (2009) on the PlayStation 3 and established that, due to the console's utilisation of AES encryption (Ridgewell, 2011); a native analysis method was required. The write blocker experiment conducted by Conrad et al. (2009) concluded that it is not possible to prevent evidence being altered during the analysis of the Sony PlayStation 3. However the methodology produced by Conrad et al. (2009) remains valid, as the analysis undertaken by investigators is repeatable.

According to Ridgewell (2011) the PlayStation 3 adopts an AES 128 encryption format, exploitable through the various processes of retrieving the cryptographic keys used by Sony, identified by hacking group fail0verflow. They also utilised various network forensic techniques and software tools in order to evaluate the console's security vulnerabilities, observing that the PlayStation 3 TCP & UDP communications are unencrypted.

Microsoft Xbox 360

The work undertaken by Xynos et al. (2010) expands upon the research of Vaughan (2004), Burke and Craiger (2007) and Dementiev (2006), establishing that is possible to recover remnants of information relating to online gameplay from the consoles hard drive; such as time and date stamps and the online gamer ID's of all players that had participated. As highlighted in Read et al. (2013) there is a need to keep up to date with the modding community, as some developments may have far reaching consequences, which could even include hiding entire partitions from forensics tools.

Identified forensic challenges

The greatest challenge presented to digital investigators in relation to the PlayStation 4 is the non-standard file system; unlike the Xbox One that at least allows NTFS metadata retrieval (Moore et al., 2014). The hard drive contained in the system appears encrypted and this presents a significant barrier. The hard drive can be imaged via a write blocker, however its encrypted nature means it would be difficult to provide an in depth analysis that includes operating system artifacts. For this reason the most useful route is via the user interface, as with other embedded and smart devices (Sutherland et al., 2014), whilst using appropriate write blocking technology to prevent changes to the data.

A further challenge is the user's ability to alter the information stored within the PlayStation Network (PSN). A user accessing a PSN account via an alternative console, PS4 Companion APP (Sony, 2014a) or PlayStation Vita (Sony, 2014b) possesses the ability to modify or remove potential evidence.

As with many other eighth generation games consoles, the sharing of user-generated content via social media is prevalent on the PlayStation 4. The very nature of sharing hi-scores, game achievements and recorded videos with others requires the device to be connected to the Internet and use of Sony's cloud services. From a forensic investigator's perspective, this may mean the hard drive is not the most important data source as it has been in previous generations of games systems. It is possible that user generated content will not even appear on the hard drive at all; online investigations may be required to obtain evidence.

Analytical procedure

In the production of any guidance or methodology for information extraction, which may be relied upon in courtroom proceedings, standard best practice must be adhered to. In the UK the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence version 5 (Association of Chief Police Officers (2012)) provides current best practice for evidence acquisition. All tests performed on the PlayStation 4 have been carried out with respect to ACPO guidance.

Preliminary analysis

We performed an initial study of available literature and an empirical investigation of the PlayStation 4 to identify the areas that a digital forensic investigation may wish to examine. In particular, the Frequently Asked Questions (FAQ) posted by Shuman on the official PlayStation blog (Shuman, 2013) proved to be insightful when trying to identify which areas to analyse. The empirical investigation comprised of powering on the PlayStation 4, navigating through the various in-game menus and noting areas that may provide evidence of usage and/or communication during an investigation. We primarily concentrated on

finding areas that may help identify the who, what, when and where aspects of an investigation. The "who" focused on identifying which user generated the evidence (The PlayStation 4 can hold up to 16 user profiles (Sony Computer Entertainment America and LLC, 2014)), "what" content can be created with the new features of the device, timestamp information to indicate "when" the information was generated, "where" the information could be stored (hard drive, external media, Internet/cloud). After exhausting the features on the device, a number of areas were revealed that could help answer these questions. The features found to be of interest are detailed in Table 1.

Experiment methodology

An experimental methodology was devised by empirically exploring the areas identified in Table 1 and noting locations that may be of interest to an investigator, an overview of the process we undertook is presented in Fig. 1. The methodology was created to assess if it was possible to retrieve data from each location. This involved deliberately introducing data into those different areas and observing if it could be retrieved later. During the course of the experiment, firmware updates became available for the PlayStation 4. Each revision was noted, installed, and the experiment methodology was run again to assess if there were any negative impacts to the evidence acquisition process described in Section 6. The following selection of firmware was used: 1.01, 1.50, 1.51, 1.52, 1.60, 1.61, 1.62, 1.70, 1.72, 1.75 and 1.76 (the latest at the time of writing). Unfortunately we were unable to test all revisions, as the console would only allow us to update to the latest, skipping incremental versions.

The experiment was carried out (for each firmware version) as follows.

- Activate video capture device, record time.

Ensure that all of our actions on the system are recorded for future reference.

- Activate PlayStation 4. Record time as set on console. Observe any offset between real time and time on console. Offset must be applied to any data retrieved to ensure correct time is recorded.
- Introduce sample dataset, record time and data introduced. The sample data (detailed in Section 4.3) is designed to deliberately cause the console to store information in relevant areas from Table 1. Through meticulous recording, we can later identify if our actions are retrievable from the PlayStation 4.
- Turn off PlayStation 4. Deactivate video capture device, record time. The video capture provides evidence of our introduced changes to the system during this iteration of the experiment.
- Forensically image PlayStation 4 hard drive. Though the files are inaccessible, we keep an image of the hard drive as best evidence such that if our empirical investigation alters evidential data, we can restore the hard drive from the image file and reassess. We used FTK Imager v.3.1.5 to create the forensic images, and the EnCase E01 format to compress files, as the uncompressed RAW images are large.
- Turn on PlayStation 4; investigate areas in Table 1 to identify user actions introduced during this experiment iteration.
- Compare the data retrieved in relation to the data introduced. Note information, timestamps and any other items indicating use of the PlayStation 4.

After a new firmware update was applied, the hard drive was forensically wiped and then reinitialised in the PlayStation 4 to ensure any recovered data was from the current iteration of the experiment and not from a prior run. The

Table 1
Features of interest to investigators.

Features	Reason
PlayStation Network (PSN)	The vast majority of features available to Sony PlayStation 4 users are reliant upon a PSN membership.
Sony Entertainment Network (SEN)	Viewing SEN content through a PC web browser, will reveal the user's real name, address, credit or debit card information, transaction history, linked devices and sub account information.
Internet Browser	The Internet browser does not support PDF or office documents. Thumbnails are stored in the browser history provide an indication of user's most recent activity. Google search terms, Google map searches, 100 web pages visited, 100 Bookmarks (Sony Entertainment Inc, 2014) and 8 most recently visited webpages are available.
ShareFactory	The ShareFactory enables players to share, via USB/social media, content recorded via the PlayStation camera or recent game footage. In addition, users possess the ability to edit footage and to record voiceovers or video commentary.
System Storage Management	Provides system storage information such as D disk usage, application saved data, video & screen captures and available disk space.
Error History	A log of various errors encountered by the system, including time/date values, error codes and the nature of the error.
What's New	Recent user activity and those on their friends list including recent gameplay, recent achievements and new additions to their friends list.
Trophies	Relate to specific gaming titles and provide time/date values of when achievements were awarded.
Profile	Personal data/unique user handles and other content generated by a user.
Friends	A user's friends in their Friends list can be linked to Facebook. Is it possible to find communications between the user of the system and others. Real name requests can be sent, meaning that a user's real name will be displayed in all communications. Up to 2000 friends.
Party Messages	The Party feature allows up to 8 users to enter a group conversation.
Messages	Messages between individuals and multiple users.

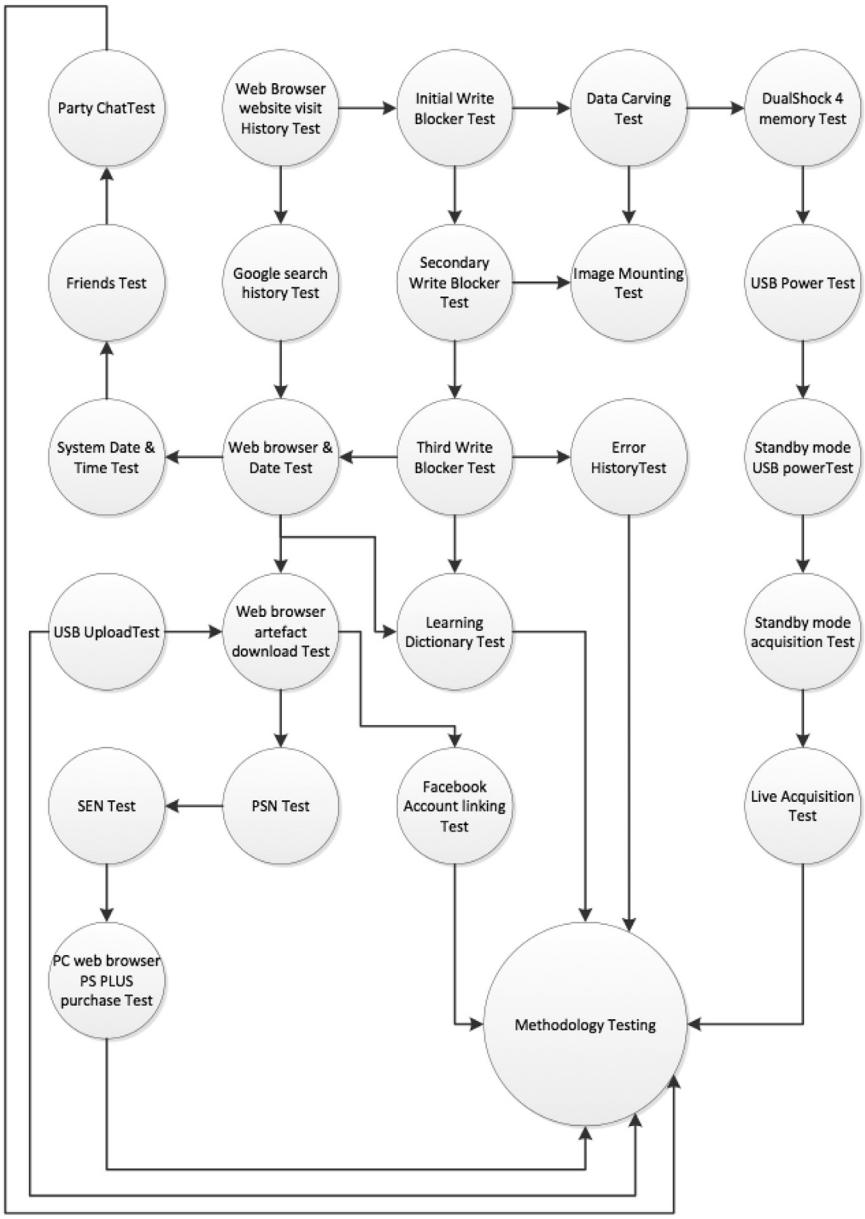


Fig. 1. Empirical exploration of the PlayStation 4.

purpose of running the experiment after a change in firmware is to determine if these changes will help or impede our ability to obtain data.

Test data

The PlayStation 4 can store information on the local hard drive and online. Different accounts had to be created in order to assess the features in Table 1. Local (offline) user accounts comprised of three users, User1, User2 and User3. Two further online accounts, the free PSN (PlayStation Network) account and the subscription-based PlayStation Plus account was also created to ensure all features would be available. The PlayStation Plus account was used to download a free title, "War Thunder", and participate in online gameplay to check for usage later.

To assess the messages functions, contacts were added to the Friends List and both individual and group messages were sent to selected users. A Facebook account was created to enable both the social media aspect of The ShareFactory and the Share button feature on the DualShock 4 controller. A number of other Facebook users were linked to this account to determine if they appeared elsewhere on the console.

The Trophies feature worked with both offline and online game play. Two software titles available to us, "Call of

Duty: Ghosts" and "Need For Speed Most Wanted" were used in both modes to assess if usage patterns could be determined by in-game trophy awards.

To assess the Error History, we observed that interacting with Internet dependent features offline would result in error messages being added to the log. We would remove the Internet connection, note the time and the function accessed, and then determine if the information was generated. This knowledge allowed us to deliberately create known system errors to assess the Error History feature.

The Internet browser is known to store 100 visited websites in its history and bookmarks, and 8 most recently used webpages. To assess this, we accessed 103 websites and stored 103 bookmarks, consisting of direct links to images, web pages, websites and duplicate entries.

A number of features allow the user to store data to a FAT32 formatted USB memory stick. We stored Share-Factory projects and pictures obtained from the Internet web browser to a flash drive for later analysis.

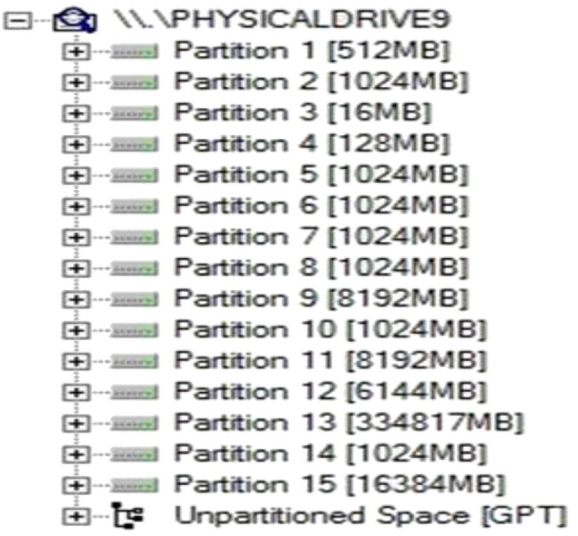


Fig. 2. Sony PlayStation 4 partitions viewed from FTK Imager on a 400GB drive.

Forensic analysis of a PlayStation 4

As presented in Fig. 1, a number of different tests were conducted to assess the ability of a forensic investigator to identify usage of a PlayStation 4. The test data in Section 4.3 was introduced to successive firmware updates (see Section 4.2), and any notable changes between revisions are discussed below.

Initial findings

An initial triage of a PlayStation 4 hard disk, using FTK Imager v3.1.1.8, revealed that the disk structure consists of an unknown filesystem split into 15 partitions as can be seen in Fig. 2. Our analysis of the PlayStation 4 will concentrate on using the native user interface to locate information.

Data carving test

We employed the data carving utility of AccessData's Forensic ToolKit (FTK) v3.2 in an attempt to retrieve additional files from a forensic image taken of the PlayStation 4. FTK v3.2 was unable to detect the presence of any files. This strongly suggests either encryption or a bespoke container format.

Web browser, bookmarks history and recent items

Several experiments were conducted upon the PlayStation 4 Internet web browser. The first of which aimed to determine whether the browser stores only unique websites visited, as seen in the PlayStation 3 (Conrad et al., 2009). The experiment involved visiting 103 websites and selecting various web links. It was noted during the experiment that in addition to all web links selected, Google search terms also appear in the PlayStation 4 web browser history. Furthermore, an analysis of the web browser history, bookmarks and most frequently used pages concluded that the time & date upon which events occurred, is not obtainable via the native interface.

Further experiments involved utilising the Internet web browser to store pictures upon the console's hard drive. It was established that there are only two means by which to successfully complete this task. The first is by storing web images as bookmarks, the second is to store screenshots captured via the share button on the DualShock 4 controller.

Time & date test

We conducted a system wide analysis of the Sony PlayStation 4, focussing upon the retrieval of date and time stamp information. It was discovered that the majority of features, such as Trophies, What's New etc., provided such information. In contrast, applications such as the Internet web browser did not present any form of date and time information, whilst the Party and Messages features presented only the dates upon which messages were sent and received.

Drive backup and restoration

After performing an analysis of the PlayStation 4 via the user interface, we tried restoring the hard drive back to the acquired image taken before turning on the console. The purpose of this was to determine if the system would accept a previously stored system, which a forensic examiner could use to verify their findings. We converted our image to RAW before transferring onto the drive with the UNIX tool dd. FTK Imager (v3.1.5) was used to verify the restored drive that confirmed it was identical to the image file. The console booted the restored version without any issues.

Offline write blocker test

Inspired by Conrad et al. (2009) we used a Tableau T35is write blocker as a man-in-the-middle given it has SATA

ingress and egress connections (Fig. 3). We kept the system offline to examine what could be obtained from the hard drive alone. Unlike Conrad's experiment on the PlayStation 3, we were able to successfully boot the PlayStation 4 and view data via the in-game menus. However, any functions attempting to write to the hard drive (such as System Storage Management calculating storage space) caused the system to become unstable and stop responding. A hard reset was required to boot the system again.

An offline analysis of the PlayStation 4 utilising the T35is concluded that it is possible to retrieve the key information outlined in Table 1 with the exception of the ShareFactory, System Storage Management and What's New. It was noted during the analysis that any interaction with some PSN dependent features would result in the generation of system errors due to the system being offline. The T35is prevented the errors from being written to the log and the system became unstable.

These results were obtainable for all firmware revisions up to and including 1.62. After we conducted the experiment during the firmware 1.70 iteration, we found that all the PSN areas of the console were now inaccessible offline, and required logging into the PSN network.

During the firmware 1.72 iteration experiment, it was only possible to recover data relating to the Internet web browser and system setting information.

Furthermore on firmware 1.75 the system would boot successfully with the write blocker but any attempt made to open the Applications pane would result in system instability. From 1.75 onwards we had to use a Voom Shadow 3 (see Section 5.8 below) to let the PlayStation 4 write changes to a buffer whilst maintaining forensic integrity of the original drive.

Online write blocker test

This experiment compliments that in Section 5.6; by using a T35is write blocker (up to firmware 1.72) or a Voom Shadow 3 (firmware 1.72 and later) and enabling the Internet connection to allow access to online content, whilst disabling the ability to make changes to the local hard drive. We felt it was necessary to assess whether such a method would also prevent the modification of PSN dependent content. The experiment consisted of sending multiple messages to a specific user, whilst utilising the write blocker as a pass-through.

Upon restarting the console it was noted that the message sent was not visible. In order to validate the results the experiment was repeated. The second iteration revealed that the content of both messages were now visible. The results indicate that, investigators must be wary of messages previously sent via the PSN can be cached locally and remotely potentially leading to differences between an online and offline investigation.

Shadow drive test

The changes implemented in firmware version 1.75 prevented us from conducting an analysis of the Sony PlayStation 4 whilst utilizing the Tableau T35is write blocker. Accessing any of the menus in the same fashion as on earlier firmware resulted in system instability. As such a suitable alternative method of maintaining evidential integrity was sought.

The Voom Shadow 3 (Fig. 4) was identified as a potential alternative. In order to assess the device's suitability, we connected the Voom Shadow 3 as a bridge between the PlayStation 4 and its hard drive. The console successfully booted and we were able to fully navigate the system without the stability issues experienced with the Tableau.

Shadow drive offline analysis test

An offline analysis of the Sony PlayStation 4 ensued, focussing upon the recovery of data relating to the key features identified in Table 1. It was established that, in contrast to the analysis conducted upon Firmware version 1.72 with the Tableau (see Section 5.6), data associated with the features below were now obtainable offline with the Voom Shadow 3:

- Internet web browser
- System Storage Management
- System time & date
- Error History

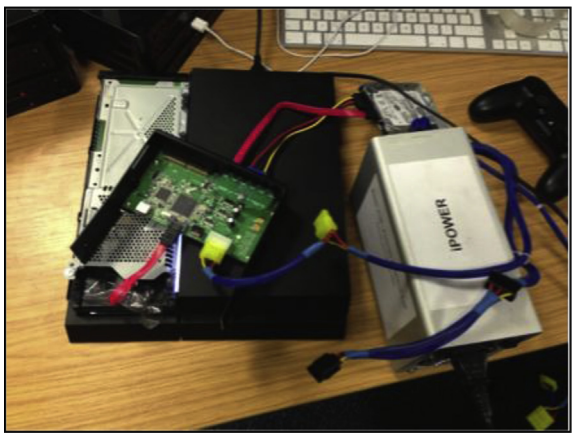


Fig. 3. Tableau T32is used as a man-in-the-middle between the PlayStation 4 and its hard drive.

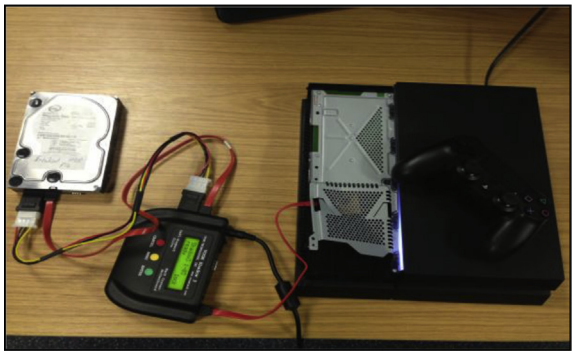


Fig. 4. : A PlayStation 4 hard drive connected via the Voom Shadow 3.

- Capture Gallery
- Basic profile information
- Party Messages
- Messages
- Notifications

Shadow drive online web browser analysis

We used the Voom Shadow 3 to conduct an online analysis of the PlayStation 4 Internet web browser. The console was provided a LAN Internet connection and powered on. We selected the user and proceeded to sign out of the PlayStation Network (PSN). The console's web browser was then launched; nine selections were made from the web browser history and the respective websites visited. The browser history was documented and the console restarted. The history, bookmarks and most frequently used pages were consulted and revealed that the alterations made during the analysis had not been stored.

Shadow drive validation procedure

The PlayStation 4 hard drive was removed and imaged using FTK Imager v3.1.1. It was reconnected and the online Internet web browser analysis performed. We then removed the drive and verified its integrity. Both the generated MD5 & SHA1 hash values were a match.

Local account passcode login

A local account used throughout the experiments was selected, and the passcode was set equal to '0000' in Settings/Users/Login Settings/Passcode Management. The console was rebooted ensuring the Voom Shadow 3 was in write protect mode. We were subsequently prompted to enter the login passcode. We selected options/forgotten passcode and were then prompted to login to PSN. We then selected a new passcode, 9999 and access to the system was granted. The console was rebooted, prompting the login passcode. We entered 0000 and access to the system was granted. This allows an investigator to unlock a PlayStation 4 to look at local content without making changes to the system.

The PlayStation network

Up to firmware version 1.70 the PSN dependent content, such as Profile and Trophies could be accessed while the console was offline. From 1.70 onwards we had to connect the console to the Internet to access such information. This could be conducted with specialist hardware like the Voom Shadow 3 drive used in earlier experiments, but we explored the possibility of using the login data on a separate PlayStation 4 unit. Starting with a forensically zeroed hard drive on an identical specification PlayStation 4, a local account User1 was created and the menus were navigated to ensure the absence of data. We connected the system to the Internet and logged into the PSN with our account credentials. The following information was now available, even though this system had not been used to generate any content:

- Trophies
- Profile
- Party Messages
- Messages
- Friends
- What's New

USB upload test

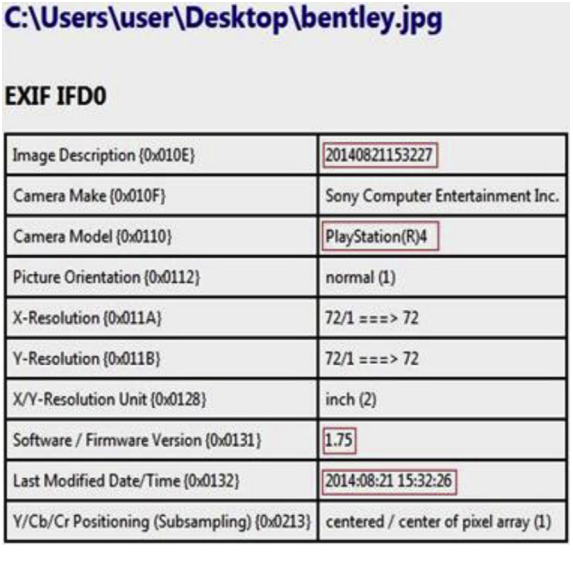
Various file formats were copied from a desktop workstation onto a FAT32 formatted flash drive. The files were stored in a folder labelled PS4 and consisted of 4 jpeg, 1 png, 2 pdf and a variety of Microsoft Office formats. The USB flash drive was then inserted into the PlayStation 4 and several attempts were made to upload the files. We found it was not possible to upload such files onto the PlayStation 4.

USB download test

We investigated what type of content a user may download onto a memory stick. The ShareFactory was used to create videos of gameplay and the Internet web browser was used to perform Google searches for pictures of vehicles. Each picture was enlarged to full screen, by pressing square on the DualShock 4 controller, and a screen capture acquired. We used the Capture Gallery to publish duplicates of the content to the USB flash drive.

Using an Exif viewer allowed us to view the metadata from the fullscreen captures (Fig. 5). The image description field relates directly to the file name present upon the Sony PlayStation 4. The file name is provided by default and users are unable to make alterations to it from the console. In addition, the metadata also presents the firmware version installed upon the console when the image was acquired. Furthermore, we see that the PlayStation 4 is also identified as the camera model.

An analysis of the USB storage device was then conducted using the hex viewer in FTK Imager. It was observed


C:\Users\user\Desktop\bentley.jpg

EXIF IFD0

Image Description {0x010E}	20140821153227
Camera Make {0x010F}	Sony Computer Entertainment Inc.
Camera Model {0x0110}	PlayStation(R)4
Picture Orientation {0x0112}	normal (1)
X-Resolution {0x011A}	72/1 ===> 72
Y-Resolution {0x011B}	72/1 ===> 72
X/Y-Resolution Unit {0x0128}	inch (2)
Software / Firmware Version {0x0131}	1.75
Last Modified Date/Time {0x0132}	2014:08:21 15:32:26
Y/Cb/Cr Positioning (Subsampling) {0x0213}	centered / center of pixel array (1)

Fig. 5. : End of file marker for MP4 files generated by ShareFactory.

that the MP4 generated via the ShareFactory contain the Application code (CUSA 0057) and the file name, which is the date and time upon which the file was created on the PlayStation 4 (Fig. 6).

Proposed best practice methodology for the forensic analysis of the Sony PlayStation 4

To obtain the information described in Table 1 a forensic investigator should carry out the following steps:

1. Remove and forensically image the PlayStation 4 hard drive. Disable Internet connectivity. As discussed in Section 5.5, the image could be used to restore from at a later date to verify results.
2. Reconnect hard drive with a SATA write blocker that has a buffer feature (in Section 5.8 we described usage of a VOOM Shadow 3) as a man-in-the-middle between drive and console.
3. Activate video capture device, record time. Switch on PlayStation 4 and synchronize the DualShock controller.
4. Record time and date as presented on PlayStation 4 and take note of any difference with actual time. This offset will need to be applied to any timestamps (see Section 5.4) retrieved from the system.
5. Navigate to and record the data presented in the various functions as follows:
   a. Error History - The Error History should be viewed first as errors may be introduced by the analyst during the investigation.
   b. Internet Web Browser - Record history, bookmarks, and most recently opened.
   c. System Storage Management
   d. Capture Gallery - A USB drive may be used to download all content from the Capture Gallery (screenshots and videos, see Section 5.15).
   e. Basic Profile Information
   f. Party Messages
   g. Messages
   h. Notifications
   i. Error History - Record the errors generated during the course of the investigation.
6. Power off PlayStation 4, video capture device, record time.

If the PSN network login credentials are available, further information as detailed in 5.13 may be obtained on another PlayStation 4 console. If unavailable, a decision will need to be made by the investigator whether to take the original system online. Even with a write blocker, the danger using the original system is that cached content may be pushed online and update/overwrite existing information.

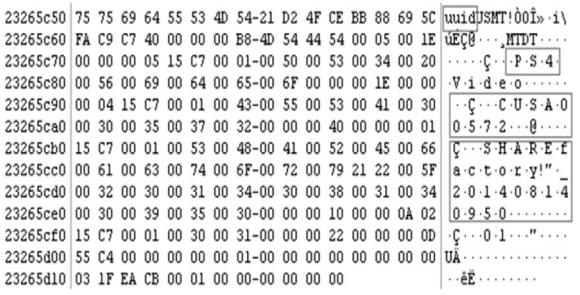


Fig. 6. Exif data from a PlayStation 4 generated image.

Conclusions

The proposed best practice methodology would allow digital investigators to perform an analysis of a write protected Sony PlayStation 4. The alteration of data is prevented and thus evidential integrity is maintained.

The amount of information retrievable however is directly dependent upon the firmware version installed on the console. Table 2 demonstrates that, during an offline analysis, it is possible to recover all user profile information from a console with up to firmware version 1.62 with a standard write blocker. Version 1.70 had limitations when viewing PSN content offline whilst 1.75 required the use of an advanced write blocker to view anything of substance. Similarly, Table 3 identifies what is retrievable during an online investigation for comparison.

Table 2
Information obtainable during an offline investigation.

Firmware version	1.62	1.72	1.75/1.76
Browser	✓	✓	✓
ShareFactory	✗	✗	✗
Capture Gallery	✗	✓	✓
System Storage Management	✗	✗	✓
Error History	✓	✓	✓
What's New	✗	✗	✗
Trophies	✓	✗	✗
Profile	✓	✗	P
Friends	✓	✗	✗
Party	✓	✗	✓
Messages	✓	✗	✓
Notifications	✓	P	P
System Settings	✓	✓	✓

✓ = Fully Retrievable.
✗ = Not Retrievable.
P = Partially Retrievable.

Table 3
Information obtainable during an online investigation.

Firmware version	1.62	1.72	1.75/1.76
Browser	✓	✓	✓
ShareFactory	✓	✓	✓
Capture Gallery	✗	✓	✓
System Storage Management	✗	✗	✓
Error History	✓	✓	✓
What's New	✓	✓	✓
Trophies	✓	✓	✓
Profile	✓	✓	✓
Friends	✓	✓	✓
Party	✓	✓	✓
Messages	✓	✓	✓
Notifications	✓	✓	✓
System Settings	✓	✓	✓

✓ = Fully Retrievable.
✗ = Not Retrievable.

As the Sony PlayStation 4 will not readily allow users to downgrade firmware, it is not possible to restore to previous revisions that allow greater offline access. As such, investigators will continue to be challenged by future firmware updates.

Further challenges are faced by the growing array of content only available online. Although evidence of usage is available on the console, many of the artifacts are only available when the PSN network is connected. Investigators may inadvertently alter data stored online by not disabling the network connectivity, and malicious users may use other devices to deliberately alter or remove incriminating content.

Future considerations

There are a growing number of accessories and interactivity options for the PlayStation 4 that may require investigation in their own right. The PlayStation camera enables users to utilize enhanced security features such as facial recognition to login. This could be used to secure the console, but could also be used to prove account ownership on a multi-user system if an individual was able to unlock a specific account. Future research should consider the implications of the PlayStation 4 connection capabilities with the Sony Vita and the PlayStation Companion App on smartphones and tablets. Any evidence of ownership data transfer and communications will be of interest to investigators.

References

Association of Chief Police Officers. ACPO good practice guide for digital evidence. 2012. Version 5.0, Metropolitan Police Service, Available online, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

Burke P, Craiger P. Xbox forensics. Journal of digital forensics practice. New York: Taylor & Francis; 2007. p. 275–82.

Conrad S, Dorn G, Craiger JP. Forensic analysis of a Sony Play Station 3 Gaming Console. In: 6th Annual Conference of the International Federation of Information Processing; 2009. Available online, http://computerforensicsllc.com/computer-forensics-expert-florida-miami-palm-beach-lauderdale-dave-kleiman-forensic-training-files/Forensic_Analysis_of_a_Sony_Play_Station_3_PS3_Gaming_Console.pdf [accessed 08.01.15].

Dementiev D. Defeating Xbox (utilizing DOS and Windows tools). 2006 [Unpublished].

Moore J, Baggili I, Marrington A, Rodrigues A. Preliminary forensic analysis of the Xbox One. DFRWS 2014 2014. Available online: http://www.dfrws.org/2014/proceedings/DFRWS2014-7.pdf [accessed 08.01.15].

Peckham M. Microsoft Silent on Xbox one Sales as Playstation 4 Wins July [online]. Available at: http://time.com/3116454/npd-july-console-sales/; 2014 [accessed 28.08.14].

Read H, Xynos K, Sutherland I, Davies G, Houiellebecq T, Roarson F, et al. Manipulation of hard drive firmware to conceal entire partitions. Digit Investig 2013;10(4):281–6.

Ridgewell W. Determination and Exploitation of potential security vulnerabilities in networked game devices [online] Available at: http://dtpr.lib.athabascau.ca/action/download.php?filename=scis07/open/walterridgewellProject.pdf; 2011 [accessed 17.12.13].

Shuman S. PS4: the Ultimate FAQ – North America (Playstation.blog) [online blog] Available at: http://blog.us.playstation.com/2013/10/30/ps4-the-ultimate-faq-north-america/; 2013 [accessed 09.11.13].

Sony. PS4™ companion app [online] Available at: http://us.playstation.com/ps4/app/; 2014 [accessed 15.12.13].

Sony. PS4 Remote Play and second screen [online] Available at: https://support.us.playstation.com/app/answers/detail/a_id/5065/~/ps4-remote-play-and-second-screen; 2014 [accessed 01.03.14].

Sony Computer Entertainment America, LLC. User profiles on PS4. [online] Available at: https://support.us.playstation.com/app/answers/detail/a_id/5214/~/user-profiles-on-ps4 [Accessed 18.12.14].

Sony Entertainment Inc. Managing bookmarks & browser history (PlayStation 4 UserGuide) [online] Available at: http://manuals.playstation.net/document/gb/ps4/browser/bookmark.html; 2014 [accessed 18.09.14].

Sutherland Iain, Xynos Konstantinos, Read Huw, Jones Andy, Drange Tom. A forensic overview of the LG Smart TV. presented at the 12th Australian Digital Forensics Conference 2014 SRI Security Congress, "Security on the Move" 1-3 December, 2014, Perth, Western Australia. 2014.

Turnbull B. Forensic investigation of the Nintendo Wii: a first glance. Small Scale Digital Forensics J 2008;(2)1:1–7.

Vaughan Chris. Xbox security issues and forensic recovery methodology (utilising Linux). Digit Investig 2004;1(3):165–72 (September 2004), http://dx.doi.org/10.1016/j.diin.2004.07.006.

Xynos K, Harries S, Sutherland I, Davies G, Blyth A. Xbox 360: a digital forensic investigation of the hard disk drive. Digit Investig 2010; 6(3–4):104–11. http://dx.doi.org/10.1016/j.diin.2010.02.004.