Forensic analysis of a Sony PlayStation 4 Sytech Digital Forensics,

Abstract

Keywords

Introduction

Literature review

Identified forensic changes.

Analysis procedure

Forensic analysis of a PlayStation 4

Best practice

Conclusion

Case Summary

A gaming console's primary purpose is as an entertainment system. However, these consoles' most recent generation offers a lot of new interactive capabilities that could be useful to a digital investigator. This essay emphasizes the worth of various systems, particularly Sony's most recent PlayStation model. This console offers multiple services, such as web browsing, downloading content, and chat functionality—all communication tools that forensic investigators may find helpful. In this essay, we preliminary analyze the PlayStation 4 gaming system. This article outlines various information sources with the PlayStation 4 that may be useful for forensic investigations and offers a technique for gathering data forensically soundly. Additionally, problems with the online and offline investigative processes are noted.

Evidence

1. PSN, the PlayStation NetworkUsers of the Sony PlayStation 4 are restricted from using certain features unless they have a PSN membership.

2. SEN is the Sony Entertainment Network. The user's real name, address, payment or debit card information, transaction history, associated devices, and sub-account information will all be visible when viewing SEN content using a PC web browser.

3. The internet browser does not support Office and PDF documents. Thumbnails, which are kept in the browser history, show the user's most recent activity. Eight most recent websites were visited, 100 online pages were accessed, 100 bookmarks, and Google search phrases and map searches were provided (Sony Entertainment Inc., 2014).

4. ShareFactory Players can share recent game footage or content captured with the PlayStation camera through USB or social media with others using the ShareFactory. Users also have the option to edit videos and record voiceovers or video comments.

5. System Storage Management offers storage data such as available disk space, video, and screen capture, application saved data, and disk use.

6. Error History record every error the system has ever made, complete with time/date values, error descriptions, and error codes.

7. Recent gameplay, achievements, and friend add all examples of recent user activity and individuals on their friend list.

8. Trophies Refer to particular video games and specify the times and dates at which achievements were given.

9. Profile: Personal information, distinctive user handles, and other user-generated material.

10. Friends: Facebook may be connected to a user's friends listed in their Friends list. Is it possible to locate communications between system users and other parties? Requests for real

names can be provided, in which case the user's actual name will appear in all correspondence: 2000 or more pals.

11. Party Messages: With the Party function, a group conversation can include up to 8 individuals.

12. Messages sent and received by one or more users.

Objectives

The methodology was developed to determine whether data could be retrieved from each place. This involves purposefully inserting data into those regions to see if it could be recovered later. Updates to the PlayStation 4's firmware became accessible during the experiment. To determine if there were any adverse effects on the evidence-gathering procedure outlined in the Section, each alteration was noted, implemented, and the experimental technique was repeated.

Forensic Analysis

Methodology for the Sony PlayStation 4's forensic examination that is recommended as best practice

A forensic investigator should take the steps listed below to get the information shown in Table 1:

1. Take out the PlayStation 4 hard disk and make a forensic image of it. Turn off Internet access. The picture might be used to restore at a later time to check the results,

2. Reconnect the hard drive with a write-blocking SATA device that provides a buffer feature (Section 5.8 mentioned using a VOOM Shadow 3 as a man-in-the-middle between the disk and console).

3. Turn on the camera and start the recording. On the PlayStation 4, please turn it on, then sync the DualShock controller.

Please take note of any differences between the PlayStation 4's displayed time and date and the actual time by recording them.

Navigate to and note the information displayed in the following functions:

a. As the analyst may introduce errors during the investigation, it is best to start by looking at the error history.

b. Internet Web Browser - Save recently opened items, bookmarks, and history.

C. Basic Profile Details Party messages,

D. Messages

E. Notifications

F. Error History - Keep track of any mistakes made while investigating.

6. Turn off the PlayStation 4 and the video recording equipment.

It may be acquired on another PlayStation 4 console if the PSN network login credentials are accessible. The investigator must decide whether to put the original system online if it is unavailable. The risk of adopting the old approach is that cached content might be placed online and updated/overwritten current data, even with a write blocker.

Tools used

Tableau T35is write blocker

Offline write blocker test

Given that the Tableau T35is write blocker includes SATA ingress and egress connections, we used it as a man-in-the-middle. We kept the system offline to see what might be gotten just from the hard drive. We could adequately boot the PlayStation 4 and access the in-game menus to view data, unlike Conrad's experiment on the PlayStation 3. The plan, however, became unstable and stopped responding whenever any programs tried to write data to the hard drive (such as

System Storage Management calculating storage capacity). To restart the system, a hard reset was necessary.

During the investigation, it was discovered that certain PSN-dependent aspects would cause system faults to be generated because the system was offline. The system became unstable because the T35is prohibited the mistakes from being recorded in the log.

These results were possible for all firmware releases up to and including 1.62. We discovered that all the PSN regions of the console were now unreachable offline and required connecting to the PSN network after running the experiment during the firmware 1.70 version.

Only information about the Internet web browser and system settings could be recovered during the firmware 1.72 iteration experiment.

Additionally, with firmware 1.75, the write blocker enabled system would correctly boot. Still, any effort to launch the Applications window would cause system instability. Keep the original drive's forensic integrity while allowing the PlayStation 4 to write changes to a buffer.

Relevant findings

A first triage of a PlayStation 4 hard disk using FTK Imager v3.1.1.8 indicated that the disk structure consists of an unidentified filesystem divided into 15 partitions. We'll focus on finding information about the PlayStation 4 by leveraging its native user interface in our investigation.

To recover more files from a forensic image of the PlayStation 4, we used accessdata's Forensic ToolKit (FTK) v3.2's data carving tool. FTK v3.2 is unable to locate any files, as expected. This strongly advises using a customized container format or encryption.

On the web browser for the PlayStation 4, several tests were run. The first examined whether the browser simply records visits to different websites. One hundred three websites were visited during the trial, and different web links were chosen. During the experiment, it was discovered

that in addition to all clicked links, the history of the PlayStation 4's web browser also contains Google search phrases. According to a study of the web browser's history, bookmarks, and most visited pages, the time and date on which events occurred are not accessible through the native interface.

In subsequent tests, photos were stored on the console's hard drive via the Internet web browser. It has been determined that there are only two ways to finish this work successfully. The first is done by saving site images as bookmarks, while the second is by saving screenshots taken with the DualShock 4 controller's share button.

Sony PlayStation 4 system, concentrating on retrieving date and time stamp data. It was found that most features, including Trophies, What's New, and others, offered this data. While the Party and Messages features displayed the dates on which messages were sent and received, programs like the Internet web browser did not show any date or time information.

They attempted to restore the hard disk to the obtained picture captured before powering on the PlayStation 4 after analyzing the device using the user interface. For a forensic examiner to use a previously stored system to confirm their conclusions, it was necessary to test whether the system would accept it. We used the UNIX utility dd to convert our image to RAW before copying it to the HDD. The restored drive was examined using FTK Imager (v3.1.5), establishing that it matched the image file exactly. The console successfully booted the corrected version.

Given that the Tableau T35is write blocker includes SATA ingress and egress connections, we used it as a man-in-the-middle in a method that was. We kept the system offline to see what might be gotten from the hard drive. We could adequately boot the PlayStation 4 and access the in-game menus to view data, unlike Conrad's experiment on the PlayStation 3. The plan,

however, became unstable and stopped responding whenever any programs tried to write data to the hard drive (such as System Storage Management calculating storage capacity). To restart the system, a hard reset was necessary.