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

ABSTRACT

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