Forensic Analysis of a Sony PlayStation 4 - A First Look

By

Allen Davies, Huw Read, Konstantinos Xynos and Iain Sutherland

Presented At

The Digital Forensic Research Conference

DFRWS 2015 EU Dublin, Ireland (Mar 23rd- 26th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

University of South Wales
Prifysgol De Cymru

SYTECH
DIGITAL FORENSICS

noroff
UNIVERSITY COLLEGE

Mr. Matthew Davies
Dr. Huw Read
Dr. Konstantinos Xynos
Prof. Iain Sutherland

Forensic analysis of a Sony PlayStation 4: A first look

DFRWS 2015

$ whoami

Presenter:
Matt Davies - Digital Forensic Analyst
Sytech Digital Forensics
Email: matt.davies@sytech-consultants.com
Company website: sytech-consultants.com
Tel: (01782) 286 300
Fax:(01782) 280 306

Dr. Huw Read - Senior Lecturer
University of South Wales
Email: huw.read@southwales.ac.uk
Tel:(01443) 654 287

Are games consoles are just toys?

- Former Walt Disney World employee arrested on Xbox child porn charges
- Milford cops say threat made through Xbox
- Couple left sickened over child porn sent to Xbox
- PlayStation sex crime: criminal used video game to get girl's naked pictures
- Police: Xbox used to lure girls
- Mississippi deputy fired over threatening Xbox live players
- Prisoners using PlayStation 3s to commit crimes

Raison d'être

- Games Consoles each have their own unique architecture and operating systems.
- In addition, manufacturers such as Sony and Microsoft utilise encryption standards.
- How do we conduct an analysis of an encrypted PlayStation 4 in a forensically sound manner, without circumventing security measures?

Objectives of Research

1. Are methodologies used in 7th generation consoles relevant to 8th generation systems?
2. What forensically sound acquisition methods are available?
3. What avenues of interest exist on the PlayStation 4?
4. What artefacts can be obtained from online/offline analysis?

Previous Work

- Vaughan (2004) – Microsoft Xbox
- Burke & Craiger (2007) - Microsoft Xbox
- Turnbull (2008) – Nintendo Wii
- Xynos et al (2010) – Microsoft Xbox 360
- Conrad et al (2010) – Sony PlayStation 3
- Ridgewell (2011) – Networked Game Devices
- Moore et al (2013) – Xbox One

Features of Interest

- PlayStation Network (PSN)
- Sony Entertainment Network (SEN)
- Internet Browser
- ShareFactory
- System Storage Management
- Error History
- What's New
- Trophies
- Profile
- Friends
- Party Messages
- Messages

Empirical Analysis

The experiment was carried out on firmware 1.01, 1.50, 1.51, 1.52, 1.60, 1.61, 1.62, 1.70, 1.72, 1.75 and 1.76 as follows.

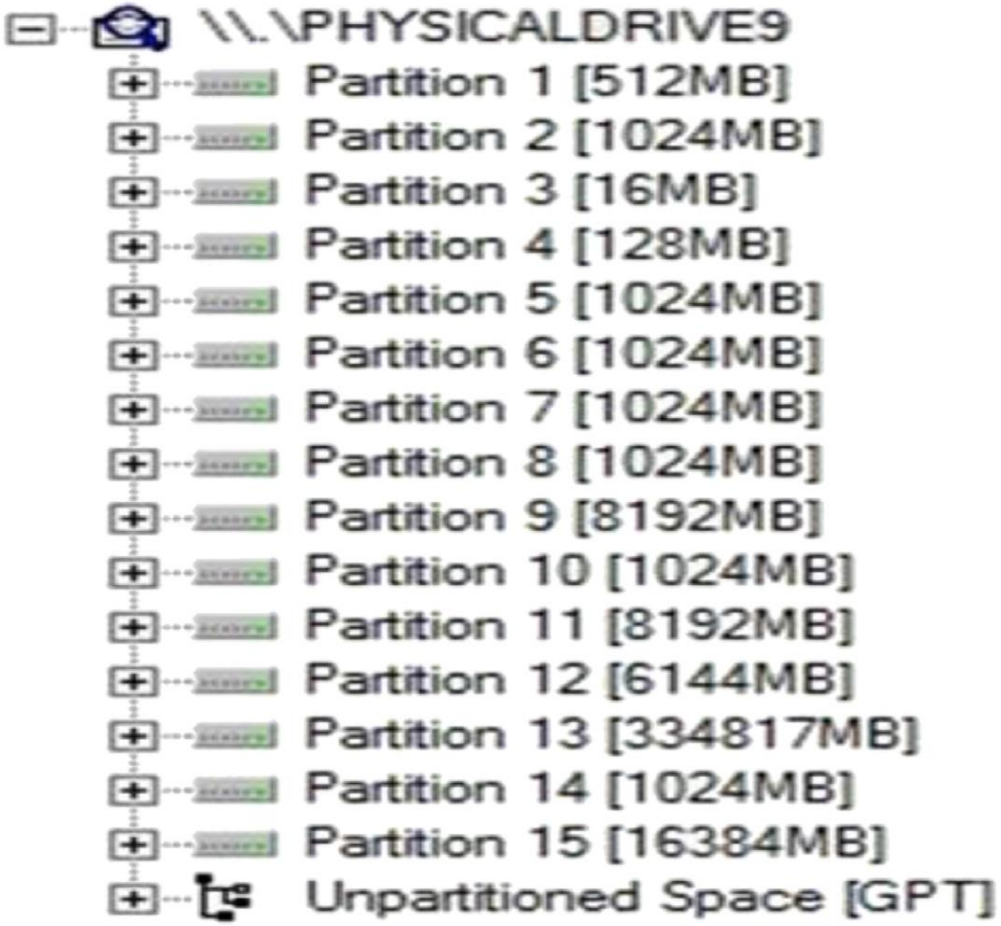
- Activate video capture device, record time.
- Activate PlayStation 4. Record time as set on console.
- Introduce sample dataset, record time and data introduced.
- Turn off PlayStation 4. Deactivate video capture device, record time.
- Forensically image PlayStation 4 hard drive.
- Turn on PlayStation 4; investigate to identify user actions introduced during this experiment iteration.
- Compare the data retrieved in relation to the data introduced.

Test Data

The following sample data was used for each firmware iteration:

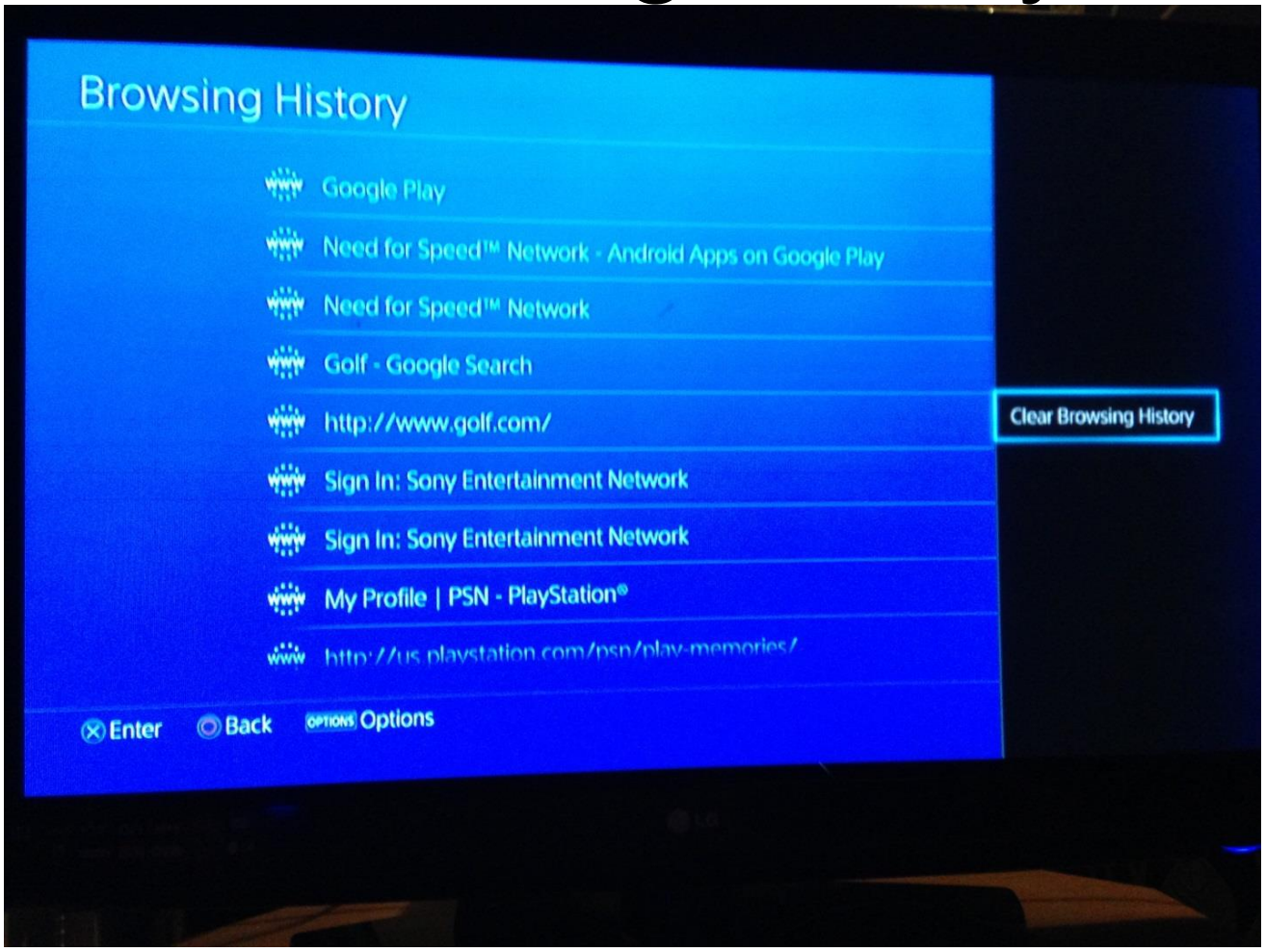
- Three offline (local) accounts: User1, User2, User3
- Two online accounts: PlayStation Network (PSN) account & PlayStation Plus
- “Friends List” contacts added to assess communication options
- Facebook account created to enable “ShareFactory” functionality
- Error History, Internet Browse URLs (Bookmarks, websites)

Initial Findings



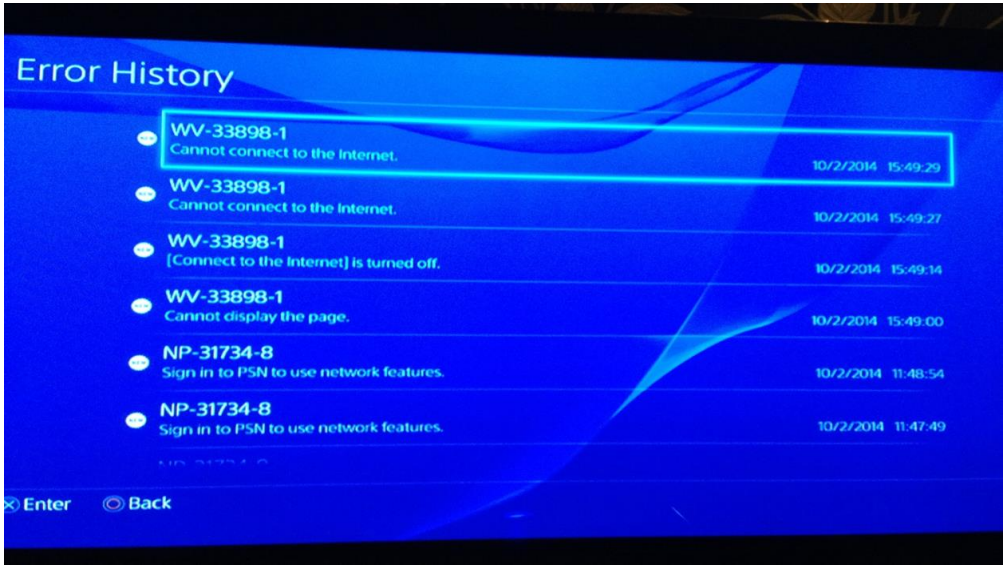
Internet Browser

Browsing History

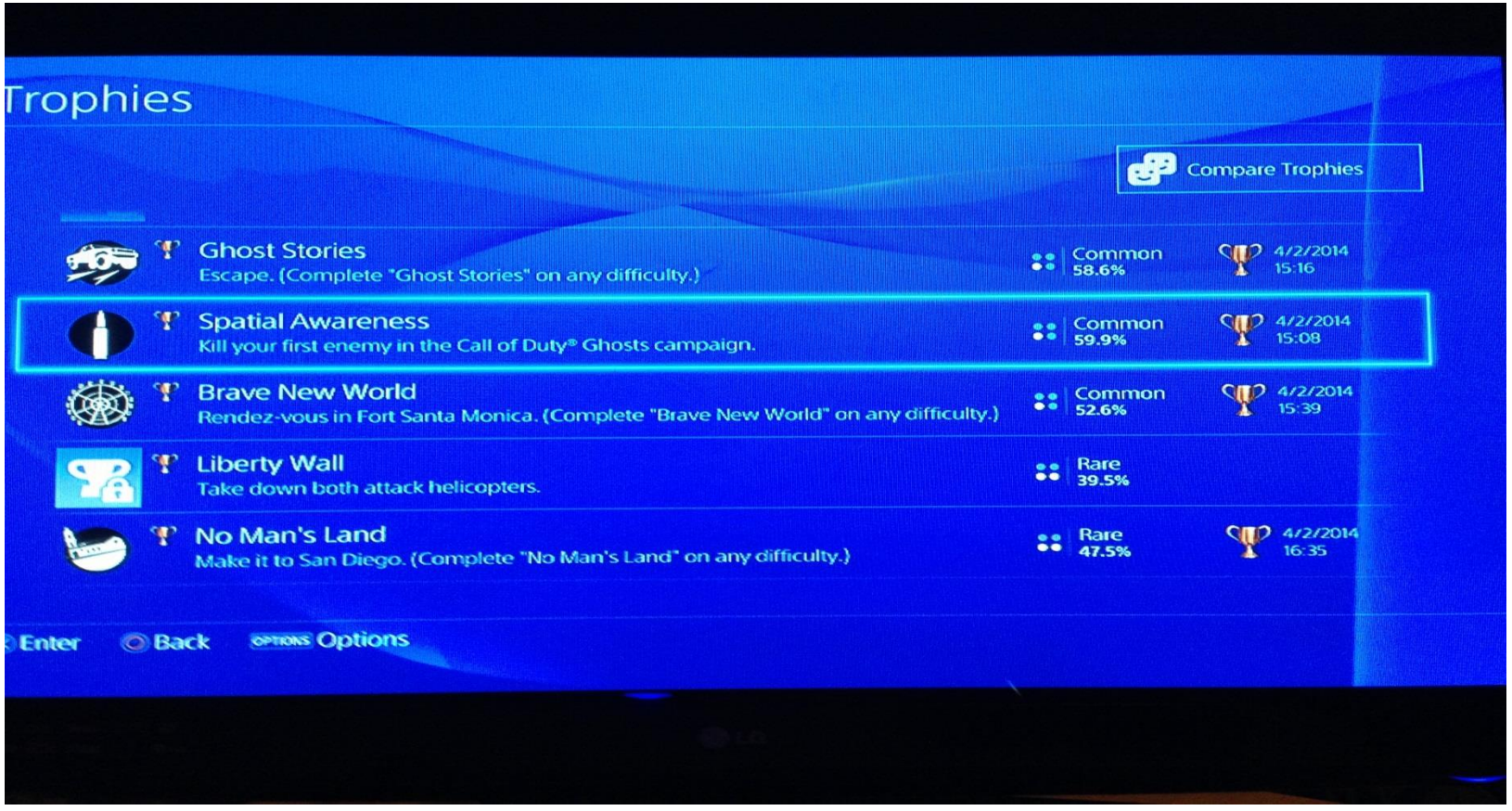


Error History

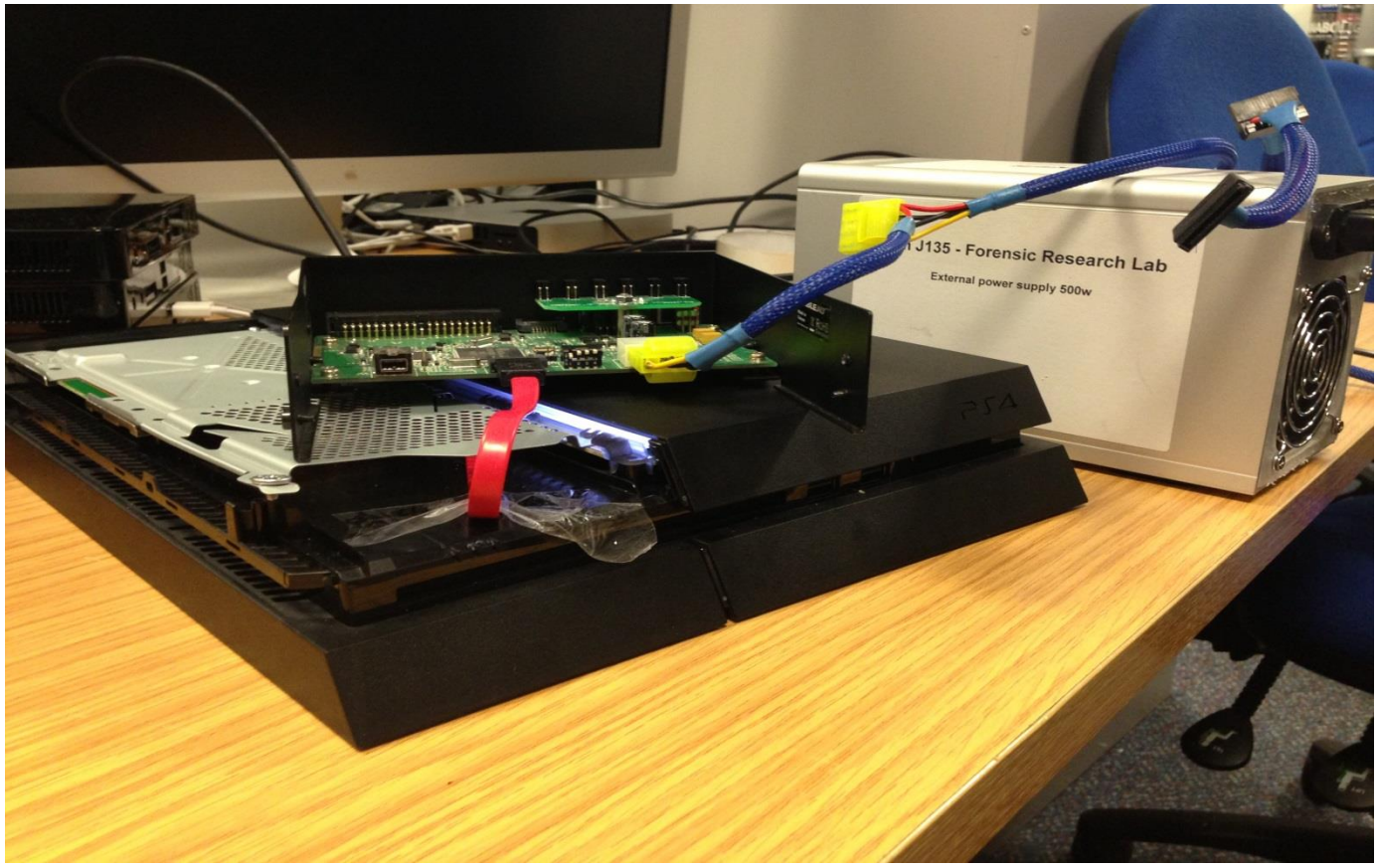
Error History - The Error History should be viewed first as errors may be introduced by the analyst during the investigation.



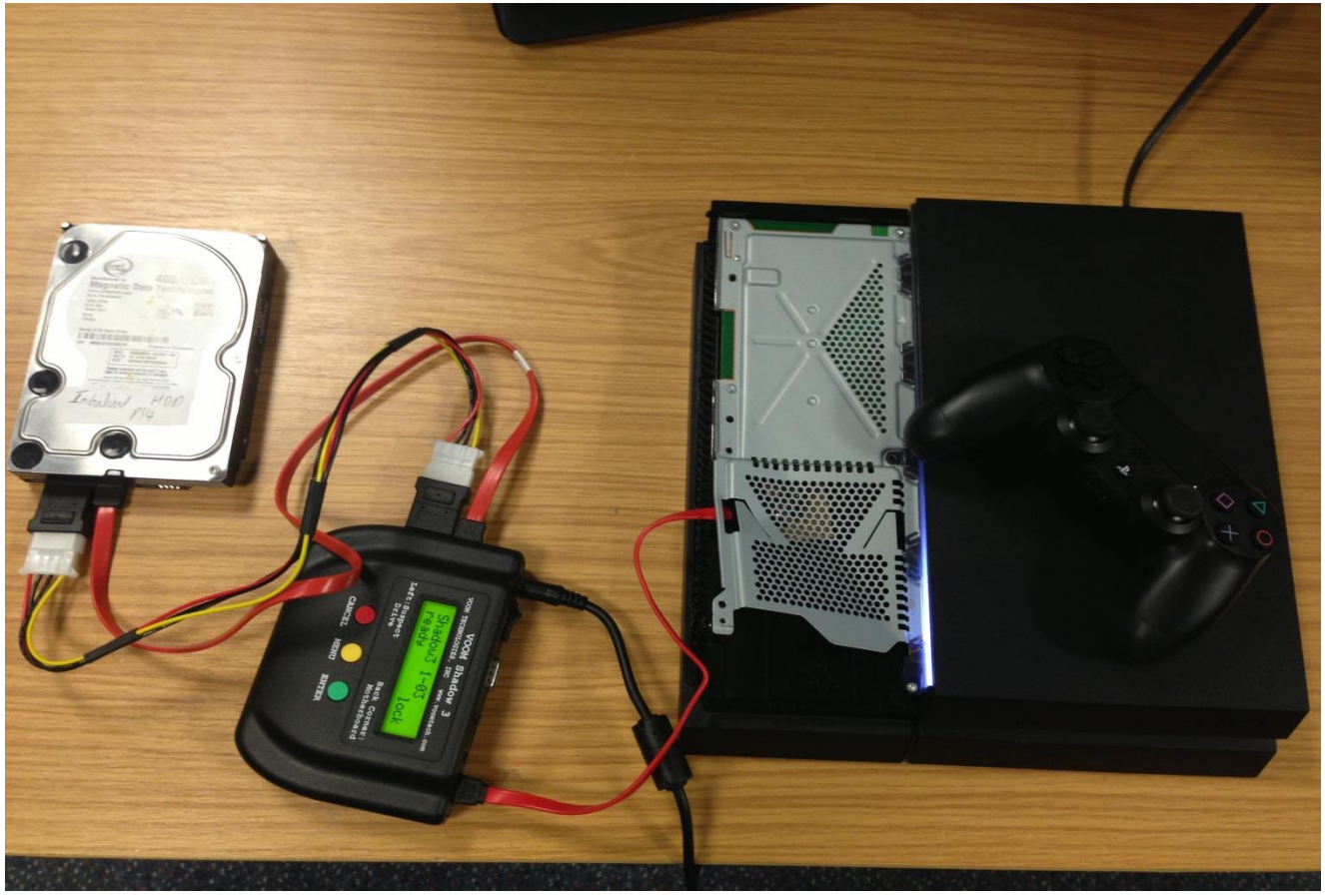
Trophies


Trophies
Compare Trophies
Ghost Stories
Escape. (Complete "Ghost Stories" on any difficulty.)
Common
58.6%
4/2/2014
15:16
Spatial Awareness
Kill your first enemy in the Call of Duty® Ghosts campaign.
Common
59.9%
4/2/2014
15:08
Brave New World
Rendez-vous in Fort Santa Monica. (Complete "Brave New World" on any difficulty.)
Common
52.6%
4/2/2014
15:39
Liberty Wall
Take down both attack helicopters.
Rare
39.5%
No Man's Land
Make it to San Diego. (Complete "No Man's Land" on any difficulty.)
Rare
47.5%
4/2/2014
16:35
Enter
Back
OPTIONS Options

Write Blocker - Tableau



Write Blocker - Shadow Drive



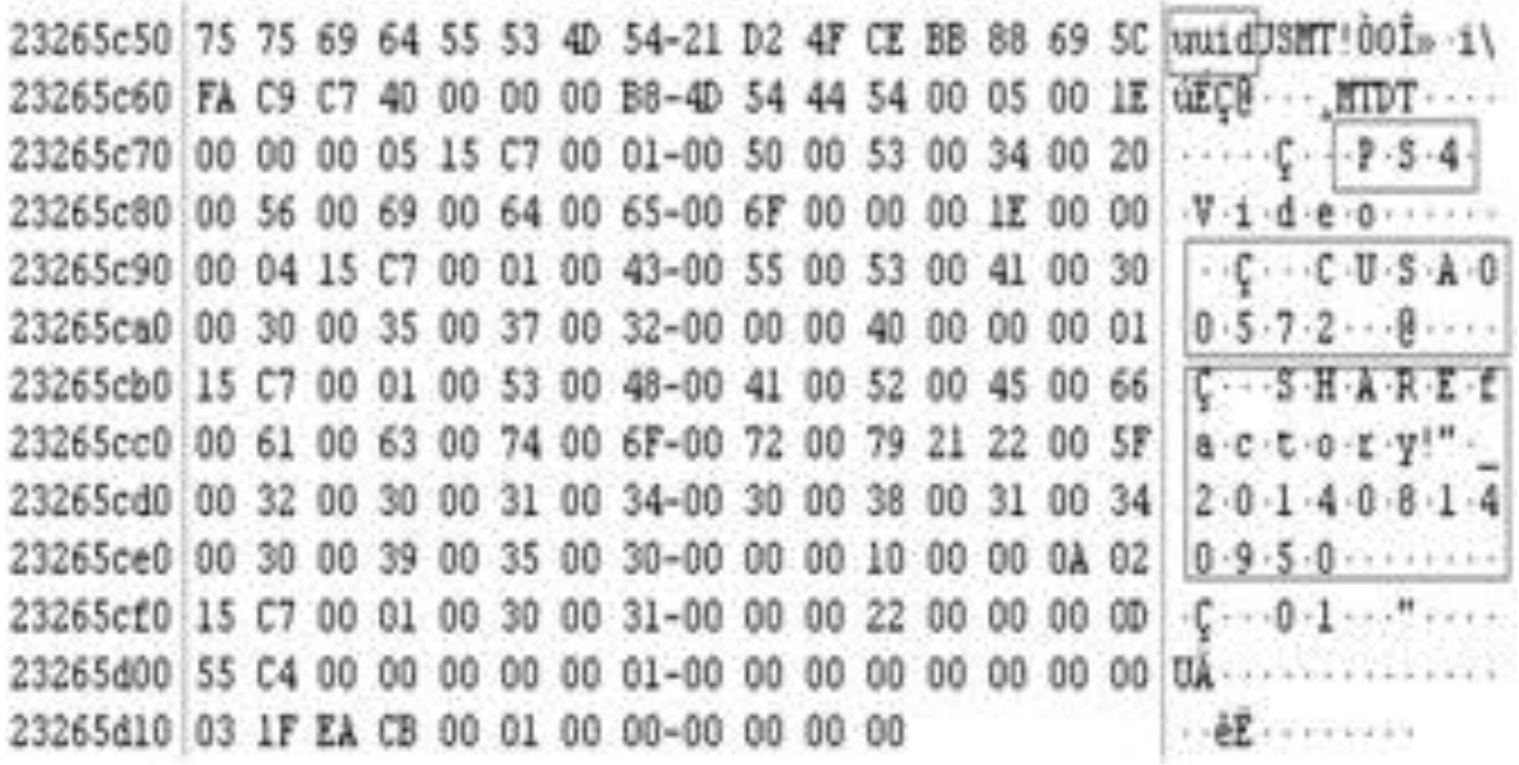
Jpeg Extraction

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)

MP4 Extraction



```
23265c50 75 75 69 64 55 53 4D 54-21 D2 4F CE BB 88 69 5C  uuidUSMT!ÒOÎ»·i\
23265c60 FA C9 C7 40 00 00 00 B8-4D 54 44 54 00 05 00 1E  úÉÇ@···¸MTDT····
23265c70 00 00 00 05 15 C7 00 01-00 50 00 53 00 34 00 20  ·····Ç···P·S·4·
23265c80 00 56 00 69 00 64 00 65-00 6F 00 00 00 1E 00 00  ·V·i·d·e·o·····
23265c90 00 04 15 C7 00 01 00 43-00 55 00 53 00 41 00 30  ···Ç···C·U·S·A·0
23265ca0 00 30 00 35 00 37 00 32-00 00 00 40 00 00 00 01  0·5·7·2···@····
23265cb0 15 C7 00 01 00 53 00 48-00 41 00 52 00 45 00 66  ·Ç···S·H·A·R·E·f
23265cc0 00 61 00 63 00 74 00 6F-00 72 00 79 21 22 00 5F  ·a·c·t·o·r·y!"·_
23265cd0 00 32 00 30 00 31 00 34-00 30 00 38 00 31 00 34  ·2·0·1·4·0·8·1·4
23265ce0 00 30 00 39 00 35 00 30-00 00 00 10 00 00 0A 02  ·0·9·5·0······
23265cf0 15 C7 00 01 00 30 00 31-00 00 00 22 00 00 00 0D  ·Ç···0·1···"····
23265d00 55 C4 00 00 00 00 00 01-00 00 00 00 00 00 00 00  UÄ··············
23265d10 03 1F EA CB 00 01 00 00-00 00 00 00              ··êË········
```

Offline Analysis

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.

Online Analysis

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.

Summary

- Best practice methodology developed.
- Evidential integrity maintained.
- Offline vs. online considerations.
- Future firmware updates will continue to challenge investigators.

Future Work

PlayStation Camera

- The PlayStation camera enables users to utilise enhanced security features such as facial recognition login. Can this be used to prove ownership, can we use a picture etc. of suspect to make system unlock?

PlayStation Vita & PS4

- The implications of the PlayStation Vita when linked to the PS4. The PS Vita enables users to remotely access and control their PlayStation 4. Evidence of usage and communication?

PlayStation Companion App - Phones & Tablets

- The PlayStation Companion App is compatible with both modern smart phones and tablets and can be used to gain remote access of the PlayStation 4.

Questions?

Presenter:
Matt Davies - Digital Forensic Analyst
Sytech Digital Forensics
Email: matt.davies@sytech-consultants.com
Company website: sytech-consultants.com
Tel: (01782) 286 300
Fax:(01782) 280 306

Dr. Huw Read - Senior Lecturer
University of South Wales
Email: huw.read@southwales.ac.uk
Tel:(01443) 654 287