Forensic Analysis of Xbox One

Ying Zhang\textsuperscript{a}, Feng Gao\textsuperscript{b}

The Third Research Institute of Ministry of Public Security Shanghai, China
\textsuperscript{a}zhangying@stars.org.cn, \textsuperscript{b}gaofeng@stars.org.cn

Abstract. With the development of internet technology, more and more people turn their attention to video game consoles to release pressure. There are several famous video game console manufacturers on the market currently, including Microsoft, Sony and Nintendo. Xbox one is one of those popular game consoles which was published by Microsoft. Nevertheless, seldom researchers focus on analysis of its operation system, file system and data. In this paper we are going to analyze the file system, data on hardware, network data and so on of Xbox one concretely.

1. Introduction

Xbox one is the eighth generation home video game consoles developed by Microsoft, which was announced in 2013. It is the successor to Xbox 360 and the third console in the Xbox family [1]. It has attracted wide attention since its release and occupied majority of user market rapidly. According to the statistics data from HIS Markit, the global install base of Xbox one has reached 39.1 million till 2018 [2]. Despite its PowerPC-based predecessor, one of the characteristics of Xbox One is its shift back to the x86 architecture utilized in the original Xbox [1]. In other words, Xbox one is no longer viewed as single gaming consoles but rather as portable machines containing operating system.

Previous research has shown that this console has been utilized in criminal activities including identity theft, child pornography, economic fraud and so on [3]. That means, Xbox one is supposed to be examined and analyzed in detail as evidence, aiming to seek potential clues regarding the crime. In this paper we will start from a new console and perform various operations to this machine. Forensic image is conducted for each operation in order to record slight modifications. After the completion of all operations, file system, date on hardware, network date and other information would be examined and analyzed in detail.

2. Methodology

2.1. Hard Driver Disk Analysis

In order to examine concrete structure and data in Xbox one, we put emphasis on hard disk drive analysis. As described above, image is conducted in each step and supposed to be analyzed via profession tools. Details about each step will be demonstrated as follow.

Phase 1. The hard disk drive is removed from a brand-new gaming console and forensically imaged while using a write-blocker. When it is completed, the image is named ‘xbox_one_1.001’ to distinguish it from others. After that, we put the drive back to console and turn it on. It is critical to check whether there is any default content in user interface.
Phase 2. In operation interface, we restored the console to factory settings and turn off the machine. The hard disk drive is removed and forensically imaged as well. When it is completed, the image is named ‘xbox_one_factory_settings.001’ to mark its situation.

Phase 3. We put the drive back and turn on the machine. In user interface, wifi information is configured to gaming console. That means the console is allowed to connect to internet. According to instructions, the console is restarted so as to ensure configuration works. Then the hard disk drive is imaged and named ‘xbox_one_wifi_logon.001’.

Phase 4. In this step, user account is supposed to be log on. This operation is conducted to enable communications between various users. Besides that, user account is required in Xbox live configuration as well. Then the hard disk drive is imaged and named ‘xbox_one_user_logon.001’.

Phase 5. System update will be performed in this step. This operation is conducted to enable operating system works and prevent the console from lack of system files. Then the hard disk drive is imaged and named ‘xbox_one_system_update.001’.

Phase 6. Game installation will be performed next. Considering the necessity of analysis, one popular game Fallout 4 will be installed on the gaming console, including setting up and updating. Then the hard disk drive is imaged and named ‘xbox_one_game_installation.001’.

Phase 7. After installation, user can start playing Fallout 4. Concretely speaking, configuration and performing would be conducted in the step. Then the hard disk drive is imaged and named ‘xbox_one_game_running.001’.

2.2. Network Traffic Analysis
It is known to all that Xbox one could be used in an online environment. That means, the network interaction between gaming consoles and related servers is critical for investigators. Details of network data capture and analysis will be demonstrated as follow.

Connect test laptop to internet via Ethernet cable firstly. Then portable wifi is inserted to laptop through USB interface.

Install relevant programs of portable device in laptop. After that, above program is executed to commit wireless network configuration, including ID and password. Above operations aim to share network in wireless way. In this situation, only Xbox One is connected to wireless network, making it easy to capture sent and received network packages.

Professional tool in laptop such as Wireshark is utilized to record network packages when playing Fallout 4.

3. Image Description
As described in previous chapters, we removed hard disk drive from console, restored to factory settings, logged on network and user account, updated system, installed game and played it successively. Various images were conducted so as to record slight modification in drive. Details are demonstrated in table 1.

| Name                          | Description               | Created Time |
|-------------------------------|---------------------------|--------------|
| xbox_one_1.001                | new machine               | 2016/12/23   |
| xbox_one_factory_settings.001 | restore to factory settings | 2017/10/12   |
| xbox_one_wifi_logon.001       | wireless network log on   | 2017/10/20   |
| xbox_one_user_logon.001       | user log on               | 2017/10/23   |
| xbox_one_system_update.001    | system update             | 2017/10/24   |
| xbox_one_game_installation.001| game installation         | 2018/08/17   |
| xbox_one_game_running.001     | play game                 | 2018/08/17   |

Information including hash value and created time is recorded, which helps users analyzing system file in follow chapters. Besides that, we would conduct comparison between different images from the
point of partition structure, partition size, created time, modified time, file structure, file type, properties and so on. Generally speaking, more details would be demonstrated in following chapters from multiple aspects.

4. Partition Layout
It is found that the hard disk drive is constituted of five partitions and one unpartitioned space via analyzing all images listed above. Details are listed in Table 2.

| Number | Partition          | File System | Size (GB) |
|--------|--------------------|-------------|-----------|
| 1      | Temp Content       | NTFS        | 41.0      |
| 2      | User Content       | NTFS        | 365       |
| 3      | System Support     | NTFS        | 40.0      |
| 4      | System Update      | NTFS        | 12.0      |
| 5      | System Update 2    | NTFS        | 7.0       |
| 6      | Unpartitioned Space| GPT         |           |

According to the examination, the partition layout is quite close in all images. In other words, there are the same partitions in the hard disk drive whatever their phase for one console. Take image ‘xbox_one_1.001’ for example, fig. 1 shows concrete information for each partition.

5. Partition and File Analysis
After a preliminary examination, we could find that Xbox one utilizes a special operating system instead of a regular one such as Windows or Linux. Furthermore those files in each partition seem to be encrypted and difficult to be analyzed. Nevertheless we will conduct research from another point of view as showed next.

In order to find file modifications at different phases, we calculate SHA 256 hash digests for each file. Concretely speaking, we calculate hash value for all files of each partition originating from above 7 images.
5.1. Temp Content
The file structure of this partition is relatively fixed, including $Bitmap, $Boot, $sosrst.xvd and so on. Take image ‘xbox_one_1.001’ and ‘xbox_one_factory_settings.001’ for example, fig. 1 shows timestamps modification for each file.

**Figure 2. Timestamps.**

According to fig. 2, the creation time of all files under root directory is May 26, 2013 to a new console, while the creation time turns to September 2, 2014 for the restored one. It is speculated that there is a special system version to new console, which is generated in May 26, 2013. And restoration allows consoles to retrieve back to a relatively close version.

In addition, there are 3 more files called AppTempStorage, AppuserStorage and ConnectedStorage-retail in phase 1, while 1 more files called DeploymentSoftwareDistribution.xvd in phase 2. ConnectedStorage-retail disappears in phase 2 and does not help in discerning its function. But based on its name, we presume that this file is created for storage connection, such as a portable drive to console’s USB port, or other expansions for the machine. Similarly, it is speculated that Deployment Software Distribution.xvd is used for software management.

A new format called XVD is found during the examination. Previous research [4] assumed it is abbreviation of Xbox Virtual Disk. There are a lot of speculation about definition of XVD in Xbox community [5]. Jailbreakers have been analyzing this type since its release and giving various opinions. Some people treat it as modified Windows image, while others consider it as a brand-new format developed by Microsoft.
5.2. User Content
Like Temp content, this partition is constituted of fixed files as well, including $Bitmap, $Boot and $UpCase. Take image ‘xbox_one_system_update.001’ and ‘xbox_one_.

Game installation.001’ for example, there are 4 more files after game installation, called E4EAB7AC-7E08-4571-8BE1-CA99D2C75D45, e4eab7ac-7e08-4571-8be1-ca99d2c. 75d45.22c21d21-1f1b-46b5-916a-a0d690ae61e1, e4eab7ac-7e08-4571-8be1-ca99d2c75d45.de37e6d6-559b-40b0-b1ad-ba2779fbeb4 and Microsoft.Avatars_8wekyb3d8bbwe. UWA.

As shown above, those files are named after strings of hexadecimal digits [3]. It is impossible to obtain any clues form file name. Nevertheless, those strings could be treated as part of metadata, considering their size and timestamps.

According to previous description, we only installed Fallout 4. It is speculated that above files could probably be configuration files for the game itself. We started installing Fallout 4 at 10:44 am August 17, 2018, which is coincident with creation time of above files. Besides that, the size of Fallout 4 is 26.8GB, which is quite close to file E4EAB7AC-7E08-4571-8BE1-CA99D2C75D45. And all three files listed above owns the same ID ‘E4EAB7AC-7E08-4571-8BE1-CA99D2C75D45’.

Therefore, file E4EAB7AC-7E08-4571-8BE1-CA99D2C 75D45 is the video game itself as far as we are concerned. In addition, other files with the same ID are possibly game-related configuration files.

5.3. System Support
This partition is constituted of fixed files, including folder controllers, oddfwupd and file $Bitmap, $Boot and cms.xvd. Take image ‘xbox_one_game_installation.001’ and ‘xbox_one_game_running.001’ for example, there are 2 more files after game running, called working.pfm and eram.bin. Undoubtedly they are relevant to game execution. In addition, timestamps of file E4EAB7AC-7E08-4571-8BE1-CA99D2C75D45.xct and E4EAB7AC-7E08-4571-8BE1-CA99D2C75D45.xvi are modified with game running, which confirms previous speculation.

5.4. System Update
This partition is constituted of fixed files, including folder $Extend, A, B and file $Bitmap, $Boot and updater.xvd. Based on its name, we presume that this partition is used for system updation. Take image ‘xbox_one_user_logon.001’ and ‘xbox_one_system_update.001’ for example, table 3 shows hash value modification for each file.
According to table 3 and other analysis, the modified time of updater.xvd is changed to October 23, 2017, which is consistent with system update time.

5.5. System Update 2
This partition is constituted of fixed files, including folder $Extend and file $Bitmap and $Boot. Take image ‘xbox_one_game_installation.001’ and ‘xbox_one_game_running.001’ for example, it is found that no files change except of $LogFile.

6. Network Package Examination
No username, password or account information were found after analyzing network package. However, we find some packages concerning DNS protocols, which are shown in fig. 3
Figure 3. Packages of DNS Protocol

Via analyzing those packages, it seems that game consoles issues NDS parsing requests regarding Xbox Live logon, related information access and Xbox Live configuration. Besides that, we also notice that game console has issued parsing requests to a website called ‘Bethesda.net’ as well. After
validation, it is an American game publisher, which is responsible for development of Fallout 4. Moreover, we synchronized user data through Xbox Cloud. By comparing respective data, we can find that game console keep sending requests to Xbox Live server so as to obtain relevant data.

7. Summary
As the eighth generation of video game console, Xbox one has highly recommended for its quality since its release. Unfortunately, it is also utilized in illegal and criminal events due to its special characteristics. In this paper we demonstrate concrete analysis of Xbox one, including operation system, file system, format and data. Concrete analysis has been revealed in this paper, including partition layout, partition content and special file distributed there.

Considering the above factors, it is expected that more research would be concentrate on special data format, file and network packages. And new Xbox series are supposed to be analyzed in the future.

Acknowledgments
This paper is supported by National key research and development plan, The People’s Republic of China ministry of science and technology, project number: 2017YFC0803805.

References
[1] Information on https://en.wikipedia.org/wiki/Xbox_One
[2] Information on http://games.qq.com/a/20180614/031775.htm?p=1
[3] Jason Moore, Ibrahim Baggili, Andrew Marrington, Armindo Rodrigues, Preliminary forensic analysis of the Xbox One, in: Digital Investigation 11, 2014, S57-S65.
[4] Information on http://xbox-emulation.dcemu.co.uk/
[5] Information on http://bbs.wfun.com/forum-xboxone-1.html